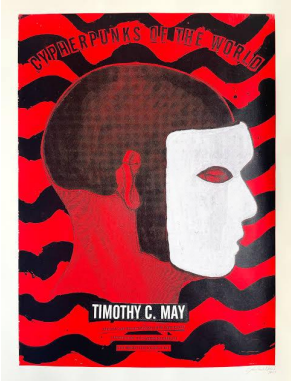
The Cyphernomicon



Tradução : iamcais , Alex emidio.

1. Introdução

1.1. direitos autorais
O CYPHERNOMICON: Cypherpunks FAQ e Mais, Versão 0.666,
1994-09-10, Direitos De Autor Timothy C. De Maio. Todos os direitos reservados.
Veja os detalhes de isenção de responsabilidade. Use seções curtas em "justo
use" disposições, com crédito apropriado, mas não coloque o seu
nome em minhas palavras.

1.2. Prefácio
- O Cypherpunks ter existido desde setembro, 1992. Em que
tempo, uma grande quantidade foi escrito sobre criptografia, chave
depósito, Clipper, a Net, a auto-estrada da Informação, cibernética
terroristas, e criptografia de anarquia. Nós encontramos a nós mesmos (ou
placed nós mesmos), no centro da tempestade.
- Este FAQ pode ajudar a preencher algumas lacunas sobre o que estamos
a respeito, o que nos motiva, e para onde estamos indo. E talvez
alguns conhecimentos úteis sobre a criptografia, remetentes, o anonimato,
dinheiro digital, e outras coisas interessantes.
+ As Questões Básicas
+ Grande Divisão: de privacidade vs. conformidade com as leis
+ liberdade de expressão e a privacidade, mesmo se significa que alguns criminosos
não pode ser pego (um stand a Constituição dos EUA foi
fortemente em favor de, em um momento)
- a casa de um homem é seu castelo...a essência da Magna
Carta sistemas de...direitos do indivíduo para ser seguro
a partir de revistas aleatórias
+ ou invasivo táticas para capturar os criminosos, regular

comportamento e controle de população
- as necessidades legítimas para exigir o cumprimento de leis, para responder a situações
+ isso é um paralelo com o problema de auto-proteção vs.
proteção por lei e a polícia
- como se viu no debate arma
- crypto = armas no sentido de ser um indivíduo
preventivo de proteção
- passado o ponto de não retorno
- Forte de criptografia como material de construção para uma nova era
+ O transnacionalismo e o Aumento do número de Graus de Liberdade
- os governos não podem esperança de controlar os movimentos e
comunicações dos cidadãos; as fronteiras são transparentes
+ Nem todos os membros da lista de compartilhar todos os pontos de vista
- Isso não é "Oficial Cypherpunks FAQ." Não há tal coisa
podem existir. Este é o FAQ eu queria escrito. Pontos de vista
expressas são de minha autoria, com o máximo de entrada de outros, como
muito consenso, como eu posso controlar. Se você deseja radicalmente
diferentes FAQ, escreva-o de si mesmo. Se você não gosta deste
FAQ, não leiam. E dizer a seus amigos para não lê-lo.
Mas não compromete o desempenho do meu caixa de correio, ou a 500 outros no
lista, com mensagens sobre como você poderia ter redigido Seção
12.4.7.2 de forma ligeiramente diferente, ou como Seção 6.9.12 não
não refletir completamente as suas opiniões. Por razões óbvias.
- Todas as FAQs são produtos de um autor principal, por vezes, de
um comitê. Para esta FAQ, eu sou o único autor. Pelo menos
da versão que você está lendo agora. Versões futuras podem
tem mais a entrada de outros, embora isso me deixa nervoso
(Sou a favor de novos autores a escrever seu próprio material, ou utilizar
links de hipertexto, ao invés de tomar a minha escrita básica e
anexar o seu nome-é verdade que eu inclua o
citações de muitas pessoas aqui, mas eu fazê-lo explicitamente
citando o trecho que escreveu....vai ser difícil
para os autores posteriores marcar claramente o que a Tim Pode escreveu
sem sobrecarregar excessivamente o texto. Os revisionistas do
dilema.
- A lista tem um monte de radicais, libertários, alguns anarco-
os capitalistas, e até mesmo alguns socialistas
- Principalmente relacionados com o computador pessoal, como pode ser esperado. (Há
alguns cientistas políticos, eruditos clássicos, etc.
Até mesmo alguns atual ou ex-advogados.)
+ Posso Falar para as pessoas?
- Como eu disse, não. Mas às vezes eu fazer declarações sobre o que

"a maioria de" lista de membros acreditam, que "muitos" acredito, ou o que
"alguns crêem".
- "Mais" é o meu melhor julgamento, do que a maioria acredita,
pelo menos o vocal maioria Cypherpunks discussões
(no físico reuniões, festas, etc.) e no
A lista. "Muitos" significa menos, e "alguns" menos ainda. "Poucas"
significa uma distinta minoria. Note que este é o
últimos 18 meses de actividade (para não enviar
esclarecimentos agora para tentar "influenciar o voto").
- Em particular, alguns membros podem ser bastante desconfortável
sendo descrita como anarquistas, criptografia anarquistas, dinheiro
lavadores, etc.
+ Meus comentários não agradar a todos
- em quase todos os pontos já apresentados, alguns têm discordado
- lutas, batalhas, chamas, idee correções
- em questões que vão desde o controle de armas a Dolphin para Criptografar
vários animal de estimação teorias realizada caro
- Alguém já fez um mundano piada sobre pseudônimos sendo
como transtorno de personalidade múltipla, e uma chama voltou
dizendo: "isso não é engraçado. Eu sou MPD, e o meu é ASSIM o MPD.
Por favor, pare imediatamente!"
- não pode ser ajudado....pode não apresentar todos os lados para todos os argumentos
+ Foco deste documento está centrada no mercado AMERICANO, por várias razões
- a maioria na lista são dos estados unidos, e eu estou na EUA
- NSA e criptografia comunidade é, em grande parte centrado nos EUA,
com alguns Europeia forte atividades
- A lei dos EUA é susceptível de influenciar no exterior lei
+ Estamos em uma bifurcação na estrada, uma Grande Divisão
- Vigilância vs. Liberdade
- nada no meio...forte de criptografia e privacidade
fortemente limitado, ou coisas que eu descrever aqui vai ser
feito por algumas pessoas....daí o "tombamento fator" aplica-se
(ponto de não retorno, cavalos do celeiro)
+ Eu não fazem nenhuma reivindicação para falar "para o grupo." Se você está
ofendido, escrever a sua própria FAQ. Meu foco em coisas vagamente
chamado de "crypto anarquia" é apenas isto: meu _focus_. Este foco
naturalmente, se infiltra em algo como este FAQ, basta
como alguém mais interessados na mecânica do PGP seria
dedicar mais espaço para PGP problemas que eu tenho.
- Gary Jeffers, por exemplo, dedica a maior parte de sua "CEB" para
questões em torno da PGP.
+ Vai deixar de fora alguns dos altamente detalhada de itens de...
- Clipper, FOLHA, custódia, Tocas, etc.

uma miríade de programas de criptografia, a granel, cifras, variantes no
PGP, etc. Alguns desses que listei...os outros eu tive a
jogue as mãos e simplesmente ignorar. (Manter o controle de
zilhões de versões para dezenas de plataformas...)
- fácil se perder nos detalhes, enterrado na besteira

1.3. Motivações
1.3.1. Com tanto material disponível, por outro FAQ?
1.3.2. Sem acesso conveniente aos arquivos da lista....e quem poderia
ler 50 MB de coisas de qualquer maneira?
1.3.3. Por que não a Internet? (Mosaico, Http, URL, etc.)
- Por que não navegável documento da Web?
- Isso está se tornando moda. Muitas URLs estão incluídos aqui, em
verdade. Mas fazendo todos os documentos em documentos da Web tem
desvantagens.
+ Razões por que não:
- Não há acesso fácil para mim.
- Muitos outros, a falta de acesso. O texto ainda regras.
- Não, de todo claro que uma coleção de centenas de
fragmentos é útil
- Eu gosto do estruturada editores disponíveis no meu Mac
(especificamente, MAIS, uma estrutura de tópicos editor)
-
1.3.4. Quais os Pontos Essenciais São
- É fácil perder a noção de que os problemas principais são, o que
o que realmente importa pontos. Em um FAQ como este, um grande
quantidade de "sujeira" é apresentado, isto é, uma vasta quantidade de
diversos, tangencial, e epifenomênicas material.
Nomes de PGP versões, variantes no steganograhy, e outros
tais coisas, tudo o que vai mudar nos próximos
meses e anos.
+ E ainda é, em parte, o que é um FAQ é para. A chave é apenas
para não perder o controle das ideias-chave. Eu já mencionei que eu
acho que são importantes ideias muitas vezes. A saber:
- que muitas abordagens para criptografia existe
- que os governos, essencialmente, não pode deixar de a maioria destes
abordagens, falta de estabelecimento de um estado policial (e
provavelmente não é mesmo)
- núcleo de questões de identidade, autenticação, pseudônimos,
a reputação da empresa, etc.

1.4. Quem Deve Ler Este
1.4.1. "Eu deveria ler isso?"

- Sim, de ler isso vai apontar para outras fontes de
informações, irá responder as perguntas mais freqüentes,
e vai (espero) a cabeça fora do reaparecimento do mesmo
cansado de temas a cada poucos meses.
- Use uma ferramenta de busca, se você tiver um. O Grep para as coisas que
de seu interesse, etc. A granularidade de este FAQ não
se presta para a Web de conversão de, pelo menos não com presentes
as ferramentas.
+ O que _Won é Ser Coberto Aqui
+ básico de criptografia
+ muitos bons textos, perguntas frequentes, etc., escrito por tempo integral
estudando criptografia e educadores
em particular, algumas das idéias não são simples, e
tomar várias páginas de bem escrito texto para obter o
ponto
- de não ser o foco deste FAQ
- política básica rants

1.5. Comentários sobre Estilo e Rigor
1.5.1. "Porque é que este FAQ não em forma de Mosaico?"
- porque o autor (tcmay, como de 7/94) não tem Mosaico
de acesso, e mesmo se fizesse, não seria, necessariamente,....
- linear do texto ainda é bom para algumas coisas...pode ser lido em
todas as plataformas, podem ser impressos, e pode ser pesquisado com
padrão grep e ferramentas semelhantes
1.5.2. "Por que a mistura de estilos?"
+ Existem três tipos principais de estilos aqui:
- Padrão de prosa seções, explicando algumas ponto ou listagem
coisas. Mini-ensaios, como a maioria dos posts para Cypherpunks.
+ Curto, estrutura de tópicos estilo comentários
- que eu não tenha tempo ou força de vontade para expandir
prosa formato
- que funcionam melhor no formato de contorno de qualquer maneira
- como este
+ Citações de outros
- Cypherpunks são um brilhante grupo. Um monte de coisas inteligentes
tem sido dito nos 600 dias x 40 posts/dia = 24,000
posts, e estou tentando usar o que eu posso.
+ Infelizmente, apenas uma pequena fração pode ser usado
- porque eu simplesmente não _read_ mesmo uma fração de
esses posts mais uma vez (embora eu só salvo
vários milhares de posts)
- e porque inclusive muitos desses lugares

simplesmente faça a FAQ por muito tempo (ainda é muito longo, eu
suponho)
- Eu espero que você pode lidar com as alterações no tom de voz, na
estilos, e até mesmo em formatos. Ele vai muito tempo para
fazer tudo de leitura de maneira uniforme.
1.5.3. Apesar de o comprimento de coisa, uma vasta quantidade de material é
faltando. Houve centenas de análise incisiva por
Cypherpunks, dezenas de levantamento de artigos em Clipper, e
milhares de inteligente observações. Infelizmente, apenas algumas delas aqui.
- E com 25 ou mais livros na Internet, centenas de perguntas frequentes
e URLs, é claro que todos nós estamos afogando em um mar de
informações sobre o Líquido.
- Ironicamente, o bom e velho livros têm muito mais
relevantes e atemporal informações.
1.5.4. Advertências sobre a plenitude ou precisão deste FAQ
+ nem todos os pontos são totalmente delineados...a natureza de estrutura de tópicos
significa que quase todos os pontos podem ser adicionados-para,
subdividida, taxonomized, e geralmente recheadas com
mais pontos, contrapontos, exemplos
- como uma árvore gigante...galhos, folhas, emaranhada hierarquias
+ É inevitável que conflitantes pontos será feita de uma
documento deste tamanho
- opiniões, mas não ficar corrigido em todos os lugares
- contextos diferentes levam a diferentes pontos de vista
- simples falha por mim para ser totalmente consistente
- e muitos pontos levantados aqui, se colocar em um ensaio
para os Cypherpunks lista, gerar comentários, réplicas,
o debate, e até mesmo acrimónia....Eu não posso esperar para ter todas as
os lados representada totalmente, especialmente como os problemas são
muitas vezes obscuro, não resolvida, em disputa, e, geralmente,
controverso
- inconsistências nos pontos aqui na FAQ

1.6. Correções e Elaborações
+ "Como lidar com correções ou esclarecimentos?"
- Enquanto eu tenho feito o meu melhor para garantir a precisão, os erros de
sem dúvida, existe. E como qualquer um pode ver da leitura do
Cypherpunks lista, cerca de *qualquer* declaração feita sobre qualquer
sujeito pode produzir uma enxurrada de contestações, ressalvas,
expansões, e outros enfeites. Alguns assuntos, tais como a natureza
de dinheiro, o papel dos Cypherpunks, e o papel do
a reputação da empresa, produzir dezenas de opiniões diferentes a cada
o tempo eles vêm!

- Então, não é provável que os meus pontos aqui vai ser qualquer
diferente. Felizmente, o grande número de pontos aqui
significa que cada um deles vai ser discordou.
Mas a matemática é bastante clara: se cada leitor encontra mesmo
uma coisa é discordar e, em seguida, envia a sua refutação ou
elaboração....desastre! (Especialmente se algumas pessoas não podem
guarnição citações corretamente e acabam incluindo uma grande parte da
texto.)
+ Recomendações
- Enviar correções de _fact_ para mim
- Se você não concordar com minha opinião, e você acha que você pode
mudar minha mente, ou causar-me a incluir a sua opinião como um
elaboração ou como um dissidente vista, em seguida, enviá-lo. Se
seu ponto requer muito debate ou é um profundo
desacordo, então eu duvido que eu tenha tempo ou energia para
o debate. Se você quiser ouvir as suas opiniões, escrever a sua própria FAQ!
- Finalmente, enviar o que você quer. Mas eu, claro, vai
avaliar comentários e aplicar uma reputação baseado no filtro para
o tráfego. Aqueles que me enviar, concisa e bem fundamentado
correções ou esclarecimentos são mais prováveis de serem ouvidos
para que aqueles que a barragem me com menor esclarecimentos
e elaborações.
- Em suma, este não é um projeto do grupo. O "sopa de pedra
FAQ:" não é o que isto é.
+ Mais informações
- Por favor, não me envie e-mail pedindo mais informações
em um determinado tópico--eu simplesmente não pode lidar personalizado
a pesquisa. Este FAQ é longa o suficiente, e o Glossário no
final contém informação adicional, portanto, que eu não
expanda sobre estes temas (a menos que haja uma gerais
o debate sobre a lista). Em outras palavras, não suponha esse
FAQ é um ponto de entrada para uma maior base de dados eu vou
gerar. Eu odeio soar tão rude, mas eu vi o
as solicitações que chegam em cada vez que eu escrever um bom
artigo.
+ Dicas nos comentários
- Comentários sobre o estilo de escrita, a forma "eu teria
escrito _this_ forma," são especialmente perigosas.
+ Problemas de crédito
- inevitável que as omissões ou colisões irão ocorrer
- idéias de muitos pais
- algumas idéias têm sido "no ar" por muitos anos
+ slogans são especialmente problemáticos

- "Eles podem ter a minha...."...Eu de crédito Barlow com isso, mas
Eu já ouvi outros usá-lo de forma independente (eu acho pelo menos
Eu usei ele antes de ouvir Barlow usado)
- "Se crypto é ilegal, apenas bandidos terão de criptografia"
- "Big Brother " De Dentro"
- se há algo que realmente incomoda você, enviar-me uma nota

1.7. Agradecimentos
1.7.1. Agradecimentos
- Meu chefe agradecimentos vão para as várias centenas de ativo
Cypherpunks cartazes, do passado e do presente.
- Todos os direitos reservados. Direitos De Autor Timothy C. De Maio. Não tente
vender este ou incorporá-lo em tudo o que é vendido.
Citando breve seções é "fair use"...citando longo
seções não.

1.8. Ideias e Notas (não impresso)
1.8.1. Gráficos para cobrir
- a duas quadras...plaintext para cryptotext
- Cypherpunks FAQ
- compilado por Timothy C. Maio, tcmay@netcom.com
- com a ajuda de muitos Cypherpunks
- com material de outras fontes
- <creditado entre parênteses em ângulo>
1.8.2. "Portanto, não pergunte"

1.9. As coisas estão se movendo rapidamente em criptografia e criptografia de política
1.9.1. difícil manter este FAQ atual, como informações de alterações
1.9.2. PGP em estado de fluxo
1.9.3. novas versões de ferramentas vindo constantemente
1.9.4. E todo o Clipper coisa foi transformado em sua cabeça
recentemente, a Administração está fazendo muitos pontos...
já fiz aqui em são agora processados discutível e são, principalmente, de
interesse histórico apenas.
- Gore carta para Cantwell
- Whit Diffie descreveu uma conferência sobre os principais sistemas de garantia de depósito em
Karlsruhe, na Alemanha, que parecia ter novas ideias
- TIS? (não pode utilizar esta informação?)

1.10. Notas: O Cyphernomicon: o CypherFAQ e Mais
1.10.1. 2.3.1. "O Livro de Encyphered Nomes"
- Ibn al-Taz Khallikak, o Pine Barrens Horror.

- Liber Grimoiris....Cifur???
- a difusão do Sumério areias, através do portão de
Ishtar, para os becos de Damasco, temperado com o
o sangue dos Ocidentais
- Chaves de Salomão, Kool Dee e o Rap Cryps Ido
para Croatan
- Pedro Krypotkin, o russo de criptografia anarquista
- Vinte e nove Primos, Califórnia
1.10.2. 2.3.2. O CYPHERNOMICON: um Cypherpunk FAQ e Mais---
Versão 0.666
1.10.3. 1994-09-01, direitos de Autor Timothy C. Maio, tcmay@netcom.com
1.10.4.
- Escrito e compilado por Tim Poderá, exceto como observado por
créditos. (Influenciado por anos de bons posts sobre o
Cypherpunks lista.) É concedida permissão para postar e
distribuir este documento em uma inalterado e completo
estado, sem fins lucrativos e com finalidades educacionais somente.
Razoável citando em "fair use" disposições
permitido. Veja os detalhes isenção de responsabilidades
e passivos no capítulo Introdução.

2. MFAQ--Perguntas Mais Freqüentes

2.1. direitos autorais
O CYPHERNOMICON: Cypherpunks FAQ e Mais, Versão 0.666,
1994-09-10, Direitos De Autor Timothy C. De Maio. Todos os direitos reservados.
Veja os detalhes de isenção de responsabilidade. Use seções curtas em "justo
use" disposições, com crédito apropriado, mas não coloque o seu
nome em minhas palavras.

2.2. RESUMO: MFAQ--Perguntas Mais Freqüentes
2.2.1. Pontos Principais
- Estas são as principais perguntas que continuam a surgir. Não
necessariamente, a pergunta mais básica, apenas os que recebem
perguntou um monte. O que a maioria das FAQs.
2.2.2. Ligações para Outras Secções
2.2.3. Onde Encontrar Informações Adicionais
- os recém-chegados a criptografia deve comprar Bruce Schneier "Aplicada
Criptografia"...ele vai salvar muitas horas no valor de
perguntas desnecessárias e sem noção observações sobre
criptografia.
- a várias perguntas frequentes publishe no newsroups (como sci.cripta,
alt.segurança.pgp), são muito úteis. (também em rtfm.mit.edu)

2.2.4. Diversos Comentários
- Eu não tinha certeza do que incluir aqui no MFAQ--talvez
as pessoas podem fazer sugestões de outras coisas para incluir.
- Meu conselho é que se algo de seu interesse, use o
edição/ferramentas de busca para encontrar o mesmo tópico principal
a seção. Geralmente (mas não sempre) há mais material em
os capítulos principais do que aqui no MFAQ.

2.3. "O que é o 'Big Picture'?"
2.3.1. Forte de criptografia é aqui. É amplamente disponível.
2.3.2. Isso implica muitas mudanças na maneira como o mundo funciona. Privada
os canais entre as partes que nunca conheceu e que nunca
irá encontrar são possíveis. Totalmente anônimo, unlinkable,
untraceable comunicações e trocas são possíveis.
2.3.3. As transações só podem ser: *voluntário*, uma vez que as partes são
untraceable e desconhecido e pode se retirar a qualquer momento. Este
tem profundas implicações para a abordagem convencional de
usando a ameaça da força, dirigida contra os partidos
os governos ou por outras pessoas. Em particular, as ameaças de força
irá falhar.
2.3.4. O que emerge é claro, mas eu acho que vai ser um
forma de anarco-capitalista de mercado do sistema que eu chamo de "crypto
a anarquia." (Voluntária apenas comunicações, com nenhum terceiro
partes intrometendo.)

2.4. Organizacional
2.4.1. "Como posso obter--e fora--a Cypherpunks lista?"
- Enviar uma mensagem para "cypherpunks-request@toad.com"
- Qualquer auto-processados comandos?
- não enviar solicitações para a lista como um todo....isto irá
marca você como "sem noção"
2.4.2. "Por que os Cypherpunks lista, por vezes, ir para baixo, ou perder o
lista de subscrição?"
- A máquina host, toad.com, propriedade de John Gilmore, teve
os problemas usuais, tais máquinas têm: sobrecarga,
a escassez de espaço em disco, atualizações de software, etc. Hugh
Daniel tem feito um trabalho admirável de manter em bom
forma, mas os problemas não ocorrem.
- Pense como um aviso de que listas e sistemas de comunicação
permanecem um tanto frágil....uma lição para o que é necessário para
fazer dinheiro digital mais robusta e confiável.
- Não há funcionários remunerados, nenhum hardware para orçamento
melhorias. O trabalho feito é estritamente voluntária.

2.4.3. "Se eu apenas juntei os Cypherpunks lista, o que devo fazer?"
- Ler por um tempo. As coisas vão ficar mais claras, temas
surgem, e algumas perguntas serão respondidas. Este é
um bom conselho para qualquer grupo ou lista, e é especialmente assim para
uma lista com 500 ou mais pessoas sobre ele. (Que atingiu mais de 700 em um
ponto, em seguida, um par de lista de interrupções bateu o número
um pouco para baixo.)
- Leia as referências mencionadas aqui, se você pode. O
sci.cripta FAQ deve ser lido. E compra de Bruce Schneier
"Applied Cryptography", a primeira chance de você chegar.
- Juntar as coisas que interessam a você, mas não faça um tolo
de si mesmo. Reputação importa, e você pode vir a se arrepender
ter vir transversalmente como um tedioso tolo em suas primeiras semanas no
a lista. (Se você é um tedioso enganar após as primeiras
semanas, que pode ser apenas a sua natureza, é claro.)
- Evitar gritando e falando sobre tópicos não relacionados, tais como
aborto (pró ou contra), armas (pró ou contra), etc. O costume
tópicos que costumam gerar muito calor e não muito
luz. (Sim, a maioria de nós tem opiniões fortes sobre estes e
outros temas, e, sim, que, às vezes, deixar que os nossos pontos de vista de fluência
em discussões. Não há como negar que certas
ressonâncias de existir. Eu só estou pedindo cautela.)
2.4.4. "Eu sou inundado por volume da lista; o que posso fazer?"
- Esta é uma reação natural. Ninguém pode segui-lo todos;
passar inteiramente muitas horas de um dia ler a lista, e eu
certamente não pode segui-lo todos os. Escolha de áreas de especialização e
em seguida, siga-los e ignorar o resto. Depois de tudo, não vendo
coisas da lista pode ser pior do que não, mesmo sendo
subscreveram a lista!
- Bater a tecla "delete" rapidamente
- encontrar alguém que vai prepará-la para você (Eric Hughes tem
dito repetidamente que qualquer pessoa pode retransmitir a lista dessa maneira;
Hal Finney tem oferecido uma lista criptografada)
+ Melhor utentes podem ajudar. Algumas pessoas têm usado mail-para-notícias
sistemas e, em seguida, leia a lista como um grupo de notícias local, com
threads.
- Eu tenho Eudora, que oferece suporte off-line de leitura e
recursos de classificação, mas eu geralmente acabam de ler com um
on-line programa de correio (elm).
- A lista de discussão, um dia poderá ser alterado para um
grupo de notícias, a la "alt.cypherpunks." (Isso pode afetar alguns
as pessoas cujos sites não carregar em alt grupos).
2.4.5. "É muito fácil se perder no emaranhado de detalhes aqui. São

há alguma maneira de acompanhar o que está ** realmente importante?"
- Primeiro, um monte de coisas postada na Usenet newsgroups,
e no Cypherpunks lista, é periférico coisas,
epifenomênicas sujeira que vai arrasar no primeiro forte
brisa. Sujo detalhes sobre o PGP conchas, sobre o RSA
criptografia de velocidades, sobre NSA supercomputadores. Há apenas
não há razão para que as pessoas com que me preocupar "IDEIA fraca chaves" quando
tantas questões mais prementes existe. (Deixe os especialistas
se preocupe.) Pouco de tudo isso faz alguma diferença real, assim como
pouco das coisas nos jornais diários é memorável ou
merece ser memorável.
- Segundo, "ler as fontes." Ler "1984", "O Shockwave
O Piloto," O "Atlas Shrugged," "Nomes Verdadeiros." Leia o Chaum
artigo sobre como fazer Big Brother obsoleto (outubro de 1985,
"Communications of the ACM").
- Terceiro, não perder de vista os valores fundamentais: privacidade,
soluções tecnológicas através de soluções jurídicas, evitando
tributação, ignorando as leis, etc. (Nem todos irão concordar
com todos esses pontos.)
- Em quarto lugar, não se afogar no detalhe. Pegar algumas áreas de
interesse e siga _them_. Você pode não precisar de saber o
funcionamento interno de DES ou todos os interruptores na PGP para fazer
contribuições em outras áreas. (Na verdade, você certamente não.)
2.4.6. "Quem são os Cypherpunks?"
- Uma mistura de cerca de 500-700
+ Pode descobrir quem enviando mensagem para majordomo@toad.com
com o corpo de mensagem de texto "que cypherpunks" (sem aspas,
curso).
- Isso é uma falha de privacidade? Talvez.
- Muitos dos estudantes (eles têm o tempo, a Internet
contas). Lotes de informática/programação pessoal. Lotes
dos libertários.
- citação de Fios artigo, e a partir de "Whole Earth Review"
2.4.7. "Quem executa o Cypherpunks?"
- Ninguém. Não há nenhuma definição formal de "liderança". Nenhum governante = sem
cabeça
= um arco = anarquia. (Procurar a etimologia da anarquia.)
- No entanto, a lista de discussão atualmente reside em física
máquina, e essa máquina cria alguns nexo de controle,
bem como ter uma festa no nte e casa. A lista
administrador está atualmente Eric Hughes (e tem sido, desde a
o início). Ele é ajudado por Hugh Daniel, que muitas vezes não
manutenção do toad.com e por John Gilmore, que possui

o toad.com máquina e conta.
- Em uma situação extrema de abuso ou sem comentar,
essas pessoas poderia chutar alguém de fora da lista e bloqueá-los
a partir de resubscribing via majordomo. (Eu presumo que eles pudessem--
isto nunca aconteceu.)
- Para enfatizar: ninguém nunca chutou de fora da lista, assim
tanto quanto eu sei. Não mesmo Detweiler...ele pediu para ser removido
(quando a lista subscreve foram feitas manualmente).
- Quem define a política, não é política! Nenhuma carta, nenhum
agenda, não itens de ação. O que as pessoas querem trabalhar em
si mesmos. Que é tudo o que pode ser esperado. (Algumas pessoas
ficar frustrado com essa falta de consenso, e eles
às vezes, começar a arder e discursando sobre "Cypherpunks
nunca fazer nada", mas esta falta de consenso é para ser
o esperado. Ninguém está sendo pago, ninguém tem de contratação e
disparo de autoridade, para qualquer trabalho que é feito tem que ser
voluntária. Alguns grupos de voluntários, está mais organizado do que nós
são, mas existem outros fatores que fazem com que esta mais
possível para eles do que para nós. C'est la vie.)
- Aqueles que se ouviu na lista de discussão, ou na física
reuniões, são aqueles que escrevem artigos que as pessoas acham
interessante ou que dizem as coisas da nota. Parece justo para mim.
2.4.8. "Por que não as questões que me interessam obter discutido?"
- Talvez eles já tenham sido-a várias vezes. Muitos recém-chegados
são, muitas vezes, chagrined para encontrar arcano temas a ser discutido,
com pouco discussão de "o básico."
- Isso não é surpreendente....as pessoas a superar o "básico"
depois de alguns meses e quero passar para mais emocionante (para
- os temas. Todas as listas são assim.
- Em qualquer caso, depois de ler a lista por um tempo, talvez
várias semanas--vá em frente e pergunte. Fazer seu tópico
mais fresco pode gerar mais respostas do que, digamos, pedindo
o que há de errado com o Clipper. (Uma verdadeira sobrecarregados tópico,
naturalmente.)
2.4.9. "Como foi que os Cypherpunks grupo de começar?"
2.4.10. "De onde veio o nome 'Cypherpunks' vem?"
+ Judas Milhon, aka St. Jude, então editor do "Mondo 2000,"
foi nas primeiras reuniões...ela disse "Vocês são
apenas um monte de cypherpunks." O nome foi adotado
imediatamente.
- O 'cyberpunk' gênero de ficção científica lida frequentemente com
questões do ciberespaço e da segurança do computador ("ice"), para
o link é natural. Um ponto de confusão é que

cyberpunks são popularmente considerado como, bem, como "punks,"
enquanto muitos Cyberpunks são frequentemente libertários e
anarquistas de várias faixas. Na minha opinião, os dois são
não em conflito.
- Alguns, no entanto, prefere um mais sóbrio nome. O reino UNIDO
ramo chama-se o "reino UNIDO de Criptografia de Privacidade
Associação". <verificar isso> no Entanto, as vantagens do
nome de são claras. Para uma coisa, muitas pessoas estão aborrecidas por
sério nomes. Por outro, fica-nos notado por
jornalistas e outros.
-
- Estamos, na verdade, não muito "punk" em tudo. Sobre como punk
como a maioria dos nossos cyberpunk primos, o que é dizer, não
muito.
+ o nome
- Crypto Cabal (isso antes do sci.cripta FAQ pessoas
apareceu, eu acho), Criptografia Frente de Libertação, outros nomes
- nem todo mundo gosta do nome...como é a vida
2.4.11. "Por que não o Cypherpunks grupo anunciou metas,
ideologias, e os planos?"
- A resposta curta: nós somos apenas uma lista de discussão, um frouxo
associação de pessoas interessadas em coisas semelhantes
- sem orçamento, sem direito de voto, sem liderança (exceto a "liderança
o soapbox")
- Como poderia um consenso emergir? A abordagem usual é
para um grupo eleito (ou um grupo que tomou o poder) para
escrever a carta e metas, para promover sua agenda. Tal é
não é o caso aqui.
- É este FAQ de facto de uma declaração de metas? Não se eu puder
ajudá-lo, para ser honesto. Várias pessoas antes de mim planejado
uma espécie de FAQ, e tinham-se concluído-los, eu certamente
não teria sentido que eles estavam falando de mim, ou para o
do grupo. Para ser consistente, então, eu não posso ter outros pensam
desta forma sobre _this_ FAQ!
2.4.12. "O que os Cypherpunks realmente feito?"
- disseminação de criptografia: Cypherpunks ter ajudado
(PGP)...publicidade, um fórum alternativo para o sci.crypt (em
de muitas maneiras, a melhor...melhor relação S/N, mais educado)
- Fios, Toda a Terra de Revisão, NY Times, artigos
- remetentes, criptografados remetentes
+ O Cypherpunk - e Julf/Kleinpaste estilo de remetentes foram
tanto escrita muito rapidamente, em poucos dias
- Eric Hughes escreveu o primeiro Cypherpunks reenvio de e-mails em um

fim-de-semana, e ele passou o primeiro dia do fim de semana
aprender o suficiente Perl para fazer o trabalho.
+ Karl Kleinpaste escreveu o código que, eventualmente, se transformou
em Julf do reenvio de e-mails (adicionado desde que, é claro) em um
da mesma forma curto espaço de tempo:
- "O meu primeiro servidor anon, para godiva.nectar.cs.cmu.edu
2 anos atrás, foi escrito em poucas horas, um entediado
à tarde. Ele
não era como featureful como acabou sendo, mas foi
"concluir" para
seus objetivos iniciais, e livre de bugs."
[Karl_Kleinpaste@cs.cmu.edu, alt.privacidade.anon-servidor,
1994-09-01]
- Que outras ideias interessantes, tais como dinheiro digital, tem
ainda não realmente emergiu e ganhou usar, mesmo depois de anos de
discussão ativa, é um interessante contraste com esse
implantação rápida de remetentes. (Baseado em texto de natureza
tanto em linha reta de criptografia/assinatura e de remailing é
semanticamente mais simples de entender e, em seguida, usar do que são
coisas como o dinheiro digital, DC-redes, e outros de criptografia
protocolos.)
- idéias para scripts Perl, e-mail manipuladores
- discussão geral, com pessoas de vários políticos
persuasões
- conceitos: piscinas, Informações da Frente de Libertação, BlackNet
-
2.4.13. "Como eu Posso Aprender Sobre Criptografia e Cypherpunks Info?"
2.4.14. "Porque é que há, por vezes, desdém para o entusiasmo e a
propostas de recém-chegados?"
- Nenhum de nós é perfeito, então às vezes a gente está impaciente com
os recém-chegados. Além disso, os comentários visto tendem a ser problemas de
desacordo--como em todas as listas e newsgroups (acordo
tão chato).
- Mas muitos recém-chegados também não conseguiram fazer a leitura básica
que muitos de nós fez, literalmente, _years_ antes de se juntar a este
a lista. Criptologia é um assunto bastante técnico, e pode-se
não mais pular e esperar ser levado a sério sem
qualquer preparação do que em qualquer outra técnica de campo.
- Por fim, muitos de nós já respondeu a perguntas de
os recém-chegados muitas vezes para ser entusiasmado é
mais. Familiaridade raças desprezo.
+ Os recém-chegados deveriam tentar ser paciente sobre a nossa impaciência.
Às vezes, reformulando a pergunta gera interesse.

Frescura matéria. Muitas vezes, tomada de um incisivo comentário
em vez de apenas perguntar a uma questão básica, pode gerar
respostas. (Assim como na vida real.)
- "Clipper sux!" não vai gerar muita resposta.

2.4.15. "Deve-se juntar Cypherpunks lista de discussão?"
- Se você está lendo isso, é claro, muito provavelmente, você está
os Cypherpunks lista já, e esse ponto é discutível--você
em vez disso, pode estar se perguntando se você should_leave_ a Lista!
- Só se você estiver preparado para lidar com 30-60 mensagens de um dia,
com volumes de flutuação descontroladamente

2.4.16. "Por que não o Cypherpunks lista criptografada? Não acreditem
na criptografia?"
- qual é o ponto, para um público-registráveis lista?
- exceto para fazer com que as pessoas saltar através de aros, para colocar uma grande
encargos sobre o sapo (a menos que a todos foi dada a mesma chave, de modo
que apenas uma criptografia pode ser feito...o que ressalta
a loucura)
+ têm sido propostas, principalmente, como um pedaço de pau para forçar
as pessoas a começar a usar a criptografia...e para obter o criptografada
o tráfego aumentou
- envolvendo atrasos para aqueles que preferem não ou não pode usar
criptografia (os alunos em terminais, em países estrangeiros
que proibiram de criptografia, empresas assinantes....)

2.4.17. "O que faz "Cypherpunks escrever código' significa?"
- um esclarecimento de declaração, não um imperativo
- tecnologia e soluções concretas sobre brigas e
conversa
- se você não escrever o código, tudo bem. Nem todo mundo faz (na verdade,
provavelmente menos de 10% da lista de gravações graves código, e
menos de 5% de gravação de criptografia ou software de segurança

2.4.18. "O que significa 'Grande Irmão Dentro' Significa?"
concebido por sinceramente (tcmay) em Clipper reunião
- Matt Thomlinson, Postscript
- impresso por ....

2.4.19. "Eu Tenho uma Nova Idéia para uma Cifra---devo Discutir isso Aqui?"
- Por favor, não. Cifras requerem uma análise cuidadosa, e deve
seja em formato de papel (isto é, apresentado em uma detalhada de papel,
com as referências necessárias para mostrar que a devida diligência
foi feito, equações, tabelas, etc. A rede é um pobre
substituto.
- Também, a quebra de um aleatoriamente apresentados cifra não é
trivial, mesmo se o nível de codificação, eventualmente, é mostrada a ser fraco.
A maioria das pessoas não tem a inclinação para tentar quebrar um

cifra a menos que haja algum incentivo, tais como a fama ou dinheiro
envolvidos.
- E as novas cifras são notoriamente difíceis de design. Especialistas são
as melhores pessoas para fazer isso. Com todas as coisas à espera de ser
feita (como descrito aqui), trabalhando em uma nova codificação é, provavelmente,
a menos eficaz coisa de amador pode fazer. (Se você estiver
não um amador, e ter quebrado de outras pessoas cifras
antes, então você sabe quem você é, e esses comentários não
aplica. Mas eu vou adivinhar que menos de um punhado de gente em
esta lista tem as informações necessárias para fazer cifra
o design.)
- Há um grande número de cifras e sistemas, quase todos os
não duradoura significado. Não testado, não documentada, não utilizado-
-e, provavelmente, indigno de qualquer tipo de atenção. Não me adicionar à
o ruído.
2.4.20. São todos os Cypherpunks libertários?
2.4.21. "O que podemos fazer?"
- Implantar o forte de criptografia, para garantir o gênio não pode ser colocado em
a garrafa
- Educar, hall de entrada, discutir
- Semear a dúvida, de desprezo..ajudar a fazer programas de governo olhar
tolo
- Sabotagem, prejudicar, monkeywrench
- Exercer outras atividades
2.4.22. "Porque é que a lista não moderado? Por que não há filtragem de
em matéria de desreguladores como Detweiler?"
- tecnologia sobre a lei
- cada pessoa faz a sua própria escolha
- também, não há tempo para a moderação, e a moderação é geralmente
desperdiçados
+ quem deseja ter alguns pontos de vista silenciados, ou alguns
cartazes bloqueado, é aconselhada para:
- contrato com alguém para ser seu Pessoal Censurar,
passando-se a eles apenas material aprovado
- assine um serviço de filtragem, tais como o Raio e o Harry
estão fornecendo
2.4.23. "O Que Eu Posso Fazer?"
- política, espalhar a palavra
- escrever o código ("Cypherpunks escrever código")
2.4.24. "Devo divulgar o meu novo programa de criptografia?"
- "Eu desenhei um crypting programa, que eu acho que é
inquebrável. Eu desafio qualquer um que esteja interessado em obter
em contato comigo, e descriptografar um encriptados através de uma massagem."

"Com os maiores cumprimentos,
Babak Sehari." [Babak Sehari, sci.cripta, 6-19-94]

2.4.25. "Peça Emily Post Cripta"
+ meu variação de "Pedir Emily Postnews"
- para aqueles que não sabem, a contundente crítica de
sem noção lançamentos
+ "Eu acabei de inventar uma nova codificação. Aqui está um exemplo. Aposto que você
não pode quebrá-lo!"
- Por todos os meios de pós criptografados lixo. Nós, os que temos
nada melhor para fazer com o nosso tempo de responder vai ser
mais do que feliz para passar horas de funcionamento do seu material através de
nossa codebreaking Crays!
- Certifique-se de incluir uma amostra de texto não criptografado, para fazer
- se aparecer ainda mais sem noção.
+ "Eu tenho um cypher eu acabei de inventar...onde devo postar isso?"
+ "Um dos mais erros básicos de tomada de cifras é
basta adicionar
camada sobre camada de ofuscamento e fazer uma cifra que
é agradável e
- "complexo". Leia Knuth na tomada de número aleatório
geradores para o
- loucura em que esse tipo de abordagem. "<Eric Hughes, 4-17-
94, Cypherpunks>
+ "As cifras de levar a presunção de culpa, não de inocência.
Cifras
- projetado por amadores, invariavelmente falham sob o escrutínio de
especialistas. Este
- fato sociológico (bem confirmada) é onde o
presunção de
- a insegurança surge. Esta não é a ignorância, para assumir
que isso vai
- alteração. O ônus da prova é do reclamante de
de segurança, e não em
- o codebreaker. <Eric Hughes, 4-17-94, Cypherpunks>
+ "Eu só ficou muito chateado com alguma coisa, devo desabafar a minha
a raiva na lista de discussão?"
- Por todos os meios! Se você está cansado de fazer os seus impostos, ou apenas
ler uma coisa no jornal que realmente irritou você,
definitivamente enviar uma raiva mensagem para as 700 ou então
leitores e ajudar a fazer _them_ raiva!
- Encontrar um falso link para criptografia ou questões de privacidade para torná-lo

parecem mais relevantes.

2.4.26. "O que são alguns dos principais Cypherpunks projetos?"

+ remetentes
+ melhor remetentes, os recursos mais avançados
- digital postagem
- preenchimento, de lotes/latência
- agente de recursos
- mais deles
- ventos (10 sites em 5 países, como mínimo)
- ferramentas, serviços
- dinheiro digital em melhores formas
-

2.4.27. "O que sobre sublistas, para reduzir o volume na lista principal".

- Já há meia dúzia de sub-listas, dedicado à
reuniões de planejamento, para a construção de hardware, e para explorar
DC-Redes. Há um reenvio de e-mails para os operadores, ou de haver usado
para ser. Existem também listas dedicadas a temas semelhantes, como
Cypherpunks, incluindo Robin Hanson, "AltInst" lista
(Instituições alternativas), Nick Szabo do "libtech-l lista",
o "IMP-Interesse" (Internet Mercantil Protocolos) lista de
e assim por diante. A maioria são muito baixos de volume.
+ Que poucas pessoas ouviram falar de qualquer um deles, e que o tráfego
os volumes são extremamente baixos, ou zero, não é tudo o que
surpreendente, e corresponde a experiências em outros lugares. Vários
motivos:
- Sublistas são um incômodo para lembrar, a maioria das pessoas se esqueça de
eles existem, e não acho que o post para eles. (Este
"esquecendo-se" é um dos aspectos mais interessantes do
ciberespaço; bem-sucedida listas parecem ser Schelling pontos
que accrete ainda mais sócios, embora sem êxito listas
desvanecer-se em nada.)
- Há um desejo natural de ver as palavras no maior
de dois fóruns, para que as pessoas tendem para postar para a lista principal.
- As sublistas, por vezes, foram formados em uma explosão de
exuberância sobre algum assunto, que, em seguida, desapareceu.
- Tópicos muitas vezes abrangem vários subinterest áreas, de modo a postagem
para a lista principal é melhor do que a cópia de todas as
sublistas.
- Em qualquer caso, os Cypherpunks lista principal é "," por agora,
e tem impulsionado outras listas efetivamente fora do negócio. Um
tipo de Gresham da Lei.

2.5. Crypto

2.5.1. "Porque é que a criptografia é tão importante?"
+ Os três elementos que são centrais para a nossa visão moderna de
a liberdade e privacidade (a la Diffie)
- proteger as coisas contra roubo
- provando que podemos dizer que estamos
- expectativa de privacidade em nossas conversas e escritos
- Embora não haja explícita "direito à privacidade" enumerado
na Constituição dos EUA, o pressuposto de que um indivíduo
é para ser seguro em seus artigos, lar, etc., na ausência de uma válidos
garante, é central. (Nunca houve uma decisão ou da lei.
que as pessoas tem para falar em uma linguagem que é
compreensível para os bisbilhoteiros, wiretappers, etc., nem tem
mais do que nunca, uma regra que proíbe a utilização privativa de encrption. Eu
falar isso para lembrar os leitores de a longa história de
crypto liberdade.)
- "Informação, tecnologia e controle de ambos é poder.
Anônimo telecomunicações tem o potencial para ser o
maior equalizador na história. Trazendo este poder como
muitos como possível irá mudar para sempre o discurso do poder
neste país (e o mundo)." [Mateus J Miszewski, ATO
AGORA! 1993-03-06]
2.5.2. "Quem usa criptografia?"
- Todos, de uma forma ou de outra. Vemos criptografia de todo
gente...o chaves em nossos bolsos, as assinaturas no nosso
carteira de habilitação de motorista e outros cartões, os IDs de fotografia, o
cartões de crédito. Bloqueio de combinações, porta chaves, números PIN,
etc. Todos são parte de criptografia (apesar de a maioria pode chamar isso de
"segurança" e não muito matemáticos coisa, como
criptografia é geralmente pensado para ser).
- Whitticism: "aqueles que regularmente
conspiram para participar no processo político são
já a criptografia." [Whit Diffie]
2.5.3. "Quem precisa de criptografia? O que têm a esconder?"
+ pessoas honestas necessidade de criptografia, porque não são desonestos
pessoas
- e pode haver outras necessidades de privacidade
- Há muitas razões por que as pessoas precisam de privacidade, a capacidade
para manter algumas coisas em segredo. Financeira, pessoal,
o psicológico, o social, e muitas outras razões.
- Privacidade em seus trabalhos, em seus diários, em seus respectivos
vidas. Em suas escolhas financeiras, seus investimentos, etc.
(O IRS e imposto de autoridades de outros países dizem
tenho o direito de ver privado de registros, e até agora os tribunais

fez-las. Eu discordo.)
- as pessoas criptografar pela mesma razão, eles feche e trave
suas portas
- Privacidade em suas formas mais básicas de
2.5.4. "Eu sou novo para o crypto-onde devo começar?"
- livros...Schneier
- refrigerante
- sci.cripta
- falar.política.crypto
- Perguntas frequentes de
2.5.5. "Eu preciso estudar criptografia e teoria dos números para fazer uma contribuição?"
- Absolutamente não! A maioria dos métodos de criptografia e matemáticos são tão ocupado fazendo a sua coisa de que eles pouco tempo ou interesse para políticas e atividades empresariais.
Especialização é para insetos e pesquisadores, como de alguém .sig diz.
- Muitas áreas estão maduros para a contribuição. Modularização de funções significa que as pessoas podem se concentrar em outras áreas, assim como os escritores não têm para aprender como definir o tipo, ou corte pena canetas, ou de mistura de tintas.
- Nonspecialists deve tratar a maioria estabelecido cifras como "caixas pretas" que funciona como anunciado. (Não estou dizendo que eles fazer, só de que a análise deles é melhor deixar para os especialistas um... pouco de ceticismo não pode ferir, embora).
2.5.6. "Como criptografia de chave pública de trabalho, basta colocar?"
- A abundância de artigos e livros descrevem este, cada vez detalhe crescente (eles começam com o básico, em seguida, obter para o suculento).
+ Eu encontrei uma explicação simples, com o "brinquedo números", a partir de Mateus Ghio:
- "Você escolhe dois números primos; por exemplo, 5 e 7. Multiplicá-los juntos, é igual a 35. Agora você calcular o produto de uma menor que a cada número, mais um. (5-1)(7-1)+1=21. Existe uma relação matemática que diz que x = x^21 mod 35 para qualquer x de 0 a 34. Agora você fator de 21, yeilds 3 e 7.

"Você escolhe um desses números para ser a sua chave privada e o outro é a sua chave pública. Então você tem:
Chave pública: 3
Chave privada: 7

"Alguém criptografa uma mensagem para você por tomar plaintext
mensagem de m de tornar a mensagem de texto cifrado c: c=m^3 mod 35

"Você descriptografar c e localizar m usando a chave privada: m=c^7
mod 35

"Se os números são várias centenas de dígitos (como no
PGP), é quase impossível adivinhar a chave secreta."
[Mateus Ghio, alt.anônimo, 1994-09-03]
- (Há um erro matemático aqui...exercício da esquerda para a
estudante.)
2.5.7. "Eu sou um recém-chegado a esse tipo de coisa...como devo começar?"
- Iniciar a leitura de alguns dos materiais citados. Não se preocupe
muito sobre a compreensão de tudo.
- Siga a lista.
- Encontrar uma área que lhe interessa e se concentre.
Não há nenhuma razão por que os defensores da privacidade precisa entender
O grupo Diffie-Hellman key exchange em detalhes!
+ Mais Informações
+ Livros
- Schneier
- Brassard
+ Revistas, etc.
- Os processos
- Jornal da Criptologia
- Cryptologia
- Grupos de notícias
- sites de ftp
2.5.8. "Quem é a Alice e o Bob?"
2.5.9. "O que é a segurança através da obscuridade"?
- a adição de camadas de confusão, engano
- raramente é forte em um infromation-teórico ou
criptografia sentido
- e pode ter "atalhos" (como um nó que parece complexo
mas o que fica em aberto se aproximou da forma certa)
- algoritmos de criptografia, muitas vezes escondida, sites ocultos
- Não se enganem, estas abordagens são frequentemente usados.
E eles podem adicionar um pouco para a segurança global (usando
arquivo de criptografia de programas como o FolderBolt no topo do PGP é um
exemplo)...
2.5.10. "Tem DES sido quebrado? E o que sobre o RSA?"
- DES: pesquisa de força Bruta do espaço no texto normal escolhido
ataques é feeasible em torno de 2^47 chaves, de acordo com

Biham e Shamir. Isso é cerca de 2^9 vezes mais fácil do que o
"raw" de espaço. Michael Wiener foi estimado que um macine
de batata frita especial poderia quebrar o DES desta forma, para alguns
mil dólares por chave. A ANS pode ter tais máquinas.
- Em qualquer caso, o DES não foi o esperado para durar tanto tempo por muitos
(e, na verdade, a NSA e NIST propôs uma descontinuação gradual alguns
anos atrás, o "CCEP" (Comercial COMSEC Endosso
O programa), mas ele nunca pegou e parece esquecido hoje.
Clipper e EES parecem ter agarrou o centro das atenções.
- IDÉIA, a partir da Europa, é suposto ser muito melhor.
- Como RSA, isso é improvável. Factoring ainda não está comprovada
para ser NP-co

2.5.11. "A ANS Quebra de Foo?"

- DES, RSA, IDÉIA, etc.
- O governo pode quebrar o nosso cifras?

2.5.12. "Pode métodos de força bruta quebra de criptografia de sistemas?"

- depende do sistema, o espaço, os auxiliares
informações avialable, etc.
- poder de processamento, geralmente, tem sido dobrando a cada 12-18
meses (Lei de Moore), de modo que....
- Gaiado é de 80 bits, que é provavelmente seguro de bruta
ataque de força para 2^24 = 1.68e7 vezes tão longo quanto o DES.
Com Wiener estimativa de 3,5 horas para quebrar o DES, este
implica 6700 anos usando o hardware de hoje. Partindo-se de um
otimista duplicação de hardware de energia por ano (para o
mesmo custo), ele vai levar de 24 anos antes de os custos de hardware
de um ataque de força bruta em Skipjack vêm para baixo para que ele
agora os custos para atacar DES. Supondo que nenhum outro fracos em
Skipjack.
- E note que as agências de inteligência são capazes de gastar muito
mais do que o que Wiener calculado (lembre-se de Norma de Hardy
descrição da Colheita)

2.5.13. "A ANS saber sobre a chave pública de ideias antes de Diffie e
Hellman?"

+ de muito debate, e alguns manhoso e possivelmente enganosa insinuação
- Simmons afirmou que ele aprendeu de PK em Gardner coluna, e
certamente ele deve ter sido em uma posição para saber
(armas, Sandia)
-
+ Inman alegou que a NSA tinha um P-K conceito em 1966
- se encaixa com Dominik ponto sobre selado criptosistema de caixas de
com nenhuma forma de carregar novas chaves
- e consistentes com a ANS, tendo essencialmente acesso exclusivo a

nação superior matemáticos (até Diffies e Hellmans
foreswore financiamento do governo, como resultado do anti-
Pentágono sentimentos dos anos 70)

2.5.14. "A ANS saber sobre o público-abordagens-chave antes de Diffie
e Hellman?"

- vem para cima de um monte, com alguns na ANS, tentando maliciosamente
sugiro que _of course_ eles sabiam sobre isso...
- Simmons, etc.
- Bellovin comentários (são bons)

2.5.15. "Pode NSA crack RSA?"

- Provavelmente não.
- Certamente não por "procurando o espaço," uma idéia que
aparece a cada poucos meses . Isso não pode ser feito. 1024-bit chaves
implica a cerca de 512 bits primos, ou 153-dígito decimal
primos. Há mais de 10^150 deles! E apenas cerca de
10^73 partículas em todo o universo.
- Tem o factoring problema foi resolvido? Provavelmente não. E
provavelmente não vai ser, no sentido de que o factoring é, provavelmente,
no NP (embora esta não tenha sido provada) e P é, provavelmente,
não NP (também não provadas, mas muito forte suspeita). Enquanto
haverá avanços em factoring, é extremamente
improvável (no sentido religioso) que o factoring 300
número de dígitos de repente se tornar "fácil".
- A RSA vazamento de informações, de modo a torná-lo mais fácil para
com o crack do que é fator de módulo? Suspeita por alguns,
mas basicamente desconhecido. Eu seria capaz de apostar contra ele. Mas mais
duvidoso que o ponto acima.

+ "Quão forte é o forte de criptografia?"

- Basicamente, mais forte do que qualquer um dos piegas de "códigos" para
amado de suspense escritores e produtores de cinema. Moderno
as cifras não são crackable "dizendo o computador para executar
através de todas as combinações" (mais precisamente, o número
de combinações excede em muito o número de átomos no
o universo).

2.5.16. "Não mais poderosos computadores fazem cifras quebráveis?"

+ Os efeitos do aumento de energia do computador conferir mesmo
maior vantagem para a codificação do usuário do que a cifra
disjuntor. (Mais comprimentos de chaves no RSA, por exemplo, exigem
polinominalmente mais tempo para usar, mas exponencialmente mais tempo
para quebrar, grosseiramente falando.) Incrivelmente, é provável que
estamos perto de ser capaz de usar comprimentos de chave que não pode
ser dividido com todos a alimentação do computador que nunca vai existir
no universo.

+ Análoga à impenetrável campos de força, protegendo o
de dados, com mais energia necessária para "perfurar" que
existe no universo
- Vernor Vinge de "bolhas", em "A Paz e a Guerra."
- Aqui estou supondo que não há cortes curtos para factoring
existem...esse é comprovada, mas suspeita. (Nenhum grande
atalhos, i.é., o factoring não é "fácil".)
+ Um módulo de milhares de casas decimais pode exigir mais
total de "energia" para o factor, usando abordagens previsíveis,
que está disponível
- reversível computação pode ajudar, mas eu suspeito que não muito
- Ata da mecânica quântica abordagem é completamente
não testado...e pode não escala bem (por exemplo, pode ser
marginalmente possível obter a precisão de medição para
use este método para, digamos, 100-números de dígitos, mas
totalmente impossível obtê-lo para 120-números de dígitos, deixe
sozinho 1000 dígitos)

2.5.17. "Será forte criptografia ajuda racistas?"
- Sim, isso é uma consequência de ter secure virtual
comunidades. A liberdade de expressão tende a funcionar de que maneira!
- Ariana Nação pode usar criptografia para recolher e divulgar
informações, mesmo em "controlada" nações como Alemanha
essa proibição grupos como Nação Ariana.
- Claro, "na Internet ninguém sabe que você é um cão" de modo
explícitas de racismo com base na superficiais características externas
é correspondentemente mais difícil.
- Mas forte de criptografia habilitar e capacitar os grupos que têm
crenças diferentes das que o local da maioria, e vai permitir que
ignorar as leis regionais.

2.5.18. Trabalhando em novas cifras--por que não é uma prioridade Cypherpunks
(como eu o vejo)
- É um problema de alocação de recursos. ("Todos os criptografia é
a economia." E. Hughes) Muito trabalho foi de codificação
design, e o mundo parece ter vários estável, robusto
cifras para escolher. Qualquer trabalho adicional por criptografia
amadores-que a maioria de nós, em relação à profissional
matemáticos e codificação de designers--é provável que
as coisas para a frente de forma significativa. Sim, poderia acontecer...mas
não é provável.
+ Considerando que existem áreas onde o profissional estudando criptografia
tem feito muito pouco:
- PGP (note que PRZ fez *não* tire um tempo para tentar
inventar suas próprias cifras, pelo menos não para a Versão

2.0)...ele se concentrou sobre onde seus esforços teriam
a melhor recompensa
- implementação de remetentes
- problemas envolvendo as conchas e outras ferramentas para uso de criptografia
- dinheiro digital
- problemas relacionados, tais como a reputação, a linguagem de design,
teoria dos jogos, etc.
- Estas são as áreas de "moleza", as áreas onde
o maior estrondo para o fanfarrão mentiras, para misturar algumas metáforas
(a metralha?).
2.5.19. "Há alguma inquebrável cifras?"
- Uma vez almofadas são de informações sobre o curso-teoricamente
seguro, por exemplo, inquebrável pela alimentação do computador.
+ Convencionais, cifras, incluindo a chave pública cifras,
algumas cifras não pode ser frágil em _our_ universo, em qualquer
quantidade de tempo. A lógica funciona da seguinte maneira:
- O nosso universo, presumivelmente, tem algum número finito de
partículas (atualmente estimada em 10^73 partículas).
Isso leva ao "mesmo se todas as partículas foram um Cray Y-
MP levaria..." o tipo de experiências com o pensamento.

Mas eu estou pensando em _energy_ aqui. Ignorando reversível
cálculo para o momento, cálculos de dissipar a energia
(alguns discordar neste ponto). Há alguns uppper
limite de quantas básicas de cálculos jamais poderia ser feito
com a quantidade de energia livre no universo. (Um áspero
o cálculo pode ser feito através do cálculo da energia
saída de estrelas, coisas caindo em buracos negros, etc.,
e, em seguida, supondo-se sobre kT por operação lógica. Este
devem ser precisas dentro de algumas ordens de magnitude.)
Eu ainda não fiz esse cálculo, e não aqui, mas o
resultado provavelmente seria algo ao longo das linhas de X
joules de energia que poderia ser aproveitado para o cálculo,
resultando em Y primitivas básicas computacional passos.

Posso, então, encontrar um módulo de 3000 dígitos ou 5000 dígitos,
ou seja o que for, que leva o *mais* do que este número de passos
para o fator. Portanto, inquebrável em nosso universo.
- Advertências:

1. Talvez realmente existem atalhos para factoring. Certamente
melhorias no factoring métodos irá continuar. (Mas de
claro que essas melhorias não são coisas que converter

factoring em menos de exponencial-em-comprimento
problema...que é, factoring, parece estar "muito duro".)

2. Talvez reversível cálculos (la Landauer, Bennett,
et. al.) na verdade, o trabalho. Talvez isto significa um "factoring
a máquina" pode ser construído, o que leva a um fixo, ou muito lentamente
crescendo, a quantidade de energia. Neste caso, "para sempre" significa
Canhoto é provavelmente certo.

3. Talvez a mecânica quântica ideia de Peter Shor é
possível. (Duvido, por várias razões.)

2.5.20. "Quão seguro é o RSA?" "Quão seguro é o PGP?" "Eu ouvi dizer que o PGP tem bugs?"
- Esta nuvem de perguntas é certamente o mais comum tipo que
aparece no sci.cripta. Ele às vezes fica sem respostas,
às vezes é uma resposta rude, e apenas ocasionalmente faz
levar a uma fruiful discussão.
- O simples anwer: Estas cifras parecem ser seguro, ter
não há falhas óbvias.
- Mais detalhes podem ser encontrados em vários questão em outro lugar no
esta FAQ e nas várias secções de Faq e as referências de outros têm
publicado.

2.5.21. "Quanto tempo faz a encriptação de ter para ser bom?"
- Isso, obviamente, depende do que você está criptografia. Alguns
as coisas só precisa ser seguro para curtos períodos de tempo, por exemplo, um
alguns anos, ou até menos. Outras coisas podem voltar para assombrá
você--ou levá-lo jogado na prisão, muitos anos mais tarde. Eu posso
imagine segredos que precisam ser mantidos por muitas décadas, até mesmo
séculos (por exemplo, o medo descendentes serão
pagar o preço de um segredo revelado).
- Ele é útil para pensar _now_ sobre a alimentação do computador provável
para estar disponível no ano de 2050, quando muitos de vocês lendo
isso ainda será redor. (Eu estou argumentando que _não_
paralelismo, etc., vai causar RSA cair, só que alguns
comprimentos de chave (por exemplo, 512-bit) pode cair em seguida. Melhor ser
seguro e usar 1024 bits ou até mais. Aumento do computador
o poder torna-chaves mais viável, também.).

2.6. PGP

2.6.1. Há, realmente, uma grande quantidade de informações lá fora sobre o PGP,
a partir de versões atuais, para sites, para o servidor de chaves problemas, e assim por
em. Existem também várias boas perguntas frequentes sobre o PGP, no MacPGP, e

provavelmente, em quase todas as grandes versão de PGP. Eu não esperava
para competir aqui com mais especializados FAQs.
- Eu também não sou um PGP especialista, utilizando-o apenas para envio de e
receber e-mails, e raramente fazer muito mais com ele.
- As diversas ferramentas, para todas as principais plataformas, são uma especialidade
para si.
2.6.2. "Onde posso obter PGP?"
2.6.3. "Onde posso encontrar PGP?"
- Esperar por vários dias e um post virá pelo que
dá algumas indicações.
- Aqui estão alguns sites corrente com esta redação: (atente para
alterações)
2.6.4. "É PGP seguro? Eu ouvi alguém o tivesse...."
- relatórios periódicos, lenda urbana, que PGP foi
comprometida, que Phil Z. foi "persuadido" a....
+ implausível, por várias razões
- Phil Z já não controla o código-fonte por si mesmo
- o código-fonte está disponível e pode ser inspecionado...seria
ser muito difícil de escorregar nas principais portas traseiras que seria
não ser aparente no código-fonte
- Phil tem negado este, e os rumores que parecem vir do
ociosa especulação
+ Mas PGP pode ser quebrado?
- não foi testado de forma independente em um profundo,
cryptoanalítico forma, ainda, o parecer do tcmay)
- NSA não está dizendo
+ Áreas para o ataque
+ IDEIA
- alguns estão dizendo duplicação do número de rodadas
deve ser donatário
- os geradores de números aleatórios...Colin Prumo da admissão
2.6.5. "Eu deveria usar o PGP e outros criptografia na minha empresa
estações de trabalho?"
- máquinas de propriedade de empresas e universidades, geralmente em
redes, geralmente não seguro (isto é, eles podem ser
comprometida de várias maneiras)
- ironicamente, a maioria das pessoas que se inscrevem todas as suas mensagens,
que usar um monte de criptografia, são apenas máquinas
- PCs e Macs e outros nonnetworked máquinas são mais
seguro, mas são mais difíceis de usar o PGP (como, de 1994)
- estas são generalizações--há inseguro e PCs
seguro estações de trabalho
2.6.6. "Eu só tenho PGP--eu deveria usá-lo para todos os meus e-mails?"

- Não! Muitas pessoas não podem facilmente usar o PGP, então, se você quiser
comunicar-se com eles, não criptografar tudo. Utilização
criptografia, onde é importante.
- Se você quiser apenas as pessoas mais usam criptografia, ajuda com
os projetos para uma melhor integração de criptografia existente em
encarregados do envio da correspondência.
2.6.7. A NSA está aparentemente preocupado com o PGP, preocupado com a disseminação
de PGP para outros países, e preocupado com o crescimento da
"comunidades internas" que se comunicam através de "tubos pretos" ou
"túneis criptografados" que são impenetráveis para eles.

2.7. Clipper
2.7.1. "Como o governo pode fazer isso?"
- incredulidade de que a proibição, censura, etc. são legais
+ várias formas estas coisas acontecem
- não testado nos tribunais
- a guerra regulamentos
+ interpretações conflitantes
- por exemplo, "bem-estar geral" cláusula utilizada para justificar
restrições na expressão, liberdade de associação, etc.
+ sempre que o dinheiro público ou instalações utilizadas (como com
igrejas obrigados a contratar os Satanistas)
- e esta cada vez mais interconnnected mundo, é
às vezes, muito difícil de evitar sobreposição com o público
financiamento, instalações, etc.
2.7.2. "Por que não Cypherpunks desenvolver suas ganhou concorrentes de criptografia
chip?"
+ Muitas razões para não:
custo
- foco
- experiência
- difícil vender um tal padrão concorrentes
- melhor deixar o mercado como um todo, fazer estas escolhas
2.7.3. "Por que é criptografia tão assustadora para os governos?"
+ Retira o poder do estado para snoop, brasileiras, para
o vigiar, controlar
- Sacerdotal confessionários foram uma importante forma, a Igreja continuou a
guias sobre os moradores...um mundo, base do sistema de
eclesiástico narcóticos
+ De criptografia tem alta alavancagem
+ Ao contrário direta ataques com bombas, HERF e EMP ataques,
a sabotagem, etc, crypto é auto-lhes...uma bootstrap
tecnologia

- as pessoas usá-lo, dá-lo a outros, colocá-lo em redes
- outros usá-lo para seus próprios fins,
- um efeito de cascata, crescendo geometricamente
- e minando a confiança nos governos, permitindo a
propagação de múltiplos pontos de vista (especialmente
não aprovados visualizações)
2.7.4. "Eu só entrou para a lista e me perguntando por que eu não veja
mais debate sobre Clipper?"
- Entender que as pessoas raramente escrevo textos em resposta a
perguntas como "Por que é Clipper ruim?" Para a maioria de nós,
obrigatório chave de caução é axiomatically mal; nenhum debate é
necessário.
- Clipper foi completamente descartadas por quase todos dentro
horas e dias após o seu anúncio, 16 de abril de 1993.
Centenas de artigos e editoriais temos a condenou.
Cyperpunks atualmente não tem nenhum ativo apoiadores do obrigatórios
chave de caução, a partir de todas as indicações, então não há nada para
o debate.

2.8. Outras Cifras e Criptografia Produtos

2.9. Remetentes e Anonimato
2.9.1. "O que são remetentes?"
2.9.2. "Como remetentes de trabalho?" (um grande número de lançamentos tem
lidou com isso)
- A melhor maneira de entendê-los é "just do it", que
é, enviar alguns remailed mensagem para si mesmo, para ver como a
funciona de sintaxe. As instruções estão amplamente disponíveis-algumas são
citado aqui, e até a data de instruções que aparecem no
habitual de grupos da Usenet.
- O modo de exibição simples: mensagens de Texto são colocados em envelopes e
enviado para um site que tenha acordado para remail-los com base na
instruções de encontrar. A criptografia não é necessário--embora
é claro que é recomendado. Essas "mensagens em garrafas"
são passados de site para site e, em última análise, para o
destinatário final.
- A mensagem é texto puro, com as instruções contidas _in
o text_ em si (isso foi uma fortuita a escolha do padrão
por Eric Hughes, em 1992, pois permitiu o encadeamento,
independência a partir de determinados sistemas de email, etc.).
- Uma mensagem será algo assim:

::

Pedido-Remailing-se A: remailer@bar.baz

Corpo de texto, etc., etc. (O que poderia ser mais remailing
instruções digital, franquia, etc.)

- Estes aninhadas mensagens não faça suposições sobre o tipo de
envio de e-mails que está sendo utilizado, desde que ele pode lidar reta ASCII
o texto, que todos os e-mails pode, claro. Cada mensagem de email
em seguida, atua como uma espécie de "agente" transporte de instruções
para onde deverá ser enviado o próximo, e talvez outras coisas
(como atrasos, preenchimento, remessa postal, etc.)
- É muito importante notar que qualquer reenvio de e-mails não
veja o conteúdo dos envelopes ele é remailing, desde
a encriptação é utilizada. (O original do remetente pega uma desejado
trajetória através do labirinto de remetentes, criptografa em
a sequência adequada (último é mais íntimos, em seguida, avançar para
por último, etc.), e, em seguida, os remetentes sequencialmente desencriptar
os envelopes exteriores como obtê-los. Dentro de Envelopes
envelopes.)
2.9.3. "Não pode remetentes ser usado para intimidar as pessoas?"
- Certo, então pode liberdade de expressão, anônimo correio físico ("veneno
caneta letras"), etc.
- Com endereço de e-mail, as pessoas podem tela de seu e-mail, utilize os filtros,
ignorar palavras que não gosta, etc. Muitas opções. "Paus
e as pedras" e todas as coisas que aprendemos no jardim de Infância
(bem, eu nunca estou certo de que o Gen X aprendidas....).
- Extorsão feita um pouco mais fácil por anônimo utentes, mas
extorsão, ameaças pode ser feita de outras maneiras, como através de
correio físico, ou a partir de telefones públicos, etc.
- Ações físicas, ameaças, etc. são outra questão. Não
domínio de criptografia, de per si.

2.10. Vigilância e Privacidade
2.10.1. "A ANS monitora essa lista?"
- Provavelmente. Temos sido bastante visível, e há muitos
caminhos para o monitoramento ou até mesmo inscrevendo-se na Lista.
Muitos apelidos, muitos pontos de presença.
- algumas preocupações que Cypherpunks lista foi infiltrado
e é um "round up"lista de
- Houve mesmo mensagens anônimas pretendendo nome
provavelmente CIA, DIA, e NSA spooks. ("Ser consciente.")
- Lembre-se, a lista de assinantes _não_ é um segredo--ele pode

ser obtido através do envio de um "quem cypherpunks" mensagem para
majordomo@toad.com. Qualquer pessoa no mundo pode fazer isso.

2.10.2. "Essa lista é ilegal?"

- Depende do país. Nos EUA, existem muito forte
proteções contra a "censura prévia" para publicação
o material, de forma que a lista é bastante bem protegida....fechar
ele para baixo seria criar uma Primeira Alteração caso de grandes
importância. O que é improvável. Conspiração e sedição leis
são mais complexas para analisar; não há indicações de que
o material aqui ou na lista é ilegal.
- Defesa de atos ilegais (subversão das leis de exportação,
espionagem, etc.) geralmente é legal. Mesmo defendendo a
derrubada do governo.
- A situação em outros países é diferente. Alguns
países proibição não aprovados criptografia, para que esta lista é
suspeito.
- Praticamente, qualquer pessoa que ler esta lista é, provavelmente,
em um lugar que não faz nenhuma tentativa para controlar
criptografia ou é incapaz de monitorar o que cruza o seu
fronteiras.

2.10.3. "Pode pressionamentos de teclas realmente ser monitorado remotamente? Qual a probabilidade de
isso?"

- Sim. Van Eck, RF, monitores, fácil (afirma-se) construir
este
- Como provável? Depende de quem você é. Ames, o espião da KGB, foi
provavelmente monitorado perto do final, mas eu duvido que muitos de nós
são. Os custos são simplesmente muito alto...as vans do lado de fora, a
pessoal necessário, etc.
- os verdadeiros perigos de envolver fazer isso "fácil" e "quase
automática" para tal monitoramento, tais como Clipper e
ESTRATÉGIA europeia de emprego. Em seguida, eles, essencialmente, basta virar o interruptor e o
o monitoramento acontece...sem bagunça, sem barulho.

2.10.4. "Não seria alguns crimes de ser interrompido se o governo poderia
monitorar o que ele queria?"

- Com certeza. Esta é uma velha história. Alguns criminosos seria pego
se seus diários, que pode ser examinado. Câmeras de televisão em
todas as casas seria reduzir crimes de .... (Você está ouvindo,
Winston?).
- Orwell, o fascismo, a vigilância estados, o que você tem a
ocultar, etc.

2.11. Legal

2.11.1. "Pode criptografia de ser banido?"

- ham operadores, ondas curtas
- il gelepal, looi para waptime aolditolq
+ como é que isto é diferente de exigir a fala, em alguns idioma?
- Navaho código de locutores da 2 ª guerra mundial,,,,moderno paralelo

2.11.2. "O governo vai tentar proibição de criptografia?"

- Este é, naturalmente, a grande preocupação que a maioria de nós tem sobre Clipper e o Caucionadas Padrão de Criptografia em geral. Mesmo se pensamos que a proibição de criptografia será, por fim, um falha ("pior do que a Proibição," alguém disse), tais a proibição poderia fazer coisas muito desconfortável para muitos e seria uma grave limitação de liberdades básicas.
- Nós não sabemos, mas temos medo de algo ao longo dessas linhas. Ele vai ser difícil impor uma tal proibição, como tantas avenidas para a comunicação existe, e mensagens criptografadas podem ser rígido para detectar.
- O seu objetivo, no entanto, pode ser _control_ e refrigeração efeito usando o "confisco civis" pode ter em potencial crypto usuários. Como as leis de drogas. (Whit Diffie foi o primeiro a enfatizar esta motivação.)

2.11.3. "Como poderia criptografia de ser banido?"

- o mais provável: as restrições sobre as redes, a la ondas de rádio ou serviço postal
- poderia citar várias necessidades, mas na ausência de um mecanismo como acima, difícil de fazer
- proibição absoluta, imposta com a caducidade civil penalidades
- a guerra, o tipo de políticas (crypto tratados como sedição, traição...alguns de alto perfil de penas de prisão)

cenário a - postado por Sandfort?

2.11.4. "Qual é a situação sobre a exportação de criptografia?"

+ Há muito debate sobre isso, com o caso do Phil Zimmermann, possivelmente, ser um importante caso de teste, deve encargos de ser arquivado.
- como de 1994-09, o Grande Júri em San Jose não disse qualquer coisa (que foi cerca de 7 a 9 meses, desde que começou a sobre esta questão)
- Dan Bernstein tem argumentado que a ITAR abrange quase todos os aspectos de exportação de criptografia material, incluindo os códigos, documentação, e até mesmo "conhecimento". (Controversa, é pode ser uma violação da ITAR para conhecimento de criptografia pessoas até mesmo para deixar o país com a intenção de desenvolver

criptografia de ferramentas no exterior.)
- As várias distribuições do PGP, que ocorreram através de
ftp anônimo fontes não implica que a ITAR não está sendo
imposta, ou não será no futuro.

2.11.5. "O que é o estatuto jurídico da assinatura digital?"
- Ainda não testei no tribunal. Idem para a maioria dos protocolos de criptografia,
incluindo digital de registro de data e hora, contratos eletrônicos,
problemas de perda de chaves, etc.

2.11.6. "Não posso reclamar, eu esqueci a minha senha?"

2.11.7. "É perigoso falar abertamente sobre essas idéias?"
- Depende do seu país. Em alguns países, talvez não. No
os EUA, não há muito o que fazer (embora as pessoas
esteja ciente de que os Cypherpunks ter recebido um monte de
atenção por parte da mídia e por políticos, e, portanto, uma vocais
presença nesta lista, muito provavelmente, coloca um de uma lista de
crypto problemas políticos).
- Algumas empresas podem também sentir-se vista aqui expressos não são
consistente com suas políticas corporativas. Sua milhagem pode
variar.
- Traição e rebelião leis não são susceptíveis de ser aplicável.
- alguns Cypherpunks penso assim
- Outros de nós, tomar a Primeira Alteração muito a sério:
que _all_ falar é permitida
- NSA agentes ameaçou Jim Bidzos mortos

2.11.8. "Não é a posse de uma chave significa a posse do *identidade*?"
- Se eu obter a sua chave, eu sou você?
- Certamente não é fora do contexto da criptografia
transação. Mas, dentro do contexto de uma transação, sim.
Garantias adicionais/speedbumps pode ser inserido (como
biométricos credenciais adicionais frases-chave, etc.), mas
estes são essencialmente parte da "chave", então o básico
a resposta é "sim". (Há periodicamente preocupações
levantadas sobre isso, citando os perigos de se ter todos os
identidade vinculada a uma única credencial, ou um número, ou chave.
Bem, existem maneiras de lidar com isso, como, por exemplo, a adoção de
protocolos de limite de uma exposição, que limita a quantidade
do dinheiro que pode ser retirado, etc. Ou as pessoas podem adotar
protocolos que requerem segurança adicionais, atrasos de tempo,
countersigning, etc.)
+ Isso pode ser testado em tribunal em breve, mas a resposta para
muitos contratos e operações de criptografia será que
a posse da chave = posse de identidade. Até mesmo um tribunal
o teste pode significar pouco, para os tipos de operações I

esperar para ver.
- Que é, em sistemas anónimos, "que te vai processar?"
- Então, guarda a sua chave.

2.12. Dinheiro Digital
2.12.1. "O que é a digital de dinheiro?"
2.12.2. "Quais são os principais usos do forte de criptografia para negócios e transações econômicas?"
- Comunicações de segurança. Garantir a privacidade da transação registros (evitando eavesdroppes, concorrentes)
- A assinatura Digital de contratos (um dia vai ser padrão)
- Dinheiro Digital.
- Reputações.
- Dados Paraísos. Que ignoram as leis locais sobre o que pode ser armazenado e o que não pode (por exemplo, regras bobas de quão longe registros de crédito pode ir).
2.12.3. "O que são cartões inteligentes e como eles são usados?"
+ Mais cartões inteligentes como eles agora existem estão muito longe de ser anônimo digital de caixa de principal interesse para nós. No de fato, a maioria deles são apenas glorificado cartões de crédito.
- com nenhum ganho para os consumidores, uma vez que consome normalmente não paga para perdas por fraude
- (de modo a atrair consome, eles te oferecem incentivos?)
- Podem ser pequenos computadores, normalmente de crédito-cartão de tamanho, ou apenas cartões de controle de acesso através de computadores locais.
+ Inviolável módulos, por exemplo, se adulterados, eles destruir os dados importantes, ou pelo menos, dar provas de depois de ter sido adulterado.
+ De segurança de fabricação
- alguma variante de "cortar-e-escolha" de inspeção de instalações
+ Utiliza de cartões inteligentes
- cartão de crédito convencionais usa
- pagamento de contas postagem
- ponte e as portagens
- pagamentos para os itens recebidos eletronicamente (não necessariamente anonimamente)

2.13. Crypto Anarquia
2.13.1. "O que é Criptografia Anarquia?"
- Alguns de nós acreditamos várias formas de criptografia forte fará com que o poder do estado em declínio, talvez até mesmo

colapso bastante abruptamente. Acreditamos que a expansão em
o ciberespaço, com comunicações seguras, dinheiro digital,
o anonimato e a pseudonímia, e outros crypto-mediada
medicamentosas, vai mudar profundamente a natureza de
as economias e as interações sociais.

Os governos têm um tempo difícil a cobrança de impostos,
regular o comportamento dos indivíduos e corporações
(pequenos, pelo menos), e, geralmente, coagindo as pessoas quando ele
não pode sequer dizer que _continent_ pessoas estão on!

Leia Vinge de "Nomes Verdadeiros" e do Cartão "Ender do Jogo" para
alguns de ficção inspirações. "Galt Gulch" no ciberespaço,
o que a internet está rapidamente a tornar-se já.

Eu chamo isso de um conjunto de idéias "crypto anarquia" (ou "crypto-
a anarquia", como você quiser) e tenho escrito sobre isso
extensivamente. A revista "Wired" (questão 1.2), "Toda a
Earth Review" (Verão, 1993), e "The Village Voice" (Ago.
6º, 1993) realizou bons artigos sobre isso.

2.13.2. A Criptografia Manifesto Anarquista

- uma cópia completa do meu 1988 pastiche do Communisto
Manifesto está incluído no capítulo sobre a Criptografia de Anarquia.
- ele precisa reescrever, mas históricos, amor eu deixei ele
inalterado.
- Estou orgulhoso de que muito da sua exactidão.

2.13.3. "O que é BlackNet?"

- BlackNet -- uma experiência em mercados de informação, utilizando
anônimo mensagem de piscinas para a troca de instruções e
itens. Tim Poderá experiência de guerrilha ontologia.
- BlackNet -- um regime experimental concebido por T. Maio
sublinhado a natureza das informações anônimas mercados.
"Qualquer e todos os" segredos podem ser oferecidos para venda através do anônimo
e-mails e mensagem de piscinas. O experimento foi transmitida através de
reenvio de e-mails para os Cypherpunks lista (não Pode) e daí para
várias dezenas de grupos da Usenet por Detweiler. As autoridades
são disse a ser investigá-lo.

2.13.4. "Que efeito de criptografia têm sobre os governos?"

- Um tópico enorme, que eu venho pensando desde o final de 1987
quando me dei conta de que a criptografia de chave pública e anônimo
dinheiro digital sistemas, informação de mercados, etc. significava que a
fim dos governos como os conhecemos. (Eu chamei esse
desenvolvimento de "crypto anarquia." Nem todo mundo é fã dele.

Mas ele está vindo, e rápido.)
- "Colocando a NSA fora do negócio", como o artigo do NYT colocar
ele
A espionagem está mudando. Para pegar um exemplo, "digital mortos
cai." Qualquer mensagem pode ser enviada através de um caminho untraceable
com remetentes....e, em seguida, publicado em forma criptografada em um
grupo de notícias legível na maioria dos países, incluindo o Ex -
União Soviética. Isso significa que o antigo stand by dos microfilmes
em uma lata de Coca-cola para a esquerda por uma certa árvore em uma estrada rural--um
método cheio de atrasos, perigos e aborrecimentos--é agora
passe. A mesma mensagem pode ser enviado a partir do conforto de
em casa de forma segura e untraceably. Mesmo com uma digital
assinatura para evitar a falsificação e a desinformação. Este espião
pode ser um Lockheed trabalhador na Aurora do programa, um SIGINT
oficial de Woomera, ou descontentes chip designer
Motorola. (Sim, uma medida defensiva é para limitar o acesso a
computadores pessoais, para executar apenas o software padrão que tem
nenhuma criptografia capacidade. Tais embargos, já podem aplicar -
para alguns cargos sensíveis, e podem algum dia ser um
condição de emprego.)
- Lavagem de dinheiro
- A cobrança de impostos. Consultores internacionais. Perpétua
os turistas. Virtual corporações.
- O terrorismo, assassinato, crime, Tríades, Yakuza, Jamaicanos,
Máfia russa...redes virtuais... Aryan Nation ido
digital
2.13.5. "Como rapidamente pode algo como criptografia anarquia vem?"
- Partes estão acontecendo, já que as mudanças na
o mundo não são algo que eu tomar nenhum crédito. Em vez disso,
estão em curso mudanças no papel das nações, do poder,
e a capacidade de impor comportamentos. Quando as pessoas podem
queda de sistemas que não gosta, pode mover-se para diferentes
legal ou jurisdições fiscais, em seguida, mudar as coisas.
+ Mas uma mudança de fase pode ocorrer rapidamente, assim como o de Berlim
A parede era inexpugnável um dia, e até a próxima.
- "Público raiva cresce silenciosamente e explode de repente. T. C.
Em maio, "mudança de fase" pode estar mais perto do que pensamos. Ninguém
na Rússia em 1985 realmente achava que o país ia cair,
além de 6 anos." [Mike Ingle, 1994-01-01]
2.13.6. "Poderia forte de criptografia a ser usado para os doentes e nojento e
perigoso propósitos?"
- Claro. Assim, pode portas trancadas, mas nós não insistir em uma
"política de porta aberta" (fora de certos singular do grêmio e

casas de cômodos!) Modo de fazer muitas formas de permitir privacidade
plotters, molestors, racistas, etc. para atender e enredo.
- Crypto está em uso por Ariana Nação, tanto pela pró - e anti-
o aborto grupos, e provavelmente por outros tipos de terroristas.
Esperar mais usa no futuro, como coisas, como o PGP continuar
para espalhar.
- Muitos de nós são explicitamente anti-democrática, e a esperança de usar
criptografia para minar o chamado democrática
os governos do mundo

2.13.7. "O que é o Jantar Criptógrafos Problema, e por que é tão
importante?"

+ Esta é tratada na seção principal, mas aqui é David
Chaum Abstrata, a partir de sua 1988 papel"
- Resumo: "Manter confidenciais que envia as mensagens que,
em um mundo onde qualquer físico de transmissão pode ser rastreada
a sua origem, parece impossível. A solução apresentada
aqui é incondicionalmente ou criptograficamente segura,
dependendo se ele é baseado no uso de uma vez teclas ou
em chaves públicas. respectivamente. Ele pode ser adaptado para
lidar de forma eficiente com uma ampla variedade de práticas
considerações." ["O Jantar Criptógrafos Problema:
Incondicional do Remetente e do Destinatário Untraceability," David
Chaum, Diário da Criptologia, I, 1, 1988.]
-
- DC-redes não foram implementados, tanto quanto eu sei, mas
eles representam um "puro", versão de física remetentes
estamos todos tão familiarizados com o agora. Um dia eles vão ter
um grande impacto. (Eu sou um grande fã do trabalho de muitos
parecem ser, como há pouca discussão no sci.cripta e
o como.)

2.13.8. "Por que não o governo simplesmente proibir tais métodos de encriptação?"

+ Esse sempre foi o Problema Número Um!
- criado por Stiegler, Drexler, Salin:, e vários outros
(e, na verdade, levantadas por alguns como uma objeção à minha mesmo
ao abordar estas questões, a saber, que a ação, em seguida, pode ser
levado para a cabeça fora do mundo que eu descrever)
+ Tipos de Proibições sobre Criptografia e Sigilo
- Proibição de Utilização Privada de Criptografia
- Proibição de Armazenar e Encaminhar Nós
- Proibição e Tokens de Autenticação ZKIPS
- Requisito para a divulgação pública de todas as transações
+ Notícias recentes (3-6-92, mesmo dia em que Michaelangelo e
Cortador de grama Homem) que o governo está propondo uma sobretaxa

em empresas de telecomunicações e serviços de longa distância para pagar novas equipamentos necessários para a toque de celulares!
- S. 266 e facturas relacionadas com a
- esta foi a argumentar em termos de parar os traficantes de drogas e outros criminosos
- mas, como o governo pretende lidar com os várias formas fo usuário final de criptografia ou "confusão" (a confusão que vai vir de compressão, packetizing, simples de criptografia de arquivo, etc.)
+ Tipos de Argumentos Contra Tais Proibições
- Os "Direitos Constitucionais" Argumentos
+ "É Tarde Demais" Argumentos
- PCs já estão amplamente espalhados, a execução de dezenas de a compressão e encriptação de programas...é muito final de insistir "em claro" transmissões, qualquer que seja pode ser (é código de programa distinguível de mensagens criptografadas? Não.) criptografado por fax, modem geralmente (embora com algumas restrições)
- as LANs sem fios, pacotes, rádio, IV, do texto comprimido e imagens, etc....tudo vai derrotar qualquer esforços curtos de a polícia de intervenção do estado (que ainda pode acontecer)
+ A "Briga Dentro da NSA" Argumentos
- COMSEC vs. PROD
+ Afetará os direitos de privacidade das empresas
- e há muita evidência de que as empresas estão em fato a ser espiado, por governos estrangeiros, pelos NSA, etc.
+ Eles Vão Tentar Proibir Tais Técnicas de Criptografia
+ Picadas (talvez usando vírus e bombas lógicas)
- ou "de bário", para rastrear o código
+ De responsabilidade Legal para empresas que permitem que os funcionários usem tais métodos
- talvez, até mesmo, no seu próprio tempo, através da suposição de que os funcionários que usam software ilegal métodos em suas próprias tempo são, talvez, correios ou agentes para a sua corporações (um tênue ponto)

2.13.9. "Poderia anônimo mercados facilitar repugnante serviços, tais como assassinatos para contratar?"
- Sim, mas há algumas coisas que vai ajudar a diminuir o impacto total.
- Para fazer essa brutalmente concreto, veja como caução faz assassinato de contratos muito mais seguro do que eles são hoje a

negociar. Em vez de um partido de ser pego em uma FBI
sting, como é frequentemente o caso quando amadores tentar organizar
hits, eles podem usar uma garantia de serviço para isolar-se
a partir de:

1. De ser analisado, porque as trocas são manipulados através de
pseudônimos

2. A partir do assassino pegando o dinheiro e não a realização de
o sucesso, porque a custódia do agente detém o dinheiro até que o
assassinato é verificada (de acordo com algumas prototocol, tal
reportagem do jornal...mais uma vez, uma área de mais trabalho,
felizmente).

3. De ser preso quando o dinheiro é levantado, como este
tudo é feito através de dinheiro digital.

Existem algumas maneiras de reduzir a popularidade deste
Assassinato, Incorporou o sistema. (Coisas que eu venho pensando
sobre por cerca de 6 anos, e o que discutimos sobre o
Cypherpunks lista e, na Extropians lista.)

2.14. Diversos
2.14.1. "Por que as pessoas não só concordam em uma abordagem?"
- "Por que não podemos todos apenas apoiar minha proposta?"
- "Eu propunha uma nova codificação, mas ninguém está interessado...você
Cypherpunks nunca _do_ nada!"
- Este é um dos the, de forma mais consistente questões divisórias no
a lista. Muitas vezes uma pessoa vai se tornar apaixonado de alguma abordagem,
vai escrever posts, exortando as pessoas a se tornarem da mesma forma
apaixonado, incitando outros a "fazer alguma coisa!," e, em seguida,
quando não há interesse é evidenciado, tornar-se irado. Para ser mais
de concreto, isto acontece mais frequentemente com vários e diversos
propostas de "dinheiro digital." Em segundo lugar é para
vários tipos de "Cypherpunks ativismo", com propostas
que ficamos juntos e coletar alguns milhões de dólares para
executar Ross Perot-tipo de publicidade incentiva as pessoas a usar
PGP, com chamadas para um "Cypherpunks programa de rádio," e assim por diante.
(Nada de errado com as pessoas fazendo essas coisas, eu suponho.
O problema está na exortação de _others_ para fazer essas
coisas.)
- Esta ação coletiva, é sempre difícil de alcançar, e
com razão, na minha opinião. Comportamento emergente é mais

natural e mais eficiente. E, portanto, melhor.
+ a natureza dos mercados, agentes, diferentes agendas e metas
- padrões reais e os mercados evoluem
- às vezes por causa de um forte exemplo (o Walkman,
PGP), às vezes por causa do trabalho duro por normas
comissões (NTSC, tomadas eléctricas, etc.)
- mas quase nunca por simples apela para correção ou
ideológica acerto
2.14.2. "Quais são os limites práticos para a implantação de
crypto, especialmente coisas como dinheiro digital e remetentes?"
+ Falta de confiança de serviços
- Nós de ir para baixo, os alunos vão para casa para o verão, o tempo de inatividade
por várias razões
- Falta de robustez
2.14.3. "É de criptografia dominada pela desconfiança? Eu tenho a impressão de que
tudo se baseia na desconfiança mútua."
- Nós fechamos nossas portas...isso significa que estamos com falta de confiança?
Não, isso significa que entender que existem _some_ lá fora que
vai explorar destrancar portas. Idem para a criptografia do mundo.
- "Confie, mas verifique", como Ronald Reagan, costumava dizer. Mútuo
a desconfiança pode realmente tornar mais confiável
ambiente, por mais paradoxal que isso possa parecer. "Mesmo paranoids
ter inimigos."
- O perigo em um ambiente confiando que carece de outros
mecanismos é que "predadores" ou "desertores" (em jogo-
teórico termos) pode explorar esta confiante ambiente.
Jogos de confiança, golpes, renegging em negócios, e até mesmo
definitivas roubo.
- Crypto oferece a oportunidade para "mutuamente suspeitos,
agentes" para interagir sem a permissão "confiança".
2.14.4. "Quem é Detweiler?"
+ S. Boxx, an12070, ldxxyyy, Pablo Escobar, Hitler, Linda
Pirulito, Novelo Lance Bobo, tmp@netcom.com Jim
Riverman
- muitas vezes com a minha sig bloco, ou variantes do mesmo, anexado
- mesmo o meu número de telefone
- ele perdeu sua ColoState conta de tais táticas...
- electrocrisy
- cypherwonks
2.14.5. "Quem é Sternlight?"
- Um aposentado de política de analista, que é muitas vezes controverso na Usenet
grupos e apoio das políticas governamentais sobre a criptografia
política. Quase tão mau como Detweiler.

2.15. Mais Informações e Referências
2.15.1. "Onde posso encontrar mais informações?"
- Bem, esse é um começo. Além disso, muitas outras perguntas frequentes e Mosaico
casa de páginas (URLs) existem, abrangendo uma vasta quantidade de
conhecimento.
- Contanto que este FAQ é, ele só pode riscar a superfície em
muitos tópicos. (Eu estou especialmente divertido quando alguém diz
eles olharam para um FAQ sobre algum tópico obscuro. Nenhuma das perguntas frequentes
provavelmente para responder a todas as perguntas, especialmente obcure queridos.)
- Muitos artigos e papers estão disponíveis no
ftp.csua.berkeley.edu
site, no pub/cypherpunks. Olhar em torno de lá. Em 1981, Chaum
papel em untraceabel e-mail não é (muitas equações para
digitalização fácil), mas a 1988 papel no Jantar Criptógrafos
Redes é. (Eu laboriosamente digitalizados-a e Ocr-a, quando
Eu costumava ter a energia para fazer tais ingrata tarefas.)
+ Algumas fontes básicas:
+ Sci.cripta FAQ, publicada regularmente, Também disponível
ftp anônimo em rtfm.mit.edu. E em várias URLs,
incluindo:
URLs para o sci.cripta FAQ: xxxxxx
- RSA Data Security Inc. Perguntas frequentes
- Bruce Schneier "applied Cryptography", e do livro, 1993. Todos
o leitor desta lista deve ler este livro!
- A "geração on-line" tende a querer todo o material on-line,
Eu sei, mas a maioria das coisas boas é para ser encontrada em papel
forma, em revistas e livros. Este é provavelmente o caso
por muitos anos, dada a limitação de caracteres ASCII, o
a falta generalizada de padrões (sim, eu sei sobre o Látex,
etc.), e o prestígio acadêmico associado vinculado
revistas e livros. Felizmente, você pode encontrar _all_
universit bibliotecas dentro do intervalo de condução. Tome o meu conselho:
se você não passar, pelo menos, um todo sábado imersão
mesmo na crypto literatura na matemática secção de um
grande biblioteca, folheando o "Procedimentos de Criptografia
Conferência" os volumes, a digitalização de livros de texto, então você tem
uma fundação fraca para fazer qualquer criptografia de trabalho.
2.15.2. "As coisas estão mudando rapidamente. Nem todos os endereços de e
URLs aqui indicados são válidos. E as versões de software Como...
posso obter as informações mais recentes?"
- Sim, as coisas estão mudando rapidamente. Este documento não pode
possivelmente acompanhar as rápidas mudanças (nem pode seu

autor!).
- Lendo os vários grupos de notícias é, como sempre, a melhor maneira
para ouvir o que está acontecendo no dia-a-dia. Páginas da Web
gopher, archie, veronica, etc. deve mostrar os mais recentes
versões de pacotes de software populares.
2.15.3. "FUQs: "Frequentemente Perguntas Não Respondidas"?"
- (mais a ser adicionado)
- Com 700 ou mais pessoas sobre os Cypherpunks (lista de 94-
09), é inevitável que alguns FAQs ficará sem resposta
quando novatos (ou outros) pedir-lhes. Às vezes, o FUQs são
ignorados porque eles são tão obsoletos, outras vezes porque a
respondê-las é para continuar e infrutífera thread.
+ "P = NP?"
- Steve Smale tem chamado este novo e mais importante
problema não resolvido de última metade do século passado.
- Se P foram (inesperadamente) provado ser NP
+ É o RSA e o factoring no PN?
- ainda não provou
- factoring, pode ser mais fácil
- e o RSA pode ser mais fácil do que de factoring em geral (por exemplo,
escolhido - e conhecido-plaintext pode fornecer pistas)
- "Vai criptografia de ser banido? O que vai acontecer?"
+ "É David Sternlight um agente da NSA?"
- A sério, David S. é, provavelmente, o que ele afirma: um aposentado
o economista, que já foi muito altos no governo e
política corporativa círculos. Eu não tenho nenhuma razão para duvidar dele.
- Ele tem vistas em desacordo com a maioria de nós, e uma rinha de estilo
de expressar seus pontos de vista, mas isso não significa que ele é um
agente do governo, como muitos afirmam.
- Não na mesma classe como Detweiler.

3. Cypherpunks -- História, Organização, Agenda

3.1. direitos autorais

3.2. RESUMO: Cypherpunks -- História, Organização, Agenda
3.2.1. Pontos Principais
- Cypherpunks formada em setembro, 1992

- formado em um momento oportuno, com o PGP 2.0, Clipper, etc.
bater
- primeiros sucessos: Cypherpunks remetentes, publicidade
3.2.2. Ligações para Outras Secções
3.2.3. Onde Encontrar Informações Adicionais
- "Wired, o" problema 1.2, tinha uma reportagem de capa na Cypherpunks.
- "Whole Earth Review" Verão de 1993, tinha um longo artigo sobre
criptografia e Cypherpunks (incluído no livro "Fora de
Controle", por Kevin Kelly.
- "Village Voice", do dia 6 de agosto (?). De 1993, teve reportagem de capa na
"Crypto Rebeldes" (também reproduzido no local semanários)
- e inúmeros artigos em várias revistas
3.2.4. Diversos Comentários
- a melhor maneira de começar uma sensação para a Lista é para simplesmente ler
por um tempo; alguns meses deve fazer.

3.3. Os Cypherpunks Grupo e Lista de
3.3.1. O que é?
+ Regras formais, Carta, etc.?
- não há regras formais ou carta
- não acordada missão
3.3.2. "Quem são os Cypherpunks?"
- Uma mistura de cerca de 500-700
+ Pode descobrir quem enviando mensagem para majordomo@toad.com
com o corpo de mensagem de texto "que cypherpunks" (sem aspas,
curso).
- Isso é uma falha de privacidade? Talvez.
- Muitos dos estudantes (eles têm o tempo, a Internet
contas). Lotes de informática/programação pessoal. Lotes
dos libertários.
- citação de Fios artigo, e a partir de "Whole Earth Review"
3.3.3. "Como foi que os Cypherpunks grupo de começar?"
+ História?
- Discussões entre Eric Hughes e me levou para Eric
decisão de host para um encontro
+ Primeira reunião foi, por coincidência, na mesma semana em que o PGP
2.0 foi lançado...temos todas as cópias que dia
- sessão da manhã em fundamentos
- o sentado no chão
+ tarde jogamos o "Crypto Jogo"
- remetentes, dinheiro digital, para venda, etc.
- John Gilmore ofereceu seu site para hospedar uma lista de discussão e
sua empresa de escritórios para realizar reuniões mensais

- A lista de discussão começou quase imediatamente
- O Nome De "Cypherpunks"?
3.3.4. "Deve-se juntar Cypherpunks lista de discussão?"
- Se você está lendo isso, é claro, muito provavelmente, você está
os Cypherpunks lista já, e esse ponto é discutível--você
em vez disso, pode estar se perguntando se você should_leave_ a Lista!
- Só se você estiver preparado para lidar com 30-60 mensagens de um dia,
com volumes de flutuação descontroladamente
3.3.5. "Como eu posso participar da lista de discussão Cypherpunk?"
- enviar mensagem "majordomo@toad.com" com um _body_ texto de
"subscrever cypherpunks" (sem aspas no, de
curso).
3.3.6. "A associação?"
- sobre 500-700 a qualquer momento
- muitas pessoas se juntar, são dominados, e sair
- outros grupos: Austin, no estado do Colorado, Boston, no reino UNIDO.
3.3.7. "Por que há tantas libertários no Cypherpunks lista?"
+ A mesma pergunta muitas vezes é questionado sobre a Net em geral.
Muitas as razões sugeridas:
- Uma lista como Cypherpunks vai ter de privacidade e
defensores da liberdade. Nem todos os defensores da privacidade estão
os libertários (por exemplo, eles podem querer as leis restritivas de dados
coleção), mas são muitas. E libertários, naturalmente,
gravitam em torno de causas como a nossa.
- Net cresceu anarchically, com pouco controle. Este recurso
a free-wheeling tipos, utilizados para fazer suas próprias escolhas
e a construção de seus próprios mundos.
- Libertários são céticos de estruturas de controlo central,
assim como a maioria de programação de computadores, tipos. Eles são
céticos de que uma central de controle de execução do sistema pode
coordenar as necessidades e desejos das pessoas. (Eles são de
claro, mais do que apenas "cético" sobre isso.)
- Em qualquer caso, não há muito coerente "da oposição
acampamento" para o anarco-capitalista, ideologia libertária.
Perdoe-me por dizer isso, a minha não-libertário amigos
a lista, mas a maioria dos não-libertário ideologias que eu vi
expressas na lista têm sido fragmentadas, isoladas e
não coerentes...comentários sobre "como cuidar do
pobres?" e o fundamentalismo Cristão, por exemplo. Se não há
é uma alternativa coerente para uma basicamente libertário
ponto de vista, não vimos ele na lista.
- (É claro que alguns podem dizer que os libertários outshout
as alternativas...eu acho que isto não é realmente assim.)

3.3.8. "Como é que a lista de discussão começou?"
- Hugh Daniel, Eric Hughes, e eu conversamos sobre isso o dia
após a primeira reunião
- lista de discussão reuniu diversos interesses
- Como hoin?
3.3.9. "Como é que Cypherpunks obtenha muito cedo publicidade?"
- começou na hora certa, assim como o PGP foi ganhando
popularidade, como planos de chave de caução estavam sendo colocados (eu
soou um alarme em outubro, de 1992, seis meses antes do
Clipper anúncio), e apenas como "Fios", estava-se preparando
a sua primeira edição
- Kevin Kelly e Steven Levy participou de alguns dos nossos primeiros
reuniões, preparando o palco para muito favorável principais
histórias "com Fios" (questão 1.2, a reportagem de capa), e "Todo o
Earth Review" (Verão, De 1993)
- um nicho para um "renegade" e "macaco-arrancamento" de grupo, com
menos de um Washington foco
- publicidade na "Wired", "The Whole Earth Review", "O
Village Voice"
+ Clipper bomba ocupavam muito do nosso tempo, com alguns
efeito sobre a política de
- clima de repúdio
- links para FEP, CPSR, etc.
3.3.10. "Qual o nome?"
- Jude Milhon apelidos nos
- cypherpunkts? (por analogia com Mikropunkts, micropontos)
3.3.11. "Quais foram as primeiras reuniões, como?"
- cypherspiel, Criptografia Anarquia Jogo
3.3.12. "Onde estão os lugares que eu possa atender a outras Cypherpunks?"
- reuniões físicas
- comece o seu próprio...pizza place, sala de aula
+ outras organizações
-
+ "Este tipo de reuniões (DC 2600 reunião no Pentágono Cidade
Shopping, 1º Sex. de
- a cada mês, o tribunal de comida, cerca de 5-7 ou assim) pode
ser bons lugares para
- local cypherpunks reuniões. Tenho certeza de que há
são um monte de outras
- essas reuniões, mas a DC e Baltimore estão a
que eu saiba. <Stanton McCandlish, 7 De Abril De 1994>
- (nota que a DC já atende...)
- Hackers, raves

- encontros regionais

3.3.13. "É o Cypherpunks lista monitorado? Tem sido infiltrada?"

- Desconhecido. Não seria difícil para qualquer um para ser o monitoramento
a lista.
- Como a infiltração, nenhuma evidência para isso. Nenhum suspeito
gente aparecendo nos encontros presenciais, pelo menos até agora
como eu posso ver. (Não é uma indicação confiável.)

3.3.14. "Por que não existe um programa de recrutamento para aumentar o número de
de Cypherpunks?"

- Boa pergunta. A lista de discussão atingiu cerca de 500
assinantes de um ano atrás e manteve-se relativamente
constante desde então; muitos assinantes soube da lista
e o seu endereço em vários artigos que apareceram.
- Organizações informais, muitas vezes, de nível em associação
porque nenhuma equipe existe para divulgar, recrutar, etc. E
o tamanho é limitado, porque um grupo maior, perde o foco. Assim,
alguns estase é alcançado. Para nós, pode ser no 400-700
nível. Parece improvável que a associação da lista de jamais
entrar em dezenas de milhares.

3.3.15. "Porque tem havido algumas melhorias reais na criptografia
recentemente?"

+ Apesar de o esmagar de criptografia releases-o WinPGPs,
SecureDrives, e dezenas de outros programas--o fato é
que a maioria destes são simples variantes no que eu
acho que foram as duas principais classes de produtos a ser
introduzido nos últimos anos"
- PGP, e variantes.
- Remetentes, e variantes.
- Estas duas classes principais responsáveis por cerca de 98% de todos os produtos
ou a versão orientada para o debate sobre o Líquido, representado pelo
zilhões de "Onde eu posso encontrar PGP2.6ui para a Amiga?"
tipos de posts.
+ Por que isso é assim? Por que essas dominado? O que mais é
necessário?
+ Primeiro, PGP deu um incrível impulso para toda a questão
de uso público de criptografia. Ele trouxe de criptografia para as massas,
ou pelo menos para a rede de reconhecimento de massas. Segundo, a quase
aparecimento simultâneo de remetentes (a Kleinpaste/Julf-
o estilo e o Cypherpunks "mix"de estilo) se encaixam bem com
a súbita percepção sobre o PGP e problemas criptografia. E
outros simultânea de fatores apareceu:
- a aparência da "Wired", e o seu sucesso espetacular,
no início de 1993

- o Clipper chip firestorm, com início em abril de 1993
- o Cypherpunks grupo foi rolando no final de 1992,
alcançar visibilidade pública em vários artigos, em 1993.
(Até o final de '93, parecia ser um substantivo, como Bucky
poderia ter dito.)
+ Mas por que tão pouco progresso em outras áreas importantes?
- dinheiro digital, apesar de pelo menos uma dúzia de comunicados
projetos, programas (apenas alguns que são realmente
nada como Chaum do "dinheiro digital")
- dados paraísos, informação de mercados, etc.
- lavagem de dinheiro, esquemas, etc.
+ O que poderia mudar isso?
- Mosaico, WWW, Web
- O sucesso de um esforço de dinheiro digital

3.4. Crenças, Objetivos, Agenda
3.4.1. "Há um conjunto de crenças que a maioria dos Cypherpunks apoio?"
+ Não há nada oficial (não muito), mas há um
emergente, conjunto coerente de crenças que a maioria dos membros da lista
parecem conter:
* que o governo não deve ser capaz de rastrear em nosso
assuntos
* que a proteção de conversas e trocas é uma básicas
direito
* que esses direitos precisam ser protegidos, através de
technology em vez de através de lei
* que o poder da tecnologia, muitas vezes cria nova política
realidades (daí a lista mantra: "Cypherpunks escrever
código")
+ Gama de Crenças
- Muitos são libertário, mais suporte direitos de privacidade,
alguns são mais radicais em apppoach
3.4.2. "O que são Cypherpunks interesse?"
- privacidade
- tecnologia
- encryition
- política
- crypto anarquia
- dinheiro digital
- protocolos
3.4.3. A Privacidade e Colapso de Governos
- Parece que há duas razões principais que as pessoas são atraídas para
Cypherpunks, além gerais de atractividade de um "legal"

grupo como o nosso. A primeira razão é _personal privacy_.
Isto é, ferramentas para garantir a privacidade, a proteção de um
a vigilância da sociedade, e a escolha individual. Esta razão é
muito popular, mas não é sempre convincente (afinal,
por que se preocupar com a privacidade e, em seguida, aderir a uma lista
tem sido identificado como um "subversivo" de grupo pela Pf?
Algo para se pensar.)
- A segunda maior é a liberdade pessoal, através da redução da
o poder dos governos para coagir e fiscais. Uma espécie de digital
De Galt Gulch, por assim dizer. Libertários e
anarchocapitalists são especialmente desenhados para esta visão, uma
a visão que podem incomodar convencional liberais (quando eles
perceber o forte de criptografia significa que as coisas contador para o bem-estar,
AFDC, leis antidiscriminatórias....).
- Esta segunda visão é mais controversa, mas é, na minha
opinião, o que realmente alimenta a lista. Enquanto outros podem
frase de forma diferente, a maioria de nós perceber que estamos no
algo que vai mudar, e já está mudando-o
a natureza do equilíbrio de poder entre os indivíduos e
entidades maiores.
3.4.4. Por que é Cypherpunks chamado de uma "anarquia"?
- Anarquia significa "sem um líder" (cabeça). Muito mais comuns
do que as pessoas podem pensar.
- A associação com a bomba jogando "anarquistas" é
enganosa.
3.4.5. Por que não há uma agenda formal, organização, etc.?
- nenhuma votação, nenhuma organização para administrar tais coisas
- "se não está quebrado, não corrigi-lo"
- e como é que tudo começou e evoluiu
- também, ninguém para prender e problemas, sem absurdo sobre
o preenchimento de formulários e obter isenções de impostos, não há leis sobre
campanha de violações de lei (se nós éramos um grupo formal e
pressionou contra o Senador Foo, pode ser atingido com a lei
limitação de "interesses especiais" teoricamente)
3.4.6. Como são projetos de propostas e concluída?
- Se a anarquia, como as coisas são feitas?
- A maneira que as coisas são feitas: ações individuais e de mercado
decisões.
3.4.7. As Necessidades futuras, para que o Ciberespaço
+ Marca Pesci ideias para VR e simulações
distribuído e de alta largura de banda
- um bilhão de usuários
- espaciais ideias....coordenadas...servidores holográfico...

modelos
- WWW plus motor de renderização = espaciais VR (Biblioteca de
O congresso)
- "O Labirinto"
+ diz para evitar head-mounted displays e luvas (de ruim para
você)
+ em vez disso, "percepção cibernética".
- phi--fecks--psi (phi é o mundo externo,Fx = fects são
effectuators e sensores, o psi é o seu estado interno)
3.4.8. Privacidade, Credenciais sem identidade
3.4.9. "Cypherpunks escrever código"
- "Cypherpunks quebrar as leis que eles não gostam"
- Não ficar louco, ficar mesmo. Escrever o código."
3.4.10. Digital Em Mercado Livre
+ forte de criptografia altera a natureza e a visibilidade de muitos
económica transactionst, o que torna muito difícil para
os governos interferir ou até mesmo para fazer cumprir as leis,
contratos, etc.
- assim, alterações na natureza do contrato de execução
+ (Provas de que este não está perdido pode ser encontrado em
vários locais:
- criminal mercados, onde os governos, obviamente, não pode ser
usado
- mercados internacionais, a la "Lei do Comerciante"
- "dizer uma seleção"
- centros comerciais no ciberespaço...não identificável nacional ou
regional de jurisdição...sobreposição de muitas fronteiras...
+ contrapartidas (embora agências de classificação de risco, e outras filtro
agentes, pode ser usado por cauteloso com os clientes....ironicamente,
reputação importa ainda mais do que agora)
- não a capacidade de repudiar uma venda, para ser um doador Índio
- em todos os tipos de informações....
3.4.11. O Papel do Dinheiro
- em monetarizing transações, acesso, remetentes---digital
postagem
3.4.12. Reduções na tributação
- ventos entidades já a isenção
- paraísos fiscais
- ciberespaço a localização é problemático
3.4.13. O transnacionalismo
- regras das nações são ignorados
3.4.14. Dados Paraísos
- crédito, médico, legal, locatário, etc.

3.4.15. MOOs, MUDs, SVRs, Habitat cyberspaces
- "Nomes verdadeiros" e "Snow Crash"
- O que são
+ Habitat....Chip e Randy
- A Lucasfilm, Fujitsu
- começou como ambiente de jogo...
- muitos ambientes de usuário
- comunicações de largura de banda é um recurso escasso
- object-oriented representação de dados
+ de implementação de plataforma sem importância gama de...
recursos
- de texto puro para o Real ade Motores
- nunca cheguei até preencher totalmente a realidade
- "detalhado planejamento central é impossível; não mesmo de tentar"
- 2-D de gramática para layouts
+ "não pode confiar em ninguém"
- alguém desmontado o código e encontrou uma maneira de fazer
- se invisível
- formas de quebrar o sistema (dinheiro extra)
+ de melhorias futuras
- objectos multimédia, personalizável, objetos, locais relvados,
múltiplas interfaces
- "Global Ciberespaço Infra-estrutura" (Fujitsu, MULTA)
+ mais largura de banda significa mais coisas podem ser feitas
- B-ISDN permitirá vídeo sob demanda, VR, etc.
- protocolo de especificações, Joule (secure simultâneas operacional
sistema)
- intereaction espaços topológicos (não espacial)
+ Xerox, Pavel Curtis
+ LambdaMOO
- 1200 usuários diferentes por dia, 200 de cada vez, 5000 total
usuários
- social "realidades virtuais"--comunidades virtuais
- como propriedades emergentes surgem
- pseudo-espacial
- quartos, áudio, vídeo, múltiplas telas
- a polícia, assistentes, mediação
- eficaz teletrabalho
- necessidade de a riqueza do mundo real mercados...as pessoas podem vender
para outros
+ Existe um conjunto de regras ou idéias básicas que podem formar o
base de uma poderosa replicável sistema?
- isso permitiria franquias para ser disctrubed todo o

mundo
- redes de servidores? distinção entre o servidor e
cliente se desvanece...
- dinheiro, comercialização?
- Joule idioma
3.4.16. "É a privacidade pessoal o principal interesse dos Cypherpunks?"
- Assegurar a _right_ e o _technological feasibility_ é
mais o foco. Isso muitas vezes surge em dois contextos:
- 1. A acusação de hipocrisia, porque as pessoas não usam
pseudônimos ou, paradoxalmente, que o que não é uso
pseudônimos, assinaturas digitais
3.4.17. "Não deve crypto ser regulamentado?"
- Muitas pessoas fazem comparações com o regulamento de
automóveis, do espectro de rádio, e até mesmo de armas. O
comparação de criptografia para as armas de fogo é especialmente fácil de fazer,
e especialmente perigoso.
-
+ Uma melhor comparação é "o uso de criptografia = direito de falar como
você deseja."
- Que é, não se pode exigir que as pessoas falam em um idioma
ou o formulário que é facilmente compreensível para os bisbilhoteiros,
wiretappers, e espiões.
+ Se eu optar por falar com os meus amigos em letão, ou em
Elihiuish, ou em
- triple DES, que é o meu negócio. (Momentos de verdadeira guerra, como
na segunda Guerra Mundial
- II podem ser ligeiramente diferentes. Como libertário, eu sou
não se defende
- isso, mas eu entendo a idéia de que em tempos de guerra
falando em código
+ é suspeito. Não estamos em tempo de guerra, e ainda não
foi.)
-
- Devemos ter "voz permite"? Afinal, não é o
regulamento de
+ discurso coerente com o regulamento de automóveis?
-
- Eu fiz um ensaio satírico ao longo destas linhas um tempo atrás.
Eu não
- incluída aqui, no entanto. (Meu discurso de autorização para a sátira
expirado e eu
+ ainda não tive tempo para obtê-lo renovado.)
-

- No encerramento, o todo comparação de criptografia para armamento é
- enganosa. Falar ou escrever em formas não prontamente compreensível para
- seus inimigos, seus vizinhos, seu cônjuge, os policiais, ou local
- intruso é tão antiga como a humanidade.

3.4.18. Enfatizar o "voluntário" natureza de criptografia

+ quem não quer privacidade, poderá optar por não usar criptografia
- assim como eles podem levar a bloqueios de suas portas, instalar escutas em seus telefones, remover, as suas cortinas para não interferir com a espreitar toms e vigilância da polícia equipes, etc.
- como PRZ coloca-lo, pode gravar todas as suas letras em cartões-postais, porque eles têm "nada a esconder"
- o que nós queremos certificar-se de não acontecer é _others_ insistindo que não podemos usar criptografia para manter a nossa própria privacidade
+ "Mas, se os criminosos têm acesso a criptografia e pode manter segredos?"
- esse vem mais e mais novamente
- isso significa bloqueios não devem existir, ou.....?

3.4.19. "São mais Cypherpunks anarquistas?"

- São muitos, mas, provavelmente, não mais. O termo "anarquia" é muitas vezes incompreendido.
- Como Perry Metzger coloca "Agora, é happpens que eu sou um anarquista, mas não é isso que a maioria das pessoas associadas com o termo cypherpunk" acreditamos, e que não é justo pintá-los de que maneira -- o inferno, muitas pessoas nesta discussão lista de são abertamente hostis ao anarquismo." [P. M., 1994-07-01]
- comentários de Sherry Mayo, outros
- Mas o libertário streak é inegavelmente forte. E libertários que pensam sobre o fracasso da política e as implicações de cryptgraphy geralmente vêm para a anarco-capitalistas ou cripto-anarquista ponto de vista.
- Em qualquer caso, o "outro lado" não tem sido muito vocal em defendendo uma ideologia consistente que combina fortes de criptografia e coisas como bem-estar, direitos, e altas taxas de impostos.

(Eu não estou condenando-o. A maioria dos meus amigos de esquerda, vire fora a acreditar mais ou menos no mesmo coisas que eu acredito em...eles só anexar rótulos diferentes e negativos reações de palavras como "capitalista.")

3.4.20. "Por que há tanta discursando na lista?"

- Argumentos de ir sobre e sobre, pontos de ter feito dezenas de vezes,
flaming escala. Isto tem chegado a ser mais um problema
nos últimos meses. (Não contando com os picos quando Detweiler
foi em torno.)
+ Por várias razões:
+ os argumentos que muitas vezes são questões de opinião, e não em fatos, e
portanto, o povo continuar a repetir os seus argumentos
- agravada pelo fato de que muitas pessoas estão com preguiça de
fazer off-line de leitura, para saber sobre o que eles são
expressar uma opinião sobre
- desde que nada nunca é resolvido, decidido, votar,
etc., o debate continua
- uma vez que qualquer pessoa é livre para falar em qualquer tempo, algumas pessoas
vão continuar a fazer os mesmos pontos e mais uma vez,
com a esperança de ganhar através da repetição (eu acho)
+ uma vez que as pessoas geralmente não conheço pessoalmente o outro
os membros da lista, este promove a comentar (eu notei
que as pessoas que conhecemos, tais como a Área da Baía de
gente, não tendem a ser tão rude com os outros...qualquer
sociólogo ou psicólogo gostaria de saber por que isso é tão
imediatamente).
+ o pior ranters tendem a ser as pessoas que são mais
isolado dos outros membros da lista da comunidade;
esta é, geralmente, um bem-conhecido fenômeno da Net
- e é mais uma razão para a regional Cypherpunks
grupos que, ocasionalmente, se reunir, pelo menos, fazer algumas
social e de conversação conexões com pessoas em
sua região.
- por outro lado, a rudeza é muitas vezes justificada; pessoas
que assaltam-me, e caso contrário, o plano de privar-me do meu
propriedade da merecem a morte, não apenas insultos [não
estar preocupado, há apenas um punhado de pessoas no
lista eu seria feliz ao ver mortos, e em nenhum deles
eu iria gastar os $5000 pode tomar para comprar um contrato.
Naturalmente, as taxas podem cair.]
3.4.21. O "rejectionist" postura tantos Cypherpunks ter
- que compromisso raramente ajuda muito quando as questões básicas são
envolvidos
- a experiência com o NRA tentando compromisso, apenas para encontrar
cada vez mais repressivas leis aprovadas
- o descalabro com o FEP e a sua "FEP de Telefonia Digital
Projeto de lei" ("Nós não poderia ter colocado este projeto de lei, juntos, sem
sua ajuda") mostra a corrupção do poder; tenho vergonha de

já foi um membro da FEP, e é claro não
ser renovar a minha filiação.
- Eu, por brincadeira, sugeri que precisa de uma "Frente Popular para o
A liberação de Crypto," por analogia com o PFLP.
3.4.22. "É o Cypherpunks grupo ilegal ou sedicioso
organização?"
- Bem, há aqueles "Cypherpunk Penal" t-shirts muito
nós temos...
- Depende de qual país você está.
- Provavelmente em um par de dezenas de países, a adesão
ser desaprovou
- o material pode ser ilegal em outros países
- e muitos de nós, defendem coisas como o uso de criptografia forte para
evitar e fugir de tzxes, para ignorar as leis que não gostamos, etc.

3.5. Auto-organização de Natureza de Cypherpunks
3.5.1. Ao contrário do que algumas pessoas afirmam, não há nenhuma decisão
grupo de Cypherpunks. Qualquer pessoa é livre para fazer quase nada,
só não é livre para cometer outros para curso de ação, ou
controlar os recursos da máquina agora, a lista é executado, ou declaração
para falar com o "Cypherpunks" como um grupo (e esta última
o ponto é inaplicável, exceto por meio de reptutation e social
repercussões).
3.5.2. Outro motivo para ser feliz não há nenhuma definição formal de Cypherpunks
estrutura, corpo governante, etc., é que não existe directa
alvo de processos judiciais, ITAR vioalation acusações, difamação ou
reclamações de violação de direitos autorais, etc.

3.6. A mecânica da Lista
3.6.1. Arquivos da Lista Cyperpunks
- Karl Barrus tem uma seleção de posts no site
caos.bsu.edu disponível via
gopher. Olhar no "Cypherpunks gopher site de diretório".
3.6.2. "Por que não a lista de enviados de forma criptografada?"
- Muito trabalho, sem adicionais de segurança, só faria com que
as pessoas saltar através extra aros (o que pode ser útil, mas
provavelmente não vale a pena o aborrecimento extras e maus sentimentos).
- "Fizemos isso há cerca de 8 anos em E&S usando VMS DEC NOTAS.
Utilizou-se um plain vanilla secret algoritmo de chave e uma chave
compartilhada por todos os membros legítimos do grupo. Nós poderíamos fazer
é hoje-mas por que se preocupar? Se você tem uma chave que
generalizada, é efetivamente a certeza de que a "pessoa errada"
(no entanto, você define ele/ela) vai ter uma cópia da chave."

[Carl Ellison, Criptografados BBS?, 1993-08-02]
3.6.3. "Por que não é a lista moderado?"
- Isso geralmente aparece durante a grave flaming episódios,
nomeadamente, quando Detweiler está na lista, em um de seus vários
personnas. Recentemente, ele não veio para cima, como as coisas têm
foi relativamente tranquilo.
+ A moderação ** não acontecer
- ninguém tem o tempo que leva
- ninguém quer o ônus
+ pouco consistente com muitos de nossos anarquista inclinações, é
ele?
- (Tecnicamente, a moderação pode ser visto como "minha casa, minha
regras, e, portanto, OK, mas eu acho que você começa o meu ponto de vista.)
- "Não, por favor, não vamos nos tornar um 'moderado' grupo de notícias. Este
seria o fim da liberdade! Isso é semelhante para dar o
a polícia mais poderes, porque o crime é de até. Enquanto ele é um
a tática de lutar contra os invasores, a melhor tática é
conhecimento." [RWGreene@vnet.net, alt.a coleta.arco-íris, 1994-
07-06]"
3.6.4. "Por que não é a lista dividida em listas menores?"
- O que você chama de a lista de interrupções?
+ A sério, diversas propostas para dividir a lista em pedaços
resultaram em não muito
- um grupo de hardware...nunca mais foi visto, e eu sei que
- um "moderado criptografia de grupo", idem
- um DC-Net grupo idem...
- vários grupos regionais e o planejamento de reuniões de grupos,
aparentemente moribundo
- um "Cavar Lib" do grupo...idem
- usar Rishab do comentário:
+ Razões são claras: um grande grupo é mais bem-sucedido em
o tráfego de menores, de baixo volume de grupos...fora de vista,
fora da mente
- e tópicos de mudar de qualquer maneira, por isso a necessidade de um
"steganography" lista de discussão (defendido com veemência pelo
uma pessoa, não Romana M., por sinal) se desvanece quando
o debate turnos. E assim por diante.
3.6.5. Crítica Endereços, Números, etc.
+ Cypherpunks arquivos de sites
- refrigerante
- sites de espelho
- sites de ftp
- PGP locais

- Infobot na Wired
- majordomo@toad.com; "ajuda" como corpo da mensagem
3.6.6. "Como é que o Cypherpunk remetentes aparecem tão rapidamente?"
- remetentes foram a primeira grande vitória...um fim-de-semana do Perl
hacking

3.7. Publicidade
3.7.1. "Que tipo de cobertura que a imprensa tem o Cypherpunks chegado?"
- " Eu concordo com aqueles que sugerem que a solução para o
a ignorância se manifesta em muitos dos artigos relativos à
Net é a educação. A cobertura dos Cypherpunks de final
(pelo menos nas Vezes) me mostra que razoável precisão
é possível." [Chris Walsh, notícias.de administração.política, 1994-07-04]

3.8. Pontas Soltas
3.8.1. Sobre o alargamento do âmbito de Cypherpunks para outros countres
- uma espécie de criptografia de metro, para a difusão de ferramentas de criptografia, para
ajudar a semear a discórdia, para minar governos corruptos (para o meu
mente, todos os governos agora no planeta são intrinsecamente
corrompido e precisa ser prejudicada)
- links para o criminoso underworlds destes países é um
corajosa coisa a considerar....cheio de perigos, mas
em última análise, de desestabilização de governos

4. Objetivos e Ideologia -- a Privacidade, a Liberdade, Novas Abordagens

4.1. direitos autorais

4.2. RESUMO: Objetivos e Ideologia -- a Privacidade, a Liberdade, Novas Abordagens
4.2.1. Pontos Principais
4.2.2. Ligações para Outras Secções
- Crypto Anarquia é a consequência lógica do forte de criptografia.
4.2.3. Onde Encontrar Informações Adicionais
- Vernor Vinge de "Nomes Verdadeiros"
- David Friedman, do "Máquinas de Liberdade"
4.2.4. Diversos Comentários
- A maioria dos membros da lista são libertários, ou apoiando-se em
que sentido, então, o viés em direção a isso é evidente.

- (Se há uma coerente _non_ libertário-ideologia, que é
também consistente com o apoio forte de criptografia, eu não tenho certeza
ele foi apresentado.)

4.3. Por que uma Declaração de Ideologia?
4.3.1. Este é, talvez, um controverso área. Então, por que incluir? O
razão principal é fornecer algumas bases para o posterior
comentários sobre muitas questões.
4.3.2. As pessoas não devem esperar um uniforme ideologia na lista.
Alguns de nós são anarco-capitalista radicais (ou "crypto
anarquistas"), outros de nós são estabelecidos os Republicanos, e ainda
outros são Balanços e outros assored esquerdistas.

4.4. "Bem-vindo ao Cypherpunks"
4.4.1. Esta é a mensagem de cada novo assinante para o Cypherpunks
listas de receber, por Eric Hughes:
4.4.2. "Cypherpunks assumir a privacidade é uma coisa boa e o desejo
foram mais de ti. Cypherpunks reconhece que aqueles que querem
privacidade deve criá-lo por si mesmos e não esperar
governos, empresas, ou outros, sem rosto
as organizações, para conceder-lhes a privacidade de beneficência.
Cypherpunks sei que as pessoas têm vindo a criar as suas próprias
privacidade, por séculos, com sussurros, envelopes, de portas fechadas,
e correios. Cypherpunks não procuramos impedir que outros
as pessoas de falar sobre suas experiências ou o seu
opiniões.

"O meio mais importante para a defesa da privacidade
criptografia. Para criptografar é indicar o desejo de privacidade.
Mas para criptografar com criptografia fraca é para indicar que não muito
muito desejo por privacidade. Cypherpunks esperança de que todas as pessoas
desejando privacidade irá aprender a melhor para defendê-lo.

"Cypherpunks, portanto, são dedicados à criptografia.
Cypherpunks desejam aprender sobre ele, para ensinar, para implementar
ele, e para fazer mais do mesmo. Cypherpunks saber que
protocolos criptográficos fazer estruturas sociais. Cypherpunks
sabe como atacar o sistema e como defendê-la.
Cypherpunks sabe o quão difícil é fazer um bom
criptosistemas.

"Cypherpunks amor para a prática. Eles gostam de jogar com público
criptografia de chave. Eles gostam de jogar com anônimos e

sob pseudônimo, o reencaminhamento de correio e de entrega. Eles gostam de jogar com o DC-redes. Eles gostam de jogar com comunicações seguras de todos os tipos.

"Cypherpunks escrever código. Eles sabem que alguém tem de escrever código para defender a privacidade, e, desde a sua privacidade, eles são indo para escrever. Cypherpunks publicar seu código para que seus companheiros de cypherpunks pode praticar e brincar com ele. Cypherpunks perceber que a segurança não é construída em um dia e é paciente com o progresso incremental.

"Cypherpunks não me importo se você não gosta o software que eles escrever. Cypherpunks saber que o software não pode ser destruído. Cypherpunks saber que um dispersa do sistema não pode ser fechada para baixo.

"Cypherpunks vai fazer a redes de segurança para a privacidade." [Eric Hughes, 1993-07-21 versão]

4.5. "Cypherpunks Escrever Código"

4.5.1. "Cypherpunks escrever código" é quase o nosso mantra.

4.5.2. Este tem vindo a ser uma definição de instrução. Eric Hughes usado significa que Cypherpunks lugar mais importância, na verdade, mudar as coisas, na verdade, a obtenção de código de trabalho para fora, do que em apenas falando sobre como as coisas "deveriam" ser.

- Eric Hughes instrução necessária aqui:

- Karl Kleinpaste, autor de um dos primeiros anônimo lançamento de serviços (Carvão) disse isso sobre alguma proposta feito: "Se você tem sérios planos para como implementar uma coisa, por favor, implementá-lo, no mínimo, superior com esqueleto e implantá-lo. Prova, por exemplo, assistindo a um sistema em ação, é muito melhor do que pontification sobre isso." [Karl_Kleinpaste@cs.cmu.edu, notícias.de administração.política, 1994-06-30]

4.5.3. "A admoestação, "Cypherpunks escrever código," deve ser tomada metaforicamente. Eu acho que "escrever código" significa participar unilateral ação efetiva como um indivíduo. Que pode significar a escrita de código real, mas também pode significar dumpster diving em Mycrotronx e anônima, liberando os recuperados informações. Também pode significar a criação de uma ventos digital o banco. Não fique muito literal em nós aqui. O que é importante é que Cypherpunks assumir a responsabilidade pessoal por capacitar-se contra as ameaças à privacidade." [Sandy Sandfort, 1994-07-08]

4.5.4. Um Cypherpunks outlook: tomar as abstrações do acadêmico
conferências e torná-los concretos

- Uma coisa Eric Hughes e eu discutimos no comprimento (para 3 dias
quase sem parar de falar, em Maio de 1992) foi o glacial da taxa de
de progresso na conversão de criptografia primitivo
operações de acadêmicos de criptografia conferências em reais,
funcional código. O básico algoritmo RSA foi por mal
disponíveis, mais de 15 anos depois da invenção. (Isso foi
antes de PGP 2.0, e PGP 1.0 foi mal disponível e foi
decepcionante, com a RSA Data Security, vários produtos no
limitado nichos.) Todas as coisas legais no dinheiro digital, DC-
Redes, pouco compromisso, olivioius transferência digital de mistura,
e assim por diante, estava completamente ausente, em termos de avialable
código ou "crypto ICs" (emprestado Brad Cox frase). Se
levou de 10 a 15 anos para o RSA para realmente aparecer na real
mundo, quanto tempo levaria algumas das emocionantes coisas para
sai?
- Nós pensamos que seria uma boa idéia para encontrar maneiras de reificar
estas coisas, para obter a real execução de código. Como aconteceu,
PGP 2.0 apareceu a semana do nosso primeiro encontro, e
tanto o Kleinpaste/Julf e Cypherpunks remetentes foram
rápido, em caso negativo, as implementações de David Chaum, de 1981,
"digital misturas." (No horário certo, 11 anos mais tarde.)
- Infelizmente, a maioria das abstrações da criptologia permanecem
moradores do espaço acadêmico, sem (disponível)
implementações no mundo real. (Para ter certeza, eu suspeito
muitas pessoas têm paralelepípedos, juntamente versões de muitos desses
as coisas, no código C, o que for. Mas o seu trabalho é mais como
construindo castelos de areia, para ser perdidos quando eles de graduação ou
passar para outros projetos. Isso não é um problema
exclusivo para criptologia.)
- Hoje, vários kits de ferramentas e bibliotecas estão sob
desenvolvimento. Henry Strickland (Strick) está trabalhando em um
kit de ferramentas com base em John Ousterhout do "TCL" do sistema (Unix),
e, claro, RSADSI fornece RSAREF. Pr0duct Cypher tem
"PGP Ferramentas." Outros projetos estão em andamento. (O meu longo prazo
o interesse aqui está na construção de objetos que atuam como
criptografia de papéis poderia tê-los agir...bloco de construção
os objetos. Para isso, eu estou olhando para Smalltalk de alguns
sabor.)
- É o caso, ainda que a maioria dos modernos de criptografia de documentos
discutir abstrações teóricas que são _not mesmo close_
para ser implementado como reutilizáveis, robusto objetos ou

rotinas. Fechando a lacuna entre a trabalhos teóricos e
realização prática é uma das principais Cypherpunk ênfase.
4.5.5. Protótipos, mesmo se fatalmente falho, permitir evolutiva
de aprendizagem e aperfeiçoamento. Pense nisso como engenharia
a ação.

4.6. Capacitação tecnológica
4.6.1. (mais necessária aqui....)
4.6.2. Como Sandy Sandfort notas, "O verdadeiro ponto de Cypherpunks é
que é melhor para uso de criptografia forte do que o fraco de criptografia ou não
criptografia em todos os. Nosso uso de criptografia não tem que ser totalmente
à prova de bala, para ser de valor. Deixe que *eles* preocupar-se sobre o
os aspectos técnicos, enquanto nós, certifique-se de que eles têm que trabalhar mais
e a pagar mais para a nossa encriptado informações de que eles teriam se
foram em texto simples." [S. S. 1994-07-01]

4.7. A Liberdade De Expressão De Problemas
4.7.1. Fala
- "Discurso público, não é uma série de discursos, mas
ao invés do próprio
palavras faladas abertamente e sem vergonha....Eu desejo uma sociedade
onde todos podem falar livremente sobre o tema que eles vão.
Eu desejo que todas as pessoas podem ser capazes de escolher a quem
eles querem falar e para quem não deseja falar.
Eu desejo uma sociedade onde todas as pessoas podem ter uma garantia de
que suas palavras são direcionadas apenas para aqueles a quem eles
deseja. Portanto, eu me oponho a todos os esforços dos governos para
escutar e para se tornar indesejados ouvintes." [Eric Hughes,
1994-02-22]
- "O governo não tem o direito de restringir o uso de
criptografia de qualquer forma. Eles não podem me proibir de usar
tudo cifras que eu goste, nem podem eles exigem que eu use
qualquer que eu não gosto." [Eric Hughes, 1993-06-01]
4.7.2. "Deve haver _any_ limites de uma pessoa utilize de
criptografia?"
- Não. Usando a matemática de criptografia é meramente a
manipulação de símbolos. Nenhum crime é envolvido, ipso facto.
- Também, como Eric Hughes apontou, esta é mais uma das
nas questões onde o normativo "deve" ou "não deve"
invoca "o policial dentro." A melhor maneira de olhar é
para ver quais os passos que as pessoas podem tomar para fazer qualquer pergunta de
"deve" ser isso permitido apenas discutível.
- Os "crimes" são atos físicos, como homicídio e

seqüestro. O fato de que a criptografia pode ser utilizada por plotters
e planejadores, tornando a detecção mais difícil, é em
nenhuma forma diferente da possibilidade de que as plotters de maio
falar em uma língua estranha para o outro (cifras), ou
se encontram em uma casa privada (segurança), ou falar em uma voz suave
quando em público (steganography). Nenhuma dessas coisas deve
ser ilegal, e *nenhum deles seria exequível* exceto
no mais rígida da polícia estados (e, provavelmente, nem mesmo
de lá).
- "Crypto é thoughtcrime" é o efeito de restringir
criptografia de usar.
4.7.3. Democracia e censura
- Faz de uma comunidade têm o direito de decidir que grupos de notícias
ou revistas em sua comunidade? Faz uma nação tem
o direito de fazer o mesmo? (Tennessee, Do Iraque, Do Irã, França.
Utah?)
- Isso é o que ignora com criptografia são todos sobre: tomar
estes majoritária moralidade decisões das mãos de
o bluenoses. Ação direta para proteger as liberdades.

4.8. Questões De Privacidade
4.8.1. "Há uma agenda aqui, além de garantir a privacidade?"
- Definitivamente! Eu acho que eu posso dizer com segurança que, para quase todos os
quadrantes políticos no Cypherpunks lista. Esquerda, direita,
libertário ou anarquista, há muito mais forte
criptografia simples de privacidade. Privacidade qua privacidade é bastante
desinteressante. Se tudo o que se quer é a privacidade, pode-se simplesmente
manter para si mesmo, ficar fora de alta visibilidade listas como
isso, e geralmente ficar fora de problemas.
- Muitos de nós, veja forte de criptografia como a chave de habilitação de tecnologia
para um novo sistema econômico e social, um sistema que
desenvolver-se como o ciberespaço torna-se mais importante. Um sistema de
qual distribui com as fronteiras nacionais, que é baseado no
voluntária (mesmo anônimo) de livre comércio. Em questão é o
fim dos governos como os conhecemos hoje. (Olhar
interações na Net--nesta lista, por exemplo--e
você vai ver muitos dos chamados nacionalidades, voluntária
a interação, e a quase completa ausência de qualquer "lei".
Além do fato de ser quase sem regras per se para a
Cypherpunks lista, existem, basicamente, as leis nacionais
que são invokable de qualquer forma. Este é um rápido crescimento
tendência.)
+ Motivações para Cypherpunks

- Privacidade. Se manter a privacidade é o objetivo principal, há
não há muito mais a dizer. Manter um perfil baixo, proteger dados,
evite dar informações pessoais, limitar o número de
de empréstimos bancários e aplicações de crédito, pagamento em dinheiro, muitas vezes, etc.
- Privacidade no ativismo.
+ Novas Estruturas. Usando criptografia construções para construir
nova política, econômica, e até mesmo as estruturas sociais.
- Políticos: direito de Voto, a pesquisa, o acesso a informações
denúncia de irregularidades
- Econômica: mercados Livres, informação de mercados, aumento da
de liquidez, mercado negro
- Social: Cyberspatial comunidades, Nomes Verdadeiros
Publicamente inspectable algoritmos de sempre vencer
privadas, algoritmos secretos
4.8.2. "O que é a atitude Americana à privacidade e a encriptação?"
+ Existem dois distintos (e, talvez, simultaneamente realizada)
opiniões que têm sido encontradas na psique Americana:
- "A casa de um homem é seu castelo". "A mente do seu próprio negócio."
A fronteira e Calvinista do espírito de se manter a
de negócio para si.
- "O que você tem a esconder?" O nosiness de intrometidos,
fofocando sobre o que os outros estão fazendo, e sendo
suspeitas de quem tentar demasiado duro para esconder o que eles
estão a fazer.
+ A atitude Americana, atualmente, parece favorecer a privacidade sobre
poderes de polícia, como evidenciado por um Tempo CNN enquete:
"Em um Time/CNN sondagem de 1.000 Americanos realizados última
semana pela Yankelovich Partners, dois terços disseram que era mais
importante proteger a privacidade de chamadas de telefone que
preservar a capacidade da polícia para realizar escutas. Quando
informado sobre o Clipper Chip, 80% disseram que oposição
ele." [Philip Elmer-Dewitt, "Quem Deve Manter as Teclas"
TIME, 1994-03-04.]
- A resposta é, claramente, uma função da forma como a questão
é formulada. Pergunte pessoas se elas favor "inquebrável
criptografia" ou "fortaleza " recursos" para os terroristas,
pedófilos, e outros malfeitores, e provavelmente eles vão dar
um bastante diferente de resposta. É esta orçada sendo tomadas
pelo Clipper pessoas. Atente para isso!
- Me, eu não tenho dúvidas.
- Como Perry Metzger diz, "eu encontrar as recentes divulgações

a respeito do Governo dos EUA de testes dos efeitos da
radiação no inconsciente seres humanos, a ser ainda mais
prova de que você simplesmente não pode confiar no seu governo, com
a sua segurança pessoal. Algumas pessoas, dadas as posições de
poder, será, naturalmente, o abuso dessas posições, muitas vezes até mesmo se
tais abusos podem causar lesões graves ou morte. Eu vejo pouco
a razão, portanto, para simplesmente "confiança" do governo dos EUA --
e dado que o governo dos EUA é tão bom como eles
obter, é óbvio que o governo NÃO merece o cego
a confiança de seus cidadãos. "Confie em nós, vamos protegê-lo"
anéis muito oco em face da evidência histórica.
Os cidadãos devem proteger e preservar a sua própria privacidade-a
o governo e seus centralizado esquemas de criptografia
enfaticamente não pode ser confiável." [P. M., 1994-01-01]
4.8.3. "Como é de 1994, como 1984?"
- O anúncio da televisão para Clipper: "Clipper, porque 1994 _will_ ser
como 1984"
+ Como Mike Ingle coloca:
- 1994: Escutas telefônicas é de privacidade
O segredo é a abertura
Disfarce de segurança
4.8.4. "Prevemos que as redes de computadores vai jogar mais e
o papel mais importante em muitos aspectos de nossas vidas. Mas esse
aumento da informatização traz enormes perigos para
infração de privacidade. Cypherpunks, procurar colocar no lugar
estruturas que vai permitir que as pessoas para preservar a sua privacidade
se eles escolherem. Ninguém será forçado a usar pseudônimos ou
postar anonimamente. Mas deve ser uma questão de escolha, como
toda a informação que uma pessoa escolhe para revelar sobre si mesmo
quando ele se comunica. Agora, as redes não dão a você
que muita escolha. Nós estamos tentando dar esse poder para
pessoas." [Hal Finney, 1993-02-23]
4.8.5. "Se cypherpunks contribuir nada mais podemos criar uma verdadeira
privacidade, grupo de advocacia, defendendo o meio de real auto-
a capacitação, a partir de criptografia para nom de guerre de cartões de crédito,
em vez de defender mais a invasão de nossa privacidade, tal como o
os chamados defensores da privacidade estão fazendo agora!" [Jim Hart, 1994-
09-08]

4.9. As Questões Da Educação
4.9.1. "Como podemos conseguir mais pessoas para uso de criptografia?"
- para informá-los sobre os temas de Cypherpunks
- vigilância, escutas telefônicas, Telefonia Digital, Clipper, NSA,

FinCEN, etc....essas coisas podem assustar um monte de gente
tomada de PGP mais fácil de usar, melhor integração com e-mails,
etc.
- (Para ser franco, convencer os outros para proteger-se é
não é uma das minhas maiores prioridades. Então por que tenho escrito
este megabyte-plus FAQ? Boa questão. Chegando mais usuários
de uma forma geral é ganhar, por razões óbvias.)
4.9.2. "Quem precisa criptografar?"
+ Empresas
- os concorrentes...as transmissões de fax
+ de governos estrangeiros
- Chobetsu, GCHQ, SDECE, a Mossad, KGB
+ o seu próprio governo
- NSA intercepta dos planos de investimentos
+ Grupos De Ativistas
- Ariana Nação precisa criptografar, como o FBI anunciou a sua
a intenção de se infiltrar e subverter este grupo
- RU-486 redes
- Anistia Internacional
+ Terroristas e Traficantes de Droga
- claramente são sem noção, às vezes (Pablo Escobar usando um
celular!)
- Tríades, Máfia russa, muitos estão se tornando crypto-alfabetizados
- (Eu fui appoached-'nuff said)
+ Médicos, advogados, psiquiatras, etc.
- para preservar os registros contra roubo, espionagem, casuais
exame, etc.
- em muitos casos, a obrigação legal de ter sido anexada à
este (nomeadamente, registos médicos)
- a curiosa situação de que muitas pessoas são essencialmente
required para criptografar (não há outra maneira de assegurar que as normas
são atendidas), e ainda várias leis existe para limitar
criptografia...ITAR, Clipper, EES
- (Clipper é uma resposta parcial, se insatisfatório)
4.9.3. "Quando deve criptografia será usada?"
- É uma matéria económica. Cada pessoa tem que decidir quando
usá-lo, e como. Mim, eu não gosto de ter de fazer o download de mensagens
para a minha casa de máquina antes que eu possa lê-los. Outros usam
rotineiramente.

4.10. Libertário Problemas
4.10.1. Uma abordagem tecnológica para a liberdade e privacidade:
- "A liberdade é, praticamente, dado o máximo (ou mais) pelo

ferramentas de nós pode construir para protegê-lo, pois é por nossa capacidade
para convencer os outros que violentamente se discordar de nós, não para
nos atacar. Na Internet temos ferramentas como anon
remetentes e PGP que nos dão uma grande liberdade
de coerção, mesmo no meio da censura. Assim, estes
ferramentas de irritar os fãs de informações centralizadas de controle, a
os defensores do status quo, como nada mais no
A Internet." [<an50@desert.hacktic.nl> (Ninguém), libtech-
l@netcom.com, 1994-06-08]
+ Duncan Frissell, como de costume, colocá-lo convincentemente:
- "Se eu reter o meu capital de algum país ou empresa
Eu não estou ameaçando matar ninguém. Quando um "Democrática
Estado" decide fazer algo, ele faz isso com armadas
os homens. Se você não obedecer, eles tendem a atirar....[I]f
a mudança tecnológica aumenta os poderes dos indivíduos,
seu poder é reforçada, não importa o que o governo
não.

"Se o coletivo é enfraquecido e o indivíduo
reforçada pelo fato de que eu tenho o poder de baratos
armas, de carros, de computadores, de telecomunicações, de criptografia e, em seguida, o
coletiva tem sido enfraquecido e devemos facilitar a
a transição para uma sociedade baseada no voluntariado, em vez de
coagido a interação.

"A menos que você pode descobrir uma nova e melhorada forma de
controlar os outros, você não tem escolha." [D. F., Declínio
e a Queda, 1994-06-19]
4.10.2. "Eles que pode dar-se essencial da liberdade para obter um pouco de
temporária de segurança não merece nem liberdade nem segurança."
[Benjamin Franklin]
4.10.3. uma vista típica de governo
- "Como eu o vejo, é sempre uma casa para os agressores masquerading
como uma defesa coletiva. Às vezes ele realmente é, na verdade,
para realizar a sua anunciado defesa de função. Como nu
quarks,
puramente defensiva, os governos não podem existir. Eles são
bipolar, por natureza, com alguns pólos (por exemplo, o bullying
parte), sendo "mais iguais do que outros." [Sandy Sandfort, 1994-
09-06]
4.10.4. Infelizmente, vários dos nossos especulativa cenários para diversas leis
têm vindo a passar. Mesmo algumas das minhas próprias, tais como:
- "(Ainda Outro Pode Previsão Percebi)...O texto de um

"digital perseguição bill" foi enviado apenas para Cyberia-l." [L.
Todd Masco, 1994-08-31] (Isso foi uma brincadeira de predição eu
fez que "digital perseguição" em breve seria um crime; não
tinha sido de artigos de notícias sobre os horrores de tais
cyberspatial stalkings, independentemente de não haver nenhum real
ameaças físicas, de modo que este movimento não é tão surpreendente.
Não é surpreendente, em uma época em que a liberdade de expressão fica banido como
"assalto a fala.")

4.10.5. "Não pisar em mim."

4.10.6. No entanto, é fácil ficar muito negativas sobre a situação, para
suponha que um estado socialista está ao virar da esquina. Ou
que um novo Hitler vai chegar ao poder. Estes são susceptíveis de
a evolução, e não só por causa do forte de criptografia.
Os mercados financeiros estão a colocar restrições sobre como um fascista
o governo pode obter...o internacional de mercados de títulos, para
exemplo, irá reagir rapidamente a sinais como este. (Esta é a
teoria, pelo menos.)

4.10.7. Localidade de referência, dinheiro, TANSTAAFL, de privacidade
- encerramento, local de computação, benefícios locais
- nenhum sistema de contabilidade necessária
- claro mercados
- distorções de mercado, como o racionamento, cupons, cotas, todos os
exigem registo centralizado de manutenção
- qualquer coisa que os laços de transações econômicas de identidade
(racionamento, direitos, seguros) implica identidade-
de acompanhamento, credenciais, etc.
+ Não-localidade também aumenta drasticamente as oportunidades
para fraudes, golpes e con empregos
- porque algo está sendo prometido para entrega futura
(a essência de muitos golpes) e não é verificável localmente
- porque a "confiança" é invocada
- Localidade também corrige o "policial dentro" problema: o
custos de decisões são de responsabilidade do administrador, e não por outros.

4.11. Crypto Anarquia

4.11.1. A Criptografia Anarquia Princípio: Forte de criptografia permite
inquebrável encrypion, unforgeable assinaturas, untraceable
mensagens eletrônicas, e unlinkable pseudonomous identidades.
Isso garante que algumas transações e comunicações podem ser
inserido apenas voluntariamente. Força externa, a lei, e
o regulamento não pode ser aplicada. Esta é a "anarquia", no sentido de
não fora governantes e leis. Acordos voluntários, volta-
parou voluntariamente-organizado, em instituições como garantia

serviços, será a única forma de regra. Esta é a "crypto
a anarquia."
4.11.2. criptografia permite que um retorno aos contratos que os governos não
violação
- com base na reputação, a repetição de negócios
- exemplo: ordenação de material ilegal e untraceably
anonimamente,,,os governos são incapazes de fazer qualquer coisa
- espaços privados, com a privacidade imposta através de criptografia
permissões (credenciais de acesso)
- escrows (obrigações).
4.11.3. Soluções tecnológicas mais legalista regulamentos
+ Marc Ringuette resumiu tudo muito bem:
- "O que pretendemos é que alguns "padrões da comunidade" para
o ciberespaço, e o que eu estou sugerindo é o bastante
libertário padrão que vai como esta:

"Prefiro soluções tecnológicas e de auto-protecção
soluções
durante a sua elaboração, onde elas são viáveis.

"Este é baseada na noção de que as regras mais lá
são, mais as pessoas vão chamar para a "net polícia" para
impor-lhes. Se podemos incentivar os padrões da comunidade
que enfatizam um nível prudente de auto-proteção, em seguida,
nós vamos ser capazes de fazer mais com menos regras e menos
intrusivo nível de policiamento."[Marc Ringuette, 1993-03-14]
+ Hal Finney tornou convincentes argumentos de por que nós devemos
não nos acomodamos sobre o papel da tecnologia vis-
a-vis a política. Ele nos adverte para não crescer confiantes:
- "Fundamentalmente, acredito que vai ter o tipo de
a sociedade do que a maioria das pessoas deseja. Se queremos que a liberdade e a
privacidade, temos de convencer os outros de que estes valem a pena
de ter. Não há atalhos. Retirar-se em
a tecnologia é como puxar os cobertores por cima da sua cabeça.
É bom por um tempo, até que a realidade alcança. O
próximo Clipper ou Digital Telefonia proposta proporcionará um
despertar rude." [Hal Finney, POLI: Política vs
Tecnologia, 1994-01-02]
- "A idéia aqui é a de que a melhor solução para a baixa
sinal-para-ruído nas redes não é uma questão de
forçando as pessoas a "de estar por trás de suas palavras". As pessoas podem
ficar atrás de todos os tipos de idéias idiotas. Ao invés,
será necessário desenvolver melhores sistemas de filtragem de notícias

e-mail, para o desenvolvimento digital "reputação", que pode ser
estampada em uma de suas postagens para passar por estes inteligente
filtros, e até mesmo aplicar essas reputações de pseudônimos.
Em tal sistema, o fato de que alguém está postagem ou
discussão sob pseudônimo não é um problema, pois o incômodo
posters não ser capaz de passar." [Hal Finney, 1993-
02-23]

4.11.4. Reputação

4.11.5. Eu tenho uma moral do outlook que muitos vão achar inaceitável ou
repugnante. Para ir direto ao ponto: eu apoio a matança de
quem quebra de contratos, que roubam em grave o suficiente maneiras,
e que, do contrário, confirmar o que eu penso como crimes.
+ Eu não quero isso de forma abstrata. Aqui está um exemplo:
- Alguém está carregando drogas. Ele sabe que ele está envolvido
em. Ele sabe que o roubo é punido com a morte. E ainda
ele rouba a mercadoria.
- Concessionários entender que eles não podem tolerar isso, que
um exemplo deve ser feito, de outra forma todos os seus empregados
roubar.
- Entender que eu não estou falando sobre o estado fazendo o
matar, nem eu iria fazer a matança. Eu só estou dizendo que essas
as coisas são o natural mecanismo de aplicação de tais
mercados. Realpolitik.
- (Um meta ponto: a lei de drogas faz com que as coisas desta forma.
Legalizar todas as drogas e as empresas, seria mais como
"ordinária" de empresas.)
- Na minha altamente opinião pessoal, muitas pessoas, incluindo a maioria
Congressrodents, de ter cometido crimes que ganhar-lhes a
pena de morte; eu não vou ser triste de ver anônimo
assassinato mercados usado para lidar com eles.

4.11.6. O aumento de espionagem vai ajudar a destruir o estado-nação empires
como os EUA, que ficou muito inchado e muito
depende jogando seu peso em torno; nuclear "terrorismo"
pode derrubar algumas cidades, mas isso pode ser um preço pequeno a
paga para prejudicar totalmente o socialista de bem-estar que
lançaram tantas guerras deste século.

4.12. Pontas Soltas

4.12.1. "Por ter um "sem compromisso" postura?"
- Compromisso, muitas vezes, acaba na morte de milhares de cortes.
Melhor tomar apenas um rejectionist postura.
- A Associação Nacional do Rifle (NRA), aprendeu essa lição
o maneira mais difícil. FEP, eventualmente, pode aprendê-lo; agora eles

ser o "cooptados pelo poder central" modo de
deleitando em seu interior-o-anel viário de acesso ao Veep,
o seu voos no Força Aérea Um, e, em geral,
schmoozing com os motores e os shakers...ficar junto por
indo junto.
- Não vamos comprometer a questões básicas. Tratar a censura como um
problema a ser encaminhado ao redor (como John Gilmore sugere), não
como algo que precisa ser comprometida em. (Este é
dirigido a rumores sobre como a Net precisa de "polícia
em si," por "razoável" censura de postagens ofensivas,
pela "moderação" de grupos de notícias, etc. O que deve ser uma preocupação de
a gente é a hospedagem do seu ponto de vista bem intencionadas civil
grupos de liberdades, que, aparentemente, estão dispostos a jogar uma
papel nesta "auto-policiamento" do sistema. Não, obrigado.)
(E, já que muitas vezes as pessoas interpretam mal esse ponto, eu não sou
dizendo que as empresas privadas não definir quaisquer políticas que
desejo, de que grupos de notícias moderados não pode ser formado, etc.
Arranjos particulares são o que são. O problema é quando
a censura é imposta àqueles que não têm outro
obrigações. Governo geralmente faz isso, muitas vezes ajudado e
instigado por corporações e grupos de lobby. Isto é o que
é preciso lutar. Lutar pelo encaminhamento ao redor, através de tecnologia.)

4.12.2. Inerente males da democracia

- Para ser franco sobre isso, passei a desprezar o moderno
versão de democracia que temos. Cada problema é enquadrado em
termos de sentimento popular, em termos de como o público
iria votar. O governo da multidão no seu pior.
- As pessoas devem ser autorizados a usar calças de ganga azuis? Colocá-lo para um
votação. Os empregadores podem ter uma política de blue jeans? Passar um
lei. Deve cuidados de saúde serão fornecidas a todos? Colocá-lo para um
votação. E assim por diante, a destruir liberdades fundamentais e direitos.
Um absurdo. A tirania da maioria.
- De Toqueville avisado quando ele disse que o Americano
experiência em democracia iria durar apenas até os cidadãos
descobriu que poderia escolher os bolsos de seus vizinhos
na cédula de votação.
- Mas talvez nós possamos parar com essa bobagem. Eu apoio forte
criptografia (e sua eventual forma de criptografia anarquia), pois ele
destrói esta forma de democracia. Leva algum (e
talvez muitos) operações fora do reino de popularidade
concursos, além do alcance da vontade do rebanho. (Não, eu sou
não discutindo haverá uma completa mudança de fase. Como o
diz o ditado, "Você não pode comer o ciberespaço." Mas um monte de

consultoria, trabalho técnico, programação, etc., pode, na verdade,
ser feito com criptografia anárquico métodos, com o dinheiro que ganhou
transferido em uma variedade de maneiras para o "mundo real".
Mais sobre isso em outro lugar).
+ De criptografia anarquia efetivamente permite que as pessoas a escolher
quais são as leis que eles suportam, pelo menos em cyberspatial contextos.
Ele capacita as pessoas para quebrar o local de suas obrigações
majoritária sistemas normativos e decidir por si próprios
que leis são morais e que são besteira.
- Acontece que eu tenho fé de que a maioria das pessoas vai resolver em um
número relativamente pequeno de leis que eles (a maioria)
de apoio, uma espécie de Schelling ponto no espaço jurídico.

4.12.3. "É o Cypherpunks agenda _too extreme_?"

- Tenha em mente que a maioria dos "Cypherpunks agenda" para o
medida que pode identificá-lo, é susceptível de provocar ordinária
cidadãos em _outrage_. Falar de email anônimo, digital
dinheiro, lavagem de dinheiro, informação de mercados, os dados de paraísos,
minando a autoridade, o transnacionalismo, e todo o resto
(inserir seu favorito idéia) não é exatamente o "mainstream".

4.12.4. "Crypto Anarquia sons muito selvagem para mim."

- Eu aceito que muitas pessoas vão achar as implicações de
crypto anarquia (que segue no turno da existência de
a criptografia forte, através de Criptografia Anarquia Princípio) para
ser mais do que eles podem aceitar.
- Isso é OK (não que você precise do meu OK!). A casa de
Cypherpunks tem muitos quartos.

5. Criptologia

5.1. direitos autorais

5.2. RESUMO: Criptologia

5.2.1. Pontos Principais

- lacunas ainda existem aqui...eu tratei isso como bastante baixos
prioridade, dada a riqueza do material de criptografia

5.2.2. Ligações para Outras Secções

- detalhada de criptografia de conhecimento não é necessário para compreender muitos
as implicações, mas que ajuda a saber o básico (que

cabeças de muitos dos mais errónea interpretações)
- em particular, todos devem aprender o suficiente para, pelo menos,
vagamente compreender como a "cegueira" de obras
5.2.3. Onde Encontrar Informações Adicionais
+ uma dezena de livros importantes
- Schneier, "applied Cryptography"--é praticamente
"leitura obrigatória"
- Denning
- Brassard
- Simmons
- País De Gales, Dominic
- Salomaa
- "CRYPTO" Processo
- Outros livros que eu possa tomar ou deixar
- muitos sites de ftp, detalhadas em vários lugares neste doc
- sci.cripta, alt.privacidade.pgp, etc.
- sci.cripta.a pesquisa é um grupo novo, e é moderada, então ele
deve-se ter alguns de alta qualidade, com posts técnicos
- Perguntas mais frequentes sobre sci.cripta, da RSA, etc.
- Dave Banisar do EPIC (Electronic Privacy Information
Centro) relata: "...temos centenas de arquivos em
encriptação disponíveis através de ftp/wais/gopher/WWW a partir de cpsr.org
/cpsr/privacidade/crypto." [D. B., sci.cripta, 1994-06-30]
5.2.4. Diversos Comentários
- detalhes dos algoritmos de preencher vários livros...e fazer
- daí, não vai cobrir de criptografia em profundidade aqui (o foco principal
esse doc é o das implicações de criptografia, o
Cypherpunkian aspectos, as coisas não abrangidos em criptografia
livros-texto)
- cuidado com a perder-se em minúcias, em detalhes de
algoritmos específicos...tente manter em mente o
important aspectos de qualquer sistema de

5.3. O que esta Seção de FAQ Não Vai Cobrir
5.3.1. Por uma seção sobre a criptografia quando tantas outras fontes de existir?
- Uma boa pergunta. Eu vou estar mantendo esta secção breve, como
muitos livros podem dar ao luxo de fazer um trabalho muito melhor do que aqui
Eu posso.
- não apenas para aqueles que leram o número de livros teóricos com um
mão
5.3.2. NOTA: Esta seção pode permanecer desorganizado, pelo menos como
em comparação com algumas das seções posteriores. Muitas excelente
fontes sobre a criptografia de existir, incluindo prontamente disponível perguntas frequentes

(sci.cripta, RSADSI FAQ) e livros. Schneier livros é
especialmente recomendado e deve estar em _every_ Cypherpunk do
bookshelf.

5.4. Conceitos Básicos De Criptografia
5.4.1. "O que é criptologia?"
- vemos a criptografia de todos os que nos cercam...as chaves em nossos bolsos, o
assinaturas em nossa carteira de habilitação de motorista e outros cartões, o
foto Identificações, os cartões de crédito
+ de criptografia ou criptologia, a ciência do segredo
escrever...mas é muito mais...considere I. D. cartões, fechaduras
nas portas, combinações de cofres, os privados
informações...o segredo é tudo o que nos cerca
- alguns dizem que isso é ruim--a tensão entre "o que você tem
tem a esconder?" e "nenhum de seu negócio"
- alguns exóticos coisas: dinheiro digital, sistemas de votação, avançado
protocolos de software
- de importância para a proteção da privacidade em um mundo de
os localizadores (a la Bob e Cherie), cartões de crédito, tags
carros, etc....o dossiê sociedade
+ - comentários gerais sobre criptografia
- cadeia é tão forte quanto o seu elo mais fraco
- suponha opponnent sabe tudo, exceto a chave secreta
-
- Crypto é sobre economia
+ De códigos e Cifras
+ Códigos Simples
- Código Livros
+ Simples Cifras
+ Cifras de transposição (A=C, B=D, etc.)
- César Shift (blocos)
+ Palavra-Chave Cifras
+ Vigen�re (com César)
+ Rotor Máquinas
- Hagelin
- Enigma
- Início De Computadores (Turing, Um Colosso)
+ Moderno Cifras
+ Século 20
+ Chave Privada
+ One-Time pad (longas sequências de números aleatórios,
compartilhado por ambas as partes)
+ não quebráveis, mesmo em princípio, por exemplo, em um tempo

almofada com caracteres aleatórios selecionados por uma verdadeira
processo aleatório (die joga, decaimento radioativo,
certos tipos de ruídos, etc.)
- e ignorando o "quebráveis por break-ins"
abordagem de roubar o one-time pad, etc.
("Saco preto de criptografia")
- Computador De Mídia (Disquetes)
+ CD-ROMs e DATs
- "CD-ROM é um terrível médio para o OTP-chave
fluxo. Primeiro, você quer exatamente duas cópias do
o fluxo aleatório. CD-ROM tem um económica
vantagem somente para grandes corridas. Segundo, você quer
para destruir a parte do fluxo de já usado.
CD ROM não tem nenhuma apagar instalações, fora de
a destruição física de todo o disco."
[Bryan G. Olson, sci.cripta, 1994-08-31]
+ DES--Padrão de Criptografia de Dados
- Desenvolvido a partir da IBM Lúcifer, apoiado pela ANS
- um padrão desde a década de 1970
+ Mas é "Fraco"?
+ DES-impedimento de hardware e software estudado
+ De 1990, ainda rachado
- Mas NSA/NIST ordenou uma mudança
+ Problema Da Distribuição De Chaves
+ De comunicação com 100 outras pessoas significa
distribuição e proteção de 100 chaves
- e cada um desses 100 deve manter seu 100 chaves
seguro
- não há possibilidade de utilização generalizada
+ Chave Pública
+ De 1970: Diffie, Hellman, Merkle
+ Duas Chaves: a Chave Privada e a Chave Pública
+ Alguém pode criptografar uma mensagem para o Receptor com
Chave PÚBLICA do receptor, mas apenas o Receptor
A chave PRIVADA pode decifrar a mensagem
+ Diretórios de chaves públicas pode ser publicado
(resolve o problema da distribuição de chaves)
+ Abordagens
+ Funções Unidirecionais
- Mochila (Merkle, Hellman)
+ RSA (Rivest, Shamir, Adleman)
- baseia-se na dificuldade de factoring
números grandes (200 dígitos decimais)

- acredita ser "NP-hard"
+ patenteado e licenciado para "cuidadosamente
selecionado de clientes
- RSA, Fiat-Shamir, e outros
algoritmos não são livremente utilizável
- busca de alternativas continua
5.4.2. "Por que alguém precisa de criptografia?"
+ Por que a Necessidade
- comunicações electrónicas...telefones celulares, fax
máquinas comuns, chamadas de telefone são todos facilmente
interceptada...por governos estrangeiros, pela ANS, por
rival de traficantes de drogas, por casual amadores
+ transações que estão sendo rastreados....recibos de cartão de crédito,
cheques pessoais, I. D. cartões apresentado no momento da
comprar...permite o cruzamento, direto de dados de email
bases, mesmo o governo ataques a pessoas que compram emissões de gases de efeito
suprimentos!
- em um sentido, criptografia e dinheiro digital permite que um
voltar ao dinheiro
- Por que pessoas honestas precisa de encriptação? Porque não
todo mundo é honesto, e isto aplica-se a governos como
bem. Além disso, algumas coisas são um assunto.
- Por que alguém precisa de fechaduras nas portas? Por que não são todos os
diários disponíveis para leitura pública?
+ Whit Diffie, um dos inventores da chave pública
criptografia (e um Cypherpunk) aponta que os humanos
a interação tem sido largamente baseada em dois importantes
aspectos:
- de que você é quem você diz que é
- expectativa de privacidade em comunicações privadas
- Privacidade existe em várias formas, em várias culturas. Mas
até mesmo na polícia de estados, alguns conceitos de privacidade
importantes.
- A confiança não é o suficiente...pode-se ter adversários que vão
violar a confiança se parece justificado
+ A atual importância da criptografia é ainda mais impressionante
+ necessário para proteger a privacidade no ciberespaço, redes, etc.
- muitos mais caminhos, links, interligações
- leia Vinge de "Nomes Verdadeiros" para uma visão
+ dinheiro digital...em um mundo de agentes, knowbots, de alta
conectividade
- (não pode ser de fornecer seu número de VISTO para todos estes
coisas)

+ desenvolvimento de batalha entre:
- os defensores da privacidade...quem quer privacidade
- agências do governo...FBI, departamento de justiça, DEA, FINCEN, NSA
+ sendo combatido com:
- tentativas de restringir a criptografia (S. 266, nunca passou)
- Telefonia Digital Bill, $10K por dia de multa
- julgamento balões para exigir chave de registo
- acções futuras
+ pessoas honestas necessidade de criptografia, porque não são desonestos pessoas
- e pode haver outras necessidades de privacidade
- Phil Zimmerman ponto sobre o envio de todos os e-mails todas as letras, em cartões-postais--"o Que você tem a esconder?" de fato!
- a expectativa de privacidade em residências e no telefone conversas
+ Whit Diffie principais pontos:
+ provando que você diga que você é...firmas, autenticações
- como "selos" do passado
- a protecção da privacidade
- fechaduras e chaves sobre a propriedade e outros enfeites
+ os três elementos que são centrais para a nossa visão moderna de a liberdade e privacidade (a la Diffie)
- proteger as coisas contra roubo
- provando que podemos dizer que estamos
- expectativa de privacidade em nossas conversas e escritos
5.4.3. Qual é a história da criptologia?
5.4.4. As principais Classes de Criptografia
- (estas seções introduzir os termos em contexto, embora definições completas não serão dadas)
+ De criptografia
- privacidade de mensagens
- usando cifras e códigos para proteger o sigilo de mensagens
- DES é o mais comum de codificação simétrica (mesma chave para a encriptação e a desencriptação)
- RSA é o mais comum de cifra assimétrica (chaves diferentes para a encriptação e a desencriptação)
+ De assinaturas e Autenticação
- provar quem você é
- provando que você assinou um documento (e não alguém)
+ Autenticação
+ Selos
+ Assinaturas (escrito)

+ Assinaturas digitais (computador)
- Exemplo: códigos Numéricos em bilhetes de loteria
+ Utilizando a Chave Pública de Métodos (ver abaixo)
- Credenciais Digitais (Super Smartcards)
- Calcadeira-responder Sistemas
+ Credenciais
- Cartões de IDENTIFICAÇÃO, Passaportes, etc.
+ Segurança Biométrica
- As impressões digitais, Retina, Exames de DNA, etc.
+ Untraceable Mail
- untraceable envio e recebimento de email e mensagens
- foco: derrotar os bisbilhoteiros e análise de tráfego
- DC (protocolo de jantar criptógrafos)
+ De Criptografia De Voto
- foco: urna anonimato
- credenciais para a votação
- problemas de voto duplo, segurança, robustez, eficiência
+ Dinheiro Digital
- foco: a privacidade nas transações, purchases
- unlinkable credenciais
- cego, de notas
- "digital moedas" pode não ser possível
+ De Criptografia Anarquia
- usando o acima para fugir do gov., para ignorar fiscal coleção, etc.
- uma solução tecnológica para o problema do excesso de governo
+ Segurança
+ Bloqueios
- Fechaduras
+ Fechaduras De Combinação
- Cardkey Bloqueios
+ De violação de responder Sistemas (Selos)
+ Também conhecido como "à prova de adulteração" (enganosa)
- Alimentos e medicamentos Contentores
- Cofres, Cofres (Alarmes)
+ Armas, Permissiva, Links De Ação
- Armas Nucleares
- Controle De Armas
- Cartões inteligentes (Smartcards)
- Moeda, Cheques
+ As Somas criptográficas de Software
- Mas onde está armazenado? (Pode falsificar o sistema

a substituição de todo o pacote)
+ De Proteção Contra Cópia
- Senhas
- Chaves de Hardware ("dongles")
- Chamada em tempo de execução
+ Controle De Acesso
- Senhas, Códigos De Acesso
- Segurança Biométrica, Assinaturas Manuscritas
- Por: Contas De Computador, Caixas Eletrônicos, Cartões Inteligentes (Smartcards)
5.4.5. Hardware versus Software
- NSA diz apenas implementações de hardware pode realmente ser
considerado seguro, e ainda mais Cypherpunks e ordinária
crypto utilizadores favorecem o software abordagem
- Hardware é menos facilmente spoofable (substituição de módulos)
- O Software pode ser alterado mais rapidamente, para fazer uso da mais recente
recursos, mais rápido módulos, etc.
- Diferentes culturas, com os usuários comuns (milhões)
sabendo que eles são menos propensos a ter seus sistemas preto-
bolsa falsificada (meia-noite engenharia) que são relativamente
menos e é muito mais sensível militar sites.
5.4.6. "O que são" à prova de violação dos módulos e por que eles são
importante?"
- Esses são "à prova de bala "caixas" de outrora: casos de exposição,
abóbadas, museu casos
- que dê provas de ter sido aberto, adulterado,
etc.
+ versões modernas:
- casos de exposição
- cartões inteligentes
+ batata frita
- camadas de epóxi, materiais abrasivos, fusível de links,
etc.
- (objetivo é fazer engenharia reversa muito mais
caros)
- arma nuclear "permissiva links de ação" (PALs)
5.4.7. "O que são "uma maneira de funções"?"
- funções com não o inverso
- crypto necessidades de funções que são, aparentemente, de uma maneira, mas
que, na verdade, tem um inverso (embora seja muito difícil de encontrar,
por exemplo)
- uma forma de função, como "bolhas" (Vinge do "Abandonados em
Em tempo real")
5.4.8. Quando moderna criptologia começar?

+ "Quais são algumas das aplicações modernas da criptologia?"
+ "Zero Conhecimento de Sistemas Interativos de Provas" (ZKIPS)
- desde por volta de 1985
- "mínimos de provas"
+ provando que você sabe algo sem realmente
revelando que algo
+ exemplo prático: palavra-passe
+ pode provar que você tem a senha sem realmente
digitando no computador
- portanto, os bisbilhoteiros não pode saber sua senha
- como "20 perguntas", mas o mais sofisticado
- resumo exemplo: circuito Hamiltoniano de um grafo
+ Dinheiro Digital
+ David Chaum: "RSA números SÃO dinheiro"
- cheques, cheques bancários, etc.
- pode até saber se tentativa de dinheiro mesma verificação
duas vezes
+ até agora, nenhum equivalente direto do papel-moeda ou
moedas
- mas quando combinado com "reputação baseada em sistemas,"
pode ser
+ Credenciais
+ Provas de alguma propriedade que não revelam mais do que
só que a propriedade
- a idade, a licença para dirigir, o direito de voto, etc.
- "digital envelopes"
+ Fiat-Shamir
- passaportes
+ Votação Anônima
- protecção da privacidade com o voto eletrônico
- política, empresas, clubes, etc.
- revisão de pares de revistas eletrônicas
- consumidor, opiniões, enquetes
+ Digital Pseudônimos e Rastreáveis E-Mail
+ capacidade de adotar uma digital pseudônimo que é:
- unforgeable
- authenticatable
- untraceable
- Vinge de "Nomes Verdadeiros" e do Cartão "Ender o Jogo"
+ Placas de boletim, Samizdats, e a liberdade de expressão
+ banidos discurso, tecnologias
- por exemplo, a fórmula para o RU-486 pílula
- bootleg de software, material legalmente protegido

+ flutuante opiniões sem receios para o profissional
posição
- até pode, mais tarde, "provar", as opiniões eram o seu
+ "O Labirinto"
- armazenamento e encaminhamento de switching nós
+ cada um com tamper-responder módulos que desencriptar
mensagens recebidas
+ acumular algum número (latência)
+ retransmitir para o seguinte endereço
- e assim por diante....
+ depende de hardware e/ou a reputação
+ Chaum diz que não pode ser feito exclusivamente em software
- "Jantar Criptógrafos"
5.4.9. O que é criptografia de chave pública?
5.4.10. Por que é criptografia de chave pública é tão importante?
+ A principal vantagem de chaves públicas criptosistemas mais
convencional de chave simétrica (uma chave de criptografia
e a desencriptação) é um _connectivity_ para destinatários: um
pode se comunicar de forma segura com pessoas sem trocar a chave
o material.
- procurando a sua chave pública em um diretório
- pela criação de um canal usando o algoritmo Diffie-Hellman key exchange
(por exemplo)
5.4.11. "Não é a posse de uma chave significa a posse do *identidade*?"
- Se eu obter a sua chave, eu sou você?
- Certamente não é fora do contexto da criptografia
transação. Mas, dentro do contexto de uma transação, sim.
Garantias adicionais/speedbumps pode ser inserido (como
biométricos credenciais adicionais frases-chave, etc.), mas
estes são essencialmente parte da "chave", então o básico
a resposta é "sim". (Há periodicamente preocupações
levantadas sobre isso, citando os perigos de se ter todos os
identidade vinculada a uma única credencial, ou um número, ou chave.
Bem, existem maneiras de lidar com isso, como, por exemplo, a adoção de
protocolos de limite de uma exposição, que limita a quantidade
do dinheiro que pode ser retirado, etc. Ou as pessoas podem adotar
protocolos que requerem segurança adicionais, atrasos de tempo,
countersigning, etc.)
+ Isso pode ser testado em tribunal em breve, mas a resposta para
muitos contratos e operações de criptografia será que
a posse da chave = posse de identidade. Até mesmo um tribunal
o teste pode significar pouco, para os tipos de operações I
esperar para ver.

- Que é, em sistemas anónimos, "que te vai processar?"
- Então, guarda a sua chave.

5.4.12. O que são assinaturas digitais?

+ Usa de Assinaturas Digitais
- Contratos Eletrônicos
Direito de voto
- Verifica e de outros instrumentos financeiros (semelhante ao contratos)
- A data de Transações (aumentando os Notários)

5.4.13. De Identidade, Passaportes, Fiat-Shamir

- Murdoch, é-uma-pessoa, cartões de IDENTIFICAÇÃO nacional, vigilância sociedade
+ "Grande Mestre de xadrez Problema" e outras Fraudes e Falsificações
de central importância para as provas de identidade (uma la Fiat-Shamir)
- "terrorista" e "Máfia falsificar" problemas

5.4.14. Para onde devo olhar?

5.4.15. Crypto, Técnico

+ Cifras
- tradicional
- as one-time pads, Vernams cifras, informações, teoricamente, seguro
+ "Eu Tenho uma Nova Idéia para uma Cifra---devo Discutir Aqui?"
- Por favor, não. Cifras requerem uma análise cuidadosa, e
deve ser em papel (que é, apresentado em um
detalhada de papel, com as necessárias referências para mostrar
que diligência foi feito, equações, tabelas,
etc. A rede é um substituto pobre.
- Também, a quebra de um aleatoriamente apresentados cifra não é,
significa trivial, mesmo se o nível de codificação, eventualmente, é mostrada
para ser fraco. A maioria das pessoas não tem a inclinação para
tente quebrar uma cifra a menos que haja algum incentivo,
como a fama ou dinheiro envolvido.
- E as novas cifras são notoriamente difíceis de design. Especialistas
são as melhores pessoas para fazer isso. Com todas as coisas
esperando para ser feita (como descrito aqui), trabalhando em um novo
cifra é, provavelmente, o menos eficaz coisa de amador
pode fazer. (Se você não for um amador, e quebrado
outras pessoas cifras antes, então você sabe que você
são, e estes comentários não se aplicam. Mas eu vou adivinhar
de que menos de um punhado de pessoas nesta lista têm
o contexto necessário para fazer cifra de design.)

- Há um grande número de cifras e sistemas, quase
todos sem significado duradouro. Não testado, em situação irregular,
não utilizado--e, provavelmente, indigno de qualquer tipo de atenção.
Não adicione ao ruído.
- O que é DES e pode ser quebrado?
+ cifras
- RC4, cifra de fluxo
+ DolphinEncrypt
-
+ "Última hora Dolphin Criptografar ergueu sua inseguro cabeça
neste fórum,
- estas mesmas questões surgiram. A cifra que DE usa
não é pública e
- não foi concebido por uma pessoa conhecida
cryptographicc competência. Ele
- deve, portanto, ser considerado extremamente fraco.
<Eric Hughes, 4-16-94, Cypherpunks>
+ RSA
- O que é o RSA?
- Que detém ou controla a RSA patentes?
- Pode RSA ser quebrado?
- Quais são as alternativas ao RSA existe?
+ Funções Unidirecionais
- como diodos, as ruas de sentido único
- multiplicação de dois números grandes em conjunto é
é fácil....factoring o produto geralmente é muito difícil
- (este não é suficiente para uma utilizável de codificação, como o destinatário
deve ser capaz de executar a operação inversa..ele se transforma
fora que "alçapões" pode ser encontrado)
- Assinaturas Digitais
+ Dinheiro Digital
- O que é digital em dinheiro?
- Como se faz com o dinheiro digital diferem VISTO e similares
sistemas eletrônicos?
- Limpeza vs. Doublespending de Detecção de
- Conhecimento Zero
- Misturas e Remetentes
- Jantar Criptógrafos
+ Steganography
- tinta invisível
- micropontos
- imagens
- ficheiros de som

+ Geradores De Números Aleatórios
+ von Neumann citação sobre a vida em um estado de pecado
- também parafraseado (eu ouvi) para incluir _analog_
métodos, presumivelmente porque a não repetitivos (um formulário
semente inicial/iniciar) a natureza faz a repetição de experiências
impossível
+ Blum-Blum-Shub
+ Como Funciona
- "Blum-Blum-Shub PRNG é realmente muito simples.
Fonte flutuando na criptográfico de ftp
sites, mas é um conjunto de scripts para o Unix grande nī umero
calculadora "bc", além de alguns shell scripts, então é
não é muito portátil.

"Para criar um BBS RNG, escolha dois aleatória de números primos p e
q quais são congruentes 3 mod 4. Em seguida, o RNG é
com base na iteração x = x*x mod n. x é
inicializado como uma semente aleatória. (x deve ser um
quadrática do resíduo, o que significa que é o quadrado de
algumas número de mod n, mas que podem ser organizadas por
iterando o RNG uma vez antes de utilizar a sua saída.)"
[Hal Finney, 1994-05-14]
- Olhar para blum-blum-shub-forte-randgen.shar e afins
arquivos em pub/crypt/outros em ripem.msu.edu. (Este site
está repleta de coisas boas. Claro, só os Americanos
estão autorizados a utilizar estes geradores de números aleatórios, e
mesmo que eles enfrentam multas de us $500.000 e prisão
até 5 anos para inappopriate uso de números aleatórios.)
o código - fonte em ripem site ftp
- "Se você não precisa de alta largura de banda de aleatoriedade, há
vários bons PRNG, mas nenhum deles correm rápido. Ver o
capítulo PRNG em "Criptologia e Computacional
Teoria Dos Números"." [Eric Hughes, 1994-04-14]
+ "O que sobre hardware geradores de números aleatórios?"
+ Fichas estão disponíveis
-
+ "Hughes Aircraft também oferece um verdadeiro não-determinístico
chip (16 pinos DIP).
- Para mais informações contacte-me em kephart@sirena.hac.com"
<7 de abril de 94, sci.cripta>
+ "Deve RNG hardware ser um Cypherpunks projeto?"
- Provavelmente não, mas vá em frente. Meia dúzia de pessoas
ter obtido todos os despediu-se sobre isso, propôs um projeto-

-em seguida, deixá-lo cair.
- pode usar aplicações repetidas de uma criptografia tem
função para gerar muito bom PRNs (a RSAREF
a biblioteca tem ganchos para isso)
+ "Eu preciso de um bom gerador de números aleatórios--o que
eu devo usar?"
- "Enquanto Blum-Blum-Shub é, provavelmente, a forma legal para ir,
RSAREF usa repetidas iterações do MD5 para gerar seu
pseudo-aleatórios, que podem ser razoavelmente seguro e uso
código que você provavelmente já tem ganchos de perl
para.[BillStewart,1994-04-15]
+ Bibliotecas
- Esquema de código: ftp://ftp.cs.indiana.edu/pub/scheme-
repositório/scm/rand.scm
+ P e NP e jazz
- complexidade, factoring,
+ pode mecânica quântica ajudar?
- provavelmente não
+ De Autoridades De Certificação De
- hierarquia vs. web distribuído de confiança
- na hierarquia, as empresas podem definir-se
como CAs, como CommerceNet está falando sobre fazer
+ Ou, assustadoramente, os governos do mundo podem insistir que
eles "in the loop"
- várias maneiras para fazer isso: o sistema jurídico de invocação, o imposto de
leis de segurança nacional....Espero que o sistema jurídico
interfere na CAs e, portanto, ser a principal forma de CAs
em parceria com o governo
- Digo isso para dar às pessoas a oportunidade de plano de
alternativas, a final é executado
- Este é um dos motivos mais fortes para suportar o
dissociação de software de uso (que é, para rejeitar a
modelo específico RSADSI está usando agora)
5.4.16. Aleatoriedade
- Um assunto confuso para muitos, mas também um assunto glorioso
(maduro, com algoritmos, com profunda teoria, e prontamente
compreensível resultados).
+ Bill Stewart tinha um comentário engraçado no sci.cripta que também
mostra o quão difícil é para saber se algo é realmente aleatório
ou não: "eu posso tomar um simples gerador de X[i] = DES(X[i-1],
K), que irá produzir um bom aleatório ruído branco, mas você
não ser capaz de ver que é não-aleatória, a menos que você alugar
tempo NSA DES-cracker." [B. S. 1994-09-06]

- Na verdade, muitos aparentemente aleatória de seqüências de caracteres são, na verdade,
"cryptoregular": eles são regulares, ou não randômico, logo
como usa a chave certa. Obviamente, a maioria das cadeias de caracteres usadas
na criptografia são cryptoregular em que eles _appear_ para ser
de forma aleatória, e passar vários aleatoriedade medidas, mas são
não.
+ "Como pode a aleatoriedade de uma cadeia de bits de ser medido?"
- Ele pode aproximadamente ser estimada por medidas de entropia, como
compactável (por vários programas de compressão),
etc.
- É importante perceber que as medidas de aleatoriedade
são, em um sentido, "no olho de quem a vê"--há apenas
há prova de que uma seqüência é aleatória...há sempre espaço
para esperteza, se você vai
+ Chaitin-Kolmogoroff teoria da complexidade torna isso mais claro.
Para usar as palavras de outra pessoa:
- "Na verdade, isso não pode ser feito. A medida consistente de
entropia para o finito de objetos, como uma cadeia de caracteres ou um (finito)
série de números aleatórios é o chamado `programa de
comprimento da complexidade". Este é definido como o período de
o mais curto programa de algumas dado universal de Turing
máquina
que calcula a seqüência de caracteres. É consistente com a
sentido de que ele tem o familiar propriedades de
`ordinária" (Shannon) a entropia. Infelizmente, é
uncomputable: não existe um algoritmo que, dado um
arbitrária finito cadeia S, calcula-programa de comprimento
a complexidade de S.

Programa de comprimento complexidade é bem estudado no
literatura. Uma boa introdutório de papel é `Uma Teoria da
Tamanho do programa Formalmente Idêntica à Teoria da Informação"
por G. J. Chaitin, _Journal do ACM_, 22 (1975)
reimpresso em Chaitin livro _Information Aleatoriedade &
Incompleteness_, World Scientific Publishing Co.,
1990." [John E. Kreznar, 1993-12-02]
+ "Como posso gerar razoavelmente números aleatórios?"
- Eu digo "razoavelmente", porque do ponto: nenhum número
ou seqüência for "random". Sobre o melhor que pode
ser dito é que um número de seqüência de caracteres é o resultado de um
processo que chamamos de "random". Se feito através de algoritmos, e
de maneira determinística, chamamos este processo de "pseudo-aleatórios."
(E pseudo-geralmente é mais valioso do que "realmente

random" porque nós queremos ser capazes de gerar o mesmo
seqüência várias vezes, para repetir experiências, etc.)
5.4.17. Outros criptografia e hash programas
+ MDC, uma cifra de fluxo
- Pedro Gutman, com base no Algoritmo de Hash Seguro NIST
- utiliza chaves mais longas do que a IDÉIA, DES
- MD5
- Blowfish
- DolphinEncrypt
5.4.18. RSA força
- casual grau, 384 bits, 100 MIPS-anos (Paulo Leyland, 3-31-
94)
- RSA-129, 425 bits, 4000 MIPS-anos
- 512 bits...de 20.000 MIPS-anos
- 1024 bits...
5.4.19. DES triplo
- "Ele envolve três DES ciclos, em cifrar-descriptografar e criptografar
ordem. As chaves podem ser qualquer K1/K2/K3 ou K1/K2/K1.
O último é, por vezes, caled o "duplo-DES". Combinando
duas operações DES como este requer duas vezes mais trabalho para
quebrar como um DES, e muito mais espaço de armazenamento. Se você tem o
de armazenamento, ele apenas adiciona um bit para a efetiva tamanho da chave. "
[Colin Prumo, colin@nyx10.cs.du.edu, sci.cripta, 4-13-94]
5.4.20. Resistente a adulterações módulos (TRMs) (ou de violação de responder)
+ normalmente "tamper-indicando", a la selos
- muito difícil parar de adulteração, mas relativamente fácil de ver
se o selo foi violado (e, em seguida, não restaurado
fielmente)
- posse do "selo" é controlado...esse é o
histórico equivalente a "chave privada" no digital
sistema de assinatura, com o tecnológico, dificuldade de
forjamento a vedação a protecção
+ normalmente para crypto. chaves e criptografia. processamento de
- teste nuclear de monitoramento
- cartões inteligentes
- Caixas eletrônicos
+ um ou mais sensores para detectar intrusões
- vibração (carborundum partículas)
- alterações de pressão (la um museu de casos de exposição)
- elétrica
- destacou-vidro (Corning, Sandia)
+ tratado de proibição de testes de verificação requer esta
- fibra ótica linhas de vedação de um míssil...

- zero padrões...
- decalques....
+ Resinas epóxi
- a la Intel na década de 1970 (8086)
+ Lawrence Livermore: "Conhecedor De Projeto"
- gov agências usando isso para se proteger contra inversa
de engenharia, aquisição de chaves, etc.
+ não pode parar de um determinado esforço, embora
- grava, solventes, plasma a piscar, etc.
- mas pode causar custo ser muito alto (esp. se resina
a fórmula é variada, com freqüência, de modo que a "receita" não pode ser registado)
+ pode usar epóxi clara com "brilhos" em epóxi e
cuidado 2-posição fotografia usada para gravar padrão
- talvez com uma tampa transparente?
+ de fibra óptica de vedação (feixe de fibras, cortar)
- feixe de fibras é enrolado em torno do dispositivo e, em seguida, selado e
cortado de modo a que cerca de metade as fibras são cortadas; o padrão de aceso e
apagada fibras é uma assinatura, e é extremamente difícil
para reproduzir
- nanotecnologia pode ser usado (um dia)

5.4.21. "O que são cartões inteligentes?"
- Útil para a segurança do computador, transferências bancárias (como ATM
cartões), etc.
- pode ter inteligência local (este é o sentido usual)
- microprocessadores, observor protocolo (Chaum)
+ Smart cartões e transferência eletrônica de fundos
- Resistente a adulterações módulos
+ De segurança de fabricação
- alguma variante de "cortar-e-escolha" de inspeção de instalações
+ Utiliza de cartões inteligentes
- cartão de crédito convencionais usa
- pagamento de contas
postagem
- ponte e as portagens
- pagamentos para os itens recebidos eletronicamente (não
necessariamente anonimamente)

5.5. Criptologia-Técnico, Matemática

5.5.1. O Histórico De Criptografia
+ Máquinas Enigma

- rachado pelo inglês em Bletchley Park
- um segredo até meados da década de 1970
+ Reino UNIDO, vendeu centenas de apreendidos E. máquinas para embaixadas,
os governos, até mesmo empresas, no final dos anos 1940, início de
Anos 1950
- pode, em seguida, quebrar o que estava sendo dito pelos aliados
+ Hagelin, Boris (?)
- EUA pagou a ele para instalar alçapões, diz Kahn
+ a sua empresa, Criptografia A. G., era, provavelmente, uma NSA frente
empresa
- Suécia, EUA, em seguida, Suécia, em seguida, Zug
- rotor sistemas rachado
5.5.2. Sistemas de chave pública--HISTÓRIA
+ Inman admitiu que a ANS tinha um P-K conceito em 1966
- se encaixa com Dominik ponto sobre selado criptosistema de caixas de
com nenhuma forma de carregar novas chaves
- e consistentes com a ANS, tendo essencialmente acesso exclusivo a
nação superior matemáticos (até Diffies e Hellmans
foreswore financiamento do governo, como resultado do anti-
Pentágono sentimentos dos anos 70)
- Merkle do "quebra-cabeça" de ideias, por volta de meados da década de 70
- Diffie e Hellman
- Rivest, Shamir e Adleman
5.5.3. RSA e Alternativas para a RSA
+ RSA e outros P-K patentes estão a estrangular o desenvolvimento e
a disseminação dos sistemas de criptografia
- talvez de marketing estupidez, talvez com a ajuda
do governo (que tem um interesse em manter um
o monopólio de encriptação segura)
+ Funções unidirecionais e "o depósito somente envelopes"
- uma forma de funções
- depósito somente envelopes: permitir adições para envelopes e
somente o destinatário pode abrir
- funções de hash são fáceis de implementar funções unidirecionais
(sem a necessidade de um inverso)
5.5.4. Assinaturas Digitais
+ Usa de Assinaturas Digitais
- Contratos Eletrônicos
Direito de voto
- Verifica e de outros instrumentos financeiros (semelhante ao
contratos)
- A data de Transações (aumentando os Notários)
- Inegável assinaturas digitais

+ Unforgeable assinaturas, mesmo com ilimitado computacional
poder, pode ser alcançado se a população é limitado (uma
conjunto finito de agentes)
- o uso de um untraceable protocolo de envio, como "o
Jantar Criptógrafos Problema" de Chaum
5.5.5. A aleatoriedade e a incompressibilidade
+ melhor definição que temos é devido a Chaitin e Kolmogoroff:
uma seqüência de caracteres ou qualquer estrutura de "random" se ele não tem mais curto
descrição de si mesmo do que em si.
- (Agora, até mesmo a casos específicos de "gerado aleatoriamente
seqüências de caracteres" às vezes, vai ser compressível, mas não muito
muitas vezes. Cf. as obras de Chaitin e outros para saber mais sobre
esses tipos de pontos.)
5.5.6. Steganography: Métodos para Esconder a Mera Existência de
Dados Criptografados
+ em contraste com o freqüentemente citado ponto (feita por criptografia puristas)
que deve-se assumir que o adversário tenha acesso total ao
cryptotext, alguns fragmentos de descriptografados de texto sem formatação, e para
o algoritmo propriamente dito, isto é, assumir o pior
- uma condição que eu acho que é praticamente um absurdo e irreal
- assume infinito interceptar o poder (mesmo pressuposto de
infinita de energia do computador iria fazer todos os sistemas além de
as one-time pads quebrável)
- na realidade, ocultando a existência e a forma de um criptografados
mensagem importante
+ este será tanto mais como desafios legais para
criptografia são montados...a proposta de proibição encriptados
telecom (com us $10 MIL por dia de multa), vários governamentais
regulamentos, etc.
- RICO e outros pincel largo estratagemas pode fazer pessoas muito
cuidado, revelando que eles estão usando mesmo
criptografia (independentemente de como proteger as chaves são)
+ steganography, a ciência de esconder a existência de
informações criptografadas
- segredo tintas
- micropontos
- limitando a análise do tráfego
- LSB método
+ Embalagem de dados em fitas de áudio (LSB de DAT)
+ LSB de DAT: 2 gb áudio DAT vai permitir que mais de 100
megabytes nos LSBs
- menos, se os algoritmos são usados para moldar o espectro para
torná-la ainda mais como ruído

- mas também pode usar o maior bits, também (desde um real
mundo gravação terá de ruído de chegar até talvez
o 3º ou 4º bit)
+ vai fabricantes de investigar "composição" circuitos?
(la gordura zero?)
- mas a corrida ainda vai ser em
+ De vídeo Digital vai oferecer ainda mais espaço de armazenamento (maior
fitas)
- DVI, etc.
- HDTV final da década de 1990
+ Mensagens podem ser colocadas em GIFF, arquivos de imagem TIFF (ou mesmo
ruidosos, aparelhos de fax)
- usando o LSB método, com uma resolução de 1024 x 1024 imagem de escala de cinza
realização de 64 kb no LSB avião sozinho
- com a correção de erro, noise shaping, etc., ainda na
menos de 50KB
- cenário: já está sendo usado para transmitir a mensagem através de
internacional de fax e transmissões de imagem
+ O Velho "Dois Textos Normais" Manobra
- uma decodificação produz "Tendo um bom tempo. Queria que você estivesse
aqui."
- outros, de descodificação das mesmas matérias bits, produz "A última
submarino partiu esta manhã."
- de qualquer ordem jurídica, para produzir a chave gera o primeiro
mensagem
+ as autoridades nunca pode provar-salvar tortura ou de um
informante-que outra mensagem existe
- a menos que haja alguma forma de sinais de que o arquivo criptografado
a mensagem é, de alguma forma, "de forma ineficiente criptografados, o que sugere
o uso de um sistema dual de texto simples par de método" (ou algo do tipo
spookspeak)
- mais uma vez, certos puristas argumentam que tais problemas (que são
relacionados para o velho: "Como você sabe quando parar?"
questão) são enganosas, que se deve assumir a
adversário quase completa e acesso a tudo, exceto
a chave real, que qualquer esquema de combinar vários
sistemas não é melhor do que o que é obtido como resultado de uma
a combinação
- e apenas o total de largura de banda de dados...
+ Vários programas de existir:
- Stego
- etc. (descritos em outro lugar)
5.5.7. A Essencial Impossibilidade de Quebrar as Cifras Modernas e

Códigos
- esta é uma mudança importante do passado (e de vários
filme de suspense e romances que têm grandes computadores quebra de códigos)
- é concedido, "unbreakable" é um termo enganador
+ relembre o comentário de que a NSA não tenha quebrado qualquer
Soviética sistemas em muitos anos
- exceto para os casos, a la Walker caso, onde
plaintext versões são obtidos, por exemplo, onde humanos screwups
ocorreu
- a imagem em tantos romances de grandes computadores quebrar
códigos é um absurdo: as cifras modernas não será quebrada (mas o
primitivas de cifras usado por tantas nações do Terceiro Mundo e
suas embaixadas continuará a ser brincadeira de criança, mesmo para
high school projetos de feira de ciências...poderia ser uma boa idéia
para uma pequena cena, sobre um BCC aluno que tenha seu projeto
puxado)
+ Mas poderia novos métodos computacionais quebrar essas público
chave de cifras?
+ alguns especulativa candidatos
+ holográfico de computadores, onde um grande número são
contabilizam-ou, pelo menos, as possibilidades são somehown
estreitou-usando matrizes que (de alguma forma) representar o
números para ser fatorado
- talvez com rede de difração, canalização, etc.
- redes neurais e evolutiva de sistemas (genética
algoritmos)
- a ideia é que, de alguma forma, o enorme cálculos podem ser
convertido em algo que é inerentemente paralela
(como um cristal)
+ hyperspeculatively: encontrar a oracle para estes problemas
usando métodos não-convencionais de como controlo electrónico de VELOCIDADE e lúcido
sonhar
- alguns grupos acham que essa é a pena
5.5.8. Anônimo Transferências
- Chaum digital de mistura
- "Jantar Criptógrafos"
+ pode fazê-lo com trocadas disquetes, em um nível mais simples
- qual cada pessoa pode adicionar um novo material
+ Alice para Bob para Carol....Alice e Carol pode conspiram para
determinar o que Bob tinha acrescentado, mas um número suficiente de "mistura"
de pedaços e é possível que só se
todo mundo conspira pode uma das participantes ser pego
- talvez o cartão-baralhar resultados?

+ podem tornar-se comuns dentro de computação, sistemas de...
- por esta vaga idéia, quero dizer que várias novo OS protocolos
pode chamar vários novos mecanismos para a troca de
informações
5.5.9. Diversas Idéias Abstratas
- pode lógica de primeira ordem predicados ser comprovada em zero
conhecimento?
- Riemannn hipótese
+ P = NP?
- seria o universo mudar?
- Smale tem mostrado que, se as praças têm números reais em
eles, ao contrário números naturais (inteiros), então P =
NP; talvez isto não é surpreendente, uma verdadeira implica classificar
de uma descida recursiva, com cada quadrado tendo o ilimitado
alimentação do computador
+ oráculos
- especulativamente, um personagem pergunta se cartas de Tarot, etc.,
poderiam ser utilizados (além da normal idéia de que tais
dispositivos de ajuda psicológica)
- "uma cascata de mudanças provenientes de centenas de
casas decimais fora"
+ Criptografia quântica
- bits podem ser trocados-embora com bastante baixos
as eficiências através de um canal
- com a detecção de toques, através da mudança de duas polarizações
+ Stephen Wiesner escreveu uma 1970 papel, meia década antes
o P-K de trabalho, que delineou-não publicado até
muito mais tarde
- se especular que a NSA sabia sobre isso e anulou o
publicação
+ Mas poderia novos métodos computacionais quebrar essas público
chave de cifras?
+ alguns especulativa candidatos
+ holográfico de computadores, onde um grande número são
contabilizam-ou, pelo menos, as possibilidades são somehown
estreitou-usando matrizes que (de alguma forma) representar o
números para ser fatorado
- talvez com rede de difração, canalização, etc.
- redes neurais e evolutiva de sistemas (genética
algoritmos)
- a ideia é que, de alguma forma, o enorme cálculos podem ser
convertido em algo que é inerentemente paralela
(como um cristal)

+ hyperspeculatively: encontrar a oracle para estes problemas
usando métodos não-convencionais de como controlo electrónico de VELOCIDADE e lúcido sonhar
- alguns grupos acham que essa é a pena
- links para o nó teoria
- "cortar e escolher" protocolos (= conhecimento zero)
+ pode uma "moeda digital" ser feito?
- este é formalmente similar à idéia de um agente ativo
que é unforgeable, no sentido de que o agente ou uma moeda
é "autônomo"
+ bits podem sempre ser duplicado (a menos ligadas a hardware,
como com TRMs), então deve procurar em outro lugar
+ poderia amarrar os bits para um local específico, para que
a duplicação seria óbvio ou inútil
- a ideia é que vagamente que um agente pode ser colocado em
alguns localização...duplicações seria detectável
e irrelevantes (mesmo bits, o mesmo comportamento,
unmodifiable porque a assinatura digital)
+ teoria de codificação e criptografia no "Discretos Matemática"
- http://www.win.tue.nl/win/math/dw/index.html

5.5.10. Resistente a adulterações módulos (TRMs) (ou de violação de responder)

+ normalmente "tamper-indicando", a la selos
- muito difícil parar de adulteração, mas relativamente fácil de ver
se o selo foi violado (e, em seguida, não restaurado fielmente)
- posse do "selo" é controlado...esse é o
histórico equivalente a "chave privada" no digital
sistema de assinatura, com o tecnológico, dificuldade de
forjamento a vedação a protecção
+ normalmente para crypto. chaves e criptografia. processamento de
- teste nuclear de monitoramento
- cartões inteligentes
- Caixas eletrônicos
+ um ou mais sensores para detectar intrusões
- vibração (carborundum partículas)
- alterações de pressão (la um museu de casos de exposição)
- elétrica
- destacou-vidro (Corning, Sandia)
+ tratado de proibição de testes de verificação requer esta
- fibra ótica linhas de vedação de um míssil...
- zero padrões...
- decalques....

+ Resinas epóxi
- a la Intel na década de 1970 (8086)
+ Lawrence Livermore: "Conhecedor De Projeto"
- gov agências usando isso para se proteger contra inversa
de engenharia, aquisição de chaves, etc.
+ não pode parar de um determinado esforço, embora
- grava, solventes, plasma a piscar, etc.
- mas pode causar custo ser muito alto (esp. se resina
a fórmula é variada, com freqüência, de modo que a "receita" não pode ser
registado)
+ pode usar epóxi clara com "brilhos" em epóxi e
cuidado 2-posição fotografia usada para gravar padrão
- talvez com uma tampa transparente?
+ de fibra óptica de vedação (feixe de fibras, cortar)
- feixe de fibras é enrolado em torno do dispositivo e, em seguida, selado e
cortado de modo a que cerca de metade as fibras são cortadas; o padrão de
aceso e
apagada fibras é uma assinatura, e é extremamente difícil
para reproduzir
- nanotecnologia pode ser usado (um dia)

5.6. Crypto Programas e Produtos
5.6.1. PGP, é claro
- é uma seção própria, escusado será dizer
5.6.2. "O que sobre chips de hardware para criptografia?"
- A velocidade pode ser obtido, por certo, mas às custas de
limitando o mercado drasticamente. Bom para usos militares,
não é tão bom para utilização civil (especialmente porque a maioria de civis
não tem a necessidade de altas velocidades, todas as outras coisas sendo
de igual).
5.6.3. Carl Ellison "tran" e mistura de várias codificações em cadeias de
- "tran.shar está disponível em ftp.std.com:/pub/cme
- des | tran | des | tran | des
- para fazer o trabalho de um invasor muito mais difícil, e para fazer
diferencial cryptanalyis mais difícil
- "é em resposta a Eli de papel que eu defendia prngxor,
como em:
des | prngxor | tran | des | tran | des
com o DES instâncias no BCE (modo de reconhecimento de
Eli ataque). O prngxor destrói todos os padrões de
de entrada, qual era o propósito da CBC, sem utilizar o
comentários caminho que Eli explorada."[Carl Ellison, 1994-07-
15]

5.6.4. A Blum-Blum-Shub RNG
- sobre o mais forte de algoritmos de geração de números aleatórios sabemos que, embora de forma lenta
(se eles podem prever o próximo bit de BBS, elas podem quebrar
RSA, então....
- ripem.msu.edu:/pub/crypt/outros/blum-blum-shub-forte-randgen.shar
5.6.5. o cipher Blowfish
+ BLOWFISH.ZIP, escrito por Bruce Schneier,1994. objecto de uma
artigo do Dr. Dobb:
- ftp.dsi.unimi.it:/pub/security/crypt/code/schneier-blowfish.c.gz

5.7. Idéias Relacionados
5.7.1. "O que é a "cegueira"?"
+ Este é um primitivas básicas de operação de mais de dinheiro digital
sistemas. Qualquer bom livro sobre a criptografia deve explicar, e
cobrir a matemática necessária para unerstand-lo em detalhe. Vários
as pessoas têm explicado o que é (muitas vezes) da lista; aqui está um
breve explicação por Karl Barrus:
- "Conceitualmente, quando você cego, uma mensagem, ninguém mais pode
lê-lo. Uma propriedade sobre a cegueira é que, sob o
direito circunstâncias, se outro partido assina digitalmente um
cegos mensagem, o cego mensagem irá conter uma
assinatura digital válida.

"Então, se Alice blinds a mensagem "eu devo Alice $1000", de modo
que ele lê (dizem), "uma;dfafq)(*&" ou o que seja, e Bob
concorda em assinar esta mensagem, mais tarde, Alice pode unblind o
mensagem de Bob assinado para recuperar o original. E Bob
assinatura digital será apresentado no original, embora
ele não assinar o original diretamente.

"Matematicamente, o fato de uma mensagem significa multiplicá-lo
por um número (acho que a mensagem como sendo um número).
Desvendamento é simplesmente dividindo-se o original ofuscante
fator." [Karl Barrus, 1993-08-24]
+ E a outra explicação por Hal Finney, que veio na
contexto de como desconectam farmácia prescrições de
identidade pessoal (medos da medial dossiês(:
- "Chaum de "cegos " credencial" sistema destina-se a resolver
exatamente esse tipo de problema, mas requer um
ampla infra-estrutura. Tem que ser uma agência de

onde você fisicamente identificar-se. Ele não tem
para saber qualquer coisa sobre você que alguns físicos de IDENTIFICAÇÃO de
tal como as impressões digitais. Você e cooperar para criar
pseudônimos de várias classes, por exemplo, um "vá para o
médico" pseudônimo, e um "ir à farmácia" pseudônimo.
Estes pseudônimos ter uma certa relação matemática
que permite que você re-cego credenciais gravadas para um
pseudônimo para se aplica a qualquer outro. Mas a agência usa
seu físico de IDENTIFICAÇÃO para certificar-se de que você só obter um pseudônimo
de cada tipo....Assim, quando o médico dá-lhe uma
receita, que é uma credencial aplicado ao seu "ir para
o médico" pseudônimo. (É claro que você pode também revelar
o seu verdadeiro nome para o médico, se desejar.) Então você mostra
ele na farmácia, usando o seu "ir à farmácia"
pseudônimo. A credencial só pode ser mostrado em um presente
pseudônimo no pharamacy, mas é unlinkable para o
você obteve no médico. "[Hal Finney, 1994-09-07]
5.7.2. "Crypto protocolos são, muitas vezes, confuso. Existe uma coerente
a teoria de que estas coisas?"
- Sim, protocolos de criptografia são geralmente expressos como cenários, como
problemas com palavras, como "Alice e Bob e Eva" tipos de
complicado protocolos de interação. Não é exatamente a teoria de jogo,
não é exatamente a lógica, e não exatamente de qualquer outra coisa no
particular...em sua área.
- Sistemas especialistas, prova de regularidade cálculos, etc.
- falsificação, espionagem, motivações, reputação, confiança
modelos
+ Na minha opinião, muito mais trabalho é necessário aqui.
- Gráficos, agentes, objetos, capacidades, objetivos, intenções,
lógica
- evolutiva da teoria dos jogos, cooperação, da deserção, tit-for-
tat, ecologia, economia
- praticamente ignorada, até à data, por criptografia comunidade
5.7.3. O titular de uma chave *é* a pessoa que, basicamente,
- que é a linha de fundo
- aqueles que se preocupar com isso são livres para adotar mais forte,
mais sistemas elaborados (multi-parte, as frases de acesso, biometria
de segurança, limites de acesso de conta, etc.)
- quem tem a chave da casa é essencialmente capaz de obter acesso
(não dizendo que esta é a situação legal, mas a prática
um)
5.7.4. Forte de criptografia é ajudado por um enorme aumento na energia do processador,
redes

+ De criptografia *sempre ganha* mais de criptoanálise diferença aumenta... maior com o tempo
- "os bits ganhar"
+ Redes pode esconder mais bits...gigabits fluxo através de fronteiras, stego, etc.
- redes mais rápidas significam mais "graus de liberdade", mais caminhos para ocultar bits, aumentando exponencialmente esforços vigiar e acompanhar
- (No entanto, estes graus de freedome pode significar maiores chances de escorregar e deixando pistas que permitir a correlação. A complexidade pode ser um problema.)
+ "puxando o plugue" dói demais...desliga do mundo economia para parar ilegal de bits ("impertinente bits"?)
- um dos principais objetivos é alcançar o "ponto de não o retorno," além do que puxar a ficha de rede dói demais
- isto não é para dizer que eles não ainda puxe a respectiva ficha, danos que se dane

5.7.5. "O que é o "Diffie-Hellman" protocolo e por que é importante?"

+ O que é
- Diffie-Hellman, descrita pela primeira vez em 1976, permite-chave o exchange através de canais inseguros.
+ Steve Bellovin foi uma das várias pessoas para explaine D-H para a lista (a cada poucos meses de alguém!). Eu sou incluindo a sua explicação, apesar de sua duração, para ajudar a os leitores que não estão estudando criptografia de obter um sabor da tipo de matemática envolvida. A única coisa a observar é o uso de *exponentiations* e *a aritmética modular* (o "relógio aritmética" de nossa "nova matemática" infâncias, exceto com muito, muito grandes números!). A dificuldade de inverter o exponention (o registo discreto problema) é o que faz este um criptograficamente abordagem interessante.
- "A ideia básica é simples. Escolha um número grande p (provavelmente um primo), e uma base b que é um gerador de o grupo dos inteiros módulo p. Agora, acontece que dado um conhecido p, b, e (b^x) mod p, é extremamente difícil encontrar x. Isso é conhecido como o registo discreto problema.

"Veja como usá-lo. Deixe duas partes X e Y, escolher números aleatórios x e y, 1 < x,y < p. Cada calcular

(b^x) mod p

e

(b^y) mod p

e transmiti-los uns com os outros. Agora, X x e sabe
(b^y) mod p, então s/ele pode calcular a (b^y)^x mod p =
(b^(xy)) mod p. Y pode fazer o mesmo cálculo. Agora
elas sabem (b^(xy)) mod p. Mas os bisbilhoteiros saber
apenas (b^x) mod p e (b^y) mod p, e não pode usar os
quantidades para recuperar o segredo compartilhado. Normalmente, de
é claro, X e Y, vai usar esse segredo compartilhado como uma chave para
um convencional criptosistema.

"O maior problema com o algoritmo, conforme descrito
acima, é que não há nenhuma autenticação. Um invasor
pode sentar-se no meio e fala de protocolo para cada
parte legítima.

"Um último ponto, você pode tratar x como uma chave secreta, e
publicar
(b^X) mod p como uma chave pública. A prova é deixada como um
exercício para
o leitor". [Steve Bellovin, 1993-07-17]
- Por que é importante
+ Usando ele
+ Matt Ghio disponibilizou Phil Karn programa para
geração de números úteis para o D-H:
- ftp cs.cmu.edu:
/afs/andrew.cmu.edu/usr12/mg5n/public/Karn.DH.gerador de
+ Variantes e Comentários
+ De estação para Estação de protocolo
- "O STS protocolo é um regular D-H, seguido por um
(delicadamente concebido) a troca de assinaturas de chave
parâmetros do exchange. As assinaturas na segunda
troca de que eles não podem ser separados a partir do original
parâmetros.....STS é um bem pensado protocolo, com
muitas sutilezas já está organizado para. Para o problema em
a mão, porém, que é Ethernet sniffing, é
autenticação de aspectos que não são necessários agora, mesmo
embora eles certamente serão no futuro próximo."
[Eric Hughes, 1994-02-06]

5.7.6. grupos, vários criptografia, IDEA, DES, dificuldades em
análise
5.7.7. "Por que e como é "aleatoriedade" testado?"
- Aleatoriedade é um conceito central em criptografia. Cifras, muitas vezes,
falhar quando as coisas não são tão aleatórias como designers pensamento
eles seriam.
- A entropia, a aleatoriedade, predictablility. Pode, na verdade, nunca
prove um conjunto de dados de forma aleatória, embora possam ser bastante
confiante (cf. O teste de Kolmogorov-Chaitin teoria da complexidade).
- Ainda assim, truques podem fazer um random-olhando o bloco de texto de olhar
regular....isto é o que a descriptografia não; tais arquivos são
disse ser cryptoregular.
+ Quanto o teste é necessário, isso depende do uso,
e, sobre o grau de confiança necessário. Pode demorar
milhões de amostras de teste, ou até mais, para estabelecer
a aleatoriedade no conjunto de dados. Por exemplo:
- "Os testes padrão para 'aleatoriedade' utilizada no gov
sistemas requer a 1X10^6 amostras. A maioria dos testes são
de probabilidade padrão coisas e alguns são classificados. "
[Wray Kephart, sci.cripta, 1994-08-07]
- nunca assuma que algo é realmente aleatório apenas porque ele
looks aleatório! (Dinâmica de Markov compressores podem encontrar
nonrandomness rapidamente.)
5.7.8. "É possível saber se um arquivo é criptografado?"
- Não, em geral. Undecideability e tudo mais. (Não posso dizer
em geral, se um vírus existe no código, Adleman mostrou, e
não pode dizer, em geral, se um arquivo é criptografado, comprimido,
etc. Vai para problemas do que entendemos por criptografados ou
comprimido.)
+ Às vezes podemos ter alguns muito claros sinais:
cabeçalhos estão ligados
- outros sinais característicos
- a entropia por caractere
+ Mas os arquivos criptografados com forte métodos normalmente olhar
aleatório; na verdade, a aleatoriedade está intimamente relacionada com a
criptografia.
+ de regularidade: todos os símbolos representados igualmente, em todas as bases
(que é, em quartos duplos, triplos, e todas as n-tuplas)
- "cryptoregular" é o termo: arquivo de procura aleatória
(regular), até que a chave adequada é aplicada, então o
aleatoriedade vaDCharles Bennett, "a Física da Computação
Oficina de 1993]
- "entropia" perto do máximo (por exemplo, perto de 6 ou 7 bits por

de caracteres, enquanto a ordinária inglês tem cerca de 1,5-2
bits por caractere da entropia)
5.7.9. "Por que não usar CD-ROMs para as one-time pads?"
- O problema da distribuição de chaves, geral e dores de cabeça. Roubo
ou comprometer o material é claro, o
a maior ameaça.
- E as one-time pads, sendo cifras simétricas, dar o
incríveis vantagens de métodos de chave pública.
- "CD-ROM é um terrível médio para a OTP chave de fluxo.
Primeiro, você quer exatamente duas cópias do fluxo aleatório.
CD-ROM tem uma vantagem económica apenas para grandes corridas.
Segundo, você quer destruir a parte do fluxo de já
usado. CD ROM não tem nenhuma apagar instalações, fora da física
a destruição de todo o disco." [Bryan G. Olson,
sci.cripta, 1994-08-31]
- Se você tem um one-time pad, um DAT faz mais sentido;
barato, pode apagar os bits já usado, não requer
prensagem de um CD, etc. (Uma empresa afirma ser a venda de CD-
ROMs como as one-time pads para os clientes...os problemas de segurança
aqui deve ser óbvio para todos.)

5.8. A Natureza da Criptologia
5.8.1. "O que é realmente básico, primitivo, idéias de
criptologia, protocolos de criptografia, criptografia de anarquia, dinheiro digital,
e as coisas com que lidamos aqui?"
- Eu não quero dizer apenas coisas como a mecânica de criptografia,
mas mais conceitual básico ideias.
5.8.2. Criptografia é sobre a criação e a vinculação de espaços privados...
5.8.3. O "Núcleo" Ideias de Criptologia e o Que temos de Lidar Com
- A física tem a massa, a energia, a força, o ímpeto, angular
dinâmica, gravitação, a fricção, o Princípio da Incerteza,
A complementaridade, a Menos de Acção, e uma centena de outros, tais
conceitos e prinicples, alguns mais básicos do que os outros. Idem
para qualquer outro campo.
+ Parece para muitos de nós que crypto faz parte de um grande
estudo do núcleo de idéias envolvendo: a identidade, a prova, a complexidade,a
aleatoriedade, reputações, de corte e escolha de protocolos, zero
conhecimento, etc. Em outras palavras, as palavras de ordem.
- Mas o que são "núcleo" de conceitos, a partir do qual os outros
são derivados?
- Por que, por exemplo, fazer o "corte-e-escolha" protocolos de trabalho
tão bem, de forma justa? (O que eles fazem tem sido evidente para um
muito tempo, e eles literalmente são instâncias de Salomónicas

sabedoria. Teoria dos jogos tem explicações em termos de pagamento de salários
matrizes, equilíbrios de Nash, etc. Parece provável para mim
que os conceitos de criptografia vai ser reformulada em termos de uma
menor conjunto de idéias básicas tomadas a partir desses diferentes
campos da economia, teoria dos jogos, sistemas formais, e
ecologia. Apenas o meu palpite.)
+ declarações, afirmações, crença, prova
- "Eu sou Tim"
+ de posse de uma chave para um cadeado é geralmente tratada como prova
de...
- não sempre, mas essa é a suposição padrão, que
alguém que destranca uma porta é um do bom
pessoas..privilégios de acesso, etc.
5.8.4. Nós não parecem saber o "deep teoria" sobre o porquê de certas
os protocolos de "trabalho". Por exemplo, por que é "cortar-e-escolha", onde
Alice cortes e Bob escolhe (como bastante dividindo uma torta),
como um sistema justo? Teoria dos jogos tem muito a ver com isso.
Pagamento de salários matrizes, etc.
- Mas muitos protocolos não foram totalmente estudados. Nós sabemos
eles funcionam, mas eu acho que nós não sabemos totalmente por que eles funcionam.
(Talvez eu esteja errado aqui, mas eu já vi alguns trabalhos olhar
estas questões em detalhe.)
- A economia é certamente crucial, e tende a ficar esquecido
na análise de protocolos de criptografia....os vários "Crypto
Anais da conferência" papéis geralmente ignorar económico
fatores (exceto na área de medir a força de um
sistema em termos de custo computacional para quebrar).
- "Todos os criptografia é a economia."
- Nós saiba o que funciona e o que não. Meu palpite é que
complexo de criptografia, sistemas terão comportamentos emergentes que
são descobertos somente após a implantação, ou boa simulação
(daí o meu interesse em "protocolo de ecologia").
5.8.5. "É possível criar cifras que são inquebráveis em qualquer
quantidade de tempo com qualquer quantidade de energia do computador?"
+ Informações-teoricamente seguro vs. computacionalmente seguro
+ não quebráveis, mesmo em princípio, por exemplo, um one-time pad
com caracteres aleatórios selecionados por um verdadeiro processo aleatório
(die joga, decaimento radioativo, certos tipos de ruídos,
etc.)
- e ignorando o "quebráveis por break-ins" abordagem de
roubar o one-time pad, etc. ("Saco preto
criptografia")
- não quebráveis em "razoável" quantidades de tempo com

computadores
- É claro, uma one-time pad (cifra de Vernam) é teoricamente
inquebrável, sem a chave. Ele é "informação-
teoricamente seguro."
- RSA e similares algoritmos de chave pública são disse a ser só
"computacionalmente seguro" para algum nível de segurança
dependente do módulo de elasticidade de comprimento, recursos do computador e a hora
disponível, etc. Assim, dado o tempo suficiente e bastante computador
poder, estas cifras são quebráveis.
- No entanto, eles podem ser praticamente impossível de quebrar, dado
a quantidade de energia no universo.Para não dividir universos
aqui, mas é interessante considerar que algumas cifras
não pode ser frágil em _our_ universo, em qualquer quantidade, de
em tempo. Nosso universo provavelmente tem algum número finito de
partículas (atualmente estimada em 10^73 partículas). Este
leva para o "mesmo se todas as partículas foram um Cray Y-MP-lo
levaria..." o tipo de experiências com o pensamento.

Mas eu estou pensando em _energy_ aqui. Ignorando reversível
cálculo para o momento, cálculos de dissipar a energia
(alguns discordar neste ponto). Há alguns uppper limite
em quantas básicas de cálculos jamais poderia ser feito com o
uma quantidade de energia no universo. (Um cálculo aproximado
poderia ser feito por meio do cálculo de produção de energia das estrelas,
coisas caindo em buracos negros, etc., e, em seguida, supondo que
sobre kT por operação lógica. Este deve ser precisa para
dentro de algumas ordens de magnitude.) Eu não tiver feito isso
de cálculo, e não de hoje, mas o resultado seria provavelmente
ser algo ao longo das linhas de X joules de energia que
poderia ser aproveitado para o cálculo, resultando em Y básico
primitivas computacionais passos.

Posso, então, encontrar um módulo de 3000 dígitos ou 5000 dígitos, ou
seja o que for,que leva mais do que este número de passos para
fator.

Advertências:

1. Talvez realmente existem atalhos para factoring. Certamente
melhorias no factoring métodos irá continuar. (Mas de
claro que essas melhorias não são coisas que converter
factoring em menos de exponencial-em-comprimento
problema...que é, factoring, parece estar "muito duro".)

2. Talvez reversível cálculos (la Landauer, Bennett,
et. al.) na verdade, o trabalho. Talvez isto significa um "factoring
a máquina" pode ser construído, o que leva a um fixo, ou muito lentamente
crescendo, a quantidade de energia.

3. Talvez a mecânica quântica idéia da Costa é possível.
(Duvido, por várias razões.)

Eu continuo a achar que é útil para pensar em números muito grandes
como a criação de "campos de força" ou "bolhas" (a la Vinge) em torno de
dados. Um 5000-decimal dígitos módulo de elasticidade é tão perto de ser
inquebrável que qualquer coisa que nós vamos ver neste universo.

5.9. Prática De Criptografia
5.9.1. novamente, este material é coberto em muitas de nossas perguntas frequentes sobre o PGP e
em matéria de segurança que estão flutuando em torno de...
5.9.2. "Por quanto tempo deve-crypto ser válido?"
+ O que é, quanto tempo deve um arquivo permanecem uncrackable, ou um
assinatura digital permanecem unforgeable?
- probabalistic, é claro, com diferentes níveis de confiança
- depende de avanços na matemática e na alimentação do computador
+ Algumas mensagens precisam apenas ser válido para alguns dias ou
semanas. Outros, por décadas. Alguns contratos podem precisar de
ser unforgeable por muitas décadas. E adiantamentos em
alimentação do computador, o que parece ser uma chave forte, hoje, pode
falhar completamente, até 2020, ou 2040. (Eu estou, naturalmente, não
o que sugere que uma 300 ou 500 dígitos RSA módulo será
prática até então.)
+ muitas pessoas só precisam de segurança para uma questão de meses ou
assim, enquanto que outros podem precisar (ou acha que eles precisam) para
décadas ou até mesmo para gerações
- eles podem temer a retaliação contra os seus herdeiros, para
exemplo, se determinadas comunicações foram sempre feitas
público
- "Se você for assinar o contrato, digitalmente, por exemplo,
você gostaria de ter certeza de que ninguém poderia forjar seu
assinatura para alterar os termos após o fato-alguns
meses não é suficiente para tais fins, apenas algo que
vai durar quinze ou vinte anos, tudo bem." [Perry
Metzger, 1994-07-06]
5.9.3. "O que acha de comerciais, programas de criptografia para a proteção de

arquivos?"
- ViaCrypt, PGP 2.7
- Vários programas comerciais já existem há muitos anos (eu tenho
"Sentinela" em 1987-8...muito tempo, já descontinuado). Seleção
as resenhas nos principais revistas.
+ Kent Marsh, FolderBolt para mac e Windows
- "O melhor do Mac programa de segurança....é CryptoMactic por Kent
Marsh, Lda. Ele usa triple-DES em modo CBC, hashes de um
arbitrária senha de comprimento em uma chave, e tem um monte
do Mac-recursos de interface. (O Windows equivalente é
FolderBolt para o Windows, a propósito.)" [Bruce Schneier,
sci.cripta, 1994-07-19]
5.9.4. "Quais são alguns passos práticos para melhorar a segurança?"
- Você, como a maioria de nós, deixar de cópia de segurança disquetes de imposição
ao redor?
- Você usa várias passagens rasuras de discos? Se não, o
bits podem ser recuperados.
- (Um deles pode comprometer todo o material codificado você
têm, todos, com nada mais do que um mandado de busca do seu
instalações.)
5.9.5. Picking (e lembrar) palavras-passe
- Muitas das questões aqui também se aplicam para a escolha de remetentes,
etc. Coisas que muitas vezes são mais complicadas do que parecem. O
"estrutura" desses espaços é complicado. Por exemplo, ele pode
parecem realmente furtivo (e "alta entropia" a troca de alguns
palavras em uma canção popular e use-o como um passe
a frase....mas isso, obviamente, vale a pena apenas alguns bits de
extra entropia. Especificamente, o atacante vai gostar de tomar
os cerca de mil canções mais populares, mil ou, de modo mais
nomes populares, slogans, discursos, etc., e, em seguida, executar muitos
permutações em cada um deles.
- bits de entropia
- muitas falhas, fraquezas, fatores escondidos
- evite palavras simples, etc.
- difícil conseguir 100 ou mais bits de entropia reais
- Como Eli Brandt coloca, "Obscuridade não é um substituto para
forte números aleatórios." [E. B., 1994-07-03]
- Criptoanálise é uma questão de dedução, de formação e
refinamento de hipóteses. Por exemplo, o site
"bitbucket@ee.und.ac.za" é anunciado na Net como um
local para enviar "da NSA alimentar" a...e-mail enviado a ele fica
descartados. Então , um ótimo lugar para enviar cobertura de trânsito, não?
Não, como o NSA vai marcar este site para que ele e a sua

utilidade é soprado. (A menos que a sua utilidade é, na verdade,
outra coisa, caso em que a descida recursiva tem
começou.)
- Bohdan Tashchuk sugere [1994-07-04] usando o telefone como
números, misturadas com palavras, para melhor ajuste com humanos
a memorização de hábitos; ele observa que em 30 ou mais bits de
entropia são rotineiramente memorizado desta forma.
5.9.6. "Como posso lembrar-me de longo palavras-passe ou frases de acesso?"
- Lotes de artigos de segurança tem dicas sobre a escolha de difícil
acho que (alta entropia) palavras-passe e frases de acesso.
+ Apenas fazê-lo.
- As pessoas podem aprender a memorizar longas sequências. Eu não sou bom
neste, mas em outros aparentemente são. Ainda assim, parece
perigoso, em termos de esquecer. (E escrever um
frase-chave pode ser muito mais arriscado do que um menor, mas
mais facilmente memorizado a frase-passe é. Eu acho que roubo
de teclas e teclas de captura em máquinas comprometidas
são muito
mais importante prático fracos.)
+ As primeiras letras de longas frases que fazem sentido apenas para
o proprietário.
- por exemplo, "Quando eu tinha dez anos, eu comi a coisa toda."--->
"wiwtiatwt" (os Puristas vão tergiversar que preposicionada
frases como "quando eu era" de menor entropia. Verdade, mas
melhor do que "Josué.")
+ Visual sistemas
- Outra abordagem para obter o suficiente de entropia em
senhas/frases é um "visual key", onde uma ratos de
uma posição para outra em um ambiente visual. Que é,
um é apresentado com uma cena contendo um certo número de
nós, talvez representando objetos familiares de um
própria casa, e um caminho é escolhido. A vantagem é que
a maioria das pessoas pode se lembrar bastante complicado
(leia-se: alta entropia) "histórias". A cada objeto que aciona uma
memória do objeto à visita. (Exemplo: porta para
cozinha para o blender frigorífico ..... Esta é a
memória visual do sistema dito ser favorecido pela épico grego
poetas. Isso também fica ao redor do teclado-monitoramento
truque (mas não necessariamente o CRT-trick leitura, de
curso).

Ele pode ser um interessante hack para oferecer isso como uma frente

final de PGP. Até mesmo uma simples grade de caracteres, o que poderia
ser moused poderia ser um auxiliar na utilização a longo
frases.

5.10. DES
5.10.1. no projeto do DES
- Biham e Shamir demonstraram como "diferencial cryptanalyis"
pode fazer o ataque mais fácil do que pesquisa de força bruta do
2^56 keyspace. Wiener fez um experimento de pensamento de design de uma
"DES buster" (máquina que ya gonna call?) que poderia quebrar
uma chave DES em questão de dias. (Semelhante ao Diffie e
Hellman análise de meados da década de 70, atualizado para o atual
a tecnologia.)
+ O IBM designers sabia sobre o diferencial cryptanalyis, ele
agora é claro, e tomou medidas para otimizar DES. Depois De Shamir
e Biham publicados, Não Coppersmith reconheceu isso.
Ele escreveu um artigo de revisão:
- Coppersmith, D., "O Padrão de Criptografia de Dados (DES) e
sua resistência contra ataques." IBM Jornal da Pesquisa
e Desenvolvimento. 38(3): 243-250. (Maio de 1994)

5.11. Quebrar Cifras
5.11.1. Este não é um dos principais Cypherpunks preocupação, por uma variedade de
razões (lotes de trabalho, conhecimentos específicos, de grandes máquinas, e não um
área central, cifras sempre ganhar no longo prazo). Quebrando
cifras é algo a se considerar, portanto, esta breve seção.
5.11.2. "Quais são as possíveis consequências de deficiências no crypto
sistemas?"
- talvez a leitura de mensagens
- talvez forjar mensagens
- talvez falsificando documentos de carimbo de data / hora
- talvez a drenagem de uma conta bancária em segundos
- talvez a ganhar a criptografia do sistema de jogo
- talvez questões de vida e morte
5.11.3. "O que são as mais fracas locais em cifras, praticamente
falando?"
- Chave de gestão, sem dúvida. As pessoas deixam suas chaves
em torno de mentir , anote as suas senhas. etc.
5.11.4. Aniversário ataques
5.11.5. Por exemplo, a Criptografia '94 foi relatado em uma garupa de sessão
(por Michael Wiener com Paul van Oorschot) que uma máquina para
quebrar o MD5 cifras poderiam ser construídos por cerca de us $10 M (em 1994
dólares, claro) e poderia quebrar MD5 em cerca de 20 dias.

(Segue-se a 1993 papel em uma máquina semelhante à de quebra de DES.)

- Hal Finney fez alguns cálculos e informou-nos:
- "Eu mencionei há alguns dias atrás que uma das "garupa"sessão de papéis na criptografia conferência afirmou que uma máquina poderiam ser construídas com o que iria encontrar MD5 colisões para us $10 milhões cerca de 20 dias.....O resultado é que temos tido praticamente não há mais tempo (2^64 criações da MD5 vai dominar) e praticamente nenhum espaço (em comparação com os 2^64 armazenados valores), e nós, o efeito de um ataque de aniversário. Este é outra advertência ponto de dados sobre os riscos da dependência no espaço de custos para a segurança, ao invés de incluir custos de tempo." [Hal Finney, 1994-09-09]

5.11.6. pkzip relatado quebrado

- "Eu finalmente encontrei tempo para dar uma olhada no algoritmo de criptografia por Roger Schlafly que é usado em PKZIP e desenvolveram uma prática ataque de texto simples conhecido que pode encontrar toda a 96 bits internos do estado." [Paulo Carl Kocher, comp.riscos, 1994-09-04]

5.11.7. Jogos ataques, onde as lacunas existentes em um sistema de exploração

- concursos, que são derrotados por ataques automatizados
- todo o sistema jurídico pode ser visualizado desta forma, com as equipes de advogados olhando para ataques legais (e quanto mais complexo o código legal, mais ataques podem ser montado)
- ecologia, onde as fraquezas são explorados impiedosamente, forçando a maioria das espécies em extinção
- economias, idem, exceto rápido
- os perigos para esquemas de criptografia são claras

+ E há links importantes para o problema de excessivamente formal sistemas, ou sistemas nos quais comum "discrição" e "escolha" é substituído por regras de fora

- como com regras dizendo empregadores em grande detalhe quando e como eles podem descarga empregados (cf. a discussão de "razoável regras obrigatórias," em outro lugar)

tais regras são explorados pelos colaboradores, que seguem o "letra da lei", mas estão se apresentando em uma forma inaceitável para o empregador

relacionados com a "localidade de referência" pontos, em que problema deve ser resolvido localmente, e não com a intervenção de longe.

- as coisas nunca mais vai ser perfeito, desde o perspetive de todos os partes, mas a intromissão de fora faz com que as coisas em um

jogo, a ponto de todo este seção
+ Implicações para o dinheiro digital: excessivamente complexo jurídico
sistemas, sem as vantagens locais de dinheiro verdadeiro (liquidado localmente)
+ pode precisar injetar um pouco de supra-legal de aplicação
mecanismos para o sistema, para torná-lo convergir
- ventos de crédito de bancos de dados, além de chegar dos EUA e
outras leis
+ de violência física (um motivo para que as pessoas não "jogar jogos"
com a Máfia, Tríades, etc., é que eles sabem o implicações)
- não é antiético, como eu vê-lo, para os contratos em
que as partes entendem que uma possível ou até mesmo
provável conseqüência de sua incapacidade para executar é a morte

5.11.8. O grupo Diffie-Hellman key exchange vulnerabilidades
- "homem-no-meio" de ataque
+ sistemas de telefone de uso de voz, leitura de LCD número indicado
- como computador de energia aumenta, mesmo _this_ pode ser insuficiente

5.11.9. A engenharia inversa de cifras
- A5 código utilizado em telefones GSM foi de engenharia reversa a partir de um de descrição de hardware
- Graham Toal relatórios (1994-07-12) que GCHQ bloqueado público palestras sobre isso

5.12. Pontas Soltas

5.12.1. "Grande Mestre de xadrez Problema" e outras Fraudes e Falsificações
de central importância para as provas de identidade (uma la Fiat-Shamir)
- "terrorista" e "Máfia falsificar" problemas

6. A Necessidade De Uma Forte Criptografia

6.1. direitos autorais

6.2. RESUMO: A Necessidade De uma Forte Criptografia

6.2.1. Pontos Principais

- Forte de criptografia recupera o poder de decidir por si mesmo,
para negar o "Censor" o poder de escolher o que se lê,
assiste ou ouve.
6.2.2. Ligações para Outras Secções
6.2.3. Onde Encontrar Informações Adicionais
6.2.4. Diversos Comentários
- esta secção é curto, mas é menos concentrado do que os outros
seções; é, essencialmente, uma "transição" do capítulo.

6.3. Usos gerais e Razões de Criptografia
6.3.1. (ver também a extensa lista de "Motivos para o Anonimato"
que faz com que muitos pontos sobre a necessidade e as usa para o forte
crypto)
6.3.2. "Onde está a criptografia de chave pública realmente necessário?"
- "É o caso que há relativamente pouca necessidade de
assimétrica criptografia de chave em pequenas populações fechadas.
Por exemplo, os bancos a dar-se bem sem. O
vantagem de chave pública é que ele permite que as privadas
a comunicação em uma grande e aberto a população e com um
mínimo de predeterminação." [WHMurray, sci.cripta, 1994-08-
25]
- Que é, de chave simétrica sistemas (tais como a convencional
cifras, uma vez almofadas, etc.) funciona razoavelmente bem por
predeterminação entre as partes. E, claro, um tempo de almofadas
tem a vantagem adicional de informações-
teoricamente seguro. Mas assimétrica ou de chave pública métodos
são extremamente úteis quando: as partes não atendidas
antes, quando o material da chave não foi trocado, e quando
há preocupações sobre como armazenar o material de chave. O para-
chamado de "chave de problema de gestão", quando N as pessoas querem
comunicar pairwise uns com os outros é bem fundada.
- E, claro, criptografia de chave pública, torna-se possível todos os
outras coisas úteis, como dinheiro digital, DC-Redes, zero
provas de conhecimento, de compartilhamento de segredo, etc.
6.3.3. "Quais são as principais razões para o uso de criptografia?"
- as pessoas criptografar para o mesmo reafilho de fechar e bloquear
suas portas
+ De privacidade em suas formas mais básicas de
- texto -- registros, diários, cartas, e-mail
- som -- conversas por telefone
- outros --de vídeo
+ telefones, intercepta, celular, celular, carro, telefones,
scanners

+ fazer escuta ilegal é inútil (e ineficiente)
- e as autoridades estão isentos de tais leis
- as pessoas precisam para se proteger, de ponta a ponta
+ "Como posso proteger os meus arquivos pessoais, e meu telefone chamadas?"
- Pessoalmente, eu não me preocupar muito. Mas muitas pessoas o fazem. Ferramentas de criptografia estão amplamente disponíveis.
- Telefones celulares são notoriamente inseguros, como são telefones sem fio (menos seguro). Existem leis sobre o monitoramento, um pequeno conforto que pode ser. (E Eu estou em grande medida oposição a tais leis, por libertário razões e porque ele cria uma falsa sensação de segurança.)
- Laptops são, provavelmente, menos vulnerável a Van Eck tipos de de RF de monitoramento que são CRTs. A tendência para menor poder, LCDs, etc., todas as obras para diminuir vulnerabilidade. (No entanto, a alimentação do computador para a extração de sinais fracos de ruído está aumentando mais rápido do que o RF são decrescentes....os intercâmbios são claras.)
+ sistema de encriptação de mensagens, pois a entrega de correio é tão esquisito
- que seja, e-mail é misdelivered,através de hosts incorretamente processamento de endereços
- criptografia, obviamente, evita mal-entendidos (embora faz pouco para pegar a correspondência entregue corretamente)
+ De criptografia para Proteger Informações
- o padrão de razão
+ criptografia de e-mail está aumentando
- os vários casos judiciais sobre os empregadores leitura aparentemente privado de e-mail irá aguçar esse debate (e levantar a questão de proibindo os empregadores de criptografia; ressonâncias com a maioria-resolvido problema do razoável o uso de telefones da empresa para chamadas privadas-mais eficiente para deixar o pessoal chama de perder o horário de colaboradores para telefones públicos)
+ de criptografia de fax irá aumentar, e muito, principalmente como os avanços da tecnologia e de como os perigos de interceptação tornam-se mais aparentes
- também, maior ligações entre o remetente e o receber, como oposição ao atual "discar o número e a esperança é o direito de uma" abordagem, irá incentivar o adicional uso de criptografia
- "a abóbada eletrônica" de grandes quantidades de informação, enviado mais de T1 e T3, redes de dados, por exemplo, cópia de segurança do material

para bancos e grandes corporações
+ a quilômetros e quilômetros de fiação de rede dentro de um
corporation-LANs, WANs, Novell, Ethernet, TCP-IP, Banyan
e assim por diante-podem ser todos verificados para torneiras...que sequer
os registos de saber se algum particular fio está indo
onde deveria? (para muitos imigrantes encontros, perdido
registros, conexões ad hoc, etc.)
- a solução é ter point-to-point encryption, mesmo
dentro de corporações (para itens importantes, pelo menos)
- LANs sem fio
+ empresas estão cada vez mais preocupados com
a interceptação de informações importantes-ou mesmo aparentemente
informação do menor-e sobre hackers e outros intrusos
- chamadas para a rede de melhoria de segurança
- eles estão contratando "tigre equipes" para reforçar a segurança
+ telefones celulares
- interceptações são comuns (e isso está se tornando
publicado)
- modificações comercial scanners de descrever em
newsletters
- algo como o Lotus Notes pode ser um principal substrato para
a efetiva introdução de métodos de criptografia (idem para
hipertexto)
- fornece criptografia de "solidez" ao ciberespaço, no
sentido de criar paredes, portas, estruturas permanentes
- pode até haver requisitos legais para uma melhor segurança
através de documentos, prontuários, registros de funcionários, etc.
+ De criptografia de Sinais de Vídeo e de Criptografia para Controle de
Pirataria
- este é, naturalmente, toda uma tecnologia e indústria
- Videocypher II tem sido rachado por muitos de vídeo hackers
- toda uma indústria de casa de campo em fissuras, tais cifras fracas
- observe que a proibição de criptografia iria abrir muitas
indústrias para a destruição pela pirataria, o que é ainda
outra razão por grosso de proibição de criptografia é condenado
a falha
- Proteger vídeos caseiros--vários casos de casa de assaltos
onde privada x-rated fitas de estrelas foram tomadas, em seguida,
vendidos (Leslile Visser, a CBS Sports)
- estas razões gerais vai fazer de encriptação mais comuns,
mais socialmente e legalmente aceitável, e, portanto, fazer
eventuais tentativas para limitar o uso de criptografia anarquia
métodos simulado

+ Assinaturas digitais e Autenticação
+ para formulários eletrônicos de contratos e digital
registro de data e hora
- ainda não testei nos tribunais, apesar de este deve vir
em breve (talvez, de 1996)
+ pode ser muito útil para provar que as transações
aconteceu em um determinado momento (de Tom Clancy tem uma situação
em "Dívida de Honra", em que todos os Wall Street central
registros de estoque, negociações são varridos em um software
regime: somente os registros de comerciantes são úteis, e
eles estão preocupados com estas sendo fudged para ativar
lucros...timestamping ajudaria imensamente)
- embora certos paródias, um la a brilhante centavo golpe,
são ainda possíveis (registrar vários comércios, apenas
revelar a lucrativas)
- negociações
- AMIX, Xanadu, etc.
+ é a proteção real contra vírus (desde que todas as outras
métodos de digitalização será cada vez mais falhar)
- aos autores de software e distribuidores "assinar" seu
trabalho...sem virus escritor pode, possivelmente, forjar o digital
assinatura
+ Provas de identidade, senhas e o uso do sistema operacional
- ZKIPS especialmente em redes, onde as chances de ver
uma palavra-passe de serem transmitidas são muito maiores (uma óbvia
ponto que não é muito discutido)
+ sistemas operacionais e bancos de dados precisam de mais seguro
os procedimentos para acesso, para agentes e gostaria de pagar para
de serviços, etc.
- unforgeable tokens
+ Ciberespaço terá a melhor proteção
- para garantir a fraude e a contrafacção é reduzido
(lembre-se de Habitat de problemas com as pessoas a descobrir o
brechas)
+ OH se está também a trabalhar na "construção de mundos" em Los
Alamos, ele pode estar usando evolutiva de sistemas e
resumo de matemática para ajudar a construir a melhor e mais "coerente"
mundos
- agentes, demônios, estruturas, objetos persistentes
- criptografia para proteger essas estruturas
+ abstrato parte da matemática do ciberespaço: resumo
medida espaços, topologias, métricas de distância
- maio de figura para o equilíbrio entre o usuário

malleabilty e a rigidez do espaço
- Chaitin da AIT...ele tem medidas obtidas para estes
+ Digital Contratos
- e-mail-se muito facilmente forjado, falsificado (e perdido, extraviado)
+ Anonimato
- remailing
- lei de evasão
- samizdats,
- Cartões inteligentes, caixas eletrônicos, etc.
- Dinheiro Digital
Direito de voto
+ Informações Mercados
- dados paraísos espionagem
+ De privacidade de Compras
- para princípios gerais, para impedir que uma sociedade da vigilância
+ especializadas, listas de discussão
- fornecedores de pagar para obter os nomes (Crista etiquetas)
- Smalltalk ofertas de emprego
- na era eletrônica, será muito mais fácil de "troll" para
especializada nomes
- as pessoas vão querer "seletivamente divulgar" sua
interesses (na verdade, alguns, alguns não)
6.3.4. "O que pode limitar o uso de criptografia?"
+ "É muito difícil de usar"
- vários protocolos (considerar apenas o quão difícil é
na verdade, enviar mensagens criptografadas entre as pessoas de hoje)
- a necessidade de se lembrar de uma senha ou frase de acesso
+ "É muito trabalho"
- o argumento de que as pessoas não se preocupam em usar
palavras-passe
- em parte, porque não acho que nada vai acontecer
eles
+ "O que você tem a esconder?"
- por exemplo, imagine alguns comentários que eu gostaria de ter ficado com a Intel tinha
Eu encriptado tudo
- e os governos tendem a ver a criptografia, ipso facto,
a prova de que as ilegalidades estão sendo cometidos: drogas, dinheiro
lavagem de dinheiro, evasão de divisas
- lembre-se o "confisco" controvérsia
+ Governo está tomando várias medidas para limitar o uso de
e encriptação segura de comunicação
- algumas tentativas falharam (S. 266), alguns foram
esqueceu-se, e quase nenhum ainda têm sido testados no

tribunais
- veja as outras seções...
+ Tribunais Estão ficando para Trás, Estão Superlotadas e não conseguem Lidar
Adequadamente com Novas Questões, Tais como a Criptografia e a Criónica
- o que levanta a questão da "Ciência Tribunal" novamente
- e a migração para o privado adjudicação (regulamentação
arbitragem)
- BTW, anônimo sistemas são essencialmente o final de mérito
sistema (no sentido óbvio) e para voar na cara da
"a contratação pelos números" de facto o sistema de quotas agora
creeeping em tantas áreas da vida....pode haver regras
exigir que todos os negócios para manter o controle do sexo,
a raça e a "capacidade de grupo" (eu estou brincando, eu espero) de seus
empregados e seus consultores
6.3.5. "O que são alguns provável futuro utiliza de criptografia?"
- Vídeo conferência: sem criptografia, ou com o governo
acesso, reuniões corporativas tornar público...como se um
agente do governo estava sentado em uma reunião, a tomar notas.
(Pode ser que haja alguns que acham que isso é uma boa idéia, uma seleção
empresa de travessuras. Eu não. Muito um preço muito alto para
paga para o marginal ou ilusória melhorias.)
- apresentar suas opiniões
+ obter e oferecer tratamentos médicos
- com ou sem licenças médicas união (AMA)
- não aprovados os tratamentos
- bootleg tratamentos médicos
- informação de mercados
+ santuário de movimentos subterrâneos de ferrovias
- para esposas espancadas
- e para os pais tomar de volta os seus filhos
- (Eu não estou tomando partido)
- contrabando
- a evasão fiscal
- dados paraísos
- bookies, apostas, jogos de números
- remetentes, o anonimato
- religiosas (redes digitais confessionários)
- dinheiro digital, para a privacidade e para a evasão fiscal
- digital hits
- participação de grupo de notícias -- o arquivamento do Netnews é
lugar-comum, e aumentos na densidade de armazenamento torná-lo
provável que no futuro ninguém vai ser capaz de comprar
discos com "Usenet, 1985-1995", e assim por diante (ou acesso,

de pesquisa, etc. on-line sites)
6.3.6. "Há ilegal utiliza de criptografia?"
- Atualmente, não há cobertor leis nos EUA sobre criptografia.
+ Existem situações específicas em que a criptografia não pode ser usado livremente (ou o uso por extenso)
- sobre o rádio amador airwave...chaves devem ser fornecidos
+ Carl Elllison tem observado muitas vezes que a criptografia tem está em uso por muitos séculos, a noção de que ele é um "militares" da tecnologia que os civis tenham um pouco de como ficou falar é simplesmente falso.
- e mesmo a criptografia de chave pública foi desenvolvido em uma universidade (Stanford, em seguida, MIT)

6.4. Proteção Corporativa e Financeira de Privacidade
6.4.1. as corporações estão cada vez mais preocupados com a interceptação de informações importantes-ou mesmo aparentemente menor informações sobre hackers e outros intrusos
- chamadas para a rede de melhoria de segurança
- eles estão contratando "tigre equipes" para reforçar a segurança
+ telefones celulares
- interceptações são comuns (e isso está se tornando publicado)
- modificações comercial scanners de descrever em newsletters
- algo como o Lotus Notes pode ser um principal substrato para a efetiva introdução de métodos de criptografia (idem para hipertexto)
6.4.2. Espionagem corporativa (ou "Business Research")
+ Xeroxing de documentos
- lembre-se de forma Murrray Madeiras inspecionados arquivos de Fred Buch, suspeitando que ele havia removido os grampos e Xeroxed os documentos para a Zilog (por volta do final de 1977)
- um precedente: as formas de grampos
+ cores de papel e tinta...blues, por exemplo
- mas estas de baixa tecnologia esquemas são de fácil contornar
+ Vai sociedades de reprimir o uso de modems?
+ depois de tudo, as especificações de um chip ou produto pode ser enviado por correio fora da empresa, utilizando a empresas próprias redes!
- aplica-se a saída de letras de bem (e eu nunca ouviu falar de alguma empresa de inspeção para esse detalhe, embora pode acontecer a defesa empreiteiros)
+ e mensagens ainda podem ser escondidos (covert canais)

- embora com muito menor largura de banda e com mais esforço
requerido (ele vai parar o casual, o vazamento de informações)
- o LSB método (embora este ainda envolve digital
meios de armazenamento, por exemplo, um disquete, o que pode ser
restrito)
- vários outros regimes: enterrado em formato de processamento
(na largura de banda baixa)
- sutilezas como secretas canais não são mesmo
considerado por empresas-muitas fugas caminhos!
+ parece provável que os funcionários do governo com a segurança
folgas vai enfrentar restrições no seu acesso aos AMIX-
gostaria de sistemas, ou até mesmo para "privado" convencionais
bancos de dados
- pelo menos quando eles usam UseNet, o argumento vai,
eles podem ser supervisionado, em certa medida
+ Fora do local de armazenamento e acesso de material roubado
+ em vez de armazenar roubado plantas e esquemas em
instalações da empresa, eles podem ser armazenados em um local remoto
- possiby desconhecido para a empresa, através de cryptoanarchy
técnicas
+ "Pesquisa de negócios" é o eufemismo para empresas
espionagem
- muitas vezes a contratação de ex-DIÂMETRO e agentes da CIA
+ Empresas americanas podem intensificar a espionagem econômica
uma vez que é revelado apenas como extensiva a espionagem por
Europeus e Japoneses empresas tem sido
- Chobetsu relatórios para MITI
- Mossad aids empresas Israelenses, por exemplo, Elscint. Elbit
+ Bidzos chama isso de "digital Pearl Harbor" (ataques
segurança de rede)
seria irônico, se fracos colocar em criptografia de engrenagem
voltou para nos assombrar
+ empresas vão querer uma distância de um braço relação com
corporativa spies, para se proteger contra ações judiciais,
acusações criminais, etc.
terceiro, agências de pesquisa será utilizado
6.4.3. Criptografia para Proteger Informações
- o padrão de razão
+ criptografia de e-mail está aumentando
- os vários casos judiciais sobre os empregadores leitura
aparentemente privado de e-mail irá aguçar esse debate (e
levantar a questão de proibindo os empregadores de criptografia;
ressonâncias com a maioria-resolvido problema do razoável

o uso de telefones da empresa para chamadas privadas-mais eficiente
deixe algumas chamadas pessoais de perder o tempo de
colaboradores para telefones públicos)
+ de criptografia de fax irá aumentar, e muito, principalmente como
os avanços da tecnologia e de como os perigos de interceptação
tornam-se mais aparentes
- também, maior ligações entre o remetente e o receber, como
oposição ao atual "discar o número e a esperança é a
da direita" abordagem, irá incentivar o uso adicional de
criptografia
- "a abóbada eletrônica" de grandes quantidades de informação, enviada
mais de T1 e T3, redes de dados, por exemplo, cópia de segurança do material para
os bancos e as grandes corporações
+ a quilômetros e quilômetros de fiação de rede dentro de um
corporation-LANs, WANs, Novell, Ethernet, TCP-IP, Banyan
e assim por diante-podem ser todos verificados para torneiras...que sequer
os registos de saber se algum particular fio está indo
onde deveria? (para muitos imigrantes encontros, perdido
registros, conexões ad hoc, etc.)
- a solução é ter point-to-point encryption, mesmo
dentro de corporações (para itens importantes, pelo menos)
- LANs sem fio
- fornece criptografia de "solidez" ao ciberespaço, no sentido de
criação de paredes, portas, estruturas permanentes
- pode até haver requisitos legais para uma melhor segurança
através de documentos, prontuários, registros de funcionários, etc.
6.4.4. EUA dispostos a apreender os bens que passam através dos EUA
(Haiti, Iraque)
6.4.5. Privacidade de pesquisa
- ataques contra empresas de tabaco, exigindo a sua privadas
pesquisa de documentos a ser entregue ao FDA (porque
o tabaco é o "jogo justo" para todos esses ataques, ...)
6.4.6. Usando crypto-mediada de negócios para ignorar "bolsos"
responsabilidade ternos, abuso de regulamentos, do tribunal de sistema,
etc.
+ Abusos de Processos: a tendência de enorme
julgamentos...vários milhões de euros para uma mulher queimou quando ela
derramado café quente em uma MacDonald ($160 K por danos morais, o
resto de "danos punitivos")
- milhares de milhões de dólares para várias decisões do júri
- "bolsos" ações judiciais são uma nova forma de populismo, de
Tocqueville bolso-picking
+ Por exemplo, um shareware autor pode coletar o dinheiro digital

sem ser rastreáveis por aqueles que se sentem injustiçados
- É este "direito"? Bem , o que o contrato diz? Se
o cliente comprou ou usou o produto, sabendo que o
autor/vendedor foi untraceable, e que nenhum adicional
garantias foram dadas, o que houve fraude
comprometida?
+ de criptografia pode, com alguns custos, tomar interações fora do
alcance dos tribunais
- substituir os tribunais com PPL-estilo privada-produzido
justiça
6.4.7. anônimo comunicação e empresas
- A maioria das empresas vai evitar anônimo comunicações,
temendo as repercussões, a ilegalidade (vis-a-vis
a lei antitruste), e o "unwholesomeness" de
+ Alguns podem usá-lo para acesso concorrente inteligência, ventos
dados paraísos, etc.
- Até aqui, provavelmente através de "comprimento do braço" relações
com o apoio de consultores externos, análoga para os recortes utilizados
pela CIA e outros enfeites para isolar-se do
encargos
- Mais ousadas de todos vai ser o "crypto-zaibatsu" que usam
forte de criptografia a criptografia anarquia sabor para organizar
colusão negócios, para remover os concorrentes através da força, e para
geralmente perseguir o "lado negro da força," a moeda de um
a frase.

6.5. Assinaturas Digitais
6.5.1. para formulários eletrônicos de contratos
- ainda não testei nos tribunais, apesar de este deve vir em breve
(talvez, de 1996)
6.5.2. negociações
6.5.3. AMIX, Xanadu, etc.
6.5.4. é a proteção real contra vírus (desde que todas as outras
métodos de digitalização será cada vez mais falhar)
- aos autores de software e distribuidores "assinar" seu trabalho...não
vírus escritor pode, possivelmente, forjar a assinatura digital

6.6. Usos políticos de Criptografia
6.6.1. Os Dissidentes, A Anistia Internacional
- A maioria dos governos, quer saber o que seus assuntos são
dizendo...
- Forte de criptografia (incluindo steganography para ocultar a
existência de comunicações), é necessário

- Myanmar (Birmânia) dissidentes são conhecidos por estar usando PGP
6.6.2. relatos de que os rebeldes em Chiapas (México, os Zapatistas) estão em
a Net, presumivelmente usando PGP
- (se NSA pode realmente crack PGP, este é, provavelmente, um primeiro -
destino para compartilhar com o governo Mexicano)
6.6.3. Liberdade de expressão tem diminuído na América--criptografia fornece uma
antídoto
- as pessoas são processados por expressão de opiniões, são os livros proibidos
("Loompanics Prima" de frente para as investigações, pois alguns
crianças pedi alguns livros)
+ SLAPP naipes (Estratégico Lawsuiits Contra Públicas
De participação), concebido para assustar opiniões divergentes por
ameaçando legal ruína nos tribunais
- alguns juízes têm encontrado para os réus e ordenou a
Mãos a pagar danos próprios, mas isso ainda é um
fala-refrigeração tendência
- crypto untraceability é boa imunidade a esta tendência, e
é assim *real* liberdade de expressão

6.7. Além do bem e do Mal, ou, Por Criptografia é Necessária
6.7.1. "Por que é criptografia de bom? Porque é que o anonimato é bom?"
- Essas questões morais pop-up na Lista de vez em quando,
muitas vezes, alguém perguntou se preparando para escrever um papel para um
classe de ética ou outros enfeites. A maioria de nós na lista, provavelmente,
acho que as respostas são claramente "sim", mas muitos no público
não pode pensar assim. A velha dicotomia entre "Nenhum dos seus
danado de negócios" e "o Que você tem a esconder?"
- "É bom que as pessoas podem escrever diaried não lidas por
os outros?" "É bom que as pessoas podem falar uns com os outros
sem a aplicação da lei de saber o que eles estão dizendo?" "É
é bom que as pessoas podem bloquear as suas portas e esconder
fora da igreja?" Estes são todos essencialmente equivalente à
perguntas acima.
- O anonimato pode não ser bom ou não é bom, mas o
outlawing de anonimato exigiria um estado policial para
impor, invadiriam idéias básicas sobre o privado
transações, e gostaria de encerrar muitas opções que alguns
grau de anonimato, torna-se possível.
- "As pessoas não devem ser anônima" é uma instrução normativa
que é impraticável aplicar.
6.7.2. Falando do isolamento físico ameaças e pressões
que o ciberespaço oferece, Eric Hughes escreve: "Um dos
toda pontos de anonimato e pseudonímia é criar

imunidade a essas ameaças, que todos são baseados sobre a
corpo humano e o seu ambiente físico. Qual é o ponto de
de um sistema de anonimato, que pode ser aberto quando algo
"ruim" acontece? Estes sistemas não rejeitar o regime de
violência; em vez disso, eles simplesmente reduzi-la um pouco mais
e fazer a sua moralidade um pouco mais explícita.....Eu desejo
sistemas que não necessitam de violência para a sua existência e
estabilidade. Eu desejo o anonimato como um aliado para quebrar o domínio
da moralidade sobre a cultura." [Eric Hughes, 1994-08-31]
6.7.3. Crypto anarquia significa prosperidade para aqueles que podem agarrá-lo,
aqueles competente o suficiente para ter algo de valor para oferecer
para venda; a nora de 95% vai sofrer, mas que é apenas
apenas. Com criptografia anarquia podemos de forma indolor, sem
iniciação de agressão, elimine o improdutivo, o
parar e os coxos. - A caridade é sempre possível, mas eu suspeito
até mesmo o liberal de benfeitores vai jogar as mãos para cima no
perspectiva de uma nação em sua maioria, de trabalhadores não qualificados e,
essencialmente,
analfabetos e innumerate trabalhadores, sendo incapaz de obter
meaninful, bem remunerados empregos.)
6.7.4. Criptografia torna-se mais importante como a comunicação aumenta e, como
a computação é distribuída
+ com pedaços de um ambiente espalhados ao redor
- tem de se preocupar com segurança
- os outros também têm que proteger seus próprios produtos, e ainda
ainda oferecer/vender acesso
- espaços privados necessários em diferentes
locais de [...] multinacionais, teleconferência, vídeo

6.8. Crypo Necessários para o Funcionamento de Sistemas e Redes
6.8.1. Restrições de criptografia--difíceis, pois eles podem ser para
impor--pode, igualmente, impor severas dificuldades no funcionamento seguro
a concepção do sistema, Norma Hardy tem feito este ponto várias vezes.
- Agentes e objetos dentro de sistemas de computador, provavelmente vai precisar de
segurança, credenciais, com robustez, e até mesmo dinheiro digital
para as transações.
6.8.2. Provas de identidade, senhas e o uso do sistema operacional
- ZKIPS especialmente em redes, onde as chances de ver um
palavra-passe de serem transmitidas são muito maiores (uma óbvia
ponto que não é muito discutido)
+ sistemas operacionais e bancos de dados precisam de mais seguro
os procedimentos para acesso, para agentes e gostaria de pagar para
de serviços, etc.

- unforgeable tokens
6.8.3. Muitas vezes um não-mencionado razão de criptografia é necessário para que
a criação da iniciativa privada, ou virtual, redes
- por isso que os canais são independentes da "transportadora comum"
+ para tornar isso claro: perspectivas são perigosamente alto para um
consolidação sob controle do governo de redes
- em paralelo com estradas
+ e como estradas, insistem em equivalente de licenças
- é-uma-pessoa
- proibição de criptografia
- O Cenário de Pesadelo: "Nós próprias redes, nós não
de deixar qualquer um de instalar novas redes sem a nossa aprovação, e
vamos fazer as leis sobre o que é realizado, o que
a criptografia pode ser utilizada, e como os impostos serão recolhidos."
- Felizmente, eu duvido que esse é válida...muitas maneiras
para criar redes virtuais...satélites como o Iridium,
de fibra óptica, formas de ocultar de criptografia ou enterrá-lo em outros
tráfego
+ ciberespaço paredes...
+ mais do que apenas crypto: a segurança física é necessário (e
pela mesma razão não digital "moeda" existe)
- processos de execução controlados-accesss máquinas (como
com remetentes)
- acesso por criptografia
+ uma web do mutuamente suspeitos, máquinas pode ser suficiente
- robusto cyberspaces construído com DC-Net ("jantar
criptógrafos") os métodos?

6.9. Sinistro Tendências
6.9.1. Um número cada vez maior de leis, complexidades dos códigos de imposto,
etc.
- as pessoas não podem navegar
6.9.2. Cartões de IDENTIFICAÇÃO nacional
- autorizações de trabalho, problemas de imigração, o bem-estar de fraude, parando
terroristas, cobrança de impostos
- USPS e outras propostas
6.9.3. Key Escrow
6.9.4. Extensão da lei dos EUA em todo o mundo
- Agora que os EUA tem vencido a URSS, a um campo livre
frente para a difusão da Nova Ordem Mundial, led de
curso pela U. S. A. e seus políticos.
- os tratados, acordos internacionais
- a hegemonia económica

- U. N. mandatos, forças, "capacetes azuis"
6.9.5. AA BBS caso, significa que o ciberespaço não é o que era

6.10. Pontas Soltas
6.10.1. "Por que você não a maioria das pessoas prestam mais atenção à segurança questões?"
- Verdade é, a maioria das pessoas nunca pensa sobre a real segurança.
- Seguro fabricantes disse que as melhorias nos cofres
de metal (o tipo) foram acionados por taxas de seguros. Direto
incentivo para gastar mais
dinheiro para melhorar a segurança (custo do seguro < custo de
maior taxa de seguro).
- Agora não há quase nenhum incentivo econômico para as pessoas
preocupar-se
sobre o PINO de segurança, sobre a proteção de seus arquivos, etc.
(Bancos de comer o
custos e passá-los...qualquer banco, o qual tentou salvar algumas
dinheiro na
perdas exigindo de 10 dígitos Pinos--que as pessoas gostariam de
escrever
de qualquer maneira!--iria perder clientes. Hologramas e imagens em
cartões bancários
estão acontecendo porque os custos caíram o suficiente.)
- Crypto é economia. As pessoas vão começar a realmente se importa quando
custa-los.

6.10.2. O que motiva uma atacantes não é o valor intrínseco do
de dados, mas sua percepção de valor dos dados.
6.10.3. Criptografia permite que mais de refinamento de permissões de acesso a...
grupos, listas de
- além de tal bruta de métodos como a proibição de nomes de domínio ou "edu"
tipos de contas
6.10.4. estas razões gerais vai fazer de encriptação mais comum, mais
socialmente e legalmente aceitável, e, portanto, fazer eventuais
as tentativas para limitar o uso de criptografia anarquia métodos simulado
6.10.5. proteger os hábitos de leitura..
- (Imagine-se utilizando o seu MicroSoftCashCard para biblioteca
checkouts...)
6.10.6. Pontos negativos
- perda de confiança
- mercados em coisas desagradáveis
- espionagem
+ esperar para ver novos tipos de con empregos

- jogos de confiança
- "Fazer Dinheiro Digital Rápida"

6.10.7. A criptografia de Sinais de Vídeo e de Criptografia para Controlar a Pirataria
- este é, naturalmente, toda uma tecnologia e indústria
- Videocypher II tem sido rachado por muitos de vídeo hackers
- toda uma indústria de casa de campo em fissuras, tais cifras fracas
- observe que a proibição de criptografia iria abrir muitas
indústrias para a destruição pela pirataria, que é ainda uma outra
razão por grosso de proibição de criptografia está fadado ao fracasso

7. PGP -- Pretty Good Privacy

7.1. direitos autorais

7.2. RESUMO: PGP -- Pretty Good Privacy
7.2.1. Pontos Principais
- PGP é a mais importante ferramenta de criptografia não é, tendo
sozinho propagação de chave pública métodos em todo o mundo
- muitas outras ferramentas estão sendo construídas em cima dele
7.2.2. Ligações para Outras Secções
- ironicamente, quase nenhuma compreensão de como o PGP obras em
o detalhe é necessária; há uma abundância de especialistas que
especializar-se no que
7.2.3. Onde Encontrar Informações Adicionais
- levar a grupos de notícias atualizado comentários; basta lê-los para um
algumas semanas e muitas coisas vão fluir
- diversas perguntas frequentes sobre o PGP
+ mesmo um livro inteiro, por Simpson Garfinkel:
- PGP: Pretty Good Privacy
por Simson Garfinkel
1ª Edição, novembro de 1994 (est.)
250 páginas (est),ISBN: 1-56592-098-8, $17.95 (est)
7.2.4. Diversos Comentários
- um grande número de sites ftp, URLs, etc., e essas mudanças
- este documento não pode ficar atualizado sobre estes--veja o
ponteiros em grupos de notícias para o mais atual sites

7.3. Introdução

7.3.1. Por que o PGP taxa de seção própria?
- Como Clipper, PGP é muito grande, um conjunto de questões não ter
sua própria seção
7.3.2. "Qual é o fascínio em Cypherpunks com PGP?"
- Ironicamente, o nosso primeiro encontro, em setembro de 1992, coincidiu
dentro de alguns dias do lançamento do PGP 2.0. Arthur Abraão
desde disquetes de 2.0, completo com laser-impresso
rótulos. A versão 2.0 foi o primeiro verdadeiramente úteis versão
PGP (então eu ouço....Eu nunca tentei a Versão 1.0, que tinha
com distribuição limitada). Então, PGP e Cypherpunks compartilhado um
a história--e Phil Zimmermann, foi de algum física
reuniões.
- Prático, útil, compreensível ferramenta. Bastante fácil para
o uso. Em contraste, muitos outros desenvolvimentos são mais abstratos
e não se prestam a uma utilização por amadores e
amadores. Isso só garante PGP um lugar destacado (e
pode ser uma lição objetiva para os desenvolvedores de outras ferramentas).
7.3.3. Pontos de foco no PGP, mas pode aplicar, bem como para
semelhante programas de criptografia, como o comercial da RSA pacotes
(integrada em e-mails, programas comerciais, etc.).

7.4. O que é o PGP?
7.4.1. "O que é o PGP?"
7.4.2. "Por que foi PGP desenvolvido?"
7.4.3. Quem desenvolveu o PGP?

7.5. Importância do PGP
7.5.1. PGP 2.0 chegou em um momento importante
- em setembro de 1992, a mesma semana em que os Cypherpunks tinha
a sua primeira reunião, em Oakland, CA. (Arthur Abraão
impresso até com aparência profissional disquete de etiquetas para o PGO
2.0 disquetes distribuído. Um sentimento geral de que estávamos
formando a "hora certa".)
- apenas 6 meses antes do Clipper anúncio causou um
tempestade de interesse em criptografia de chave pública
7.5.2. O PGP tem sido o catalisador para mudanças importantes na opinião
- formou dezenas de milhares de usuários na natureza do
forte de criptografia
- levou a outras ferramentas, incluindo criptografada remetentes,
experimentos em dinheiro digital, etc.
7.5.3. "Se este material é tão importante, como é que nem todo mundo é
assinar digitalmente suas mensagens?"
- (Eu, por exemplo. Eu nunca assinar as minhas mensagens, e este FAQ é

não assinado. Talvez, mais tarde.)
- conveniência, facilidade de uso, "todos os criptografia é economia"
- insegurança do host máquinas Unix (ilusória)
- melhor integração com e-mails necessários
7.5.4. Ripem parece ser morto; o tráfego em alt.segurança.ripem é
quase zero. O PGP tem, obviamente, ganhou os corações e mentes de
a comunidade de usuários; e agora que é "legal"...

7.6. PGP Versões
7.6.1. PGP Versões e Implementações
- 2.6 interface do usuário é a versão compatível com o 2.3
+ Qual é a diferença entre as versões 2.6 e 2.6 interface do usuário?
- "PGP 2.6 é distribuído a partir do MIT e está legalmente disponível
para NÓS e residentes no Canadá. Ele usa a RSAREF biblioteca.
Ele possui um código que irá impedir a interoperação com o anterior
versões do PGP.
"PGP 2.6 interface do usuário é uma versão modificada do PGP 2.3 um que
funções de modo quase idêntico ao MIT PGP 2.6, sem o
"aleijado" código do MIT PGP 2.6. Ele está legalmente disponível
fora os EUA e o Canadá apenas." [Rat
<ratinox@ccs.neu.edu> alt.segurança.pgp, 1994-07-03]
+ DOS
- Versões
+ Muito Bom Shell
- "Quando o Microsoft Mail suporta um Editor externo,
você pode querer tentar PGS (Muito Bom Shell),
disponível como PGS099B.ZIP em vários sites de ftp. Ele
permite a execução de PGP a partir de um shell, com uma maneira fácil de
editar/criptografar arquivos." [HHM LIMPENS, 1994-07-01]
- Windows
+ Sol
- "Eu acho que você deve ser capaz de usar PGPsendmail,
disponível em ftp.atnf.csiro.au:/pub/people/rgooch'
[eric@terra.hacktic.nl (Eric Veldhuyzen), suporte para PGP
Sun Mailtool?, alt.segurança.pgp, 1994-06-29]
+ Mark Grant <mark@unicorn.com> vem trabalhando em uma ferramenta
para substituir Sun mailtool. "Privtool ("Ferramenta de Privacidade") é
pretende ser um PGP-ciente de substituição para o padrão
Estação de trabalho Sun mailtool programa, com um semelhante usuário
interface e automagick suporte para PGP-assinatura e PGP-
criptografia." [MG, 1994-07-03]
- "No momento, a versão Beta está disponível a partir da
ftp.c2.org em /pub/privtool como privtool-0.80.alcatrão.Z, e

Anexei o arquivo LEIAME.1º arquivo para que você pode verificar
fora os recursos e bugs antes de você baixá-lo. ....
Atualmente, o programa requer o Xview kit de ferramentas para
construir, e só foi compilado no SunOS 4.1 e
Solaris 2.1."
+ MacPGP
- 2.6-interface: relatórios de problemas, bombas (remover Preferencs conjunto
por versões anteriores da pasta de Sistema)
- "MacPGP 2.6 interface é totalmente compatível com o MIT MacPGP 2.6,
mas oferece várias vantagens, um chefe, um ser que
MacPGP 2.6 interface do usuário é controlável através de AppleScript. Este é um
recurso muito poderoso, e pré-escrita AppleScripts são
já disponível. Um conjunto de AppleScripts chamado
Provisório Macintosh PGP Interface (IMPI) apoio
criptografia, descriptografia e assinatura de arquivos via arrastar-n-
drop, localizador de seleção, a área de transferência, todos acessíveis
a partir de um amplo sistema de menu. Eudora AppleScripts também existe
a interface MacPGP com o programa de correio Eudora.

"MacPGP 2.6 interface do usuário v1.2 está disponível via ftp anônimo a partir de:

DIRETÓRIO DE SITES DE FTP
CONTEÚDO
-------- ---------
----
ftp.darmstadt.gmd.de pub/crypto/macintosh/MacPGP
MacPGP 2.6 interface do usuário, origem

AppleScripts para 2.6 interface do usuário estão disponíveis para os estados unidos e
Cidadãos canadenses SÓ
através de ftp anónimo a partir de:

DIRETÓRIO DE SITES DE FTP
CONTEÚDO
-------- ---------
----
ftp.csn.net mpj
IMPI & Eudora scripts

MacPGP 2.6 interface do usuário, origem
[phinely@uhunix.uhcc.Hawaii.Edu (Pedro Hinely),
alt.segurança.pgp, 1994-06-28]

- Amiga
+ VMS
- 2.6 interface do usuário é dito para compilar e executar sob VMS.
+ Versão em alemão
- MaaPGP0,1T1,1
- dtp8//dtp,dapmqtadt,gmd,de janeiro/ilaomilg/MaaP
- Ahpiqtoph_Pagalies@hh2.maus.
- (fonte: andreas.elbert@gmd.de (A. Elbert). por meio de
qwerty@netcom.com (-=Xénon=-), 3-31-94
7.6.2. Quais versões do PGP existe?
- PGP 2.7 é ViaCrypt da versão comercial da PGP 2.6
7.6.3. PGP 2.6 problemas
- Tem havido muita confusão, na imprensa e na
grupos de discussão, sobre as questões que envolvem a 2.5, 2.6,
2.6 interface do usuário, e várias versões destes. Motivações,
conspirações, etc., todos foram discutidas. Eu não estou
envolvidos como outros na nossa lista estão, por isso estou sempre confuso
muito.
+ Aqui estão alguns comentários de Phil Zimmermann, em resposta a um
enganosa relatório de imprensa:
- "PGP 2.6 sempre será capaz de ler as mensagens,
assinaturas, e as chaves de olderversions, mesmo depois de
1º de setembro. As versões mais antigas não será capaz de
ler mensagens, assinaturas e chaves produzidas pelo PGP 2.6
depois do dia 1º de setembro. Este é um modo totalmente diferente
situação. Não há qualquer motivo para as pessoas a mudar para
PGP 2.6, porque ele vai ser capaz de lidar com dados
formatos, enquanto as versões mais antigas não. Até
De setembro, o novo PGP irá continuar a produzir o antigo
formato que pode ser lido por versões mais antigas, mas vai começar
produzindo o novo formato após essa data. Este atraso
permite tempo para todos para obter a nova versão do
PGP, de modo que eles não vão ser afetados pela alteração.
Chave de servidores ainda será capaz de levar as chaves feito em
o formato antigo, porque PGP 2.6 vontade ainda de lê-los com
sem problemas. "[Phil Zimmermann, 1994-07-07, e também publicado
grupos de Usenet] [todas as datas aqui referem-se a 1994]
- "Eu desenvolvidos PGP 2.6 a ser lançado pelo MIT, e eu acho que
esta nova
acordo é um avanço no status legal de PGP,
do benefício
todos os usuários PGP. Peço a todos os usuários PGP para mudar para o PGP
2.6, e abandonar

versões anteriores. A ampla substituição dos antigos
versões com
esta nova versão do PGP se encaixa com planos para o futuro
criação de um
PGP padrão." [Phil Zimmermann, 1994-07-07, e também publicado
grupos de Usenet]
7.6.4. PGP versão 2.6.1
- "MIT lançará PGP (Pretty Good Privacy) versão
2.6.1 real logo agora. Até amanhã, eu acho. O MS-dos
lançamento de nome de arquivo será pgp261.zip e o código-fonte
vai ser no pgp261s.zip. O MIT site FTP é líquida-
dist@mit.edu no pub/PGP directory." [corrigido pela
Derek Atkins ser: net-dist.mit.edu, não é líquida-
dist@mit.edu.]

"Esta nova versão tem um monte de correções de bugs sobre a versão 2.6.
Espero que essa é a versão final desta família de PGP
código-fonte. Estamos trabalhando em uma nova versão
de PGP, reescrito do zero, o que é muito mais limpo e
mais rápido e mais adequado para o futuro aprimoramentos de nós
ter planejado. Todos os PGP esforços de desenvolvimento será
redirecionado para a nova base de código, depois de este 2.6.1
lançamento." [Phil Zimmermann, Cypherpunks lista, 1994-09-02]

7.7. Onde Obter PGP?
7.7.1. "Onde posso obter PGP no CompuServe?"
- Nota: o eu não pode manter o controle dos principais sites de ftp para o
vários pacotes de criptografia, muito menos informações sobre serviços, como
isso. Mas, aqui está ele;
- "O atual de 5-Jul-1994:"
IR EURFORUM / Utilitários PGP26UI.ZIP PGP 2.6 interface do usuário
IR PWOFORUM / uploads de Novo PGP26.ZIP PGP 2.6
PWOFORUM também tem o código fonte e documentação, além de
um número de utilitários de shell para PGP. Versão 2.3 é também
ainda redor." [cannon@panix.com, Kevin Martin, o PGP no
Compuserve??, alt.segurança.pgp, 1994-07-08]
7.7.2. Fora de linha PGP
+ ftp.informatik.uni-
oportunidades de hotéis de hamburgo.de:/pub/virus/crypt/pgp/tools/pgp-elm.zip
- outro lugar: Crosspoint: ftp.uni-
kl.de:/pub3/pc/dos/terminal/xpoint XP302*.EXE
+ "Eu recomendo Offline AutoPGP v2.10. Ele funciona
de forma integrada com praticamente qualquer leitor de e-mail off-line que

suporta .Pacotes QWK. Shareware de inscrição é de r $10.00
NÓS. O autor é Staale Schumacher, um estudante da
Universidade de Oslo, está acessível no staale@ifi.uio.no .
O programa deve ser muito amplamente disponíveis NOS bbs do
por agora. Eu uso o programa constantemente para bbs e-mail. É
realmente uma mancha de peça de trabalho. Se você tiver alguma
problemas para encontrá-lo, mande-me uma observação."
[bhowatt@eis.calstate.edu Brent H. Howatt, PGP em um
leitor off-line?, alt.segurança.pgp, 1994-07-05]
- oak.oakland.edu em /pub/msdos/off-line, versão 2.11
- ftp.informatik.uni-
oportunidades de hotéis de hamburgo.de:/pub/virus/crypt/pgp/tools/apgp211.zip
7.7.3. "Devo me preocupar sobre como obter e compilar o PGP
fontes?"
- Bem, a menos que você é um especialista sobre o funcionamento do PGP, por
que se preocupar? E uma sutil bug no gerador de números aleatórios
iludido mesmo Colin Prumo por um tempo.
- O valor de a fonte estar disponível é de que os outros podem,
se o desejarem, fazer a confirmação de que o executável
correspondem à fonte. Que este _can_ ser feito é suficiente
para mim. (Estratégia: Manter o código por um tempo, esperar
para os relatórios de falhas ou buracos, em seguida, usar com confiança.)
- As assinaturas podem ser verificados. Talvez carimbo de data / hora versões,
um dia.
- Francamente, as chances são muito maiores que as mensagens ou
pseudônimo de identidade será exposto em outras formas de
que o PGP foi comprometida. Slip-ups no envio de mensagens
por vezes, revelar identidades, como fazer inadvertida e comentários
estilística dicas.

7.8. Como Usar PGP
7.8.1. Como PGP trabalho?
7.8.2. "Como devo armazenar o segredo parte da minha chave? Posso memorizar
ele?"
- As cifras modernas, use as teclas que estão muito além da memorização
(ou mesmo digitando!). A chave é normalmente armazenado em um
casa de máquina, ou uma máquina que é razoavelmente seguro, ou no
disquete. A senha deve sempre ser memorizado ou
escritos (ugh), em uma carteira ou em outro lugar.
Seguro de "dongles" usado ao redor do pescoço, ou um anel ou assistir,
eventualmente, pode ser utilizado. Cartões inteligentes e os PDAs são de mais
provável solução intermediária (muitos PCs têm agora de placa PCMCIA
slots).

7.8.3. "Como faço para assinar as mensagens?"
- cf. o PGP docs
+ no entanto, este surgiu na Lista, e:
-
+ pgp -sta +clearsig=no message.txt
-
- Que a partir de pgpdoc2.txt. Espero que ajude. Você pode
pretende configurar seu email
- agente de utilizador para chamar esta de comando após a saída de seu
editor de mensagem padrão,
- com "message.txt" conjunto de tudo o seu editor de chamadas
a mensagem temporária
- arquivo. <Russell Whitaker,
whitaker@sgi.com, 4-15-94, Cypherpunks>
7.8.4. Por que não PGP mais fácil de usar?
- Em relação a outras possíveis aplicações de criptografia (como
dinheiro digital ou sistemas de votação), é, na verdade, _very_
fácil de usar
- semantic gap de aprendizagem...
7.8.5. Como eu deveria aprender PGP?
7.8.6. "Qual é o status da PGP a integração com outros programas?"
+ Editores
+ emacs
+ emacs suporta pgp, provavelmente, em vários sabores (eu
vi vários relatos de diferentes pacotes)..o built-
na linguagem certamente ajuda
- Rick Busdiecker <rfb@lehman.com> tem um emacs frente
final para PGP disponível
- Jin S. Choi <jsc@monolith.MIT.EDU> uma vez descrito um
pacote escreveu no diretī orio elisp que apoiou o GNU emacs:
"mailcrypt"
- há provavelmente muito mais
+ Mensagens
- Que é, há e-mails que tem uma boa ligação
PGP? Ganchos existentes correspondências são necessárias
+ emacs
+ emacs suporta pgp, provavelmente, em vários sabores (eu
vi vários relatos de diferentes pacotes)..o built-
na linguagem certamente ajuda
- Rick Busdiecker <rfb@lehman.com> tem um emacs frente
final para PGP disponível
- Jin S. Choi <jsc@monolith.MIT.EDU> uma vez descrito um
pacote escreveu no diretī orio elisp que apoiou o GNU emacs:

"mailcrypt"
- há provavelmente muito mais
- elm
- Eudora
+ PGP sendmail, etc.
- "Obter o PGPsendmail Suite, anunciou daqui alguns dias
atrás. Ele está disponível por ftp anônimo a partir de:
ftp.atnf.csiro.au: pub/people/rgooch (Austrália)
ftp.dhp.com: pub/crypto/pgp/PGPsendmail(U. S. A.)
ftp.boi.ac.reino unido: src/segurança (reino UNIDO)... Ele funciona através da
embrulho em torno de regular o sendmail programa, de modo
você começa a criptografia automática para todos os utentes, não só
Rmail. "[Richard Gooch, alt.segurança.pgp, 1994-07-10]
+ MIME
- MIME e PGP <Derek Atkins, 4-6-94>
- [o material a seguir, extraído de um anúncio
encaminhado para o Cypherpunks lista
remijn@athena.research.ptt.nl, 1994-07-05]
- "MIME [RFC 1341, RFC 1521] define um formato e
quadro geral para a representação de uma ampla
variedade de tipos de dados de email na Internet. Este documento
define um tipo de MIME dos dados, o
application/pgp tipo, para "muito bom" privacidade
a autenticação e a criptografia de email na Internet. O
application/pgp tipo de MIME destina-se a facilitar o
maior interoperação de mensagens privadas através de uma ampla
variedade de hardware e plataformas de software.
+ Leitores de notícias
- útil para automático assinatura/verificação, e endereço de e-mail
de dentro leitor de notícias
- fio
- estanho
- O "fio" leitor de notícias alegadamente tem PGP embutido.
7.8.7. "Com que frequência devo trocar a minha chave ou chaves?"
- Hal Finney aponta que muitas pessoas parecem pensar PGP
as teclas são quase-permanente. Na verdade, nunca mudando uma chave
é um convite ao desastre, como as chaves podem ser comprometidos em
várias formas (pressionamento de tecla de captura programas, disquetes, esquerda
em torno de mentir, mesmo rf monitoramento) e pode ser concebivelmente
rachado.
- "
+ "O que é um bom intervalo para os principais alterações? Gostaria de sugerir
a cada ano ou assim

- faz sentido, especialmente se a infra-estrutura pode ser
desenvolvido para tornar mais fácil
- para propagar alterações de chave. As chaves deverão ser sobrepostas em
tempo, para que você faça
- uma nova chave e começar a usá-lo, continuando a apoiar
a chave antiga para uma
- tempo. <Hal Finney, hfinney@shell.portal.com, 4-15-94,
cypherpunks>
- Hal também recomenda que o reenvio de e-mails de sites de alterar as suas chaves
ainda mais freqüentemente, talvez mensalmente.

7.9. Chaves, Chave de Contratações, e Servidores de Chaves
7.9.1. Web of trust vs. heierarchical de gerenciamento de chave
Uma das principais inovações do Phil Zimmermann foi o uso de um "web
de confiança" modelo distribuído de confiança em chaves.
- localidade, os usuários arcar com os custos
- em contrapartida, o governo estima que us $1-2 B de um ano para executar chave
certificação de agências de uma grande fração do
população
- "PGP é uma questão de escolha e a construção de uma rede de confiança que
se ajustar as sua necessidades. PGP suporta completamente descentralizada,
web personalizadas de confiança e também o mais altamente
estruturado burocrático centralizado esquema que você poderia
imaginar. Um problema com que se baseia exclusivamente em um personalizado
web of trust é que ele limitsyour universo de
correspondentes. Nós não podemos esperar que Phil Zimmermann e alguns
bem-conhecido de outros, para assinar todos da chave, e eu não
deseja limitar minha correspondência privada apenas para os
gente que eu conheço e confiar mais aquelas pessoas cujas chaves
foi assinado por alguém que conhece e confia." [William
Stallings, TRENÓ verificação da chave, alt.segurança.pgp, 1994-09-
01]
7.9.2. Abordagens práticas para a assinatura de chaves de outros
o sinal + teclas de pessoas que você conhece e deseja comunicar-se com
- face-a-face encontros ("Aqui está a minha chave.")
+ confiança-em graus variados,--as chaves assinados por outras pessoas que você
sei
- web-of-trust
- confiança-em menor medida--as teclas de pessoas-chave
registros
7.9.3. Servidores De Chaves
+ Existem vários grandes sites que parecem ser estáveis
+ MIT PGP Chave Pública do Servidor

- via www.eff.org
+ Vesselin Bontchev na Universidade de Hamburgo, opera uma
muito estável:
- Ftp: ftp.informatik.uni-hamburg.de
IP: 134.100.4.42
Dir: /pub/vírus/crypt/pgp/
Arquivo: pubkring.pgp
E-Mail: pgp-public-keys@fbihh.informatik.uni-hamburg.de
- pgpkeys.io.com
+ http://martigny.ai.mit.edu/~bal/pks-commands.html
- Este é um servidor de chaves PGP em Zurique. <Russell Whitaker, 7
De abril de 1994>
-
7.9.4. Uso da chave PGP de impressões digitais
- "Um dos melhores usos para chave de impressões digitais é para
inclusão em arquivos de assinatura e de outros lugares que uma chave
si é muito volumoso. Por divulgação generalizada da
de impressão digital, as chances de um falso chave a ser detectado
são diminuídos, uma vez que existem mais canais para a
impressões digitais para chegar aos destinatários, e mais canais para a
proprietário de uma chave para ver qualquer falsas impressões digitais out no
líquida. [Bill Stewart, 1994-08-31]
7.9.5. "Como as alterações de endereço de ser tratados? Fazer de idade chaves
ser revogado?"
- Futuras versões do PGP pode lidar melhor
- É uma maneira de problema .... "Id de usuário de revogação de certificados
são uma *boa* idéia e a chave PGP formato permite-lhes -
talvez um dia PGP vai fazer algo sobre isso." [Paul Allen,
alt.segurança.pgp, 1994-07-01]
- Persistente e-mail é uma abordagem. Algumas pessoas
estão usando organização como o ACM para fornecer este (por exemplo,
Phil Zimmermann é prz@acm.org). Outras pessoas estão usando o remapeamento
serviços. Por exemplo, "eu me inscrevi com o TRENÓ (Estável
Grandes E-mail do Banco de dados), que é uma referência cruzada
banco de dados para vinculação antigo, obsoleto E-mail com
os atuais sobre o curso do tempo.... Qualquer pessoa que usar este
chave sempre será capaz de me encontrar no TRENÓ por
a realização de uma pesquisa com "blbrooks..." como a palavra-chave. Assim,
a minha chave e associados sigs sempre bom.... Se você
está interessado em TRENÓ, seu endereço é
trenó@drebes.com." [Robert Brooks, alt.segurança.pgp, 1994-07-
01]
7.9.6. "Como posso ter certeza de que as minhas chaves não foram violados?"

+ Mantenha sua chave privada em segurança
+ se sobre uma não segura, máquina de tomar medidas para protegê-la
- offlline de armazenamento (Perry Metzger carrega a sua chave(s) de cada
de manhã, e remove-lo quando ele deixa a máquina)
+ memorizar o seu PGP senha e não escrevê-la, no
pelo menos não em qualquer lugar, perto de onde a chave privada é
disponível
- envelopes lacrados com um advogado, cofre,
etc., são possibilidades
- dada a quase impossibilidade de recuperar o arquivos
se a senha for perdida permanentemente, eu recomendo
armazená-lo _someplace_, apesar da ligeira perda na
de segurança (este é um tópico de debate...eu, pessoalmente, sinto
muito mais confortável sabendo que minha memória é feito
em algum lugar)
- Colin Prumo observou que, se alguém tem acesso à sua
pessoal chaveiro, eles também, provavelmente, ter acesso ao seu
Programa PGP e poderia fazer modificações *diretamente*.
- Derek Atkins respondeu a uma pergunta semelhante no sci.cripta:
"Com certeza. Você pode usar o PGP para verificar o seu chaveiro, e usando
o web-of-trust, em seguida, você pode ter que verificar a sua
assinaturas de todas as chaves que você assinou, e recurse
através de seu círculo de amigos. Para verificar se a sua própria
a chave não foi munged, você pode assinar algo com o seu segredo
chave e, em seguida, tente verificá-los. Isso irá garantir que o seu
chave pública não era munged." [Derek Atkins, sci.cripta, 1994-
07-06]
7.9.7. "Por que são chave revogações é necessário?"
- Chave de revogação é a "vazante-de-confiança"
- "Há um número de razões. Talvez você tenha sido coagido
para assinar a chave, ou você acha que talvez a chave foi
assinado incorretamente, ou talvez a pessoa não usa mais
o e-mail, porque eles perderam a conta, ou que
talvez você não acredite que a ligação de chave para userID
é válido para qualquer número de razões." [Derek Atkins, 4-28-
94]
7.9.8. "É-uma-pessoa" registros
+ Tem havido propostas que os governos podem e devem
criar registros de "pessoas colectivas." Isto é conhecido no
crypto comunidade como "é-uma-pessoa" credentialling, e
diversos trabalhos (nomeadamente Fiat-Shamir) têm lidado com problemas
- da falsificação maliciosos governos
- os perigos da pessoa de acompanhamento de

+ Precisamos ter muito cuidado aqui!
- isso pode limitar a propagação de 'ad hoc de criptografia' (por que
Eu quero dizer o uso da localmente-chaves geradas por razões
diferente de uso pessoal...dinheiro digital, pseudônimos, etc.)
- qualquer sistema que "problemas" bilhetes de permissão para permitir que as chaves
para ser gerada é perigoso!
+ Poderia ser uma área que os governos querem entrar.
- a la Fiat-Shamir "passaporte" (questões de Murdoch, da Líbia
exemplo)
- Sou a favor de mercados livres--não há limitações sobre o que eu registros
pode usar
7.9.9. Os servidores de chaves (esta lista está em constante mutação, mas a maioria de
compartilhamento
chaves, então tudo o que precisa é de um). Enviar "ajuda" da mensagem. Para
informações atuais, siga alt.segurança.pgp.
- cerca de 6000 chaves sobre os principais servidores de chaves, como de 1994-08.
- pgp-public-keys@martigny.ai.mit.edu
- pgp-public-keys@dsi.unimi.it
- pgp-public-keys@kub.nl
- pgp-public-keys@sw.oz.au
- pgp-public-keys@kiae.su
- pgp-public-keys@fbihh.informatick.uni-hamburg.de
- e wasabi.io.com dispõe de chaves públicas pelo dedo (eu não poderia
fazê-lo funcionar)
7.9.10. "Quais são os principais impressões digitais e por que eles são usados?"
- "Distribuindo a chave de impressões digitais permite J. Random Humanos para
a correlação de uma chave fornecida através de um método com que forneceu
através de outro. Por exemplo, agora que eu tenho a impressão digital
para o Betsi chave, eu posso verificar se a qualquer outra alegada
Betsi chave que eu vejo é real ou não.....É muito mais fácil para
leitura & cruz-seleção de 32 caracteres impressões digitais que o
todo o bloco de chave, especialmente como as assinaturas são adicionados e
o bloco de chave cresce em tamanho." [Paulo Robichaux, 1994-08-29]
7.9.11. Betsi
- Bellcore
- chave de assinatura
7.9.12. sobre ataques a servidores de chaves...
+ inundações ataques a servidores de chaves começaram; isso pode
é uma tentativa de ter os servidores de chaves encerrar utilizando
obsceno, racista, sexista frases como nomes de chave (Cypherpunks
não iria apoiar a encerrar um site para algo tão
trivial como abusivo, linguagem ofensiva, mas muitos outros
faria).

- "Parece que alguns infantil, idiota teve um grande momento
a geração de falsos chaves PGP e fazer o upload deles para o
os servidores de chaves públicas. Aqui estão algumas das teclas eu encontrei em um
keyserver:...[chaves omitido]..." [staalesc@ifi.uio.no,
alt.segurança.pgp, 1994-09-05]

7.10. PGP Front-Ends, Conchas, e Ferramentas
7.10.1. Muitos podem ser encontradas no site ftp:
+ ftp.informatik.uni-hamburg.de:/pub/virus/crypt/pgp/shells/
por diversas conchas e front-ends para PGP
7.10.2. William Stallings tinha isto a dizer em um Usenet post:
- "PGPShell: é executado diretamente sobre a versão DOS, não precisa
O Windows. Bom, interface simples. freeware

"PGP Winfront: freeware windows front-end. Usa um "controle
painel" do estilo, com muitas opções exibidas em um compacto
a moda.

"WinPGP: shareware ($45). Usa um menu suspenso estilo,
comum para muitas aplicações do Windows." [William Stallings,
Procurando por PGP front-end, alt.segurança, 1994-08-31]
7.10.3. Rick Busdiecker <rfb@lehman.com> tem um front-end para o emacs
PGP disponível
7.10.4. Pr0duct Cypher ferramentas:
+ ftp.informatik.uni-
oportunidades de hotéis de hamburgo.de:/pub/virus/crypt/pgp/tools/PGPTools.tar.gz
- Pr0duct Cypher ferramentas, e outras ferramentas em geral

7.11. Outros Programas E Ferramentas De Criptografia
7.11.1. Outras Cifras e Ferramentas
- RIPEM
- PEM
- MD5
+ RFE (Secure sistema de arquivos) 1.0
- "SFS (Secure sistema de arquivos) é um conjunto de programas que
criar e gerenciar um número de volumes de disco criptografada, e
é executado em ms-DOS e do Windows. Cada volume é apresentado como
um DOS normal de unidade, mas de todos os dados armazenados nele é encryped
no nível individual-nível de setor....SFS 1.1 é um
versão de manutenção que corrige alguns pequenos problemas no
1.0, e adiciona uma série de funcionalidades sugeridas pelos usuários.
Mais detalhes sobre as alterações são dadas no arquivo leia-me."
[Peter Gutmann, sci.cripta, 1994-08-25]

- não é a mesma coisa como CFS!
- A chave de 512 bits usando um MDC/SHS hash. (Rápido)
- só funciona em a386 ou melhor (diz V. Bontchev)
o código - fonte não está disponível?
- implementado como um driver de dispositivo (ao invés de um TSR, como SecureDrive)
- "é vulnerável a uma forma especial de ataque, o que foi mencionado uma vez aqui no sci.cripta e é descrito em detaills em busca de site catalogado documentação. Dê um saque na a seção "Criptografia" Considerações." [Vesselin Bontchev, sci.cripta, 1994-07-01]
- Comparar os SFS para SecureDrive: "Ambos os pacotes estão aproximadamente iguais em termos de interface de usuário, mas SFS parece ser um pouco mais rápido. E comentários de várias pessoas (mensagem anterior thread) parece indicam que é mais "seguro" bem." [Bill Couture <coutu001@gold.tc.umn.edu> , sci.cripta, 1994-0703]
+ SecureDrive
- criptografa um disco (sempre muito cuidado!)
- SecureDrive 1.3 D, 128-bit IDÉIA de cypher é baseado em um MD5 hash da senha
- implementado como um programa TSR (em vez de um controlador de dispositivo, como CFS)
o código - fonte disponível
+ Alguns problemas relatados (sua milhagem pode variar)
- "Eu tenho tido um pouco de dificuldade com a minha a unidade criptografada desconfiguração de arquivos. Depois de ficar seguro unidade 1.3 d instalado no meu disco rígido, acho que vários arquivos são corrompidos e muitas vezes depois acessando a unidade de um monte de arquivos com referências cruzadas são presente." [Vaccinia@uncvx1.oit.unc.edu, 1994-07-01]
- Outros relatório a ser feliz, em ms-DOS e Windows
- no OS/2 ou versões de Mac relatado; alguns dizem que o OS/2 dispositivo controlador tem de ser usado (como o Empilhador para OS/2 usa)
+ SecureDevice
- "Se você não pode encontrá-lo em outro lugar, eu tenho ele no ftp://ftp.ee.und.ac.za/pub/crypto/secdev13.arj, mas que no final de um saturada link de 64 kbps." [Alan Barrett, 1994-07-01]

7.11.2. MDC e SHS (mesmo como SHA?)

- "O MDC cifras fracas são acreditados para ser tão forte como ele é

difícil inverter a função de hash criptográfica eles
está a utilizar. SHS foi projetado pela ANS, e acredita-se
ser seguro. Pode haver outras maneiras de atacar o MDC
cifras fracas, mas ninguém está autorizado a falar e sabe como
métodos." [Vesselin Bontchev, sci.cripta, 1994-07-01]
+ Secure Hash Standard do algoritmo é público, e, portanto, pode
ser analisados e testados para os fracos (em forte contraste
com o Skipjack).
- pode substituir MD5 em futuras versões do PGP (rumor)
Velocidade do MDC: "É a velocidade de troca. MDC é poucas vezes
mais rápido do que a IDEIA, então SFS é algumas vezes mais rápido do que
SecureDrive. Mas MDC está menos provado." [Colin Prumo,
sci.cripta, 1994-07-04]
+ Rumores de problemas com SHA
- "A outra grande novidade é um problema de segurança com o Seguro
Hash Algorithm (SHA), discutido no Abr 94 DDJ. O
criptógrafos a ANS tenha encontrado um problema com o
algoritmo. Não conte a ninguém o que é, ou até mesmo
como é muito grave, mas eles prometem uma correção em breve. Todos
está esperando com ansiedade o fôlego." [Bruce Schneier, reprot
no Eurocrypt '94, 1994-07-01]

7.11.3. Stego programas

+ DOS
- S-Ferramentas (ou Fezes?). DOS? Criptografa em .e gif .wav
(SoundBlaster format) arquivos. Pode definir para não indicar
arquivos criptografados são por dentro.
- Windows
+ Macintosh
- Stego
+ programas de som
- marielsn@Hawaii.Edu (Nathan Mariels) tem escrito uma
programa que "tem um arquivo e encripta-a com a IDÉIA de
utilizando um hash MD5 da senha digitada pelo usuário.
Em seguida, armazena o arquivo no bit mais baixo (ou bits,
selecionável pelo usuário) de um arquivo de som."

7.11.4. "O que será "Muito Boa Voz de Privacidade" ou "Voz PGP" e
Outros Programas De Voz?"

+ Vários grupos, incluindo um liderada por Phil Zimmermann, são
disse estar trabalhando em algo como isso. A maioria está usando
comercialmente - e amplamente disponível entrada de som placas, la
"SoundBlaster" placas.
- hardware proprietário ou DSPs é muitas vezes a perder, pois as pessoas
não ser capaz de facilmente adquirir hardware; software

só solução (possivelmente depender de hardware internos, ou
prontamente disponíveis adicionar-em placas, como SoundBlasters) é
preferível.
+ Muitas razões importantes para fazer um projeto como este:
proliferam mais de criptografia, ferramentas e sistemas
- tirá-lo à frente de "Telefonia Digital II" e Clipper-
tipo de sistemas; fazer a ferramentas tão onipresente que proibisse
eles é muito difícil
- as pessoas a entender a voz communcations de uma forma mais natural
forma de e-mail, para que as pessoas que não usar o PGP pode
no entanto utilizar uma encriptação de voz do sistema
+ Eric Flor tem o seu próprio esforço, e tem demonstrado
hardware em Cypherpunks reuniões:
- "Neste momento, o nosso principal esforços no desenvolvimento de uma
família de extensible protocolos de criptografia e
voz em ligações ponto a ponto. Nós indend usar
as normas existentes sempre que possível.

"Atualmente, estamos planejando a construção no topo das RFCs
para o PPP (consulte as RFCs 1549, 1548, e 1334). A idéia básica
é para adicionar um novo Protocolo de Controle de Vínculo (ou, possivelmente, um
Protocolo de Controle de rede) que vai negociar base e
módulo de elasticidade e realizar a troca de chaves DH. Algumas formas de
Autenticação já são suportados pelo RFCs. Estamos
olhando para os outros." [Eric Flor, 1994-04-14]
+ Edifício em cima de capacidades multimédia dos computadores Macintosh
e o Windows pode ser uma abordagem mais fácil
- quase todos os Macs e Windows máquinas serão
multimédia/audiovisual com capacidade de em breve
- "Eu percebo que é muito possível para a concepção de um seguro
telefone
com um Vocoder, um modem e algumas de energia da cpu para fazer o
criptografia, mas eu acho que uma solução mais simples pode ser
o horizonte. ....Eu acredito que a Microsoft e muitos outros
estão explorando a interceptação telefones para PCs para que as pessoas possam fazer
coisas como navio de imagens do seu fim de semana de diversão para
os amigos. Quando o PC pode acessar facilmente telefone
comunicações, em seguida, desenvolver encriptado conversas
deve ser tão fácil como programação para o Windows :-)."
[Peter Wayner, 1993--07-08]
7.11.5. Geradores De Números Aleatórios
- Uma grande área de...
+ Sistemas caóticos, pendula

- pode ser inesperado periodicidades (espaço de fase mapas mostram
bacias de atração, apesar de comportamento é aparentemente
aleatório)
7.11.6. "Qual é a situação sobre a disputa entre NIST e RSADSI
sobre os DSS?"
- NIST afirma que não viola as patentes
- RSADSI comprou o Schnorr de patentes e pedidos DSS viola
ele
- NIST não garante, nem indemnizar os utilizadores
[Reginald Braithwaite-Lee, falar.política.crypto, 1994-07-
04]
7.11.7. "Existem programas como o telnet ou "falar" que usar o pgp?"
- "Não sei sobre o Telnet, mas eu gostaria de ver a "conversa"
seguro assim... existe. (PGP-ized ytalk, o que é.)
Ter um olhar para ftp.informatik.uni-
oportunidades de hotéis de hamburgo.de:/pub/virus/crypto/pgp/tools/pgptalk.2.0.tar.gz"
[Vesselin Bontchev, alt.segurança.pgp, 1994-07-4]
7.11.8. Digitais Do Módulo De
+ Existem dois tipos:
- brinquedo ou reproduzir versões
- real ou comercial versão(s)
+ Para uma versão de jogo, envie uma mensagem para
"timestamp@lorax.mv.com" e ele será carimbo de data / hora e
devolvidos. Claramente, este não é prova de muito, não tenha sido
testado no tribunal, e baseia-se unicamente na reputação da
timestamper. (Uma falha fatal: é trivial para redefinir o sistema de
relógios de ponto informatizados e, assim, alterar datas.)
- "boatos", equivalente a: carimbos de data / hora por servidores que estão
não utilizando o "amplamente testemunhado evento" abordagem de
Haber e Stornetta
- A versão de Haber e Stornetta é, naturalmente, muito mais
impressionante, como ele se baseia em algo mais poderoso do que
mera confiança que eles têm de definir o sistema de relógios em seus
computadores corretamente!

7.12. Questões jurídicas com PGP
7.12.1. "O que é o RSA Data Security Inc.'s de posição no PGP?"
I. Eles foram fortemente contrário de versões anteriores
II. objecções
- infringe o PKP patentes (supostas infrações, não
testado em tribunal, embora)
- quebra o rígido controle visto anteriormente
- traz a atenção indesejada a chave pública abordagens (eu

acho que o PGP também ajudou a RSA e RSADSI)
- sangue ruim entre Zimmermann e Bidzos
III. objecções
- infringe o PKP patentes (supostas infrações, não
testado em tribunal, embora)
- quebra o rígido controle visto anteriormente
- traz a atenção indesejada a chave pública abordagens (eu
acho que o PGP também ajudou a RSA e RSADSI)
- sangue ruim entre Zimmermann e Bidzos
IV. Falar de processos, ações, etc.
V. 2.6 MIT hospedagem, pode ter diminuído a tensão;
puramente especulativas
7.12.2. "PGP é legal ou ilegal"?
7.12.3. "Ainda existe um conflito entre RSADSI e PRZ?"
- Aparentemente não. O MIT 2.6 negociações parecem ter
enterrado todos esses rancor. Pelo menos oficialmente. Ouço que há
ainda animosidade, mas ele não está mais na superfície. (E
RSADSI agora está voltado para os processos judiciais e a patente se ajustar.)

7.13. Problemas com o PGP, Falhas, Etc.
7.13.1. Especulações sobre possíveis ataques do PGP
+ Existem periodicamente relatórios de problemas, a maioria apenas
rumores. Estas são golpeou-a para baixo por mais experiente
as pessoas, para a maior parte. Verdadeiro falhas podem existir, é claro,
como em qualquer pedaço de software.
- Colin Prumo reconheceu uma falha em um número aleatório
processo de geração de PGP 2.6, para ser corrigido mais tarde
versões.
+ disseminar o medo, incerteza e dúvida
- os rumores sobre a segurança do PGP versões
- processos seletivos de PGP usuários
- ameaças de morte (la contra Bidzos)
- semear confusão na comunidade de usuários
- fragmentá-la (talvez através de vários noninteroperable
versões...como estamos começando a ver agora?)
7.13.2. O que a ANS saber sobre falhas no PGP?
- Eles não estão dizendo. Ironicamente, isso viola a parte de
a sua carta, que trata de tomada de comercial de segurança
mais forte. Agora que o PGP é kosher, eles devem ajudar a fazer
é mais forte, e certamente não deve manter silêncio sobre
pontos fracos o que eles sabem. Mas para ajudá-los a fortalecer
O PGP não é muito provável.
7.13.3. O PGP timebomb

- Como eu já disse em outro lugar, tudo fica muito confuso. Muitos
versões, muitos sites, muitos pontos de vista, muitas ferramentas, muitos
conchas, muitas outras coisas. Felizmente, a maioria é
flotsam.)
- Eu não tenho ponto de vista-por vários motivos-para evitar
o "timebomb" usando 2.6 interface do usuário. Aqui está alguém
comentário: "eu gostaria de aproveitar este momento para incentivar você
a atualização para o 2.6 interface do usuário que irá superar mit timebomb e
não excluir PGP 2,3 a partir de desencriptação de mensagens.....NÃO USE
MIT 2.6, usar o PGP 2.6 interface do usuário disponíveis a partir de soda.berkeley.edu
: /pub/cypherpunks/pgp" [Matriz, na Cypherpunks, PRETO
THURSAY!, alt.segurança.pgp, 1994-09-01]
+ também pode ser derrotado com o "legal kludge":
- ftp.informatik.uni-hamburg.de :
/pub/virus/crypt/pgp/legal_kludge.txt
7.13.4. Falsificação
- "Adequado as restrições de tempo, e, em especial, em tempo real
restrições, pode ser usado para dificultar, e talvez a derrota,
ataques de spoofing. Mas com uma armazenar e encaminhar mensagens de e-mail
sistema (tais como o PGP é projetado para trabalhar com
restrições não podem, em geral, ser definido." [Ken Pizzini ,
sci.cripta, 1994-07-05]
7.13.5. "Como sabemos que o PGP não ter uma porta ou de algum
outra grande falha? Afinal, nem todos são programadores ou
estudando criptografia."
- Sim, mas muitos de nós. Muitas pessoas têm analisado o
código-fonte no PGP, de ter compilado o código em si (um
forma bastante comum para obter o executável), e de ter examinado
os geradores de números aleatórios, a seleção de primos, e
todos os outros cálculos.
+ Levaria apenas um único aguçada pessoa para explodir o
apito em uma conspiração para inserir falhas ou brechas. Este
não foi feito. (Apesar de Colin Prumo ackknowledged um
ligeira fraqueza no RNG de 2,6...está sendo corrigido.)
- "Apesar de ter o código fonte disponível não garante
que o programa é seguro, isso ajuda muito. Apesar de
muitos usuários não são programadores ou criptógrafos, outros
são, e muitos deles examinar o código cuidadosamente
e publicamente gritar sobre as fraquezas que eles aviso ou
acho que eles aviso prévio. Por exemplo, aparentemente não havia uma
grande discussão aqui sobre o xorbytes() erro no PGP 2.6.
Contraste isso com um programa comercial, onde um tal bug
pode passar despercebida durante anos." [Paulo Rubin,

alt.segurança.pgp, 1994-09-06]

7.13.6. "Posso executar o PGP em uma máquina que eu não controlo, por exemplo, o campus sistema de computador?"

- Com certeza, mas os administradores e outras pessoas podem ter acesso aos a sua chave e senha. Só as máquinas diretamente do usuário controles, e que sejam adequadamente protegida por um firewall de outros máquinas, oferecer quantidades razoáveis de segurança. Argumentando sobre se 1024 bits keylengths são "suficiente" é, ao invés de discutível se o programa PGP está sendo executado em um institucionais computador, ou uma rede de uma universidade. A ilusão de segurança podem estar presentes, mas não há real segurança. Muitas pessoas estão enganam a si mesmas que as suas mensagens são seguras. Que sua eletrônico identidades não podem ser falsificados.
- Eu não estou interessado em vários elm e emacs PGP pacotes (várias delas e wrappers existir). Qualquer sysop não só pode obter sua chave secreta armazenada no hissystem, mas ele também pode capturar sua senha enquanto você alimentá-lo para o programa PGP (supondo que você faz...muitas pessoas automatizar esta parte também). Uma vez que este sysop ou um de seus comparsas, em seguida, pode comprometer seu e-mail, sinal de mensagens e contratos como "você," eu considero isso totalmente inaceitável. Outros, aparentemente, não.
- O que pode ser feito? Muitos de nós só executar o PGP na casa de máquinas, ou em máquinas que controlam diretamente. Algumas pessoas que usam o PGP em tais máquinas, pelo menos, tomar medidas para melhor salvaguardar coisas....Perry Metzger, por exemplo, descreveu certa vez o processo de múltiplos estágios, ele passou por cada dia para recarregar seu chave de material de uma forma que ele sentia era quase seguro.
- Até que a "Internet-in-a-box" ou TIA do tipo de produtos são de mais generalizada, muitas pessoas irão se conectar de casa ou do escritório máquinas para outros sistemas que não controlam. (Para colocar este em foco mais nítido: você deseja que o seu dinheiro eletrônico a ser executar fora de uma conta que seu sysop e seus amigos podem monitor? Não mal. "Porta-moedas electrónico", que pode ser cartões inteligentes, Newton-como PDAs, ou dongle-como anéis ou pingentes, são claramente necessário. Outra discussão inteira.)

7.14. O Futuro do PGP

7.14.1. "Não PGP ajudar ou prejudicar chave pública métodos, em geral, e RSA Data Security Inc. em particular?"

- O resultado não é o final, mas no equilíbrio eu acho que o posição da RSADSI é ajudado pela publicidade PGP tem gerado. Os usuários de PGP será "pós-graduação" totalmente licenciado

versões, em muitos casos. As corporações, em seguida, usar
RSADSI produtos.
+ Curiosamente, o PGP poderia fazer o "radical" coisas que
RSADSI não estava preparado para fazer. (Usa familiar
Cypherpunks.)
- ignorando as restrições à exportação é um exemplo disso
- incorporação experimental de dinheiro digital sistemas de
- Parasitismo, muitas vezes, aumenta a taxa de evolução. Certamente
O PGP tem ajudado a luz de um fogo sob RSADSI.
7.14.2. Stealth PGP
- Xénon, Nik, S-Ferramentas,
7.14.3. "Devemos trabalhar em uma versão mais avançada, a *Muito Bom
Privacidade*?"
- mais fácil dizer do que fazer...forte compromisso de tempo
- não está claro o que é necessário...
7.14.4. "As alterações e melhorias de ser feito para PGP?"
- Considero-o um dos suprema ironia da nossa idade que
Phil Zimmermann tem denunciado Tom Rollins para fazer
várias alterações para uma versão de PGP ele se torna disponível.
+ Questões:
- Phil reputação, e do PGP
- propriedade intelectual
- Licença Pública GNU
- o mero nome do PGP
- Considerar que a RSA disse a mesma coisa, que o PGP
seria prejudicar a reputação de chave pública (esp. como Phil
foi um "amador", a mesma exata fraseologia PRZ usa para
criticar Tom Rollins!)
- Eu não estou tomando um pé aqui....Eu não sei os detalhes.
Apenas alguns ironia.

7.15. Pontas Soltas
7.15.1. Medidas de segurança no login, senhas, etc.
- Evitar a introdução de palavras-passe através da rede (tais como em rlogins
ou telnets). Se alguém ou algum agente pede para o seu
palavra-passe, ser paranóico.
- Pode usar telnet criptografado, ou algo como Kerberos, para
evitar o envio de palavras-passe na clara entre as máquinas. Lotes
de abordagens, quase nenhum deles comumente usado (pelo menos
Eu nunca vê-los).

8. O anonimato Digital Misturas, e Remetentes

8.1. direitos autorais

O CYPHERNOMICON: Cypherpunks FAQ e Mais, Versão 0.666,
1994-09-10, Direitos De Autor Timothy C. De Maio. Todos os direitos reservados.
Veja os detalhes de isenção de responsabilidade. Use seções curtas em "justo
use" disposições, com crédito apropriado, mas não coloque o seu
nome em minhas palavras.

8.2. RESUMO: o Anonimato Digital Misturas, e Remetentes

8.2.1. Pontos Principais

- Remetentes são essenciais para anônimos e pseudônima
sistemas, porque eles derrotam análise de tráfego
- Cypherpunks remetentes de ter sido um dos maiores sucessos,
aparecendo na época do Kleinpaste/Julf
reenvio de e-mails(s), mas agora se expandindo para vários sites
- Para ver uma lista de sites: com o dedo, reenvio de e-mails-
lista@kiwi.cs.berkeley.edu
(ou http://www.cs.berkeley.edu/~raph/remailer-list.html)
- O anonimato, em geral, é uma ideia central

8.2.2. Ligações para Outras Secções

- Remetentes fazer as outras tecnologias possíveis

8.2.3. Onde Encontrar Informações Adicionais

- Muito pouco tem sido escrito (formalmente, em livros e
periódicos) sobre remetentes
- David Chaum papéis são um começo

8.2.4. Diversos Comentários

- Este continua a ser um dos mais desorganizado e confuso
seções, na minha opinião. Ele precisa de um monte mais de reformulação e
reorganizando.
+ Em parte, isto é devido a vários fatores
- um grande número de pessoas têm trabalhado em remetentes,
contribuir com ideias, problemas, código, etc
- existem muitas versões, muitos sites, e os sites de alteração
de dia para dia
- muitas idéias para novos recursos
- em um estado de fluxo
- Esta é uma área onde a real experimentação com remetentes
é muito fácil e muito instrutivo...a "teoria" de
remetentes é straighforward (em comparação com, digamos, o digital
em dinheiro) e a experiência de aprendizagem é melhor do que a teoria
de qualquer maneira.
- Há verdadeiramente um grande número de recursos, idéias,
propostas, pontos de discussão, e de outras coisas. Nenhuma das perguntas frequentes
poderia começar a cobrir o chão coberto de a, literalmente,

milhares de posts sobre os remetentes.

8.3. O anonimato e Digital Pseudônimos

8.3.1. Porque é que o anonimato é tão importante?

- Permite escapar do passado, um elemento essencial do
straighening fora (uma função importante do Oeste
fronteira, a Legião Estrangeira francesa, etc., e algo que
estão perdendo como os processos viajar com a gente onde quer que se vá)
- Permite novos e diversos tipos de opiniões, como observado abaixo
- Mais basicamente, o anonimato é importante porque a identidade é
não é tão importante como tem sido feito no nosso dossiê
sociedade. A saber, se Alice deseja permanecer anônimo ou
sob pseudônimo, para Bob, Bob não pode "exigir" que ela fornecer
aqui nome "verdadeiro". É uma questão de negociação entre
- os. (Identidade não é livre...é uma credencial como qualquer
outros e não pode ser exigido, apenas negociados.)
Direito de voto, hábitos de leitura, comportamento pessoal...todas são
exemplos onde a privacidade (= o anonimato, de forma eficaz) são
crítica. A próxima seção dá uma longa lista de razões para
o anonimato.

8.3.2. Qual é a diferença entre o anonimato e a pseudonímia?

+ Não é muito, em um nível...muitas vezes usamos o termo "digital
pseudônimo de" um sentimento mais forte, em que a identidade real
não pode ser deduzido facilmente
- esse é o "anonimato", em certo sentido,
- Mas, em outro nível, um pseudônimo carrega a reputação da empresa,
credenciais, etc., e _não_ é "anônimo"
- as pessoas usam pseudônimos, por vezes, por razões caprichoso
(por exemplo, "a Partir de spaceman.spiff@calvin.hobbes.org Setembro 6, 94
06:10:30"), às vezes, para manter diferentes listas de discussão
separado (diferentes personnas para diferentes grupos), etc.

8.3.3. Desvantagens do anonimato

- calúnia e outras semelhantes perigos para a reputação da empresa
+ bate-e-corre ações (principalmente na rede)
+ por outro lado, tais devaneios pode ser ignorado (MATAR
ficheiro)
- reputação positiva
- prestação de contas com base em ameaças físicas e rastreamento é
perdido
+ Práticos problema. No Cypherpunks lista, eu, muitas vezes, tomar
"anônimo" mensagens menos a sério.
- Eles são muitas vezes mais bizarro e inflamatórios do que o normal
postos, talvez por um bom motivo, e eles certamente

mais difícil de levar a sério e responder. Isso é para ser
o esperado. (Devo observar que alguns pseudônimos, tais como
Unicórnio negro e Pr0duct Cypher, estabeleceram
respeitável digital personnas e valem bem a pena responder
a.)
- repúdio das dívidas e obrigações
+ infantil chamas e execute-amok lançamentos
- racismo, sexismo, etc.
- como "Rumormonger" na Apple?
- mas essas são razões para pseudônimo para ser usado, onde a
a reputação de um pseudônimo é importante
+ Crimes...assassinatos, subornos, etc.
- Estas são tratadas com mais detalhes na seção sobre
crypto anarquia, como esta é uma grande preocupação (anônimo
mercados para serviços)
8.3.4. "Como a privacidade e o anonimato ser atacados?"
- desvantagens listadas são, muitas vezes, citada como uma razão pela qual nós
não pode ter "anonimato"
- como tantos outros "hacker de computador" itens, como uma ferramenta para
"os Quatro Cavaleiros": droga-negociantes, de dinheiro, lavagem,
terroristas e pedófilos.
- como um refúgio para práticas ilegais, por exemplo, de espionagem, de armas
a negociação, os mercados ilegais, etc.
+ evasão fiscal ("Nós não podemos imposto de que se não podemos vê-lo.")
- o mesmo sistema que faz com que o IRS é um "parceiro silencioso" em
as transações de negócio, e que dá o IRS acesso a--
e requer--registros de negócios
+ "discriminação"
- que permite a discriminação (este _used_ estar OK)
- exclusão de comunidades, menino redes
8.3.5. "De que forma aleatória acusações e selvagem rumores de ser controlado em
anônimo fóruns?"
- Primeiro, aleatório acusações e boatos demonstrações
a norma na vida moderna; a fofoca, tablóides, rumores, etc. Nós
não se preocupe obsessivamente sobre o que fazer para parar todos esses
boatos e até mesmo os falsos comentários. (Uma tendência preocupante tem
sido a tendência para sue, ou ameaçar ternos. E
cada vez mais a atitude é que pode ser expresso por
opinions, mas não fazer declarações ", a menos que possam ser
comprovada". Que não é o que a liberdade de expressão é tudo!)
- Em segundo lugar, a reputação da empresa em questão. Baseamos nossa confiança em
declarações
em uma variedade de coisas, incluindo: uma história do passado, o que

outros dizem sobre a sua veracidade, externo fatos em nossa
a posse, e motivos.
8.3.6. "Quais são as posições jurídicas, no anonimato?"
+ Relatórios que a Suprema Corte derrubou uma lei do Sul
exigindo panfleto distribuidores para o identificar. 9l
não tem um citam sobre isso.)
- No entanto, Greg Broiles desde que esta proposta, a partir de _Talley
v. Estado de California_, 362 EUA 60, 64-65, 80 S. Ct.
536, 538-539 (1960) : "Anônimo panfletos, folhetos,
brochuras e até mesmo os livros têm desempenhado um papel importante na
o progresso da humanidade. Perseguidos grupos e seitas de
tempo ao tempo ao longo da história têm sido capazes de
criticar práticas opressivas e as leis qualquer
anonimamente ou não."

Greg acrescenta: "É mais tarde diz: "Mesmo o Federalista,
escrito em favor da adoção da nossa Constituição,
foram publicados sob nomes fictícios. É claro que
o anonimato foi, por vezes, assume-se que para a maioria
construtivo fins." [Greg Broiles, 1994-04-12]

+ E, certamente, muitos escritores, jornalistas, e outros usam
pseudônimos, e ter de enfrentar qualquer ação legal.
- Desde que não usá-lo para sonegar impostos, evadir legal
julgamentos, cometer fraudes, etc.
- Eu ouvi (não cita) que "entrando mascarado com a finalidade
de ir mascarado" é ilegal em muitas jurisdições. Difícil
acredito que, como muitos outros disfarces são tão eficazes e
são, presumivelmente, não proibiu (perucas, bigodes, maquiagem,
etc.). Eu suponho que a lei tem a ver com as pessoas wearning de esqui
as máscaras e os tais "inadequado" lugares. Más leis, se real.
8.3.7. Alguns Outros Usos para Sistemas Anónimos:
+ De Groupware e Anônimo debate e Votação
- sistemas baseados no Lotus Notes e projetado para incentivar
idéias selvagens, os comentários do tímido ou muito educado, etc.
- estes sistemas podem iniciar inicialmente na reunião e, em seguida,
ser estendido para sites remotos, e, eventualmente, para todo o país
e fóruns internacionais
- a ANS pode ter um ataque do coração em relação a essas tendências...
+ "Democracia de Parede" para mensagens criptografadas
- possibilidade de utilização de atraso no tempo de chaves (onde até mesmo o público
chave, para a leitura do texto sem formatação, não é distribuído para
algum tempo)

- sob a capa de um jornal eletrônico, com todos
a proteção constitucional que implica: letras
o editor pode ser anônima, os anúncios não precisam ser rastreados para
de validade, a publicidade reivindicações não são de responsabilidade
do papel, etc.
+ Anonymous comentários e hipertexto (para novos tipos de revistas)
+ vantagens
- honestidade
- aumento da "temperatura" do discurso
+ desvantagens
- aumento chamas
- desinformação intencional
+ Store-and-forward nós
- usado para facillitate a votação anônima e anônimo
o inquérito (ou leitura) de sistemas
- Chaum do "mix"
+ de telefone de encaminhamento para sistema digital de dinheiro para pagar
para o serviço de
- e TRMs?
+ Fibra óptica
+ de difícil rastreamento, como o de milhões de quilômetros de são estabelecidas, incluindo
praticamente indetectáveis linhas no interior de edifícios particulares
- suponha que o governo suspeita de pacotes criptografados estão indo
para os edifícios da Apple...ausente qualquer directa
conhecimento de crimes a ser ajudado, pode o
governo procura de um mapeamento de mensagens de entrada para
a saída?
- Que é, o governo vai exigir a total divulgação de
todos os roteiros?
- alta largura de banda significa muitos graus de liberdade para tais
implementação de sistemas de
+ Dentro de sistemas, por exemplo, o usuário faz logon em um sistema seguro e
é dado acesso ao seu próprio processador
- em 288-sistema de processador, como o NCR/ATT 3600 (ou mesmo
maior)
- sob sua cryptonym ele pode acessar determinados arquivos, gerar
outros, e depósito mensagem untraceably em outro e-mail
locais que outros agentes ou os usuários podem recuperar
e para a frente....
- em um sentido, ele pode usar este acesso para lançar a sua própria
agente de processos (o anonimato é essencial para muitas agente
os sistemas de base, como é dinheiro digital)
+ Incentivos econômicos para os outros para transportar correio para outros

sites...
- mais a difusão e a ocultação da verdadeira funções
+ Sistemas binários (duas ou mais peças necessárias para completar o
mensagem)
- possibilidade de utilização de vírus e worms para lidar com o
complexidades de distribuir essas mensagens
- agentes de maio de lidar com o transfer, com o isolamento entre
os agentes, então, o encaminhamento não pode ser rastreado (pense em cena
em "Double-Cruzadas", onde os fardos de maconha são passados
de avião, de barco a chopper caminhões para carros)
- isso protege contra conspirações
+ Satélites
+ segurança física, em que os satélites teria que
ser abatido para interromper a transmissão
+ cenário: WARC (ou quem) concede direitos de transmissão em
De 1996 para algum país ou consórcio, que, em seguida, aceita
qualquer e todos os clientes pagantes
- dinheiro frio
- o BCCI de operadores de satélite
+ VSATs, Banda L, Satélites De Baixa Órbita Da Terra
- Very Small Aperture Terminals
- Banda L...o que frequência?
+ LEO, como com o Iridium da Motorola, oferece diversas
vantagens
- menor potência de receptores e antenas menores
- baixo custo para o lançamento, devido ao tamanho pequeno e menor necessidade
durante 10 anos de confiabilidade
- evitar o "orbital slot de" licenciamento "pântano"
(embora eu presumo que alguns de licenciamento ainda está envolvido)
- podem combinar-se com um impulso ou nonsinusoidal transmissões
8.3.8. "Nomes Verdadeiros"
8.3.9. Muitas maneiras de obter pseudônimos:
- Telnet para a porta 25" ou usar conexões SLIP para alterar o domínio
nome; não é muito seguro
- Remetentes
8.3.10. "Como é Pseudonímia Comprometido?"
- slip-ups em grande estilo, os cabeçalhos, os sig blocos, etc.
- inadvertida de revelar, através de remetentes
- análise de tráfego de remetentes (não é muito provável, pelo menos,
não para não-NSA adversários)
- correlações, a violação da "indistinguibilidade
princípio"
8.3.11. Questões Diversas

- Mesmo digital pseudônimos pode ficar confusa...alguém
recentemente confundiu "Tommy o Turista" por ser um
real digital pseudônimo (quando é claro que é apenas
anexado a todos os posts, vai througha particular reenvio de e-mails).

8.4. Razões para o Anonimato e Digital Pseudônimos (e Rastreáveis E-Mail)

8.4.1. (D são tantos motivos, e este perguntou tantas vezes, que
Eu já colecionei várias razões aqui. Mais pode ser acrescentado,
do curso.)
8.4.2. Privacidade em geral
8.4.3. Ameaças Físicas
+ "empresa terrrorism" não é um mito: os traficantes de drogas e
outros "marginais" empresários face a esta todos os dias
- extorsão, ameaças, sequestros
+ e muitas empresas do futuro pode ser bem menos
"cavalheiresca" do que a visão convencional tem
- testemunha o sangue ruim entre Intel e AMD, e, em seguida,
imagine ficar dez vezes pior
- e rivalidades nacionais, mesmo na aparentemente legal
negócios (acho que de traficantes de armas), podem causar o uso de mais de violência
+ Máfia e outros grupos de crime organizado pode tentar extorquir
pagamentos ou concessões de participantes do mercado, fazendo com que
- os a buscar a relativa proteção de sistemas anónimos
- com reputação
+ Note que as chamadas para o ameaçou ligar para a polícia
para a proteção tem vários problemas
- as atividades podem ser ilegais ou marginalmente ilegal
(esta é a razão pela Máfia muitas vezes pode se envolver
e porque ela pode até, por vezes, ter um efeito positivo,
atuando como o cop para atividades ilegais)
- a polícia é muitas vezes demasiado ocupado para se envolver, o que
com tanto física crime o entupimento dos tribunais
- extorsão e sequestro pode ser feito usando estes muito
técnicas de cryptoanarchy causando, assim, um tipo de braços
raça
+ maltratadas e abusadas as mulheres e as famílias podem precisar
equivalente a um "programa de proteção a testemunhas"
+ por causa da facilidade de rastreamento de compras com cartão de crédito
com direito a propinas e/ou o tribunal (ou mesmo
o "hacking"), esposas espancadas pode procurar cartões de crédito, sob pseudônimos

- e algumas empresas de cartão pode obrigar, como uma espécie de
politicamente correto social gesto
+ ou grupos, como AGORA, e as Mulheres Contra o Estupro pode até
oferecer os seus próprios cartões
- talvez apoiado por algum tipo de fundo de garantia
- poderia ser de cartões de débito
+ pessoas que participam no ciberespaço, as empresas podem medo
retaliação ou de extorsão no mundo real
- ameaças por parte de seus governos (para todos os habituais
razões, além de subornos, ameaças para fechá-los para baixo,
etcl)
- ripoffs por aqueles que cobiçam o seu sucesso...
8.4.4. Votação
- Vamos levá-lo para concedido nas sociedades Ocidentais que a votação
deve ser "anônimo"--untraceable, unlinkable
- não pedimos às pessoas "o Que você tem a esconder?" ou dizer
eles "Se você está fazendo algo de forma anônima, deve ser
ilegal."
- Mesma lição que devemos aplicar para um monte de coisas para o qual o
o governo está cada vez mais exigente prova de identidade para
+ Anonymous Voto em Clubes, Organizações, Igrejas, etc.
+ uma grande avenida para a divulgação de CA métodos: "eletrônico
blackballing," votação ponderada (como com o número de ações)
+ por exemplo, uma corporação problemas "voto tokens", que pode
ser usado para votar de forma anônima
- ou até mesmo vendidos para outros (como a venda de ações, exceto
vendendo apenas o direito de voto para uma determinada eleição
é mais barato, e muitas pessoas não ligam muito sobre
eleições)
+ uma forma de se proteger contra bolsos profundos processos em, digamos,
corrida de casos de discriminação
- em que um diretor é processado por alguma ação a
empresa leva o anonimato vai dar-lhe alguns legal
proteção, alguns "negação plausível"
+ é possível configurar sistemas (cf. Salomaa) em que
alguns "supervotes" tem blackball de energia, mas o uso de
esses vetos é indistinguível de um padrão
regras de maioria voto
- por exemplo, ninguém, exceto os blackballer(s), vai saber
se o blackball foi usado!
+ será que o governo tenta limitar este tipo de
protocolo?
- alegando discriminação potencial ou abuso de

direitos de voto?
+ vai Departamento de Justiça (ou S) tentar subverter
votação anônima?
- como parte do movimento potencial para um "full disclosure"
a sociedade?
- relacionados a leis antidiscriminatórias, prestação de contas,
etc.
+ Anonymous Votação na Reputação-Based Systems (Revistas,
Mercados)
+ os clientes podem votar em produtos, em qualidade de serviço,
sobre as diversas ofertas que já estão envolvidas em
- não é claro como os direitos de voto teria distribuído
- a ideia é evitar ações judiciais e sanções por fornecedores,
etc. (como com o Bose naipe)
+ Revistas
- um exemplo canônico, e que eu deve incluir, como
ele combina anônimo arbitragem (que já é padrão,
nas formas primitivas), hipertexto (links para as resenhas),
básica e a liberdade de expressão dos problemas
- este provavelmente vai ser um dos primeiros a área de uso
- toda esta área do consumidor, comentários podem ser uma forma de obter
CA de largura de banda e execução (lotes de PK-criptografado
o tráfego de deslocamento em torno das várias redes)
8.4.5. A manutenção da liberdade de expressão
- proteção de expressão
+ evitar retaliação por controverso discurso
- este discurso pode ser controverso, injurioso, horrível,
politicamente incorreto, racista, sexista, speciesist, e
outros horrível...mas remetentes e o anonimato tornam tudo
impossível parar
- denúncia
+ discurso político
- KKK, Ariana Resistência da Liga, Preto Frente Nacional,
qualquer que seja a
- cf. o "debate" entre "Locke" e "Demóstenes" em
Orson Scott Card do romance, "Ender do Jogo."
- (Muitas destas razões são também por dados 'paraísos' vai
eventualmente, configurar...na verdade, eles já existem...homolka
de avaliação, etc.)
8.4.6. Adotar diferentes personnas, pseudônimos
8.4.7. Escolha do material de leitura, hábitos de visualização, etc.
- para evitar dossiês sobre esta sendo formado, anônimo
as compras são necessários (dinheiro funciona para itens pequenos, não para

alugueres de vídeo, etc.)
+ alugueres de vídeo
- (Nota: Existem "leis" de fazer tais liberações ilegais,
mas...)
- cabo t.v. hábitos de visualização
+ correio de ordem de compras
- sim, eles precisam do seu endereço para o navio, mas não pode ser
recortes que desconectam (por exemplo, a FedEx pode recurso de tal
serviço de, algum dia
8.4.8. O anonimato em Solicitar Informações, Serviços, Bens
+ la a controvérsia sobre a IDENTIFICAÇÃO de chamada e 900 números: as pessoas
não quer que seus números de telefone (e, portanto, identidades)
alimentado em grande consumidor de preferência de bancos de dados
- uma das coisas que eles compram, os vídeos alugados, os livros
a leitura. etc. (várias leis e proteger alguns destes
áreas, como a biblioteca de livros, alugueres de vídeo)
- listas de assinatura já estão a expansão da revenda
mercado...isso vai chegar mais rápido e com mais precisão "sintonizado"
com as assinaturas electrónicas: daí o desejo de
assine anonimamente
+ alguns exemplos de "sensível" serviços de que o anonimato pode ser
desejado em (especialmente relacionados com computadores, modems, BBSes)
+ leitura incomum ou sensível grupos: alt.o sexo.escravidão,
etc.
- ou o lançamento para estes grupos!
- recente controvérsia sobre a NAMBLA pode fazer
proteções mais desejável para alguns (e paralelas chamadas
para restrições!)
a publicação de tais grupos, especialmente dado que os registos são
perpétuo e que as agências governamentais e de leitura de arquivo
lançamentos (absolutamente trivial coisa para fazer)
- solicitar a ajuda em questões pessoais (equivalente a
"Nome Retida" visto tantas vezes)
+ discutindo controversas questões políticas (e quem sabe
o que vai ser controverso, 20 anos mais tarde, quando o cartaz
está em busca de um cargo político, por exemplo?)
- dado que alguns grupos já (1991) foi o
últimos lançamentos de pessoas que estão tentando manchar!
+ Nota: a diferença entre o lançamento de um BBS ou grupo
linha de conversação e a escrita de uma carta para um editor, é
significativo
- em parte tecnológica: é muito mais fácil compilar
registros de lançamentos do que ele é cortar-se de recortes de

cartas aos editores (apesar de que isso vai mudar rapidamente, como
scanners fazer isso fácil)
- em parte sociológica: as pessoas que escrevem cartas saber o
letras vai ser com a parte de trás problemas em perpetuidade,
que vinculado a questões de preservar suas palavras para muitos
décadas (e poderia voltar para
assombrá-los), mas as pessoas que postam para BBSes, provavelmente,
acho que suas palavras são temporários
+ e há alguns outros fatores
- sem edição
- não há atrasos de tempo (e sem a possibilidade de chamar um editor e
retirar uma carta escrita com pressa ou raiva)
+ e letras podem, e são, muitas vezes, escrito com a
"Nome Retida" assinatura-esse é, atualmente, ao lado
impossível fazer em redes
- apesar de algumas "encaminhamento" serviços informalmente
raiou
+ Empresas podem querer se proteger de ações judiciais
mais comentários por seus funcionários
+ o habitual "As opiniões aqui expressas não são aqueles de
meu empregador" pode não ser suficiente para proteger um empregador
de ações judiciais
- imagine racista ou sexista comentários, levando a ações judiciais
(ou pelo menos a ser trazidos como prova do tipo
de "atitude" promovido pela empresa, por exemplo, "eu
trabalhou para a Intel, por 12 anos e posso dizer que
os pretos fazem muito pobres engenheiros.")
+ funcionários podem fazer comentários que prejudicam a reputação
de suas empresas
- Nota: isto é diferente da situação atual, onde
liberdade de expressão tem prioridade sobre a empresa preocupações,
devido a lançamentos de um BBS são realizadas amplamente, pode
ser revistados eletronicamente (por exemplo, AMD advogados de pesquisa
a UseNet lançamentos de 1988-91 para qualquer lançamentos por
Funcionários da Intel besmirching a qualidade ou o que quer que de
Chips AMD),
- e então, os funcionários das empresas podem proteger a si mesmos,
e seus patrões, com a adoção de pseudônimos
+ Empresas podem buscar informações sem querer alerta
seus concorrentes
- atualmente, isso é feito com agentes, "executive search
as empresas," e advogados
- mas como é que vai evoluir para lidar eletrônico pesquisas?

+ existem algumas analogias com limalha de "Liberdade de
A Lei de" pedidos e patentes, etc.
+ esses "expedições de pesca" irá aumentar com o tempo, como
ele se torna rentável para as empresas de pesquisa que
montanhas de eletrônica-arquivado materiais
- estudos de impacto ambiental, de saúde e de segurança
divulgações, etc.
- pode ser algo que algumas empresas se especializam em
+ Anonymous Serviços de Consulta, Anônimo Longarinas ou
Repórteres
+ imagine um intermediário de informação, talvez em um AMIX-como
de serviço, com uma rede de longarinas
+ acho que de braços lidar newsletter escritor em Hallahan do
O Comércio, com a sua rede de longarinas alimentá-lo
dicas e informações privilegiadas
- em vez de se encontrar em segredo locais, um muito
caro proposição (no tempo e viagens), um seguro
a rede pode ser usada
- com reputações digitais pseudônimos, etc.
+ eles podem não desejar que as suas reais identidades conhecido
- ameaças de empregadores, ex-empregadores, governo
agências
+ assédio através de diversas práticas criminosas que vai
tornam-se mais comuns (por exemplo, a facilidade com que
assaltantes e até mesmo assassinos podem ser contratadas)
- parte do total de mover-se em direção anonimato
- os medos de processos, requisitos de licenciamento, etc.
+ Candidatas para Tal Anônimo Serviços de consultoria
+ An braços negócios newsletter
- uma excelente reputação de rigor e oportuna
informações
+ uma espécie de formulário eletrônico de Jane
- com escândalos e a preocupação do governo
- mas ninguém sabe de onde ele vem
+ um site que distribui para os assinantes recebe-lo
com outro maior lote de material encaminhado
- NSA, FBI, Fincen, etc. tenta controlá-la para baixo
+ Tecnologia de "Insider", relata em todos os tipos de novos
tecnologias
- modelado após Hoffler da Microeletrônica Notícias, o
Vale líder da folha de sugestões por duas décadas
- o editor paga para dicas, com pagamentos feitos em dois
partes: imediata, e dependente do tempo, de modo que o

a precisão de uma ponta, e sua principal importância (em
o julgamento do editor) pode ser proporcionalmente
recompensado
+ PK sistemas, com colaboradores capazes de criptografar e
em seguida, publicamente post (usando os seus próprios meios de
difusão)
- com suas mensagens que contenham mais material,
como autenticações, para onde enviar o
pagamentos, etc.
+ Lundberg da Indústria de Petróleo do Inquérito (ou similar)
- i.é., um bastante convencional newsletter com publicamente
conhecido autores
- neste caso, o autor é conhecido, mas as identidades
de contribuintes é bem protegido
+ Uma Conspiração Newsletter
- relatórios sobre todas as mais recentes teorias de
o mau comportamento (como em "Conspirações" deste
estrutura de tópicos)
+ uma ruga: um imenso hipertexto da web, com colaboradores
capaz de adicionar links e nós
+ naturalmente, o seu verdadeiro nome, se eles não se preocupam com
no mundo real repercussões-ou um de seus digital
pseudônimos (pode também usar cryptonyms) está conectado
+ vários algoritmos para a reputação da empresa
- soma total de tudo o que foi escrito, de alguma forma,
medida por outros comentários feitos por "votação,"
etc.
- um tipo de média móvel, permitindo o fato de
que a aprendizagem irá ocorrer, assim como um pesquisador
provavelmente fica melhor com o tempo, e que como
reputação baseada em sistemas de tornar-se melhor
entendeu, as pessoas vêm para apreciar o
importância da escrita cuidadosamente
+ e um dos mais controversos de todos: Yardley do
Inteligência Diária
no entanto, ele pode vir mais de uma vez por dia!
+ um ex-agente isto em meados da década de 90, solicitando
contribuições através de um anônimo de comutação de pacotes sysem
- refinados ao longo dos próximos dois anos
- combinação de métodos
- o governo tem vindo a esforçar-se para identificar o
o editor, "Yardley"
- ele oferece um retorno do investimento com base no valor do

informações, e ainda tem um "Pedidos" e um
Classificada secção de Anúncios
- um hipertexto da web, semelhante à Conspiração Newsletter
acima
+ Será que o Governo vai Tentar Desacreditar o Boletim Com
Informações Falsas?
- claro, o padrão de manobra na reputação-com base
sistemas
+ mas Yardley tem desenvolvido vários tipos de filtros de
para esta
- digital pseudônimos que, gradualmente, construir
reputação
- cruz-a verificação de sua própria espécie
- ele ainda usa a linguagem filtros para analisar o texto
+ e então o que?
- o mundo está cheio de desinformação, rumores,
mentiras, meias-verdades, e de alguma forma as coisas vão no....
+ Outras AMIX-como Anónimo Serviços
+ De drogas Preços e Dicas
- dicas sobre a qualidade de várias drogas (por exemplo,
"Várias fontes confiáveis disseram-nos que o
mais recente Maui Wowie é muito intensa, números de
abaixo...")
+ de síntese de fármacos (possivelmente um separado
assinatura)
- designer de drogas
- casa laboratórios
- evitar detecção
+ Os Hackers Diária
- dicas sobre hacking e cracking
- anônimo próprios sistemas (mais dicas)
- Avaliações de produtos (o anonimato necessário para permitir honesto
comentários com mais de proteção contra ações judiciais)
+ Jornais Estão se Tornando Cocerned com Tendência
Pagando Dicas de Notícias
- pelo independentes serviços de consultoria
- mas o que elas podem fazer?
+ processos são julgados, para evitar anônimo dicas quando
os pagamentos são envolvidos
- seus advogados citam a evasão fiscal e nacional
aspectos de segurança
+ Privado Bases De Dados
+ qualquer organização da oferta de acesso a bases de dados deve ser

preocupado que alguém-um cliente insatisfeito, um
denunciante, o governo, quem-será
a abertura dos arquivos
- sob vários "Privacidade de Dados" leis
- ou apenas em geral (direito penal, cível, "descoberta")
+ assim, serão tomadas medidas para isolar os dados reais da
usuários reais, talvez através de recortes
+ por exemplo, um serviço de dados vende acesso, mas de serviços de terceiros fora
as pesquisas para outros serviços através de caminhos que são
untraceable
+ este, provavelmente, não pode ser proibido em geral-embora qualquer
transação específica, pode ser declarado ilegal,
etc., no momento em que a ligação é cortada e uma nova
estabeleceu-como seria de eliminar todas as subcontratação
arranjos!
- por exemplo, se o joão de Dados do Serviço de encargos de us $1000 para um
pesquisa em widgets e, em seguida, usa um outro, possivelmente,
transitório (o que significa um recorte) serviço de dados, o
mais uma ação judicial pode fazer é forçar Joe parar de usar
este untraceble serviço
- níveis de indireção (e firewalls que impedem que os
a propagação das investigações)
+ Médico Eleições (a la AIDS pesquisas, práticas sexuais de pesquisas,
etc.)
+ relembre o método em que um participante joga uma moeda para
responder a uma pergunta...o analista pode ainda recuperar o
importante conjunto de informações, mas a "fase" é perdida
- por exemplo, um indivíduo de responder "Sim" para a pergunta
"Você já teve xyz sexo?" podem ter realmente respondeu:
"Não", mas tinha sua resposta invertida por um lance de moeda
+ os investigadores podem até adotar métodos sofisticados em que
explícita diários são mantidos, mas que são, então, transmitidos
sob um anônimo sistema de endereçamento para os pesquisadores
- perigos óbvios de autenticação, validade, etc.
+ Teste médico: muitas razões para as pessoas procurarem o anonimato
- O teste da SIDA é o principal exemplo
- mas, também, testes de condições que podem afetar
insurablity ou de emprego (por exemplo, as pessoas podem ir para
médico paraísos no México ou para onde quer que testes que podem
levar a uninsurability devem as companhias de seguros aprender
a "condição prévia")
+ exceto em AIDS e Dst, é, provavelmente, ilegal e
contra a ética médica para oferecer anônimo consultas

- talvez as pessoas vão viajar para outros países

8.4.9. O anonimato na Pertencentes a Determinados Clubes, Igrejas, ou Organizações

+ as pessoas temem retaliação ou constrangimento deve a sua associação de serem descobertas, agora ou mais tarde

- por exemplo, um membro da igreja que pertence a controversa grupos ou clubes

- principalmente ou inteiramente, aqueles em que o contato físico ou outros o contato pessoal não é necessário (um conjunto limitado)

- semelhante à célula baseada em sistemas descritos em outro lugar

+ Candidatos anônimos, clubes ou organizações

- Earth First!, Agir, Animal Liberation Front, etc.

- NAMBLA e similares controverso grupos

- todos esses tipos de grupos que têm muito vocal, muito visível membros, visível até mesmo ao ponto de buscar a cobertura de televisão

- mas há provavelmente muito mais do que seria de se juntar a esses grupos se há identidades poderia ser blindado público o grupo, por causa de suas carreiras, suas famílias, etc.

+ ironicamente, a empresa repressão de atividades fora de casa considerado hostil para com a corporação (ou expô-los a secundária de ações judiciais, reivindicações, etc.) poderá causar uma maior utilização de anônimo sistemas

- célula-base de participação em grupos

- o crescimento do anônimo participação em grupos (usando pseudônimos) tem um benefício em aumentar o quadro associativo por as pessoas de outra forma com medo de entrar, por exemplo, um radical grupo ambiental

8.4.10. O anonimato em Dar Conselhos ou Ponteiros para Informações

- suponha que alguém diz que está vendendo alguns ilegal ou o contrabando de produtos...isso também é ilegal?

- sistemas de hipertexto vai fazer esse inevitável

8.4.11. Comentários, Críticas, Comentários

- "Eu sou secções de ensino para uma classe deste termo, e amanhã Eu estou indo para: 1) dizer a meus alunos como usar um reenvio de e-mails, e 2) solicitar comentários anônimos no meu ensino.

"Eu acho que ele irá torná-los menos apreensivos sobre como fazer honesto sugestões e comentários (supondo que nenhum deles se incomoda, é claro)." [Patrick J. LoPresti patl@lcs.mit.edu, alt.privacidade.anon-servidor, 1994-09-08]

8.4.12. Proteção contra ações judiciais, "bolsos" leis

+ não permitindo que a riqueza de uma entidade para ser associado

com ações
- isso também funciona pela ocultação de bens, mas o IRS em carrancas
que, portanto, desvincular a publicação ou correspondência com nome
entidade real é geralmente mais fácil
+ "bolsos"
- vai ser no interesse de alguns, para esconder a sua
identidades, de modo a impedir esses tipos de processos
(arquivado, por qualquer motivo, com ou sem razão)
- postagens e comentários podem expor os autores de ações judiciais
por difamação, falsidade ideológica, concorrência desleal, e assim por
em (tanto de graça discurso beknighted estados)
+ os empregadores também podem ser expostos aos mesmos fatos,
independentemente de onde os seus colaboradores, publicado a partir de
- sobre o frágil fundamento de que um funcionário estava agindo em
a sua entidade patronal, o nome, por exemplo, na defesa de um Intel
produto na Usenet
- isso, BTW, é outra razão para as pessoas procurarem maneiras de
esconder alguns dos seus bens-para evitar o confisco no profundo
bolsos de processos (ou família de doenças, em que vários
agências de tentar apreender os bens de qualquer pessoa que pode)
- e mesmo computadores que permitem que essas transações
também permite mais rápida determinação de quem tem o
mais profundos bolsos!
+ isolando a entidade de repercussões de "sexista" ou
"racista" comentários susceptíveis de provocar ações judiciais, etc.
- (Não riam-muitas empresas estão a ficar preocupado com o que
o que seus empregados escrever na Usenet podem desencadear processos
contra as empresas.)
+ muitas operações, pode ser considerado ilegal em alguns
jursidictions
+ mesmo em alguns que o serviço ou fornecedor de bens não tem
controle sobre
- exemplo: arma os tomadores de ser responsabilizado por armas de fogo
mortes no Distrito de Columbia (embora
recentemente cancelada)
- o labirinto de leis pode causar alguns buscam o anonimato para
proteger-se contra este labirinto
+ Cenário: Anônimo doador de órgãos bancos
+ por exemplo, uma forma de "mercado" raros tipos de sangue, ou seja,
sem expondo uma auto forçada, doação ou outros
sanções
- "forçado doação" envolve as ações ajuizadas pelo
potencial destinatário

- no momento de oferecer, pelo menos...o que acontece quando a
negócio é consumado é outro domínio
- e uma forma de evitar que um número crescente de governo
picadas
8.4.13. Jornalismo e de Escrita
+ escritores tiveram uma longa tradição de adotar pseudônimos,
para uma variedade de razões
- porque eles não conseguiam obter publicado sob a sua Verdadeira
Nomes, porque eles não _want_ seus nomes verdadeiros
publicado, para se divertir, etc.
- George Elliot, de Lewis Carroll, Saki, de Mark Twain, etc.
- repórteres
+ radio disc jockeys
- um Cypherpunk, que trabalha para uma empresa de tecnologia usa o
"no ar personna" de "Arthur Dent" ("Guia do Mochileiro")
por sua parte-o tempo de transmissão de rádio do trabalho comum...
situação, diz-me
+ denunciantes
- este foi um dos primeiros a usar
+ politicamente sensíveis pessoas
- "
+ Eu então tenho uma conta no anon.penet.fi, como
o "Lt.
- Starbuck" da entidade, e todas as posteriores FAQ atualizações foram de
que conta.
- Por razões que parecia importante, no momento, eu levei
a mim mesmo para
- torne-se o moderador/editor do FAQ."
- <an54835@anon.penet.fi, 4-3-94, alt.fã.karla-homolka>
+ Exemplo: Remetentes foram utilizados para a saia de publicação de interdição
a Karla Homolka caso
- vários autores, sob pseudônimo, emitido atualizações regulares
- muita consternação no Canadá!
+ para evitar processos judiciais ou reivindicações de danos para escrever,
edição, distribuição ou venda de "danos" materiais é
outra razão para sistemas anónimos a surgir: os
envolvidos no processo de buscar a imunizar-se
a partir de várias ato ilícito extracontratual, que são o entupimento dos tribunais
- produtores, distribuidores, diretores, escritores, e até mesmo
atores de x-rated ou de outra forma "inaceitável" material
pode ter a proteção de sistemas anónimos
- imagine fibra óptica e a proliferação de vídeos e
talk-shows....bluenoses e procuradores irá usar "do fórum

de compras" para bloquear o acesso, para processar os produtores,
etc.
8.4.14. Escolar, Científico ou Profissional
- proteger outras reputação (profissional, autoral,
pessoal, etc.)
- maior variedade de acções e comportamentos (os autores podem levar
chances)
- flutuante ideias sob pseudônimos
- mais tarde a vinculação desses pseudônimos para uma identidade própria, se
necessário (um case de credencial de transferência)
- flutuante incomum pontos de vista
- Peter Wayner escreve: "eu acho que muitas pessoas que
sair na técnica de grupos de notícias seria muito familiar
com o anônimo procedimentos de avaliação praticado pelo acadêmico
revistas. Há algum valor quando um revisor pode falar
sua mente sobre um papel, sem se preocupar com a vingança. De
é claro que todo mundo me garante que o sistema nunca está realmente
anônimo porque há alwys apenas três ou quatro pessoas
qualificado para analisar cada papel. :-) ....Talvez devêssemos
sair de nosso caminho para fazer anônimo, técnico comentários
sobre trabalhos e ideias de grupos de notícias para o fascilitate
desenvolvimento de um anônimo comentários cultura
cypberspace." [Peter Wayner, 1993-02-09]
8.4.15. O Teste médico e Tratamento
- anônimo exames médicos, la o teste da SIDA
8.4.16. Abuso De Recuperação
+ problema pessoal discussões
- o incesto, o estupro, emocional, Dear Abby, etc.
8.4.17. Ignorando das leis de exportação
- Remetentes anônimos ter sido útil para ignorando o
ITARs...esta é a forma como o PGP 2.6 espalhou-se rapidamente, e (esperamos!)
untraceably do MIT e sites americanos de ventos locais.
8.4.18. Grupos de sexo, discussões de temas polêmicos
- diversas alt.grupos de sexo
- As pessoas podem sentir vergonha, pode temer repercussões do
seus empregadores, não pode desejar a sua família e amigos para
ver seus posts, ou pode simplesmente estar ciente de que a Usenet é
arquivado em muitos, muitos lugares, e está disponível em CD-
ROM e vai ser trivialmente pesquisável nas próximas décadas
+ 100% de rastreabilidade do público em postagens na UseNet e
outros bbs é muito cercear a liberdade de expressão
e torna-se uma das principais justificativas para o uso de
anónimo (ou pseudononymous) e placas de redes

- não podem ser chamadas de leis contra a compilação, como
com o Britânico de dados de leis, mas, basicamente, há pouco
o que pode ser feito quando as postagens ir para dezenas de milhares de
máquinas e são arquivados em perpetuidade, por muitos, de esses
nós e pelos milhares de leitores
- os leitores que podem incorporar o material em suas próprias
lançamentos, etc. (daí o absurdo da lei Britânica)

8.4.19. Evitar a espionagem política

+ TLAs, em muitos países, o monitor de quase todas internacional
comunicações (e um monte de comunicações domésticas, também)
- as empresas e os indivíduos podem querer evitar represálias,
sanções, etc.
- PGP é relatado para estar em uso por vários grupos dissidentes,
e vários Cypherpunks estão envolvidos na assistência.
- "...um aplicativo legítimo, é permitir internacional
grupos políticos ou empresas para o exchange autenticado
mensagens sem serem sujeitos a risco de
espionagem/compromisso por uma de três letras agência, estrangeiros
agência de inteligência, ou de terceiros." [Sean M. Dougherty,
alt.privacidade.anon-servidor, 1994-09-07]

8.4.20. Controversa discussão política, ou a filiação em
políticos, grupos, listas de discussão, etc.

+ Recall Casa UnAmerican Comitê De Atividades
- e é variante moderna: "você agora, ou já
foi, um Cypherpunk?"

8.4.21. Prevenção de Perseguição e Assédio

- evitar física de rastreamento (assédio, "wannafucks," tormentos,
etc.)
- as mulheres e outros são muitas vezes enviados "wannafuck?" mensagens de
os homens que superam 20-para-1 em muitos newsgroups--
pseudônimos de ajuda.
- dada a facilidade com que os líquidos I. D. s pode ser convertido para
localização física de informação, muitas mulheres podem estar preocupado.
+ machos pode estar em causa, bem como, dado as ameaças de morte
emitidos por, por exemplo, S. Boxx/Detweiler.
- como acontece, S. Boxx ameaçou-me, e eu fazer a minha casa
o número de telefone e o local é facilmente conhecido...mas eu estou
armado e pronto.

8.4.22. válvula de alívio de pressão: saber se pode fugir ou de cabeça para o
a fronteira e o não ser sobrecarregado com um passado

- talvez a alta taxa de reincidência é correlacionada com este
incapacidade de escapar...depois de um con, marcado para a vida
(certamente negado o acesso a empregos com altos salários)

8.4.23. impede ações judiciais, intimações, emaranhado jurídico
máquinas
8.4.24. Por Motivos De Negócios
+ Corporações podem fazer pedidos de suprimentos, informações, sem
tombamento sua mão
- a Disney compra de terras, através anônimo recortes (para
evite dirigir o preço maneira)
- ingredientes secretos (apocrifamente, Coca-Cola)
- evitar os "bolsos" síndrome citada acima
- para vencer o zoneamento e requisitos de licenciamento (por exemplo, um determinado
tipo de negócio não pode ser "permitido" em um escritório em casa,
assim, o proprietário terá que usar recortes para se esconder de
aplicadores)
- proteção de (e para) os empregadores
+ empregados de empresas podem ter mais do que apenas
reivindicamos a sua vista não são aqueles do empregador
- por exemplo, um racista post poderia expor a IBM para a aplicação de sanções,
encargos
+ assim, muitos funcionários podem ter para continuar a isolar seus
identidades
- blanc@microsoft.com é agora
blanc@pilão.com...coincidência?
+ clandestinidade empregados (original preocupação com Preto Net
e AMIX)
- os empregadores podem ter todos os tipos de preocupações, daí a necessidade
para os funcionários para ocultar suas identidades
- observe que este interects com o licenciamento e zoneamento
aspectos
- editores de serviço-prividers
+ Necessários para Certos Tipos de Reputação Baseado em Sistemas de
+ um respeitado cientista pode querer flutuar uma especulativo
ideia
- e ser capaz de comprovar mais tarde ele foi, de fato, sua idéia
8.4.25. Proteção contra retaliação
- denúncia
+ organizando boicotes
- (em uma era de leis que regulam a liberdade de expressão, e "SLAPP"
ações judiciais)
+ o visto de pessoas (Cantwell e Siegel) ameaçando aqueles que
comentário com ternos
- o escritório de advocacia que apresentou a 5.000 grupos....também levanta
o problema, novamente, do qual o Líquido deve ser subsidiado
- participação em fóruns públicos

+ como uma pessoa ameaçou com uma ação judicial sobre a sua Usenet
comentários de colocá-lo:
- "E agora eles estão me ameaça. Simplesmente porque eu abertamente
expresso a minha opinião sobre a sua extremamente irresponsável
comportamento. De qualquer forma, eu já cancelado o artigo
a partir do meu site e me publicamente appologize para publicando-a em
o primeiro lugar. Estou com medo :) eu tirar todas as minhas palavras para trás.
Vai usar o anônimo serviço da próxima vez :)"
8.4.26. Prevenção De Acompanhamento, Vigilância, Dossiê Sociedade
+ evitando dossiers em geral
- muitos dossiers que está sendo mantido; o anonimato permite que as pessoas
pelo menos segurar a onda um pouco
+ de recrutamento, procura de emprego, onde a revelar a identidade de uma pessoa
não é sempre uma boa ideia
- alguns headhunters estão trabalhando para um empregador atual!
- dossiês
8.4.27. Alguns Exemplos de Cypherpunks Lista
+ S, Boxx, aka Sue D. Nym, Pablo Escobar, O Carrasco,
e an12070
- mas, Lourenço, Detweiler por qualquer outro nome
+ ele deixou escapar o seu pseudônimo-o verdadeiro nome links de várias maneiras
- dicas de estilo
- menção de coisas que só o "outro" era provável que
ouviu
+ sysops reconheceu certas ligações
- *não* * * Julf, embora Julf presumivelmente sabia a identidade
de "an12070"
+ Pr0duct Cypher
- Jason Burrell aponta: "Tome Pr0duct Cypher, para
exemplo. Muitos acreditam que o que ele está fazendo(*) é um
Coisa boa, e eu vi ele/ela usando o Cypherpunk
remetentes para esconder sua identidade....* Se você não
sabe, o (s)ele é a pessoa que escreveu PGPTOOLS, e um hack
por PGP 2.3 para descriptografar mensagens escritas com 2.6. Eu
suponha (s)ele está fazendo isso de forma anônima, devido à ITAR
regulamentos." [J. B., 1994-09-05]
+ Unicórnio Negro
- É o pseudônimo de um Washington, D.C. advogado (eu acho),
quem tem laços comerciais conservadoras banqueiros e
homens de negócios na Europa, especialmente Liechtenstein e
A suíça. Seu envolvimento com o grupo Cypherpunks
levou a adotar este pseudônimo.
- Ironicamente, ele entrou em uma batalha com S. Boxx/Detweiler

e ameaçou com ação judicial. Esta causa um pouco
instrutivo debate para ocorrer.

8.5. Untraceable E-Mail
8.5.1. A Idéia Básica de Remetentes
- As mensagens são criptografadas, envelopes, dentro de envelopes, assim
fazer o rastreamento com base na aparência externa impossível. Se
o reenvio de e-mails de nós manter o mapeamento entre as entradas e
saídas secretas, a "trilha" é perdida.
8.5.2. Por que é untraceable de correio de tão importante?
+ Tenha em mente que "untraceable mail" é o padrão
situação por correio normal, onde um selos de um envelope,
aplica um carimbo, e ela cai de forma anônima, em uma caixa de correio.
Não há registros são mantidos, nenhum endereço de retorno é necessário (ou
confirmada), etc.
- regional do carimbo postal mostra a área geral, mas não de origem
caixa de correio
+ Muitos de nós acreditamos que o atual sistema de anônimo
o email não seria "permitido", se apresentou hoje para a
primeiro tempo
- Serviço Postal, iria a procura personalizada de selos,
verificável endereços de retorno, etc. (não é infalível, ou
seguro, mas...)
+ Motivos:
- para evitar que os dossiês de que está em contato com quem está sendo
compilado
- para fazer contatos de um assunto pessoal
- muitos usos reais: a manutenção de pseudônimos, anônimos
contratos, protegendo negócios, etc.
8.5.3. Como fazer Cypherpunks remetentes de trabalho?
8.5.4. Como, em termos simples, pode me enviar email anônimo?
8.5.5. Chaum Digital de Mistura
- Como digital misturas de trabalho?
8.5.6. "São hoje, os remetentes seguros contra análise de tráfego?"
- A maioria não. Muitos chave de mistura digital funcionalidades estão faltando, e
as lacunas podem ser exploradas.
+ Depende de recursos utilizados:
Reordenação (por exemplo, de 10 mensagens em 10 de mensagens)
- Quantização para tamanhos fixos (mais diferentes tamanhos de dar
pistas)
- Criptografia em todas as fases (até o cliente, é claro)
- Mas, provavelmente, não, dado que a actual remetentes, muitas vezes, falta
recursos necessários para deter a análise de tráfego. Preenchimento é

duvidoso, lote muitas vezes não é feito em todas as (pessoas apreciam
velocidade, e muitas vezes downcheck remetentes que são "muito lento")
- Melhor ver hoje remetentes como experiências, como
protótipos.

8.6. Remetentes e Digital Misturas (Uma Grande parte!)
8.6.1. O que são remetentes?
8.6.2. Cypherpunks remetentes comparado com Julf do
+ Aparentemente longos atrasos são de montagem no penet reenvio de e-mails.
Reclamações sobre a duração de uma semana, atrasos, respondeu por:
- "Bem, ninguém é você parar de usar o excelente
série de cypherpunk remetentes, começando com um de cada
remail@vox.hacktic.nl. Esses remetentes bater o inferno fora
de anon.penet.fi gratuito. Quer mesmo dia ou, no pior dia seguinte
serviço de criptografia PGP permitido, de encadeamento e gateways
para a USENET." [Marcos Terka, O atraso normal para
anon.penet.fi?, alt.privacidade.anon-servidor, 1994-08-19]
+ "Como é grande a carga de Julf do reenvio de e-mails?"
- "Eu falei para Julf recentemente e o que ele realmente precisa é de
$750/mês e um fora de us $5000 para atualizar seu feed/máquina.
Eu em considerar a possibilidade do patrocínio (mas não
deixe que isso o impeça outras pessoas tentando).....Julf tem buuilt até
leal, confiante seguinte de mais de 100.000 pessoas e
6000 mensagens/dia. A atualização parece-lhe uma boa
idéia.....Sim, há outros remetentes. Vamos usá-los
se podemos e diminuir a carga sobre Julf." [Steve Harris,
alt.privacidade.anon-servidor, 1994-08-22]
- (Agora, se a deman no Julf do reenvio de e-mails é grande, parece
como uma grande oportunidade para implementar algum tipo de taxa-base de
sistema, para pagar por uma maior expansão. Sem dúvida, muitos de
os utilizadores teria de cair fora, mas essa é a natureza do
de negócios.)
8.6.3. "Como remetentes de trabalho?"
- (O MFAQ também tem algumas respostas.)
- Simplesmente, eles trabalham tirando um bloco de texto e entrada
procurando instruções sobre onde enviar o restante
bloco de texto, e o que fazer com ele (a descriptografia, atrasos,
a postagem, etc.)
+ Alguns remetentes pode processar o Unix programa de email(s) para as saídas
diretamente, operando em cabeçalhos de email
- nomes de programas...
+ Eu acho que o "::" formato de Eric Hughes veio com sua
primeiros dias olhando para este acabou por ser um verdadeiro

ganhar (talvez comparável à de John McCarthy decisão de usar
parenthesized s-expressões Lisp?).
- permite arbitary encadeamento, e todas as mensagens de correio que
tem texto no padrão ASCII--que é de todos os utentes, eu
acredito que, em seguida, pode utilizar o Cypherpunks remetentes
8.6.4. "O que são alguns usos de remetentes?"
- Thi é principalmente respondeu em outras seções, com destaque para os
usa do anonimato e digital pseudônimos: remetentes são de
curso de habilitação de tecnologia de anonimato.
+ usando remetentes para a folha de análise de tráfego
- Um interessante comentário de alguém que não faz parte de nosso
grupo, na discussão da proposta para desligar reino UNIDO
computadores da Usenet (devido as leis Britânicas sobre
a calúnia, sobre a pornografia, por exemplo): "PGP esconde o
de destino. Os remetentes descartar a origem da informação. Mais
paranoid remetentes introduzir um atraso aleatório no reenvio
a folha de análise de tráfego. Você ficaria surpreso o que pode ser
feito :-).....Se você usar uma cadeia, em seguida, o primeiro reenvio de e-mails
sabe quem você é, mas o destino é criptografado. O
última reenvio de e-mails sabe o destino, mas não é possível saber o
de origem. Intermediários nem sei." [Malcom
McMahon, JANET (reino UNIDO) a proibição de USENET?, comp.org.fep.falar,
1994-08-30]
- Então, a palavra está se espalhando. Note a ênfase em Cyphepunks-
tipo de remetentes, ao contrário Julf estilo anônimo
serviços.
+ opções para distribuir mensagens anônimas
+ através de remetentes
- a abordagem convencional
- vantagens: o destinatário não precisa fazer nada especial
- desvantagens: é isso--destinatário pode não acolher o
mensagem
+ para um grupo de notícias
- um tipo de mensagem piscina
- vantagens: mundo dist
- para um site de ftp ou Web-site acessível
- uma lista de discussão
8.6.5. "Por remetentes necessário?"
+ Hal Finney resumiu as razões bem em uma resposta de volta
no início de 1993.
- "Há várias vantagens, fornecida pela
remetentes anônimos. Um dos mais simples e menos
controverso seria a derrota de análise de tráfego na

ordinária de e-mail.....Duas pessoas que desejam se comunicar
particular pode usar o PGP ou algum outro sistema de criptografia para
ocultar o conteúdo de suas mensagens. Mas o fato de que
eles estão se comunicando uns com os outros ainda é visível
para muitas pessoas: os administradores em seus sites e, possivelmente, em
intervenientes locais, bem como vários net bisbilhoteiros. Ele
seria natural para lhes desejo um montante adicional
de privacidade, que teria de disfarçar que eles foram
comunicando-se com o bem como o que eles estavam dizendo.

"Remetentes anônimos tornar isso possível. Por encaminhamento
correio entre si através de remetentes, enquanto ainda
identificando-se na mensagem (criptografada)
conteúdo, mesmo que eles tenham mais privacidade das comunicações que
com criptografia simples.

"(O Cypherpunk visão inclui um mundo em que
literalmente centenas ou milhares de tal remetentes
operar. E-Mail pode ser conduzida através de dezenas de estes
serviços, misturando-se com outras dezenas de milhares de
mensagens, re-criptografados em cada passo do caminho. Este
deve fazer a análise de tráfego praticamente impossível. Por
envio periódico de manequim mensagens que acabou de cair
até em algum passo, as pessoas podem até disfarçar _when_ eles são
comunicação.)" [Hal Finney, 1993-02-23]

"O mais controverso visão associada com anônimos
remetentes é expressa em tais histórias de ficção científica como
"Nomes verdadeiros", por Vernor
Vinge, ou "Ender do Jogo", de Orson Scott Card. Estes
retratam o mundo em que as redes de computadores estão em
utilização generalizada, mas em que muitas pessoas escolhem para
participar através de pseudônimos. Desta forma, eles podem
tornar impopular argumentos ou participar de franziu a testa.-após
transações sem que suas atividades estão sendo vinculados
suas verdadeiras identidades. Ele também permite que as pessoas a desenvolver
reputação com base na qualidade de suas idéias, ao invés de
de seu trabalho, riqueza, idade ou condição social." [Hal Finney,
1993-02-23]
- "Outras vantagens dessa abordagem incluem a sua extensão a
eletrônica de transações on-line. Já hoje em dia, muitos
são mantidos registros de nossos negócios financeiros - cada vez que
comprar um item sobre o telefone usando um cartão de crédito, o

é registrado pela empresa de cartão de crédito. Em tempo, ainda mais
este tipo de informação pode ser recolhida e, possivelmente,
vendido. Um Cypherpunk visão inclui a capacidade de se envolver
em transações de forma anônima, o uso de "dinheiro digital", que
não seria rastreáveis para os participantes. Particular
para a compra de "soft" de produtos, como música, vídeo e software
(que todos podem ser entregues através da internet, eventualmente), ele
deve ser possível para envolver em tais transações
de forma anônima. Portanto, esta é outra área onde anónimo-mail
é muito importante." [Hal Finney, 1993-02-23]
8.6.6. "Como eu faço para usar um reenvio de e-mails?"
+ (Nota: reenvio de e-mails instruções são postados _frequently_. Lá
é de nenhuma maneira que eu possa manter-se atualizado com eles aqui. Consulte a
várias listas de discussão e o dedo ou sites que usam a Web
docs, para encontrar as instruções mais atual, chaves, uptimes,
etc._
+ Raph Levien dedo site é muito impressionante:
+ Raph Levien, tem um impressionante utilitário que executa o
remetentes e relatórios de uptime:
- dedo remailer-list@kiwi.cs.berkeley.edu
- ou use a Web em
http://www.cs.berkeley.edu/~raph/remailer-list.html
- Raph Levien também tem um reenvio de e-mails de encadeamento de script
ftp://kiwi.cs.berkeley.edu/pub/raph/premail-
0.20.tar.gz
+ Chaves para remetentes
- remailer-list@chaos.bsu.edu (Mateus Ghio mantém)
+ "Por remetentes operar somente em cabeçalhos e não o corpo
de uma mensagem? Por que não são assinaturas retirados por
remetentes?"
- "A razão para construir mensagens que fielmente passar o
todo o corpo de
a mensagem, sem qualquer tipo de alteração, é que ele
permite que você
enviar a QUALQUER organismo através do que mailer e confiar em sua
fiel chegada ao
o destino." [John Gilmore, 93-01-01]
- O "::" formato especial é uma exceção
- Bloco assinatura no final da mensagem de órgãos
especificamente deve _not_ ser removido, mesmo que este
pode causar violações de segurança se eles são acidentalmente deixados para
quando não se pretende. A tentativa de tira-sigs, que
vem em muitos sabores, seria um pesadelo e que poderia

tira outras coisas, também. Além disso, algumas pessoas podem querer um
sig ligado, mesmo para uma mensagem criptografada.
- Como de costume, ninguém é, naturalmente, livre para ter um reenvio de e-mails
que munges mensagem de órgãos como lhe aprouver, mas eu esperar
tais remetentes vai perder clientes.
- Outra possibilidade é uma outra forma especial, tais como
"::Final", que poderia ser usado para delimitar o bloco a ser
remailed. Mas vai ser difícil a obtenção de um tal de "babado"
aceite.
+ "Como remetentes lidar com linhas de assunto?"
- De várias maneiras. Alguns ignorá-lo, alguns preservá-lo, alguns
até pode aceitar instruções para criar uma nova linha de assunto
(talvez na última reenvio de e-mails).
- Há razões para não ter uma linha de assunto propagadas
através de uma cadeia de remetentes: ele marca a mensagem e
portanto faz análise de tráfego trivial. Mas há também
motivos para se ter uma linha de assunto--torna mais fácil a
destinatário-e por isso estes esquemas para adicionar uma linha de assunto
existem.
+ "Pode apelidos ou pseudônimos ser usado com os Cypherpunks
remetentes?"
- Certamente assinado digitalmente IDs são utilizados (Pr0duct Cypher,
por exemplo), mas não apelidos preservados em campos
o remailing e-mail-para-Usenet gateways.
- Isso poderia ser adicionado para os remetentes, como um extra
de campo. (Eu ouvi os campos de email que são mais tolerantes a
adicionado coisas que o Netnews campos, tornando-mail-para -
Notícias gateways perder o extra-campos.)
+ Alguns reenvio de e-mails de sites de apoio-los
- "Se você quer um alias atribuído no vox.hacktic.nl, um
apenas precisa enviar algum e-mail vazio para
<ping@vox.hacktic.nl> e o endereço de e-mail foi enviar
a partir será inculded na base de dados.....Desde
vox.hacktic.nl é um UUCP nó a resposta pode demorar
algum tempo, geralmente algo como 8 a 12 horas."[Alex
de Joode, <usura@vox.hacktic.nl>, 1994-08-29]
+ "O que fazer remetentes fazer com as várias partes de
mensagens? Eles enviar o material incluído depois de criptografada
bloco? Deve-se? O que sobre cabeçalhos?"
+ É evidente que existem muitas abordagens que podem ser tomadas:
- Enviar tudo como está, deixando para o remetente
certifique-se de que nada incriminador é esquerda
- Fazer certas escolhas

- Eu sou a favor enviar tudo, a menos que especificamente autorizado não
para, como isto faz com que menos pressupostos sobre a intenção
formato de mensagem e, assim, permite maior flexibilidade na
a concepção de novas funções.
+ Por exemplo, este é o que Mateus Ghio tinha para dizer
sobre o seu reenvio de e-mails:
- "Tudo após a mensagem criptografada é passado
ao longo da claro. Se você não quer isso, você pode
removê-lo usando o cutmarks recurso com a minha reenvio de e-mails.
(Também, remail@extropia.wimsey.com não acrescentar o
texto após a mensagem criptografada.) A razão para isto
é o que permite respostas anônimas. Eu posso criar um
pgp mensagem para um reenvio de e-mails que serão entregues para
a mim mesmo. Eu enviar-lhe o PGP mensagem, você pode acrescentar alguns
texto para ele, e enviá-lo para o reenvio de e-mails. O reenvio de e-mails
descriptografa e remails para mim, e eu a obter o seu
mensagem. [M. G., alt.privacidade.anon-servidor, 1994-07-03]
8.6.7. Reenvio De E-Mails De Sites
- Não há uma central, administrador de sites, é claro, para um
variedade de ferramentas são as melhores formas de desenvolver a própria
lista de sites. (Muitos de nós, eu suspeito, basta resolver em um
dezenas de nossos favoritos. Isso vai mudar como centenas
de remetentes aparecer; é claro, vários scripts de programas
será utilizado para gerar as trajetórias, lidou com a
aninhado criptografia, etc.)
- Os grupos de notícias alt.privacidade.anon-servidor, alt.segurança.pgp,
etc. muitas vezes relatório mais recente de sites, ferramentas, etc.
+ Software para Remetentes
+ Software para executar um reenvio de e-mails site podem ser encontradas em:
- soda.csua.berkeley.edu em /pub/cypherpunks/reenvio de e-mails/
- chaos.bsu.edu em /pub/cypherpunks/reenvio de e-mails/
+ Instruções para a Utilização de Remetentes e servidores de chaves
+ sobre como usar os servidores de chaves
- "Se você tiver acesso à World Wide Web, consulte este
URL: http://draco.centerline.com:8080/~franl/pgp/pgp-
os servidores de chaves.html" [Fran Litterio, alt.segurança.pgp, 1994-
09-02]
+ Identificação De Reenvio De E-Mails De Sites
+ dedo remailer-list@chaos.bsu.edu
- retorna uma lista de remetentes ativo
- para informação mais completa, teclas e instruções,
dedo remailer.help.all@chaos.bsu.edu
- gopher://, o caos.bsu.edu/

+ Raph Levien, tem um impressionante utilitário que executa o
remetentes e relatórios de uptime:
- dedo remailer-list@kiwi.cs.berkeley.edu
- ou use a Web em
http://www.cs.berkeley.edu/~raph/remailer-list.html
- Raph Levien também tem um reenvio de e-mails de encadeamento de script
ftp://kiwi.cs.berkeley.edu/pub/raph/premail-0.20.tar.gz
+ Reenvio de e-mails ping
- "Eu tenho escrito e instalado um reenvio de e-mails ping script
que
coleta informações detalhadas sobre os recursos e reenvio de e-mails
confiabilidade.

Para utilizar, basta dedo reenvio de e-mails-
lista@kiwi.cs.berkeley.edu

Há também uma versão Web da mesma informação, em:
http://www.cs.berkeley.edu/~raph/remailer-list.html"
[Raph Levien, 1994-08-29]
+ Sites que estão em baixo??
- tamsun.tamu.edu e tamaix.tamu.edu
8.6.8. "Como faço para configurar um reenvio de e-mails no meu site?"
- Isso não é algo para o usuário casual, mas é, certamente,
possível.
- "Gostaria que alguém seja capaz de me ajudar a instalar o reenvio de e-mails
scripts de arquivos? Eu não tenho nenhuma experiência Unix e
ter *não* idéia de por onde começar. Eu ainda não sei se o root
o acesso for necessário para estes. Qualquer ajuda seria
apreciado." [Robert Luscombe, 93-04-28]
- Sameer Parekh, Mateus Ghio, Raph Levien ter tudo escrito
manual de instruções....
8.6.9. "Como a maioria dos Cypherpunks remetentes escrito, e com o que
ferramentas?"
- como scripts que manipular os ficheiros de correio, substituindo
cabeçalhos, etc.
- Perl, C, TCL
- "O cypherpunks remetentes de ter sido escrito em Perl, que
facilita a experimentação, ensaio de novas interfaces.
A ideia pode ser migrar para C, eventualmente, para a
eficiência, mas durante a fase experimental podemos querer
para experimentar novas ideias, e é mais fácil modificar um Perl
script de um programa C." [Hal Finney, 93-01-09]
- "Eu aprecio o cypherpunks coisas, mas perl é ainda

não muito
padrão amplamente utilizado ferramenta, e não cada um de nós deseja
aprender a
prós e contras de um outro idioma... Assim que eu me aplaudir
a C
versão..." [Johan Helsingius, "Julf," 93-01-09]

8.6.10. Lidar com reenvio de e-mails Abuso

+ A Batata Quente
- um reenvio de e-mails que está sendo utilizado muito fortemente, ou suspeitos
abuso, pode optar por distribuir sua carga para outros
remetentes. Geralmente, ele pode, em vez de remailing para o
próximo site, sites de sua escolha. Assim, ele pode
reduzir os holofotes sobre ele e também aumentar a cobertura
tráfego por dispersão alguma porcentagem de sua tráfego
outros sites (nunca reduz o seu trânsito, apenas diminui
o foco sobre ele).
+ Ataques de congestionamento
- ataques de negação de serviço
- gosto soprando apitos em eventos desportivos, para confundir o
ação
- DC-Redes, perturbação (disruptionf da DC-Redes por inundações
é um problema semelhante ao rompimento dos remetentes por
correio bombas)
+ "Como pode remetentes lidar com o abuso?"
- Diversas reenvio de e-mails operadores de ter encerrado a sua
remetentes, porque cansei de lidar com
os problemas, ou porque os outros ordenou.
- Fonte de nível de bloqueio
- Pago mensagens: pelo menos isso faz com que os agressores _pay_ e
pára de certos tipos de spam/bombardeio de ataques.
- Em matéria de desreguladores são tratadas de forma anônima formas no Chaum do DC-
Net esquemas; pode ser uma maneira de usar isso aqui.
+ Karl Kleinpaste foi um pioneiro (cerca de 1991-2) de remetentes.
Ele tornou-se desencantado:
- "Há 3 sites lá fora, que têm o meu software:
anon.penet.fi gratuito, tygra, e uiuc.edu. Eu tenho filosófica
desacordo com o "alcance universal" política de
anon.penet.fi (cujo código é agora um longa-independente de tensão
a partir do software original que eu dei Julf -- de fato, por agora
pode ser uma reescrita completa, eu simplesmente não sei);
....Muito francamente, depois de ter tentado executar anon servidores por duas vezes,
e ter tido tanto cair devido a real jurídica
dificuldades, eu não confio em pessoas com mais."

[Karl_Kleinpaste@cs.cmu.edu, alt.privacidade.anon-servidor,
1994-08-29]
- ver discussões em alt.privacidade.anon-servidor para saber mais sobre
seus problemas legais com remetentes, e por que ele fechou sua
para baixo
8.6.11. Gerações de Remetentes
+ Primeira Geração de reenvio de e-mails Características--Agora (desde 1992)
- Scripts Perl, simples de processamento de cabeçalhos de criptografia
+ Segunda Geração De Reenvio De E-Mails Características--Talvez 1994
- digital postagem de alguma forma (talvez simples ou de cupons de
"selos")
- mais flexibilidade no manuseio de exceções
- objectos de correio pode dizer reenvio de e-mails que configurações usar
(atrasos, latência, etc.(
+ De Terceira Geração Reenvio De E-Mails Características--1995-7?
- a negociação do protocolo
+ Chaum-como "mistura" características
- resistente a adulterações módulos (reenvio de e-mails de software é executado em um
ambiente selado, que não são visíveis para o utilizador)
+ De Quarta Geração Reenvio De E-Mails Características--1996-9?
- Quem sabe?
- Agent-based (Telescript?)
- DC-Net-based
8.6.12. Reenvio de e-mails de identidade garantia
+ poderia ter algumas usa...
- o que é um incentivo qualquer um teria?
- destinatários poderia origem-bloquear qualquer reenvio de e-mails que não
tem algum meio de lidar com grave abuso...perfeito
solução de mercado livre
- também pode ser obrigatória
8.6.13. Reenvio De E-Mails Características
+ Existem dezenas de variações propostas, truques, e
métodos que pode ou não pode adicionar ao geral de reenvio de e-mails
de segurança (entropia, confusão). Estes são muitas vezes discutidas em
a lista, um de cada vez. Alguns deles são:
+ Usando a si mesmo como um reenvio de e-mails nó. Rota do tráfego
através do próprio sistema.
- mesmo se todos os outros sistemas estão comprometidos...
- Atrasos aleatórios, acima de tudo o que é necessário para atender
reordenação de requisitos
- MIRVing, enviando um pacote em várias partes
- A criptografia é, claro, uma característica primordial.
+ Digital postagem.

- Não tanto um recurso como um incentivo/de persuasão para obter
mais remetentes e apoiá-los melhor.
+ "O que são características de um reenvio de e-mails de rede?"
- Um grande número de características que foram consideradas; alguns são
derivados de outros, mais recursos básicos (por exemplo, "aleatória
atrasos" não é uma característica básica, mas é uma proposta de forma
de alcançar a "reordenação", que é o que é realmente
necessário. E a "reordenação" é apenas o caminho para se atingir a
"decorrelation" de mensagens de entrada e saída).
+ A "Mistura Ideal" é que vale a pena considerar, apenas como o "ideal
op amp" é estudada por engenheiros, independentemente de
nunca pode ser construído.
- uma caixa preta que decorrelates de entrada e de saída
pacotes para algum nível de difusão
- à prova de violação, em que o mundo exterior não pode ver o
processo interno de decorrelation (Chaum imaginou
à prova de violação ou adulteração de responder circuitos de fazer
o decorrelation)
+ Características do Mundo Real Misturas:
+ Decorrelation de entrada e saída de mensagens. Este
é o recurso mais básico de qualquer mistura ou reenvio de e-mails:
obscurecendo a relação entre qualquer mensagem de entrar
a mistura e qualquer mensagem deixando a mistura. Como este é
alcançar é o que a maioria dos recursos aqui são todos
sobre.
- "Difusão" é obtido por loteamento ou atrasar
(perigo: baixo volume de tráfego derrotas simples, fixo
atrasos)
- Por exemplo, em algum período de tempo, 20 mensagens de introduzir um
nó. Em seguida, 20 ou assim (pode ser menos, pode ser
mais...não há nenhuma razão para não adicionar mensagens, ou
jogar fora alguns) mensagens de deixar.
+ De criptografia deve ser apoiada, mais que o decorrelation
é facilmente derrotado por uma simples inspeção de pacotes.
- criptografia de chave pública, claramente, é o preferido (mais
as chaves estão disponíveis fora)
- para a frente de criptografia, usando o D-H abordagens, é uma útil
ideia a explorar, com teclas descartados após
de transmissão....assim fazendo intimações problemática
(isto tem sido usado com seguro de telefones, por exemplo).
+ Quanitzed tamanhos de pacotes. Obviamente, o tamanho de um pacote
(por exemplo, 3137 bytes) é uma forte sugestão como a mensagem de
identidade. A quantificação para um tamanho fixo destrói essa sugestão.

+ Mas desde que algumas mensagens podem ser pequenos e grandes,
um prático compromisso é, talvez, a quantificação de um
de vários padrões:
- pequenas mensagens, por exemplo, 5K
- média de mensagens, por exemplo, 20K
- grande de mensagens....tratados de alguma forma (talvez split
de segurança, etc.)
- Mais análises são necessárias.
+ Reputação e o Serviço
- Quanto tempo no mercado?
- Política de registo? As mensagens são registrados?
- a expectativa de funcionamento conforme indicado
+ Os Objetivos Básicos de reenvio de e-mails Usar
+ decorrelation da direcionado para dentro e saída de mensagens
- indistinguibilidade
+ "remailed as mensagens sem cabelo" (desculpas para o
buraco negro fãs lá fora)
- não distinguir charateristics que pode ser usado para
fazer correlações
- sem "memória" de aparência anterior
+ isso significa de tamanho de mensagem de preenchimento para quantizada tamanhos,
normalmente
- quantas diferentes tamanhos depende de uma série fo coisas,
como o tráfego, os tamanhos de mensagens, etc.
+ De criptografia, de curso de
- PGP
- caso contrário, as mensagens são trivialmente distinguíveis
+ De quantização ou Preenchimento: Mensagens
- acolchoado em tamanhos padrão, ou pontilhada em tamanho para ocultar
oringinal tamanho. Por exemplo, 2K típico de curto
mensagens, 5K típicas da Usenet artigos, e 20K para
artigos longos. (Mensagens muito mais difícil de se esconder em
um mar de muito menor mensagens, mas outras possibilidades
existem: atrasar a longo mensagens de até N de longo
mensagens tem sido acumulado, dividindo-as mensagens
em partes menores, etc.)
+ "O que são os quanta de remetentes? Que é, quais são as
preferencial tamanhos de pacotes para remailed mensagens?"
- No curto prazo, agora, o remailed tamanhos de pacote são
muito bonito o que eles começaram a ser, e.g, 3-6KB ou
então. Alguns remetentes podem pad para níveis quantizados, ou seja,
5K ou 10K ou mais. Os níveis não foram resolvidos
em.

- No longo prazo, eu suspeito muito menor pacotes
ser selecionado. Talvez na granularidade de pacotes ATM.
"ATM Remetentes" são susceptíveis de vir. (Isto altera
a natureza do tráfego de análise um pouco, como a _number_ de
remailed pacotes aumenta.
- Um dissidente argumento: redes ATM não dar remetente
o controle sobre os pacotes...
- Seja o que for, eu acho que os pacotes vão ficar menor, e não maior.
Questões interessantes.
- "Baseado em Hal números, gostaria de sugerir uma razoável
quantização para os tamanhos de mensagem ser um pequeno conjunto de
geometricamente crescente de valores, nomeadamente, 1K, 4K, 16K,
64K. Em retrospecto, parece o óbvio
a quantização, e não progressões aritmética." [Eric
Hughes, 1994-08-29]
- (Eudora engasga em 32K, e então divide as mensagens em cerca de
25K, para deixar espaço para comentários sem mais
divisão. Tais considerações de ordem prática pode ser importante
para considerar.)
+ - Mail De Retorno
- Um problema complicado. Pode não ter uma solução simples.
+ Abordagens:
- Pós mensagem criptografada para uma piscina. Remetente (que forneceu
a chave para usar) é capaz de recuperar de forma anônima pelo
a natureza de piscinas, e/ou afixação pública.
+ Retorno envelopes, usando algum tipo de procedimento para
garantir o anonimato. Uma vez que o software é, por natureza, nunca
seguro (sempre pode ser desmontada), as questões são
complicada. A segurança pode ser obtido através da organização de
com os remetentes no caminho de retorno para fazer determinadas
coisas para determinadas mensagens.
- remetente envia instruções para remetentes sobre como
tratar as mensagens de determinados tipos de
- o destinatário que está respondendo não pode deduzir o
identidade, porque ele não tem acesso ao
instruções do remetentes de ter.
- Pense nisso como Alice envio para Bob enviar para
Charles....envio para Zeke. Zeke envia uma resposta de volta
para Yancy, que tem instruções para enviar esta de volta para
Xavier, e assim por diante até a cadeia. Só se Bob,
Charles, ..., Yancy conspirar, pode o mapeamento do
inverter o sentido de ser deduzido.
- São estes esquemas complicados? Sim. Mas assim são muito

outros protocolos, tais como a obtenção de tipos de letra a partir de uma tela
para uma impressora a laser
+ Reordenação das Mensagens é Crucial
+ latência ou fan-out em remetentes
+ muito mais importante do que o "atraso"
- fazer alguns cálculos!
+ o canard sobre "latência" ou atraso continua vindo até
- um "atraso" de X não é nem necessária nem suficiente
para alcançar reordenação (pense nisso)
- essencial para a remoção de tempo de correlação de informações,
para remover uma "marca distintiva" ("ideal remailed
as mensagens têm nenhum cabelo")
+ A importância de como você vai pagar, digital postagem
+ padrão do mercado
- os mercados são como scarece os recursos são alocados
- reduz o envio de spam, a sobrecarga de bombardeio
- congestionamento de preços
- incentivos para a melhoria
+ mecanismos de feedback
- da mesma maneira que os restaurantes consulte impactos rapidamente
- aplica-se a outros de criptografia usos, além de remetentes
+ Diversos
- por ter um de nós, ainda garante segurança
(verdadeiro, que os conspiradores de todos os outros nós podem causar
a rastreabilidade, mas como uma conspiração é caro e seria
ser revelado)
+ público "lançamento", a idéia é muito atraente: em nenhum momento
o último nó de saber quem é o próximo nó vai ser...todos os
ele sabe que é uma chave pública para esse nó
+ assim como o nó seguinte na linha de receber a mensagem,
curto de ler todas as mensagens?
- primeiro, a segurança não é muito comprometida com a classificação de
as postagens públicas por algum tipo de ordem definida pelo
cabeçalho (por exemplo, "Fred" é uma abreviação para alguns P-K,
e, portanto, o destinatário sabe que olhar na
Fs...obviamente ele lê mais do que apenas o Fs)
+ mensagens de saída pode ser "broadcast" (enviados para muitos de nós,
por um literal ou difusão pública de lançamento, ou por
aleatoriamente pegando muitos de nós)
- este "quadro negro" do sistema significa que nenhum ponto a ponto
a comunicação é necessária
+ Timed-release estratégias
+ criptografar e, em seguida, solte a tecla posterior

- "innocuously" (como?)
- através de um serviço remailing
- DC-Net
- através de uma garantia de serviço ou um advogado (mas pode o advogado entrar em água quente para liberar a chave para controverso de dados?)
- com uma série de tais versões, a chave pode ser "difundida"
- algumas empresas podem se especializar em timed-release, tal como oferecendo um P-K com a chave privada a ser lançado algum tempo depois
- em uma ecologia de cryptoid entidades, isso vai aumentar os graus de liberdade
+ isso reduz a responsabilidade legal do retransmitters...com precisão podem alegar que eles estavam apenas de passagem de dados, que não havia nenhuma maneira que eles poderia saber o conteúdo dos pacotes
- é claro que eles já podem reclamar isso, devido ao criptografados natureza
+ One-Shot Remetentes
- "Você pode ser um anônimo endereço de mg5n+getid@andrew.cmu.edu. A cada vez que você solicitar uma anon endereço, você tem um diferente. Você pode obter como muitos como você gosta. Os endereços não expiram, no entanto, talvez por isso não é o ideal 'one-shot' do sistema, mas permite que responde sem estabelecer uma ligação com o real" nome/endereço' ou a qualquer um dos seus outros posts/nyms." [Mateus Ghio, 1994-04-07]

8.6.14. Coisas Necessárias em Remetentes

+ retorno de receitas
- Rick Busdiecker observa que "A idéia de um Retorno-Recepção-Para: campo tem sido ao redor por um tempo, mas a semântica nunca foi preso. Alguns daemons mailer gerar respostas o que significa que os bits foram entregues." [R. B., 1994-08-08]
+ instruções
- agentes, daemons
- os procedimentos por negociação
+ digital postagem de suma importância!!
- resolve muitos problemas, e incentiva remetentes
+ estofamento
+ de preenchimento para tamanhos fixos

- preenchimento fixo potências de 2 aumentaria a média
mensagem de tamanho por cerca de um terço
- lotes de remetentes
- vários jursidictions
- robustez e consistência
+ em execução no hardware seguro
- não logs
- não há monitoramento por operador
- limpeza de todos os arquivos temporários
- instanciado rapidamente, de uma forma fluida
- melhor randomização de remetentes

8.6.15. Diversos Aspectos de Remetentes

+ "Como muitos reenvio de e-mails de nós são realmente necessários?"
- Nós nos esforçamos para obter como muitos como possível para distribuir o
processo para muitas jurisdições, e com muitos opeators.
- Curiosamente, tanto teórica difusividade pode ocorrer com
um único reenvio de e-mails (levando-se em centenas de mensagens e
o envio de uma centena de, por exemplo) como com muitos
remetentes. A nossa intuição é, acho eu, que muitos remetentes
oferecer melhores difusividade e melhor se esconder. Por que isso é
então (se for) precisa de mais cuidado para o pensamento do que eu vi
feito até então.
- Em um meta-nível, nós pensamos vários remetentes diminui a
chance de ser comprometido (este, no entanto, não é
diretamente relacionadas com a difusividade de um reenvio de e-mails de rede-
-importante, mas não diretamente relacionados).
- (By the way, um tipo de sneaky ideia é tentar sempre
declarar a si mesmo para ser um reenvio de e-mails. Se as mensagens foram
de alguma forma, remonta à própria máquina, pode
afirmação: "Sim, eu sou um reenvio de e-mails." Em princípio, poderia ser
a única reenvio de e-mails no universo e ainda tem alta
o suficiente difusão e confusão. Na prática, ser o
só reenvio de e-mails seria muito perigoso.)
+ De difusão e confusão em redes de reenvio de e-mails
+ De considerar um único nó, com uma mensagem de entrada, e
duas mensagens de sair; esta é, essencialmente, o menor
"reenvio de e-mails op"
- A partir de uma prova de ponto de vista, qualquer mensagem de saída
pode ser a
- e ainda nem pode ser provado
- Agora imagine essas duas mensagens que estão sendo enviadas através de 10
remetentes...sem adicional de confusão é adicionado...por quê?
- Então, com 10 mensagens gong em uma cadeia de 10 remetentes,

se 10 de deixar...
- O efeito prático de N remetentes é garantir que
comprometer de alguma fração de não destruir
segurança geral
+ "O que fazer remetentes fazer com misaddressed e-mail?"
- Depende do site. Alguns operadores enviam notas
(o que se faz com preocupação), alguns apenas descartar
com defeito-mail. Este é um fluido área. Pelo menos um
reenvio de e-mails (wimsey) pode postar mensagens de erro uma mensagem
piscina--esta idéia pode ser generalizada para fornecer "entrega
recibos" e outros comentários.
O Ideal de mistura, a la Chaum, presumivelmente descartar
mal-formado mail, embora os agentes podem existir para
prescreen e-mail (não obrigatório agentes, é claro, mas
voluntariamente-selecionado agentes)
- Como em tantas áreas, a legislação não é necessário, basta
anúncio de políticas, a escolha pelos clientes, e o
reputação de reenvio de e-mails.
- Um bom motivo para ter robusta geração de correio em um
própria máquina, de modo a minimizar tais problemas.
+ "Pode NSA monitor de remetentes? Têm eles?"
+ Certamente eles _can_ de várias maneiras, directamente,
o monitoramento de tráfego de rede ou indiretamente. Se eles _do_
é desconhecido.
- Houve vários rumores ou falsificações, alegando
que NSA é a rotina de vinculação IDs anônimos para real IDs
no penet reenvio de e-mails.
+ Cypherpunks remetentes são, se usado corretamente, mais
seguro em aspectos fundamentais:
- muitos deles
- não usado persistentes, atribuído IDs
- suporte para encriptação: de entrada e de saída
mensagens olhar completamente diferente de
- lote, estofamento, etc. suporte
- E corretamente executado remetentes dificultará/difundir o
a conexão entre a entrada e saída de mensagens--o
principal ponto de reenvio de e-mails!
+ O uso de mensagem de piscinas para relatório de erros de reenvio de e-mails
- Um bom exemplo de como a mensagem de piscinas pode ser utilizado para
denunciar anonimamente coisas.
- "O wimsey reenvio de e-mails tem um engenhoso método de retornar
mensagens de erro de forma anônima. Especificar um assunto no
mensagem enviada wimsey que seja relevante para você,

mas não identificar você (como um conjunto de letras aleatórias).
Esse assunto não aparece no remailed mensagem.
Em seguida, assine a lista de discussão

erros-request@extropia.wimsey.com

enviando uma mensagem com o Assunto assinar. Você vai
receber uma msg
para TODOS os erros detectados nas mensagens de entrada e de TODOS os
mensagens devolvidas." [anônimo, 93-08-23]
- É claro que a leitura de anúncios classificados com alguns
mensagem enigmática significativo para você sozinho. E mais
importante, untraceable para você.
+ pode haver papel para diferentes tipos de remetentes
- aqueles que suportam a encriptação, aqueles que não
+ como muitos de fora dos EUA possível de países
- especialmente para o *último* - hop, para evitar problemas de intimação
- primeira-classe de remetentes que remail *qualquer* endereço
+ remetentes que só remail para *outros remetentes*
- útil para os tímidos, para aqueles com suporte limitado,
etc.
-
+ "Deve-mail fingindo ser usado como parte de reenvio de e-mails
estratégia?"
- "1. Se você falsos mail falando SMTP diretamente, o IP
nome de domínio ou endereço do site de tomada de saída
conexão será exibida em um campo Recebido no cabeçalho
em algum lugar."

"2. Falso mail por meios tortuosos é geralmente desaprovado.
Não há necessidade de se ter um back-door abordagem aqui--é
ruim politicamente, como em Internet e política." [Eric Hughes,
94-01-31]
- E se o mail pode realmente ser de forma consistente e sustentada
falso, haveria menos necessidade de remetentes, certo?
(Na verdade, ainda é uma necessidade, análise de tráfego, provavelmente
quebra qualquer "Porta 25" fingir esquema.)
- Além disso, tal estratégia não seria provável para ser
robusto ao longo do tempo, como ele se baseia na exploração transitória
falhas e fornecedores específicos. Uma má ideia de todo.
+ Dificuldades na obtenção de reenvio de e-mails anônimos redes amplamente
implantado
- "A parte difícil é encontrar uma maneira de preservar o anonimato

onde a maioria dos sites na Internet continuam a
log de tráfego cuidadosamente, recusar-se a instalar o novo software
(especialmente anon-positivo de software), e são
administrado por pessoas com simplista e ultrapassada
ideias sobre a identidade e a punição. "[Greg Broiles,
1994-08-08]
+ Reenvio de e-mails desafio: o isolamento da última perna de uma cadeia de
acusação
+ Estratégia 1: Obter deles declararam ser portadores comuns, como
a empresa de telefonia ou um serviço de entrega de correio
+ por exemplo, nós não processar um pacote real
deliveryperson, ou até mesmo a empresa em que trabalha, para
entrega de um ilegais pacote
- conteúdo considerado para ser desconhecido para a transportadora
- (Eu já ouvi reclamações de que apenas as transportadoras que fazem outros
acordos para cooperar com a aplicação da lei pode ser
tratados como portadores comuns.)
+ Estratégia 2: Mensagem de piscinas
+ sites ftp
- com planos para os usuários "inscrever-se" todos os novos
mensagens (assim, monitoramento de órgãos não é possível saber
que, se alguma, as mensagens estão sendo procurados)
- este fica em torno da reclamação sobre muito volume
na Usenet (mensagens de texto são uma pequena fração de
outro tráfego, especialmente de imagens, então a reclamação é
apenas um dos potencialidade)
+ Estratégia 3: Ventos remetentes como última etapa
- provavelmente, definido pelo remetente, que presumivelmente conhece o
destino
- Um grande número de "secundário remetentes" quem concorda
remail um número limitado...
+ "Estamos apenas brincando com remetentes e tal?"
- Dói-me dizer isto, mas, sim, que são basicamente
brincando aqui!
- Reenvio de e-mails de tráfego é tão baixo, o preenchimento é tão casual, que
fazendo correlações entre entradas e saídas é não
criptograficamente difícil de fazer. (Pode _seem_ rígido, com
papel e lápis tipos de cálculos, mas ele vai ser
brincadeira de criança para o Crays no Forte.)
- Mesmo se isso não é assim para qualquer mensagem em particular,
a manutenção de um ID persistente-como Pr0duct Cypher faz,
com o digital sigs, sem que, eventualmente, fornecendo o suficiente
dicas vai ser quase impossível. No momento.

- As coisas vão melhorar. Melhor e mais detalhada
"criptoanálise de reenvio de e-mails correntes" é extremamente necessária.
Até então, nós estamos, de fato, apenas jogar. (O jogo pode ser
úteis, apesar de tudo.)
+ "Não dar em qualquer dicas" princípio (para remetentes)
- evitar dar qualquer informação
- não sei dizer qual de nós são fontes e o que são sumidouros;
deixe os atacantes assumem todos é um reenvio de e-mails, uma fonte de
- não sei dizer quanto tempo uma palavra-passe é
- não diga quantas rodadas são em tit-for-tat torneio

8.7. Postagem anônima para a Usenet
8.7.1. Julf do penet sistema tem sido, historicamente, a principal forma de
postar anonimamente para a Usenet (usado por ninguém menos que uma luminária de
L. Detweiler, em seu "an12070/S. Boxx" personna). Este tem
particularmente sido o caso com os lançamentos de "apoio" grupos,
ou emocionais grupos. Por exemplo,
alt.sexuais.abuso.de recuperação.
8.7.2. Criptograficamente segura remailes agora estão sendo usados
cada vez mais (e dimensionamento de leis e várias jurisdições
sugerem ainda mais será usado no futuro).
8.7.3. dedo remailer.help.all@chaos.bsu.edu dá a estes resultados
[como de 1994-09-07-se uma corrente resultado antes de usar!]
- "Postagens anônimas para a usenet pode ser feita através do envio de
anônimo-mail para um dos seguintes e-mail-para-usenet
gateways:

do grupo.name@demon.co.uk
do grupo.name@news.demon.co.uk
do grupo.name@bull.com
do grupo.name@cass.ma02.bull.com
do grupo.name@undergrad.math.uwaterloo.ca
do grupo.name@charm.magnus.acs.ohio-state.edu
do grupo.name@comlab.ox.ac.uk
do grupo.name@nic.funet.fi
do grupo.name@cs.dal.ca
do grupo.name@ug.cs.dal.ca
do grupo.name@paris.ics.uci.edu (remove os cabeçalhos)
do grupo.name.usenet@decwrl.dec.com (Preserva todos os cabeçalhos)"

8.8. Anônimo Mensagem de Piscinas, grupos de notícias, etc.
8.8.1. "Por que algumas pessoas usam mensagem de piscinas?"

- Fornece untracable comunicação
- mensagens
- segredos
- transações
+ Pr0duct Cypher é um bom exemplo de alguém que
se comunica principalmente através anônimo piscinas (para mensagens de
ele). Recentemente, alguém perguntou sobre isso, com este comentário:
- "Pr0duct Cypher escolhe não vincular seu "real
vida" identidade com o 'nym usado para assinar o software que ele
ou ela escreveu (PGP Ferramentas, Magia Dinheiro ?). Isso é bastante
um compreensível sentimento, dado que as maçãs podres no
A NSA está disposto a ir muito além legal de se preocupar, e fazer
ameaças de morte contra pessoas com de alta visibilidade pública
(veja os tópicos sobre um agente da NSA, ameaçando executar
Jim Bidzos de RSA mais na sua estacionamento)." [Richard
Johnson, alt.segurança.pgp, 1994-07-02]
8.8.2. alt.anônimo.mensagens é como uma piscina grupo
- mas, é principalmente usado para mensagens de teste, discussões de
o anonimato (apesar de que existem melhores grupos), etc.
8.8.3. "Poderia ser realmente anônimo grupos de notícias?"
- Uma idéia: newgroup um grupo moderado, em que apenas mensagens
sans cabeçalhos e outros identificadores, deverá ser aceite. O
"moderador", o que pode ser um programa--só iria postar
mensagens depois que este foi assegurada. (Pode ser uma interessante
experimento.)
+ alt.anônimo.mensagens foi newgrouped por Rick Busdiecker,
1994-08.
- Início de usos foram, como seria de esperar, por pessoas que tropeçou
todo o grupo e imputada a ele tudo o que quiseram.

8.9. Questões jurídicas com Remetentes
8.9.1. Qual é o estatuto jurídico de remetentes?
- Não há nenhuma lei contra isso neste momento.
- Nenhuma lei dizendo que as pessoas tem que colocar endereços de retorno na
mensagens, no telefone (chamadas de telefones públicos ainda são legais), etc.
- E as leis pertinentes de não ter de produzir identidade
(o "panfleto" de caso, onde folheto distribuidores não têm
para produzir ID) parece aplicar-se a esta forma de
comunicação.
+ No entanto, os remetentes podem vir sob o fogo:
+ Sysops, MIT caso
- potencialmente graves para os remetentes se o caso é
decidiu, de tal forma que o sysop da criação de um grupo que

foi propício para penais pirataria foi, propriamente, um
crime...que poderiam fazer com que todos os envolvidos no remetentes
culposa
8.9.2. "Pode reenvio de e-mails logs ser intimada?"
- Conte com isso acontecendo, talvez muito em breve. O FBI foi
subpoenaing e-mail arquivos para um Netcom cliente (Lewis De
Payne), provavelmente porque eles acham que o endereço de e-mail irá levar
- los para o local de super-hacker Kevin Mitnick. Tinha o
partes usadas remetentes, eu estou bastante certo de que estaríamos vendo
semelhante intimações para o reenvio de e-mails logs.
- Não há isenção para remetentes que eu conheço!
+ As soluções são óbvias, porém:
- usar muitos remetentes, para fazer subpoenaing de volta através do
a cadeia de muito trabalhoso, muito caro, e propensos a falhar
(mesmo se uma das partes não cooperar, ou está fora do
a competência do tribunal, etc.)
- ventos, multi-jurisdicionais remetentes (selecionada pelo
usuário)
- não reenvio de e-mails logs mantidos...destruí-los (não há nenhuma lei atualmente
diz que ninguém tem para manter registros de email! Isso pode
alteração....)
- "forward secrecy"," a la Diffie-Hellman forward secrecy
8.9.3. Como remetentes ser perseguidos, atacados, e desafiou?
8.9.4. "Pode pressão de ser colocado sobre o reenvio de e-mails operadores para revelar
tráfego
logs e, assim, permitir que o rastreamento de mensagens?"
+ Humano operado sistemas que tenham registos, com certeza. Este é
por que nós queremos que várias coisas em remetentes:
* não logs de mensagens
* muitos remetentes
* várias jurisdições legais, por exemplo, ventos remetentes
(quanto mais, melhor)
* implementações de hardware que executa instruções
perfeitamente (Chaum digital mix)
8.9.5. Chamadas para limites no anonimato
+ De crianças e a net vai fazer com que muitas chamada limites para
redes, no anonimato, etc.
- "Mas há um lado escuro para este emocionante fenômeno, um
que muito raramente é compreendida por usuários inexperientes.
Porque eles
oferecem acesso instantâneo aos outros, e considerável
o anonimato para
os participantes, os serviços de tornar possível que as pessoas -

especialmente com conhecimentos de informática kids - para encontrar-se em
desagradável, doenças sexualmente explícito situações sociais.... E
Eu gradualmente
vir a adoptar o modo de exibição, o que será motivo de controvérsia entre
muitos online
os usuários, que o uso de apelidos e outras formas de
o anonimato
devem ser eliminadas ou severamente reprimido para forçar as pessoas
online em
pelo menos tanto a prestação de contas por suas palavras e
ações como
existe no real, encontros sociais." [Walter S. Mossberg,
O Wall Street Journal, 6/30/94, fornecido por Brad Dolan]
Eli Brandt veio com uma boa resposta para isso: "O
som-mordida resposta para isso: você quer que o seu filho
nome, endereço e número de telefone disponível para todos
aqueles que espreita pedófilos em todo o mundo? Responsável pais
incentivar os filhos a usar remetentes."
- Supremo Tribunal disse que a identidade do folheto distribuidores
não precisa ser divulgada, e pseudônimos, em geral, tem uma longa
e nobre tradição
- BBS operadores têm proteções da Primeira Emenda (e.g..
requisitos de registo seriam atiradas para fora, exatamente como
se o registro dos jornais eram para ser tentada)
8.9.6. Remetentes e Escolha de Jurisdições
- O alvo de um remailed mensagem, e o assunto
material, pode muito bem influenciar o conjunto de remetentes usado,
especialmente para o muito importante "última reenvio de e-mails" (Note-se: ele
nunca deve ser necessário dizer remetentes se eles são
primeiro, o último ou os outros, mas o último reenvio de e-mails pode, na verdade,
ser capaz de dizer que ele é a última...se a mensagem estiver no
texto não criptografado para o destinatário, com adicional de reenvio de e-mails
comandos incorporados, por exemplo).
- Uma mensagem de pornografia envolvendo crianças podem ter um reenvio de e-mails
site localizado em um estado como a Dinamarca, onde a pornografia infantil leis
são menos restritivas. E uma mensagem crítica do Islã pode
não ser melhor enviadas através de uma final de reenvio de e-mails, em Teerã. Eric
Hughes tem apelidado este "arbitragem regulatória" e
várias extensões já é prática comum.
- Claro, o remetente pega o reenvio de e-mails em cadeia, de forma que estes
o senso comum noções podem não ser seguido. Nada é
perfeito, e os costumes evoluem. Eu posso imaginar esquemas de
desenvolvimento para a escolha de clientes, em um reenvio de e-mails pode não

aceitar como cliente determinadas abusadores, com base no digital
pseudônimos < peludo).
8.9.7. Possíveis medidas legais para limitar o uso de remetentes e
anônimo sistemas
- mantenha o reenvio de e-mails responsável por conteúdo, i.é., não comum
estado de portador
- inserir disposições em vários "anti-pirataria" leis para
criminalizar anônimo posts
8.9.8. Criptografia e remetentes podem ser usados para proteger os grupos de "profundo
bolsos" ações judiciais
- produtos (esp. de software) pode ser vendido "como é", ou com
contratos apoiados por serviços de garantia (código mantidos em um
garantia do repositório, ou dinheiro guardado lá para trás até
committments)
+ jurisdições, legais e fiscais, não pode fazer "chegar costas", que
expor os grupos mais do que eles concordaram
- como é frequentemente o caso com as corporações no real
mundo, que são tributados e multa para diversos fins
(amianto, etc.)
- (Para aqueles que pânico ao pensar isso, o remédio para
o cuidado será organizar contratos com o direito
entidades...provavelmente pagando mais por menos produto.)
8.9.9. Poderia remetentes anônimos ser usado para prender as pessoas, ou para
reunir informações para investigações?
- Primeiro, há tão poucas atual remetentes que este é
improvável. Julf parece um não-narc tipo, e ele está localizado na
A finlândia. Os Cypherpunks remetentes são em sua maioria executados por pessoas
como nós, por agora.
- No entanto, tais picadas e set-ups têm sido utilizados no passado
por narcóticos e "vermelho esquadrões." Esperar o pior do Sr.
Policial. Agora que o mal os hackers são identificados como riscos,
esperar que se move nesta direção. "Cryps" são, obviamente,
"crack" negociantes.
- Mas o uso de criptografia, que CP remetentes de suporte (Julf do
não), faz com que este, essencialmente, discutível.

8.10. Segurança de Redes de reenvio de e-mails
8.10.1. A Necessidade de uma Análise Mais Detalhada das Misturas e Remetentes
+ "Tem reenvio de e-mails sistemas sido adequadamente cryptanalyzed?"
- Não, na minha opinião, não. Alguns cálculos ter sido feito,
apenas principalmente algumas estimativas sobre a quantidade de "confusão" tem
foi criado pelo reenvio de e-mails de nós.
- Mas pensar que um monte de complicação e confusão

faz uma forte criptografia de sistema é um erro básico espécie de...
como pensar um Enigma rotor da máquina torna-se uma boa cifra
sistema, pelos padrões de hoje, só porque milhões de
combinações de caminhos através do sistema de rotor são
possível. Não é assim.
+ Deduzir Padrões de Tráfego e Deduzindo Nyms
- A principal lição de matemática criptologia tem sido a de que
aparentemente aleatórios coisas, na verdade, pode ser mostrado para ter
estrutura. Isto é o que a criptoanálise é toda sobre.
- A mesma situação aplica-se a "aparentemente aleatório" mensagem
o tráfego, em mistura digital, redes de telefone, etc.
"Criptoanálise de remetentes" é claro que é possível,
dependendo do modelo subjacente. (Na verdade, é sempre
possível, ele só não pode produzir qualquer coisa, como com
criptoanálise cifras.)
+ sobre o tempo de correlação de reenvio de e-mails de criptanálise
- imagine que Alice e Bob, comunicando-se através de
remetentes...um observador, incapaz de seguir específicos
mensagens através do remetentes, ainda podiam notar
par de correlações entre as mensagens enviadas e
recebido por esses dois
+ como tempo de correlações entre os eventos, mesmo se o
intervir caminho ou eventos são misturados
- por exemplo, se dentro de poucas horas de cada submarino
saída de Santo Loch uma chamada é colocada Moscou,
pode-se fazer a tirar certas conclusões sobre o que é um
Russo espião, independentemente de não saber o
intermediário caminhos
- ou, mais perto de casa, correlacionando as retiradas de um
banco para depósitos em outra, mesmo se a intervenção
as transferências são misturados
+ só porque ela parece "aleatório", não significa que ele é
- Scott Collins especula que uma "dinâmica de Markov
compressor" pode-se discernir ou descobrir o não-
a aleatoriedade no reenvio de e-mails usa
- Criptoanálise de remetentes tem sido lamentavelmente falta. Um
enorme fração de posts sobre reenvio de e-mails melhorias fazer
mão-acenando argumentos sobre a necessidade de mais tráfego,
mais atrasos, etc. (Eu não estou apontando dedos, como eu faço
o mesmo informal, qualitativa comentários, também. O que é
é necessário uma análise rigorosa de reenvio de e-mails de segurança.)
- Nós realmente não temos qualquer bom estimativas de segurança geral
como uma função do número de mensagens que circulam, a

a latência (o número de mensagens armazenadas antes de reenviar), o
número de reenvio de e-mails saltos, etc. Este não é criptograficamente
"emocionante" de trabalho, mas ainda é necessário. Não houve
muito foco na comunidade acadêmica digital misturas ou
remetentes, provavelmente porque David Chaum, de 1981, no papel
"Rastreáveis E-Mail" cobria a maior parte de, teoricamente,
material interessante. Isso, e a falta de comercial
produtos ou o uso de largura.
+ Tempo de correlações podem revelar padrões individuais
mensagens de falta. Isto é, repetido communicatin entre Alice
e Bob, mesmo se feito através de remetentes e mesmo se o tempo
atrasos/tempos de permanência são incorporados, pode revelar não randômico
correlações envio/receção de mensagens.
- Scott Collins especula que uma dinâmica de Markov compressor
aplicada ao tráfego teria de revelar tais
correlações. (A aplicação de tais testes para o digital
dinheiro e outros tais sistemas poderiam ser úteis para olhar.)
- Outro muitas vezes esquecido fraqueza é que muitas pessoas
enviar mensagens de teste para si, um ponto destacado por Phil
Karn: "Outra forma que muitas vezes as pessoas se deixam ser
pego é que eles inevitavelmente enviar uma mensagem de teste para
- se o direito antes de forjados mensagem em questão.
Isso mostra, claramente, no sistema de envio do sendmail
logs. É um ponto a se considerar com o reenvio de e-mails correntes demais,
se você não confia em última máquina na cadeia." [P. K.,
1994-09-06]
+ O que é necessário:
- acordo sobre algumas terminologias (isso não requer
consenso, apenas a escrita de forma clara o papel de facto
estabelecer a terminologia)
- uma fórmula relativo grau de untraceability para os principais
fatores que entram em remetentes: tamanho do pacote e
a quantização, a latência (nº de mensagens), reenvio de e-mails políticas,
cronometragem, etc.
- Também, a análise de como deliberada sondas ou ataques podem
ser montado para deduzir padrões de reenvio de e-mails (por exemplo, Fred sempre
remails para Josh e Suzy e raramente para Zeke).
- Eu acho que essa análise combinatória seria um pouco agradável
monografia de alguém para escrever.
8.10.2. Uma muito necessária coisa. Hal Finney tem postado alguns cálculos
(por volta de 1994-08-08), mas mais de trabalho é extremamente necessária.
8.10.3. Em particular, devemos ser céticos de mão-acenando análises
o "ele se parece complicada para seguir o trânsito"

classificação. As pessoas pensam que a adição de "bagunçado" truques", como
MIRVing mensagens, que a segurança é maior. Talvez seja,
talvez não. Mas ele precisa de análise formal antes dos créditos
pode ser confidantly acreditava.

8.10.4. Remetentes e entropia

- Qual é a medida da "mistura" do que se passa em uma mistura, ou
reenvio de e-mails?
- Mão=acenando sobre entropia e reordenação pode não ser muito
úteis.
+ De voltar para Shannon conceito de entropia como medir o
grau de incerteza...
+ tentando "adivinhar" ou "prever", onde uma mensagem deixando
um nó de saída do sistema
- não ter claros de entrada e pontos de saída, contribui para o
dificuldade, um pouco analogamente, para ter uma palavra-passe
de comprimento desconhecido (um invasor não pode simplesmente tentar de tudo 10-
personagem de senhas, como ele não tem idéia do comprimento)
- as vantagens de cada nó a ser um reenvio de e-mails, de
tendo claramente identificadas as fontes e sumidouros de
+ Esta previsibilidade pode depender de uma _series_ de mensagens
enviado entre Alice e Bob...como?
- parece que pode haver links para Persi Diaconis o trabalho em
"perfeito embaralha" (um problema que parecia fácil, mas
que enganavam solving, até recentemente...deve dar-nos
o conforto que a nossa incapacidade de enfrentar o real, de carne de
este problema não é muito surpreendente

8.10.5. Scott Collins acredita que o reenvio de e-mails redes podem ser
cryptanalyzed aproximadamente da mesma forma como de números pseudo-aleatórios
geradores são analisados, por exemplo, com a dinâmica de Markov
compressores (DNCs). (Eu sou mais cético: se cada reenvio de e-mails é
usando uma informação-teoricamente seguro RNG para reordenar o
mensagens, e se todas as mensagens são do mesmo tamanho e
curso) são encypted com informações-teoricamente seguro
(OTP) dígitos, em seguida, parece-me que o remailing seria
o próprio ser de informação-teoricamente seguro.)

8.11. Jantar Criptógrafos

8.11.1. Essa é, efetivamente, o "ideal de mistura digital," actualizado a partir de
Chaum do hardware original mistura de formulário para um puramente baseado em software
o formulário.

8.11.2. David Chaum em 1988, o papel em Jornal de Crypology (Vol. 1, Nº
1) traça um caminho completamente indetectáveis de comunicação
usando apenas software (não resistente a adulterações módulos necessários)

- os participantes em um anel (daí o "jantar criptógrafos")
- Chaum imagina que 3 criptógrafos estão a jantar e
são informados por seus garçom que o jantar já
sido pagas, talvez pela ANS, ou talvez por um dos
si...eles desejam determinar qual destas é verdadeira,
sem revelar o que eles são pagos!
- todo mundo vira uma moeda (H ou T) e mostra-lo para o seu vizinho
à esquerda
+ todos os relatórios se ele vê "iguais" ou "diferentes"
- nota-se que com 2 participantes, ambos já sabe
a outras moedas (ambos são de esquerda!)
- no entanto, alguém que pretenda enviar uma mensagem, tais como Chaum do
exemplo de "eu pago o jantar", em vez disso, diz o oposto
o que ele vê
+ algumas análises deste (analisá-lo do ponto de vista de
um dos métodos de criptografia) mostra que o 3 criptógrafos
vai saber que um deles pagos (se este protocolo é
executado fielmente), mas que a identidade não pode ser
"localizado"
- um diagrama é necessário...
+ isso pode ser generalizado...
+ mais mensagens
- use várias rodadas do protocolo
+ mais rápido do que moeda de inversão
- cada participante e, a sua esquerda parceiro de compartilhar uma lista de
"pré-invertido" de moedas, tais como verdadeiramente bits aleatórios
(decaimento radioativo, ruído, etc.) armazenados em um CD-ROM ou
qualquer que seja a
- eles, assim, podem "virar moedas" tão rápido quanto eles podem ler o
disco
+ mensagens simultâneas (colisão)
- uso de retirada e de repetição de protocolos (como Ethernet usa)
+ conluio dos participantes
- uma questão interessante...lembre-se de que os participantes são
não se restringe à simples topologia em anel
- diversas subgraphs pode ser formado
- um participante que teme o conluio pode escolher um subgraph
isso inclui aqueles que ele duvida irá conspirar (um complicado
edição)
+ anonimato do receptor
- pode usar o P-K para criptografar a mensagem para alguns P-K e, em seguida,
"broadcast" e da força de cada participante para tentar
descriptografá-lo (apenas o anônimo destinatário, na verdade,

o sucesso)
- Chaum completa de 1988, "Jornal da Criptologia" artigo
disponível no Cypherpunks site de arquivamento,
ftp.soda.csua.edu em /pub/cypherpunks
8.11.3. O que "DC-Net" Significa
- um sistema (gráfico, subgraphs, etc.) de comunicação
os participantes, que não precisam de ser conhecidas, pode
comunicar informações de tal forma que nem o remetente nem
o destinatário é conhecido
+ incondicional remetente untraceability
- o anonimato da emissora podem ser informações-
teoricamente seguro, isto é, verdadeiramente impossível quebrar e
que não exige suposições sobre sistemas de chave pública, o
dificuldade de factoring, etc.
+ receptor untraceability depende de chave pública protocolos, para
a rastreabilidade é computacionalmente dependentes
- mas este é acreditado para ser seguro, de curso de
+ de largura de banda pode ser aumentada por vários meios
- shared keys
- bloquear a transmissão ao acumular mensagens
- hiearchies de mensagens, subgraphs, etc.

8.12. Futuro Remetentes
8.12.1. "Quais são as características necessárias para a Próxima Geração
Reenvio de e-mails?"
+ Algumas metas
- geralmente, mais perto dos objetivos traçados no Chaum, de 1981,
papel em "Rastreáveis E-Mail"
- Anonimato
- Digital Postagem, como você vai pagar, de mercado ,de preços
- Análise de tráfego frustrado
+ À Prova De Balas Sites:
- Ter offshore (fora dos EUA) de sites é legal, mas
ter sites resistente a pressões de universidades e
site corporativo administradores é ainda maior
consequência prática. Os provedores comerciais, como
Netcom, Portal, e Panix, não pode ser contado para ficar
e a luta deve pressões de montagem (este é apenas o meu palpite,
não é uma aspersão contra seus backbones, orgânicos
ou Internet).
- Localização de remetentes em muitos de fora dos EUA países é uma Boa
Idéia. Como com a lavagem de dinheiro, muitos países significa
muitas jurisdições, e a quase impossibilidade de

o controle por um único país.
+ Digital Postagem, ou Pay-as-you-Go Serviços:
- Alguma taxa para o serviço. Assim como o serviço de telefone, modem
tempo real, postagem, etc. (Mas ao contrário de estrada de condução,
cujo uso é subsidiado.)
- Isso vai reduzir envio de spam, irá incentivar o reenvio de e-mails
serviços para melhor manter seus sistemas, e
- As taxas de ser definido pelo processo do mercado, da forma habitual.
"O que o tráfego vai suportar." Descontos, favorecido
os clientes, descontos, cupons, etc. Aqueles que não desejam
para carregar, não precisa (eles vão ter que lidar com o
problemas).
+ Gerações
- 1ª Geração--Hoje reenvio de e-mails:
- 2ª Geração--Futuro Próximo (c. De 1995)
- 3ª Geração-
- 4ª Geração--
8.12.2. Remailing como um efeito colateral de filtragem de e-mail
- Dean Tribble propôs...
- "Parece que o plano é fornecer uma conveniente mail
ferramenta de filtragem que fornece reenvio de e-mails capacidade de um LADO
EFEITO! O que é uma ótima maneira de espalhar remetentes!" [Hal Finney,
93-01-03]
8.12.3. "Há alguma remetentes que fornecer-lhe com um anônimo
conta para que outras pessoas possam enviar mensagens, que são
em seguida, encaminhado para você em um PGP de forma criptografada?" [Mikolaj
Habryn, 94-04]
- "Sim, mas ele não está funcionando para o real ainda. Dê-me alguns
meses até que eu volte o computador + netlink para ele. (É
execução de testes, porém, assim que se você quiser testá-lo, e-mail
- me, mas ele não está funcionando para o real, por isso não *uso ela.)"
[Sameer Parekh, 94-04-03]
8.12.4. "Reenvio De E-Mails Alianças"
+ "Reenvio de e-mails da Guilda"
- para fazer há de ser um custo para flakiness (expulsão) e um
benefício para a robustez, qualidade, fiabilidade, etc.
(maior)
- pings, testes, cooperativa remailing
- espalhar o tráfego para reduzir a eficácia dos ataques
- que executam os protocolos de
- por exemplo, para compartilhar o tráfego no último salto, para reduzir
ataques em um único reenvio de e-mails

8.13. Pontas Soltas
8.13.1. Digital de espionagem
+ espião redes pode ser executado com segurança, untraceably, indetectavelmente
- anônimo contatos, pseudônimos
- digital morto cai, tudo feito eletronicamente, sem chance...
de ser pego, revelou-se como um "ilegal" (um espião com
não diplomática tampa para salvá-lo) e tiro
+ portanto, muitos graus de liberdade nas comunicações que
controlando todas elas é essencialmente impossível
- Teledesic/Iridium/etc. os satélites vão aumentar esse
capacidade de mais
+ a menos de criptografia é bloqueado--e de forma relativamente rápida e
impiedosamente--a situação aqui descrita é imparável
- o que alguns chamam de "espionagem" outros seria apenas a chamada de graça
comunicação
- (Algumas lições importantes para manter corporativa ou empresarial
segredos...basicamente, você não pode.)
8.13.2. Remetentes precisa de alguns "imprecisão", provavelmente
+ por exemplo, se um reenvio de e-mails possui uma rigorosa política de
a acumulação de N mensagens, em seguida, reordenação e remailing
eles, um invasor pode enviar N - 1 mensagens de e sei que
de N mensagens deixando a mensagem que deseja
siga; alguns incerteza ajuda aqui
- a matemática de como esta pequena quantidade de incerteza,
ou de dispersão, pode ajudar é algo que precisa de um detalhadas
análise
- pode ser que deixar um pouco de incerteza, como com a
keylength problema, pode ajudar a
8.13.3. Tentando confundir os espiões, adicionando palavras-chave
provavelmente vai pegar
+ o "remailer@csua.berkeley.edu" reenvio de e-mails agora adiciona real
parágrafos, como este exemplo recente:
- "Eu fixo o SKS. Ele veio com um escopo e um russo
noite de escopo. É do assassino. O meu amigo sabe sobre um
muito bom armeiro que tenha um machineshop e sabe como
para converter o material para automático."

- Como eficaz, este estratagema é debatida
8.13.4. Restrições em sistemas anónimos
Anônimo o teste da SIDA. Kits de auto-teste foram
sob FDA revisão de 5 anos, mas aconselhamento defensores
de liberação retardada em razão de que algumas pessoas vão reagir
mal, e talvez matar-se sobre a obtenção de um positivo

o resultado do teste...eles querem que o sistema existente de prevalecer. (Eu
mencionar isso para mostrar que sistemas anónimos são somtimes
oposição por razões ideológicas.)

9. Política: Clipper,Chave de Caução, e de Telefonia Digital

9.1. direitos autorais
O CYPHERNOMICON: Cypherpunks FAQ e Mais, Versão 0.666,
1994-09-10, Direitos De Autor Timothy C. De Maio. Todos os direitos reservados.
Veja os detalhes de isenção de responsabilidade. Use seções curtas em "justo
use" disposições, com crédito apropriado, mas não coloque o seu
nome em minhas palavras.

9.2. RESUMO: a Política: Clipper,Chave de Caução, e de Telefonia Digital
9.2.1. Pontos Principais
- Clipper tem sido uma grande força unificadora, como 80% de todos os
Os americanos, e 95% de todos os tipos de computador, são opostos.
- "Big Brother " De Dentro"
9.2.2. Ligações para Outras Secções
- as ligações principais são _legal_
- algumas possíveis implicações para limites de criptografia
9.2.3. Onde Encontrar Informações Adicionais
- Tem havido centenas de artigos em Clipper, em quase
todas as revistas populares. Muitos destes foram enviados para o
Cypherpunks lista e poderá estar disponível nos arquivos. (Eu
ter pelo menos 80 MB de Cypherpunks lista de coisas, um monte de
artigos de jornais e revistas em Clipper!)
+ mais Clipper informações podem ser encontradas em:
- "Uma boa fonte é o Fio Online Clipper Arquivo. Enviar
e-mail para info-rama@wired.com. sem assunto e o
palavras "obter ajuda" e "get clipper/index' no corpo do
a mensagem". [students@unsw.EDU.AU, alt.privacidade.clipper,
1994-09-01]
9.2.4. Diversos Comentários
- Com um par de outras seções, eu não vou tentar ser como
completo como alguns podem desejo. Apenas muitos milhares de
páginas de coisas a considerar.

9.3. Introdução
9.3.1. O que é Clipper?
- governo mantém o esqueleto chaves
- analogias com outros sistemas
9.3.2. Por que a maioria dos Cypherpunks opor Clipper?

- medo de restrições sobre a criptografia, o descarrilamento tantas maravilhosas possibilidades

9.3.3. Por que o Clipper taxa de seção própria?

- O anúncio do "Caucionada Padrão de Encriptação,"
ESTRATÉGIA europeia de emprego, em 16 de abril de 1993, foi um evento para galvanização Cypherpunks e para um grande segmento da U. S.
população. A ESTRATÉGIA foi originalmente anunciada como "Clipper"
apesar de o uso do nome Clipper por dois produtos principais
(a Intergraph CPU e dBase ferramenta de software), e o
governo apoiado (off) no nome. Tarde demais, porém, como o
o nome "Clipper" tornou-se indelevelmente ligado a todo este a proposta.

9.3.4. "Está parando Clipper, o principal objetivo dos Cypherpunks?"

- Certamente parece assim, às vezes, como Clipper tem dominado
os tópicos desde o Clipper anúncio, em abril, 1993.
+ tornou-se assim, com monkeywrenching esforços em vários áreas
- lobby e educação contra ele (apesar de informal, tais
o lobby tem sido bem sucedido...olha artigo NYT)
- "Big Brother "Dentro" e t-shirts
- técnico monkeywrenching (Matt Blaze...hesite em reclamar
nenhum crédito, mas ele tem sido em nossa lista, participou de uma
de reunião, etc.)
- Embora possa parecer, o Clipper é apenas um aspecto...passo...iniciativa.
- Desenvolvimento de novas ferramentas de software, escrever código, a implantação de remetentes e dinheiro digital de longo alcance projetos de grande importância.
- O Clipper chave de caução proposta veio junto (4-93) em um
momento oportuno para Cypherpunks e tornou-se um grande foco.
De emergência reuniões, análises, etc.

9.4. Crypto Questões De Política

9.4.1. Peter Denning sobre a criptografia de política:

+ fornecidas pelo Pat Farrell, 1994-08-20; Denning comentários
1992-01-22, apresentado em Computadores, a Liberdade, a Privacidade e 2.
Pedro D. usa a metáfora de uma "compensação", como em uma floresta,
para o lugar onde as pessoas se encontram para negociar, interagir, etc.
Que outros chamam de mercados, agoras, ou apenas "o ciberespaço."
- "Tecnologia da informação na produção de uma clareira na qual
os indivíduos e as corporações são os principais jogadores, além de
governo. Qualquer tentativa por parte do governo para controlar o fluxo
de informação através de redes serão ignoradas ou encontrou-se com

hostilidade. Não há nenhuma maneira prática de
governo pode controlar informações, exceto informações
diretamente envolvido no negócio de governar. Ele
não deve tentar." [Peter Denning, POLÍTICAS PÚBLICAS PARA A
SÉCULO 21, PROJETO DE 1/22/92]
- Nenhuma palavra sobre como esta visão quadrados com sua mulher, controle de
freak pontos de vista.
9.4.2. Será que o governo vai e NSA, em particular, tentar adquirir alguns
tipo de controle sobre criptografia empresas?
+ especulações, aparentemente infundada, de que a RSA Data Security
é influenciada pelo NSA desejos
- pontos fracos em as chaves do DES escolhido?
- e as empresas podem ser significativamente influenciadas por contratos de
(e a retenção dos mesmos)
9.4.3. NIST e DSS
9.4.4. Restrições de exportação, Lista de Munições, ITAR
9.4.5. de idade de criptografia máquinas vendidas para os governos do Terceiro Mundo, barata
- talvez eles acham que podem fazer algumas mudanças e mais esperto
a NSA (o que provavelmente foi fraudado e que portanto, as alterações são
detectável e pode ser fatorado em)
- e só de saber que o tipo de máquina é uma enorme vantagem
9.4.6. 4/28/97 O primeiro de vários P-K e RSA patentes expira
+ U.S. Patent Number: 4200770
- Título: Criptografia Aparelho e Método
- Inventores: Hellman, Diffie, Merkle
- Cessionário: Universidade De Stanford
- Arquivado Em: Setembro 6, 1977
- É Concedido: 29 De Abril De 1980
- [Expira: 28 De Abril De 1997]
+ lembre-se de que qualquer uma destas várias patentes detidas por
Chave pública de Parceiros (Stanford e M. I. T., com RSA Data
Segurança o chefe dispensador de licenças) pode bloquear um
esforço para ignorar os outros
- embora isso possa obter lutou em tribunal
9.4.7. criptografia serão necessárias dentro de sistemas de computador
- para a operação do sistema de proteção
- para autônomos agentes (agentes ativos)
- para o dinheiro eletrônico

9.5. Motivações para a Criptografia Leis
9.5.1. "O que a aplicação da lei e do FBI preocupações?"
- "O Diretor do FBI, Louis Freeh está preocupado. Os bandidos estão
começo a ver a luz, e ele é digital. ... Freeh

temores de que alguns bastante desagradável pessoas descobriram que podem cometer um roubo e mais, sem mesmo sair de casa.
Pior, para Freeh e outros policiais topo, utilizando bastante tecnologias básicas e inteligente, os criminosos podem fazer seus crimes sem se preocupar em fazer hora.

"Alguns bandidos, espiões, traficantes de drogas, terroristas e fraudes já utilizam as ferramentas da era da informação para outfox agentes de aplicação da lei. Hackers usam PBXs para ocultar suas faixas como eles rip off empresas de telefonia e de poke em torno de outras pessoas arquivos. Reprogramação celular telefones dar policiais se encaixa." [LAN Revista,"É de 1984?," Ted Bunker, De Agosto De 1994]
- Seus medos têm alguma validade...da mesma forma que o governantes Gutenberg tempo poderia ter algumas preocupações sobre as implicações de livros (quebra de guildas, propagação de nacional de segredos, a pornografia, o ateísmo, etc.).
9.5.2. "O que motivou Clipper? O que os Federais espero ganhar?"
- ostensivamente para parar os terroristas (apenas os simplórios queridos, se as alternativas são permitidos)
- para forçar um padrão em média, os Americanos
- possivelmente para limitar a criptografia de desenvolvimento
+ Phil Karn fornece uma interessante motivação para Clipper:
"A chave de caução só existe porque a ANS não quer risco de culpa se algum terrorista ou traficante de drogas eram para usar uma unescrowed NSA-produzidos .....O fato de que um terrorista ou traficante de drogas pode facilmente ir para outro lugar e obter outro forte mais fortes ou mais algoritmos sem chave de caução é irrelevante. A ANS simplesmente não se importa, contanto que *eles* não pode ser culpado por tudo que acontece. Clássico CYA, nada mais.....Uma análise semelhante aplica-se ao controle de exportação regulamentos de criptografia." [Phil Karn, 1994-08-31]
- Bill Sommerfeld notas: "Se este é realmente o caso, Matt Blaze resultados devem ser particularmente devastador para - os." [B. S., 1994-09-01]
9.5.3. Steve Witham tem uma opinião interessante sobre por que o pessoal gosta Dorothy Denning e Donn Parker, o suporte chave de caução para ardentemente:
- "Talvez as pessoas gostam de Ponto e Não acho que o governo como um sistemas de administração tipo de trabalho. Aqui estão eles, especialistas em segurança a aconselhar os administradores de sistemas sobre coisas como...

definição de permissões
a alocação de cotas de
registo de utilizadores e dando-lhes palavras-passe.....
decidir que utilitários estão e não estão disponíveis
decidir qual o software que os usuários precisam, e instalá-lo
(de má vontade, baseando-se em quem gritar mais alto)
configuração de conexões para outras máquinas
decidir quem pode fazer login a partir de "estrangeiros hosts"
chegando mail configurar e executar
a compra de novo hardware de fornecedores
especificando o hardware para os fornecedores
...

"Estas são as coisas que especialistas em segurança de computador aconselhar.
Talvez martelo especialistas de ver as coisas como as unhas.

"Só um país não é um host do sistema de propriedade e administrado
pelo governo, os cidadãos não estão convidados ou usuários."
[Steve Witham, Governo, pelo Administrador, 1994-03-23]

9.5.4. Quem gostaria de usar chave de caução?
9.5.5. "Será forte criptografia realmente frustrar os planos do governo?"
- Sim, ele vai dar aos cidadãos as capacidades básicas que
governos estrangeiros tiveram por muitos anos
+ Apesar de falar sobre codebreakes e a competência dos
NSA, o fato simples é que não há grandes Soviética cifras ter
foi quebrado por muitos anos
+ relembre o comentário de que a NSA não tenha quebrado qualquer
Soviética sistemas em muitos anos
- exceto para os casos, a la Walker caso, onde
plaintext versões são obtidos, por exemplo, onde humanos
screwups ocorreu
- a imagem em tantos romances de grandes computadores quebrar
códigos é um absurdo: as cifras modernas não será quebrada (mas o
primitivas de cifras usado por tantas nações do Terceiro Mundo e
suas embaixadas continuará a ser brincadeira de criança, mesmo para
high school projetos de feira de ciências...poderia ser uma boa idéia
para uma pequena cena, sobre um BCC aluno que tenha seu projeto
puxado)
9.5.6. "Por que o governo quer chaves curtas?"
- Produtos comerciais têm sido muitas vezes quebrada por hackers. O
A ANS tem, na verdade, uma carta para ajudar as empresas a proteger seu
segredos; apenas não tão fortemente que a criptografia é

inquebrável por eles. (Isso, naturalmente, tem sido parte da
a tensão entre os dois lados da NSA para o passado
par de décadas.)
+ Então, por que o governo quer aleijado comprimentos de chave?
- "A questão é: como impedir hackers enquanto
permitindo NSA acesso? A resposta óbvia é forte
algoritmo(s) e relativamente truncado chaves." [Grady Ala,
sci.cripta, 1994-08-15]

9.6. Atual De Criptografia Leis
9.6.1. "Tem de criptografia sido restrito em outros países que não o
EUA?"
- Muitos países têm restrições civil/uso privado de
crypto. Alguns ainda insistem que as empresas enviar todos os
transmissões em claro, ou que as teclas de ser fornecida para o
governo. As Filipinas, por exemplo. E, certamente,
regimes Comunistas do Bloco, ou o que sobrou dela, vai
provavelmente terá várias leis que restringem criptografia. Possivelmente
leis draconianas....em muitas culturas, o uso de criptografia é
equivalente a espionagem.

9.7. Crypto Leis Fora dos EUA
9.7.1. "Internacional de Caução, e Outra Nação de Criptografia Políticas?"
- O foco ao longo deste documento sobre a política dos estados unidos deve
não calmaria não-Americanos em complacência. Muitas nações
já tem mais Pesadas que as políticas sobre o uso privado de
a criptografia que o dos EUA é ainda contemplando
(publicamente). França proíbe privada de criptografia, que
a execução é dito ser problemática (mas eu não gostaria de
o DGSE estar no meu rabo, que com certeza). Terceiro Mundo
países têm muitas vezes proibições sobre a criptografia, e a mera posse de
aleatório-olhando bits, pode significar um espionagem convicção e uma viagem
para a forca.
+ Há também vários relatos de que as nações Europeias são
se preparando para cair na linha de trás dos EUA em key escrow
- Noruega
- Holanda
- Grã-bretanha
+ Uma conferência em DC no 6/94, com a presença de Pentecostes Diffie (e
relatou-nos no 6/94 CP reunião) tinha internacional
garantia arranjos como um tópico, com a criptografia de política
os tomadores do NIST e NSA descrevendo várias opções
- más notícias, porque ele pode permitir tratados bilaterais para

substituem direitos básicos
- poderia ser um plano para conseguir a chave de caução obrigatória
+ há também questões práticas
+ quem pode decodificar internacional de comunicações?
- queremos realmente os franceses leitura da Intel
comunicações? (lembre-Matra-Harris)
- satélites? (como o Irídio)
- o que de multi-nacionais de mensagens, como um criptografados
mensagem postada uma mensagem de piscina na Internet é...
para ser caucionada com cada um dos 100 nações?
9.7.2. "Vai países estrangeiros utilização dos EUA-chave com base em sistema de custódia?"
- Muita pressão. Muitas provas de compatibilidade.
9.7.3. "É A Europa, Considerando A Tecla De Caução?"
- Sim, em espadas. Muitos sinais, com relatórios vindos
em residentes da Europa e de outros lugares. Os Europeus
tendem a ser um pouco mais tranquila em assuntos de política pública (em
menos em algumas áreas).
- "O problema atual de Comunicações Semana Internacional'
informa-nos de que a União Europeia Sênior do Grupo de Funcionários
para a Segurança de Sistemas de Informação tem vindo a considerar
planos para unificar a tecla de garantia na Europa.

"De acordo tinha sido sustentada por argumentos sobre quem deve
mantenha as chaves. A frança e a Holanda queria seguir o
NSA e têm os governos nacionais a assumir este papel;
outros jogadores queriam organizações de usuários para fazer isso." [
rja14@cl.cam.ac.reino unido (Ross Anderson), sci.cripta, Key Escrow
também na Europa, 1994-06-29]
9.7.4. "O que as leis de vários países têm em criptografia e a
uso de criptografia para o tráfego internacional?"
+ "A França realmente proibida a encriptação?"
- Existem relatórios recorrentes que a França não permite
irrestrito uso de criptografia.
- Difícil dizer. Leis sobre os livros. Mas não há indicações de que
muitos francês usuários de PGP, dizem, estão sendo processados.
- uma nação cujo líder, François Mitterand, era um Nazista
collaborationist, trabalhando com Petain e o Vichy
governo (Klaus Barbie envolvidos)
+ Alguns Países Específicos
- necessidade (mais info aqui)
+ Alemanha
- BND coopera com os EUA.
- Holanda

- Rússia
+ Informações
- "Confira o site de ftp csrc.ncsl.nist.gov para um
documento chamado algo como "leis.wp" (Há
vários destes, em vários formatos.) Este contém uma
levantamento das posições dos diversos países, feito para
NIST por um casal de pessoas em Georgetown, ou George
Washington, ou algum tipo de universidade." [Filipe Fites,
alt.segurança.pgp, 1994-07-03]
9.7.5. França planejamento Big Brother cartão inteligente?
- "PARIS, FRANÇA, 1994 MAR 4 (NB) -- O governo francês
confirmou seus planos para substituir o cidadão de papel, baseado em ID
cartões de crédito, do tamanho de cartões "smart card" cartões de IDENTIFICAÇÃO.
.....
"As cartas contêm detalhes de transacções recentes, bem
como agir como uma "bolsa eletrônica" por menor valor
transações utilizando um número de identificação pessoal (PIN)
como a autorização. "Bolsa de transacções" são geralmente separados
o cartão de crédito/débito do sistema, e, quando a bolsa é
vazio, ele pode ser recarregado de cartão em um adequado ATM
ou varejista terminal." (Steve Ouro/19940304)" [este foi
enviada a mim por postar]
9.7.6. PTTs, regras locais sobre a utilização do modem
9.7.7. "O que são as leis Europeias sobre "Privacidade de Dados" e por isso são
que tal uma idéia terrível?"
- De vários países Europeus aprovaram leis sobre o
a compilação de dados computadorizados em pessoas sem o seu
permissão explícita. Isso se aplica a quase todos os
registos informáticos--listas de discussão, dossiês de crédito
registros, arquivos de funcionários, etc.--embora existam exceções
e, em geral, as empresas podem encontrar maneiras de compilar registros
e permanecem dentro da lei.
- As regras são abertas ao debate, e o casual, o indivíduo que
não podem pagar advogados e consultores, é susceptível de ser
quebrar as leis repetidamente. Por exemplo, armazenar o
postagens de pessoas no Cypherpunks lista em qualquer sistema
recuperados pelo nome de violar a grã-Bretanha Privacidade de Dados
leis. Que quase nenhum caso, nunca iria resultar em um
acusação (por razões práticas) não significa que as leis
são aceitáveis.
- Para muitos, essas leis são uma "boa idéia." Mas as leis perder
o ponto principal, dar um falso sentido de segurança (como a real
dossiê-compiladores são facilmente capazes de obter isenções, ou

são agências do governo de si), e interferir no que
as pessoas fazem com a informação que devidamente e legalmente vem
há caminho. (Estar em alerta para os "direitos civis" grupos como
a ACLU e do FEP para empurrar para tais leis de privacidade de dados. O
a ironia de Kapor ligação da Lotus e o falha
"Marketplace" CD-ROM do produto não pode ser ignorada.)
- Criação de uma lei que proíbe a manutenção de determinados tipos de
registros é um convite a ter de dados "inspetores"
vasculhar uma de arquivos. Ou algum tipo de verificações no local,
ou até mesmo o software chave de caução.
- (Forte de criptografia faz com que essas leis difíceis de aplicar. Ou
as leis de trânsito, ou a municípios com tais leis, em seguida, irá ter
para limitar o forte de criptografia....não que isso vai ajudar no
longo prazo.)
- Os mesmos pontos de aplicar para o bem-intencionados propostas para tornar o
empregador monitoramento de trabalhadores ilegais. Isso soa como uma
melhoria de privacidade idéia, mas esmagá-lo contra os direitos de
o empregador para garantir que o trabalho está sendo feito, para
basicamente executar o seu negócio como ele vê o ajuste, etc. Se eu contratar um
programador e ele está usando meus recursos, em minha rede
ligações, para executar uma operação ilegal, ele expõe a minha
empresa de danos, e é claro que ele não está fazendo o trabalho que eu
pagou a ele para fazer. Se a lei proíbe-me para acompanhar este
situação, ou pelo menos, de forma aleatória, em seguida, ele pode
explorar desta lei, para sua vantagem e a minha desvantagem.
(Novamente, os perigos das rígidas leis, associadas ou não
soluções,(mentiu teoria de jogo.)
9.7.8. sobre a situação na Austrália
+ Mateus Gream [M.Gream@uts.edu.au] nos informou que o
exportar situação em Oz é tão melhor do que nos EUA [1994-
09-06] (como se já não sei...muito como todos nós gostamos de despejo
na Amerika para sua fascista leis, é claro que quase todos os
os países estão levando sua Nova Ordem Mundial Ordens de Marcha
a partir de os EUA, e que muitos deles têm ainda mais
repressivas de criptografia leis já em vigor...eles não
obter a discussão dos EUA recebe, por razões aparentes)
- "Bem, foda-se que para de pensar que eu estava vivendo sob uma menos
regime restritivo-e eu pode dizer adeus a um
o mercado internacional para o meu software.]
- (Eu deixei seu blunt língua é, para o impacto.)
9.7.9. "Para aqueles interessados, NIST ter um documento curto para FTP,
Identificação e Análise dos Estrangeiros Leis e Regulamentos
Referente à Utilização dos Comerciais de Produtos de Criptografia para

Voz E Comunicação De Dados'. Datado De Janeiro De 1994." [Owen Lewis,
Re: França Proíbe de Criptografia, alt.segurança.pgp, 1994-07-07]

9.8. Telefonia Digital

9.8.1. "O que é a Telefonia Digital?"

- A Telefonia Digital projeto de lei, proposto pela primeira vez no governo Bush e
novamente por Clinton, em muitos aspectos é muito pior do que a de corte.
Tem recebido menos atenção, por várias razões.
- Para uma coisa, ele é visto como uma extensão por alguns dos
existente escuta capacidades. E, é bastante abstrato,
acontecendo por trás das portas da companhia telefônica muda.
- As implicações são graves: a obrigatoriedade de escuta e de caneta
registar (quem está chamando quem) capaibilities, civil
multas de até us $10.000 por dia por insuficiência de
a conformidade obrigatória a assistência deve ser fornecida, etc.
- Se ele for passado, ele poderia ditar o futuro da tecnologia. Empresas de telecomunicações
quem instalar certifique-se de que o upstart tecnologias
(por exemplo, Cypherpunks que encontrar maneiras de navio de voz sobre
linhas de computador) também são obrigados a "jogar o mesmo
regras." Sendo necessário para instalar o governo acessível ao toque
pontos mesmo em pequenos sistemas de curso efetivamente
destruí-los.
- Por outro lado, ele está ficando mais difícil e mais difícil de fazer
Telefonia Digital viável, até mesmo por mandato. Como Jim
Kallstrom do FBI, que coloca: ""Hoje vai ser o mais barato
dia em que o Congresso poderia corrigir essa coisa," Kallstrom
disse. "Dois anos, a partir de agora, ele vai ser geometricamente mais
caro."" [LAN Revista,"É de 1984?," Ted Bunker,
De agosto de 1994]
- Isso nos dá uma meta para atirar para: sabotar o mais recente
a tentativa de obter Telefonia Digital transmitido em lei e pode
torná-lo muito difíceis para nunca ser passado.
+ "Hoje vai ser mais barata dia em que
- O congresso poderia corrigir essa coisa," Kallstrom, disse. "Dois
anos a partir de agora,
- ele vai ser geometricamente mais caro."
- A mensagem é clara: o atraso de Telefonia Digital. Sabotá-la
no tribunal da opinião pública, a espalhar a palavra, torná-lo
flop. (Releia sua "Arte da Guerra" de Sun Tsu dicas em
lutando contra seu inimigo.)
-

9.8.2. "O que são os perigos da Telefonia Digital, Bill?"

- Faz escutas telefônicas invisíveis para o tappee.

+ Se transformado em lei, torna-escritório central de escutas telefônicas
trivial, automático.
- "O que deve preocupar as pessoas é o que não está nas notícias (e
provavelmente nunca chegará até ele já está incorporado na comunicação
sistemas). Um verdadeiro "Clipper" irá permitir remoto tocar
a demanda. Isso é facilmente feito para todos-digital
sistemas de comunicações. Se você entender roteadores de rede
e o protocolo é fácil imaginar como seria simples
a "re-encaminhar" uma cópia de um destino de comunicação para onde quer que você
quer que ele vá..." [domonkos@access.digex.net (andy
domonkos), comp.org.fep.falar, 1994-06-29]
9.8.3. "O que é a Telefonia Digital proposta/projeto de lei?
- proposta de alguns anos atrás...disse ser inspiração para PGP
- reintroduzido o dia 4 de Fevereiro, 1994
- anterior versrion:
+ "1) DE TELEFONIA DIGITAL PROPOSTA
- "Para assegurar a aplicação da lei da capacidade de continuar a realizar
tribunal-
- autorizado torneiras, a administração, a pedido do
o
- Dept. de Justiça e o FBI, proposto ditigal de telefonia
- legislação. A versão apresentada ao Congresso em Setembro.
1992
- seria exige que os prestadores de comunicação eletrônica
serviços
- e private branch exchange (PBX) operadores para garantir
que o
- capacidade do governo legalmente intercepção de comunicações
não é
- reduzido ou evitado completamente com a introdução de
avançado
- tecnologia".

9.9. Clipper, Caucionada Do Padrão De Criptografia
9.9.1. O Clipper Proposta
- Uma bomba caiu em 16 de abril de 1993. Alguns de nós viu
ele vem, como estávamos debatendo...
9.9.2. "Quanto tempo tem o governo está planejando chave de caução?"
- desde 1989
- ironicamente, nós temos cerca de seis meses de aviso prévio
- a minha própria "Um Balão de Ensaio para a Proibição de Criptografia" alertou a
mundo ao pensamento de D. Denning....ela nega ter
conhecido sobre os principais escorw até o dia antes da

anunciou, o que eu acho improvável (para não chamá-la de uma
mentiroso, mas...)
+ Phil Karn tinha a dizer para o Professor Dorothy Denning,
várias semanas antes de o Clipper anúncio:
- "O uso privado de criptografia forte fornece, para o
primeira vez, uma verdadeira e eficaz salvaguarda contra este
tipo de governo abuso. E é por isso que ele deve continuar
para ser livre e não regulamentada.
- "Eu deveria crédito por fazer-nos a todos um muito importante
serviço por levantar esta questão. Nada poderia ter acendido uma
maior fogo, aqueles de nós que acreditamos em um
aos cidadãos o direito de usar criptografia de suas propostas
para proibir ou regular. Há muitos de nós aqui, que
compartilhar esta crença *e* possuir habilidades técnicas para transformar
- o em prática. E eu prometo a você que vamos lutar
para esta crença até o amargo fim, se necessário." [Phil
Karn, 1993-03-23]
-
-
9.9.3. Tecnicamente, o "Caucionada Encryption Standard" ou EES. Mas
início de todos ainda o chama "Clipper", mesmo se NSA
tardiamente percebi Intergraph ganhou produto tem sido chamado de
isso por muitos anos, a la Fairchild chip do processador do
mesmo nome. E o produto de banco de dados com o mesmo nome. Eu
mostraram isso dentro de minutos de ouvir sobre isso em
Em 16 de abril de 1993, e postou um comentário para este efeito em
sci.cripta. Como nora eles podem não ter visto em muitos
meses de trabalho, o que muitos de nós viu dentro de segundos?
9.9.4. Necessidade de Clipper
9.9.5. Mais "justificativas" para a tecla de garantia
+ anonymous as consultas que exigem a descoberta de
identidades
- o suicídio de intervenção em crise
- confissões de abusos, crimes, etc. (Tarasoff lei)
- registros da empresa de que a Pf quer olhar
+ Algumas necessidades legítimas para caucionados de criptografia
- para as empresas, para ignorar as senhas que partiram,
demitido, funcionários falecidos,
9.9.6. Por que o governo desenvolva Clipper?
9.9.7. "Quem são os designados depositários?"
- Commerce (NIST) e o Tesouro (Serviço Secreto).
9.9.8. Whit Diffie
- Milhas Schmid foi o arquiteto

+ internacional de key escrow
- Denning tentou defendê-la....
9.9.9. O que são programas relacionados?
9.9.10. "Onde os nomes "Clipper" e "Skipjack" vem?
- Primeiro, a NSA e NIST asneira grande tempo, escolhendo os
o nome "Clipper", que tem sido o nome de 32 bits
Processador RISC (um dos primeiros) a partir de Fairchild, mais tarde
vendido para Intergraph. É também o nome de um banco de dados
compilador. A maioria de nós viu isso imediatamente.
-
+ Clippers são os barcos, por isso, são skipjacks ("Um pequeno veleiro
ter um
- fundo com a forma de um plano V e os lados verticais" Sou
Património. 3º).
- Sugere um tema náutico, que se encaixa com o
Cheseapeake arredores de
- a Agência (e barcos de pequeno porte têm sido, tradicionalmente, uma forma
para o
+ Agências de dispor de supostos traidores e espiões).
-
- No entanto, o ponto crucial não é um barco, nem é Tessera, de modo a
tendência falha.

9.10. Detalhes técnicos do Clipper, Skipjack, Tessera, e EES
9.10.1. Clipper chip de fabricação detalhes
+ ARM6 núcleo a ser utilizado
- mas também rumores de MIPS núcleo de Tessera
- MIPS núcleo supostamente a ser projetado em futuras versões
- Nacional também construído (e pode operar) um seguro de wafer fab
linha para a ANS, supostamente localizada no terreno da Ft.
Meade--embora eu não possa confirmar a localização ou apenas o que
Nacional do envolvimento atual ainda é. Só pode ser para
de média densidade fichas, como material de chave (construído sob
condições de segurança).
9.10.2. "Porque é que o algoritmo de Clipper classificados?"
- para evitar a não-garantia de versões, o que ainda poderia usar o
(presumivelmente forte algoritmo e hardware, mas não ser
caucionada
- criptoanálise é sempre mais fácil se os algoritmos são conhecidos
:-}
- governo geral sigilo
- backdoors?
9.10.3. Se o Clipper é falho (o Blaze Soprador de FOLHAS), como pode

ainda ser útil para a ANS?
- por minar comercial alternativas através subsidiado
custos (que eu não acho que vai acontecer, dada a terrível
PR Clipper tem chegado)
- exigidos por lei ou regras de exportação
- e o Incêndio de ataque é que-no momento-não é fácil de usar (e
qualquer pessoa capaz de usá-lo é susceptível de ser sofisticado o suficiente
para usar preencryption de qualquer maneira)
9.10.4. Que sobre as fraquezas do Clipper?
- Nos pontos de vista de muitos, uma má abordagem. Que é, argumentando
sobre as rugas joga nas mãos dos Federais.
9.10.5. "Quais são alguns dos pontos fracos em Clipper?"
- a idéia básica da chave de caução é uma violação da liberdade
+ acesso às chaves
- "
+ "Há uma grande porta no lado com um
- grande sinal de néon dizendo: "os Policiais e outras Pessoas Autorizadas
Só";
- o alçapão é o fato de que qualquer pessoa, com fax
a máquina pode fazer
- si e "Pessoa Autorizada" crachá e andar.
<Bill Stewart, bill.stewart@pleasantonca.ncr.com, 4-15-
94, sci.cripta>
- possível volta portas no Skipjace algoritmo
+ geração de custódia de chaves
-
+ "Não há outro alçapão, o que é que se pode
prever a garantia
- chaves roubando os parâmetros utilizados pela Chave
Geração de Mesa
- de defini-los, você não precisa obter a custódia de chaves de
o keymasters,
- você pode gen-las. "<Bill Stewart,
bill.stewart@pleasantonca.ncr.com, 4-15-94, sci.cripta>
9.10.6. Mykotronx
- MYK-78o chip, atrasos, VTI, fusíveis
- National Semiconductor é trabalhar com Mykotronx em um
implementação mais rápida do
Clipper/Topo/Skipjack/qualquer que seja o sistema. (Pode ou não pode
ser conectado diretamente com o iPower linha de produtos. Também,
o processador MIPS core podem ser utilizados, em vez do BRAÇO
o núcleo, que é dito ser muito lento.)
9.10.7. Ataques a ESTRATÉGIA europeia de emprego

- sabotar o caução de base de dados
+ roubá-lo, causando assim um colapso na confiança
- Perry Metzger proposta
- FUD

9.10.8. Qual é o algoritmo que segredo?

9.10.9. Gaiado é de 80 bits, que é de 24 bits de mais de 56 bits do DES. então,

9.10.10. "Quais são as implicações de um bug na Tessera encontrado pelo Matt Blaze?"

- Tecnicamente, Blaze trabalho foi feito em um cartão de Tessera, que implementa o Skipjace algoritmo. O Clipper sistema de telefone pode ser um pouco diferente e os detalhes podem variar; o Incêndio ataque pode até não funcionar, pelo menos não na prática.
- " O anúncio feito no mês passado foi de cerca de uma descoberta que, com uma meia-hora ou mais de tempo, em média, PC, um usuário poderia forjar um falso FOLHAS de dados usado pelo governo para acessar a porta de trás em Clipper criptografia). Com tais um falso FOLHA, o Clipper chip na outra extremidade iria aceitar e descriptografar a comunicação, mas a porta de trás não gostaria de trabalhar para o governo." [Steve Brinich, alt.privacidade.clipper, 1994-07-04]
- "O "final" pré-versão para impressão (datada de 20 de agosto, de 1994) de o meu papel, "Falha de Protocolo no Caucionada Criptografia Padrão" já está disponível. Você pode obtê-lo em PostScript formulário via ftp anônimo de research.att.com em ficheiro /dist/mab/eesproto.ps . Esta versão substitui a anteprojecto (3 de junho) a versão que ocupavam anteriormente o mesmo arquivo. Maior parte da substância é idêntico, apesar de algumas seções são expandidos e alguns pequenos erros está agora corrigido." [Matt Blaze, 1994-09-04]

9.11. Produtos, Versões -- Tessera, Skipjack, etc.

9.11.1. "O que são as várias versões e produtos associados ESTRATÉGIA europeia de emprego?"

- Clipper, o MYK-78 chip.
- Skipjack.
+ Tessera. A placa PCMCIA versão do Caucionada Criptografia Standard.
- a versão de Matt Blaze encontrado um caminho para explodir a FOLHA
- National Semiconductor "iPower" cartão pode ou não pode suporte Tessera (relatos conflitantes).

9.11.2. A AT&T Certeza de Comunicações

- NSA pode ter, pressionando-os a não liberação com DES

produtos
9.11.3. Tessera cartões
- iPower
- Especificações para a Tessera cartão de interface pode ser encontrado
em vários lugares, incluindo "csrc.ncsl.nist.gov"--veja o
arquivo cryptcal.txt [David Koontz, 1994-08-08].

9.12. Status atual do EES, Clipper, etc.
9.12.1. "A Administração realmente de volta em Clipper? Eu ouvi
que Al Gore escreveu uma carta a Rep. Cantwell, fazer logoff."
- Não, mas Clipper perdeu a vapor (empresas não estavam
interessado em comprar um Clipper de telefones, e a AT&T era muito tarde
na obtenção de "Fiador" phones out).
- O Gore anúncio, na verdade, pode indicar uma mudança na
a ênfase na "chave de software de caução" (meu melhor palpite).
- O nosso próprio Michael Froomkin, um advogado, escreve: "A letra é
uma nulidade. Quase cotações do testemunho dado um ano
antes pelo NIST para o Congresso. Obter uma cópia do Senador Leahy
a reação de fora da fep servidor www. Viu-o para o vazio
a coisa é....Nada mudou, exceto Cantwell caiu
o seu projeto de lei para nada." [A. Michael Froomkin,
alt.privacidade.clipper, 1994-09-05]

9.13. Nacional De Infra-Estrutura De Informação, Digital Auto-Estrada
9.13.1. Hype na auto-estrada da Informação
- É contra a lei para falar sobre a Informação
Auto-estrada sem usar pelo menos um dos sobrecarregado de trabalho
metáforas: estrada da mata, pedágio boths, passando faixas de rodagem, ombros,
rampas de acesso, fora de rampas, excesso de velocidade, o I-modo, Infobahn, etc.
- A maior parte do que é agora flutuando em torno de repente-moda
idéia Digital Superduperway é pouco mais do que o hype.
E louco de metáforas. Extravio de zelo, confuso tangencial
a evolução do progresso real. Muito parecido com os libertários
supondo que o programa espacial é algo que deve, de alguma forma,
a trabalhar.
- Por exemplo, a tão badalada "Pizza Hut" na Net (em casa
pizza páginas, eu acho). Ele já está sendo apelidado de "o
primeiro verdadeiro caso de comércio na Internet." Sim, como o Coque de
máquinas na rede de tantos anos atrás, eram exemplos de
O comércio através da Internet. Puro hype. Madison Avenue absurdo. Bom
para o nosso tablóide geração.
9.13.2. "Porque é que o Nacional de Infra-estrutura de Informação é uma má idéia?"
- NII = Superestrada da Informação = Infobahn = Iway = uma dúzia de

outros supostamente inteligente e punning nomes
+ Al Gore proposta:
- links de hospitais, escolas, governo
+ difícil imaginar que a roda livre anarquia do
Internet iria persistir..mais prováveis implicações:
- "é-uma-pessoa" credenciais, isto é, uma prova de identidade,
e, portanto, de acompanhamento, de todas as interações
- médica e psiquiátrica registros seriam parte de
este (psiquiatras estão desconfiados isso, mas eles podem
não tem escolha, mas para cumprir Nacional de Saúde
Planos de cuidados a serem debatidos)
+ Existem outros maus aspectos:
- controle do governo, a ineficiência do governo, governo
snooping
- a distorção dos mercados ("acesso universal")
- restrição de inovação
- não é necessário...outras redes estão fazendo perfeitamente bem,
e será colocado onde eles são necessários e serão
localmente pago
9.13.3. NII, Vídeo de sinal de linha
+ "Tone"
- empresas de telefonia oferecem um limite de conexão e carga
para a conexão, não fazendo decisões sobre o conteúdo (relacionadas
para a "Common Carrier" o estado)
+ vídeo-cabo, eu não acredito que existe um análogo
set-up sendo olhado
+ cabo t.v.
- Carl Kadie comentários para Sternlight
9.13.4. As perspectivas e os perigos da Net subsídios
- "o acesso universal," esp. se o mesmo acontece em cuidados de saúde
- aqueles que pagam fazer as regras
+ mas esse acesso terá strings attached
- limites de criptografia
-
- acesso universal também convida mais de spam, a la
"Freenet" spam, em que a gente conseguir manter validado como
novos usuários: qualquer acesso universal sistema que não está a pagar
você vai ser sensíveis a isso, *ou* irá resultar em chamadas
para IDENTIFICAÇÃO universal de sistema (é-uma-pessoa credentialling)
9.13.5. NII, auto-estrada, o I-modo
- crypto política
- regulamentação, licenciamento de

9.14. Governo do Interesse em obter o Controle do Ciberespaço
9.14.1. Além Clipper, Telefonia Digital, e o Nacional
Infra-estrutura de informação, o governo está interessado em
outras áreas, tais como e-mail de entrega (Serviço Postal dos EUA
proposta) e de manutenção de sistemas de rede em geral.
9.14.2. Telefonia Digital, redes ATM, e trata de ser cortado
- Rumores de negócios que está sendo cortado
- um novo projecto está fora [John Gilmore, 1994-08-03]
- Criptografia de hardware no total ATM velocidades
- e SONET (redes experimentais, Bay Area?)
9.14.3. O USPS planos para o mail, autenticação, efeitos sobre a
a concorrência, etc.
+ Isso poderia ter um efeito devastador sobre a e-mail e em
ciberespaço em geral, especialmente se ele está vinculado a outros
as propostas do governo, em uma tentativa de ganhar o controle de
ciberespaço.
- Digital Telelphony, Clipper, pornografia leis e idade
execução (a Ação Amador caso), etc.
+ "O USPS realmente têm o monopólio de correio de primeira classe?"
- e em "rotas"?
- "O simpático PO foi recentemente visitando o email
os quartos de 2) amigável PO foi recentemente visitando
o correio quartos de empresas na Área da Baía, a abertura de
FedX, etc. pacotes (não protegidos por leis de privacidade de
o PO do correio de primeira classe), e multando empresas (us$10.000
por violação, se bem me lembro), para envio de não-tempo-
os documentos sensíveis, através de FedX, quando poderiam ter sido
enviadas por correio de primeira classe." [Lew Glendenning, USPS
assinatura digital annoucement, sci.cripta, 1994-08-23] (Um
citação ou uma notícia iria fazer isso mais credível,
mas já ouvi falar de semelhante verificações no local.)
- Os problemas com órgãos do governo, concorrentes estão bem
conhecido. Primeiro, eles têm muitas vezes de má qualidade de serviço do serviço civil..
empregos, unfireable trabalhadores, etc. Segundo, muitas vezes, não podem ser
processado por inexecução. Terceiro, eles muitas vezes têm de governo-
concedido monopólios.
+ O USPS proposta pode ser uma abertura baleado em uma tentativa de
controle de ganho de correio eletrônico...ele nunca teve o controle do e-
e-mail, mas o seu monopólio sobre o correio de primeira classe pode ser argüida por
eles estendem ao ciberespaço.
- Nota: a FedEx e o outro pacote e pernoite letra
portadores enfrentam várias restrições no seu serviço, para
exemplo, eles não podem oferecer "rotas" e as economias

o que resultaria num.
- Um USPS aquisição do e-mail de negócios significaria um fim
para muitos Cypherpunks objectivos, incluindo remetentes,
digital postagem, etc.
- O desafio será conseguir estes sistemas implantados como
rapidamente quanto possível, para fazer qualquer aquisição pelo USPS todos
o mais difícil.

9.15. Chave De Software Garantia
9.15.1. (Esta seção precisa de muito mais)
9.15.2. as coisas estão acontecendo rápido....
9.15.3. TIS, Carl Ellison, em Karlsruhe
9.15.4. objeções a tecla de garantia
- "Exploração de depósitos em transações imobiliárias é um clássico
exemplo. Construído-em escutas são *não garantia, a menos que o
o governo é parte do seu contrato. Como alguém no
lista disse uma vez, só porque a Máfia chamar-se
"empresários" não torná-los legítimos; chamar
extorquido escutas "escrow" não é um serviço.

"O governo não tem nenhum negócio, fazendo-me a obter o seu
permissão para falar com alguém sobre qualquer coisa em qualquer
língua que eu escolher, e eles não têm de negócios insistindo eu
comprar "a comunicação do serviço de proteção" de alguns dos seus
amigos para fazê-lo, mais do que o aforenamed
"empresários" têm qualquer negócio insistindo para eu comprar o "fogo
"seguro de *eles*." [Bill Stewart, 1994-07-24]
9.15.5. Micali da "Feira de Custódia"
- vários esforços em curso
- precisa seção aqui
- Observação: os participantes em Karlsruhe relatório de Conferência que um
Grupo alemão podem ter publicado no software key escrow
anos antes Micali arquivado sua patente (relatórios que NSA
os funcionários eram "felizes")

9.16. A Política, A Oposição
9.16.1. "O que deve Cypherpunks dizer sobre Clipper?"
- Uma grande quantidade tem sido escrito sobre esta lista e em dezenas
de outros fóruns.
- Eric Hughes colocá-lo muito bem há um tempo atrás:
- "O hipotético backdoor em clipper é um charlatão
problema através de uma comparação, como é a discussão de como fazer uma chave
sistema de custódia

'trabalho'. Não ser suckered falar de um problema
que não é
importantes. Se alguém quer falar sobre o potencial de volta
portas, recusar-se a se especular. A existência de uma porta da frente
(key escrow) tornar a porta de trás problemas pálido em comparação.

"Se alguém quer falar sobre como chave de custódia de obras,
recusar-se a
elaborada. Dizer que uma determinada chave do sistema de custódia de
é ruim tem uma grande medida de cumplicidade em dizer que
garantia de sistemas, em geral, são OK. Sempre argumentar que este
chave particular sistema de custódia é ruim, porque é uma chave
sistema de custódia, não porque ele tem falhas processuais.

"Este direito problema é que o governo não tem o direito de meu
comunicações privadas. Cada outro problema é o errado
problema e diminui a partir desta central. Se nós derrotar um
sistema particular sem derrotar todos os outros possíveis, tais
sistemas ao mesmo tempo, não ganhamos em tudo; temos
atrasou o momento do acerto de contas." [Eric Hughes, o Trabalho
obra!, 1993-06-01]

9.16.2. O que a maioria dos Americanos pensa sobre Clipper e a privacidade?"
- insights sobre o que estamos diante de
+ "Em um Time/CNN sondagem de 1.000 Americanos, realizado na semana passada,
por Yankelovich
- Parceiros, dois terços disseram que era mais importante para
proteger a privacidade de telefone
- chamadas de preservar a capacidade da polícia para conduzir
escutas.
- Quando informado sobre o Clipper Chip, 80% disseram que
opôs-se a ela."
- Philip Elmer-Dewitt, "Quem Deve Manter as Chaves", o Tempo,
Mar. 4, de 1994

9.16.3. Alguém, na verdade, suporte Clipper?
+ Na verdade, existem usos legítimos para formas de garantia:
- sociedades
- outras parcerias

9.16.4. "Que se opõe ao Clipper?"
- Association for Computing Machinery (ACM). "O USACM insta
a Administração, neste momento, retirar o Clipper
Chip de proposta e para começar, uma aberta e pública de revisão do
política de criptografia. O caucionadas criptografia iniciativa
levanta questões vitais de privacidade, aplicação da lei,

a competitividade e a inovação científica que deve ser
discutidas abertamente." [EUA ACM, DC Office" <usacm_dc@acm.org>,
USACM Chamadas para Clipper Retirada, comunicado de imprensa, 1994-06-
30]
9.16.5. "O que há de tão ruim chave de caução?"
+ Se é realmente voluntária, não pode ser um uso válido para isso.
+ São alçapões justificada em alguns casos?
+ Empresas que desejam recuperar os dados criptografados
+ vários cenários
- empregado criptografa arquivos importantes, então morre ou é
caso contrário não disponível
+ funcionário sair da empresa antes de desencriptação de todos os arquivos
- alguns podem ser arquivados e não precisava ser aberto
por muitos anos
- o empregado poderá exigir o "resgate" (intimamente relacionado com
vírus extorsão casos)
- os ficheiros são encontrados, mas o original encryptor é
desconhecido
+ Provável situação é que os algoritmos de encriptação será
mandatado pela corporação, com uma "chave mestra" mantidos
disponível
- como de um alçapão
- a existência de uma chave mestra pode até não ser
divulgados dentro da empresa (de cabeça preocupações
sobre a segurança, abusos, etc.)
+ Governo está a tentar obter os alçapões colocar em
- S. 266, que falhou por fim (mas não antes de
a criação de um ruckus)
+ Se o governo exige que ele...
- Key escrow significa que o governo pode estar dentro de sua casa
mesmo sem você saber
- e a chave de caução não é realmente garantia...o que é que um ser
de volta da "custódia" de serviço?
9.16.6. Por que os governos não devem ter chaves
- pode, em seguida, definir as pessoas pelo fingimento de mensagens, com o plantio de
provas
- pode espionar objectivos para os seus próprios fins (que história
diz-nos pode incluem o suborno, espionagem corporativa, drogas
execução, assassinatos e toda sorte de ilegal e
desprezível atividades)
- pode sabotar contratos, negócios, etc.
- gostaria de dar-lhes acesso a interna, comunicação corporativa
- prejudica toda a validade de tais contratos e de

padrões de criptografia de identidade (vibrações de confiança)
- dando o Rei ou o Estado o poder de representar
o outro é uma grave injustiça
- imagine que o governo do irã de ter um backdoor para ler
o segredo periódicos de seus súditos!
- 4ª Alteração
- privilégio de advogado-cliente (com alçapões, nenhuma maneira de saber
que o governo não foi violada a confidencialidade)
9.16.7. "Como pode o Clipper chip ser frustrado ou derrotado?"
- Politicamente, mercado de sábio, e o técnico
- Se implantado, que é
+ Maneiras para Derrotar Clipper
- preencryption ou superencryption
- Soprador de FOLHAS
- plug-compatível, engenharia reversa chip
- sabotagem
- minando a confiança
- Sun Tzu
9.16.8. Como pode Clipper ser derrotado politicamente?
9.16.9. Como pode Clipper ser derrotado, no mercado?
9.16.10. Como pode Clipper ser derrotado, tecnologicamente?
9.16.11. Perguntas
+ Clipper questões e perguntas
- um grande número de perguntas, comentários, desafios,
dicas, detalhes, de questões
- toda a grupos de notícias dedicado a este
+ "O que o criminoso ou terrrorist vai ser inteligente o suficiente para usar
criptografia burra o suficiente para usar Clipper?"
- Esta é uma das Grandes Perguntas sem Resposta. Clipper da
torcedor do são mãe em um presente. Sugerindo....
+ "Por que não criptografar os dados antes de utilizar o Clipper/EES?"
- "Por que você não pode criptografar os dados antes de o clipper chip?

Duas respostas:

1) as pessoas que você deseja comunicar-se com o não ter
hardware para
descriptografar seus dados, estatisticamente falando. A beleza
de clipper
a partir da NSA, o ponto de vista é que eles estão aproveitando
o
base instalada (esperam) de telefones e tornando-o
impossível

(novamente, estatisticamente) para uma grande fração do
tráfego
untappable.

2) Eles não vão licença mau pessoas como você para fazer
equipamentos como o
sistema de descrever. Eu vou apostar que o chip
a distribuição será
feito de maneira a evitar um número significativo de tais
sistemas de
sendo construído, garantindo que (1) continua a ser verdade." [Tom
Cavaleiro, sci.cripta, 6-5-93]

-
+ Quais são as implicações obrigatório chave de caução?
+ "escrow" é enganosa...
- errado, o uso do termo
- implica um voluntário, e retornáveis, situação
+ "Se a chave de caução é "voluntária" qual é o grande negócio?"
- Os impostos são supostamente "voluntária" também.
- Um homem sábio se prepara para o que é _possible_ e até mesmo
likely, não apenas o que é anunciado como parte do público
política; políticas podem e mudam. Há uma abundância de
precedente para uma "voluntária" do sistema a ser obrigatória.
- A forma do Clipper/EES sistema sugere eventual
obrigatória estado; a forma de tal proibição é discutível.
+ "O que é 'superencipherment", e pode ser usado para derrotar
Clipper?"
- preencrypting
- poderia ser visto como uma língua não-inglesa
+ como poderia Clipper chip saber sobre ele (entropia medidas?)
- far-fetched
- não iria resolver o tráfego anal. problema
- Qual é a conexão entre a corte e as leis de exportação?
+ "Não fazer o Clipper base de dados ripe-alvo?"
- para o subversion, sabotagem, espionagem, roubo
- presumivelmente cópias de segurança será mantida, e _these_ também será
objectivos
+ "É Clipper apenas para encriptação de voz?"
- Clipper é um chip de criptografia de dados, com os dados digitais
fornecido por um ADC localizado fora do chip. No
a princípio, ele poderia, assim, ser utilizados para a criptografia de dados em
de modo geral.

- Na prática, o nome Clipper é geralmente associado
com o uso do telefone, enquanto "Capstone" é o padrão de dados
(algumas diferenças, também). O "Skipjack" é utilizado o algoritmo de
em vários desses sistemas propostos (Tessera, também).
9.16.12. "Por que é Clipper pior do que o que temos agora?"
+ John Gilmore, respondeu a essa pergunta em um bom ensaio. Eu sou
incluindo a coisa toda, incluindo uma digressão em
telefones celulares, porque dá uma visão--e
nomes de alguns nomes de NSA mentirosos--de como a NSA e NIST ter
usado seus poderes para impedir a verdadeira segurança.
- "É pior porque o mercado continua se movendo em direção a
de forma real de criptografia.

"Se Clipper tiver êxito, será através do deslocamento real
criptografia segura. Se o real encriptação segura torna
em massa do mercado de produtos de comunicação, Clipper vai
falharam. A questão toda não é para obter algumas
Clippers usado por policiais; o ponto é que para torná-lo um
padrão em todo o mundo, em vez de ter 3 chave triplo-DES
com o RSA e o grupo Diffie-Hellman tornar o mundo
standard.

"Teríamos digno de criptografia digital telefones celulares
agora, exceto para a intervenção ativa do Jerry
Rainville da ANS, de quem "organizou" uma reunião dos padrões
comissão de dentro Pés. Meade, mentiu sobre exportação
controle para manter comitê de documentos limitado a um pequeno
grupo, e tenho uma vontade de enganar da Motorola, Louis
Finkelstein, para propor um esquema de encriptação de uma criança
poderia quebrar. O is-54-padrão digital de telefonia celular
não descrevem o esquema de criptografia-é descrito
em um documento separado, que as pessoas comuns não podem ficar,
apesar de parte do funcionário credenciado
standard. (Acho que credencia organismos de normalização embora -
- está certo, uma vez que o puro NIST.)

"A razão do segredo é porque, obviamente,
fraco. O sistema gera 160 bits "chave" e, em seguida,
simplesmente XORs contra cada bloco de comprimido
a fala. Levar qualquer um a dez ou de vinte blocos e recuperar a
chave XORing frequentes padrões de fala (como o silêncio, ou
a letra "a") contra peças dos blocos para produzir
tenta adivinhar a chave. Você experimente cada um acho que em alguns blocos,

e a probabilidade de produzir algo que decodifica
como fala em todos os blocos é pequeno o suficiente para que você vai
sabe quando o seu palpite é a verdadeira chave.

"A ANS está continuando a sujeira ao redor no Celular Digital
comitê de padrões (TR 45.3) este ano. Eu encorajo
quem está interessado a participar da comissão, talvez como
um observador. Contato com o Setor de Telecomunicações
Associação de DC e inscreva-se. Como as normas
o comitê, que é aberto ao público e reúne-se em vários
lugares por todo o país. Eu vou dar uma de advogado se
você é um estrangeiro, uma vez que a comissão pode ainda
acredito que eles devem excluir os estrangeiros do
a discussão pública de criptografia. De alguma forma, a criptografia
conferências não têm nenhum problema com isso; eu acho que é
chamou a Primeira Alteração. NSA conhece a lei aqui --
de fato, impõe-lo através do Departamento Estadual -- mas mentiu para
o comitê". [John Gilmore, "Por que é clipper pior do que
"sem criptografia, como nós o temos," comp.org.fep.falar, 1994-04-
27]

9.16.13. no confiando o governo

- "O QUE TENHO A MORAL DA HISTÓRIA, TIO REMUS?....Quando o
governo faz qualquer anúncio (ESPECIALMENTE uma negação),
você deve descobrir o que o governo está a tentar obter
você fazer--e não o oposto. Contrarianism com um
vengance. De todos os conselhos que eu já oferecidos no
Cypherpunks Canal, este é absolutamente o mais certo."
[Sandy Sandfort, 1994-07-17]
- se os Fundadores dos estados unidos poderia ver o corrupto,
estado socialista, esta nação degenerou para eles seriam
quebrar os silos de mísseis e roubo de armas nucleares para uso
contra o poder central da base de dados.

+ o governo pode ser confiável para executar a chave do sistema de custódia?

- "Eu só ouvi a notícia de que mais de 1300 funcionários têm IRS
foram disciplinados por acessos não autorizados para
eletronicamente arquivados declarações de imposto de renda. ..Eu tenho certeza que eles
vai fazer muito melhor, porém, quando o FBI corre o telefone
sistema, o Post Office controles de identidade digital e
Hillary, que cuida da nossa saúde." [Sandy Sandfort, 1994-
07 a 19]
- Este é apenas um dos muitos exemplos: o caso Watergate ("eu sou
não é um bandido!"), Iran-Contras, braços negócios, a cocaína
envios pela CIA, Teapot Dome, enxerto, pagamentos de salários,

a corrupção, assassinatos, Yankee-Cowboy Guerra, Boêmio
Grove, Casolaro, mais assassinatos, invasões, guerras. O
governo que é medroso demais para jamais admitem perder uma
guerra, e, acentuadamente, evita o contacto diplomático com
inimigos não conseguiu vencer (Vietnã, Coréia do Norte,
Cuba, etc.), enquanto rapidamente se tornando papaizinho para o
países fez vencer...os EUA parece ser
falta praticidade. (Me, eu considero que é errado
que ninguém diga que eu não posso negociar com pessoas de outro
país, se é o Haiti, África do Sul, Cuba, Coreia,
seja o que for. Crypto anarquia significa que nós vamos ter _some_ do
maneiras de burlar essas leis, de fazer a nossa própria moral
decisões sem levar em conta o vigor populares
o sentimento dos países em que vivemos no
de momento.)

9.17. Questões jurídicas com Caucionada Criptografia e Clipper
9.17.1. Como John Gilmore colocá-lo em um convidado editorial no "San
Francisco Examiner," "...a gente quer que o público veja uma grave
o debate sobre por que a Constituição deve ser queimado em ordem
para salvar o país." [J. G., 1994-06-26, citado por S.
Sandfort]
9.17.2. "Eu não vejo como Clipper confere ao governo poderes ou
recursos que ela já não tem. Comentários?"
9.17.3. É Clipper realmente voluntário?
9.17.4. Se o Clipper é voluntário, que vai usá-lo?
9.17.5. Restrições de Uso Civil de Criptografia
9.17.6. "Tem de criptografia sido restrito nos EUA?"
9.17.7. "Que legal que medidas estão sendo tomadas?"
- Zimmermann
- ITAR
9.17.8. relata que o Departamento de Justiça tem um cumprimento
execução papel na ESTRATÉGIA europeia para o emprego [ouvida por alguém de Dorothy
Denning, 1994-07], provavelmente envolvendo a verificação de que a lei
as agências de aplicação da...
9.17.9. Estado
+ "Será que o governo vai agências Clipper?"
- Ah, a constrangedora pergunta. Eles afirmam que eles vão, mas
existem também relatos de que sensíveis agências não
usá-lo, que o Clipper é inseguro demais para eles (a chave
de comprimento, de compromisso de garantia de dados, etc.). Também pode
ser diferentes procedimentos (todas as agências são iguais, mas alguns
são mais iguais do que outros).

- Clipper está classificado para a construção de usar, para esse regras
muitas agências e muitos usos. Uma interessante dupla
standard.
+ "É a Administração de backup fora do Clipper?"
+ indústria oposição surpreendeu
- grupos de no verão passado, o Citicorp, etc.
- opinião pública
- editorial comentários
- então eles podem estar preparando alternativa.
- e Gilmore FOIA, Blaze ataque, o Denning
nonreview, o segredo das algortithm
+ não vai funcionar
- espiões não usá-lo, criança "the pornographers" provavelmente não
usá-lo (se existem alternativas, que podem ser toda a
ponto)
- os terroristas não usá-lo
- É Clipper em apuros?
9.17.10. "Vai Clipper ser voluntário?"
- Muitos adeptos do Clipper ter citado a natureza voluntária
de Clipper--como expresso em algumas declarações de política--e
tenho usado isso para contrariar a crítica.
+ No entanto, mesmo se realmente voluntária, algumas questões
+ inadequada papel do governo para tentar criar uma
comercial padrão
- embora o NIST papel pode ser usado para combater este ponto,
em parte,
o governo pode e faz com que seja difícil para os concorrentes
- controles de exportação (declarações oficiais sobre este existir)
+ Cita voluntário de status:
- declaração original diz que vai ser voluntário
- (necessário obter algumas declarações aqui)
+ Cites para eventual obrigatório de status:
- "Sem essa iniciativa, o governo irá, eventualmente,
tornar-se impotente para defender a nação." [Louis Freeh,
diretor do FBI, várias fontes]
- Steven Walker Confiáveis Sistemas de Informação é um dos
muitos que pensam assim: "com Base em sua análise, Walker adicionado,
"Estou convencido de que em cinco anos a partir de agora, eles vão dizer 'Este
não está funcionando', então nós vamos ter que mudar as regras." Em seguida,
ele previu, Clipper vai ser obrigatória para todos os
codificado de comunicações." [
+ Paralelos para outros programas voluntários
- impostos

9.18. Preocupações
9.18.1. Questões Constitucionais
4º Alterar
- privacidade do cliente-advogado, etc.
+ Pf pode ter acesso sem audiências públicas, registros
- segredo de inteligência tribunais
-
+ "É incontestável (até onde eu li) que, sob
certos circum-
- posições, a comunidade de inteligência Federal wil ser
permitido
- obter Clipper chaves, sem qualquer ordem judicial em público
gravar. Apenas
- interno, classificada processos de proteger as nossas
privacidade." <Steve Waldman, steve@vesheu.sar.usf.edu,
sci.cripta, 4-13-94>
9.18.2. "Quais são alguns dos perigos de Clipper, se ele é amplamente adotado?"
+ remetente/receptor de IDENTIFICAÇÃO são acessíveis sem ir para a chave
garantia
- isso não faz análise de tráfego, listas de contato, fácil
gerar
+ distorções dos mercados ("chilling effects") como um plano de
governo
- faça alternativas caro, difícil de exportação, os motivos do
suspeita
- uso de ITAR para impedir alternativas (seria ajudou a se
Cantwell projeto de lei para liberalizar controles de exportação de
criptografia de RH (3627) passa)
+ VHDL implementações possíveis
- especula Lew Glendenning, sci.cripta, 4-13-94
- e lembre-MIPS de ligação (ser cuidado)
9.18.3. Mercado Isssues
9.18.4. "Quais são os pontos fracos em Clipper?"
+ Carl Ellison analisados desta forma:
- "Diverte-forca-humor osso em me ver as pessoas
ocupado debater a qualidade do Skipjack como um algoritmo
e a qualidade da revisão de sua força.

Alguém se propõe a oscilar sobre o Grand Canyon
usando

linha de costura

amarrado a
corrente de aço
amarrado a
tricô fio

e você está debatendo se a corrente de aço foi X-
raio corretamente para ver se há falhas no metal.

"A geração da chave, o chip de fabricação, ordens judiciais,
distribuição de chaves, uma vez adquirida a partir de custódia de agências
e de segurança de chaves, dentro de caução agências são algumas das
real fraquezas. Uma vez que aqueles são tão fortes como o meu uso de
RSA de 1024 bits e verdadeiramente aleatória de chaves de sessão em manter
chaves nos dois lados de uma conversa com ninguém
o meio capaz de pegar a chave, então precisamos olhar
a cadeia de aço no meio: Skipjack em si." [Carl
Ellison, 1993-08-02]
+ Data: segunda-feira, 2 de Agosto de 93 17:29:54 EDT
A partir de: cme@ellisun.sw.stratus.com (Carl Ellison)
Para: cypherpunks@toad.com
Assunto: cross-post
Status: OU

Caminho: transfer.stratus.com!ellisun.sw.stratus.com!cme
A partir de: cme@ellisun.sw.stratus.com (Carl Ellison)
Grupos de notícias: sci.cripta
Assunto: Skipjack revisão como um lado-track
Data: 2 de Agosto de 1993, 21:25:11 GMT
Organização: Stratus Computador, Marlboro MA
Linhas: 28
Message-ID: <23k0nn$8gk@transfer.stratus.com>
NNTP Anfitrião de registo: ellisun.sw.stratus.com

Diverte-forca-humor osso em me ver as pessoas
ocupado o debate
qualidade do Skipjack como um algoritmo e a qualidade de
a revisão de suas
força.

Alguém se propõe a oscilar sobre o Grand Canyon
usando

linha de costura
amarrado a
corrente de aço
amarrado a
tricô fio

e você está debatendo se a corrente de aço foi X-
raio corretamente
para ver se há falhas no metal.

Geração de chave, chip de fabricação, ordens judiciais,
distribuição de chaves de uma vez
adquirida a partir de custódia de agências e de segurança de chaves, dentro
garantia agências
alguns dos verdadeiros pontos fracos. Uma vez que aqueles são tão fortes como
o meu uso de
RSA de 1024 bits e verdadeiramente aleatória de chaves de sessão em manter
chaves nos dois lados
de uma conversa com ninguém no meio capaz de obter
a chave, então nós
precisamos olhar para a cadeia de aço no meio: Skipjack
em si.

- "A geração da chave, o chip de fabricação, ordens judiciais,
distribuição de chaves, uma vez adquirida a partir de custódia de agências
e de segurança de chaves, dentro de caução agências são algumas das
o real fraquezas. Uma vez que aqueles são tão fortes quanto os meus
o uso do RSA de 1024 bits e verdadeiramente aleatória de chaves de sessão em
manter as chaves dos dois lados de uma conversa com nenhum
no meio capaz de pegar a chave, então precisamos
olhe para a cadeia do aço no meio: Skipjack
em si."

9.18.5. O que isso Significa para o Futuro

9.18.6. Gaiado

9.18.7. Exceções de segurança nacional

- grep Gilmore FOIA para mencionar que a segurança nacional
as pessoas vão ter acesso direto e que isso não vai ser
mencionados para o público
+ "O "Segurança Nacional" exceção construído em Clipper
proposta
- deixa extraordinariamente elo fraco na cadeia de
procedimentos
- para proteger a privacidade do usuário. Para colocar incríveis poderes de

vigilância
- tecnologicamente ao alcance de alguns, na esperança de que assim
fraco de uma cadeia
- vai ligá-los, teria um valor perigoso loucura. Ele
voa na cara
- da história. <Steve Waldman, steve@vesheu.sar.usf.edu, 4-
14-94, falar.política.criptografia>

9.18.8. No meu ponto de vista, qualquer foco nos detalhes do Clipper, em vez de
o conceito geral de chave de caução desempenha em suas mãos.
Isto não é para dizer que o trabalho de Blaze e os outros é
equivocado....na verdade, é muito bom trabalho. Mas uma geral
foco no _details_ do Skipjack não faz nada para aliviar o meu
preocupações sobre a _principle_ do governo com mandato de criptografia.

Se fosse "chave da casa de custódia" e lá estavam faltando detalhes
sobre o número de dentes permitido nas teclas, seria, então,
todos respirar um suspiro de alívio se os detalhes dos dentes foram
esclareceu? Claro que não. Mim, eu nunca vou usar uma chave de caução
sistema, mesmo se a fita azul do painel de hackers e
Cypherpunks estudos o projeto e declara que ele seja
criptograficamente de som.

9.18.9. Preocupação sobre Clipper
- permite comunicações passado para ser lido
+ autoridades poderiam--talvez--li um monte de coisas, mesmo
ilegalmente, em seguida, usar isso para outras investigações (antigo
"tivemos um anônimo" dica de manobra)
- "O problema com o Clipper é que ele fornece polícia
agências com dramaticamente melhorada alvo de aquisição.
Não há nada para impedir a NSA, ATF, o FBI (ou Especial
Divisão de projetos do Departamento de Justiça) a partir de
a revisão de todo o tráfego da internet, contanto que eles são
disposta a deixar de usá-lo em um processo criminal."
[dgard@netcom.com, alt.privacidade.clipper, 1994-07-05]

9.18.10. Algumas pessoas têm sugerido que a nova caução de agências de ser
escolhidos a partir de grupos como a Anistia Internacional e a ACLU.
A maioria de nós está em oposição à "ideia" de key escrow
(acho que de ser dito para garantia fotos de família, diários, ou
as chaves de casa) e assim, mesmo a esses tipos de céticos grupos
são inaceitáveis como depositários.

9.19. Pontas Soltas

9.19.1. "São alçapões--ou alguma forma de caucionada criptografia--
justificada em alguns casos?"

+ Com certeza. Existem várias razões para que indivíduos, empresas, etc. pode querer usar criptografia, protocolos que permitem a eles descriptografar mesmo se eles perderam a chave, talvez indo para o advogado e a obtenção de novo o envelope selado eles esquerda com ele, etc.
- ou através de um formulário de "software key escrow", que permite acesso
+ Empresas que desejam recuperar os dados criptografados
+ vários cenários
- empregado criptografa arquivos importantes, então morre ou é caso contrário não disponível
+ funcionário sair da empresa antes de desencriptação de todos os arquivos
- alguns podem ser arquivados e não precisava ser aberto para muitos anos
- o empregado poderá exigir o "resgate" (intimamente relacionado com vírus extorsão casos)
- os ficheiros são encontrados, mas o original encryptor é desconhecido
+ Provável situação é que os algoritmos de encriptação será mandatado pela corporação, com uma "chave mestra" sempre disponível
- como de um alçapão
- a existência de uma chave mestra pode até não ser divulgados dentro da empresa (para a cabeça de preocupações sobre a segurança, abusos, etc.)
- A obrigatoriedade de uso de chave de caução, a la obrigatória Clipper sistema, ou o sistema de muitos de nós acredita que está sendo desenvolvido para software key escrow (SKE, também chamado de "NÃO," para "governo o acesso a chaves, por Carl Ellison) é completamente diferentes, e é inaceitável. (Clipper é discutido em muitos lugares aqui.)

9.19.2. DSS

+ De continuar a confusão sobre patentes, normas, licenciamento, etc.
- "FIPS186 é DSS. O NIST é da opinião de que DSS não violar PKP de patentes. PKP (ou, pelo menos, Jim Bidzos) leva a posição que ele faz. Mas por várias razões, PKP não vai processar o governo. Mas Bidzos ameaça processar festas privadas que infringir. Fique atento...." [Steve Wildstrom, sci.cripta, 1994-08-19]
- mesmo Taher ElGamal acredita que é um fraco padrão
- subliminar canais de problemas

9.19.3. Os EUA são, muitas vezes, hipócrita sobre direitos básicos

- planos para "desarmar" os Haitianos, como fizemos para o Somalians (o que tornou aqueles que desarmado ainda mais vulnerável aos

local senhores da guerra)
- funcionários do governo está propondo para o "silêncio" de uma rádio
estação em Ruanda eles sentem é o envio de errado
mensagem! (Ouviu falar em "McNeil-Lehrer Notícias de hora em Hora," 1994-07-21]
9.19.4. "é-uma-pessoa" e RSA-estilo de credenciais
+ uma idéia perigosa, de que o governo vai insistir que as teclas de ser
ligados a pessoas, com apenas um por pessoa
- esta é uma falha no sistema AOCE
- muitos aplicativos que precisam de novas chaves geradas muitas vezes

10. Questões Legais

10.1. direitos autorais
O CYPHERNOMICON: Cypherpunks FAQ e Mais, Versão 0.666,
1994-09-10, Direitos De Autor Timothy C. De Maio. Todos os direitos reservados.
Veja os detalhes de isenção de responsabilidade. Use seções curtas em "justo
use" disposições, com crédito apropriado, mas não coloque o seu
nome em minhas palavras.

10.2. RESUMO: Questões Legais
10.2.1. Pontos Principais
10.2.2. Ligações para Outras Secções
- É triste dizer, mas as considerações legais incidem em cerca de
cada aspecto de criptografia
10.2.3. Onde Encontrar Informações Adicionais
10.2.4. Diversos Comentários
- "Eu sou um cientista, Jim, não um advogado." Portanto, tome o meu
jurídico comentários aqui com um grão de sal, que representam apenas
dicas de verdade, como eu lia, a partir das discussões
em vários fóruns e listas.

10.3. Básicos da Legalidade de Criptografia
10.3.1. "É isso é legal ou ilegal?"
- Certamente o _talking_ sobre ele é mais legal, pelo menos
nos EUA e no momento da redação deste artigo. Em outras
países, a pena de prisão pode variar.
+ Ações resultantes de criptografia, e de criptografia anarquia, pode
bem ser ilegal. Como é frequentemente o caso quando a tecnologia é
aplicada sem qualquer sentido para o que as leis dizem
é permitida. (A Caixa de Pandora e tudo mais.)
- Cypherpunks realmente não me importo muito com tais trivialidades como
as "leis" de alguns região geográfica. Cypherpunks fazer
suas próprias leis.

+ Existem duas grandes formas de fazer as coisas:
- Primeiro, observando a legislação e normas e de encontrar
formas de explorá-los. Esta é a aderência favorecido pela
advogados, dos quais$são muitos neste país.
- Em segundo lugar, "just do it". Em áreas onde a lei não
pego, isso pode significar irrestrita tecnológica
de desenvolvimento. Bons exemplos são o computador e o chip
de negócios, onde as questões de legalidade raramente se levantou (exceto
nas áreas habituais de execução de contratos, etc.). Mais
recentemente, o negócio de chips descobriu advocacia, com
uma vingança.
- Em outras áreas, onde a lei está centralmente envolvido,
"just do it" pode significar muitas técnicas violações dos
lei. Exemplos: serviço de pessoal de tarefas (domésticas e
baby-sitters), a contratação de postos de trabalho sem licenças,
permissões, etc., e assim por diante. Muitas vezes, estes são "ilegais
mercados," supostamente.
- E tenha em mente que o sistema jurídico pode ser usado para
complicações as pessoas, para pressioná-los a "suplicar" para alguns
encargos, para fazer logoff, etc. (Em as armas de fogo de negócios, o
pressões e ameaças também são usadas para causar algum
fabricantes, como a Ruger, para fazer logoff em um radical pro-arma
postura, de modo a ser concedido favores e mais leves do tratamento.
A pressão sobre a criptografia-empresas de produção são, provavelmente, muito
semelhantes. Jogar bola, ou nós vamos executar você no estacionamento
muito.)
10.3.2. "Qual é o estatuto jurídico de criptografia tão sombrio?"
- Primeiro, pode ser mais opaca para mim do que para a real advogados
como Mike Godwin e Michael Froomkin, ambos os quais têm
foi na nossa lista, às vezes. (Embora a minha impressão de
falando para Godwin é que muitos ou mesmo a maioria dos problemas
não foram abordadas nos tribunais, e muito menos resolvido
definitivamente.)
- Em segundo lugar, problemas criptografia geralmente não atingiu a
tribunais, refletindo o nascente estado da maioria das coisas
falei sobre ele aqui. Coisas como "trivial" como digital
e assinaturas digitais do módulo de ainda não ser
contestada em tribunais, ou declarado ilegal, ou qualquer coisa
semelhantes que possam produzir um precedente definição de sentença. (Stu
Haber concorda que tais testes estão faltando.)
- Finalmente, as questões são profundas, indo para o coração de
questões de auto-incriminação (divulgação de chaves,
o desprezo), de propriedade intelectual e leis de exportação (quer

para a prisão de alguém para falar sobre números primos?), e o
incrivelmente bizantino, mundo do dinheiro e financeira
instrumentos.
- Um estudo jurídico de criptografia, que eu ouvir o Professor é Froomkin
fazendo-poderia ser muito importante.
10.3.3. "Tem o básico da legalidade de criptografia e leis sobre criptografia sido
o teste?"
- Como de costume, o foco dos EUA aqui. Eu sei pouco da situação
em non-U.S. países (e em muitos deles a lei é
o que os governantes dizem que é).
- E eu não sou um advogado.
+ Alguns fatos:
- não direto Constitucional a declaração sobre a privacidade (que
muitos acham que é implícita)
- crypto não era um grande problema (espionagem foi, e foi
tratados duramente, mas a criptografia de coisas não era um
problema per se)
+ só nos últimos anos tem-se tornado importante...e
vai se tornar muito mais
- como criminosos, criptografar, como terroristas criptografar
- como o imposto é evitado através de técnicas descritas aqui
- conluio de negócios ("crypto intertravamento
direcções," preço de sinalização)
- preto mercados, informação de mercados
+ Lawrence Tribo..nova alteração
- assustador, como pode colocar limites.... (mas improvável
acontecer)
+ De criptografia no Tribunal
- a maioria não testado
- pode teclas de ser obrigado?
- Espere alguns casos importantes nos próximos anos
10.3.4. "Pode autoridades forçar a divulgação de uma chave?"
+ Mike Godwin, consultor jurídico da FEP, foi perguntado sobre isso
queston _many_ vezes:
- "Note que um tribunal poderia citar-lhe para o desprezo não
o cumprimento da intimação reduz tecum (uma intimação
exigir que você produzir objetos ou documentos) se
falha ao virar intimada cópias de segurança....Para ser honesto, eu
não acho que *qualquer* medida de segurança é adequada contra um
o governo que está determinado a sair de sua autoridade
e seus direitos de cidadãos, mas de criptografia chega perto." [Mike
Godwin, 1993-06-14]
+ Tortura está fora (em muitos países, mas não em todos). Verdade

soro, etc., idem.
- "Mangueira de borracha de criptografia"
+ Questões constitucionais
- a auto-incriminação
+ sobre o "Sim" do lado:
+ é mesmo, dizem alguns, como forçar a combinação de um cofre
que contenham informações ou bens roubados
- mas alguns dizem-e um tribunal pode ter decidido sobre isso-que
o seguro pode sempre ser cortados e abertos, e assim, a questão é
principalmente simulado
- ao forçá-chave divulgação é compelido testemunho
- e pode-se sempre alegar ter esquecido a chave
- por exemplo, o que acontece quando um suspeito simplesmente amêijoas até?
- mas as autoridades podem rotineiramente demanda de cooperação em
investigações, pode aproveitar os registros, etc.
+ sobre o "Não" lado:
- não pode forçar um suspeito para falar, seja sobre onde ele se escondeu
o saque ou onde sua sequestrar a vítima está escondido
- praticamente falando, alguém sob acusação não pode ser
forçado a revelar banco Suíço contas....isso parece
para ser diretamente análoga a uma chave criptográfica
- assim, a chave para abrir uma conta, parece ser a
mesma coisa
- um memorizado chave não pode ser forçado, diz alguém com FEP
ou CPSR
+ "Seguro" analogia
+ Você tem um seguro, não conte a combinação
- você simplesmente se recusam
- você alega ter esquecido que
- você realmente não sabe
- cops pode cortar o cofre aberto, de forma convincente uma combinação
não é necessário
- "interefering com uma investigação"
- no balanço, parece claro que a divulgação do
chaves de criptografia não pode ser forçado (embora a prática
penalidade para a não-divulgação pode ser grave)
+ Tribunais
+ compelido testemunho é certamente comum
- se não é cobrado, não se pode tomar o 5º (pode ser
algumas rugas aqui)
- desprezo
+ O que não imunizar divulgação:
+ inteligente piadas sobre "eu sou culpado de lavagem de dinheiro"

- pode ser usada?
- o juiz declarar a imunidade se aplica neste caso?
- Eric Hughes destacou que a forma de o
instrução é a chave: "a Minha chave é: "eu sou um assassino."" é
não é uma admissão legal de qualquer coisa.
- (Pode haver algumas sutilezas que a chave não conter
evidências importantes-talvez a localização de um corpo enterrado-
-mas eu acho que essas questões são relativamente pequenos.)
- mas este não foi realmente testado, tanto quanto eu sei
- e muitas pessoas dizem que essa cooperação pode ser
exigiu...
- Desprezo, declarações de esquecer
10.3.5. Esquecer senhas, e o testemunho
+ Esta é outra área de intensa especulação:
- "Eu esqueci. Então me processar."
- "Eu esqueci. Foi apenas um arquivo temporário que estava a trabalhar,
e eu simplesmente não consigo lembrar a senha que eu escolhi." (Menos um
face-a-face abordagem.)
+ "Eu me recuso a dar a minha palavra-passe no argumento de que ele pode
tendem a incriminar-me."
+ Exemplo canônico: "Minha senha é: 'eu vender ilegal
a droga.'"
- Eric Hughes destacou que este não é um real
admissão de culpa, apenas um forma sintática, portanto, é
um absurdo a afirmação de que ele é delator. Estou de acordo.
Eu não sei se qualquer tribunal testes confirmaram isso.
+ Sandy Sandfort teoriza que este exemplo pode funcionar, ou
pelo menos, levar a uma interessante legais dilema:
- "Por exemplo, a frase poderia ser:

Eu tiro um policial na parte de trás e enterrou seu corpo
sob
o pórtico em 123 Main St., em qualquer lugar dos EUA. A arma
é
envolto em um oleosa pano na casa da minha mãe no sótão.

"Me recuso a responder, alegando que a minha senha é
uma instrução que tendem a incriminar-me. Eu
apenas a dar a minha senha se eu tenho imunidade de
ministério para as ações a que ele alude."

"Muito bonito, eu sei, mas quem sabe, ele poderia funcionar." [S. S.,
1994-0727]

10.3.6. "O que sobre a rejeição do chaves? De assinaturas digitais? De contratos?
- No curto prazo, os tribunais são relativamente silenciosa, como poucos estas questões têm atingido os tribunais. Coisas como assinaturas de contrato e violações poderiam ser tratadas como atualmente (isto é, o juiz deve observar a circunstâncias, etc.)
+ É claro que esta é uma grande preocupação. Existem duas principais vias de lidar com isso"
- O "purista" abordagem. Você *são* sua chave. Contrapartidas. Guardar suas chaves. Se a sua assinatura é usado, o responsável. (As pessoas podem diminuir a sua exposição, utilizando protocolos de limite de risco, de forma semelhante à maneira ATM os sistemas permitem apenas, digamos, us $200 por dia para ser retirado.)
- O sistema jurídico pode ser usado (talvez) para lidar com essas questões. Talvez. Pouco tem sido testada nos tribunais. Os métodos convencionais de verificar a falsificação de assinaturas vai não trabalho. A lei do contrato com assinaturas digitais será um nova área.
- O problema do *repúdio* ou *a rejeição* foi reconhecido logo no início da cryptologic círculos. Alice confronta-se com uma assinatura digital, ou seja o que for. Ela diz: "Mas eu não sinal de que", ou "Oh, essa é a minha chave antiga--é obsoleto" ou "Meu sysadmin deve ter visualizada através de meus arquivos", ou "eu acho que os key escrow caras são tudo de novo."
- Eu acho que só a postura purista vai reter a água no longo prazo.(Uma dica de presente: untraceable dinheiro significa, para a maioria dos operações de interesse com dinheiro digital, uma vez que o crypto coisas tem sido tratada, se o sig foi roubado ou não é discutível, porque o dinheiro acabou...nenhum tribunal pode regra de que o sig foi inválido e, em seguida, recuperar o dinheiro!)
10.3.7. "O que são alguns argumentos para a liberdade para criptografar?"
- proibições são difíceis de aplicar, exigindo uma extensa polícia invasões
- cartas pessoais, diários, conversas
- nos EUA, diversas disposições
- o anonimato é muitas vezes necessário
10.3.8. Restrições no anonimato
- "identidade de custódia" é o que Eric Hughes chama
- linits em quedas de email, em contas anônimas, e, talvez o em última análise,--em compras de qualquer e todos os bens
10.3.9. "São quadros de avisos e provedores de Internet "common carriers" ou não?"

- Não está claro. BBS operadores são claramente realizada mais responsável para o conteúdo que a empresa de telefonia, por exemplo.

10.3.10. Muita esperteza está passando por lei

- Muitos esquemas de ignorar as leis de impostos, regulamentos, etc., são, como os Britânicos gostam de dizer, "muito bonito pela metade." Por exemplo, afirma que o dólar é definido como 1/35ª de uma onça de o ouro e que o moderno dólar é apenas 1/10 do presente. Ou que Ohio falha ao inserir corretamente a União, e, portanto, todos os leis aprovadas posteriormente são inválidos. O mesmo poderia ser dito de esquemas de implantar o dinheiro digital ser, alegando que o comum as leis não se aplicam. Bem, aqueles que tentam tais regimes de frequência descubra o contrário, às vezes na prisão. Pisar com cuidado.

10.3.11. "É legal para defender a derrubada de governos ou a a quebra de leis?"

- Embora muitos Cypherpunks não são radicais, muitos outros de nós somos, e nós, muitas vezes, defendem "o colapso dos governos" e outras coisas tais como esquemas de lavagem de dinheiro, evasão de divisas, novos métodos de espionagem, informação de mercados, dados paraísos, etc. Este rasises preocupações evidentes sobre a legalidade.

- Primeiro, tenho que falar, principalmente dos EUA questões...as leis da Rússia ou Japão ou o que pode ser completamente diferente. Desculpe para os EUA centrada no foco deste FAQ, mas que do jeito que está. O Líquido começou aqui, e ainda é predominantemente aqui, e as leis dos estados unidos estão sendo propagada em todo o mundo como parte da Nova Ordem Mundial e o colapso da outra superpotência.

- É legal para defender a substituição de um governo? No os estados unidos, é o básico do processo político (embora os cínicos pode-se argumentar que ambas as partes representam o mesmo que regem a filosofia). Defendendo a *derrube violento* dos EUA o governo aparentemente é ilegal, apesar de que eu não cite em isso.

+ É legal para defender a atos ilícitos em geral? Certamente muito da liberdade de expressão é precisamente este: discutindo a droga usar, por boicotes, etc.

+ FEP gopher site tem isso em um "defensor da Lei, Brandenburg v. Ohio. ":

- "Em 1969 caso de Brandemburgo v. Ohio, o Supremo Tribunal derrubou a condenação de uma Ku Klux Klan membro sob um criminoso sindicalismo lei e estabelecido um novo padrão: o Discurso não pode ser suprimido ou punidos, a menos que ele se destina a produzir iminente sem lei de ação", e é " provável para produzir tais

ação". Caso contrário, a Primeira Emenda protege mesmo
o discurso que defende a violência. O teste é de Brandemburgo
a lei hoje. "

10.4. Pode Crypto ser Banido?
10.4.1. "Por que não o governo simplesmente _ban tais métodos de encriptação?"
+ Esse sempre foi o Problema Número Um!
- criado por Stiegler, Drexler, Salin:, e vários outros
(e, na verdade, levantadas por alguns como uma objeção à minha mesmo
ao abordar estas questões, a saber, que a ação, em seguida, pode ser
levado para a cabeça fora do mundo que eu descrever)
+ Tipos de Proibições sobre Criptografia e Sigilo
- Proibição de Utilização Privada de Criptografia
- Proibição de Armazenar e Encaminhar Nós
- Proibição e Tokens de Autenticação ZKIPS
- Requisito para a divulgação pública de todas as transações
+ Notícias recentes (3-6-92, mesmo dia em que Michaelangelo e
Cortador de grama Homem) que o governo está propondo uma sobretaxa
em empresas de telecomunicações e serviços de longa distância para pagar novas
equipamentos necessários para a toque de celulares!
- S. 266 e facturas relacionadas com a
- esta foi a argumentar em termos de parar os traficantes de drogas e
outros criminosos
- mas, como o governo pretende lidar com os
várias formas fo usuário final de criptografia ou "confusão"
(a confusão que vai vir de compressão,
packetizing, simples de criptografia de arquivo, etc.)
+ Tipos de Argumentos Contra Tais Proibições
- Os "Direitos Constitucionais" Argumentos
+ "É Tarde Demais" Argumentos
- PCs já estão amplamente espalhados, a execução de dezenas de
a compressão e encriptação de programas...é muito
final de insistir "em claro" transmissões, qualquer que seja
pode ser (é código de programa distinguível de
mensagens criptografadas? Não.)
criptografado por fax, modem geralmente (embora com algumas
restrições)
- as LANs sem fios, pacotes, rádio, IV, do texto comprimido e
imagens, etc....tudo vai derrotar qualquer esforços curtos de
a polícia de intervenção do estado (que ainda pode acontecer)
+ A "Briga Dentro da NSA" Argumentos
- COMSEC vs. PROD
+ Afetará os direitos de privacidade das empresas

- e há muita evidência de que as empresas estão em
fato a ser espiado, por governos estrangeiros, pelos
NSA, etc.
+ Eles Vão Tentar Proibir Tais Técnicas de Criptografia
+ Picadas (talvez usando vírus e bombas lógicas)
- ou "de bário", para rastrear o código
+ De responsabilidade Legal para empresas que permitem que os funcionários usem
tais métodos
- talvez, até mesmo, no seu próprio tempo, através da suposição de que
os funcionários que usam software ilegal métodos em suas próprias
tempo são, talvez, correios ou agentes para a sua
corporações (um tênue ponto)
10.4.2. A longo prazo, a impossibilidade de proibição de criptografia
- stego
- transmissão direta para a sobrecarga de satélites
- samizdat
- compressão, algoritmos ....todos feitos de texto sem formatação de disco rígido para
encontrar
10.4.3. A proibição de criptografia é comparável à
+ a proibição de máscaras de ski, porque os criminosos podem esconder a sua identidade
- Nota: sim, há leis sobre "indo para o mascarado para o
propósito de ser "mascarados"," ou algo do tipo
+ insistindo que todo discurso estar em línguas compreensíveis por
os bisbilhoteiros
- (Não quero dizer "línguas oficiais" para lidar com o
Federais, ou o que os empregadores podem razoavelmente insistir)
- proibição de cortinas, ou pelo menos a exigência de que "Clipper
cortinas" ser comprados (de cortinas transparentes, no
comprimentos de onda de governos do mundo pode usar)
- posição de caução, por via eletrônica pulseiras como criminosos
desgaste
- restrições sobre livros que, possivelmente, ajudar os criminosos
- proibição de armadura (proposto em algumas comunidades)
- proibição de detectores de radar
- (Note que estas proibições se tornar mais "razoável" quando o
itens como armaduras e radar detectos são alcançados, em
menos para muitas pessoas. Não para mim, claro.)
10.4.4. Por isso, não os Governos Parar Esses Sistemas?
- Citando a segurança nacional, a proteção da propriedade privada,
decência e senso comum, etc.
+ De Medidas Legais
- Proibição de propriedade e de operação do "anônimo" sistemas de
+ Restrições sobre algoritmos criptográficos

- RSA patente pode ser um começo
+ RICO, ações civis, lavagem de dinheiro, leis
- FINCEN, Crimes Financeiros Centro de Informações
- IRS, a Justiça, a NSA, FBI, DIÂMETRO da CIA
- tenta forçar outros países a cumprir com os EUA.
leis bancárias

10.4.5. Cenário de uma proibição de criptografia

- "Paranóia é de criptografia do risco profissional." [Eric Hughes, 1994-05-14]
+ Há muitos cenários. Aqui está um gráfico de uma de Areia Sandfort:
- "Lembre-se de que as instruções para cozinhar um sapo vivo. O o governo não pretende parar até que eles tenham efetivamente eliminada a sua privacidade.

PASSO 1: Clipper torna-se de facto de criptografia standard.

PASSO 2: Quando Cypherpunks e outros "criminosos" abster-se de Clipper em favor de confiança forte de criptografia, o governo é "forçado" a proibição não caucionada sistemas de criptografia. (Tenho que pegar os pedófilos, traficantes de drogas e terroristas, afinal).

PASSO 3: Quando Cypherpunks e outros criminosos superencryption com Clipper ou falsificar Folhas, a governo vai regretably ser forçado a envolver-se em aleatório mensagem de monitoração para detectar estes ilegal técnicas.

Cada uma dessas etapas serão tomadas, porque nós não aceitar passivamente as coisas tais como irrestrito escutas e precauções razoáveis como telefonia digital. Ele será retratado como nossa culpa. Conte com isso." [Sandy Sandfort, 6-14-94]

10.4.6. Pode o fluxo de bits de ser interrompido? É o gênio realmente fora de a garrafa?

- Nota-se que Carl Ellison tem sustentado que o gênio era nunca _in_ a garrafa, pelo menos não nos estados unidos não a guerra situações (uso de criptografia, especialmente em de comunicação, em tempo de guerra, obviamente, levanta as sobrancelhas)

10.5. Questões jurídicas com PGP

7.12.1. "O que é o RSA Data Security Inc.'s de posição no PGP?"
I. Eles foram fortemente contrário de versões anteriores
II. objecções
- infringe o PKP patentes (supostas infrações, não
testado em tribunal, embora)
- quebra o rígido controle visto anteriormente
- traz a atenção indesejada a chave pública abordagens (eu
acho que o PGP também ajudou a RSA e RSADSI)
- sangue ruim entre Zimmermann e Bidzos
III. objecções
- infringe o PKP patentes (supostas infrações, não
testado em tribunal, embora)
- quebra o rígido controle visto anteriormente
- traz a atenção indesejada a chave pública abordagens (eu
acho que o PGP também ajudou a RSA e RSADSI)
- sangue ruim entre Zimmermann e Bidzos
IV. Falar de processos, ações, etc.
V. 2.6 MIT hospedagem, pode ter diminuído a tensão;
puramente especulativas
7.12.2. "PGP é legal ou ilegal"?
7.12.3. "Ainda existe um conflito entre RSADSI e PRZ?"
- Aparentemente não. O MIT 2.6 negociações parecem ter
enterrado todos esses rancor. Pelo menos oficialmente. Ouço que há
ainda animosidade, mas ele não está mais na superfície. (E
RSADSI agora está voltado para os processos judiciais e a patente se ajustar.)

10.6. Questões jurídicas com Remetentes
8.9.1. Qual é o estatuto jurídico de remetentes?
- Não há nenhuma lei contra isso neste momento.
- Nenhuma lei dizendo que as pessoas tem que colocar endereços de retorno na
mensagens, no telefone (chamadas de telefones públicos ainda são legais), etc.
- E as leis pertinentes de não ter de produzir identidade
(o "panfleto" de caso, onde folheto distribuidores não têm
para produzir ID) parece aplicar-se a esta forma de
comunicação.
+ No entanto, os remetentes podem vir sob o fogo:
+ Sysops, MIT caso
- potencialmente graves para os remetentes se o caso é
decidiu, de tal forma que o sysop da criação de um grupo que
foi propício para penais pirataria foi, propriamente, um
crime...que poderiam fazer com que todos os envolvidos no remetentes
culposa
8.9.2. "Pode reenvio de e-mails logs ser intimada?"

- Conte com isso acontecendo, talvez muito em breve. O FBI foi
subpoenaing e-mail arquivos para um Netcom cliente (Lewis De
Payne), provavelmente porque eles acham que o endereço de e-mail irá levar
- los para o local de super-hacker Kevin Mitnick. Tinha o
partes usadas remetentes, eu estou bastante certo de que estaríamos vendo
semelhante intimações para o reenvio de e-mails logs.
- Não há isenção para remetentes que eu conheço!
+ As soluções são óbvias, porém:
- usar muitos remetentes, para fazer subpoenaing de volta através do
a cadeia de muito trabalhoso, muito caro, e propensos a falhar
(mesmo se uma das partes não cooperar, ou está fora do
a competência do tribunal, etc.)
- ventos, multi-jurisdicionais remetentes (selecionada pelo
usuário)
- não reenvio de e-mails logs mantidos...destruí-los (não há nenhuma lei atualmente
diz que ninguém tem para manter registros de email! Isso pode
alteração....)
- "forward secrecy"," a la Diffie-Hellman forward secrecy
8.9.3. Como remetentes ser perseguidos, atacados, e desafiou?
8.9.4. "Pode pressão de ser colocado sobre o reenvio de e-mails operadores para revelar
tráfego
logs e, assim, permitir que o rastreamento de mensagens?"
+ Humano operado sistemas que tenham registos, com certeza. Este é
por que nós queremos que várias coisas em remetentes:
* não logs de mensagens
* muitos remetentes
* várias jurisdições legais, por exemplo, ventos remetentes
(quanto mais, melhor)
* implementações de hardware que executa instruções
perfeitamente (Chaum digital mix)
8.9.5. Chamadas para limites no anonimato
+ De crianças e a net vai fazer com que muitas chamada limites para
redes, no anonimato, etc.
- "Mas há um lado escuro para este emocionante fenômeno, um
que muito raramente é compreendida por usuários inexperientes.
Porque eles
oferecem acesso instantâneo aos outros, e considerável
o anonimato para
os participantes, os serviços de tornar possível que as pessoas -
especialmente com conhecimentos de informática kids - para encontrar-se em
desagradável, doenças sexualmente explícito situações sociais.... E
Eu gradualmente
vir a adoptar o modo de exibição, o que será motivo de controvérsia entre

muitos online
os usuários, que o uso de apelidos e outras formas de
o anonimato
devem ser eliminadas ou severamente reprimido para forçar as pessoas
online em
pelo menos tanto a prestação de contas por suas palavras e
ações como
existe no real, encontros sociais." [Walter S. Mossberg,
O Wall Street Journal, 6/30/94, fornecido por Brad Dolan]
Eli Brandt veio com uma boa resposta para isso: "O
som-mordida resposta para isso: você quer que o seu filho
nome, endereço e número de telefone disponível para todos
aqueles que espreita pedófilos em todo o mundo? Responsável pais
incentivar os filhos a usar remetentes."
- Supremo Tribunal disse que a identidade do folheto distribuidores
não precisa ser divulgada, e pseudônimos, em geral, tem uma longa
e nobre tradição
- BBS operadores têm proteções da Primeira Emenda (e.g..
requisitos de registo seriam atiradas para fora, exatamente como
se o registro dos jornais eram para ser tentada)
8.9.6. Remetentes e Escolha de Jurisdições
- O alvo de um remailed mensagem, e o assunto
material, pode muito bem influenciar o conjunto de remetentes usado,
especialmente para o muito importante "última reenvio de e-mails" (Note-se: ele
nunca deve ser necessário dizer remetentes se eles são
primeiro, o último ou os outros, mas o último reenvio de e-mails pode, na verdade,
ser capaz de dizer que ele é a última...se a mensagem estiver no
texto não criptografado para o destinatário, com adicional de reenvio de e-mails
comandos incorporados, por exemplo).
- Uma mensagem de pornografia envolvendo crianças podem ter um reenvio de e-mails
site localizado em um estado como a Dinamarca, onde a pornografia infantil leis
são menos restritivas. E uma mensagem crítica do Islã pode
não ser melhor enviadas através de uma final de reenvio de e-mails, em Teerã. Eric
Hughes tem apelidado este "arbitragem regulatória" e
várias extensões já é prática comum.
- Claro, o remetente pega o reenvio de e-mails em cadeia, de forma que estes
o senso comum noções podem não ser seguido. Nada é
perfeito, e os costumes evoluem. Eu posso imaginar esquemas de
desenvolvimento para a escolha de clientes, em um reenvio de e-mails pode não
aceitar como cliente determinadas abusadores, com base no digital
pseudônimos < peludo).
8.9.7. Possíveis medidas legais para limitar o uso de remetentes e
anônimo sistemas

- mantenha o reenvio de e-mails responsável por conteúdo, i.é., não comum estado de portador
- inserir disposições em vários "anti-pirataria" leis para criminalizar anônimo posts

8.9.8. Criptografia e remetentes podem ser usados para proteger os grupos de "profundo bolsos" ações judiciais
- produtos (esp. de software) pode ser vendido "como é", ou com contratos apoiados por serviços de garantia (código mantidos em um garantia do repositório, ou dinheiro guardado lá para trás até committments)
+ jurisdições, legais e fiscais, não pode fazer "chegar costas", que expor os grupos mais do que eles concordaram
- como é frequentemente o caso com as corporações no real mundo, que são tributados e multa para diversos fins (amianto, etc.)
- (Para aqueles que pânico ao pensar isso, o remédio para o cuidado será organizar contratos com o direito entidades...provavelmente pagando mais por menos produto.)

8.9.9. Poderia remetentes anônimos ser usado para prender as pessoas, ou para reunir informações para investigações?
- Primeiro, há tão poucas atual remetentes que este é improvável. Julf parece um não-narc tipo, e ele está localizado na A finlândia. Os Cypherpunks remetentes são em sua maioria executados por pessoas como nós, por agora.
- No entanto, tais picadas e set-ups têm sido utilizados no passado por narcóticos e "vermelho esquadrões." Esperar o pior do Sr. Policial. Agora que o mal os hackers são identificados como riscos, esperar que se move nesta direção. "Cryps" são, obviamente, "crack" negociantes.
- Mas o uso de criptografia, que CP remetentes de suporte (Julf do não), faz com que este, essencialmente, discutível.

10.7. Questões jurídicas com Caucionada Criptografia e Clipper

9.17.1. Como John Gilmore colocá-lo em um convidado editorial no "San Francisco Examiner," "...a gente quer que o público veja uma grave o debate sobre por que a Constituição deve ser queimado em ordem para salvar o país." [J. G., 1994-06-26, citado por S. Sandfort]

9.17.2. "Eu não vejo como Clipper confere ao governo poderes ou recursos que ela já não tem. Comentários?"

9.17.3. É Clipper realmente voluntário?

9.17.4. Se o Clipper é voluntário, que vai usá-lo?

9.17.5. Restrições de Uso Civil de Criptografia

9.17.6. "Tem de criptografia sido restrito nos EUA?"
9.17.7. "Que legal que medidas estão sendo tomadas?"
- Zimmermann
- ITAR
9.17.8. relata que o Departamento de Justiça tem um cumprimento
execução papel na ESTRATÉGIA europeia para o emprego [ouvida por alguém de Dorothy Denning, 1994-07], provavelmente envolvendo a verificação de que a lei as agências de aplicação da...
9.17.9. Estado
+ "Será que o governo vai agências Clipper?"
- Ah, a constrangedora pergunta. Eles afirmam que eles vão, mas existem também relatos de que sensíveis agências não usá-lo, que o Clipper é inseguro demais para eles (a chave de comprimento, de compromisso de garantia de dados, etc.). Também pode ser diferentes procedimentos (todas as agências são iguais, mas alguns são mais iguais do que outros).
- Clipper está classificado para a construção de usar, para esse regras muitas agências e muitos usos. Uma interessante dupla standard.
+ "É a Administração de backup fora do Clipper?"
+ indústria oposição surpreendeu
- grupos de no verão passado, o Citicorp, etc.
- opinião pública
- editorial comentários
- então eles podem estar preparando alternativa.
- e Gilmore FOIA, Blaze ataque, o Denning nonreview, o segredo das algortithm
+ não vai funcionar
- espiões não usá-lo, criança "the pornographers" provavelmente não usá-lo (se existem alternativas, que podem ser toda a ponto)
- os terroristas não usá-lo
- É Clipper em apuros?
9.17.10. "Vai Clipper ser voluntário?"
- Muitos adeptos do Clipper ter citado a natureza voluntária de Clipper--como expresso em algumas declarações de política--e tenho usado isso para contrariar a crítica.
+ No entanto, mesmo se realmente voluntária, algumas questões
+ inadequada papel do governo para tentar criar uma comercial padrão
- embora o NIST papel pode ser usado para combater este ponto, em parte,
o governo pode e faz com que seja difícil para os concorrentes

- controles de exportação (declarações oficiais sobre este existir)
+ Cita voluntário de status:
- declaração original diz que vai ser voluntário
- (necessário obter algumas declarações aqui)
+ Cites para eventual obrigatório de status:
- "Sem essa iniciativa, o governo irá, eventualmente,
tornar-se impotente para defender a nação." [Louis Freeh,
diretor do FBI, várias fontes]
- Steven Walker Confiáveis Sistemas de Informação é um dos
muitos que pensam assim: "com Base em sua análise, Walker adicionado,
"Estou convencido de que em cinco anos a partir de agora, eles vão dizer 'Este
não está funcionando', então nós vamos ter que mudar as regras." Em seguida,
ele previu, Clipper vai ser obrigatória para todos os
codificado de comunicações." [
+ Paralelos para outros programas voluntários
- impostos

10.8. Questões jurídicas com Dinheiro Digital
10.8.1. "O que é o estatuto jurídico do dinheiro digital?"
- Não foi testado, como um monte de protocolos de criptografia. Ele
pode ser de muitos anos, antes de estes sistemas são testados.
10.8.2. "Há um empate entre dinheiro digital e lavagem de dinheiro?"
- Não tem que ser, mas muitos de nós acreditam que o
uma ampla implantação do digital, untraceable dinheiro
possibilitar novas abordagens
- Daí a importância do dinheiro digital por criptografia anarquia e
idéias relacionados.
- (No caso de não ser óbvio, eu considero lavagem de dinheiro, uma
não-crime.)
10.8.3. "É verdade que o governo dos EUA pode limitar fundos
transferências de fora dos EUA?"
- Muitos problemas aqui. Certamente algumas leis existem. Certamente
as pessoas são processados todos os dias, por violação moeda
leis de exportação. Muitos caminhos existem.
- "LEGALIDADE - não Há e nunca vai ser uma lei restringindo
o envio de fundos fora dos Estados Unidos. Como faço para
sabia que? Simples assim. Como um país dependente internacional
comercial (bilhões de dólares ao ano e contando), o
Economia americana seria destruído." [David Johnson,
privacy@bem.sf.ac.nós, "Offshore Banking & Privacidade"
alt.privacidade, 1994-07-05]
10.8.4. "São "moedas alternativas" permitido nos EUA? E o que é
a implicação do dinheiro digital de várias formas?

- Tokens, cupões, certificados de presente são permitidos, mas de rosto
vários regulamentos. A batata frita de cassino eram tratados como
o dinheiro, mas agora são mais regulados (inter-casino de conversão
não é mais permitido).
- Qualquer tentativa de usar esses cupons como uma moeda alternativa
enfrentar os obstáculos. O cupom poderá ser permitido, mas fortemente
regulamentado (requisitos de apresentação de relatórios, etc.).
- Perry Metzger notas, obrigações ao portador, são ilegais no
Estados unidos (portador de bond, representado em dinheiro, em que nenhum nome foi
anexado ao título--o "portador" poderia vendê-lo por dinheiro
ou resgatá-lo...funcionou muito bem para o transporte de grandes quantidades
de dinheiro em forma compacta).
+ Nota: Duncan Frissell afirma que as obrigações ao portador são _not_
ilegal.
- "Sob a Equidade Fiscal e de Responsabilidade Fiscal, Lei de
1982 (TEFRA), quaisquer pagamentos de juros feito no *novo* problemas de
doméstica obrigações ao portador não são dedutíveis como um
comuns e necessárias despesas de negócios, de modo nenhum ter sido
emitido desde então. Ao mesmo tempo, os Federais
administrativamente parou de emitir títulos do tesouro em
formulário do portador. Antigas questões de governo e de dívida corporativa
no formulário do portador ainda existem e virão a existir e o comércio
30 ou mais anos depois de 1982. Além disso, os residentes dos EUA
pode comprar legalmente estrangeiros de títulos ao portador." [Duncan
Frissell, 1994-08-10]
- Alguém tem uma visão um pouco diferente: "O passado não
Portador de emissões de obrigações maduro, em 1997. Eu também acredito que a
cobrar juros, e para resgatar o vínculo, na data do vencimento, você
deve dar seu nome e fiscal-número de identificação para o pagamento de
agente. (Eu posso verificar com o departamento que lida aqui
se alguém estiver interessado no pertinentes OCC normas que
aplicar)" [prig0011@gold.tc.umn.edu, 1994-08-10]
- Eu citar este terríveis detalhes para dar aos leitores uma idéia sobre
quanto a confusão que existe sobre estes assuntos. O
conselho habitual é "buscar a competente conselho", mas na verdade
a maioria dos advogados não tem idéias claras sobre o melhor
estratégias, e o run-of-the-moinho advisor pode enganar
um perigosamente. Pisar com cuidado.
- Isso tem implicações para o digital cash, é claro.
10.8.5. "Por que dinheiro digital e afins techologies tomar posse
no início mercados ilegais? Que é, será que a Turba ser um dos primeiros a
adotante?"
- untraceability necessário

- e a reputação são importantes para eles
- eles mostraram, no passado, que eles vão tentar de novo
abordagens, a la o dinheiro movimentos dos cartéis de drogas,
novos métodos para a segurança, etc.
10.8.6. "Caixa eletrônico...será que vai ter que cumprir com as leis, e
como?"
- As questões serão levantadas sobre o anonimato aspectos, o
utilidade para evadir impostos e requisitos de informação,
etc.
- um bagunçado problema, a certeza de ser debatido e legislado sobre para
muitos anos
+ dividir o dinheiro em vários pedaços...é essa "estruturação"? é
isso é legal?
- algumas regras indicam a estruturação de per se, não é
ilegal, apenas a evasão fiscal ou de moeda, controle de evasão
- o que, em seguida, de sistemas que _automatically_, como uma base de
recurso, dividir o dinheiro em vários pedaços e mover
eles?
10.8.7. Moeda, controles de vôo, capital regulamentos, boicotes,
ativo convulsões, etc.
- todos são pressões para encontrar maneiras alternativas de capital para o
o fluxo de
- todos para a falta de confiança, o que, paradoxalmente, para
os legisladores, faz com que a fuga de capitais tudo o mais provável
10.8.8. "Vai reguladores bancários permitir digital de dinheiro?"
- Não é tarefa fácil, isso é certo. O labirinto de regulamentos,
restrições de impostos, leis e decisões judiciais é assustador. Eric
Hughes passei muito tempo lendo sobre as leis em relação à
bancos, papel comercial, impostos, etc., e concluiu muito
o mesmo. Eu não estou dizendo que é impossível-de fato, eu acredito
que um dia vai acontecer, de alguma forma--, mas os obstáculos são
formidável.
+ Algumas questões:
+ Será que tal operação ser permitido ser centralizado ou com base
nos EUA?
- Quais estados? Que leis? Banco vs. Poupança e Empréstimo vs.
União de crédito vs. Corretor de Títulos vs. algo mais?
+ Os clientes poderão acessar tais entidades ventos,
fora dos EUA?
- forte de criptografia torna a comunicação possível, mas pode
ser difícil, e não uma parte do tecido empresarial, etc.
(e, portanto, não é tão útil-se alguém tem para enviar PGP-
criptografados instruções para um banqueiro, e não pode usar

a limpeza de infra-estruturas....)
+ A cobrança de impostos, lavagem de dinheiro, leis, leis de divulgação,
"conheça o seu cliente" leis....todos são áreas onde um
digital "banco" pode ser desligado imediatamente. Qualquer banco e não
preencher os formulários (incluindo obrigatório
relatório de transações de determinadas quantidades e tipos de
e a Segurança Social/Contribuinte, Número de clientes)
enfrenta enormes multas, penalidades e sanções regulatórias.
- e a jogadores existentes no bancárias e de valores
o negócio não vai ficar de braços cruzados enquanto os recém-chegados enter
de mercado; procurarão forçar os recém-chegados para pular
através do mesmo aros que tinha (estudos indicam
grandes corporações, na verdade, _like_ burocracia, como
ajuda-los em relação às empresas de menor dimensão)
- Concluson: Digital, os bancos não ser "lançado" sem um
muito trabalho por advogados, contadores, peritos fiscais,
lobistas, etc. "Limonada digital bancos" (TM) será
não sobreviver por muito tempo. Crianças, não tentem isto em casa!
- (Muitas novas indústrias que estão familiarizados com software,
microcomputadores--tinha muito pouco regulamento, com razão. Mas
o efeito é que muitos de nós não estão preparados para entender
a enorme quantidade de burocracia que as empresas de outros
áreas, nomeadamente a banca, cara.)
10.8.9. Obstáculos legais para o dinheiro digital. Se os governos não querem
anônimo dinheiro, eles podem tornar as coisas difíceis.
+ Como Perry Metzger e Eric Hughes já disse muitas vezes,
regulamentos podem tornar a vida muito difícil. De conformidade com
leis é um grande custo de fazer negócios.
- ~"O custo de conformidade em um típico EUA banco é de 14% de
custos operacionais."~ [Eric Hughes, citando uma "Americano
Banqueiro" do artigo, 1994-08-30]
+ Labirinto de regulamentos é navegável por grandes
instituições, com equipes de advogados, contadores, fiscais
especialistas, etc., mas é, essencialmente, além do
capacidades de muito pequenas instituições, pelo menos no
EUA
- isso pode ou não pode ser, como computadores
proliferam. Um "banco-in-a-box" programa pode ajudar. Meu
a suspeita é de que um determinado tamanho de funcionários necessários
para lidar com o face-a-face reuniões e aro de salto.
+ "Nova Ordem Mundial"
- EUA pedindo outros países para "jogar bola" na bancário
o sigilo, a evasão fiscal, a extradição, a imigração, etc.

- este é fechar o ex-lacunas e escapar
escotilhas que se permitiu que as pessoas a escapar repressivas
tributação...as implicações para o digital de dinheiro que os bancos são
claro, mas preocupante.

10.9. Legalidade do Digital Bancos e Dinheiro Digital?
10.9.1. Em termos de leis bancárias, dinheiro, informação, dinheiro
capitais estatutos, e a confusão de leis conectado com
transações financeiras de todos os tipos, os Cypherpunks temas
e as idéias são basicamente _illegal_. Ilegal no sentido de que
qualquer pessoa que tentar configurar o seu próprio banco, ou moeda alternativa
sistema, ou como seria desligar rapidamente. Como um
informal, despercebido _experiment_, tais coisas são razoavelmente
seguro...até que não são percebidos.
10.9.2. A palavra-chave aqui é "lançamento", na minha opinião. O
"o lançamento de" o BankAmericard (agora VISTO) na década de 1960, não foi
feito de ânimo leve ou casualmente...é necessário exércitos de advogados,
contadores, e outros bureacrats para fazer o lançamento, tanto
legal e bem sucedida. A mera "idéia" de um cartão de crédito foi
não o suficiente...que foi, essencialmente, a parte mais fácil de tudo.
(Alguém contemplar o lançamento de um sistema de dinheiro digital
fariam bem em estudar BankAmericard como um exemplo...e
vários outros exemplos também.)
10.9.3. O mesmo será verdade para qualquer dinheiro digital ou similar sistema de
o que pretende operar mais ou menos abertamente, a interface
existentes com instituições financeiras, e que não é
explicitamente pretende ser um Cypherpunkish de metro
a atividade.

10.10. Exportação de Criptografia, ITAR, e Leis Similares
10.10.1. "Quais são as leis e regulamentos de exportação de criptografia,
e onde posso encontrar mais informações?"
- "A resposta curta é que o Departamento de Estado, o Office
de Controles de Defesa Comercial (DOS/DTC) e o Nacional
Administração de segurança (NSA) não permitir irrestrito
de exportação (como está sendo feito com WinCrypt) para qualquer
programa de criptografia que a ANS não pode quebrar com menos de
uma certa quantia (que eles são relutantes em revelar) de
esforço. Para o tempo de resposta, consulte
ftp://ftp.csn.net/cryptusa.txt.gz e/ou chamada DOS/DTC no
703-875-7041." [Michael Paul Johnson, sci.cripta, 1994-07-
08]
10.10.2. "É ilegal enviar encriptado coisas fora dos estados unidos?"

- Isso veio à tona várias vezes, com pessoas que eles já
ouviu isso.
- Em tempos de guerra, guerra real, o envio de mensagens criptografadas podem
de fato, ser suspeito, talvez até ilegais.
- Mas os EUA atualmente não possui tais leis, e muitos de nós
enviar muitos encriptado coisas fora dos EUA Para remetentes,
para amigos, etc.
Arquivos criptografados são muitas vezes difíceis de distinguir de
ordinária arquivos compactados (alta entropia), de modo que a lei
aplicação teria um tempo difícil.
- No entanto, outros países podem ter leis diferentes.
10.10.3. "Qual é a situação sobre a exportação de criptografia?"
+ Há muito debate sobre isso, com o caso do Phil
Zimmermann, possivelmente, ser um importante caso de teste, deve
encargos de ser arquivado.
- como de 1994-09, o Grande Júri em San Jose não disse
qualquer coisa (que foi cerca de 7 a 9 meses, desde que começou a
sobre esta questão)
- Dan Bernstein tem argumentado que a ITAR abrange quase todos os
aspectos de exportação de criptografia material, incluindo os códigos,
documentação, e até mesmo "conhecimento". (Controversa, é
pode ser uma violação da ITAR para conhecimento de criptografia pessoas
até mesmo para deixar o país com a intenção de desenvolver
criptografia de ferramentas no exterior.)
- As várias distribuições do PGP, que ocorreram através de
ftp anônimo fontes não implica que a ITAR não está sendo
imposta, ou não será no futuro.
10.10.4. O porquê e o Como de Criptografia Não é o Mesmo Armamento
- a arma de comparação, tem vantagens e desvantagens
- "o direito de manter e portar armas"
- mas, então, isso abre as portas para as restrições,
os regulamentos, as comparações de criptografia para armas nucleares, etc.
-
+ "Crypto não é capaz de matar pessoas de forma direta. Crypto
consiste
- inteiramente de informação (voz, se você tem) que não pode
ser
- interditada. Criptografia tem fins civis.
- -
- <Robert Krawitz <rlk@think.com>, 4-11-94, sci.cripta>
10.10.5. "O que é ITAR e o que ela cobre?"
+ ITAR, o Tráfico Internacional de Armas Regulamentos, é
a definição do conjunto de regras para a exportação de munições-e

criptografia é tratada como munições.
- os regulamentos para a interpretação de leis de exportação
+ NSA pode ter dúvidas de que a ITAR iria realizar-se no tribunal
- Alguns podem argumentar que isso contrariava a Constituição,
e daí iria falhar no tribunal. Novamente, não foram poucos
se qualquer sólido testes de ITAR no tribunal, e algumas indicações
que NSA advogados relutam em vê-lo testado, temendo
ele não iria passar na prova.
- dúvidas sobre a legalidade (Carl Nicolai viu papéis, uma vez que
confirmado em uma FOIA)
- Brooks instrução
- Cantwell Projeto De Lei
- não foi totalmente testado no tribunal
+ relatórios de NSA preocupações que ele não iria realizar-se em tribunal se
nunca desafiou
- Carl Nicolai, depois FOIA resultados, conversas com Phil
+ Ações legais que Cercam ITAR
- O ITAR leis podem ser usadas para combater hackers e
Cypherpunks...o resultado da Zimmermann acusação
será um sinal importante.
+ O que ITAR cobre
- "ITAR 121.8(f): `Software inclui, mas não está limitado a
o sistema de design funcional, fluxo de lógica, algoritmos,
programas aplicativos, sistemas operacionais e suporte
software para projeto, implementação, teste, operação,
diagnóstico e reparação." [citado por Dan Bernstein,
falar.política.crypto, 1994-07-14]
- piada Bidzos sobre o registro internacional de armas
revendedor
+ ITAR e de código (código pode ser publicado na Net?)
- "Por que não o ITAR importa?"
- Phil Karn está envolvido com isso, assim como vários outros
aqui
+ Dan Bernstein tem alguns fortemente realizada pontos de vista, com base em sua
longa história de luta contra a ITAR
- "Vamos supor que o algoritmo é capaz de
manter sigilo das informações, e que não é
restrito para a decifração, bancário, analógico lutando,
especial de cartões inteligentes, autenticação de usuário, dados
autenticação, compressão de dados, ou de proteção contra vírus.

"O algoritmo é, em seguida, em USML Categoria XIII(b)(1).

"É, portanto, um artigo de defesa. ITAR 120.6. "[Dan
Bernstein, publicação de código para o sci.cripta,
falar.política.crypto, 1994-08-22]
- "O envio de um artigo de defesa dos Estados Unidos em
de qualquer maneira (exceto o conhecimento em sua cabeça) é
exportação. ITAR 120.17(1).

"Para postar o algoritmo constitui exportação. Há
outras formas de exportação, mas não entrarei aqui.

"O algoritmo em si, sem qualquer fonte de código, é
de software." [Dan Bernstein, publicação de código para o sci.cripta,
falar.política.crypto, 1994-08-22]
- "O estatuto é a Lei de Controle de Exportação de Armas; o
os regulamentos são
International Traffic in Arms Regulations. Preciso
referências, ver
o meu `International Traffic in Arms Regulations: Um
Editor do Guia."" [Dan Bernstein, o código para postagem
sci.cripta, falar.política.crypto, 1994-08-22]
+ "Código de postagem é bom. Nós fazemos isso o tempo todo; temos
o direito de fazê-lo; ninguém parece estar tentando nos parar
de fazê-lo." [Bryan G. Olson, o código para postagem
sci.cripta, falar.política.crypto, 1994-08-20]
- Bernstein concorda que alguns bustos ter ocorrido, mas
adverte: "Milhares de pessoas distribuídas em criptografia
violação do ITAR; apenas duas, para meu conhecimento, foram
condenado. Por outro lado, o guv'mint é rapidamente
catching up com a realidade, e o Phil Zimmermann caso
pode ser o início de uma grave repressão." [Dan
Bernstein, publicação de código para o sci.cripta,
falar.política.crypto, 1994-08-22]
- A opinião comum de que a liberdade acadêmica significa um é de OK
provavelmente não é verdade.
+ Hal Finney ordenadamente resumiu o debate entre Bernstein
e Olsen:
- "1) Ninguém foi processado por postar código
sci.cripta. O Zimmermann caso, se nada nunca vem
dele, não era sobre o lançamento de código na Usenet, AFAIK.

"2) Não relevante governo tem publicamente
expressou sua opinião sobre se o código de postagem
sci.cripta seria legal. As conversas Dan

Bernstein postado tratadas com seus pedidos para permissão de
para exportar seu algoritmo, não para postar código no sci.cripta.

"3) não sei se alguém vai ser
processado por postar o código no sci.cripta, e nós não
sabe qual o resultado de tal acusação
ser". [Hal Finney, falar.política.crypto, 1994-008-30]

10.10.6. "Pode ITAR e outras leis de exportação de ser ignorada ou contornado por
fazer o desenvolvimento de ventos e, em seguida, _importing_ forte de criptografia
para os EUA?"

- A IBM está supostamente fazendo apenas isso: o desenvolvimento de uma forte criptografia
de produtos para OS/2 em seus laboratórios no exterior, assim contornando a
leis de exportação (que têm enfraquecido as chaves para algumas de suas
produtos de segurança de rede de 40 bits que são permitidos).

+ Alguns problemas:

- não pode enviar docs e o know-how para instalações offshore (alguns
óbvio problemas de aplicação, mas isso é como a lei
lê)

- não pode mesmo ser capaz de transferir pessoas de conhecimento para
instalações offshore, se o chefe intenção é, em seguida, ter
desenvolver produtos de criptografia ventos (fundo algumas
Questões constitucionais, penso eu...alguns tons de como
a U.R.S.S. justificava negar partida de vistos para
"precisava" de trabalhadores)

- Assim como em muitos casos invovling criptografia, não há
definição de casos legais que eu estou ciente.

10.11. A Arbitragem Regulamentar

10.11.1. Jurisdições com mais favorável leis verá requerentes
vai lá.

10.11.2. Semelhante a "fuga de capitais" e "pessoas com o seu voto
pés."

10.11.3. É o outro lado da "jurisdição de compras." em
procuradores compras em torno de uma competência que vai ser
mais prováveis para condenar. (Como com a Ação Amador BBS caso,
tentou, em Memphis, Tennessee, e não na Califórnia.)

10.12. Criptografia e Pornografia

10.12.1. Houve um monte de atenção da mídia dada a esta,
especialmente a pedofilia (a pedofilia não é a mesma coisa que
pornô, é claro, mas os dois são muitas vezes discutidas em artigos
sobre a rede). Como Rishab Ghosh colocá-lo: "eu acho que o
pedófilo possibilidades da Internet capturar o

a imaginação dos media-os seus desejos mais profundos, talvez."
[R. G., 1994-07-01]
10.12.2. O fato é que os dois são feitos um para o outro. O
untraceability dos remetentes, o unbreakability do forte
crypto se os arquivos forem interceptadas pela aplicação da lei, e
a capacidade de pagar de forma anônima, tudo isso significa o início de usuários de
comercial remetentes provavelmente vai ser essas pessoas.
10.12.3. Evitar embaraçar picadas! Manter o seu emprego no ensino fundamental
a escola! Re-eleito para o conselho da igreja!
10.12.4. pedofilia, bestialidade, etc. (modificadas imagens)
10.12.5. Ação amador BBS operador interessado em criptograa....um pouco
pouco tarde demais
10.12.6. Existem novas perspectivas para a entrega de mensagens como parte de
picadas ou aprisionamento de ataques, onde os bits descriptografar em
provas incriminatórias quando a chave é usada. (XOR de
curso)
10.12.7. Assim como a aplicação da lei as pessoas estão reclamando, forte de criptografia
e remetentes vai fazer novos tipos de pornografia redes. O nexus
ou de origem não será conhecido e os clientes não serão
conhecido.
- (Uma estratégia interessante: reclamação de clientes desconhecido, e
as leis locais. Fazer a "captação" do cliente
responsabilidade (talvez através de agentes).

10.13. Usenet, a Calúnia, as Leis Locais, Jurisdições, etc.
10.13.1. (De importância secundária para criptografia temas, mas importante para
questões de vir a legislação sobre o Líquido, as tentativas de
"recuperar o controle", etc. E um pouco de um amontoado de idéias, também.)
10.13.2. Muitos países, muitas leis. Muito do tráfego Usenet, presumivelmente,
viola diversas leis do irã, a China, a França, o Zaire, e o
Dos EUA, para citar f ew locais que têm leis sobre o pensamento
pode ser expressa.
10.13.3. Será que este resultado de sempre nas tentativas de encerrar o Usenet, ou em
menos os feeds em vários países?
10.13.4. Sobre o tema da Usenet, possivelmente, ser desligado do reino UNIDO.
(um recente rumor, e infundadas), este comentário: "o Que você
tem que entender é que a USENET tipo de redes e toda a
estrutura da lei no publshing são fundamentalmente
incompatiable. Com USENT qualquer pessoa pode distribuir untracably
pornográfico, calunioso, blasfemo, direitos autorais ou até mesmo
oficialmente informações secretas. Agora, o que você acha HMG
e, para que o assunto, o overwhealming maioria dos oridnary
as pessoas, neste país, acho que é o mais importante. USENET ou

essas leis?" [Malcolm McMahon, malcolm@geog.leeds.ac.uk,
comp.org.fep.falar, 1994--08-26]
10.13.5. Será bem-sucedido? Não completamente, como e-mail, gopher, Web,
etc., ainda dispõe de acesso. Mas os efeitos podem chegar a mais
usuários casuais, e, certamente, afetar a estrutura como sabemos
é hoje.
10.13.6. Vai criptografia de ajuda? Não diretamente-ver acima.

10.14. As Normas De Emergência
10.14.1. Pedidos De Emergência
- diversas NSDDs e similares
- "Sete Dias em Maio," cenário
10.14.2. Legal, sigilo ordens
- George Davida, U. oif Wisconsin, recebeu uma carta em 1978
ameaça de us $10 MIL por dia de multa
- Carl Nicolai, PhasorPhone
- A ANS confirmou que partes do EES são patenteados,
em segredo, e que as patentes serão públicos e
em seguida, usado para deixar os concorrentes devem tornar o algoritmo
conhecido.
10.14.3. Pode o FCC-Requisitos de tipo para "limpar" a radiodifusão
(ou chaves fornecido para Feds) ser uma base para uma legislação semelhante
de redes privadas e privadas uso de criptografia?
- isso parece ser impraticável, dado o crescimento da
telefones celulares, redes locais sem fios, etc....não posso muito bem
mandato de que as empresas de difusão interna
comunicações em claro!
- compressão, comutação de pacotes, e todos os outros tipos de
"distorções" dos dados, requer transmissões
legível por agências do governo exigiria fornecendo o
governo com mapas (de onde os pacotes estão indo), com
específicos algoritmos de descompressão, etc....muito prático

10.15. Patentes e direitos de autor
10.15.1. A web de patentes
- o que acontece é que todo mundo está fazendo nada de substantivo
gasta muito do seu tempo e dinheiro em busca de patentes
- patentes são essenciais negociação fichas em lidar com
outros
- por exemplo, DSS, Schnorr, RSADSI, etc.
- por exemplo, Stefan Marcas está em busca de patentes
- Cylink processando...
10.15.2. Papel da RSA, Patentes, etc.

+ Bidzos: "Se você ganhar dinheiro com RSA, vamos ganhar dinheiro" é o
regra simples
- mas é claro que ele vai além disso, como o mesmo "livre" usa
pode ter que pagar
- Sobreposição de patentes a ser utilizado (aparentemente) a medida em que o
a vida de carteira
+ 4/28/97 O primeiro de vários P-K e RSA patentes expira
+ EUA Número De Patente: 4200770
- Título: Criptografia Aparelho e Método
- Inventores: Hellman, Diffie, Merkle
- Cessionário: Universidade De Stanford
- Arquivado Em: Setembro 6, 1977
- É Concedido: 29 De Abril De 1980
- [Expira: 28 De Abril De 1997]
+ lembre-se de que qualquer uma destas várias patentes detidas por
Chave pública de Parceiros (Stanford e M. I. T., com RSA Data
Segurança o chefe dispensador de licenças) pode bloquear um
esforço para ignorar os outros
- embora isso possa obter lutou em tribunal
+ 8/18/97 O segundo de vários P-K e RSA patentes expira
+ U.S. Patent Number: 4218582
- Título: Chave Pública de Criptografia Aparelho e Método
- Inventores: Hellman, Merkle
- Cessionário: O Conselho de Curadores da Leland Stanford
Universidade Júnior
- Arquivado Em: Outubro 6, 1977
- É Concedido: 19 De Agosto De 1980
- [Expira: 18 De Agosto, 1997]
- isso pode ser contestado, pois descrevem algortihms em
termos gerais e usou a mochila algoritmo como o chefe
exemplo
+ 9/19/00 O principal RSA patente expira
+ U.S. Patent Number: 4405829
- Título: Criptografia Sistema de Comunicação e Método de
- Inventores: Rivest, Shamir, Adleman
- Cessionário: Instituto de Tecnologia de Massachusetts
- Arquivado Em: Dezembro 14, 1977
- É Concedido: 20 De Setembro De 1983
- [Expira: 19 De Setembro, 2000]

10.15.3. Os processos judiciais contra a RSA patentes

+ vários são os de fabricação de cerveja
- Cylink está processando (estranho rumores de que a NSA estava envolvido)
- Roger Schlafly

10.15.4. "O que sobre a ação movida pelo Cylink contra a RSA Data Security Inc.?"
- Muito curioso, considerando que ambos são parte da Chave Pública Parceiros, o consórcio de Stanford, MIT, Cylink, e RSA Data Security Inc. (RSADSI)
- o processo foi arquivado no verão de 1994
+ Um estranho rumor que ouvi, a partir de uma fonte respeitável, foi que a NSA havia pedido PKP para fazer algo (?) e que Cylink tinha acordado, mas RSADSI tinha recusado, ajudando a empurrar o a suit junto
- todos os links com as ameaças de morte contra Bidzos?
10.15.5. "O sistema de patentes ser usado para bloquear o governo usar da patentes para fins de nós não gosta?"
- Vem, sobretudo, no contexto de S. Micali da patente garantia de técnicas de
- "Não importa. O governo não pode ser ordenada a partir de usando uma patente. O governo federal, no final análise, pode usar qualquer patente que quiserem, sem a permissão, e o único recurso do titular da patente é a sue para royalties no Tribunal de Créditos." [Bill Larkins, falar.política.crypto, 1994-07-14]

10.16. Questões Práticas
10.16.1. "E se eu dizer que as autoridades Esqueci-me da Minha palavra-Passe?"
- (ou chave ou a frase de acesso...você ter uma idéia)
- Este surge várias vezes, mas a resposta continua obscuro
10.16.2. Civil vs. Penal
+ "Este é um civil mattep, e o pights de ppivaay um haq em cpiminal mattepq
- tendem a vaniqh em aivil litígio. O paptieq para um lawquit ódio
- tpemeldouq powepq para dopae o othep qide para peteal ildopmatiol peletalt
- para o aaqe, <@pad Templetol, 4-1-94, aomp,pgr,edd,tal
10.16.3. o direito é, essencialmente, aquilo que os tribunais dizem que é

10.17. A liberdade de expressão está Sob Ataque
10.17.1. A censura vem em muitas formas. O direito penal, ameaças de conceder ou contrato de remoção, todos estão limitando a fala. (Mais motivos para anônimo fala, é claro.)
10.17.2. Discussões de criptografia pode ser alvos de futuro repressão. Sedição leis, conspiração leis, RICO, etc. Como muito antes de falar sobre estes assuntos, ganha uma carta de advertência

a partir de sua universidade ou sua empresa? (É o "big stick"
de ultimate ação do governo que estimula esses universidade e
as políticas da empresa. A Apple medos de ser encerrado por ter
"envolvimento" com uma conspiração terrorista, da Universidade Emory, medos
está sendo processado por milhões de dólares para "conspirar" para
degradar wimmin de cor, etc.)

Quanto tempo antes de "rec.armas" não é mais levado em muitas
sites, pois eles temem ter suas universidades ou empresas
associadas ao debate de "armas de assalto" e "cop killer
balas"? Previsão: Muitas empresas e universidades, em
a pressão da Polícia, irá bloquear grupos em que criptografadas
os arquivos são lançados. Afinal, se um criptografa, deve-se ter
algo a esconder, e que poderia expor a universidade para
legal ação de algum grupo que se sentir prejudicada.
10.17.3. A liberdade de expressão está sob ataque em todo o país. O ato ilícito
o sistema está sendo usado para reprimir opiniões divergentes (e que
você acha que eu sou apenas um capitalista, apenas um livre marqueteiro, o
o uso de "SLAPP fatos"--"Estratégico de ações Judiciais Contra Públicas
Participação"--por empresas ou entidades de incorporação imobiliária para
ameaçar aqueles que se atrevem a falar publicamente contra a sua
projetos é um absurdo, um absurdo que os tribunais têm apenas
recentemente, começou a corrigir).

Estamos nos tornando uma nação de ovelhas, temendo o raid da meia-noite,
o bater na porta. Temos medo de que, se nos conte uma piada,
alguém vai brilho em nós e ameaçar processar-nos _and_ nossa
empresa! E por isso, as empresas estão adotando o "discurso" códigos e
outros, como bagagem de Orwell estado totalitário.
O politicamente correto está estendendo seus tentáculos em quase
cada aspecto da vida na América.

10.18. Sistemas de Acesso, e a Lei
10.18.1. Questões legais sobre o acesso aos sistemas de
+ Preocupações:
- acesso por menores de idade à material explícito sexualmente
+ acesso a partir de regiões onde o acesso "não deve ser
permitido"
- exportação de criptografia, por exemplo
- o Memphis acesso para a Califórnia BBS
+ Abordagem atual: tendo a promessa da acessor
- "Eu não vou exportar esta fora dos EUA ou Canadá."
- "Eu sou maior de idade para acesso a este material."

+ Futuros possíveis abordagens:
+ De retorno, para garantir acessor é da região afirmou
- é fácil o suficiente para ignorar com recortes e remetentes
+ "Credenciais"
- la a US Postal Service proposta de cartão de IDENTIFICAÇÃO (e outros)
+ criptograficamente credenciais autenticadas
- Chaum credenciais do sistema (certamente melhor do que muitos não-privacidade-preservar as credenciais de sistemas)

10.18.2. "O que é uma "transportadora comum" e como um serviço de tornar-se um?"

- (Este tópico tem a sua importância para criptografia e remetentes, vis uma vis se remetentes devem ser tratados como comuns operadoras.)
- Portadores comuns são que o telefone e a entrega do pacote serviços. Eles não são responsáveis pelo conteúdo de chamadas de telefone, para o conteúdo de pacotes (drogas, a pornografia, etc.), ou por atos ilegais conectado com seus serviços. Um dos negócios é comum em portadores de não examinar o interior dos pacotes. Common carriers essencialmente, concorda em tomar todo o tráfego que paga a taxa e não discriminar com base no conteúdo. Assim, um serviço de telefone não vai perguntar o que o sujeito de uma chamada está a ser, ou ouvir em, para decidir, para fazer a conexão.
- Alguns dizem que, para ser um meio de transporte comum exige a disposição para trabalhar com a aplicação da lei. Isto é, a Federal Express é não somos responsáveis pelo conteúdo dos pacotes, mas eles têm que cooperar em razoável formas com a aplicação da lei para abrir ou faixa de pacotes suspeitos. Alguém tem uma cite para isso? É verdade?
- Transportadora comum de status também é citado para as livrarias, que não são presume-se que a leitura de cada um e de cada uma das os livros que vender...então se alguém sopra sua mão em um uma experiência, a livraria não é responsável. (O autor/editor pode ser, mas isso é uma<unk>nt problema.)
- Como alguém se torna um meio de transporte comum? Não está claro. De um ponto de vista é que um serviço deve "comportar-se como" uma empresa de transporte comum e então espero e oro para que um tribunal de vê-lo dessa forma.
+ De computador comuns de serviços de operadoras? Um tema de grande interesse.
- "De acordo com uma discussão que eu tive com Dave Lawrence (postmaster em UUNET, bem como moderador de notícias.de administração.newgroups), UUNET é registrado com a FCC

como um "Enhanced Service Provider", o que, de acordo com
Dave, quantidades similares de proteção, como "meio de transporte Comum."
("Common Carrier" parece não ser adequado ainda, desde que
O congresso é tão atrás a tecnologia curva)." [L. Todd Masco,
1994-08-11]
- Como para redes de reenvio de e-mails que estão sendo tratados como portadores comuns,
totalmente claro neste momento. Certamente o fato de que
os pacotes são totalmente criptografadas e unreadabel vai para a parte de
a questão sobre concordando em não para a tela.
+ Mais sobre a empresa de transporte comum debate:
- "Ah, a eterna Transportadora Comum debate. A resposta é
o mesmo últimos tempos. "Transportadora comum" status
tem pouco a ver com a isenção de responsabilidade. Ele tem
mais a ver com ser incapaz de rejeitar passageiros, mercadorias,
ou telefonemas.....A abundância de não-common carrier entidades
são imunes a acusação de idéias que eles
unkowingly comunicar -- livrarias, por exemplo, (a menos que
eles são *conscientemente* porno livrarias de errado
jurisdição)....Compuserve foi realizada não se responsabiliza por uma
(alegada) difamação por um de seus administradores. Não por causa do
empresa de transporte comum, mas porque eles não tinham conhecimento ou
de controlo....Remetentes não têm conhecimento ou controle, portanto,
sem intencionalidade (culpado de conhecimento), portanto, não passivo como um
questão de direito---não um júri questão BTW." [Duncan
Frissell, 1994-08-11]

10.19. Credenciais
10.19.1. "São as credenciais necessárias? Vai métodos digitais será usada?"
10.19.2. Eu vou dar um radical vista. Pergunte a si mesmo por que as credenciais são
ever necessário. Talvez para a condução de um carro, e o como, mas em
nesses casos, o anonimato não é necessária, como a pessoa é na
de carro, etc.

Credenciais para a idade de beber? Por quê? Deixe os pais impor
este, como diz o argumento sobre a observação de sexo e violência na
t.v. (Se se aceita a lógica da exigência de barras para impor
o comportamento das crianças, então é uma ladeira escorregadia para
necessitando de televisão que os tomadores de seleção de cartões inteligentes (smartcards)
os espectadores, ou de exigir uma licença para acessar a Internet,
etc.)

Em quase nenhum dos casos, eu vejo a necessidade de realizar "trabalhos" com
a mim. Talvez uma carteira de motorista, como eu disse. Em outras áreas,

por quê?
10.19.3. Então, Cypherpunks, provavelmente, não deve gastar muito tempo
se preocupar com a permissão de deslizamentos e "salão de passes" será
tratados. Pouca necessidade para eles.
10.19.4. "O que sobre credenciais para o trabalho específico de desempenho, ou para
o estabelecimento com base no tempo contratos?"
- Credenciais de provar que tenha concluído certas classes,
ou chegaram a determinados níveis de habilidade, etc.?
- Em transações que "desempenho futuro" é necessário, como no
um contrato para uma casa construída, ou para fazer alguma semelhantes
trabalho, então é claro que a ideia de linha ou imediata
limpeza é falso...como pagamento de um estranho uma soma de dinheiro
na sua promessa de que ele estará de volta no dia seguinte para iniciar
a construção de uma casa para você.

Partes de longo prazo, não-localmente-casos resolvidos, podem
contrato com um agente de custódia, como descrito acima. Este
é como o "privada produzido lei" nós já discutimos isso
muitas vezes. A essência: acordos voluntários.

Talvez provas de identidade será necessário ou solicitado,
talvez não. Mas estes não são a essência do negócio.

10.20. De Custódia De Agentes
10.20.1. (a principal discussão deste está sob Criptografia Anarquia)
10.20.2. De custódia de Agentes como uma forma de lidar com contrato renegging
- Na linha de compensação tem o perigo implícito em todos os
negociações que Alice vai entregar o dinheiro, Bob irá verificar
que autorizou, em hisaccount (nos antigos termos, Bob
teria de esperar palavra que sua conta bancária Suíça acaba de ser
creditado) e, em seguida, Bob vai conseguir concluir o seu fim de
a barganha. Se a transação é verdadeiramente anônimo, sobre
linhas de computador, então é claro que Bob simplesmente trava-se o seu modem
e a ligação é interrompida. Esta situação é tão antiga como
tempo, e sempre envolveu outros protocolos em que a confiança,
a repetição de negócios, etc., são factores. Ou conivência de agentes.
- Muito antes de a "custódia" de Clipper, verdadeira garantia foi
planejado. De caução como garantia de agentes. Ou colagem de agentes.
- Alice e Bob querem a realização de uma transação. Nem confia
os outros;
de fato, eles são desconhecidos uns dos outros. Nas etapas "de Ester
Garantia De Serviço." Ela é _also utraceable_, mas tem
estabeleceu uma assinado digitalmente presença e um bom

reputação pela sua imparcialidade. Seu negócio está sendo um garantia
agente, como uma ligação de agência, e não na "queima" de qualquer
festa. (A matemática isso é interessante: enquanto a
os lucros a serem obtidos a partir de qualquer pequeno conjunto de transações é
menos do que seu "capital de reputação," é no seu interesse
abrir mão de lucros a partir da queima e ser honesto. É
também é possível marcar que Esther não pode lucrar
a queima de tanto Alice quanto Bob ou de ambos, ou seja, por
devidamente criptografar o caucionadas coisas.)
- Alice pode colocar sua parte da transação em conivência com
Ester, Bob pode fazer o mesmo, e, em seguida, Ester pode lançamento
os itens para as partes quando as condições forem atendidas, quando ambos
as partes concordam, quando o julgamento de algum tipo ocorre, etc.
(Há uma dúzia de problemas aqui, é claro, sobre como as controvérsias
são liquidada, sobre a qual as partes certificar-se de que
Ester tem os itens, ela diz que tem, etc.)

10.21. Pontas Soltas
10.21.1. Legalidade de tentar quebrar a criptografia de sistemas de
+ "O que é a legalidade da quebra de cifras fracas?"
- Suponha que eu encontrar algum aleatório olhando bits e encontrar uma maneira de
aparentemente diminuir a entropia, talvez, de transformá-los
na HBO ou canal Playboy? Que crime eu
comprometida?
- "Roubo de serviços" é o que vai ter para mim. Apenas
ouvia as transmissões podem agora ser um crime (celular,
polícia canais, transmissões via satélite). No meu ponto de vista, um
refrigeração developemt, por razões de ordem prática (aplicação
significa monitorização invasiva) e para o bom senso básico
ética razões: como pode a ouvir o que as terras em seu
propriedade de ser ilegal?
- Isso também abre a porta para que as leis que proíbem a ouvir
certos "bandido" ou "sem licença" braodcast estações.
Sombras da Cortina de Ferro. (Eu não estou falando sobre FCC
de licenciamento, por si só.)
+ "Não poderia nunca ser ilegal para tentar quebrar uma criptografia
sistema, mesmo se os dados subjacentes não é
"roubadas"?"
+ Criminalização *ferramentas* em vez de ações
- Os EUA está se movendo na direção de tornar mera
a posse de certas ferramentas e métodos ilegais, ao invés de
de criminalizar as ações reais. Este tem sido o
caso-ou assim eu ouço, que eu posso citar real leis--

com o "assaltante de ferramentas." (Algumas controvérsias isso, apontando para
a venda de lockpicks, livros sobre serralharia, etc.
Ainda, ver o que acontece se você tentar publicar uma
detalhada livro sobre como contrafacção de moeda.)
- Direito de Black prazo para isso?
+ De alguma forma, ele já é. Criptografia de vídeo é esse
caminho. Então, é celular.
- os participantes de retornar de uma Bahamas conferência sobre pirata
vídeo métodos (acho que por isso que foi nas Bahamas) tinha
seus trabalhos e demonstração de materiais apreendidos pela Alfândega
- A falsificação é, eu acho que, nessa situação, também.
Apenas explorar certos aspectos é verboten. (Eu não
reivindicamos que todos os aspectos são, é claro.)
- Interceptação de sinais de transmissão pode ser ilegal--
satélite ou celular tráfego (e Digital
Telefonia Lei pode ainda fazer tais intercepta ilegal
e punível no projeto de formas)
+ Ilegalidade da quebra de criptografia, a la
transmissão/scanner leis
- (Este veio em uma conversa com Steve Bellovin)
+ Aspectos
+ PPL lado...difícil convencer um PPL agente para "impor"
este
- mas o mercado de sanções contra aqueles que publicamente uso
as informações são do curso possível, assim como com
quem ouvir as conversas e fofocas
amplamente (considerando que o ato de ouvir, não é uma
o crime)
- legal de execução leva à complacência, para o abaixo-
par de segurança
+ é uma indesejável expansão do poder do estado para impor
leis contra a descriptografia de números
- e pode levar a global restrições sobre o uso de criptografia
10.21.2. wais, gopher, WWW, e implicações
- fronteiras mais transparente...não limpar _where_ pesquisas são
ocorrendo, arquivos transferrred, etc. (bem, é
determinísticos, de modo algum agente ou programa, presumivelmente, sabe,
mas é provável que os seres humanos não)
10.21.3. "Por que há tão muitos proeminentes Cypherpunks interessado em
a lei?"
- Bate-me. Nada é mais stultfyingly chato para mim do que
a sujeira e "encontrado itens" natureza do direito.
- No entanto, para uma determinada raça do hacker, lei hacking é o

desafio final. E é importante para alguns Cypherpunks
gols.
10.21.4. "Como vai crypto ser combatido?"
- Os suspeitos do costume: pornografia, pedofilia, terroristas, imposto de
evasores, espiões
+ Afirmações de que a "segurança nacional" está em jogo
- Como alguém já disse: "a segurança Nacional é a raiz
palavra-passe para a Constituição"
+ alegações de discriminação
- como um exemplo de criptografia permite que os ventos de contas bancárias,
uma carta de seguro, etc...essas são coisas que
vai agitar o bem-estar social sistemas de muitas nações
10.21.5. Stego também pode ser útil no fornecimento de operadores a bordo com
"plausível deniabillity"--eles podem alegar ignorância da LSB
conteúdo (não estou dizendo que isso vai ficar em cima tribunal muito
bem, mas de qualquer porta no meio de uma tempestade, especialmente a porta 25).
10.21.6. Uma mensagem pode ser provado para ser criptografada, e com que chave?
10.21.7. Legalidade digitais, assinaturas e carimbos de data / hora?
- Stu Haber confirma que isso não foi testado, não
precedentes estabelecidos
10.21.8. Um problema legal para provar a criptografia existe
- O XOR ponto. Qualquer mensagem pode ser transformada em qualquer outro
a mensagem, com a devida XOR intermédio de mensagem.
Implicações para a stego, bem como para a prova legal
(dificuldade de). Como bits de deixar as impressões digitais, a mera
presença de um determinado XOR pad em um réu do disco é
nenhuma prova de que ele colocou lá...a polícia poderia ter plantado
o delator chave, que transforma o "gi6E2lf7DX01jT$" em
"Dope está pronto." (Eu vejo problemas de "cadeia de evidências"
tornando-se ainda mais crítica, talvez com o uso de
"independente do módulo de autoridades" para fazer hashes de
apreendidos provas-hashes no sentido de criptografia e não
hashes no habitual polícia sentido.)
10.21.9. "Quais são os perigos de padronização e oficial
sanção?"
- Os EUA tem tido uma tendência a padronizar
alguns tecnologia e, em seguida, punir desvios da
standard. Exemplos: telefones, cabos (franquias concedidas,
os concorrentes excluídos)
- Franquias, padrões...
+ A minha preocupação: dinheiro Digital serão abençoados...home banking,
A Microsoft, de outros bancos, etc. O Tesouro gente vai entrar
em, etc.

- Os concorrentes terão um tempo difícil, como o governo lança
obstáculos na frente deles, como os EUA faz
acordos internacionais com outros países, etc.

10.21.10. Restrições de encriptação de voz?

+ pode surgir por uma irônica razão: as pessoas podem usar Net
conexões para falar em todo o mundo por us $1 de uma hora ou menos,
ao invés de us $1 por minuto; isso pode causar operadoras de telecomunicações para clamor
restrições
- impor essas restrições, em seguida, torna-se problemático,
a menos que o canal é monitorada
- e se encriptados...

10.21.11. Imprecisão das leis

- Pode parecer surpreendente que uma nação tão enredados em
complicado legalidade como os estados unidos, com mais advogados por
capita do que qualquer outra grande nação e com um código legal
que é composto de centenas de milhares de páginas de
regulamentos e interpretações, na verdade, é uma nação com
um código legal que é difícil de fixar para baixo.
- Qualquer sistema formal, rígida, de regras pode ser "gamed contra"
ser um adversário. Os legisladores sabem disso, e por isso as leis
são mantidos difusa suficiente para impedir mecânica de jogo; este
não pára por aí, de ser um exército de advogados (na verdade,
ele garante isso). Alguns diriam que as leis são mantidos
fuzzy para aumentar o poder dos legisladores e reguladores.
- "A regulamentação do banco neste país são mantidas deliberadamente
um pouco vago. O regulador da palavra é o de decidir
princípio, não uma interpretação minuciosa de estatuto. O
as linhas são confusos, e porque eles são por dentro, os bancos
não pressione sobre eles quase tão difícil como quando há clara
legal idioma disponível para ser interpretado em um tribunal.

"A incerteza do ambiente regulatório _increases_
a espera, os reguladores têm sobre os bancos. E o
reguladores de são conhecidos por serem decididamente mimado. Seus
as decisões são, em grande parte não sujeita a recurso (exceto para o
flagrante coisas, o que os reguladores são inteligentes o suficiente para não
para o fazer muitas vezes), e não há proteção contra cross-
a vinculação de problemas. Se um banco faz algo desagradável, digamos,
hipoteca bancária, eles podem se encontrar, dizer que a sua interestadual
ramificação possibilidades parecem de repente muito redutor.

"O Departamento. do Tesouro não quer untraceable
transações." [Eric Hughes, Cypherpunks lista, 1994-8-03]

- Tenta esgueirar-se em torno das leis, especialmente no
contexto de moedas alternativas, Perry Metzger notas:
"Eles estão simplesmente tentando impedi-lo de jogar jogos. O
a lei não é como a geometria -- não há axiomas e regras
para derivar uma coisa da outra. O princípio geral
é que eles querem controlar todas suas transações, e se
você torná-lo difícil eles vão usar a lei existente para
prisão você, ou irá produzir uma nova lei para tentar fazer o mesmo."
[Perry Metzger, 1994-08-10]
- Esta imprecisão e regulamentares critério está intimamente relacionado
para aqueles regimes malucos para evitar o pagamento de impostos, alegando , para
exemplo, que o "dólar" é definido como 1/35º da onça
de ouro (e que, portanto, os ganhos de "dólares de verdade"
são uma pequena fração da ostensivo de lucros), que Ohio
não entrar legalmente a União e, portanto, o imposto de renda foi
nunca devidamente ratificado, etc, etc, etc. Muitas dessas teorias
foi testado-e rejeitada. Digo isto porque alguns
Cypherpunks mostrar sinais de pensamento "dinheiro digital" oferece
oportunidades semelhantes. (E eu espero ver semelhantes golpes.)
- (Um exemplo relacionado. Pode uma acumulação de dinheiro
levado para fora do país? Dependendo de quem você perguntar, "é
depende". A retirá-lo na sua mala de viagem rasises todo o tipo
de possibilies de apreensão (violação da moeda de exportação
leis, lavagem de dinheiro, etc.). Fiação pode invocar
FinCEN dispara. O IRS pode afirmam que é a "fuga de capitais"
para evitar o pagamento de impostos--o que pode muito bem ser. Basicamente, o seu próprio
o dinheiro não é mais seu. Pode haver maneiras de fazer isso-eu
espero que sim--mas o ponto é que as regras são difusa,
e o poder discricionário para apreender os bens são grandes.
Procurar competente conselho, e depois orar.)
10.21.12. papel do Uniform Commercial Code (UCC)
- não foi discutida em círculos de criptografia muito, mas as "regras do
estrada"
- em muitos maneira, uma implementação do anarco-capitalismo, em
que a UCC é um descendente (módulo alguns detalhes) do
"A lei do Comerciante" que tratou de relações entre estados soberanos
poderes, o comércio no mar, etc.
- coisas, como eletrônica de fundos transfere, cheques, liablities
para forjado sigs, etc.
- Eu espero que eventual UCC envolvimento em esquemas de dinheiro digital
10.21.13. "O que sobre a corrida para legislar, para aprovar leis sobre
no ciberespaço, a informação superduperhighway, etc.?
+ O Congresso dos EUA, sente que tem de fazer "algo" sobre

coisas que muitos de nós sentem não precisa de regulamento ou de "ajuda"
a partir do Congresso.
- crypto legislação
- set-top boxes de cabo, de acesso, de Informação Nacional
Infra-Estrutura (Cabo Versão)
- acesso a informações, parental lock-outs, violência classificações,
materiais sexualmente explícitos, etc.
Relacionados para o "faça alguma coisa!" mentalidade Nacional de Saúde
Cuidado, armas, violência, etc.
- Por que não basta não fazer nada?
+ Assustador possibilidades sendo falado:
+ dando televisão conjuntos de IDs únicos ("V chips") com cabo
acesso através destes chips
- amarrar os cartões de IDENTIFICAÇÃO para estes, ou seja, Joe Cidadão, de
Provo, Utah, seria "permitido" para visualizar um NC-17
violência-nominal programa
- Isso seria desastroso: registros, vigilância,
dossiês, a permissão, a centralização
- "Como podemos corrigir isso?" mentalidade é muito prejudicial. Muitos
as coisas simplesmente não podem ser "corrigidos" por central planejadores....olhar
em economias para um exemplo. O mesmo é geralmente verdade para
tecnologias.
10.21.14. no uso de ventos de custódia de agentes de proteção contra
convulsões
- desprezo as leis entram em jogo, mas a ideia é fazer com que
- se impotentes para alterar a situação, e, portanto, não
deliberadamente desobedecer a tribunal
+ Também pode dizer ventos agentes que fazer com arquivos, e
quando a liberá-los
- Eric Hughes propõe: "Uma solução para isso é para dar
a frase-chave (ou outras informações de acesso) para alguém
que não vai dar para você se você estiver sob coação,
investigação, ordem judicial, etc. Seria o desejo de que
esta entidade ser em uma jurisdição diferente, onde um
a investigação pode acontecer." [E. H., 1994-07-26]
- Sandy Sandfort acrescenta: "Antes de apreensão/roubo, você gostaria de
fazer um acordo com uma ventos "escrow agent".
Após a apreensão você gostaria de enviar o seu computador
instrução que diz, "criptografar o meu disco com a conivência
agentes de chave pública." Depois disso, apenas o agente de custódia
pode descriptografar o disco. Claro, o agente de custódia
só que quando você tinha estipulado
estavam em vigor." [S. S., 1994-07-27]

relacionados aos dados de paraísos e ventos de crédito/P. I. paraísos
10.21.15. Pode o FCC-Requisitos de tipo para "limpar" a radiodifusão
(ou chaves fornecido para Feds) ser uma base para uma legislação semelhante
de redes privadas e privadas uso de criptografia?
- isso parece ser impraticável, dado o crescimento da
telefones celulares, redes locais sem fios, etc....não posso muito bem
mandato de que as empresas de difusão interna
comunicações em claro!
- compressão, comutação de pacotes, e todos os outros tipos de
"distorções" dos dados, requer transmissões
legível por agências do governo exigiria fornecendo o
governo com mapas (de onde os pacotes estão indo), com
específicos algoritmos de descompressão, etc....muito prático
10.21.16. Coisas que poderiam desencadear uma aba privacidade ou limitações no
crypto
- De forma anônima publicação da adoção de registros [sugerido por Brian
Williams, 1994-08-22]
- armas nucleares segredos (segredos, não apenas o
sedutoras coisas que qualquer um brilhante estudante de física
montam juntos)
- repugant mercados (assassinatos, órgão de vendas, etc.)
10.21.17. As pressões sobre os civis não revelar criptografia de conhecimento
+ Exemplo: telefone móvel de criptografia padrões.
- "Esta foi a linha oficial até poucos meses atrás - que
A5 era forte e A5X enfraquecido exportação
versão....No entanto, uma vez que nós temos A5 descobrimos que
ele não era particularmente forte não é fácil, 2^40
ataque. A linha do governo, em seguida, mudou para `você
não devemos discutir isso em público porque isso iria prejudicar
Britânico de vendas de exportação'....Talvez tudo não passou de uma manobra para obter
Saddam para comprar A5 batata frita algumas questionáveis, negociante de armas
escreva. [Ross Anderson, "mobil telefone na europa <gms-
padrão>, uma precedência?," sci.cripta, 1994-08-15]
- Agora este exemplo vem da grã-Bretanha, onde o
a comunidade de inteligência sempre teve mais de lattitude
nos EUA (um Ato dos Segredos Oficiais, sobre os limites
prima, sem traquinas Constituição para ficar no caminho, e até mesmo
mais de um rapaz de rede que nós temos nos EUA
mil-complexo industrial).
- E a ameaça pelo NSA funcionários têm Jim Bidzos, o
o presidente da RSA Data Security, Inc., morto se ele não
jogar bola. {"Chaves do Reino" San Jose Mercury
Notícias]

10.21.18. "identidade de custódia", de Eric Hughes, por restrições e-mail
contas de e eletrônicos, caixas de PO (se tem falado sobre,
aparentemente...sem detalhes)

11. Vigilância, Privacidade, E As Agências De Inteligência

11.1. direitos autorais
O CYPHERNOMICON: Cypherpunks FAQ e Mais, Versão 0.666,
1994-09-10, Direitos De Autor Timothy C. De Maio. Todos os direitos reservados.
Veja os detalhes de isenção de responsabilidade. Use seções curtas em "justo
use" disposições, com crédito apropriado, mas não coloque o seu
nome em minhas palavras.

11.2. RESUMO: a Vigilância, Privacidade, E as Agências de Inteligência
11.2.1. Pontos Principais
11.2.2. Ligações para Outras Secções
11.2.3. Onde Encontrar Informações Adicionais
- Bamford ("The Puzzle Palace"), Richelson (vários livros,
incluindo "dos EUA, as Agências de Inteligência"), Burrows ("Deep
O preto", sobre o NRO e espião de satélites), a Acção Encoberta
Trimestral
11.2.4. Diversos Comentários

11.3. Vigilância e Privacidade
11.3.1. Nós percorremos um longo caminho desde o Secretário de Estado do Stimpson
famoso "Senhores, não leia outros cavalheiros mail"
instrução. É agora amplamente tomadas para concedido que os Americanos
são para ser controlada, vigiada, e até mesmo interceptado pelo
várias agências de inteligência. O FBI e o departamento de Segurança Nacional
Agência, a CIA, o National Reconnaissance Office, etc.
(Sim, esses grupos têm várias cartas dizendo-lhes que
eles podem espionar, o que legalidades eles têm que atender, etc. Mas
eles ainda espião. E não há um alvoroço--o "o Que você tem
tem a esconder?" do lado de Americano de privacidade dicotomia.)
11.3.2. Duncan Frissell nos lembra de Justiça Jackson, 1948
opinião divergente em alguns casos:
- "O governo poderia simplificar a aplicação do código penal, por
exigir que todos os cidadãos "para manter um diário que iria mostrar
onde ele foi, em todos os momentos, com quem ele foi, e o que ele
foi até." [D. F. 1994-09-06, a partir de um artigo no WSJ]
- (Deve ser observado que os dispositivos de rastreamento--colares,
pulseiras, implantáveis transmissores--existem e estão em uso
com os presos. Alguns pais são mesmo de instalá-los em

crianças, é alvo de rumores. Uma preocupação para o futuro?)
11.3.3. "O que é o "estado de vigilância"?"
- o problema com a criptografia é a _centralization_ de
escutas...muito mais fácil do que o plantio de bugs
+ "Deve ser dada alguma liberdade para a segurança?"
+ "Quem está disposto a trocar liberdade por segurança
- não merece nem
+ liberdade nem segurança
- Ben Franklin
- a desvantagem é muitas vezes ilusória-polícia estados de resultado quando
os trens são feitos para rodar em tempo
- "É um pouco irônico que a Administração está lamentando,
tão alto,
sobre a união Soviética/rússia espião da CIA-como se esta fosse
injusto --
enquanto eles estão proclamando abertamente o direito de espionar
cidadãos
e estrangeiros através de Clipper." [Carl Ellison, 1994-02-23]
+ Câmeras estão se tornando onipresentes
+ barato, integrado, nova technologes
- SDI lente olho de peixe
- Caixas eletrônicos
- traffic, radares de velocidade, esquinas
- loja de segurança
- Códigos de barras-o pior medo de todos...e não plausível
+ Reconhecimento automático ainda está faltando
- ficando cada vez melhor, lentamente
- redes neurais, etc. (mas estas exigem formação)
11.3.4. "Por que o governo monitor _my_ de comunicação?"
- "Por causa da economia e a estabilidade política....Você pode
construir computadores e dispositivos de monitoramento em segredo, implantar
eles em segredo, e ouvir _everything_. Para ouvir
tudo com porretes e produtos farmacêuticos não
só o custo mais mão-de-obra e equipamentos, mas também gerar uma
radicalizar reação a um estado policial." [Eric
Hughes, 1994-01-26]
- Como sistemas de Telefonia Digital e Clipper torná-lo muito
fácil para os governos para a monitorização de rotina aos seus cidadãos,
usando uma tecnologia automatizada que requer drasticamente menos
envolvimento humano do que o anterior polícia estados necessária.
11.3.5. "Como a quantidade de vigilância está realmente sendo feito hoje?"
+ FBI e policiais Atividades de Vigilância
- o FBI mantidos registros de reuniões (entre Americanos

empresas e Nazista interesses), e pode ter usado esses
registros durante e após a guerra, a pressão de empresas
+ NSA e a Agência de Segurança Atividades de Vigilância
- coleta de inteligência económica
- na 2ª guerra mundial, economia de Guerra Conselho (que foi renomeado Conselho
da economia de Guerra) manteve guias sobre os embarques de petróleo
e outros produtos
+ MINARETE, palavra de código para a ANS "lista de observação" material
(intercepta)
- SIGINT OPERAÇÃO MINARETE
- originalmente, assistir a lista de material foi "TOP SECRET
ALÇA ATRAVÉS DE APLICAÇÕES DE COMINT CANAIS DE UMBRA GAMMA"
+ NSA segmentação é feita principalmente através de uma lista chamada
Inteligência Diretrizes para aplicações de comint Prioridades (IGCP)
- banca examinadora composta de representantes das diversas
órgãos de inteligência e de
- intiated em torno de 1966
+ revelações seguintes Documentos do Pentágono, que nacional
segurança elsur pegou conversas privadas (parte
dos Trabalhos)
- temporização de PP foi o final de 1963 e início de 1964...sobre o tempo UB
foi ficar indo
+ F-3, a NSA antena principal sistema de intercepção de ASCII
as transmissões a partir de onu-TEMPESTed terminais e PCs
- os sinais podem ser captado através de paredes até um pé
de espessura (ou mais, considerando-se como tais impulsos de rejeição
ao redor)
+ Conjunta do FBI/NSA Atividades de Vigilância
+ Operação Shamrock foi um empate entre a ANS e o FBI
- a partir de 1945, embora não tivesse sido anteriormente intercepta,
muito
- COINTELPRO, os dissidentes, os radicais
+ 8/0/45 Operação Trevo começa
- um sub rosa esforço para continuar o monitoramento
arranjos de WW II
- ITT Comunicações acordado para virar todos os cabos
+ RCA Comunicações também virou todos os cabos
- tinha até uma ex-Signal Corps oficial como vice-presidente para
tratamos de todos os detalhes
direto de conexões RCA linhas foram feitas, para o cuidado
o monitoramento por parte do ASA
- cabos e de empresas, escritórios de advocacia,
as embaixadas, os cidadãos foram todos mantidos

+ 12/16/47 Reunião entre Sóstenes Behn, da ITT,
Geral Ingles da RCA, e Sec. de Defesa James
Tinha
- para discutir a Operação do Trevo
- para organizar as isenções de acusação
+ 0/0/63 Operação Trevo entra em uma nova fase como RCA
Opções globais para informatizado operação
coincidente com a Colheita na ANS
- e é perfeito para iniciar o UB/Severn operações
+ 1/6/67 Hoover oficialmente termina "saco preto"
operações
- preocupado com o tiro saiu pela culatra
- já tinha ajudado a ANS pelo roubo de códigos, cifras,
descriptografados tráfego, o plantio de bugs linhas de telefone, etc.
- a partir de embaixadas, empresas
- claro se essas operações continuação
de qualquer maneira
+ Reviravolta: pode ter sido a motivação para a ANS e
UB/Severn a buscar outras vias, tais como a utilização de
criminosos como recortes
- e é paralela à "Canalizadores" Unidade utilizada pelo Branco
Casa
+ 10/1/73 AG Elliot Richardson ordens do FBI e SS a
parar o pedido de vigilância da NSA material
- NSA concordou em deixar de fornecer a este, mas não disse
Richardson sobre Shamrock ou Minarete
- no entanto, os eventos deste ano (1973) marcou o fim de
Minarete
+ 3/4/77 Justiça Depto. recomenda contra a repressão
de qualquer NSA, FBI ou o pessoal de Operações do Trevo
e o Minarete
- decidiu que NSCID N.º 9 (aka Nº 6) deu NSA
suficiente margem de manobra
- 5/15/75 Operação Trevo oficialmente encerrada
- e o Minarete, do curso de
+ Operação Trevo-Detalhes
+ 8/0/45 Operação Trevo começa
- um sub rosa esforço para continuar o monitoramento
arranjos de WW II
- ITT Comunicações acordado para virar todos os cabos
+ RCA Comunicações também virou todos os cabos
- tinha até uma ex-Signal Corps oficial como vice-presidente para
tratamos de todos os detalhes

direto de conexões RCA linhas foram feitas, para o cuidado
o monitoramento por parte do ASA
- cabos e de empresas, escritórios de advocacia,
as embaixadas, os cidadãos foram todos mantidos
+ 12/16/47 Reunião entre Sóstenes Behn, da ITT,
Geral Ingles da RCA, e Sec. de Defesa James
Tinha
- para discutir a Operação do Trevo
- para organizar as isenções de acusação
+ 0/0/63 Operação Trevo entra em uma nova fase como RCA
Opções globais para informatizado operação
coincidente com a Colheita na ANS
- e é perfeito para iniciar o UB/Severn operações
+ 8/18/66 (quinta-feira) Nova análise de site em Nova York
Operação Trevo
+ Louis Tordella cumpre com a CIA Dep. Dir. de Planos e
arranja para configurar um novo posto de escuta para a análise
as fitas de RCA e ITT (que tinha sido
enviado à ANS e, em seguida, de volta)
- Tordella mais tarde foi envolvido na configuração do relógio
lista em 1970 para o BNDD, (Operação Minarete)
- LPMEDLEY foi o nome de código, de uma televisão de fita
processamento de loja (lembra do "Homem da U. N. C. L. E."
- mas NSA tinha muito afastar-se, mais tarde,
- 5/15/75 Operação Trevo oficialmente encerrada
+ 10/1/73 AG Elliot Richardson ordens do FBI e SS a
parar o pedido de vigilância da NSA material
- NSA concordou em deixar de fornecer a este, mas não disse
Richardson sobre Shamrock ou Minarete
- no entanto, os eventos deste ano (1973) marcou o fim de
Minarete
- Abzug comitê solicitado pelo New York Daily News relatório,
7/22/75, que a NSA e o FBI tinha sido monitoramento
comercial cabo de tráfego (Operação Trevo)
+ 6/30/76 175 relatório de página na Justiça Depto.
investigação de Trevo e o Minarete
- apenas 2 cópias preparados, classificados como "TOP SECRET" UMBRA,
ALÇA ATRAVÉS DE APLICAÇÕES DE COMINT DOS CANAIS DE
+ 3/4/77 Justiça Depto. recomenda contra a repressão
de qualquer NSA, FBI ou o pessoal de Operações do Trevo
e o Minarete
- decidiu que NSCID N.º 9 (aka Nº 6) deu NSA
suficiente margem de manobra

+ NSA programa, iniciado em agosto de 1945, para monitorar todos os telegramas entrar ou sair dos EUA
- lembra da Yardley do regime na década de 1920 (e provavelmente em alguns outros)
- só é conhecido Louis Tordella e agentes envolvidos
- compartimentalização
+ Enredo Links de Operação Trevo para Operação Ultra Preto
- muitos links, a partir de sigilo, a compartimentalização, e a ilegalidade dos métodos utilizados e a subversão do governo de energia
- "Shamrock foi soprado...Ultra Black entocada mesmo mais profundo."
+ NSA, FBI e a vigilância dos Cubanos simpatizantes
- "lista de observação", usado
- estavam lá os links para Meyer Lansky e Trafficante via o JFK-a Máfia de conexão?
- diversas Watergate quebra de ligações (Cubanos usado)
- Hoover terminou preto-saco de operações em 1967-8
+ NSA, FBI, e os Dissidentes (COINTELPRO-tipo de actividades)
+ 10/20/67 NSA é solicitado para iniciar a coleta de informações relacionados com a desordem civil, guerra manifestantes, etc.
- Inteligência do exército, do Serviço Secreto americano, a CIA, o FBI e o DIA foram todos os envolvidos
- sem dúvida, este continua (dado o sucesso do FBI e do Serviço Secreto em seguir os principais atos de o terrorismo e tentativas de assassinatos)
+ Huston Plano e Planos Relacionados com (1970-71)
- 7/19/66 Hoover oficialmente termina saco preto operações
+ 1/6/67 Hoover oficialmente termina saco preto operações
- temendo o tiro saiu pela culatra, preocupado com o seu lugar na história
+ 6/20/69 Tom C. Huston recomenda maior atividade de inteligência sobre a dissidência
- memorando para a NSA, CIA, DIA, FBI
- esta, mais tarde, torna-se base de Huston Plano de
+ 6/5/70 Reunião na Casa Branca para se preparar para Huston Plano; Comissão Interinstitucional de Inteligência (Ad Hoc), ICI
- Nixon, Huston, Ehrlichman, Haldeman, Noel Gayler de NSA. Richard Helms da CIA, J. Edgar Hoover, do FBI,

Donald V. Bennett, do DIA
- William Sullivan do FBI chamado para cabeça ICI
+ NSA entusiasticamente apoiada ICI
- PROD chamado Benson Buffham como elo de ligação
procurado, o aumento sub-reptícia entradas e
eliminação de restrições legais doméstica
vigilância (não que eles tinham sentido vinculado por
legalisms)
- destinatários para ser "Preconceituoso" e com ainda mais
segurança do que o tradicional TOP SECRET, IDENTIFICADOR de VIA
APLICAÇÕES DE COMINT DOS CANAIS DE
-
+ 7/23/70 Huston Plano de circulado
- 43 páginas, intitulado Nacional de Recolha de informação
Plano: Análise e Estratégia
- pediu o aumento sub-reptícia (entradas para códigos
cifras, planos, listas de membros)
- segmentação de embaixadas
+ 7/27/70 Huston Plano cancelado
pressão pelo Procurador-Geral John Mitchell
- e, talvez, por Hoover
- Huston rebaixado; ele renunciou um ano depois
- mas o Plano não estava realmente morto...talvez Huston do
o erro foi em ser jovem e vocal e fazer o
relatório muito visível e ninguém nega o suficiente
+ 12/3/70 Inteligência Comissão de Avaliação (IEC) cumpre
(Filho-do-Huston Plano)
- John Dean dispostos no outono de '70
- Robert C. Mardian, Assistente AG Interno de Segurança
dirigiu-se a IEC
- Benson Buffham de NSA/PROD, James Jesus Angleton de
CIA, George Moore, do FBI, Coronel João Downie do DOD
- essencialmente adoptado todas Huston Plano de
+ 1/26/71 NSA problemas NSA Contribuição para Domésticas
Inteligência (como parte do IEC)
- ampliação do escopo da vigilância relacionados a medicamentos (via
BNDD e FBI), o estrangeiro
- "não há indicação de procedência" no material gerado
- full compartimentalização, NSA para assegurar o cumprimento
+ 8/4/71 G. Gordon Liddy atende IEC reunião, para obter
a investigar o vazamento de Documentos do Pentágono
- canal do NSA/PROD para Encanador Unidade em Branco
Casa, ignorando outras agências

+ 6/7/73 New York Times revela detalhes de Huston Plano de
- texto integral publicado
- ensaios de Meteorologista comprometida e, finalmente,
descarrilou ele
+ 10/1/73 AG Elliot Richardson ordens do FBI e SS a
parar o pedido de vigilância da NSA material
- NSA concordou em deixar de fornecer a este, mas não disse
Richardson sobre Shamrock ou Minarete
- no entanto, os eventos deste ano (1973) marcou o fim de
Minarete
+ FINCEN, IRS, e Outros de acompanhamento Econômico
- definir, em Arlington como um grupo para monitorar os fluxos de
dinheiro e informações
+ eventualmente, estes grupos vão ver a necessidade ativamente
invadir sistemas de computadores utilizados por vários grupos que
estão sob investigação
- laços da morte de Alan Standorf? (Vint Hill)
- Casolaro, Riconosciutto
11.3.6. "O governo quer monitorar transações econômicas?"
- Indisputável, eles _want_ para. Se eles têm real
planos para fazer isso é mais discutível. O Clipper e Digital
Telefonia propostas são duas das indicações eles
tenha grandes planos estabelecidos para garantir a sua fiscalização
recursos são mantidos e estendidos.
- O governo vai-se cada vez mais em pânico como mais Líquido
o comércio se desenvolve, à medida que o comércio se move ventos, e como
a criptografia se espalha.
11.3.7. O risco de que a vigilância da sociedade: Você não pode se esconder
- raramente discutido como uma preocupação
- nenhuma válvula de escape, não há lugar para aqueles que cometeram erros, para
escape para
- (historicamente, este é um caminho para os criminosos para obter de volta em um
melhor faixa--se uma identidade digital significa que o seu registo
para sempre segue-los, isso pode...)
+ Um problema crescente na América e outros "democratas"
países é a tendência para tornar obrigatório que uma vez foram
voluntária escolhas. Por exemplo, a impressão digital para crianças
ajuda em casos de rapto pode ser uma coisa razoável a fazer
voluntariamente, mas alguns distritos escolares estão planejando fazer
é obrigatório.
- Isso tudo é parte do "Vamos aprovar uma lei" mentalidade.
11.3.8. "Eu deveria recusar-se a dar o meu Número de Segurança Social para os
que pede para ele?"

- É um pouco fora de criptografia, mas a questão não param de chegar
até no Cypherpunks lista.
- Na verdade, eles nem precisa pedir
mais....ele é conectado a tantos _other_ coisas que pop
até quando eles introduza o seu nome que é um ponto discutível. No
outras palavras, o mesmo dossiês que permitem o cartão de crédito
empresas para enviar você "pré-aprovados cartões de crédito" a cada poucos
dias iguais dossiês que MCI, Sprint, AT&T, etc. são
utilizando para você se inscrever.
11.3.9. "O que é "Privacidade 101'?"
- Eu não conseguia pensar em uma maneira melhor para introduzir o tópico de
como as pessoas podem proteger a sua privacidade, evite
a interferência do governo, e (talvez) evitar o pagamento de impostos.
- Duncan Frissell e Areia Sandfort ter dado um monte de
dicas sobre isso, alguns deles simplesmente o senso comum, alguns dos
- os mais misteriosos.
+ Eles são a realização de um seminário, intitulado "PRIVACIDADE 101" e
os arquivos são disponíveis pela Web em:
- http://www.iquest.com/~fairgate/privacy/index.html
11.3.10. Telefones celulares são acompanhados por região...as pessoas estão ficando
chamadas de telefone como eles cruzam em novas zonas, "boas-vindas" - os
- mas isso implica que a sua posição já está sendo controlada
11.3.11. Uso ubíquo de Cpfs e outros dados pessoais, I. D.
11.3.12. câmeras que podem reconhecer rostos são colocados em muitas público
lugares, por exemplo, aeroportos, portos de entrada, os edifícios do governo
- e mesmo em alguns lugares privados, por exemplo, cassinos, lojas que
tive problemas com determinados clientes, os bancos que enfrentam
roubos, etc.
11.3.13. especulação (para os paranoids)
- vigilância secretas pelo não-invasivo de detecção de
métodos...tomografia por emissão de pósitrons, para ver que parte do
o cérebro está ativo (acho que a paranoia possibilidade!)
- normalmente necessidades especiais compostos, mas...
11.3.14. Diários não são mais privadas
+ pode ser aberta sob várias condições
- intimação no julgamento
- descoberta em vários processos judiciais, incluindo o divórcio,
custódia, calúnia, etc.
- negócios
- os psiquiatras (sob Tarasoff decisão) pode ter registros
aberto; o que pode-se pensar que a necessidade de crimes
confessou diminui a ser relatado, este é certamente um
nova era

- Packwood diário estabelece a tendência: diários não são
mais sacrossanta
- Uma implicação para criptografia e Cypherpunks tópicos é que
diários e registros similares podem ser armazenadas em criptografados
formas, ou situadas em locais offshore. Pode haver mais
e mais uso de ventos ou registos codificados.

11.4. As Agências de Inteligência dos EUA: NSA, FinCEN, CIA, DIA, NRO, FBI
11.4.1. O foco aqui é em agências nos estados unidos, por várias razões. Mais
Cypherpunks são atualmente os Americanos, a ANS tem uma dominante
papel em tecnologia de vigilância, e os EUA são o foco de
mais atual de criptografia debate. (A grã-bretanha tem o GCHQ, o Canadá tem
sua própria SIGINT grupo, os holandeses têm...., A França tem DGSE e
assim por diante, e (...)
11.4.2. Tecnicamente, não são todos iguais. E alguns podem tergiversar com a minha
chamar o FBI, que uma "agência de inteligência." Todos têm
vigilância e monitoramento de funções, ainda que de diferentes
sabores.
11.4.3. "É a ANS envolvidos na vigilância doméstica?"
+ Não totalmente confirmada, mas muita evidência de que a resposta
é "sim":
* anterior vigilância doméstica (Operação Trevo,
telégrafos, ITT, conluio com o FBI, etc.)
* relações de reciprocidade com GCHQ (reino UNIDO)
* arranjos em reservas indígenas para micro-ondas
intercepta
* a tecnologia permite que ele (SIGINT, linhas de telefone)
* a Lei de Segurança Nacional de 1947, e, mais tarde,
esclarecimentos e Ordens Executivas, torna provável
- E o impulso para a Telefonia Digital.
11.4.4. "Qual será o impacto do amplo uso em criptografia
recolha de informação?"
- Leia Bamford para algumas coisas sobre como o NSA intercepta
no exterior de comunicações, como eles venderam deliberadamente-
aleijado de criptografia de máquinas para as nações do Terceiro Mundo, e como
muito medo de que o spread do forte, essencialmente,
inquebrável de criptografia. "O Puzzle Palace", foi publicado em
1982...as coisas só pioraram em relação a isso desde então.
- Declarações de altos funcionários da inteligência refletir essa
preocupação.
- Digital morto cai, irá mudar todo o jogo de espionagem.
Informação de mercados, os dados de paraísos, rastreáveis e-mail todos os...
essas coisas terão um profundo efeito sobre o nacional

questões de segurança.
- Eu espero que o pessoal gosta de Tom Clancy para escrever romances sobre
como de segurança nacional dos EUA interesses estão sendo ameaçados
por "inquebrável de criptografia." (Eu gosto de algumas Clancy romances, mas
não há como negar que ele é um ponta-direita que abertamente
crítica das tendências sociais, e que ele acredita druggies
deve ser morto, o governo é necessário para afastar
mal, e os cidadãos comuns não deveriam ter ferramentas o
o governo não pode superar.)
11.4.5. "O que será que os efeitos da criptografia convencional de espionagem?"
- Enorme efeitos; atente para este ser citado como uma razão
para proibir ou restringir o crypto-porém de sentido que pode ser.
+ Efeitos:
- informação de mercados, a la BlackNet
- digital mortos gotas -- por que usar latas de Coca-cola perto de árvores de carvalho
quando você pode colocar as mensagens em arquivos e pós-las
em todo o mundo, com untraceably? (mas, mais importante, com uma
assinatura digital!)
- transparência das fronteiras
- o comércio de armas, braços negócios
- vírus, armas
11.4.6. NSA orçamento
- Us $27 bilhões ao longo de 6 anos, dar ou tomar
- na verdade, pode aumentar, apesar do fim da Guerra Fria
- novas ameaças, estados menores, propagação de armas nucleares, preocupações
sobre o comércio, lavagem de dinheiro, etc.
- primeira regra de burocracias: eles sempre ficar maior
+ NSA-Cray Computador supercomputador
+ comunicado de imprensa, 1994-08-17, dá algumas dicas sobre o
capacidades procurado pela vigilância do estado
- "O Cray-3/SSS vai ser um sistema híbrido, capaz de
vetor de processamento paralelo, escalável paralelo
processamento e uma combinação de ambos. O sistema irá
consistem em um processador duplo de 256 milhões de word Cray-3 e
um 512,000 processador de 128 milhões de byte único da instrução
multiple data (SIMD) de matriz.....SIMD matrizes de um
milhões de processadores são esperados para ser possível utilizando
a versão atual do Processador-Em-Memória (PIM)
chips desenvolvidos pela Supercomputação, Centro de Pesquisa
uma vez que o desenvolvimento do projeto está concluída. O PIM chip
contém 64 único-bit e 128 kilobytes bits
da memória. Cray Computador irá pacote PIM chips
utilizando a avançada vários chip do módulo de embalagem

a tecnologia. Os chips são fabricados Nacional
Semiconductor Corporation."
- Este é, provavelmente, o supercomputador descrito no
Gunter Ahrendt relatório
11.4.7. FINCEN, IRS, e Outros de acompanhamento Econômico
- Financial Crimes Enforcement Network, um consórcio ou tarefa
força de DEA, departamento de justiça, do FBI, da CIA, DIA, NSA, IRS, etc.
- definir, em Arlington como um grupo para monitorar os fluxos de
dinheiro e informações
- eventualmente, estes grupos de ver a necessidade de invadir
sistemas de computador usado por vários grupos que estão sob
investigação
- Cf. "Com fio", ambos de novembro ou dezembro, 1993
11.4.8. "Por que tantos serviços de informática, de telecomunicações, e a agência de crédito
empresas localizadas perto de inteligência dos estados unidos, agência de sites?"
+ Por exemplo, o cluster de telecomunicações e de informação de crédito
agências (TRW Crédito, Transunion, etc.) e em torno da
McLean/Langley área da Virgínia do Norte (incluindo
Herndon, Viena, Tyson Canto, Chantilly, etc.)
- a mesma coisa de que me recordo, de vários computadores de rede
provedores, como UUCP (ou o que for), América Online,
etc.
- A menos conspiratórias vista: porque todos estão localizados perto
Washington, D.C., para diversas autoridades, lobby, etc.
razões
+ Mais conspiratórias vista: para garantir que o
as agências de inteligência têm acesso fácil a comunicação,
direto de telefones fixos, etc.
- agências de informações de crédito é necessário limpar as identidades
são fabricados para as agências de inteligência, WitSec,
etc. (as três principais agências de crédito têm de ser
cúmplices destas criações, como "fantasmas" mostra-se
imediatamente quando o ex registros são cruzadas)
- Como Paul Ferguson, Cypherpunk e gerente de US Sprint,
coloca: "Estamos localizados em Herndon, Virgínia, direito
a rua a partir de Dulles Aeroporto e um pulo, saltar &
saltar para baixo da rua, o novo NRO office. ,-)"
[P. F., 1994-08-18]
11.4.9. Força-tarefa 157, ONI, Kissinger, Castelo Banco, Nugan Hand Bank,
CIA
11.4.10. NRO construção de controvérsia
- e uma agência eu não tinha visto listados até agosto, de 1994: "O
Central De Imagens Do Office"

11.4.11. SIGINT ouvir mensagens
+ possível monkeywrenching?
- provavelmente muito difícil, mesmo para um EMP bomb (não-nuclear,
o que é)
11.4.12. "Que passos está a ANS tomando?"
* além de ameaças de morte contra Jim Bidzos, que é
* Clipper um plano para expulsar os concorrentes (preço, exportação
leis, assédio)
* cooperação com outras agências de inteligência, de outras nações
- Nova Ordem Mundial
* ameaças de morte foram provavelmente apenas um caso de bullying, mas...
poderia ser parte de uma campanha de terror--para fechar
até os críticos ou pelo menos fazer com que eles hesite em

11.5. Vigilância em Outros Países
11.5.1. Em parte, isto se sobrepõe sobre a discussão anterior de criptografia leis
em outros países.
11.5.2. Não-AMERICANO de Vigilância de Organizações
+ BnD -- Bundesnachrichtendiens
Alemão - serviço de segurança
- BND está em busca de emenda constitucional, comprar pode não precisar de
ele, como o simples chamada para ele contou a todos o que já é
existente
- "aspirador de pó no éter"
- Gehlen...Frente Oriental Inteligência
- Pullach, fora Munchen
- eles sempre tentaram obter a aprovação para fazer doméstica
espionagem...uma chave para o poder
+ Bundeskriminalamt (BKA) -- W. alemão FBI
- HQ encontra-se em Wiesbaden
- bomba explodiu quando a ser examinado, matando um
oficial (relacionada com a Pan Am/Lockerbie/PFLP-GC)
- sinal tem duas águias negras (de costas)
- BVD -- Binnenlandse Veiligheids Dienst, holandês Interno
Serviço De Segurança
+ SDECE
- Inteligência francês (foreign intelligence), vinculada ao
Greepeace navio bombardeio na Nova Zelândia?
- SDECE tinha links para a Surpresa de outubro, como um pouco de francês
os agentes estavam em negociações, os braços envios
fora de Marselha e Toulon, e em reuniões com
Russbacher e os outros
- O horário de verão, Direction de la Surveillance du Territoire,

counterespionage braço da França (paralelo ao FBI)
+ DSGE, Direção G□n□ralé " de la S□curit□ Ext□riere
- fornece projecto de deferments para quem entregar roubado
informações
+ Suécia, Forsvarets Radioanstalt ("Rádio Agência
Defesa")
- rachado alemão de comunicação entre os ocupados, a Noruega e a
ocupou a Dinamarca
- Beurling, com papel e lápis só
+ Mossad, LAKAM, Israel
+ HQ em Tel Aviv, perto de SEDE da AMAN, de inteligência militar
- não HQ mover-se em torno de um monte?
- LAKAM (sp?), um supersecret inteligência Israelense
agência...foi mostrado a PROMIS software em 1983
+ aprendidas de Paquistanesa de sucesso na construção de uma bomba atômica
e tomou medidas contra os Paquistaneses liderança:
a destruição do avião que transportava o Presidente (Zia?)
e alguns especialistas dos EUA
- Mossad sabia do DIA e CIA envolvimento em BCCI
financiamento da bomba atômica Paquistanesa esforços (e links para
outros traficantes de armas que permitiram dispara e similares
para chegar Paquistão)
- revelações por Vanunu foram projetados para assustar o Árabe e
Mundo muçulmano-e enviar um sinal de que a morte de
O presidente Zia era para ser o destino de qualquer líder Paquistanês
que continuou o programa
11.5.3. Eles são muito ativos, embora eles ficam menos publicidade do que fazer
a Americana, CIA, NSA, FBI, etc.

11.6. Métodos de vigilância e Tecnologia
11.6.1. (alguns dos que isso fica especulativa e por isso não pode ser para
do agrado de todos,)
11.6.2. "O que é que a TEMPESTADE e qual é a importância disso?"
- TEMPESTADE apprarently significa nada, e, portanto, não é uma
acrônimo, apenas um nome. A todos os caps é o padrão
ortografia.
- Emissão de RF, um conjunto de especificações para o cumprimento
- Van Eyck (ou Van Eck?) radiação
+ Principalmente Crt são a preocupação, mas também de painéis LCD e o
o circuito interno de PCs, estações de trabalho ou terminais.
- "Muitas telas de LCD podem ser lidos à distância. O sinal de
não é tão forte como o que de pior vdus, mas é
ainda considerável. Eu tenho demonstrado ataques Zenith

laptops a 10 metros ou então com um curso de ESL 400 monitoramento
receptor e 4m de antena dipolo; com o mais moderno
receptor, uma antena direcional e de uma tranquila RF
ambiente não há nenhuma razão por 100 metros deve ser
impossível." [Ross Anderson, a Tempestade de Ataques em Notebook
Computadores ???, comp.segurança.diversos, 1994-08-31]

11.6.3. Quais são algumas das Novas Tecnologias de Espionagem e Vigilância

+ Bugs
+ NSA e a CIA foram desenvolvidos novos níveis de miniaturizados bugs
- por exemplo, sistemas passivos que apenas driblar fora interceptado
material, quando interrogado (por exemplo, quando nenhum bug varre
estão em curso)
- muitas destas novas incomodando tecnologias foram utilizadas na
John Gotti caso em Nova York...o fim da Guerra Fria
significava que muitas destas tecnologias se tornou disponível
para utilização não-defesa lateral
- o uso de tais incomodando a tecnologia é assustadora
desenvolvimento: conversas podem ser ouvidas dentro lacrado
casas de todo ruas, e tudo o que vai ser
necessário é obrigatória mandado de
+ DRAM de armazenamento de compressão de voz...6-bit companded,
frequência-limitada, de modo que 1 seg de discurso leva
50Kbits, ou 10K quando compactado, para um total de 36 Mb
por hora, isso vai caber em um único chip
- leitura pode ser feita a partir de uma "nave-mãe" (módulo de um
maior erro que se senta em algum local mais seguro)
- ou via apertado de feixes de lasers
+ Bugs são Móveis
- rastreamento de paredes, usando MIT-construído em tecnologia para microrobots
- alguns podem até voar para distâncias curtas (alguns klicks)
+ Escutas
- tantas abordagens aqui
- telefone opções são quase totalmente digital (la ESS IV)
- novamente, o software de hacks para permitir escutas
+ Vans equipadas para espionar a PCs e redes
+ TEMPESTADE sistemas
+ a tecnologia é um pouco restrito, empresas, fazendo isso
o trabalho está sob limitações de não enviar para alguns clientes
- não há leis contra a blindagem, é claro

- estes veículos são justificados para a "guerra às drogas" e
a proliferação de armas controle esforços (N. E. S. T., anti-
O iraque, etc.)
+ De longa distância de audição
- refletor parabólico, cancelamento de ruído (de qualquer off-
eixo fontes), de alto ganho de amplificação, de análise de fonema
- redes neurais que aprender os padrões de fala e, portanto, pode
melhorar a clareza
+ leitura labial
- com eletronicamente estabilizado CCD geradores de imagens, de 3000mm lentes
- rede neural baseada em leitura labial programas, com a aprendizagem
sistemas capazes de melhorar o desempenho
- para os cargos sensíveis, a disponibilidade de novas
outros métodos de acelerar a conversão para seguro
sistemas baseados em criptografados de telecomunicações e o
prevenção de voz baseado em sistemas de
11.6.4. Telefonia Digital II é um grande passo em direção a mais fácil
vigilância
11.6.5. Acompanhamento cidadão
+ o que os governos do mundo gostaria de rastreamento
os movimentos, ou pelo menos os principais movimentos, de suas
assuntos
- faz o preto mercados um pouco mais difícil
- superfícies terroristas, os imigrantes ilegais, etc. (não
perfeitamente)
+ permite o rastreamento de "criminosos sexuais"
- que muitas vezes têm de se registar com a polícia local,
anunciar para os seus vizinhos os seus crimes anteriores, e
geralmente o desgaste de uma carta vermelha em todos os tempos--eu não sou
defender estupradores e molestadores de crianças, apenas observando o
precedente perigoso esta é a definição
- porque sua natureza de burocracias querer saber
onde "seus" assuntos são (dossiê sociedade = contabilidade
sociedade...registros são fundamentais)
+ Bill Stewart salientou que o nacional de cuidados de saúde
sistemas, e a emissão de números de segurança social para
crianças, representam uma forma de acompanhar os movimentos de
as crianças, através de visitas a hospitais, escolas, etc. Talvez até mesmo
verificação aleatória de pontos em locais onde as crianças se reúnem (shoppings,
escolas, parques infantis, antros de ópio, etc.)
- crianças em tais lugares são presume-se que a menor
direitos, daí...
- isso poderia ser usado para rastrear crianças raptadas,

não-privativas de liberdade, pais, etc.
- isso poderia ser uma cunha na porta: como as crianças,os
o sistema já está em vigor para continuar o acompanhamento de
(sobre o direito calendário, também...iniciar o systme este
década e, em 2010 ou 2020, quase todo mundo vai ser em
ele)
- (Um verdadeiro paranóico gostaria de vincular essas idéias para a criança
fotos muitas escolas estão solicitando, muitos polícia local
os departamentos são oficialmente ajudando, etc. Um dossiê
a sociedade precisa tiros caneca em todos os perps.)
- Estas são todas as razões por que os governos continuam a empurrar
para sistemas de identidade e tentarão sabotar os esforços de
proporcionar o anonimato
+ De vigilância e Identificação do Pessoal
+ câmeras que podem reconhecer rostos são colocados em muitas
lugares públicos, por exemplo, aeroportos, portos de entrada, governo
edifícios
- e mesmo em alguns lugares privados, por exemplo, cassinos, lojas de
que tiveram problemas com determinados clientes, bancos
que cara roubos, etc.
+ "suspeitos movimentos detectores"
+ câmeras que rastreia os movimentos, a vadiagem, o contacto com os olhos
com outros clientes
+ redes neurais utilizadas para classificar behvaiors
- posição legal, não é necessária, já que esses sistemas são
usado apenas para acionar outros de vigilância, não
provar a culpa em um tribunal de lei
- exemplo: os bancos têm câmeras, em 1998, que podem
identificar possíveis assaltantes de banco
- câmera as imagens são enviadas para uma central de monitoramento
facilidade, de modo que o habitual manobra de parar o silêncio
o alarme não vai funcionar
- aeroportos e estações de trem (medos de terroristas),
outros lugares públicos
11.6.6. Telefones celulares são acompanhados por região...as pessoas estão ficando
chamadas de telefone como eles cruzam em novas zonas, "boas-vindas" - os
- mas isso implica que a sua posição já está sendo controlada
11.6.7. vindo de vigilância, Van Eck, a pirataria, vans
- Um interessante sinal do que está para vir é fornecida neste
conto de um membro da lista: "Na grã-Bretanha, temos um detector de TV
Vans'. Estas são para detectar licença evasores (você precisa pagar
uma licença anual para os canais da BBC). Eles são fornecidos
pelo Departamento do Comércio e Indústria. Eles usam algo

como uma pequena microônibus e usar Van Eck princípios. Eles têm
dois dirigível detectores de van telhado para que eles possam
triangular. Mas a TELEVISÃO tem lojas para notificar o Governo do
compradores - então, que é a forma básica em que a licença evasores
são detectados. ... Eu li de um caso de uma placa de boletim
onde alguém não ter uma TELEVISÃO, mas usado com um PC. Ele tem um
bater na porta. Eles disseram que ele parecia ter uma TELEVISÃO, mas
eles não podiam fazer o que canal ele estava assistindo!
[Martin Spellman, <mspellman@cix.compulink.co.uk>, 1994-
0703]
- Este tipo de vigilância é provável que se torne mais e mais
comum, umad levanta sérias questões sobre o que _other_
informações eles vão olhar para. Talvez a pirataria de software
os aplicadores (Software Publishers Association) vai olhar para
cópias ilegais do Microsoft Word ou do SimCity! (Esta área
precisa de mais discussão, obviamente.)
11.6.8. escutas
- deveria notificar as metas dentro do prazo de 90 dias, salvo se prorrogado
por um juiz
- Foreign Intelligence Surveillance Act dos casos, são isentos de
este (é provável que Cypherpunks interceptado, se eles
foram, para criptografia de atividades abrangidos por esta
caso " estrangeiros fronteiras sendo cruzados, a segurança nacional
implicações, etc. são todos os motivos plausíveis, sob a
Act)

11.7. Vigilância De Alvos
11.7.1. Coisas que o Governo Pode Monitor
- além de coisas óbvias como diplomática tráfego por cabo,
as chamadas telefónicas de e para pessoas suspeitas de serem terroristas e criminosos,
etc.
+ ligações entre os Congressistas e embaixadas estrangeiras
- reclamações no NYT (c. 9-19-91) que a CIA tinha arquivos no
Congressistas opostos auxílio Contras
+ Crescer lâmpadas para cultivo de maconha
- ataques hidropônico oferta de casas e apreensão de correspondência
listas
- registros de lançamentos de alt.drogas e alt.psicoativas
- vitamina compradores clubes
+ Consumo de energia
- para uso spot de crescer lâmpadas
+ mas também pode ser refinada a ponto estrangeiros ilegais sendo
abrigados ou qualquer outro consumo de energia doméstico

"inconsistente com relatados usa"
- o mesmo para a água, de esgoto, etc.
+ matérias dos produtos químicos
- como monitores de nitrato de amônio e outros bomba
materiais
- ou como matéria-prima para a produção de cocaína (lembre-se de vários
as apreensões de remessas de produtos químicos para a América latina)
- check-out de livros, a la FBI "Biblioteca de Programa de Conscientização"
de volta de 1986
- participação em conferências importantes, tais como Hackers Conferência
(poderia ter cenas envolvendo este), Segurança do Computador
Conferência
11.7.2. Inteligência económica (Espionagem em Empresas, Estrangeiras e
Doméstica)
+ "Não NSA uso da inteligência económica de dados obtidos em
intercepta?"
- Alguns de nós especulamos que isso é assim, que este tenha sido
acontecendo desde a década de 1960, pelo menos. Por exemplo, Bamford
observou, em 1982, que a ANS tinha a presciência dos planos
pelos Britânicos para desvalorizar a libra no final da década de 1970,
e o conhecimento de vários planos corporativos.
- A ANS autoriza códigos utilizados pela CIA, por isso parecem
impossível para a ANS não ter sabido CIA de drogas
o contrabando de atividades. A ANS é muito circunspecta,
no entanto, e raramente (ou nunca) comentários.
+ têm sido chamadas de o governo ajudar de alguma forma
Americana de negócios e a competitividade global por "nivelamento
o campo de jogo" através de espionagem
- especialmente como a ameaça do bloco Soviético
diminui e como a ameaça do Japão e
Alemanha aumenta
- os líderes da NSA e a CIA têm ainda falou abertamente sobre a
virando-se para a supervisão económica
+ Problemas com esta proposta:
- ilegal
- antiética
+ quem recebe a informação de inteligência? Não NSA só chamar
até a Apple e a dizer "Temos interceptado alguma mensagem de
Taiwan, que descrevem seus planos para as fábricas. São você
interessados?"
- situação dos EUA é diferente do Japão e da MITI (que
é frequentemente retratado como o modelo de como isso deve
de trabalho), em que temos muitas empresas com pouco ou nenhum

história da obediência às recomendações do governo
+ e países estrangeiros provavelmente vai aprender a esta espionagem
e tomar as medidas adequadas
- por exemplo, aumentando a criptografia de
11.7.3. Guerra contra as Drogas e a Lavagem de Dinheiro está Causando Aumento
De vigilância e Monitoramento
- controlo dos fluxos de capitais, as transacções em dinheiro, etc.
- cooperação com a Interpol, de governos estrangeiros, e até mesmo o
Soviéticos e a KGB (ou o que se torna um deles)
- novos sistemas de radar são de monitoramento de aeronaves ligeiras, barcos,
etc.

11.8. Questões Legais
11.8.1. "Meu chefe monitor de meu trabalho?" "Meu falência em 1980, a ser
usado para me negar um empréstimo?", etc.
- Libertários têm um conjunto diferente de respostas que fazer
muitos outros: a resposta para todas essas perguntas é principalmente
"sim," moralmente (desculpem a normativa de vista).
11.8.2. Tema: a proteção de alguns direitos, invasão de privacidade está a ser
justificado
- por exemplo, ao forçar o empregador registros para ser entregue, ou de
a apreensão de vídeo de aluguer de registros (em razão de captura
sexual deviants)
- diversas leis sobre o monitoramento do empregado
11.8.3. Governo cartões de IDENTIFICAÇÃO, capacidade de identidades falsas
- O governo usa seus poderes para se forjar credenciais, com
o conluio das principais agências de crédito (que, obviamente,
ver essas identidades falsas "pop para a existência full-blown."
- WitSec, FINCen, Identificações falsas, laços para empresas de cartão de crédito
- DEA picadas, Heidi, em La Jolla, Tava, falsas declarações, falsificação
banco de aplicativos, IDs falsos
- "acima de tudo" atitude é típica do que guarda...
os guardiões?
- WitSec, duplicidade
11.8.4. Legalidades da NSA vigilância
- leia Bamford, para alguns, por volta de 1982 poinra
- REINO UNIDO-EUA
- ECPA
- segurança nacional isenções
- muita confusão; no entanto, as leis nunca tive qualquer
influência real, e eu não posso imaginar a ANS está sendo processado!

11.9. Documentação e Bases de Dados

11.9.1. "O dossiê nunca esquece"
+ todas as transgressões de qualquer lei de qualquer país pode ser armazenado
indefinidamente, expondo o transgressor à prisão e
a detenção a qualquer momento ele entra em um país com um registro em
ele
- (Este veio com respeito aos ingleses, tendo singular
idéias sobre segurança do computador, pirataria e privacidade de dados;
é bem possível que um Americano passa através de
Londres poderia ser detido por alguma obscura violação anos
no passado.)
- o que é especialmente preocupante em uma sociedade na qual jurídica
códigos de preencher toda quartos e em que quase todos os dias
produz alguns violação de alguma lei
11.9.2. "O que sobre os problemas de privacidade com casa comercial, set-top
caixas, os anunciantes, e o NII?"
- Queremos que nossas preferências na pasta de dentes alimentados em bancos de dados
para que os anunciantes podem segmentar-nos? Ou que a nossa comida
compras de ser correlacionadas e analisadas pelo governo para
lugar violações da Dieta Lei de Saúde?
- Primeiro, as leis que dizer às pessoas o que registros são
"permitido" para manter estiver errado, de cabeça e levar a polícia
estado inspeções de unidades de disco, etc. Os chamados "Dados
Privacidade leis das diversas nações Europeias são um pesadelo.
Forte de criptografia torna-se discutível.
- Em segundo lugar, é principalmente para as pessoas para proteger o que eles querem
protegidos, não para aprovar leis exigindo que outros proteger
é para eles.
- Na prática, isso significa usar o dinheiro ou fazer
acordos com bancos e empresas de cartão de crédito que vai
proteger a privacidade. Determinar se eles têm ou não é outra
problema, mas várias ideias sugerem-se (John Gilmore
diz que muitas vezes ele se junta a grupos em variantes de seu nome, para
ver quem está vendendo o seu nome para listas de discussão.)
- Ausente quaisquer leis que proíbem a privacidade, a preservação da
empresas de cartão de crédito provavelmente primavera cima, se há um
a demanda do mercado. Dinheiro Digital é um exemplo. Outras variantes
abundam. Cypherpunks não deve permitir que tais alternativas para
ser banido, e claro que deve trabalhar em suas próprias tais
sistemas.
11.9.3. agências de crédito
- TRW Crédito, Transunion, Equifax
- links para WitSec
11.9.4. venda de bases de dados, ligação de registos...

- vários estados têm admitido a venda de seu motorista
licença de bases de dados

11.10. Polícia Estados e Informantes
11.10.1. A polícia afirma precisar de uma sensação de terror para ajudar a ampliar a
o poder e o estado, uma espécie de "shrechlichkeit," como os Nazistas
usado para chamá-lo. E muitos informantes. Polícia estados necessidade
disposto cúmplices voltar-se para seus vizinhos, ou até mesmo a sua
os pais, tão pouco Pavel Morozov se tornou um Herói do
Povo soviético, pelo envio de seus pais para a sua morte em
Stalin campos de trabalho para o crime de expressar negativo
opiniões sobre o glorioso Estado.
- (A canonização de Pavel Morozov, recentemente, foi repudiado
por russa atual líderes--talvez até mesmo pela tarde-Soviética
era leades, como Gorbachev-que apontou a corrosivo
efeitos de incentivar as famílias a narc em cada
outros...algo que os EUA têm esquecido...será que vai ser 50
anos antes de nossos líderes admitir que ter filhos virar
Daddy para a utilização ilegal "crypto" não foi uma boa idéia?)
11.10.2. As crianças são incentivadas no âmbito federal com mandato de D. A. R. E.
programas para se tornar Junior Narcóticos, narcing seus pais para
os policiais e conselheiros que entram em suas escolas.
11.10.3. O BATF tem uma linha gratuita (800-ATF-ARMAS) para snitching no
vizinhos que se pensa que estão a violar as leis federais de armas.
(Os relatórios são este é backfiring, como proprietários de armas de chamar a
número do relatório de locais de políticos liberais e arma-
ladrões.)
11.10.4. Alguns o país em que vivemos, hein? (Desculpas para não-EUA leitores,
como sempre.)
11.10.5. As implicações para o uso de criptografia, para não confiar nos outros,
etc., são claros
11.10.6. Perigos de informantes
+ mais da metade de todos os IRS processos surgem de dicas de
cônjuges e ex-cônjuges...eles têm dentro de drogas, o
motivo, e os meios
- um pensamento preocupante, mesmo na era da criptografia
+ EUA está aumentando a uma sociedade de narcóticos e fezes
pombos, com "CIs" (informantes confidenciais), protegido
testemunhas (com falsas Identificações e luxuosos estilos de vida), e com
todos os tipos de vagas de ameaças e promessas
- em um sistema com dezenas de milhares de leis, quase todos os
comportamento quebras de, pelo menos, algumas leis que, muitas vezes, inevitavelmente,
e, portanto, uma poderosa espada que paira sobre todos de cabeça

- corrosão de confiança, especialmente no seio da família (DARE
programa nas escolas incentiva as crianças a narc em seus
os pais que são "toxicodependentes"!)

11.11. As Leis De Privacidade

11.11.1. Será proposto leis de privacidade de ter um efeito?
+ Eu suspeito que é exatamente o oposto: o emaranhado de leis-parte
da totalitário freezeout-vai "marginalizar" mais
as pessoas e levá-los a buscar formas de proteger a sua própria
a privacidade e proteger-se de sanções sobre a sua
ações
+ liberdade de expressão vs. delitos, SLAPP ternos, sedição, encargos,
ilegal de investigação, etc.
- a liberdade de expressão é desaparecendo sob uma torrente de leis,
os requisitos de licenciamento, e até mesmo regras de zoneamento
+ proibição de trabalho sobre medicamentos, procedimentos médicos, etc.
- contra o direito de divulgar informações sobre o uso de drogas
(MDMA caso em Stanford), em determinados tipos de nascimento
controle
- "Se encrytion é ilegal, apenas bandidos terão
criptografia."
+ as leis de privacidade, já estão causando criptografia ("arquivo
de proteção"), que será obrigatório em muitos casos, como com médicos
registros, a transmissão de ficheiros sensíveis, etc.
- por si só isto não está em conflito com o governo
requisito para tappable acesso, mas a prática
implementação de um sistema de dois níveis-seguro contra
civil seringueiros, mas legível nacional de segurança
seringueiros-é um pesadelo e que é provavelmente impossível
alcançar

11.11.2. "Por que coisas como as "Leis de Privacidade de Dados" tão ruim?"
- A maioria dos países Europeus têm leis que limitam a coleção
de registos informáticos, dossiers, etc., exceto para
aprovado usa (e os próprios governos e seus
agentes).
- Os americanos têm leis. Eu já ouvi chamadas para isso,
o que eu acho que é muito ruim.
- Não gosto da idéia de outras pessoas a compilação de dossiês
em nós, parando eles, é ainda pior situação. Dá
o estado o poder para entrar em empresas, casas, e examinar
computadores (outra coisa que é completamente inaplicável). Ele cria
ridícula situações em que, digamos, alguém fazendo-se uma
informatizado lista dos seus contactos do telefone está compilando uma

ilegal banco de dados! Isso faz com que o e-mail de um crime (os registros
que são mantidas).
- eles próprios são grandes invasões de privacidade
- você vai me colocar na cadeia, porque eu tenho bases de dados
de e-mail, Usenet posts, etc.?
- Na minha opinião, os defensores da "privacidade" são muitas vezes confundidos
sobre este problema, e não conseguem perceber que as leis sobre
privacidade, muitas vezes, tirar os direitos de privacidade de _others_.
(Direitos raramente estão em conflito--contrato plus self-privacidade
cuidar de 99% das situações em que direitos são alegado
para estar em conflito.)

11.11.3. sobre as diversas "leis de privacidade de dados"

- muitos países adotaram essas leis de privacidade de dados,
envolvendo restrições sobre os registros que podem ser mantidos, a
o registro de coisas como listas de discussão, e pesado
sanções para aqueles que se encontram manter arquivos de computador considerado
impermissable
- isso leva a invasões de privacidade....esta muito Cypherpunks
lista teria que ser "aprovado" por um burocrata em muitos
países...o oportunites (e inevitabilidades) de abuso
são óbvias
- Existe uma central de contradição a ser executado através de
dabase regulamentos propostos por muitos chamados "privacidade
os defensores". Para ser aplicável eles requerem enormes
governo snooping em atividades de banco de dados em nosso
workstatins e PCs, especialmente as atividades de muitos
de pequeno em casa de empresas (tais como lista de discussão
empresários que muitas vezes trabalham fora de casa).

"Assim, o resultado desses chamados "privacidade" regulamentos
é destruir a nossa última pedaços de privacidade contra
governo, e acalmar-nos em cegamente deixando ainda mais de
os detalhes de nossa vida pessoal em mainframes de
as principais agências governamentais e relatórios de crédito
agenices, que se eles não são explicitamente excluídos da
as leis de privacidade (como é comum) pode simplesmente evitá-los usando
ventos havesn mútua, de acordos com os
os investigadores, a polícia e as agências de inteligência." [Jim
Hart, 1994-09-08]

11.11.4. "O que Cypherpunks pensar sobre isso?"

+ dividido mente...enquanto ninguém gosta de ser monitorado, o
questão é o quão longe se pode ir para impedir que outros sejam
monitorado

- "Leis de Privacidade de dados" como um mau exemplo: calcam liberdade para escrever, a fim de manter um computador privado

11.11.5. Afirmações a bases de dados precisa ser verificada (de crédito, reputação, quem disse o quê, etc.)

- se eu simplesmente afirmar que o zé não é empregado, e esta espalha...

11.12. Nacional de IDENTIFICAÇÃO de Sistemas

11.12.1. "Os cartões de IDENTIFICAÇÃO são apenas licenças do motorista no Auto-Estrada Da Informação." [desconhecido...pode ter sido o meu cunhar]

11.12.2. "Qual é a preocupação?"

11.12.3. Seguro e Nacionais de Cuidados de Saúde irá Produzir o "Nacional ID" que vai ser Quase Imprescindível

- os hospitais e os médicos terão de ter o cartão de dinheiro... os pagamentos serão evocar suspeita e pode mesmo não ser viável

11.12.4. Cartão de IDENTIFICAÇÃO nacional Argumentos

- "trabalhador permitir" (outra proposta, 1994-08, que seria chamada para o cartão nacional de autorizar a permissão de trabalho)
- imigração, o benefício
- possível de tie-in para o sistema que está sendo proposto pelos EUA Serviço Postal: um registro de chaves públicas (será que eles também "a questão" o público-privada do par de chaves?)
- chave de software de custódia e idéias relacionados
- "Eu duvido que um só têm de "flash" o seu cartão e estar no seu caminho. Mais corretamente, seria necessário enviar para ser "escaneados" e estar no seu caminho. Este seria também servir a ser um convenientes localizador de marca se instalou no sistemas de portagens e de diversos "pontos de verificação de segurança". Por seria alguém que não tem nada a esconder cuidado se a cada movimento que pode ser monitorados? O seu para o seu próprio bem, certo? Muito logo deslizando o seu ID nos slots em everyplace que você for lá vai ser comum." [Korac MacArthur, comp.org.fep.falar, 1994-07-25]

11.12.5. "O que são algumas preocupações acerca do Universal de Cartões de IDENTIFICAÇÃO?"

- "Papierren, bitte! Schnell!
- que iriam permitir a rastreabilidade para o max (como a gente costumava dizer)... de rastreamento de movimentos, a erosão da privacidade
- de que seria necessário para ser usado para o setor bancário transações, acesso à rede, etc. (Como de costume, não pode ser soluções alternativas, hacks, ...)
- "é-uma-pessoa" credentially, onde o governo se mete

na emissão de chaves criptográficas (a la USPS
proposta), onde apenas "aprovado usa" são permitidos, etc.
- carimbos de data / hora, credenciais
11.12.6. Serviço Postal de avaliação de balão para cartão de IDENTIFICAÇÃO nacional
- "É verdade que eles compartilham a tecnologia, sua intenção
e o propósito é muito diferente. Chaum a proposta tem como
a intenção e o objetivo de prover e proteger o anonimato, em
operações financeiras. A intenção e a finalidade dos EUA
Serviço Postal é identificar e autenticar para o
o governo e para garantir a rastreabilidade de todos os
operações financeiras." [WHMurray, alt.privacidade, 1994-07-
04]
11.12.7. Cenário para a introdução de cartões de IDENTIFICAÇÃO nacional
- Imagine que o veículo inscrições exigem a apresentação de
este cartão (tenho os imigrantes ilegais para fora de seus carros, ou,
mais amigavelmente, a burocracia faz simplesmente a IDENTIFICAÇÃO de carros
parte do processo).
- Instantaneamente isso faz com que aqueles que se recusam a obter um cartão de
IDENTIFICAÇÃO
não é possível obter licença válida tags. (Aplicação já está
muito bom....Eu era mais puxado de um par de vezes para
quer esquecer de colocar o meu novo adesivos, ou para a condução de
com o Oregon expirado tags.
+ O "Nacional, Cartão de Benefícios", por exemplo, é então necessário
para obter placa de licença tags.e talvez outras coisas, como o carro
e seguro de casa, etc. Seria muito difícil para
lutar contra esse cartão, como não poderia unidade, não poderia pagar
impostos ("Awhh!" Eu ouvi você dizer, mas considere as penalidades,
o tie-ins com os empregadores, etc. Você pode executar, mas você não pode
ocultar.)
- o cartão de IDENTIFICAÇÃO nacional seria, presumivelmente, ser amarrado para
imposto de renda arquivamentos, de várias maneiras, eu não entrarei em detalhes aqui.
O Serviço Postal, com o objetivo de entrar para esta área,eu acho,
criou a idéia de petição eletrônica, sistemas de IDENTIFICAÇÃO,
etc.
11.12.8. Comentários sobre cartões de IDENTIFICAÇÃO nacional
- De que algumas pessoas vão ser capazes de saia de um sistema, ou que
o sistema irá, em última análise, ser inaplicável, não
diminuir a preocupação. As coisas podem ficar muito dura no
entretanto.
- Vejo grandes perigos aqui, em amarrar um cartão de IDENTIFICAÇÃO nacional para
transações somos essencialmente incapazes de evitar neste
sociedade: condução, seguro (e não vamos discutir

o seguro...o que eu quis dizer é inevitável no sentido de legal
questões, delitos, etc.), passagens de fronteira, etc. Agora, como vai
um arquivo impostos sem um cartão de memória, se é tornado obrigatório
para interações com o governo? Dizendo: "os impostos não são
colecionáveis" não é uma resposta adequada. Eles podem não ser
colecionáveis para street punks e outros que habitam o
economia subterrânea, mas com certeza eles são para a maioria de nós.

11.13. Sistema Nacional De Saúde Questões
11.13.1. Seguro e Nacionais de Cuidados de Saúde irá Produzir o "Nacional
ID" que vai ser Quase Imprescindível
- os hospitais e os médicos terão de ter o cartão de dinheiro...
os pagamentos serão evocar suspeita e pode mesmo não ser viável
11.13.2. Estou menos preocupado com o farmacêutico irá me add para alguns
banco de dados, ele mantém que o meu médico vai ser instruído para
compilar um dossiê para os padrões do governo e, em seguida, zip-lo fora
sobre o Infobahn para as autoridades.
11.13.3. Perigos e problemas do Plano Nacional de Saúde
- rastreamento de cartão de IDENTIFICAÇÃO nacional
- "Se você acha que o BATF é ruim, espere até que o BHCRCE vai
em ação. "O que é o BHCRCE?", você pergunta. Por isso, é o
Burea de Reforma dos Cuidados de Saúde Imposição de Conformidade - o
BATF, FBI, FDA, CIA, IRS, tudo em um." [Dave
Feustel, falar.política.armas, 1994-08-19]
- Bill Stewart apontou os perigos das crianças
números de segurança social, de sistemas de rastreamento nas escolas e
hospitais, etc.

11.14. Credenciais
11.14.1. Este é um dos mais esquecidos e ignorados aspectos de
criptologia, especialmente de Chaum de trabalho. E ninguém no
Cypherpunks ou em qualquer outro lugar é atualmente trabalhando em "cegos
credenciais" para o uso diário.
11.14.2. "É uma prova de identidade é necessário?"
- Esta questão é debatida um monte, e é importante. Falar de um
cartão de IDENTIFICAÇÃO nacional (o que sacode chamada de um "passaporte interno") é
no ar, como parte dos cuidados de saúde, bem-estar, e
legislação sobre imigração. Mercados electrónicos fazer isso também
um problema para o ATM/smart card comunidade. Este é também
intimamente ligada com a natureza do anônimo reamailers
(onde a identidade física é, claro, geralmente faltam).
+ Primeiro, "identidade" pode significar coisas diferentes:
- Visão convencional de Identidade: pessoa Física, com

data de nascimento, características físicas, impressões digitais, social
números de segurança, passaportes, etc.--toda a nuvem de
"identidade" itens. (Biométricos.)
- Pseudônimo de Vista da Identidade: Persistente personnas,
mediada com criptografia. "Você é a sua chave."
- A maioria de nós lidar com a identidade como uma mistura desses modos de exibição: nós
raramente verificação biométrica credenciais, mas contamos, também, com
física pistas (voz, aparência, etc.). Eu suponho que
quando eu estou a falar "Duncan Frissell," quem eu nunca
conheci em pessoa, o que ele é, de fato, Duncan Frissell. (Alguns
fazer o salto a partir desta expectativa para querendo que o
governo impor esta afirmação, que é, desde I. D.)
+ É frequentemente afirmado que a identidade física é importante na
para:
- acompanhar os trapaceiros, welchers, contrato breakes, etc.
- permitir que algumas pessoas a se envolver em algumas transações, e
proibir que outros (idade credenciais, para beber, para
exemplo, ou---menos amigavelmente--autorizações de trabalho em algum campo)
- tributação, direito de voto, outros esquemas vinculados à física
existência
+ Mas a maioria de nós realizar negócios com pessoas sem nunca
verificar as suas credenciais de identidade...principalmente seus
a notícia de que eles são "Bill Stewart" ou "Scott Collins," e
nós nunca ir além.
- isso pode mudar como credenciais digitais proliferam e
como interações causam verificações automáticas para ser feita (um
razão pela qual muitos de nós temos para oferecer suporte a Chaum do "cego
as credenciais de" idéia-sem criptografia proteções, nós vamos
ser constantemente controladas em todas as interações).
+ Um princípio orientador: Deixar esta questão de se
a demanda física credenciais de IDENTIFICAÇÃO até o *festas
envolvidos*. Se Alice quer ver Bob "é-uma-pessoa"
credencial, e tomar o seu palmprint, ou seja o que for, que é uma
problema para eles trabalharem fora. Eu não vejo nenhuma razão moral, e
certamente, não é comum razão, pessoas de fora para interferir
e insistir para que a IDENTIFICAÇÃO seja produzido (ou que a IDENTIFICAÇÃO seja proibido,
talvez como uma espécie de "violação de direitos civis"). Depois de
todos, nós interagir no ciberespaço, no Cypherpunks lista,
sem qualquer controle externo sobre a identidade.
- e os contratos comerciais são melhores negociado localmente, com
externo de aplicação da contratada pelas partes (privada-
produzido lei, visto já com as companhias de seguros,
colagem de agentes de arbitragem, arranjos, etc.)

- Praticamente falando, i.é., não normativamente falando,
as pessoas vão encontrar maneiras de contornar sistemas de identidade. Dinheiro é um
forma, remetentes são outra. A imposição de uma rígida identidade-
baseado no sistema é difícil.
11.14.3. "Não precisamos de "é-uma-pessoa" credenciais para coisas como votos
na Net?"
- Que é, qualquer sysadmin pode facilmente criar quantas usuário
contas de como ele quer. E os usuários finais podem se inscrever com
vários serviços sob vários nomes. A preocupação é que
este estilo de Chicago voto (fictícia de pessoas) pode ser utilizado
a inclinação votos na Usenet.
- Preocupações semelhantes surgir em outros lugares.
- Na minha opinião, este é um poderoso motivo trivial para o suporte "é-
uma pessoa" credenciais.
11.14.4. Localidade, credenciais, validações
+ Considere as implicações de privacidade de algo tão simples como
um lote de estacionamento do sistema. Duas abordagens principais:
- Primeira Abordagem. Pagamento em dinheiro. Carro entra muito, o motorista paga
dinheiro, uma "validação" é dada. Não há rastreabilidade existe.
(Há uma pequena chance de que um condutor pode dar a sua
adesivo para um novo controlador, e, assim, enganar o estacionamento
muito. Este tende a não acontecer, devido aos inconvenientes
de formação de um mercado em tais adesivos (coordenação com
outro carro, etc.) e porque o adesivo é relativamente
baratos.)
- Segunda Abordagem. Faturamento de motorista, registro de licença
placas. A rastreabilidade está presente, especialmente se o local
parque de estacionamento, está vinculado a empresas de cartão de crédito, DMV,
a polícia, etc. (estas link-ups estão na lista de desejo de
as agências de polícia, para "congelamento" fugitivos, criança
suporte delinqüentes, e outros criminosos.
- Estas são as preocupações de uma sociedade com um monte de
de pagamentos eletrônicos, mas sem mecanismos para a preservação
privacidade. (E atualmente não há grande demanda para esta
tipo de privacidade, para uma variedade de razões, e este
reduz a pressão para anônimo credencial de métodos).
- Uma propriedade importante do verdadeiro dinheiro (ouro, notas de banco que
são bem confiáveis) é que ele se instala imediatamente, exigindo
não há tempo de vinculação de contratos (capacidade para rastrear o
pagador e coletar em uma transação inválida)

11.15. Registros de todos anúncios na UseNet
11.15.1. (idem para CompuServe, Gênio, etc.) vai existir

11.15.2. "Que tipos de monitoramento da rede é possível?"
- Arquivos de todos tráfego Usenet. Isso já é feito por
comercial CD-ROm fornecedores, e outros, de modo que este seria
trivial para várias agências.
- Arquivos de e-Mail. Mais problemático, como e-mail é ostensivamente não
público. Mas o correio passa através de muitos sites, geralmente em
o formulário não criptografado.
- Análise de tráfego. Ligações monitoradas. Telnet, ftp, e-
mail, Mosaid, e outras conexões.
- Filtrada exames de tráfego, com a palavra-chave de correspondência de texto armazenadas
nos arquivos.
11.15.3. Registros: observação de que as empresas privadas podem fazer a mesma coisa,
exceto que vários "direito à privacidade" leis pode tentar
interferir com este
- o que faz com que o seu próprio constitucional problemas de privacidade, de
curso
11.15.4. "Como você pode esperar que algo que você enviou na UseNet para
vários milhares de sites não serão potencialmente realizada contra
você? Você desistiu de qualquer pretensão de privacidade, quando você transmissão
as suas opiniões-e até mesmo declarações detalhadas de seu
atividades para um público de milhões de pessoas. Você realmente acha que
que estas mensagens públicas não estavam sendo arquivados? Qualquer
cidadão, iria encontrá-lo em quase direta para classificar
uma merreca de vários megabytes um dia por palavras-chave, nomes de
cartazes, etc." [Eu não tenho certeza se eu escrevi isso, ou se alguém
outra coisa que eu esqueci de fazer uma observação de did]
11.15.5. este problema já está chegando: um gay programador que foi
demitidos discutiu sua raiva em um dos gays tábuas e disse:
ele estava pensando em ligar em seu ex-empregador para
generalizada cópia do software Autocad...um funcionário da Autodesk
respondeu com "Você acabou de fazer!"
11.15.6. as empresas podem usar o GREP e Em Localização, como ferramentas para
pesquisa redes públicas de qualquer debate de si mesmo ou de seus
produtos
- por boca grande empregados, clientes insatisfeitos, conhecido por
os críticos, etc.
- mesmo comentários positivos que podem ser utilizados na publicidade
(sujeitos a várias leis)
11.15.7. 100% de rastreabilidade do público em postagens na UseNet e outros
bbs é muito cercear a liberdade de expressão e
torna-se uma das principais justificativas para o uso de
anónimo (ou pseudononymous) e placas de redes
- não podem ser chamadas de leis contra a compilação, como

com o Britânico de dados de leis, mas, basicamente, há pouco
o que pode ser feito quando as postagens ir para dezenas de milhares de
máquinas e são arquivados em perpetuidade, por muitos, de esses
nós e pelos milhares de leitores
- os leitores que podem incorporar o material em suas próprias
lançamentos, etc. (daí o absurdo da lei Britânica)

11.16. Efeitos de Vigilância sobre a Propagação da Criptografia
11.16.1. A vigilância e o monitoramento servirá para aumentar o uso de
criptografia, em primeiro lugar, as pessoas com algo a esconder, e
em seguida, por outros
- um efeito bola de neve
- e várias agências do governo-se usar
criptografia para proteger seus arquivos e seus arquivos de privacidade
11.16.2. para os cargos sensíveis, a disponibilidade de novas
outros métodos de acelerar a conversão para seguro
sistemas baseados em criptografados de telecomunicações e o
prevenção de voz baseado em sistemas de
11.16.3. Vigilância Tendências
+ Tecnologia está a tornar cidadão-unidade de vigilância mais e
mais trivial
+ câmeras de vídeo em todos os cantos da rua são tecnologicamente
fácil de implementar, por exemplo
- ou câmeras em lojas, em aeroportos, em outras públicos
lugares
- o tráfego de câmeras
- rastreamento de compras com cartões de crédito, carteira de
de licenças, etc.
- monitoramento de computador emissões (a TEMPESTADE de problemas, muitas vezes um
questão de paranóico especulação)
+ interceptação da Net...escuta telefônica, interceptação de
sem criptografia de comunicações, etc.
- e elaboração do dossier entradas com base em público
lançamentos
+ Tudo isso faz com que os esforços no sentido de uma pessoa de acompanhamento,
credenciais sociedade mais urgente.
Monkeywrenching, sabotagem, educação pública, e
desenvolvimento de alternativas são necessários.
- Se a fiscalização do estado cresce tão rapidamente como agora
parece estar fazendo, mais medidas desesperadas podem ser
necessário. Pessoalmente, eu não iria chorar se
Washington, D.C. e seus arredores tem eletrocutado com um terrorista
nuke; os inocentes devem ser substituídas com rapidez suficiente, e

a morte de tantos políticos ghouls certamente seria
a pena. A destruição da Babilônia.
+ Precisamos receber a mensagem sobre "cegos " credenciais"
(o que pode mostrar algum campo, como a idade, sem mostrar tudo
campos, incluindo o nome e tal) lá fora. Mais
radicalmente, precisamos fazer com que as pessoas a questionar o porquê de
as credenciais são tão importantes como muitas pessoas parecem
pensar.
- Eu defendo que as credenciais são raramente necessários para mutuamente
acordadas as transações

11.17. Pontas Soltas
11.17.1. USPS envolvimento no correio eletrônico, assinaturas,
autenticação (proposto em julho-agosto de 1994)
+ Vantagens:
- vários locais
- uma missão já orientada para a entrega
+ Desvantagens:
- tem realizado muito, comparado ao permitido compettion
(Federal Express, UPS, Aéreos, etc.)
- é vinculada ao governo (agora quase independentes, mas
não realmente)
- poderia tornar-se obrigatória, ou restrito a concorrência
determinados nichos (como com o pacote de serviços, que
não pode ter "rotas", e não estão autorizados a competir em
o barato letra de regime)
- um grande e embruteceu a burocracia, com a união de mão de obra
- Links para outros programas (software key escrow, Digital
Telefonia) não é clara, mas parece provável que um quase-
governo de agência como o USPS seria cooperativo com
governo, e gostaria de colocar limites nos sistemas de criptografia
permitido.
11.17.2. as ameaças de morte
+ NSA oficial ameaçou Jim Bidzos morto se ele
não alterar a sua posição sobre alguma negociação em andamento.
Isso foi relatado no jornal, e eu procurei
confirmação:
- "Tudo relatado no Merc Notícia é verdadeira. Eu sou
certos de que ele wasnot falando para a agência, mas quando
isso aconteceu foi muito grave, pelo menos, parecia
estar. Houve um longo silêncio depois que ele fez a ameaça,
com um concurso de encarar. Ele foi muito intensa.

"Eu o respeito e a confiança nos outros dois que estavam no quarto de
(eles ficaram chocados e, literalmente, sem palavras, olhando para
suas voltas) e plano para pedir a ANS, por escrito, pedido de desculpas e
a confirmação de que ele não estava falando para a agência.
Vamos ver se eu entendi. Se o incidente fez
seus relatórios de viagem, eu tenho uma chance de conseguir uma carta."
[jim@RSA.COM (Jim Bidzos), comunicação pessoal, publicado
com a permissão para falar.política.crypto, 1994-06-28]

11.17.3. Identidades falsas...não pode ser "apagado" do computador
bancos de memória. A teia de associações, implicações, regra
disparos...tudo isso significa que a simples remoção (ou a inserção de um
falsa identidade) produz descontinuidades, ilógico
a evolução, buracos...a história não é facilmente alterado.

12. Dinheiro Digital e Net Comércio

12.1. direitos autorais

12.2. RESUMO: Dinheiro Digital e Net Comércio

12.2.1. Pontos Principais

- forte de criptografia faz com que certas formas de dinheiro digital possível
- David Chaum é, mais uma vez, centralmente envolvidos
- não real sistemas implantados, apenas pequenos experimentos
- o legal e regulamentar emaranhado vai afetar
implantação em formas grandes (fazer um "lançamento" de dinheiro digital
um notrivial o assunto)

12.2.2. Ligações para Outras Secções

- reputação
- situação jurídica
- crypto anarquia

12.2.3. Onde Encontrar Informações Adicionais

- http://digicash.support.nl/

12.2.4. Diversos Comentários

- uma área enorme, cheio de termos especiais
- muitos instrumentos financeiros
- a teoria do dinheiro digital não é completa, e a confusão
abunda
- esta seção é também mais desorganizado e confuso do que eu

como; eu vou limpá-lo em fufure lançamentos.

12.3. A Natureza do Dinheiro
12.3.1. A natureza do dinheiro, da banca e das finanças, é um tema que
perpassa a maioria das discussões de dinheiro digital. Surpreendente.
Mas também uma área que está ainda mais detalhado do que é criptografia.
E interminável confusão de termos, semântica quibblings no
lista, e assim por diante. Eu não me dedicando muito espaço para tentar
explique economia, administração, e a profunda natureza ou dinheiro.
12.3.2. Há, claro, muitas formas de dinheiro de hoje (estes
os termos não são equivalentes...)
+ moedas, contas (que se presume ser difícil forjar)
- "ontológica leis de conservação"--o dinheiro não pode estar em
dois lugares de uma só vez, não pode ser o dobro gasto
- isso é apenas parcialmente verdadeiro, e a falsificação de tecnologia é
tornando discutível
- obrigações ao portador e outros "imediatamente numerário" instrumentos de
- diamantes, ouro, obras de arte, etc. ("portable riqueza")
12.3.3. Muitas formas de dinheiro digital. Assim como existem dezenas de
as principais formas de instrumentos, assim também haverá muitas formas
de dinheiro digital. Nichos será preenchido.
12.3.4. A natureza profunda do dinheiro é claro para mim. Há dias
quando eu acho que é apenas um gigante con jogo, com o valor em dinheiro
só porque os outros vão aceitá-lo. Nos outros dias, quando eu acho
é um pouco amarrado para "coisas reais" como o ouro e a prata. E
nos outros dias, quando eu estou despreocupado (desde que eu o tenho,
e funciona).
12.3.5. O dinheiro digital discussões da mesma forma confusa pela
ideias diferentes sobre o dinheiro. Dinheiro Digital não é necessariamente um
forma de _currency_, mas em vez disso, é um mecanismo de transferência. Mais
como um "digital de seleção," na verdade (apesar de que ele pode dar origem a
novas moedas, ou para uso mais amplo de outros já existentes
moeda...em algum momento, pode tornar-se indistinguível
a partir de uma moeda).
12.3.6. Eu aconselho que as pessoas não se preocupar excessivamente muito sobre o
verdadeiro e
natureza profunda de dinheiro, e em vez de pensar sobre o dinheiro digital como
um protocolo de transferência de alguns underlyng forma de dinheiro, que
pode ser moedas de ouro ou francos Suíços, ou galinhas, ou mesmo
gigante de pedra rodas.
12.3.7. Princípio vs. Propriedades de Dinheiro
- Física de moedas, como o dinheiro, tem certas propriedades básicas:
difíceis de serem falsificados, inútil contrafacção se fez

de ouro ou de prata, fungibilidade, assentamento imediato (não há necessidade
limpar com um distantes banco, sem atrasos, etc.),
untraceability, etc.
- Dinheiro Digital, em vários sabores, tem drasticamente
propriedades diferentes, por exemplo, pode exigir que a compensação, a qualquer
único digtital nota é infinitamente copiáveis, pode permitir
rastreabilidade, etc. Uma complicada mistura de propriedades.
+ Mas por que é físico dinheiro (espécie) do jeito que é? O que
propriedades da conta para isso? Quais são os princípios fundamentais
que implicam essas propriedades?
- hardware (espécie como o ouro) vs. software (bits, prontamente
copiáveis)
- immediale, local de compensação, por causa da fé racional que
o dinheiro irá limpar
- limites de taxa de transferência de física dinheiro por tamanho,
peso do dinheiro, considerando que "fraude eletrônica" e as variantes
de drenagem de uma conta em segundos
- A minha idéia é que nós gastamos muito tempo pensando sobre o
principles (tais como localidade, transitividade, etc.) e
esperar para, em seguida, _derive_ as propriedades. Talvez precisamos
em vez disso, focar no _objects_, os conjuntos de protocolo-
derivada coisas, e examinar suas propriedades emergentes. (Eu
tenho meu próprio pensamento ao longo destas linhas, envolvendo "protocolo de
ecologias" em que os agentes de bang uns contra os outros, a la
Doug Lenat velha "Eurisko" do sistema, e assim descobrir
fracos, pontos de força, e até mesmo são geneticamente
programada para adicionar novos métodos que aumentam a segurança.
Isso, como você pode imaginar, é um longo prazo, especulativo
projeto.)
12.3.8. "Pode uma "moeda digital" ser feito?"
- A resposta parece ser "não"
+ Software é infinitamente copiáveis, o que significa um software
representação digital de dinheiro poderia ser replicada em muitos
vezes
- isto não é para dizer que ele poderia ser _spent_ muitas vezes,
dependendo do processo de limpar...mas isso não é
uma "moeda", no sentido que dizer
- O Software é trivialmente replicável, ao contrário de ouro ou de prata
moedas, ou até mesmo papel moeda. Se e quando o papel moeda
torna-se trivialmente replicável (cor e copiadoras quase
lá chegado), espera que a mudança da natureza do dinheiro.
(Especulação: o dinheiro será substituído por cartões inteligentes,
provavelmente não é do anonymous ordenar nós somos a favor.)

+ bits podem sempre ser duplicado (a menos ligadas a hardware, como
com TRMs), então deve procurar em outro lugar
+ poderia amarrar os bits para um local específico, para que
a duplicação seria óbvio ou inútil
- a ideia é que vagamente que um agente pode ser colocado em
alguns localização...duplicações seria detectável
e irrelevantes (mesmo bits, o mesmo comportamento, unmodifiable
porque a assinatura digital)
- (este é formalmente similar à idéia de um agente ativo
que é unforgeable, no sentido de que o agente ou de uma moeda
"standalone")
12.3.9. "O que é a "granularidade" da digital de dinheiro?"
+ fina granularidade, ou seja, sub-cento quantidades
- útil para muitas transações on-line
- dentro de computadores
- o suplemento de taxas por interemediaries
- muito pequenas compras
+ média de granularidade
- alguns centavos, até um dólar (por exemplo)
- também útil para muitas pequenas compras
- fechar equivalente a "loose change", ou pequenas notas, e
provavelmente útil para os mesmos fins
- portagens, taxas, etc.
- Isso é aproximadamente o nível de muitos DigiCash protocolos são
visa
+ de grande granularidade
- vários dólares
- mais como um "convencional" de transações on-line
-
- os custos de transação são cruciais; online vs. offline
compensação
- Digital Silk Road é uma proposta por Dean Tribble e Norma
Hardy para reduzir os custos de transacção
12.3.10. O Debate sobre dinheiro e finanças fica complicado
- termos legais, contabilístico, gíria, etc.
- Eu não vou aventurar nesse mato aqui. É uma especialidade
por si só, com várias dezenas de tipos principais de instrumentos de
e derivados. E, claro, com grandes doses de lei.

12.4. Cartões Inteligentes
12.4.1. "O que são cartões inteligentes e como eles são usados?"
+ Mais cartões inteligentes como eles agora existem estão muito longe de ser
anônimo digital de caixa de principal interesse para nós. No

de fato, a maioria deles são apenas glorificado cartões de crédito.
- com nenhum ganho para os consumidores, uma vez que consome normalmente não paga para perdas por fraude
- (de modo a atrair consome, eles te oferecem incentivos?)
- Podem ser pequenos computadores, normalmente de crédito-cartão de tamanho, ou apenas cartões de controle de acesso através de computadores locais.
+ Inviolável módulos, por exemplo, se adulterados, eles destruir os dados importantes, ou pelo menos, dar provas de depois de ter sido adulterado.
+ De segurança de fabricação
- alguma variante de "cortar-e-escolha" de inspeção de instalações
+ Utiliza de cartões inteligentes
- cartão de crédito convencionais usa
- pagamento de contas postagem
- ponte e as portagens
- pagamentos para os itens recebidos eletronicamente (não necessariamente anonimamente)

12.4.2. Visto Bolsa Eletrônica

12.4.3. Mondex

12.5. David Chaum do "DigiCash"

12.5.1. "Por Chaum, tão importante para a digital de dinheiro?"
- Chaum nome aparece com freqüência neste documento, e em outros Cypherpunk escritos. Ele é sem dúvida o seminal pensador nesta área, tendo sido muito quase o primeiro a escrever sobre várias áreas: untraceable e-mail, dinheiro digital, cegueira, unlinkable credenciais, DC-redes, etc.
- Eu falei-lhe de 1988 "Crypto" conferência, dizendo-lhe: sobre os meus interesses, minha 'labirinto' idéia para o correio de encaminhamento de (que ele tinha previsto, em 1981, sem o conhecimento de mim no tempo), e algumas dicas sobre "crypto anarquia." Ficou claro para mim que Chaum tinha pensado longa e profundamente sobre estes questões.
- Chaum de artigos deve ser lido por todos os interessados neste a área. (Não, seus trabalhos são _not_ "em-linha". Por favor, consulte a "Crypto" Procedimentos e materiais relacionados.)
- [DIGICASH comunicado de IMPRENSA, "primeiro do Mundo em caixa eletrônico pagamento através de redes de computadores," 1994-05-27]

12.5.2. "Qual é a sua motivação?"
- Chaum parece ser um libertário, pelo menos no social

problemas, e está muito preocupado com o "Grande Irmão" tipos de
preocupações (lembre-se que o título de um dos seus 1985 MCCA artigo).
- O seu trabalho na Europa tem a maioria concentrada nas unlinkable
credenciais para pagamentos de portagens, o voto electrónico, etc.
Sua empresa, a DigiCash, está trabalhando em diversos aspectos do
dinheiro digital.
12.5.3. "Como é que o seu sistema de trabalho?"
- Tem havido muitos resumos sobre Cypherpunks lista. Hal
Finney escreveu pelo menos meia dúzia, e outros
foi contribuído por Eric Hughes, Karl Barrus, etc. Eu não
ser, incluindo a qualquer deles aqui....ele só leva muitas
páginas para explicar como o dinheiro digital funciona em detalhes.
- (O maior problema que as pessoas têm com dinheiro digital em
não tomar o tempo para entender o básico da matemática,
de cegueira, etc. Eles erradamente, que "dinheiro digital"
pode ser entendido pelo senso comum de raciocínio sobre as já existentes
dinheiro, etc. Este erro tem sido repetida em vários
half-assed propostas de "dinheiro líquido" e "digi dólares.")
+ Veja aqui a abertura de alguns parágrafos de um dos Hal
explicações, para fornecer um vislumbre:
- "Mike em uma Única pergunta sobre digicash. O sistema mais simples, eu
sabe do que é anônimo é o um por Chaum, Fiat, e
Naor, que já discutimos aqui algumas vezes. A ideia
é o que o banco escolhe um RSA módulo de elasticidade, e um conjunto de
expoentes e1, e2, e3, ..., onde cada expoente ei
representa
uma denominação e, possivelmente, de uma data. Os expoentes devem
ser relativamente primo a (p-1)(q-1). O PGP tem um GCD rotina
o que pode ser usado para verificar válido expoentes..

"Como com RSA, para cada expoente público ei corresponde um
segredo expoente di, calculado como a multiplicativo
inverso do ei mod (p-1)(q-1). Novamente, o PGP tem uma rotina
para calcular os inversos multiplicativos.

"Neste sistema, uma parte do dinheiro é um par (x, f(x)^di),
onde f() é uma função unidirecional. MD5 seria um
escolha razoável para f(), mas repare que ela produz um
Resultado de 128 bits. f() deve levar isso de 128 bits de saída de
MD5 e "reblock" para ser um multi-número de precisão por
estofamento-lo; PGP tem um "preblock" rotina que faz isso,
seguindo o padrão PKCS.

"A forma como o processo funciona, com a cegueira, é como
isso. O usuário escolhe uma aleatória x. Isto provavelmente deve
pelo menos, 64 ou 128 bits, o suficiente para impedir exaustiva
a pesquisa. Ele calcula f(x), que é o que ele quer que o
banco para assinar aumentando o poder de di. Mas ao invés de
o envio de f(x) para o banco diretamente, o usuário primeiro blinds
escolhendo um número aleatório r, e calcular D=f(x)
* r^ei. (Devo deixar claro que ^ é o poder
operador, não xor.) D é que ele envia para o banco,
juntamente com algumas informações sobre o que ei é, o que diz
a denominação do dinheiro, e também informações sobre
o seu número de conta." [Hal Finney, 1993-12-04]

12.5.4. "O que está acontecendo com DigiCash?"

- "Pagamento a partir de qualquer computador pessoal para qualquer outra
estação de trabalho, através de e-mail ou Internet, tem sido demonstrado
pela primeira vez, usando o dinheiro eletrônico da tecnologia. "Você
pode pagar para ter acesso a um banco de dados, aquisição de software ou um
boletim por e-mail, jogar um jogo de computador ao longo da rede,
receber us $5 devidos a você por um amigo, ou apenas pedir uma pizza. O
as possibilidades são verdadeiramente ilimitadas" de acordo com David
Chaum, Diretor de DigiCash TM, que anunciou e
demonstrado o produto durante o seu discurso no
primeira conferência sobre a World Wide Web, em Genebra, este
a semana." [DIGICASH comunicado de IMPRENSA, pela primeira vez no Mundo eletrônico
pagamento em dinheiro através de redes de computadores," 1994-05-27]
- DigiCash é David Chaum da empresa, criada para comercializar
esta obra. Localizado perto de Amesterdão.
+ Chaum é também central invovled no "CAFÉ", um Europeu
comitê de investigação de formas para implantar o dinheiro digital em
Europa
- a maioria normas, questões de privacidade, etc.
- as estradas de pedágio, balsas, parquímetros, etc.
- http://digicash.support.nl/
- info@digicash.nl
- As pessoas têm relatado que as suas perguntas não são
sendo respondidas; pode ser por vários motivos.

12.5.5. As Complexidades do Dinheiro Digital

- Não há dúvida quanto à complexidade: muitos protocolos,
semântica confusão, muitos partidos, as chances de conluio,
de ocultação, o repúdio, e o como. E muitos derivados
entidades: agentes, serviços de garantia, bancos.
- Não há nenhum substituto para a _thinking hard_ sobre vários
cenários. Pensar sobre como organizar off-line de compensação,

como lidar com reclamações de pessoas que afirmam que sua digital
o dinheiro foi roubado, pessoas que querem vários tipos especiais de
serviços, tais como recibos, e assim por diante. É uma ecologia
aqui, não apenas um conjunto de equações simples.

12.6. On-line e off-line de Compensação, o Dobro da Despesa
12.6.1. (esta seção ainda em construção)
12.6.2. Este é um dos principais pontos de divisão entre os sistemas.
12.6.3. On-Line De Compensação
- (inserir explicação)
12.6.4. Offline Compensação
- (inserir explicação)
12.6.5. Duplo gastos
- Algumas abordagens envolvem a constante crescimento em tamanho de moedas
cada transferência, de modo que gastou o dinheiro em primeiro lugar pode ser deduzido
(ou variantes deste). E N. Ferguson desenvolvido um sistema de
permitindo até N despesas da mesma moeda, onde N é
um parâmetro. [Howard Gayle lembrou-me isso, 1994-08-29]
- "Por que todo mundo acha que a lei deve ser imediatamente
invocado quando o casal de gastos é detectada?....Duplo
a despesa é informativa é da propriedade do dinheiro digital
sistemas. Precisamos encontrar intenção maliciosa em um formal
propriedade? O óbvio moralismo sobre a lei e a dupla
gastadores é inadequado. Ele evoca imagens de vingança e
retribuição, o que é estúpido, para não falar de negativo
valor econômico." [Eric Hughes, 1994-08-27] (Este também
relaciona-se com Eric bom ponto de que nós também, muitas vezes, do quadro de criptografia
problema em termos de carregado de termos como "trapaça", "spoofing"
e "inimigos", quando mais neutro, em termos levaria menos
significado-a obscurecer a bagagem e não dar nossos "inimigos"
(:-}) as munições para aprovar leis com base em tais termos.)
12.6.6. Questões
+ Chaum double-gastos com sistemas de detecção de
- Chaum fez um grande esforço para desenvolver o sistema que
preservar o anonimato por único-a despesa instâncias, mas
que quebra de anonimato e, assim, revelar a identidade de duas
gastos instâncias. Eu não tenho certeza de que as forças de mercado
causou-lhe para pensar sobre isso como sendo tão importante, mas
ele cria que muitas dores de cabeça. Além de ser desastrada,
exigem física ID, ele invoca um sistema jurídico para tentar
coletamos de "duplo gastadores", e admite-se que o
extremamente grave violação de privacidade permitindo que picadas.
Por exemplo, Alice paga Bob uma unidade de dinheiro, em seguida, rapidamente

Alice passa o que o dinheiro antes do Bob pode...Bob, em seguida, é
revelado como um "duplo gastador" e a sua identidade revelada
para whomver queriam...Alice, IRS, Gestapo, etc. Um muito
quebrado idéia. Aceitável, principalmente para pequenas transações.
+ Multi-despesa vs on-line de compensação
- Eu sou a favor on-line de compensação. Simplificando: o primeiro gastos
é a única despesa. O cara que fica para o trem
armário onde o dinheiro fica armazenado é o cara que recebe-lo.
Este garantir que a carga de manter o segredo é
o segredo titular.
- Quando Alice e Bob transferência de dinheiro, Alice faz o
transferência, Bob confirma-a como válida (ou verifique que o seu
o banco tem recebido o depósito), e a transação é
concluída.
- Com velocidades de rede a aumentar dramaticamente, na linha de
compensação deve ser viável para a maioria das transações. Fora
linha de sistemas pode, naturalmente, ser útil, especialmente para
transações pequenas, aquelas manipuladas com moedas e
notas de pequeno valor.
-
12.6.7. "Como na linha de limpeza de anônimos dinheiro digital de trabalho?"
- Há um monte de matemática conectado com cegueira,
exponentions, etc. Ver Schneier livro para uma introdução
ou vários documentos de Chaum, Marcas, Bos, etc.
- Na linha de compensação é semelhante para as duas partes em uma transação
a troca de mercadorias e de dinheiro. A transação é clearled
localmente, e imediatamente. Ou eles poderiam organizar a transferência de
fundos em um banco, e o banqueiro poderia dizer-lhes sobre o
telefone de que a transação foi desmarcada--true "em-linha
compensação." Cartões de débito funcionam desta forma, com dinheiro
transferido de forma eficaz imediatamente de uma conta
em outro. Cartões de crédito adicionais rugas,
como o crédito aspecto, mas, basicamente, ainda na linha de
compensação.
- Conceitualmente, o princípio orientador ideia é simples: quem
fica para o trem armário onde o dinheiro é guardado *primeiro*
fica com o dinheiro. Não pode nunca ser "o dobro de gastos," só
as pessoas que recebem para o armário e encontrar nenhum dinheiro dentro.
Chaumian ofuscante permite que o "trem do armário" (por exemplo, Crédito
Suisse) para dar o dinheiro para a entidade fazer a alegação de
sem saber como, o número correlatos anteriores
números que eles "venderam" para outras entidades. O anonimato é
preservado, absolutamente. (Ignorando a discussão de questões

de câmeras assistindo a caixa de recebimento, se é que alguma vez realmente
se apanhada.)
- Uma vez que o "handshaking" em-linha limpeza é aceito,
com base no "primeiro para o dinheiro o obtém de" princípio e, em seguida,
redes de tais câmaras pode prosperar, pois cada um é
confiante sobre a limpeza. (Há algumas coisas importantes
necessário para fornecer o que eu vou dub "fechamento" para o circuito.
As pessoas precisam de ping sistema, depositar e levantar,
para estabelecer a confiança e a tampa. Muito como o reenvio de e-mails
redes. Na verdade, muito parecido com eles.)
- Em compensação, apenas um número é necessário para fazer um
transferência. Conceitualmente, o que é. Apenas um número. É até
o titular do número para protegê-lo cuidadosamente, o que é
como deve ser (por razões de localidade, ou de auto-
a responsabilidade, e como qualquer outra opção que apresenta
repúdio, a rejeição e o "Twinkies me fez fazer isso"
o tipo de absurdo). Uma vez que o número é transferido e
reblinded, o número antigo não tem mais nenhum direito sobre o
dinheiro guardado no banco credit Suisse, por exemplo. Que o dinheiro é
agora fora do trem armário e em um novo. (As pessoas
sempre perguntam, "Mas onde está o dinheiro, realmente?" Eu vejo digital
dinheiro *sinistros* em contas existentes detentor de dinheiro
lugares, normalmente os bancos. Há todos os tipos de "reclamações"--
Eric Hughes já nos alegrou com as histórias de suas explorações
do mundo de comercial de papel. Meu uso do termo
"reclamação" aqui é o "momento certo número, você
obter acesso" tipo. Como a combinação de um cofre. O trem
armário idéia torna isso mais claro, e fica em torno da
a confusão sobre "digimarks" de "e$" na verdade, qualquer _being_
tipo de dinheiro e de si mesmo).

12.7. Usa para Dinheiro Digital
12.7.1. Usa para dinheiro digital?
- Proteção de privacidade
- Prevenção de rastreamento de movimentos, contatos, preferências
+ Mercados ilegais
- jogos de azar
- subornos, pagamentos de salários
- assassinatos e outros contrato de crimes
- instalação de cercas, aquisição de bens
+ Evasão fiscal
renda esconder
- ventos de transferências de fundos

- mercados ilegais
- Serviços on-line, jogos, etc.
+ Agoric mercados, como para a alocação de computador
recursos
- onde os programas, os agentes de "pagar" pelos serviços utilizados, fazer
"lances" para futuros serviços, coletar "alugar", etc.
+ Portagens, taxas de estacionamento, onde unlinkablity é desejado.
Este comunicado de imprensa trecho deve dar o sabor de
se pretende utiliza para pagamento de portagens:
- "O produto foi desenvolvido pela DigiCash TM Corporation
detida a subsidiária holandesa, DigiCash TM BV. É
relacionados à empresa anteriormente produto lançado para a estrada
o preço, que foi licenciado para Amtech TM
Corporation, de Dallas, Texas, líder mundial no
automático estrada de cobrança de portagens. Este sistema permite
privacidade protegida pagamentos para o uso da estrada em plena auto-estrada
a velocidade de uma leitora de cartão inteligente aposta para o interior de uma
do veículo. Também relacionados com a abordagem da UE apoiaram
CAFÉ projeto, do qual o Dr. Chaum é o Presidente, que usa
resistente a adulterações fichas inserido em carteiras electrónicas."
[DIGICASH comunicado de IMPRENSA, "primeiro do Mundo em caixa eletrônico
pagamento através de redes de computadores," 1994-05-27]
12.7.2. "Quais são algumas das motivações para o anônimo digital de dinheiro?"
+ Pagamentos que são unlinkable a identidade, especialmente para
coisas como portagens na ponte, pedágios, etc.
- onde linkablity implicaria posição de rastreamento
- Por que não, use moedas? Esta ideia é para "smart card"-tipo de
sistemas de pagamento, envolvendo a comunicação sem fios.
Singapura planejada (e talvez tenha implementado) tal
o sistema, excepto não houve considerações de privacidade.)
+ Pagar as coisas enquanto estiver usando pseudônimos
- nenhum ponto em ter um pseudônimo se o sistema de pagamento
revela a identidade de uma pessoa
+ Evasão fiscal
- isso é o que o digicash proponentes não gostam de
falar muito alto, mas é claro que é uma time-honored
a preocupação de todos os contribuintes
+ Porque não há nenhuma razão por que o dinheiro deve ser
vinculada à identidade pessoal
- um ponto geral, incluir outros

12.8. Outros Dinheiro Digital Sistemas De
12.8.1. "Parece que há muitas variantes....o que é a história?"

- Muita confusão. Muitos dos sistemas que não estão em todos os
anônimo, que são apenas extensões dos sistemas existentes.
O prestígio do dinheiro digital é tal que muitas pessoas estão
alegando que os seus sistemas não são "dinheiro digital", quando de curso
eles não são (pelo menos não no Chaum/Cypherpunk sentido).
- Então, cuidado. Contrapartidas.

12.8.2. Criptografia e Cartões de Crédito (e na linha de compensação)

+ De criptografia secure digital cash pode encontrar uma grande utilização
em efetivamente estendendo a modalidade de cartões de crédito
de baixo nível, de pessoa para pessoa transações.
- Que é, a conveniência dos cartões de crédito é uma das suas
principais utilizações (os outros sendo que o avanço do crédito real,
ignorada aqui). Na verdade, garantido cartões de crédito e débito
cartões que não oferecem esse avanço do crédito, mas são
usado principalmente para acumular o "telefone" e "evitar
o transporte de dinheiro" vantagens.
- Verifica oferecem a "não levar dinheiro" vantagem", mas tomar
tempo para limpar. Traveller's cheques são a mais pura forma de
isso.
- Mas indivíduos (como Alice e Bob) pode utilizar atualmente
o sistema de cartão de crédito mútuo transações. Eu não estou
a certeza de todas as razões. Como isso poderia mudar?
- Crypto pode permitir unforgeable sistemas, através de alguma variante de
assinaturas digitais. Que é, Alice pode aceitar um telefonou
o pagamento do Bob sem nunca ser capaz de sinal de Bob
assinatura electrónica de si mesma.
- "Crypto Cartões de Crédito" pode permitir que os usuários finais (clientes, em
o sistema atual) para lidar com transações, como este, sem
tendo comerciantes intermediários.
- Tenho certeza de que o cartão de crédito existente roupas teria
algo a dizer sobre isso, e não pode ser de vários
obstáculos no caminho. Seria melhor comprar o VISTO
e MasterCard pessoas trabalhando através deles. (E eles
provavelmente estudaram este problema; o que pode mudar a sua
posições é forte criptografia, disponível no local para os usuários.)
- (On-line de compensação--para evitar a dupla de gastos e cópia
de dinheiro-é um aspecto importante de muitas dinheiro digital
protocolos, e do VISTO do tipo de protocolos. Felizmente,
as redes estão se tornando onipresentes e rápido. Uso doméstico é
ainda uma lata de vermes, embora, com normas concorrentes
com base no vídeo cabo, fibra ótica, ISDN, ATM, etc.)

12.8.3. Muitos sistemas de ser lançada. Aqui está uma amostra:

+ Mondex

- "Ao contrário da maioria dos outros bolsa eletrônica de sistemas, Mondex, como dinheiro, é anônimo. Os bancos que emitem Mondex cartões não vai ser capaz de manter o controle de quem recebe os pagamentos. De fato, é o único sistema em que dois titulares do cartão pode transferir dinheiro para outro.

"Se você quer ter um produto que substitui o dinheiro, você tem que fazer tudo o que o dinheiro faz, só que melhor" Mondex executivo sênior, Michael Keegan disse. "Você pode dar dinheiro para o seu irmão, que dá para o sujeito que vende jornais, que dá a uma instituição de caridade, que coloca em o banco, que não tem nenhuma idéia de onde ele estava. Que é o que o dinheiro está."" [New York Times, 1994-09-06, fornecida por John Jovem]

+ CommerceNet

- permite que os usuários da Internet para comprar e vender mercadorias.

- "Eu li ontem do L. A. Times sobre algo chamado CommerceNet, onde vendedores e compradores de estação de trabalho nível do equipamento pode atender e realizar busniess....Perto do final do artigo, falou sobre um método proposto para a troca de "assinaturas digitais", através de Moasic (para que compradores e vendedores poderia _know_ que eles estavam que eles disse que eles estavam) e que eles estavam indo para "enviar para os Padrões da Internet corpo"" [Cypher1@aol.com, 1994-06-23]

+ Sphinx

- artigo publicado em 1 de ACM Conference on Computer e Segurança De Comunicações, Nov. 93, disponível através do anônimo ftp de PROSPERO.ISI.EDU como /pub/papers/segurança/sphinx-cccs93.ps.Z

- "Sphinx: Uma estrutura para a prática de moeda electrónica em o Internet ... Gennady Medvinsky e Clifford Neuman

"O sphinx é um framework que suporta electrónica em tempo real pagamentos com prestação de anonimato sobre uma não segura rede. Ele é projetado para permitir que novos tipos de serviços na Internet, que não tem sido prática a data por causa da ausência de um seguro, escalável, potencialmente anônimo método de pagamento.

"Sphinx estabelece um equilíbrio entre incondicionalmente anônimo moeda electrónica, e assinado instrumentos análogo para as verificações que são mais escalável, mas identificar

os objetos em uma transação. Ele faz isso por
estabelece o quadro dentro do qual proposta eletrônica
moeda protocolos pode ser integrado com o escalável,
mas não anônimo, banco eletrônico de infra-estrutura que
tem sido proposto para a rotina de transações".
+ Hal Finney teve uma reação negativa ao seu sistema:
- "Eu não acho que foi nada bom. Eles têm uma
extremamente simplista do modelo, e seus "protocolos" são
da ordem, a envia o banco algum dinheiro de papel, e B
envia Um caixa eletrônico em troca.....Eles não
ainda não ofuscante do dinheiro. Cada peça de dinheiro tem um
número de série único que é conhecida a moeda
fornecedor. Este seria, claro, permitir a correspondência de
retirado e depositado moedas....Esses caras parecem
leu o trabalho no campo (referência), mas,
eles não parecem ter entendido." [Hal Finney,
1993-08-17]
+ VISTO Bolsa Eletrônica
- (Um monte de coisas apareceram, incluindo listagens de
os parceiros da aliança (como Verifone), a tecnologia,
os planos para a implantação, etc. Lamento que eu não posso
incluir mais aqui. Talvez quando este FAQ é um Web doc, mais
podem ser incluídos.)
- "FINANÇAS PESSOAIS - Buscando o Cartão Que Iria Criar Um
Sem Mundo. O Washington Post, 03 De Abril De 1994,
Última Edição Por: Albert B. Crenshaw, Washington Post ...

"Agora que os cartões de crédito estão nas mãos de praticamente
todos vida, respiração adultos no país-não
falar um monte de filhos, e a ocasional animal de estimação da família-
e agora que quase como muitas pessoas têm cartões ATM,
cartão de empresas está se perguntando onde o crescimento futuro será
vem.

"Em *Visa* Internacional, a resposta é: Substituem o dinheiro
com o plástico.

"No mês passado, a gigante associação de emissores de cartão de
anunciou que havia se formado uma coalizão de serviços bancários e
empresas de tecnologia para desenvolver normas técnicas para
um produto apelidado de "Bolsa Eletrônica", um plástico
cartão destinado a substituir as moedas e notas pequenas
transações." [fornecidos por Duncan Frissell, 1994-04-05]

- O falar das "câmaras" e o envolvimento de VISTO
Internacional e os Suspeitos do Costume sugerir
identidade-ofuscante protocolos não estão em uso. Eu também vejo nenhuma
menção de DigiCash, ou até mesmo o RSA (mas talvez eu perdi-
-e a presença de RSA não significa necessairly
identidade-ofuscante protocolos estão sendo planejados).

Cenário provável: Este é *não* dinheiro digital como pensamos
do mesmo. Ao contrário, esta é uma evolução futura de fluxos de caixa ATM
cartão e cartão de crédito, otimizado para uma mais rápida e mais barata
compensação.

Assustador Cenário: Este poderia ser o veículo para o longo
os rumores de que "a proibição de dinheiro." (Só porque conspiração
teóricos e Número da Besta Xtian fundamentalistas
acredito que não torná-lo plausível.)
- Quase nada de interesse para nós. Não há métodos para
o anonimato. Não se engane, este não é o dinheiro digital
que Cypherpunks defendem. Isso dá a agências de crédito
e o governo (os dois trabalham lado a lado) completo
rastreabilidade de todas as compras, a geração automática de relatórios de
padrões de despesa, listas de destino para aqueles que frequentam
sobre-a-ser-banido empresas, e invasivos
fiscalização de todos os inter-pessoais, as transações econômicas.
Este é o AntiCash. Cuidado com o Número de AntiCash.
12.8.4. Nick Szabo:
- "Internet comercialização, em si, é um problema _huge_
cheio de armadilha e a oportunidade: Mom & Pop BBS,o
comercial Lamas, bancos de dados, com fins lucrativos pirata e pornô
conselhos de administração, etc. estão surgindo em toda parte, como ervas daninhas,
a abertura de uma vasta gama de necessidades de privacidade e as formas de
abuso de privacidade. Remetentes, dinheiro digital, etc. não vai se tornar
parte deste comércio na Internet modo de vida, a menos que eles são
implantado em breve, teórica, com defeitos e tudo, em vez de
aguardar até que O Sistema Perfeito vem junto. Crypto-
a anarquia no mundo real vai ser complicado, "a natureza, vermelha em
dentes e garras", e não tudo de bom e limpo, como se diz na
livros de matemática. A maioria dos thedebugging vai ser feito em qualquer
torre de marfim, mas com a falência de empresas que
violar a sua privacidade do cliente, a confiscação dos BBS
os operadores que se afastam de fora as leis de alguns jurisdição
e estragar a sua privacidade, acordos, etc. Qualquer pessoa que
pensa que eles podem carne um protocolo em segredo e, em seguida,

implantá-lo, completo e funcionando, está em um mundo de
ferido. Para aqueles que recebem a sua Boa sistemas
lá e usados, há grande potencial para o crescimento do negócio
-- acho que dos us $trilhões confiscados a cada ano por
os governos de todo o mundo, por exemplo." [Nick Szabo,
1993-8-23]
12.8.5. "O que sobre _non-anonymous_ digital de dinheiro?"
- a la as várias extensões do existente de crédito e débito
cartões, cheques, etc.
+ Há ainda um uso para este, com várias motivações"
* para os usuários, pode ser _cheaper_ (menores custos de transação)
totalmente anônimo dinheiro digital
* para os bancos, também pode ser mais barato
* os usuários podem querer trilhas de auditoria, prova, etc.
* e, claro, os governos têm várias razões para
querendo rastreáveis sistemas de caixa
- aplicação da lei
- os impostos, o revestimento, a economia subterrânea
12.8.6. A Microsoft planeja introduzir o home banking de negócios
- "De PORTLAND, oregon. (AP) - a Microsoft Corp. deseja substituir
seu talão de cheques com um computador em casa que permite que o banco fazer
todo o trabalho de gravação verificações, a contagem de cartão de crédito
encargos e pagamento de contas.... O serviço também faixas de crédito
cartão de contas, os levantamentos de caixas automáticos (atm),
transferências de poupança ou de outras contas, linhas de crédito,
cartões de débito, ações e outros investimentos, e projeto de lei
pagamentos." [Associated Press, 1994-07-04]
- Planejada links com um consórcio de bancos, liderado por EUA
Bancorp, usando o seu "Dinheiro" pacote de software.
- Comentário: Tais movimentos como este,--e não se esqueça de que o cabo de
empresas-pode resultar em uma rápida transição para uma forma de
o home banking e "dinheiro digital." Obviamente, este tipo de
dinheiro digital, como está sendo planejado, hoje, é muito de
o tipo de dinheiro digital que nos interessa. Na verdade, ele é
o oposto do que queremos.
12.8.7. Cartão de crédito de compensação...pessoas não podem usar o sistema
- se algo não anônimos, como cartões de crédito não pode ser utilizado
por fim usuários (Alice e Bob), por que devemos esperar de um
anônimo versão de este seria o mais fácil de usar ou
mais possível?
- (E dando aos usuários encriptado links para agências de crédito seria
pelo menos, deixar os problemas de segurança com cartão de crédito
os números sobre as ligações que podem ser observados.)

- Mondex afirma que seu sistema vai permitir esse tipo de pessoa-
a pessoa de transferência de anônimos dinheiro digital (eu vou acreditar
quando eu vê-lo).

12.9. Questões jurídicas com Dinheiro Digital
10.8.1. "O que é o estatuto jurídico do dinheiro digital?"
- Não foi testado, como um monte de protocolos de criptografia. Ele
pode ser de muitos anos, antes de estes sistemas são testados.
10.8.2. "Há um empate entre dinheiro digital e lavagem de dinheiro?"
- Não tem que ser, mas muitos de nós acreditam que o
uma ampla implantação do digital, untraceable dinheiro
possibilitar novas abordagens
- Daí a importância do dinheiro digital por criptografia anarquia e
idéias relacionados.
- (No caso de não ser óbvio, eu considero lavagem de dinheiro, uma
não-crime.)
10.8.3. "É verdade que o governo dos EUA pode limitar fundos
transferências de fora dos EUA?"
- Muitos problemas aqui. Certamente algumas leis existem. Certamente
as pessoas são processados todos os dias, por violação moeda
leis de exportação. Muitos caminhos existem.
- "LEGALIDADE - não Há e nunca vai ser uma lei restringindo
o envio de fundos fora dos Estados Unidos. Como faço para
sabia que? Simples assim. Como um país dependente internacional
comercial (bilhões de dólares ao ano e contando), o
Economia americana seria destruído." [David Johnson,
privacy@bem.sf.ac.nós, "Offshore Banking & Privacidade"
alt.privacidade, 1994-07-05]
10.8.4. "São "moedas alternativas" permitido nos EUA? E o que é
a implicação do dinheiro digital de várias formas?
- Tokens, cupões, certificados de presente são permitidos, mas de rosto
vários regulamentos. A batata frita de cassino eram tratados como
o dinheiro, mas agora são mais regulados (inter-casino de conversão
não é mais permitido).
- Qualquer tentativa de usar esses cupons como uma moeda alternativa
enfrentar os obstáculos. O cupom poderá ser permitido, mas fortemente
regulamentado (requisitos de apresentação de relatórios, etc.).
- Perry Metzger notas, obrigações ao portador, são ilegais no
Estados unidos (portador de bond, representado em dinheiro, em que nenhum nome foi
anexado ao título--o "portador" poderia vendê-lo por dinheiro
ou resgatá-lo...funcionou muito bem para o transporte de grandes quantidades
de dinheiro em forma compacta).
+ Nota: Duncan Frissell afirma que as obrigações ao portador são _not_

ilegal.
- "Sob a Equidade Fiscal e de Responsabilidade Fiscal, Lei de
1982 (TEFRA), quaisquer pagamentos de juros feito no *novo* problemas de
doméstica obrigações ao portador não são dedutíveis como um
comuns e necessárias despesas de negócios, de modo nenhum ter sido
emitido desde então. Ao mesmo tempo, os Federais
administrativamente parou de emitir títulos do tesouro em
formulário do portador. Antigas questões de governo e de dívida corporativa
no formulário do portador ainda existem e virão a existir e o comércio
30 ou mais anos depois de 1982. Além disso, os residentes dos EUA
pode comprar legalmente estrangeiros de títulos ao portador." [Duncan
Frissell, 1994-08-10]
- Alguém tem uma visão um pouco diferente: "O passado não
Portador de emissões de obrigações maduro, em 1997. Eu também acredito que a
cobrar juros, e para resgatar o vínculo, na data do vencimento, você
deve dar seu nome e fiscal-número de identificação para o pagamento de
agente. (Eu posso verificar com o departamento que lida aqui
se alguém estiver interessado no pertinentes OCC normas que
aplicar)" [prig0011@gold.tc.umn.edu, 1994-08-10]
- Eu citar este terríveis detalhes para dar aos leitores uma idéia sobre
quanto a confusão que existe sobre estes assuntos. O
conselho habitual é "buscar a competente conselho", mas na verdade
a maioria dos advogados não tem idéias claras sobre o melhor
estratégias, e o run-of-the-moinho advisor pode enganar
um perigosamente. Pisar com cuidado.
- Isso tem implicações para o digital cash, é claro.
10.8.5. "Por que dinheiro digital e afins techologies tomar posse
no início mercados ilegais? Que é, será que a Turba ser um dos primeiros a
adotante?"
- untraceability necessário
- e a reputação são importantes para eles
- eles mostraram, no passado, que eles vão tentar de novo
abordagens, a la o dinheiro movimentos dos cartéis de drogas,
novos métodos para a segurança, etc.
10.8.6. "Caixa eletrônico...será que vai ter que cumprir com as leis, e
como?"
- As questões serão levantadas sobre o anonimato aspectos, o
utilidade para evadir impostos e requisitos de informação,
etc.
- um bagunçado problema, a certeza de ser debatido e legislado sobre para
muitos anos
+ dividir o dinheiro em vários pedaços...é essa "estruturação"? é
isso é legal?

- algumas regras indicam a estruturação de per se, não é
ilegal, apenas a evasão fiscal ou de moeda, controle de evasão
- o que, em seguida, de sistemas que _automatically_, como uma base de
recurso, dividir o dinheiro em vários pedaços e mover
eles?
10.8.7. Moeda, controles de vôo, capital regulamentos, boicotes,
ativo convulsões, etc.
- todos são pressões para encontrar maneiras alternativas de capital para o
o fluxo de
- todos para a falta de confiança, o que, paradoxalmente, para
os legisladores, faz com que a fuga de capitais tudo o mais provável
10.8.8. "Vai reguladores bancários permitir digital de dinheiro?"
- Não é tarefa fácil, isso é certo. O labirinto de regulamentos,
restrições de impostos, leis e decisões judiciais é assustador. Eric
Hughes passei muito tempo lendo sobre as leis em relação à
bancos, papel comercial, impostos, etc., e concluiu muito
o mesmo. Eu não estou dizendo que é impossível-de fato, eu acredito
que um dia vai acontecer, de alguma forma--, mas os obstáculos são
formidável.
+ Algumas questões:
+ Será que tal operação ser permitido ser centralizado ou com base
nos EUA?
- Quais estados? Que leis? Banco vs. Poupança e Empréstimo vs.
União de crédito vs. Corretor de Títulos vs. algo mais?
+ Os clientes poderão acessar tais entidades ventos,
fora dos EUA?
- forte de criptografia torna a comunicação possível, mas pode
ser difícil, e não uma parte do tecido empresarial, etc.
(e, portanto, não é tão útil-se alguém tem para enviar PGP-
criptografados instruções para um banqueiro, e não pode usar
a limpeza de infra-estruturas....)
+ A cobrança de impostos, lavagem de dinheiro, leis, leis de divulgação,
"conheça o seu cliente" leis....todos são áreas onde um
digital "banco" pode ser desligado imediatamente. Qualquer banco e não
preencher os formulários (incluindo obrigatório
relatório de transações de determinadas quantidades e tipos de
e a Segurança Social/Contribuinte, Número de clientes)
enfrenta enormes multas, penalidades e sanções regulatórias.
- e a jogadores existentes no bancárias e de valores
o negócio não vai ficar de braços cruzados enquanto os recém-chegados enter
de mercado; procurarão forçar os recém-chegados para pular
através do mesmo aros que tinha (estudos indicam
grandes corporações, na verdade, _like_ burocracia, como

ajuda-los em relação às empresas de menor dimensão)
- Concluson: Digital, os bancos não ser "lançado" sem um
muito trabalho por advogados, contadores, peritos fiscais,
lobistas, etc. "Limonada digital bancos" (TM) será
não sobreviver por muito tempo. Crianças, não tentem isto em casa!
- (Muitas novas indústrias que estão familiarizados com software,
microcomputadores--tinha muito pouco regulamento, com razão. Mas
o efeito é que muitos de nós não estão preparados para entender
a enorme quantidade de burocracia que as empresas de outros
áreas, nomeadamente a banca, cara.)
10.8.9. Obstáculos legais para o dinheiro digital. Se os governos não querem
anônimo dinheiro, eles podem tornar as coisas difíceis.
+ Como Perry Metzger e Eric Hughes já disse muitas vezes,
regulamentos podem tornar a vida muito difícil. De conformidade com
leis é um grande custo de fazer negócios.
- ~"O custo de conformidade em um típico EUA banco é de 14% de
custos operacionais."~ [Eric Hughes, citando uma "Americano
Banqueiro" do artigo, 1994-08-30]
+ Labirinto de regulamentos é navegável por grandes
instituições, com equipes de advogados, contadores, fiscais
especialistas, etc., mas é, essencialmente, além do
capacidades de muito pequenas instituições, pelo menos no
EUA
- isso pode ou não pode ser, como computadores
proliferam. Um "banco-in-a-box" programa pode ajudar. Meu
a suspeita é de que um determinado tamanho de funcionários necessários
para lidar com o face-a-face reuniões e aro de salto.
+ "Nova Ordem Mundial"
- EUA pedindo outros países para "jogar bola" na bancário
o sigilo, a evasão fiscal, a extradição, a imigração, etc.
- este é fechar o ex-lacunas e escapar
escotilhas que se permitiu que as pessoas a escapar repressivas
tributação...as implicações para o digital de dinheiro que os bancos são
claro, mas preocupante.

12.10. Perspectivas para o Uso de Dinheiro Digital
12.10.1. "Se o dinheiro digital é tão grande, por que não está sendo usado?"
- Ainda não foi concluído. Protocolos ainda estão sendo pesquisados,
papéis estão ainda a ser publicado. Em qualquer área, tais
como portagens pagamentos, poderá ser possível implantar uma
aplicação-sistema específico, mas não há "geral"
solução (ainda). Não há digital "moeda" ou unforgeable
objeto que representa valor e, portanto, o dinheiro digital área é

mais parecido com o da mesma forma não-simples mercados
instrumentos financeiros, papel comercial, obrigações, warrants,
verifica, etc. (Áreas que não são inerentemente simples e que
foram necessários muitos de informatização e comunicação para
fazer gerenciável.)
- Flakiness de Redes. Falha de sistemas, e-mail está atrasado
inexplicavelmente, inscrições para listas de começar almoçou, e todas as
outros tipos de rupturas ocorrem. A maioria das interações no
Redes envolve uma quantidade razoável de humanos de adaptação à mudança
condições, screwups, soluções, etc. Estes não são
condições que inspirar confiança em automatizada dinheiro
sistemas!
- O difícil de Usar. Algumas pessoas usam sistemas que necessitam de
geração de código, clientes, etc. Semantic gap (geração de
coisas em uma estação de trabalho Unix não é como tomar um
talão de cheques de fora). Protocolos de criptografia são geralmente difíceis de
uso e confuso.
- Falta de necessidade premente. Embora as pessoas têm tentado vários
experiências com dinheiro digital tokens ou cupons (Magia
Dinheiro/Brega Tokens, o HeX mercado, etc.), há pouco
mundo real incentivo para experimentar com eles. E a maioria dos
o denominado tokens são verdadeiramente trivial quantidades de
dinheiro, não para qualquer coisa vale a pena gastar tempo para aprender. Nenhum
mercado para compradores para "passear." (Você não
comprar o que você não vê.)
- Questões jurídicas. O IRS não vendo
moedas alternativas, especialmente se utilizados na tentativa de
ignorar ordinária de cobrança de impostos esquemas. Esta e outras
questões legais (resgates em dólares) colocar uma estrada
frente a sério planeja usar o dinheiro digital.
- Questões De Investigação. Nem todos os problemas resolvidos. Ainda sendo
desenvolvido, papéis de serem publicados. Chaum do sistema não
parecem estar totalmente pronto para implantação, certamente não
fora bem definidos os mercados verticais.

12.10.2. "Por que não dinheiro digital em uso?"

- A Meta Problema: *o* dinheiro digital? As diversas tentativas de
dinheiro digital, ou digital, o dinheiro existe, mas a maioria são imperfeitos,
experimental, crufty, etc. Chaum do DigiCash foi anunciado
(Página Web, etc.), mas é, aparentemente, nem mesmo remotamente
utilizável.

+ Razões Práticas:

- nada para comprar
- não há padrão de sistemas que são fáceis de usar

- vantagens do anonimato e untraceability raramente são
explorar
- A Magia Dinheiro/Brega Tokens de experimentar o Cypherpunks
a lista é instrucive. Lotes de trabalho detalhado, muitos posts--
e ainda não é usada para qualquer coisa (concedido, não há muito
sendo comprados e vendidos na Lista, então...).
- Cenário para Usar em um Futuro Próximo: vertical
aplicação, tal como uma ponte de pedágio do sistema que oferece
o anonimato. Em uma vertical do aplicativo, os problemas de compatibilidade,
interfaces, formação e podem ser gerenciados.

12.10.3. "por que não dinheiro digital que está sendo usado?"

+ muitas razões, muitas razões!
+ questões difíceis, obscuros problemas
- a evolução técnica não é final, Chaum, Marcas, etc.
+ venda de usuários
- que não têm computadores, PDAs, os meios para fazer o
local cálculos
- que deseja versões portáteis do mesmo
+ A infra-estrutura para o dinheiro digital (Chaum anónimo-
estilo, e variantes, tais como Marcas) não existe,
e não pode existir em mais alguns anos. (Claro, eu
pensei que ia levar "vários anos" em 1988,
então o que eu sei?)
- As questões são conhecidas: falta de normas, falta de
protocolos, a falta de experiência do cliente, e, provavelmente,
obstáculos regulatórios. Uma perspectiva assustadora.
- Qualquer "lança" terá que ser bem financiado, bem
planejado, ou feito sub rosa, em alguns quase-legal, ou mesmo
mercado ilegal (como jogos de azar).
- "O povo americano manter alegando em pesquisas que eles querem
melhor proteção de privacidade, mas o fato é que a maioria não está
disposto a fazer qualquer coisa sobre ele: é apenas uma preferência,
não é um sólido imperativo. Até que algo Muito Ruim acontece
para muitos povos, como um resultado da perda de privacidade, que eu realmente não
acho que muita coisa vai ser feito que requer reais de trabalho e
inconveniência de pessoas, como mover-se para algo diferente
de cartões de crédito para longa distância transações e...
isso é uma tragédia."[L. Todd Masco , 1994-08-20]

12.10.4. "É forte de criptografia necessária para digital de dinheiro?"

- Sim, para a maior prova de balas formulário, o formulário de maior
interesse para nós e especialmente para os agentes autônomos
sistemas
+ Não, por certo fraco versões (não-métodos de criptografia de

segurança, controle de acesso, biometria, etc. métodos)
- por exemplo, o faturamento do Internet geralmente não é feito com
crypto
- e numeradas contas Suíças pode ser visto como uma forma fraca de
dinheiro digital (com a perda de algumas funcionalidades)
- "recibos de depósitos," como em ouro ou em moeda envios
12.10.5. em por que nós não podemos ter isso por um tempo, de um não-Cypherpunk
comentarista:
- "Governo requer informações sobre os fluxos de dinheiro, tributáveis
itens, e grandes operações financeiras.....Como resultado, ele
seria quase impossível definir um moderno anônimo
sistema de dinheiro digital, apesar do fato de que temos o
tecnologia.....Eu acho que nós temos mais de um direito à privacidade
com digicash transações, e eu também acho que há uma
mercado anônimo digicash sistemas. "[Thomas Conceder
Edwards. falar.política.crypto, 1994-09-06]
12.10.6. "Por que fazer um monte de programas de coisas como dinheiro digital tem
problemas na Net?
+ Muitas razões
- falta de infra-estrutura comercial, em geral, na
Net...o povo não está acostumado a comprar coisas que, de publicidade
não é recomendado (ou pior), e quase tudo é
"livre".
- falta de robustez e integridade nas diversas
protocolos: eles não estão "prontos para o horário nobre" na maioria
casos (PGP é sólido, e algumas boas shells existem para PGP,
mas a muitos outros protocolos de criptografia na maioria das vezes não
implementada, pelo menos, não é amplamente).
+ O Líquido corre "open-loop", como store-and-forward entrega
sistema
- O Líquido é mais uma store-and-forward netword, pelo menos,
na granularidade visto pelo usuário em enviar
mensagens, e, portanto, é "loop aberto." As mensagens podem ou
não seja recebido em tempo hábil, e que não é pouco
oportunidade para negotiaton em uma base em tempo real.
- Este circuito aberto natureza funciona normalmente...mensagens
durante a maior parte do tempo. E a "mensagem na garrafa"
a natureza se encaixa com remetentes anônimos (com
latência/atraso), com mensagem de piscinas, e com outros
programas de análise de tráfego mais difícil. Uma "fechada
loop," sistema responsivo é mais probabilidades de morrer para ser do tráfego
analisados pela correlação de pacotes, etc.
- mas o remetente não sabe se ele fica meio (retorno

recibos não comumente implementado...pode ser uma boa
função para incorporar; sistemas baseados em agentes
(Telescript?) certamente vai fazer isso)
- este circuito aberto natureza faz os protocolos de negociação,
dinheiro digital muito difícil de usar-é muito humano
é necessária intervenção
- Nota: Estes comentários se referem principalmente à _mail_ sistemas,
que é onde a maioria de nós já experimentou estes
idéias. Não-mail de sistemas, tais como mosaicos ou telnet ou
o como, ter melhor ou mais rápido mecanismos de feedback e
pode ser preferível para a implementação de Cypherpunks
gols. Pode ser que o foco natural em discussão
listas de e-mail, etc., tem distrair-nos. Talvez um foco
nos MUDs, ou mesmo ftp, teria sido mais
fecundo...mas nós somos uma lista de discussão, e a maioria das pessoas
são muito mais familiarizado com o e-mail do que com archie ou
gopher ou WAIS, etc.
- O legal e regulamentar obstáculos para um sistema real, usado
para as transações reais, são formidáveis. (Os obstáculos para
um "jogo" do sistema não são tão graves, mas, em seguida, reproduzir sistemas
tendem a não ficar muito desenvolvedor atenção.)

12.10.7. Cenário para a implantação de dinheiro digital

- Eric Hughes passou um tempo olhando para este. Muitos
problemas para ir para aqui, mas ele tinha esse interessante
cenário, repetidas quase que na sua totalidade aqui:
- "É muito improvável que os estados unidos com o banco será o único a
implantar anônimo digital de dólares em primeiro lugar. É muito mais
a probabilidade de que o primeiro dólar de dinheiro digital será emitido
no exterior, possivelmente, de Londres. Pela mesma razão, não
dólar regulamentação sobre os bancos neste país não é o mesmo
como o dólar regulamento, por isso, é bastante possível que o
Nova York, os bancos podem ser o primeiro emitentes de dinheiro digital, em
libras esterlinas, dizem.

"Não vai ser dividido em dois estágios, na verdade, a implantação digital
dinheiro. Por dinheiro digital, aqui, refiro-me a um retalho fenômeno,
disponível em ninguém. A primeira será para digitalizar dinheiro, e
a segunda será como ele. Esforços já estão
bem encaminhado para fazer mais-ou-menos secure digital fundos
as transferências razoavelmente baixas taxas de transação (não
os custos de transação, que são muito mais do que apenas taxas).
Esses esforços, enquanto eles mantêm alguns rastreabilidade,
quase certamente irá ter sucesso primeiro no mercado,

porque (e isso é vital) o ambiente regulador
contra o anonimato não é comprometida.

"Uma vez, no entanto, que o dinheiro tenha sido digitalizado, um dos
serviços disponíveis para compra pode ser anônimo
transferência de fundos. Espero que o primeiro de digitalização de
dinheiro não será plenamente fungíveis. Por exemplo, se você permitir
- me para retirar o dinheiro da sua conta de verificação automática
de débito, há risco de que o dinheiro não estará lá quando eu
pergunte para ele. Portanto, que tipo de dinheiro não vai ser
completamente fungíveis, como o dinheiro autorizado a partir de um
pessoa de não ser totalmente idêntico com o dinheiro do
outro. Pode ser uma questão do risco, pode ser uma oportunidade
o problema, pode ser uma taxa problema; eu não sei, mas é
improvável para ser perfeito.

"Agora, como a característica tamanho de um negócio diminui,
os custos relativos de lidar com qualquer imperfeição
há irá ser maior. A saber, o pequeno leitor vai
ainda tem algum problema a ser paga, embora, certamente,
menos do que agora. Digital em dinheiro resolve muitos desses problemas.
A compensação é imediata e final (nenhuma transação
reversões). O número de entidades de lidar é com muito
reduzida, espero que a um. A necessidade e o risco e o custo de
contas a receber de clientes é eliminado. É anônimo. Lá
vai ser serviços que desejo dessas vantagens, o suficiente
para suporte digital, caixa de infra-estrutura. [Eric Hughes,
Cypherpunks lista, 1994-08-03]

12.11. Comércio na Internet
12.11.1. Esta tem sido uma cerveja tópico para os últimos dois anos.
Em 1994 coisa aquecido em várias frentes:
- DigiCash anúncio
- NetMarket anúncio
- vários outros sistemas, incluindo Visto de Bolsa Eletrônica
12.11.2. Eu não tenho nenhuma idéia de quais vai ter sucesso...
12.11.3. NetMarket
- Mosaico de conexões, usando PGP
+ "O NetMarket Empresa está oferecendo agora criptografadas PGP Mosaico
sessões de forma segura para a transmissão de informações de cartão de crédito
através da Internet. Peter Lewis escreveu um artigo sobre
NetMarket na página D1 de hoje do New York Times (8/12/94).
Para obter mais informações sobre NetMarket, ligue para

http://www.netmarket.com/ ou telnet netmarket.com." [
Cara, H. T. Haskin <guy@netmarket.com>, 1994-08-12]
- Usa PGP. Aclamado pelo NYT, como o primeiro grande uso de
criptografia para alguma forma de dinheiro digital, mas isso não é
corrigir.

12.11.4. CommerceNet

- permite que os usuários da Internet para comprar e vender mercadorias.
- "Eu li ontem do L. A. Times sobre algo chamado
CommerceNet, onde vendedores e compradores de estação de trabalho de nível
o equipamento pode atender e realizar busniess....Perto do fim do
o artigo, eles falaram sobre uma proposta de método para
a troca de "assinaturas digitais", através de Moasic (de modo que os compradores
e os vendedores poderiam _know_ que eles estavam que eles disseram que
foram) e que eles estavam indo para "enviar-lo para o
Os Padrões da Internet corpo"" [Cypher1@aol.com, 1994-06-23]

12.11.5. EDI, ordens de compra, documentação de redução, etc.

- Nick Szabo é um fã desta abordagem

12.11.6. abordagens

- enviar números de VISTOS em correio normal....obviamente inseguro
- enviar números de VISTOS no e-mail criptografado
+ estabelecer duas vias de compensação protocolos
- a melhor forma de garantir que o destinatário vai cumprir serviço como...
uma confirmação de que o cliente assinar (em vez de "sig tomadas
sobre o telefone" abordagem)
- várias formas de dinheiro digital

12.11.7. leve vs. pesado processos para o comércio na Internet

- Chris Hibbert
- e o recorrente problema da centralização versus descentralização
autenticação e certificação

12.12. Cypherpunks (Experiências De"Magia"De Dinheiro)

12.12.1. O que é Magia Dinheiro?

- "A magia do Dinheiro é um sistema de dinheiro digital projetado para uso sobre
correio eletrônico. O sistema é on-line e rastreáveis.
On-line significa que cada transação envolve uma troca
com um servidor, para evitar a dupla de gastos. Untraceable
significa que é impossível para qualquer um de rastreamento
transações, ou para corresponder a uma retirada com um depósito, ou
para combinar duas moedas de qualquer forma."

"O sistema consiste em dois módulos, o servidor e o
o cliente. Magia Dinheiro utiliza o PGP ascii-blindado mensagem
formato para todas as comunicações entre o servidor e o cliente.

Todo o tráfego é criptografado, e as mensagens do servidor para
o cliente são assinados. Untraceability é fornecida por um
Chaum-estilo cego assinatura. Observe que o cego assinatura
é patenteada, como é o RSA. Usando-o para fins experimentais
só não deve ter problemas.

"Digicash é representado por discreta moedas, o
denominações dos quais são escolhidos pelo operador do servidor.
As moedas são RSA-assinado, com um email diferente/d para cada par
denominação. O servidor não armazena qualquer dinheiro. Todos
as moedas são armazenados pelo módulo cliente. O servidor aceita
moedas antigas e cegos sinais de novas moedas, e verifica o
antigos em um gasto lista."
[...resto de excelente resumo pronunciado...altamente recomendado
que você desenterrá-lo (arquivos, Web site?) e ler]
[Pr0duct Cypher, Magia Dinheiro Digicash Sistema, 1992-02-04]
+ Magia Dinheiro
- ftp://csn.org/pub/mpj/crypto_XXXXXX (ou algo parecido
que) <Derek Atkins, 4-7-94>
- ftp:csn.org//mpj/I_will_not_export/crypto_???????/pgp_too
ls <Michael Paul Johnson, 4-7-94>
12.12.2. Matt Thomlinson experimentou um derivado versão chamada
"GhostMarks"
12.12.3. houve, também, um "Brega Tokens" derivados
12.12.4. Problemas típicos com Tais Experiências de
- Não vale nada...fazer o dinheiro significativa é um
obstáculo a ser superado
- Se vale nada, não vale a pena o esforço considerável para usar
ele ("criar a Magia do Dinheiro de clientes" e outros assustador Unix
coisas!)
- robustez...sites de ir para baixo, etc.
- mesmo problemas foram vistos em Extropians lista com "HEx"
de câmbio e de sua moeda, o "thorne." (Eu mesmo pago real
dinheiro para Edgar Swank para comprar alguns thorned..., enfim, o mercado
era muito fina negociados e os thornes me fez nenhum bem.)

12.13. Questões práticas e Preocupações com Dinheiro Digital
12.13.1. "É físico prova de identidade necessário para linha de limpeza?"
- Não, se o dinheiro do outlook é executada. Dinheiro é dinheiro. Ressalva
emptor.
- O "primeiro para o armário" abordagem faz com que o banco não
particularmente preocupado com isso, como um banco Suíço vai
permitir o acesso a uma conta numerada pela apresentação do

número, e talvez uma chave. Prova de identidade *pode* ser necessário,
de acordo com o "protocolo" eles e o cliente
estabelecida, mas não precisa ser. E a última coisa que o
banco está preocupado é ser capaz de "encontrar e julgar"
ninguém, como não há nenhuma maneira que eles possam ser responsáveis por um quarto duplo
gastos do incidente. As belezas do local de compensação! (Que
é o que as moedas de ouro de fazer, e o papel-moeda se realmente pensamos
podemos passar isso para os outros.)

12.13.2. "É dinheiro digital rastreáveis?"

- Existem vários tipos de "dinheiro digital," que vão desde
versões de cartões VISA completamente indetectáveis (Chaumian)
dinheiro digital.
- Isso vem um monte, com as pessoas na Net grupos de notícias ainda
aviso aos outros para não usar dinheiro digital devido a facilidade
de rastreabilidade. Não é assim.
- "Não é o tipo proposto por David Chaum e seus colegas, em
os países baixos. Todo o impulso de suas pesquisas sobre
a última década tem sido o uso de criptografia
técnicas para efectuar transacções electrónicas seguras, a partir de
fraude, enquanto, ao mesmo tempo, protegendo a privacidade pessoal.
Eles, e outros, têm desenvolvido uma série de esquemas para
UNTRACEABLE dinheiro digital." [Kevin Van Horn,
falar.política.crypto, 1994-07-03]

12.13.3. "Existe o perigo de que as pessoas vão perder os números que
eles precisam resgatar o dinheiro? Que alguém poderia roubar o
número e, assim, roubar seu dinheiro?"

- Com certeza. Há o perigo de que eu vou perder o meu obrigações ao portador, ou
esqueça meu Suíço, número de conta bancária, ou perder o meu tesouro
mapa para onde eu sepultei o meu dinheiro (como Alan Turing, supostamente,
fez na segunda guerra mundial).
- As pessoas podem tomar medidas para limitar o risco. Mais seguro de computadores.
Dongles usado ao redor de seus pescoços. Protocolos que envolvem
autenticação biométrica para seu computador local ou chave
armazenamento de PDA, etc. Limites de saques por dia, etc.
As pessoas podem armazenar números chaves com pessoas de confiança,
talvez criptografados com outras teclas, pode deixá-los com
de seus advogados, etc. Todos os tipos de arranjos podem ser feitos.
De identificação pessoal, mas é um destes mecanismos.
Usado frequentemente, mas não é essencial para o underlyng protocolo.
Novamente, os bancos Suíços (talvez agora o Liechtenstein
anstalts são um exemplo melhor) não necessitam de física ID
para todas as contas. (Mais geralmente, se Charles quer

criar um banco onde são feitos depósitos e, em seguida, dado
a primeira pessoa que canta tom certo, por que devemos
cuidados? Esse exemplo extremo, é útil apontar que
contractual arrangements não precisa envolver entidades governamentais ou de
as normas sociais sobre o que constitui prova de identidade.)

12.14. Ciberespaço e Dinheiro Digital

12.14.1. "Você não pode comer o ciberespaço, então, o que é bom digitais dinheiro?"
- Isso vem um monte. As pessoas assumem que não é prático
forma de transferência de bens, quando na verdade ele é feito todo o
em tempo. Isto é, os fluxos de dinheiro do domínio puramente
"informativa" reino para o physcial reino Consultores,
escritores, comerciantes, etc., todos usam suas cabeças e, assim,
ganhar dinheiro real.
- Mesmo se aplica ao ciberespaço.

12.14.2. "Como posso manter-se anônimo quando compra itens físicos usando
anônimo dinheiro digital?'
- Muito difícil. Uma vez que você está visto, e sua imagem pode ser
tomadas(talvez desconhecido para você), bancos de dados terão de você.
Não muito pode ser feito sobre isso.
- As pessoas têm esquemas propostos para anônimo embarque e
pickup, mas o simples fato é que a entrega física de qualquer
classificação compromete o anonimato, assim como no mundo de hoje.
- A finalidade do anônimo dinheiro digital é, em parte, pelo menos,
torná-lo mais difícil, para não dar Big Brother seu
itinerário detalhado de estrada com portagem movimentos, teatro, cinema,
pagamentos, etc. Na medida em que a física pode câmeras
ainda rastrear carros, pessoas, envios, etc., anônimo
dinheiro digital não resolve este vigilância problema.

12.15. Proibição de Dinheiro

12.15.1. "Quais são as motivações para a proibição do dinheiro?"
- (Nota: Isso não aconteceu. Muitos de nós ver sinais de que
acontecendo. Outros são céticos.)
+ Motivos para a Eliminação do Dinheiro:
- A guerra às Drogas....precisa dizer mais?
- superfície de economia subterrânea, através da retirada de papel
moeda e forçando todo o tipo de transacção monetária em formulários
que pode ser facilmente controlado, regulado e a tributação.
- evasão fiscal, sob a tabela economia (poderia também ser
motivo para inviolável de caixas registradoras, com o lugar
verificações para garantir a conformidade)
+ bem-estar, invalidez, pensões, segurança social, auto-

depósitos
a fraude, double-dipping
- redução de roubo de bem-estar cheques, pagamentos de incapacidade,
etc....um problema em algumas localidades, e automáticas
depósito/dinheiro cartão de abordagens estão sendo avaliados.
- redução geral de roubo, batedores de carteira
- redução da burocracia: todas as transferências electrónicas (poderia
ser parte de uma "reinvenção do governo", iniciativa)
+ imigrantes ilegais, bem-estar, cheats, etc. Dar a cada um
Carteira de Identidade nacional (eles vão chamá-lo de algo
diferente. para torná-lo mais palatável, tais como "Social -
Serviços Portátil de Inventário da Unidade" ou "Direitos de Saúde
O documento").
- (Ligações Nacionais Cartão de Cuidados de Saúde, ao bem-estar do Cartão,
para outros I. D. esquemas projetados para reduzir a fraude, faixa
cidadão-unidades, etc.)
+ de sistemas de racionamento que dependem não-transacções de dinheiro
(como foi explicado anteriormente, as distorções do mercado de
o racionamento de sistemas, em geral, requerem a identificação,
correlação para pessoa ou de um grupo, etc.)
- este racionamento pode incluído preços subsidiados, a negação
de acesso (por exemplo, certos alimentos negado a determinados
pessoas)
12.15.2. Para que isto não ser considerado um paranóico ranting, deixe-me salientar
que muitas ações já foram tomadas, o que limita a forma
de dinheiro (leis bancárias, lavagem de dinheiro, moeda
restrições...mesmo a proibição de competir moedas
próprio)
12.15.3. Perigos da proibição do dinheiro
- Gostaria de congelamento todas as transações, dando-Big Brother
poder sem precedentes (a não ser que o dinheiro formulários foram
anônimo, a la Chaum e os sistemas de suporte)
- Iria permitir a rastreabilidade completa....como o celular
os telefones que tenho Simpson
- 666, Heinlein, Shockwave Rider, etc.
12.15.4. Dado que não existe a exigência de identidade
associado com o dinheiro, devemos lutar contra qualquer sistema que
proposta para ligar os dois.
12.15.5. O valor do pagamento em dinheiro
- faz uma transação puramente local, resolvido no local
- a alternativa, um complicado sistema de contabilidade, envolvendo
outros partidos, etc., é muito menos atraente
- muitas transações estes dias não são mais tratadas em

dinheiro, o que aumenta os custos e obtém outras partes envolvidas
onde eles não deveriam estar envolvidos.

12.15.6. "As pessoas vão aceitar a proibição de dinheiro?"

- Houve um tempo em que eu diria que os Americanos, pelo menos,
teria rejeitado tal coisa. Muitas memórias de
"Papieren, bitte. Macht schnell!" Mas agora eu acho que a maioria dos
Os americanos (e Europeus) são então usados para a produção de
documentos para cada transação, e então utilizado para o VISTO de utilização
cartas e cartões ATM em postos de gasolina, supermercados, e até mesmo
em mercados de pulga, que vai de bom grado, mesmo ansiosamente--
adotar tal sistema.

12.16. Novas Oportunidades

12.16.1. Criptografados livros abertos ou anónimos auditoria

- Eric Hughes trabalhou em um esquema de utilização de um tipo de cegueira
para o fazer "criptografado livros abertos", pelo qual os observadores podem verificar
que um banco é balancear os seus livros sem mais detalhadas
olha para contas individuais. (Eu tenho minhas dúvidas sobre
paródias, ataques, etc., mas estão sempre a ser considerada
em qualquer novo protocolo.)
- "Kent Hastings se perguntou como um banco offshore poderia fornecer
garantias aos depositantes. Eu me perguntava a mesma coisa de alguns
meses atrás, e começou a trabalhar no que Perry chama a
anônimo auditoria problema. Eu tenho o que eu considero ser
o núcleo de uma solução.
...A seguir é longo.... [TCM Nota: Demasiado longo para incluir
aqui. Eu sou incluindo apenas o suficiente para convencer os leitores de que
alguns novos tipos de serviços bancários ideias podem vir de
criptografia.]

"Se a gente usar o conteúdo criptografado livros na
limite organizacional aponta para criar jurídico adequado
opbligations, podemos, principalmente, ignorar o que se passa dentro de
a confusão de números aleatórios. Isto é, mesmo se o dobro de livros
estavam sendo mantidos, as obrigações legais criados devem
o suficiente para garantir que tudo pode ser desfeita, se necessário.
Isso não impede que redes de corromper as empresas de
indo para baixo de uma vez por todas, mas permite a redes de
as empresas honestas para operar com mais segurança de
honestidade." [Eric Hughes, PROTOCOLO: Encriptado Livros Abertos,
1993-08-16]

12.16.2. "Como componentes de software pode ser vendido, e como criptografia
figura?"

+ De Software reutilizáveis, Brad Cox, Sprague, etc.
- bom artigo na "Wired" (repetido em "Fora de Controle")
- Em primeiro lugar, certamente, o software é vendido. O problemas é por isso que o
"componentes de software" mercado ainda não desenvolvido, e por
tais instâncias específicas de software, como a música, a arte, texto,
etc., não foram vendidos em pedaços menores.
+ Comércio na Internet é uma enorme área de interesse, e o futuro
desenvolvimento.
- actualmente a desenvolver-se muito lentamente
- muitas informações conflitantes...várias mailing
listas de lotes de hype...
+ Dinheiro Digital é frequentemente citado como um necessário ativar a ferramenta, mas
Eu acho que a resposta é mais complicada do que isso.
- questões de conveniência
- questões de que não há nenhuma recorrente de mercado (como há
em, digamos, o chip de negócios...de software não ficar comprei
e mais uma vez, na unidade de aumento de volumes)

12.17. Pontas Soltas
12.17.1. Razões para não ter nenhum envolvimento do governo no comércio
- Mesmo uma pequena participação, por meio de regulamentos especiais,
concedido frachises, etc., produz interesses escusos. Para
exemplo, em uma comunidade que tinha de esperar para obter
as licenças de construção quer _others_ esperar o mesmo tempo, ou
mais. Ou, as empresas que tinham que atender a certo padrão,
mesmo se razoável, vai exigir que as novas empresas fazer isso
também. O efeito é sempre um alargamento tar pit de regras,
restrições e atrasos. Distorções de mercado resultado.
+ Olhada em como é difícil para o ex-URSS para
dispensar a partir de 75 anos de planejamento central. Eles
agora são quase totalmente Máfia-estado controlado (por isso eu
significa que a "privatização" de outrora não-privado
empresas se beneficiaram aqueles que acumularam dinheiro e
influência, e que estes foram, principalmente, a Máfia russa e
os antigos ou actuais políticos...a repercussão desta
corrompido "giveaway" serão sentidos nas próximas décadas).
- É um sinal encorajador: O próspero mercado negro na Rússia-
-que todos os Cypherpunks, claro, torcer-se, gradualmente,
deslocar os antigos sistemas de negócios com os novos, como no
todas as economias. Eventualmente, a forma corrupta-comprei empresas
vai afundar ou nadar com base no mérito, e o recém-criado
as empresas vão competir com eles.
12.17.2. "Purista" Abordagem de Chaves, em Dinheiro, a Responsabilidade

+ Existem duas principais abordagens para o problema:
- Proprietário da chave é o responsável por usa de sua chave
- ou, Outros são responsáveis
+ Pode ser misturado situações, tais como quando uma tecla é roubado...mas isso precisa também ser planejado, para por a chave proprietário, através do uso de protocolos que o limite de exposição. Para exemplo, algumas pessoas vão usar uma única chave acessos imediatamente o respectivo património líquido...a maioria das pessoas vai partição a sua exploração e a sua introduzidos de acesso de forma a naturalmente, o limite de exposição se qualquer tecla for perdido ou comprometida. Ou esquecido.
- poderia envolver sua holding bancária, chaves, ou conivência de agentes
- ou n-fora-de-m sistemas de votação
- Contratos são a essência...que contratos de pessoas voluntariamente entrar?
- E localidade--que é melhor para manter as teclas de seguro que o o proprietário? Qualquer coisa que transfere a culpa para "bancos" ou "a sociedade" quebra o ciclo de feedback de responsabilidade, fornece uma "saída" para os mais preguiçosos, e incentiva a fraude (pessoas que repudiar contratos, alegando a sua chave foi roubado).

13. Ativismo e Projetos

13.1. direitos autorais
O CYPHERNOMICON: Cypherpunks FAQ e Mais, Versão 0.666, 1994-09-10, Direitos De Autor Timothy C. De Maio. Todos os direitos reservados. Veja os detalhes de isenção de responsabilidade. Use seções curtas em "justo use" disposições, com crédito apropriado, mas não coloque o seu nome em minhas palavras.

13.2. RESUMO: o Ativismo e Projetos
13.2.1. Pontos Principais
13.2.2. Ligações para Outras Secções
13.2.3. Onde Encontrar Informações Adicionais
13.2.4. Diversos Comentários

13.3. O ativismo é uma Tarefa Difícil
13.3.1. "pastorear gatos"..tentar mudar o mundo através exortação parece particularmente ineficaz noção
13.3.2. Há sempre um monte de desperdício de tempo e a retórica do Cypherpunks lista como várias pessoas tentaram fazer com que os outros siga a sua liderança, para adotar a sua visão. (Nada de errado com

isso, se feito corretamente. Se alguém leva, por exemplo, ou tem um particularmente interessante visão ou plano, este pode, naturalmente, acontecer. Muitas vezes, porém, a situação era que alguém vaga planos para um produto em que foram declaradas por eles para ser o normas que outros devem seguir. Vários esquemas para dinheiro digital, em muitos formas e modos, sempre foi o exemplo claro disto.)

13.3.3. Isso está relacionado também ao que Kevin Kelley chama de "fax efeito." Quando algumas pessoas possuem máquinas de fax, eles não são de muito uso. Tentando usar as mesmas ferramentas que um tem é como tentar convencer as pessoas a comprar máquinas de fax, de modo que você pode se comunicar por fax com eles...pode acontecer, mas provavelmente, por outras razões. (Felizmente, a interoperabilidade dos PGP fornecido um meio de comunicação comum que tinha sido falta anteriores plataforma específica de codificação de programas).

13.3.4. Utópico esquemas são também uma venda difícil. Esquemas sobre o uso de dinheiro digital para fazer a inflação impossível, esquemas para recolher impostos com sistemas anónimos, etc.

13.3.5. Harry Browne, "Como eu Encontrei a Liberdade em um Unfree Mundo" é vale a pena ler; ele aconselha ficar chateado e frustrado de que o mundo não é o movimento em direção a um gostaria.

13.4. Cypherpunks Projetos

13.4.1. "O que são Cypherpunks projetos?"

- Sempre uma parte fundamental--talvez _the_ parte fundamental--de Cypherpunks a atividade. "Cypherpunks escrever código." Do trabalho sobre o PGP para remetentes para conjuntos de ferramentas de criptografia para pedidos FOIA, e um monte de outras coisas, Cypherpunks hackear o sistema em vários maneiras.
- Matt Blaze do soprador de FOLHAS, Phil Karn "deslize" do sistema, Peter Wayner de artigos....todos são exemplos. (Muitos Cypherpunks os projetos são, também, ou principalmente, por outros motivos, portanto, não é possível em todos os casos, solicitar o crédito para este de trabalho.)

13.4.2. Extensões para PGP

13.4.3. Propagação do PGP e criptografia em geral.

- educação
- disquetes contendo ensaios, programas
- sites de ftp
- raves, convenções, encontros

13.4.4. Remetentes

+ ideal Chaumian mistura tem determinadas propriedades

- latência para a folha de análise de tráfego
- criptografia
- não há registros mantidos (violação do hardware de resistência, etc.)
- Cyperpunks remetentes
- julf remetentes
+ abusos
- inundações, porque a transmissão de email custos não são suportados por remetente
+ anonimato produz potencial para abusos
- ameaças de morte, extorsão
- O progresso continua, com novos recursos adicionados. Ver o a discussão em remetentes seção.

13.4.5. Steganography

- ocultar a existência de uma mensagem, ao menos para algumas quantidade de tempo
- segurança através da obscuridade
- tinta invisível, micropontos
+ Usa
- em caso de criptografia é outawed, pode ser útil para evitar autoridades
- se um número suficiente de pessoas fazem isso, aumenta a dificuldade de aplicação de anti-crypto leis (todos os
+ Stego
- JSTEG: soda.berkeley.edu:/pub/cypherpunks/aplicativos/jsteg
- Stego: sumex-aim.stanford.edu

13.4.6. Anônimo Sistemas De Transação

13.4.7. Encriptação de voz, Voz PGP

- Clipper, ficando o gênio fora da garrafa
- CELP de compressão, DSPs
- SoundBlaster abordagem...não pode ter o suficiente de processamento de alimentação
+ hardware versus software puro
- novos Macs, incluindo av Macs e Sistema 7 Pro, tem interessante recursos
+ Zimmermann planos de ter sido amplamente divulgada, de que ele é olhando para as doações, que ele está buscando a ajuda de programação, etc.
- o que não augura nada de bom para ver como um produto a partir de ele
- francamente, eu esperava que ele vai vir de alguém
- Eric Flor está perseguindo o próprio hardware da placa, com base no 2105
+ "É a pessoa de construção encriptado telefones?"

-
+ Sim, vários projetos estão em andamento. Eric Flor
o mesmo mostrou uma
- PCB de um em um Cypherpunks reunião, usando um
baratos chip DSP.
-
+ De Software-apenas versões, com alguns compromissos em discurso
qualidade
- provavelmente, também estão em andamento. Phil Zimmermann
descreveu o seu progresso em
+ o último Cypherpunks reunião.
-
- ("Software" só pode significar uso off-the-shelf, amplamente
disponível DSP
+ placas de como SoundBlasters.)
-
- E eu sei de pelo menos mais dois projectos.
Se qualquer um vai
+ materializar ninguém sabe.
-
- E vários hacks já foi feito. Próximo usuários
tiveram
- correio de voz por anos, e determinadas Macs agora oferecer
algo similar.
+ Adição de criptografia não é um obstáculo enorme.
-
- Há um ano, vários Cypherpunks sites de reunião em torno de
os EUA foram
- ligados através da Internet utilizando a encriptação DES. O
qualidade do som era
- pobres, por várias razões, e nós desligamos o DES
em questão de
- minutos. Ainda, um criptografada chamada de conferência de áudio.
13.4.8. DC-Redes
- O que é, como funciona
- Chaum completa de 1988, "Jornal da Criptologia" artigo
disponível no Cypherpunks site de arquivamento,
ftp.soda.csua.edu em /pub/cypherpunks
+ De jantar Criptógrafos Protocolos, aka "DC Redes"
+ "O que é o Jantar Criptógrafos Problema, e por que é
tão importante?"
+ Esta é tratada na seção principal, mas aqui está
David Chaum Abstrata, a partir de sua 1988 papel"

- Resumo: "Manter confidenciais quem envia o que
mensagens, em um mundo onde qualquer físico de transmissão
pode ser rastreado até sua origem, parece impossível. O
a solução aqui apresentada é incondicionalmente ou
criptograficamente segura, dependendo se ele é
com base em um tempo de uso de chaves ou chaves públicas.
respectivamente. Ele pode ser adaptado para endereço
eficientemente uma grande variedade de práticas
considerações." ["O Jantar Criptógrafos Problema:
Incondicional do Remetente e do Destinatário Untraceability,"
David Chaum, Diário da Criptologia, I, 1, 1988.]
-
- DC-redes não foram implementados, tanto quanto eu sei,
mas eles representam um "puro", versão de física
remetentes estamos todos tão familiarizados com o agora. Um dia
eles vão ter um grande impacto. (Eu sou um grande fã de
este trabalho do que muitos parecem ser, como há pouco
discussão no sci.cripta e afins.)
+ "O Jantar Criptógrafos Problema: Incondicional Remetente
e o Destinatário Untraceability," David Chaum, Diário de
Criptologia, I, 1, 1988.
- disponível de cortesia das Informações da Frente de Libertação de
no soda.csua.berkeley.edu site
- Resumo: "Manter confidenciais quem envia o que
mensagens, em um mundo onde qualquer físico de transmissão
pode ser rastreado até sua origem, parece impossível. O
a solução aqui apresentada é incondicionalmente ou
criptograficamente segura, dependendo se ele é
com base em um tempo de uso de chaves ou chaves públicas.
respectivamente. Ele pode ser adaptado para lidar de forma eficiente com
uma grande variedade de considerações de ordem prática." ["O
Jantar Criptógrafos Problema: Incondicional do Remetente e
Destinatário Untraceability," David Chaum, Diário de
Criptologia, I, 1, 1988.]
- Nota-se que as iniciais "D.C." tem várias relacionados
significados: Jantar Criptógrafos, Dinheiro Digital/DigiCash,
e David Chaum. Coincidência?
+ Informal Explicação
- Nota: eu já postei essa explicação, e variantes,
várias vezes desde que eu escrevi em meados de 1992. No
verdade, eu postei sobre o "Extropians" mailing
lista, como "Cypherpunks" não existe.
- Três Cypherpunks está jantando, talvez em Palo

O Alto. Seu garçom diz que o projeto de lei tem
já foram pagos, seja pela ANS, ou por um deles.
O garçom não dizer mais. Os Cypherpunks gostaria de saber
se um deles pagos, ou a NSA pago. Mas eles
não quero ser indelicado e forçar o Cypherpunk
pagador para o 'admitir, então, que realizam este protocolo (ou
procedimento):

Cada Cypherpunk vira uma moeda boa por trás de um menu colocado
vertical entre ele e o Cypherpunk em seu
direito. A moeda é visível para si E para o
Cypherpunk à sua esquerda. Cada Cypherpunk pode ver o seu próprio
moeda e a moeda de seu direito. (PARE AQUI!
Por favor, tome o tempo para fazer um esboço da situação
Eu descrevi. Se você perdeu, aqui, tudo o que segue
vai ser um borrão. É muito ruim o estado da rede hoje
não suporta figuras e diagramas facilmente.)

Cada Cypherpunk, em seguida, informar em voz alta se os dois
moedas que se pode ver são os MESMOS ou são DIFERENTES, por exemplo,
"Cabeças-Caudas" significa DIFERENTES, e assim por diante. Por agora,
suponha que o Cypherpunks são verdadeiras. Um pouco de
o pensamento mostra que o número total de "DIFERENÇAS"
deve ser 0 (moedas de todos vieram do mesmo), ou
2. Paridade ímpar é impossível.

Agora, os Cypherpunks concorda que se um deles pago, ele
ou ela vai DIZER O CONTRÁRIO do que eles realmente ver.
Lembre-se, eles não anunciam que sua moeda virou até
como, só se era o mesmo ou diferentes como a sua
vizinho.

Suponha que nenhum deles paga, por exemplo, a ANS pago. Em seguida,
todos eles relatam a verdade e a paridade é mesmo
(0 ou 2 diferenças). Eles, então, saber o NSA
pagos.

Suponha que um deles pagou a conta. Ele relata a
o oposto do que ele realmente vê, e a paridade é
de repente, estranho. Isto é, há 1 diferença relatou.
Os Cypherpunks, agora sabemos que um deles pagos. Mas pode
eles determinar o que?

Suponha que você é um dos Cypherpunks e você sabe que você
não pagar. Um dos outros dois fez. Você quer
comunicado IGUAIS ou DIFERENTES, com base no que o seu vizinho
para a direita (cuja moeda que você pode ver) tinha. Mas você
não posso dizer qual dos outros dois está mentindo! (Você pode
ver você do lado direito do vizinho moeda, mas você não pode ver
a moeda que vê à sua direita!)

Tudo isso generaliza para qualquer número de pessoas. Se nenhum
eles pagos, a paridade é mesmo. Se um deles pagos,
a paridade é ímpar. Mas qual deles pago não pode ser
deduziu. E deve ficar claro que a cada rodada pode
transmitir um pouco, por exemplo, "eu pago" é um "1". Mensagem
"Ataque ao amanhecer" poderia, assim, ser "enviado" untraceably com
várias rodadas de protocolo.
- A "Criptografia de Ouija Board": eu explicar isso para o povo como um
espécie de tabuleiro de ouija. Uma mensagem, como "eu pago" ou mais
interessante "Transferir fundos a partir....," apenas "emerge"
fora do grupo, com nenhum meio de saber onde ele
veio. Verdadeiramente surpreendente.
+ Problemas e Armadilhas
- No Chaum do papel, a explicação acima é dado
rapidamente, em poucas páginas. O _rest_ do papel é
dedicada a lidar com as muitas "armadilhas" e
os ataques que vêm e que devem ser tratadas antes de
a DC protocolo é remotamente possível. Eu acho que todos
os interessados em design de protocolo deve ler este
de papel, e o siga-nos documentos por Bos, Pfitzmann,
etc., como objeto de lições para lidar com complexos de criptografia
protocolos.
+ O Problemas:
- 1. O conluio. Obviamente, os Cypherpunks pode compactuar
para deduzir o pagador. Este é o melhor tratado com
a criação de vários subcircuitos (grupos a fazer o
protocolo que entre si). Muitas mais coisas aqui.
Chaum dedica a maior parte do papel para este tipo de
questões e suas soluções.

2. Com cada rodada do presente protocolo, um único bit é
transmitida. O envio de uma mensagem longa significa que muitas moeda
vira. Em vez de moedas e menus, os vizinhos
gostaria de trocar listas de números aleatórios (com o
direito parceiros, conforme o protocolo acima, é claro.

Detalhes são fáceis de descobrir.)

3. Desde que as listas são, essencialmente, as one-time pads, o
o protocolo é incondicionalmente segura, i.é., não
suposições são feitas sobre a dificuldade de
fatoração de grandes números ou quaisquer outros crypto
pressupostos.

4. Os participantes em um tal de "DC-Net" (e aqui estamos nós
chegando ao coração da "criptografia anarquia" idéia)
poderia trocar de CD-ROMs ou DATs, dando-lhes o suficiente
"lançamentos" para zilhões de mensagens, todos os
untraceable! A logística não são simples, mas um
pode imaginar dispositivos pessoais, como cartão inteligente ou
O Apple Newton," que pode lidar com esses protocolos
(primeiras aplicações poderão ser para untraceable
brainstorming comentários, seguro de voto em institucionais
definições, etc.)

5. As listas de números aleatórios (lançamentos) pode ser
gerado com o padrão de métodos de criptografia,
requer apenas uma chave para ser trocado entre o
participantes adequados. Isso elimina a necessidade
para a one-time pad, mas significa que o método é agora
só criptograficamente segura, o que é muitas vezes
suficientes. (Não acho que "só criptograficamente
seguro" significa insegura....as mensagens podem permanecer
encriptado para os próximos bilhões de anos)

6. Colisões ocorrem quando vários são enviadas mensagens
ao mesmo tempo. Vários esquemas podem ser concebidos para
lidar com isso, como fazer logoff quando você detectar outro
remetente (mesmo quando a paridade é visto em vez de estranho
paridade). Em grandes sistemas, isto é, provavelmente, uma
problema. Deliberada interrupção, ou a prática de spam, é uma
grande problema--um disruptor pode desligar o DC-net
através do envio de bits de saída. Como com remailes, o anonimato
significa liberdade de detecção. (Anônimo pagamentos para
enviar uma mensagem pode ajudar, mas os detalhes são obscuro para
a mim.)
+ Usa
- * Untraceable mail. Útil para evitar a censura, para
evitando ações judiciais, e para todos os tipos de criptografia anarquia

coisas.
- * Totalmente anônimo quadros de avisos, sem rastreabilidade
de postagens ou respostas. Materiais ilegais pode ser
oferecidos para venda (meu 1987 exemplo canônico, que
assustou algumas pessoas: "Stealth bomber projetos
para a venda. Post oferta mais alta e incluir chave pública.").
Pense por alguns minutos sobre isso e você vai ver o
implicações profundas.
- * Descentralizada nexo de atividade. Desde mensagens
"emergir" (a la tabuleiro de ouija metáfora), não há
central área de postagem. Nada para o governo
desligar, completa deniability pelos participantes.
- * Só você sabe o que seus parceiros estão....em qualquer dado
circuito. E você pode estar em tantos circuitos como você
deseja. (O pagamento pode ser feito para os outros, para criar uma
fins lucrativos. Eu não sei lidar com esse problema, ou com
o problema de como as reputações são tratados, aqui.)
- Deve ficar claro que a DC-redes oferecem alguns dos incríveis
oportunidades. Eles não foram implementadas, e
ter recebido quase nenhuma atenção comparado ao normal
Cypherpunks remetentes. Por que isso? Programação
a complexidade (e a base de criptografia primitivos
que são necessários) parece ser a chave. Diversos grupos têm
anunciou planos para imlement alguma forma de DC-net, mas
nada apareceu.
- software versus hardware,
- Yanek Martinson, Strick, Austin grupo, Rishab
- IMO, este é o projeto ideal para testar a eficácia de
conjuntos de ferramentas de software. As primitivas necessárias, incluindo bit
compromisso, sincronização, manipulação e conspiração, são
testes severos de sistemas de criptografia. Em contrapartida, eu duvido
que mesmo o Pfaltzmans ou Bos tem puxou uma execução
simulação de...
13.4.9. D-H sockets, no UNIX, deslize o dedo para
+ deslize
- Matt Blaze, João I. de did (codificação), Phil Karn, Perry
Metzger, etc. são as principais pessoas envolvidas
- evoluiu a partir de "mobile IP", com links de rádio, encaminhamento
- redes virtuais
- colocando a criptografia no nível do IP, de forma transparente
- ignorando as fronteiras nacionais
- Karn
- em soda site

+ deslize do sistema, para o encaminhamento de pacotes
- de ponta a ponta, gateways, links, Mach, SunOS
13.4.10. Dinheiro Digital, Bancos, Cooperativas De Crédito
- Magia Dinheiro
- Banco Digital
- "Abrir Encriptado Livros"
- não é fácil para fazer...as leis, regulamentos, especialização em banking
- falhas técnicas, problemas de dinheiro digital
+ várias abordagens
- limpeza de
- tokens, selos ou cupons
- o anonimato protegidos por transações
13.4.11. Dados Paraísos
+ informações financeiras, relatórios de crédito
- ignorando jurisdições locais, prazos, regras arcanas
- reputação
- insider trading
- médico
- técnicos, científicos, patentes
- criptografia de informações (recursivamente o suficiente)
- não precisa ser conhecido localização....distribuído em
ciberespaço
- Um dos mais comercialmente interessante aplicações.
13.4.12. Tecnologias Relacionadas
- Agorics
- Evolutiva De Sistemas De
- Realidade Virtual e Ciberespaço
- Agentes de
+ De Segurança Do Computador
+ Kerberos, o Gnu, palavras-passe
- polêmica recente
- demônio instalado para visualizar os pacotes
- Cygnus irá liberá-lo de graça
- GuardWire
+ Van Eck, HERF, EMP
- Uma vez Cypherpunk projeto proposto logo no início foi a
duplicação de certas NSA recursos para monitorar
de comunicações electrónicas. Isso envolve "van Eck"
radiação (RF) emitida pela Crt e outros aparelhos eletrônicos
de computadores.
+ Provavelmente, por várias razões, este não tem sido perseguido,
pelo menos não publicamente.
- legalidade

- custos
- dificuldade em encontrar alvos de oportunidade
- não muito CPish projeto!

13.4.13. Matt Blaze, AT&T, vários projetos

+ um modelo diferente de confiança...múltiplos universos
- não heierarchical interfaces, mas a desconfiança de interfaces
- heterogêneos
- onde colocar criptografia, onde a desconfiança, etc.
+ quer criptografia no nível mais baixo possível
- quase tudo o que deve ser desconfiavam
- todos desconfiavam da interface deve ser criptograficamente protegido...de autenticação, criptografia
+ "páginas em preto"---suporte para criptografia de comunicação
- "páginas de cor"
- um conjunto de serviços de rede que identiy e entregar informações de segurança, conforme necessário....chaves, que ele confia, protocolos, etc.
+ front-end: API de alto nível para requisitos de segurança
- como o DNS? o cache de modelos?
- locais de confiança de agente....
+ "as pessoas não nasceu ainda" (fitas de backup de Internet comunicações)
- fitas armazenadas em montanhas, o acesso muito mais poderoso computadores
+ "Crytptographic de Sistema de Arquivo" (CFS)
- criptografia de arquivo
- não existe um único modo de DES parece ser adequada...uma mistura de modos de
+ deslize do sistema, para o encaminhamento de pacotes
- de ponta a ponta, gateways, links, Mach, SunOS

13.4.14. Conjuntos De Ferramentas De Software

+ Henrique Strickland do TCL baseado no kit de ferramentas de criptografia para
- outros Cypherpunks, incluindo Hal Finney e Marianne Mueller, manifestaram opiniões positivas de TCL e TCL-TK (toolkit)
- Pr0duct Cypher toolkit
- C++ Bibliotecas De Classe
- VMX, Visual Basic, Visual C++
- Smalltalk

13.5. As respostas para Nossos Projetos (Ataques, Desafios)

Submenu inverter 13.5.1. "O que são as prováveis atitudes em relação ao mainstream Cypherpunks

projetos, tais como remetentes, criptografia, etc.?"
- Reação já foi amplamente favorável. Jornalistas
como Steven Levy, Kevin Kelly, João conclui markoff, e Juliano
Dibbell ter escrito favoravelmente. Reação de pessoas que eu tenho
falou também tem sido amplamente favorável.
13.5.2. "O que são as prováveis atitudes em relação a mais outre
projetos, tais como dinheiro digital, criptografia anarquia, dados paraísos,
e como?"
- Consternação é muitas vezes encontrou-se. As pessoas estão com medo.
- Os jornalistas que escreveram sobre essas coisas (os
mencionado acima), além de ter ficado com a reação inicial
e parecem genuinamente intrigado com as alterações que são
vinda.
13.5.3. "Que tipos de _attacks_ que podemos esperar?"
+ Depende de projetos, mas alguns tipos de ataques
é provável. Alguns já ocorreu. Exemplos:
* inundações de remetentes, ataques de negação de serviço-para
pântano sistemas e força de remetentes para reconsiderar
operações
- este é fixa (principalmente) com o "digital postagem" (se
postagem cobre os custos e gera um lucro, então o
mais, melhor)
* deliberadamente ilegal ou malicicious mensagens, como
ameaças de morte
- projetado para colocar legais e de sysop pressões sobre o
reenvio de e-mails operador
- vários remetentes foram atacados este caminho, ou pelo
menos ter tido essas mensagens
- fonte de bloqueio às vezes funciona, embora não seja claro
se outro reenvio de e-mails é usado pela primeira vez (de muitas questões aqui)
* a instauração de processo para o conteúdo dos posts
+ violações de direitos autorais
- por exemplo, o encaminhamento de Clarinete artigos através de Hal
Finney do reenvio de e-mails tem Brad Templeton para escrever aviso
cartas para Hal
- pornografia
- ITAR violações de Comércio com o Inimigo Agir
- espionagem, sedição, traição
- segredos empresariais,de
- Esses ataques irão testar o compromisso e a coragem de
reenvio de e-mails ou de anonimato dos operadores de serviço

13.6. A Implantação De Criptografia

13.6.1. "Como pode Cypherpunks divulgar criptografia e PGP?"
- artigos, editoriais, programas de rádio, conversar com os amigos
- O Líquido em si é provavelmente o melhor lugar para divulgar o
problemas com o Clipper e chave de caução. O Líquido desempenhou um
papel importante-talvez o papel dominante--na geração de desprezo
para Clipper. Em muitos maneira os temas debatidos aqui na Net
têm uma enorme influência sobre a mídia de reação, em editoriais,
sobre a organização reações, e, claro, na opinião
de técnicos, pessoal. A notícia se espalha rapidamente, zilhões de
teorias são discutidas e debatidas, e o consenso tende a
surgem rapidamente.
- raves, Draper
- Libertário Partido, anarquistas...
+ de conferências e feiras
- Avakov Ray Arachelian passou disquetes no PC Expo
13.6.2. "Quais são os obstáculos a uma Maior Utilização de Criptografia
(Culturais, Éticas, Jurídicas)?"
+ "É muito difícil de usar"
- vários protocolos (considerar apenas o quão difícil é
na verdade, enviar mensagens criptografadas entre as pessoas de hoje)
- a necessidade de se lembrar de uma senha ou frase de acesso
+ "É muito trabalho"
- o argumento de que as pessoas não se preocupam em usar
palavras-passe
- em parte, porque não acho que nada vai acontecer
eles
+ "O que você tem a esconder?"
- por exemplo, imagine alguns comentários que eu gostaria de ter ficado com a Intel tinha
Eu encriptado tudo
- e os governos tendem a ver a criptografia, ipso facto,
a prova de que as ilegalidades estão sendo cometidos: drogas, dinheiro
lavagem de dinheiro, evasão de divisas
- lembre-se o "confisco" controvérsia
- BTW, anônimo sistemas são essencialmente o final de mérito
sistema (no sentido óbvio) e para voar na cara da
"a contratação pelos números" de facto o sistema de quotas agora
creeeping em tantas áreas da vida....pode haver regras
exigir que todos os negócios para manter o controle do sexo,
a raça e a "capacidade de grupo" (eu estou brincando, eu espero) de seus
empregados e seus consultores
+ Tribunais Estão ficando para Trás, Estão Superlotadas e não conseguem Lidar
Adequadamente com Novas Questões, Tais como a Criptografia e a Criónica
- o que levanta a questão da "Ciência Tribunal" novamente

- e a migração para o privado adjudicação
- cenário: qualquer ensaios que estão a ser decidido em 1998-9
terá que ter sido iniciado em 1996, e com base na
a tecnologia e as decisões da volta de 1994
+ Governo está tomando várias medidas para limitar o uso de
e encriptação segura de comunicação
- algumas tentativas falharam (S. 266), alguns foram
esqueceu-se, e quase nenhum ainda têm sido testados no
tribunais
- veja as outras seções...
13.6.3. Questões Práticas
- Educação
- Proliferação
- Ignorando As Leis
13.6.4. "Como deve de projetos e progresso melhor maneira de o conseguir?"
- Esta é uma pergunta difícil, que temos vindo a debater-se com uma
par de anos agora. Lotes de abordagens.
- Escrever código
- Organizacional
- Lobby
- Eu tenho que dizer que existe uma síndrome de nós pode provavelmente fazer
w,a Frustrada Cyperpunks Síndrome. Manifestada por alguém
flaming a lista para não saltar para juntar a eles em seu
(normalmente) meia-boca esquema para construir um digitais do banco, ou
escrever um livro, ou o que seja. "Vocês simplesmente não se importam!" é
o costume de chorar. Muitas vezes, esses flamers acabam deixando-o da lista.
- A geografia pode desempenhar um papel, como pessoas de outra forma isolada
áreas parecem ficar mais ligado às suas idéias e, em seguida, obter
irritado quando a lista como um todo não adotá-los (este é
impressão minha, pelo menos).
13.6.5. Crypto enfrenta a complexidade barreira que todas as tecnologias
rosto
- A vida ficou mais complicada em algumas maneiras, mais simples em
outras formas (não temos de pensar sobre culinária, sobre
ferrar os cavalos, sobre o clima, etc.). Criptografia é
actualmente bastante complicado, especialmente se vários
paradigmas são utilizados (criptografia, assinatura, dinheiro, etc.).
- Como uma nota pessoal, eu estou praticamente se afogando em um.c.
adaptadores e cabos de alimentação para computadores, impressoras a laser,
Videocassetes, filmadoras, aparelhos de som portáteis, computadores portáteis,
guitarras, etc. Tudo com uma bateria recarregável tem para
ser cobrado, mas não em excesso, e não é permitida a execução-
para baixo...eu esqueci de ligar no meu antigo Powerbook 100

par de meses, e as baterias de chumbo-ácido saiu na
a mim. Pessoalmente, eu estou afogando nessa porcaria.
- Digo isto só porque eu sinta uma reação
chegando...as pessoas vão dizer "dane-se" para a nova tecnologia que
na verdade, complica sua vida mais do que simplifica
suas vidas. "Crypto ajustes" que gostam de brincar com
"criar um cliente" para jogar com dinheiro digital
continuar a fazê-lo, mas 99% dos procurados, os usuários não.
(Uma nação que não podem-ou não-definir o seu VCR relógio será
dificilmente abraçar a complexidade do dinheiro digital. A menos que
as coisas mudam, e a utilização torna-se tão fácil como usar um caixa eletrônico.)
13.6.6. "Como podemos conseguir mais pessoas para se preocupar com segurança no
geral de criptografia e, em particular?"
- Verdade é, a maioria das pessoas nunca pensa sobre a real segurança. Segurança
os fabricantes têm dito que as melhorias nos cofres foram
impulsionado por taxas de seguros. Um direto de incentivo para gastar mais
dinheiro para melhorar a segurança (custo do seguro < custo de
maior taxa de seguro).

Agora não há quase nenhum incentivo econômico para as pessoas
de se preocupar com a segurança do PIN, sobre a proteção de seus arquivos,
etc. (Bancos de comer os custos e passá-los...qualquer banco, o qual
tentei economizar alguns dólares em perdas exigindo de 10 dígitos
Pinos--que as pessoas gostariam de *escrever* de qualquer maneira!--iria perder
os clientes. Hologramas e imagens em cartões bancários são
acontecendo porque os custos caíram o suficiente.)

Pessoalmente, o meu principal interesse é assegurar os Federais não
diga que eu não posso ter segurança, tanto quanto eu quero comprar. Eu
não compartilhe a preocupação acima citado que nós temos que encontrar
maneiras de dar a outras pessoas a segurança.
- Outros discordam com minha indiferença, apontando que
a obtenção de lotes de outras pessoas para usar criptografia torna mais fácil
para aqueles que já se proteger. Eu concordo, eu só
não se concentrar no trabalho missionário.
- Para aqueles que assim o desejassem, ponto para as pessoas o quão vulneráveis
seus arquivos são, como a ANS pode monitorar a rede, e assim por
em. Todos os habituais histórias assustadoras.

13.7. Ação política e de Oposição
13.7.1. Forte ação política é emergentes na Net
- clique com o botão direito asa teóricos da conspiração, como Linda Thompson
+ Net tem resposta rápida para eventos de notícias (Waco, Tienenmen,

A rússia)
- com histórias, muitas vezes utilizado pelos meios de comunicação (muitos dos repórteres
Líquida, fácil de abater para referências, Net recentemente tornou-se
tres moda)
- Aryan Nation no Ciberespaço
- (Estes desenvolvimentos incomodar muitas pessoas que eu mencioná-los para.
Nada pode ser feito sobre quem usa o forte de criptografia. E mais
fasicst/racista situações são agravadas pelo estado
patrocínio--leis do apartheid, a Alemanha de Hitler, Pol Pot
campos de extermínio, todos foram exemplos de o estado impor
racista, genocida leis. A criptografia inquebrável de que o
Aryan Nation fica é mais do que compensado pelos ganhos
em outro lugar, e o enfraquecimento da autoridade central.)
- mostra a necessidade de uma forte criptografia...mais os governos
infiltrar-se e monitorar esses grupos políticos

13.7.2. Cypherpunks e Esforços de Lobby

+ "Porque não Cypherpunks ter um esforço de lobby?"
+ nós não estamos "centrado", perto de Washington, D.C., o que parece
para ser uma coisa essencial (como com o FEP, ACLU, ÉPICO, CPSR,
etc.)
- D.C. Cypherpunks uma vez se ofereceu (abril, 1993) para fazer
este enfoque especial, mas não muito se tem ouvido
desde. (Para ser justo com eles, a pressão política é
muito longe da maioria dos Cypherpunks interesses.)
- sem orçamento, sem funcionários, sem o office
+ "pastorear gatos" + nº de participações financeiras = por que não fazer
mais
+ é muito difícil de coordenar dezenas de livre-pensamento,
opinativo, pessoas inteligentes, especialmente quando não há
chicote de mão, nenhum incentivo financeiro, não há maneira de forçá-los
em linha
- Eu estou, obviamente, não se defende tal força, apenas observando um
truísmo de sistemas
+ "Deve Cypherpunks defendem a quebra de leis para alcançar
objetivos?"
- "Meu jogo é obter a criptografia disponível para todos, sem
violar a lei. Isso significa lutar contra Clipper, lutando
idiota restrições de exportação, ficando o governo
mudar sua postura em criptografia, através de arguements
e a carta apontando os problemas que Isso significa ...
a escrita ou a promoção de forte cryptography....By violar
a lei, dar-lhes a chance de marca
"criminal" e ignorar a encorajar outras pessoas a ignorar o que

você tem a dizer." [Bob Snyder, 4-28-94]

13.7.3. "Como pode nonlibertarians (liberais, por exemplo) ser convencido da necessidade de uma forte criptografia?"

- "Para os liberais, gostaria de examinar algum animal de estimação causa e examinar as consequências que podem causar a tornar-se ilegal"." Para exemplo, se seus amigos são "pro-choice", você pode perguntar o que fariam se o direito de permanentes proibido o aborto. Será que eles pensam que era errado para uma vítima de estupro para obter um aborto só porque era ilegal? Como seria eles se sentem sobre o aborto "underground railroad" organizado através de uma rede de "estações", coordenado através da Internet usando ilegal "criptografia"? Ou será que eles a confiança Clipper em uma situação como essa?

"Todos na América é apaixonado por algo. Tais a paixão normalmente dispensa com o mero legalismo, quando se trata de para que o crente se sente, é uma questão de fundamental o certo e o errado. Bater-lhes com um argumento que aborda a sua paixão. Criar um pro-crypto argumento de que a ajuda preservar o objeto de sua paixão." [Sandy Sandfort, 1994-06-30]

13.7.4. A tensão Entre os Governos e os Cidadãos

- os governos querem mais acompanhamento...grandes antenas para espionar telecomunicações",
- pessoas que proteger-se, às vezes, são vistos com suspeita
+ - Americanos têm sido geralmente de duas mentes sobre privacidade:
- Nenhum de seus porra de negócios, a casa de um homem é a sua castelo..individualismo áspero, auto-suficiência, o Calvinismo
- O que você tem a esconder? Rastreamento nos vizinhos
+ Esses pontos de vista conflitantes são realizadas simultaneamente, quase como um tensor que não puder ser resolvido para alguns resultante vetor
- esta dicotomia cortes através de decisões judiciais, bem

13.7.5. "Como os Cypherpunks grupo diferem dos grupos de lobby como a FEP, CPSR, e ÉPICO?"

- Estamos mais desorganizado (anárquica), com nenhuma escritório central, não pessoal, não formal, carta, etc.
- E a agenda política dos grupos acima mencionados é muitas vezes em desacordo com a liberdade pessoal. (suporte para o acesso do público programas, subsídios, restrições empresas, etc.)
- Nós também somos uma mais radical do grupo em quase todos os sentidos, com

vários sabores de extremismo político fortemente
representado. Principalmente anarco-capitalistas e forte
libertários, e muitos "sem compromissos" defensores da privacidade.
(Como habitual, as minhas desculpas a qualquer Maoístas ou similares que
não me sinto confortável sendo consideradas em conjunto com o
libertários....se você está lá fora, você não está falando
até.) Em qualquer caso, a casa de Cypherpunks tem muitos quartos.
- Nós fomos chamados "Crypto Rebeldes" de Steven Levy da "Wired"
artigo (questão 1.2, início de 1993). Podemos representar um
radical alternative para o Rodoanel advogados que dominam
FEP, ÉPICO, etc. Não há necessidade de se comprometer em coisas como a
Clipper, a Chave de Software de Caução, Telefonia Digital, e o
NII. Mas, claro, nenhum de entrada para o processo legislativo.
- Mas há muitas vezes uma vantagem de ter muito mais
radical, purista corpo nas asas, fazendo com que o
"rejectionist" caso e mantendo o círculo interno de pessoas para um
mais resistente do padrão de comportamento.
- E, claro, há a onipresente diferença que nós
tendem a favorecer a ação direta, através da tecnologia sobre
politicagem.
13.7.6. Porque é que o controle do governo de criptografia tão perigoso?
+ perigos do monopólio do governo sobre a criptografia e sigs
- pode revogar a sua existência"
- nenhum lugar para escapar (historicamente um importante sociais
válvula de alívio)
13.7.7. NSA vista de criptografia advogados
- "Eu disse para alguém uma vez, esta é a vingança do povo
quem não podia ir para Woodstock, porque eles tinham muito trigonometria
lição de casa. É uma espécie de romantismo sobre a privacidade e o
tipo, você sabe, "você não vai obter minha chave de criptografia até você
retire-o da minha mortos dedos frios" tipo de coisas. Eu tenho que
dizer, você sabe, eu meio que achar que é cativante." [Stuart Baker,
advogado, NSA, PCP '94]
13.7.8. FEP
- eff@eff.org
+ Como Participar
- R $40, obter o formulário de muitos lugares, Efetor On-line,
- membership@eff.org
+ Efetoras Online
- ftp.eff.org, pub/FEP/Newsletters/Efetoras
+ Plataforma Aberta
- ftp://ftp.eff.org/pub/EFF/Policy/Open_Platform
Nacional De Infra-Estrutura De Informação

13.7.9. "Como pode o uso de criptografia ser ocultado?"
+ Steganography
- micropontos, tinta invisível
- onde até mesmo a existência de uma mensagem codificada recebe um tiro
+ Métodos para Esconder a Mera Existência de Dados Criptografados
+ em contraste com o freqüentemente citado ponto (feita por criptografia
os puristas) que deve-se assumir que o adversário tem completo
acesso à cryptotext, alguns fragmentos de descriptografados
texto sem formatação, e para o algoritmo propriamente dito, isto é, assumir o
pior
- uma condição que eu acho que é praticamente um absurdo e
irreal
- assume infinito interceptar o poder (mesmo pressuposto de
infinita de energia do computador iria fazer todos os sistemas além de
as one-time pads quebrável)
- na realidade, ocultando a existência e a forma de
mensagem encriptada é importante
+ este será tanto mais como desafios legais para
criptografia são montados...a proposta de proibição encriptados
telecom (com us $10 MIL por dia de multa), vários governamentais
regulamentos, etc.
- RICO e outros pincel largo estratagemas pode fazer pessoas muito
cuidado, revelando que eles estão usando mesmo
criptografia (independentemente de como proteger as chaves são)
+ steganography, a ciência de esconder a existência de
informações criptografadas
- segredo tintas
- micropontos
- limitando a análise do tráfego
- LSB método
+ Embalagem de dados em fitas de áudio (LSB de DAT)
+ LSB de DAT: 2 gb áudio DAT vai permitir que mais de 100
megabytes nos LSBs
- menos, se os algoritmos são usados para moldar o espectro para
torná-la ainda mais como ruído
- mas também pode usar o maior bits, também (desde um real
mundo gravação terá de ruído atingem de
talvez 3º ou 4º bit)
+ vai fabricantes de investigar "composição" circuitos?
(la gordura zero?)
- mas a corrida ainda vai ser em
+ De vídeo Digital vai oferecer ainda mais espaço de armazenamento (maior
fitas)

- DVI, etc.
- HDTV final da década de 1990
+ Mensagens podem ser colocadas em GIFF, arquivos de imagem TIFF (ou mesmo
ruidosos, aparelhos de fax)
- usando o LSB método, com uma resolução de 1024 x 1024 em escala de cinza
imagem segurando 64KB na LSB avião sozinho
- com a correção de erro, noise shaping, etc., ainda na
menos de 50KB
- cenário: já está sendo usado para transmitir a mensagem
através de fax internacional e transmissões de imagem
+ O Velho "Dois Textos Normais" Manobra
- uma decodificação produz "Tendo um bom tempo. Desejo que você
estava aqui."
- outros, de descodificação das mesmas matérias bits, produz "O
última submarino partiu esta manhã."
- de qualquer ordem jurídica, para produzir a chave gera o primeiro
mensagem
+ as autoridades nunca pode provar-salvar tortura ou de um
informante-que outra mensagem existe
- a menos que haja alguma forma de sinais de que o arquivo criptografado
a mensagem é, de alguma forma, "de forma ineficiente criptografado,
sugerindo o uso de um sistema dual de texto simples par de método"
(ou algo do tipo spookspeak)
- mais uma vez, certos puristas argumentam que tais problemas (que são
relacionados para o velho: "Como você sabe quando parar?"
questão) são enganosas, que se deve assumir a
adversário quase completa e acesso a tudo o
exceto a chave real, que qualquer esquema combinar
vários sistemas não é melhor do que o que é obtido como um
resultado da combinação
- e apenas o total de largura de banda de dados...
13.7.10. próximo de Computadores, a Liberdade e a Privacidade Conferência será em Março
1995, São Francisco
13.7.11. Lugares para enviar mensagens para
- cantwell@eff.org Assunto: eu RH 3627
- leahy@eff.org Assunto: eu apoio audiências em Clipper
13.7.12. Tese: Criptografia pode tornar-se imparável se a massa crítica é
atingido
- analogia: a Net...muito dispersos, muitos países, os demais
muitos graus de liberdade
- tão dispersos que tenta proibir forte de criptografia será
fútil...sem engarrafamentos, sem "passagens de montanha" (em uma corrida para
o passe, além de que a expansão não pode ser interrompido

exceto por extremamente meios repressivos)
13.7.13. Mantendo a criptografia genie sendo colocar a garrafa
- (apesar de alguns dizem que o gênio nunca foi _in_ a garrafa,
historicamente)
- assegurar que um número suficiente de pessoas estiver usando ele, e que o Líquido
está a utilizar
- um _threshold_, um ponto de não retorno
13.7.14. Ativismo aspectos práticos
+ "Porque não comprar publicidade de tempo, como Perot fez?"
+ Este e outros pontos surgem em quase todos os políticos
discussões (o que eu estou vendo no também no falar.política.guns).
As principais razões para isso não acontecer são:
- anúncios custam um monte de dinheiro
- casual pessoas raramente têm este tipo de dinheiro para gastar
- "pastorear gatos" vem à mente, por exemplo, é quase
impossível coordenar os interesses das pessoas para
recolher o dinheiro, configurar campanhas de publicidade, etc.
- Na minha opinião, um desperdício de esforços. As mudanças que eu quero não
vêm através de uma série de anúncios que são apenas os dedos no
dique. (Mais cinicamente, os Americanos estão recebendo do governo
eles foram guinchando para. Meu interesse é em ignorando
sua avareza e a repressão, não na mudança de suas mentes.)
- Outros sentem de forma diferente, a partir de postagens feitas para a lista.
Praticamente falando, entretanto, a atividade política organizada
é difícil de conseguir com o anárquico nonstructure de
os Cypherpunks grupo. Boa sorte!

13.8. As Linhas de Batalha estão Sendo Desenhados
13.8.1. Clipper reuniu-se com desdém e desprezo, agora, então, novas estratégias são
sendo julgado...
13.8.2. Estratégias de mudança, o Plano B está sendo arrastado
- medo, incerteza e dúvida
- medos sobre os terroristas, "the pornographers", pedófilos, dinheiro
os lavadores de
13.8.3. líderes empresariais como o Grove estão sendo convocados para fazer a
Clipper caso
13.8.4. Donn Parker está se espalhando pânico sobre a "anarquia" (semelhante ao meu
própria autoridade de CERTIFICAÇÃO)
13.8.5. "O que pode ser feito no rosto move-se para requerer IDENTIFICAÇÃO nacional
cartões, use oficial de chave pública registros, aderir a chave
garantia leis, etc?"
- Esta é a questão mais importante que enfrentamos.
- Curta de deixar o país (mas para onde?) ou viver um

subsistência de nível estilo de vida abaixo do radar telas do
de fiscalização do estado, o que pode ser feito?
+ Algumas possibilidades, não necessariamente bons:
+ desobediência civil
- mutilação de cartas, de "apagamento acidental", etc.
- a falsificação de cartões...provavelmente não é viável (entendemos
sobre o digital sigs)
- criação de grandes mercados negros...ainda não cobre
tudo, tal como a água, electricidade, de carteira de motorista
de licenças, etc....as coisas simplesmente demais para um mercado negro
para lidar com
- lobby contra esses movimentos...mas parece que o momentum
é forte demais na outra direção

13.9. "O que Poderia Fazer de Criptografia de Uso mais Comum?"
13.9.1. utilização transparente, como a máquina de fax, é a chave
13.9.2. mais fácil com o token de chave e/ou física de métricas de segurança
- leitores de impressão digital
- tokens anexado ao empregado emblemas
- anéis, relógios, etc. que transportar mais de chave (com vários
bits lembrado, e uma estrita "três strikes e você está
fora" do sistema)
13.9.3. maior segurança assusta, ou temores sobre "portas traseiras" pelo
governo pode acelerar a conversão
- tudo o que pode tomar um par de grandes escândalos
13.9.4. as companhias de seguros podem exigir criptografia, por vários
razões
- para proteger contra roubo, perda, etc.
- proporcionar um melhor controle contra vírus e outros
modificações que expõem as empresas têm de assegurar a
responsabilidade ternos
- o mesmo argumento citado pelo seguro políticos: quando o seguro
empresas exigiram melhores cofres, que é quando os clientes
comprei-los (e não antes)
13.9.5. Redes de ficar mais complexas, e vai fazer convencionais
sistemas de segurança inaceitáveis
- "Fortaleza" produto de Los Altos Tecnologias
- muito muitas maneiras para que os outros vejam as senhas que está sendo dada aos
host remoto, ou seja, com LANs sem fio (que vai
exigir ZKIPS)
- ZKIPS especialmente em redes, onde as chances de ver um
palavra-passe de serem transmitidas são muito maiores (uma óbvia
ponto que não é muito discutido)

- toda a explosão de largura de banda
13.9.6. As revelações de vigilância e de controlo dos cidadãos
e as corporações servem para aumentar o uso de
criptografia, em primeiro lugar, as pessoas com algo a esconder, e
em seguida, por outros. Cypherpunks já estão ajudando a espalhar
a palavra de estas situações.
- um efeito bola de neve
- e várias agências do governo-se usar
criptografia para proteger seus arquivos e seus arquivos de privacidade
13.9.7. para os cargos sensíveis, a disponibilidade de novas
outros métodos de acelerar a conversão para seguro
sistemas baseados em criptografados de telecomunicações e o
prevenção de voz baseado em sistemas de
13.9.8. os cidadãos comuns estão sendo ameaçados por causa do que eles
dizer em redes, levando-os a adotar pseudônimos
- processos judiciais, ameaças comuns, preocupações sobre como a sua
os empregadores vão reagir (muitos empregadores poderão adotar regras
limitar o discurso de seus funcionários, em grande parte devido a
preocupações que vai ser processado)
+ e alguns provedores de banco de dados estão fornecendo cruzado
lista de quem publicou o que placas-este é livremente
a informação disponível, mas não é esperado pelo povo
que suas postagens vai viver para sempre
- alguns podem ver isso como uma extorsão
- mas de qualquer proposta de leis são improváveis de sucesso
- então, como de costume, a solução é para as pessoas a proteger
- se através de meios tecnológicos
13.9.9. "agentes" que são capazes de retransmitir o material vai fazer
certos tipos de sistemas anónimos muito mais fácil de usar

13.10. Promoções, o FEP e de Telefonia Digital projeto de lei
13.10.1. Os acordos de bastidores, em Washington, está voando...aparentemente o
A administração ficou queimado pelo Clipper fiasco (que eles
poderia, em parte, write-off como sendo um resquício da era Bush)
e agora está tentando "trabalhar as questões" por trás das cenas
antes de revelar novos e de grande alcance programas. (Embora a
este texto foi escrito, a Saúde Bill é um olhar poderoso amadora
e parece ulikely para passar.)
13.10.2. Não estamos ouvindo sobre estas "ofertas" em uma maneira oportuna. Eu
ouvi pela primeira vez que uma marca nova, e "na bolsa," o negócio foi
cozinhar quando eu estava conversando com um conhecido jornalista. Ele me disse
que um novo negócio, corte entre o Congresso, a indústria de telecomunicações,
e o FEP-tipo de grupos de lobby, já era um negócio feito e

seria revelada por isso. Com certeza, o Novo e Melhorado
Telefonia Digital II Bill aparece algumas semanas mais tarde, e é
disse pela FEP representantes para ser imparável. [comentários
S. McLandisht e outros, comp.org.fep.falar, 1994-08]
13.10.3. Bem, desculpe-me por lembrar a todos que este país é
supostamente, ainda, uma democracia. Eu sei que política é feita por trás
de portas fechadas, como eu não sou nenhum naif, mas trata-corte como este
merece ser exposta e denegrida.
13.10.4. Eu já anunciou que eu não renovar minha FEP associação. Eu
não espere-os para lutar todas as batalhas, para vencer todas as guerras, mas
Eu tenho certeza que o inferno não vai ajudá - *pagar* para sua bastidores ofertas
com as empresas de telecomunicações.
13.10.5. Isso pode me causar problemas com meu amigos na FEP,
mas é como se um grupos de lobby na Alemanha, viu o
escrita na parede sobre a Solução Final, considerou
essencialmente, imparável, e então, enviou os seus líderes, para
Berchtesgaden/Camp David para se certificar de que a morte do
Judeus foi feita tão indolor quanto possível. Um tipo de joint
Administração/Telco/SS/IG Farben "compromisso". Enquanto eu não
equacionar Mitch, Jerry, Mike, Stanton, e outros com Hitler
asseclas, eu certamente não acho que a dentro-do-Rodoanel
acordos feitos é realmente nojento.
13.10.6. As nossas liberdades estão sendo vendidos.

13.11. Pontas soltas
13.11.1. Ofertas, promoções, ofertas!
- pressões pela Administração de...chave de software de caução, digital
de telefonia, cabo regulamento
+ e os fornecedores precisam de apoio do governo na legislação,
benefícios, alocação de espectro, etc.
- relatórios de que a Microsoft está fazendo lobby intensamente para obter
o controle de grandes blocos de espectro...poderia caber com cabo
set-top box negociações, Teledesic, SKE, etc.
- FEP ainda participa de algumas dessas ofertas. Estar "por dentro
o Rodoanel" tem esse tipo de efeito, onde um é um
"jogador / player" ou um "não-leitor." (Essa é a minha interpretação de
como o poder corrompe todos os grupos que entram para o Rodoanel.)
Shmoozing e um desejo de ajuda.
13.11.2. usando criptografia para ignorar as leis de contatos e trocas com outros
países
- um dia, é ilegal ter contato com a China, o próximo
o dia é recomendado
+ um dia, é legal ter contato com o Haiti, no dia seguinte

há um embargo (e, no caso do Haiti, o económico
efeitos cair sobre os pobres--dezenas de milhares de pessoas fugindo
não fugindo a governantes, mas a pobreza agravada pela
o boicote
- (Os militares governantes são apenas os habituais bandidos, mas
eles não são "nossos" bandidos, por razões da história. Aristide
quase que certamente iria ser tão ruim, Marxistas sacerdote.
Assim, considero que o breakin do embargo de ser um
moralmente boa coisa a fazer.
- quem vai dizer por que o Haiti é, de repente, a ser evitado? Por força
de lei, não menos!
13.11.3. Sun Tzu "a Arte da Guerra" tem dicas úteis (mais útil do que "O
O príncipe")
- trabalhar com os mais pequeninos
- sabotagem bom nome do inimigo
- espalhar dinheiro de volta
- Eu acho que os acontecimentos do ano passado, incluindo...
13.11.4. O flakiness dos actuais sistemas de...
- A atual infra-estrutura de criptografia é bastante esquisito, apesar de
a web distribuído-de-modelo de relação de confiança é melhor do que alguns
sistema centralizado de coure. O que eu quero dizer é que muitos
aspectos são lentos, creaky, e propícia a erros.
- Na área de dinheiro digital, o que temos agora não é o mesmo
tão avançado como foi visto com dinheiro real em Sumério vezes!
(E eu não iria confiar e-mail "mensagem na garrafa"
abordagem para qualquer tarefa não trivial transações financeiras.)
- Alguma coisa tem de mudar. A NII/auto-estrada/Infobahn
as pessoas têm planos, mas seus planos não são susceptíveis de malha
bem com a nossa. Para nós um desafio a considerar.
13.11.5. "Há perigos de ser muito paranóico?"
+ Como Eric Hughes colocá-lo, "paranóia é de criptografia do
risco profissional."
- "O efeito da paranóia, é a auto-ilusão dos seguintes
forma-se que uma possível explicação desviado em direção a
ataques mal-intencionados, por indivíduos, que cada um tem o
conhecimento técnico para antecipar. Esta inclinação cria
uma ineficiente alocação de energia mental, tende
para o pessoal, minimizando a possibilidade de
erro técnico, e ele começa a se fechar de exame
de aspectos técnicos não são totalmente compreendidos.

"Aqueles que resistem a paranóia vai se tornar melhor
criptografia do que aqueles que não o fizer, todas as outras coisas

sendo iguais. Criptografia é sobre epistemologia, que
é, a certeza da verdade, e apenas secundariamente sobre
a ontologia, isto é, o que realmente é verdade. O objetivo de
criptografia é criar um precisa ter confiança de que um
sistema é seguro e privado. A fim de criar
a confiança, o sistema deve ser seguro, mas
a segurança não é suficiente. Deve haver confiança
thatthe maneira pela qual esta segurança é para ser acreditado
é robusto e imune a ilusão.

"Paranóia cria ilusão. Como um direto e fundamental
resultado, torna-se uma piora em criptografia. No
melhor fora, torna-se uma mais lenta, como a afectação inadequada
de atenção leva para baixo falsas trilhas. Quem tem o
o excesso de capacidade intelectual para que os resíduos? Certamente não I.
o pior, paranóia faz um completamente ineficaz, não
apenas em meios técnicos, mas ainda mais no social
contexto em que a criptografia é necessariamente relevante."
[Eric Hughes, 1994-05-14]
+ Rei Alfred, de Plano, os negros
- planos para arredondar para cima de 20 milhões de negros
- RFK, links para POLICIA, Western Objetivos, Bétula, KKK
- RFA #9, 23, 38
+ o crime organizado situação, talvez a inteligência
comunidade
- prejudicial para os negros, psicológica
13.11.6. A imoralidade dos EUA boicotes e sanções
- como com o Haiti, onde um padrão e relativamente benigna
e inofensivo ditadura militar está sendo oposição, estamos
usando a força para interferir com o comércio, os transportes de alimentos,
negócios financeiros, etc.
- invasão de países que não têm atacado outros
países...um grande e novo escalonamento do militarismo dos EUA
- crypto vai facillitate meio de underming imperialismo
13.11.7. A "razoabilidade" armadilha
- fazer uma coisa razoável em uma coisa obrigatória
- isso se aplica ao que Cypherpunks deve sempre estar preparado para
suporte
+ Um exemplo: Um restaurante oferece para substituir itens dropados
(caiu no chão, literalmente) de graça...um razoável
coisa para oferecer aos clientes (algo que vejo com frequência). Então,
por que não fazer a lei? Porque, então, o razoável
critério do proprietário do restaurante seria perdido, e alguns

os clientes podem "jogo contra" (explorar a letra da
lei) o sistema. Até ameaçar com processos judiciais.
- (E libertários saber que o "minha casa, minhas regras" aplica-se
restaurantes e outras empresas, na ausência de um contrato de
ortografia exceções para fora.)
- Mais um exemplo grave é quando restaurantes (de novo) encontrá-lo
"razoável" para contratar vários tipos de pessoas qualificadas.
O que pode ser "razoável" é uma coisa, mas muitas vezes o
governo decide _formalize_ isso e tira o
direito de escolha. (Na minha opinião, nenhuma pessoa ou grupo tem qualquer
"direito" de um trabalho, a menos que o empregador oferece livremente a ele. Sim,
isso poderia incluído discriminação contra diversos grupos.
Sim, nós podemos não gostar desta. Mas a liberdade de escolha é um
muito mais básico direito de alcançar algum ideal de igualdade
é.)
- E quando a "razoabilidade" é imposta por lei, o jogo-
reprodução aumenta. Com efeito, alguns discrição é necessária para
rejeitar as reclamações baseadas em jogos. Mercados naturalmente
o trabalho, desta forma, como não há "direitos básicos" ou contratos a serem
violada.
- Felizmente, forte de criptografia faz com que este absurdo impossível.
Forçosamente, as pessoas vão se envolver em contratos voluntariamente.
13.11.8. "Como é que vamos chegar a um acordo sobre protocolos?"
- Dar essa idéia imediatamente! Contrato de comportar-se em
certas formas quase nunca é possível.
- Isso é uma acusação de anarquia?
- Não, porque a forma de contrato é uma espécie de chegar é através de
normas ou examplars que as pessoas podem começar para trás. Assim, temos
não fica "consenso" com antecedência sobre o sabor de Coca
Cola...alguém oferece Coque para venda e, em seguida, o resto é
história.
- PGP é mais um exemplo relevante. O exemplar (e modulador está em um "tomar
é o ou deixe-o", com pequenas melhorias feitas por
outros, mas dentro do formato básico.

14. Outros Avançados De Criptografia Aplicações

14.1. direitos autorais

14.2. RESUMO: Outros Avançados de Criptografia Aplicações
14.2.1. Pontos Principais
14.2.2. Ligações para Outras Secções
14.2.3. Onde Encontrar Informações Adicionais
- veja as várias "Crypto" Processo para vários artigos sobre
tópicos que podem vir a ser importantes
14.2.4. Diversos Comentários

14.3. Digitais Do Módulo De
14.3.1. digitais do módulo de
- Canônica de referência para o digital é o registro de data e hora
trabalho de Stu Haber e Scott Stornetta, de Bellcore. Artigos
apresentado em vários Criptografia conferências. O seu trabalho
envolve o usuário calcular o hash do documento ele
quer ser carimbado e enviando-o de hash para eles, onde
eles se fundem esse hash com outros hashes (e todas as anteriores
hashes, através de um sistema de árvore) e, em seguida, eles *publique* o
resultante de hash em um público muito difíceis de alterar fórum,
como em um anúncio no domingo ", New York Times."

Em sua linguagem, um anúncio é um "amplamente testemunhado
evento," e as tentativas de alterar todos ou mesmo muitas cópias de
o jornal iria ser muito difícil e caro. (Em um
sentido, a WWE é semelhante ao "beacon" termo de Eric Hughes
usado.)

Haber e Stornetta plano de algum tipo de operação comercial
para fazer isso.

Esse serviço ainda não foi testado no tribunal, tanto quanto eu
conheço. O MIT server é uma experiência, e provavelmente é
útil para experimentar. Mas é, sem dúvida, menos ainda
juridicamente significativos, é claro.
14.3.2. meu resumo

14.4. Votação
14.4.1. a fraude, é-uma-pessoa, forjando identica, aumento do "número"
tendências
14.4.2. os custos também elevados
14.4.3. Chaum
14.4.4. votação isomórfica de dinheiro digital
- onde conta as transferências são a coisa a ser votada, e

os "eleitores" são de si mesmo...a menos que este tipo de
coisa que é proibida, o que poderia criar outros problemas, então
isso faz com que uma forma de anonimato possível (mais ou
menos)

14.5. Timed-Release De Criptografia
14.5.1. "Pode qualquer coisa como um "criptografia" cápsula do tempo" ser construído?"
- Isso seria útil para a vedação de diários e registros em
tal forma que não jurídicas poderiam ter acesso, que
até mesmo o criador/encryptor seria capaz de descriptografar a
registros. Chamá-lo de "tempo de caução." Ironicamente, um muito mais
o uso correto do termo "garantia" do que vimos com o
governo de vários "key escrow" esquemas.
- Realizar registros undecryptable é fácil: basta usar uma forma de
função e os registros são inacessíveis para sempre. O truque
é ter uma maneira de levá-los de volta em algum tempo futuro.
+ Abordagens:
+ Legal Repositório. Um advogado ou um conjunto de advogados tem a chave
ou chaves e é indicado para liberá-los no futuro
em tempo. (A chave de retenção de agentes não precisam ser advogados, de
é claro, porém, que é a forma como as coisas estão agora.
- O sistema jurídico é uma time-honored forma de proteger
segredos de vários tipos, e qualquer sistema baseado em
criptografia precisa para competir fortemente com este simples
para usar, sistema bem estabelecido.
- Se o advogado da identidade é conhecido, ele pode ser
intimada. Depende de questões de jurisdição, futuro
clima político, etc.
- Mas, a identidade ocultando protocolos podem ser utilizados, de modo a que o
advogado não pode ser alcançado. Tudo o que é saber, para
exemplo, é a de que "em algum lugar lá fora" é um agente que
está segurando a chave(s). Reputação baseada em sistemas de
funciona bem aqui: o agente ganha pouco e perde muito
ao lançar uma chave de início, portanto, não tem económico
a motivação para fazê-lo. (Imagem também um monte de "ping"
indo para a "taxa" as várias ti<w agentes.)
- Criptografia com Beacons. Um "farol" agente faz muito
público uma série de mensagens, de alguma forma. Detalhes nítidos. [Eu
tenho um palpite de que usando o tempo digital de registro de serviços
pode ser útil aqui.]
+ Dificuldade de factoring, etc.
+ A ideia aqui é usar uma função que é, atualmente,
difícil de inverter, mas que pode ser mais fácil no futuro.

Este é repleta de problemas, incluindo:
a imprevisibilidade da dificuldade, imprecisão na
timing do lançamento, e em geral falta de jeito. Como Hal
Finney notas:
- "Foi uma palestra sobre este tema na Criptografia
92 ou 93 conferência, eu me esquecer de que. Ele está disponível
no processo....O método utilizado foi semelhante ao
aqui a ideia de criptografia com chave pública e
exigindo cálculo do módulo de elasticidade para descriptografar. Mas
o autor tinha mais técnicas que ele usou, iterando
funções para a frente o que levaria mais tempo para iterar
para trás. A finalidade era a de dar mais
previsível tempo para descriptografar.....Um problema com este
é que ele não coloque um tempo no chão
decodificação, mas sim um custo chão. Alguém que é
dispostos a gastar o suficiente pode descriptografar mais rápido do que
alguém que gasta menos. Outro problema é a
dificuldade de previsão de crescimento da computacionais
de energia por dólar no futuro." [Hal Finney,
sci.cripta, 1994-8-04]
+ Inviolável módulos. Uma la de um esquema de enviar o
segredos para um satélite em órbita e esperar que ele se
ser proibitivamente caro para o encontro e entrar neste
por satélite.
- Ou para obter acesso à inviolável módulos localizado
no banco de cofres, etc.
- Mas ordens judiciais e saco preto trabalhos ainda são fatores.

14.5.2. Necessidades
- jornalismo
+ time-stamping é um tipo de exemplo
- apesar de ser melhor visto na análise convencional
- persistente instituições
- shell jogos para mover o dinheiro, untraceably

14.5.3. Como
- faróis
- multi-parte chaves
- contratada-pela prestação dos serviços (como a publicação de chaves)
- Wayner, a minha proposta, Eric Hughes

14.6. Análise Do Tráfego

14.6.1. o formato digital, e os cabeçalhos da FOLHA, campos, etc., torná-lo muito
mais fácil saber quem tem o chamado de quem, por quanto tempo, etc.

14.6.2. (esp. em contraste puramente sistemas analógicos)

14.7. Steganography
14.7.1. (Mais um dos tópicos que fica um monte de posts)
14.7.2. Ocultar mensagens em outras mensagens
- "Kevin Brown, faz com que alguns pontos interessantes sobre a
steganography e steganalysis. O problema de reconhecer
se uma mensagem foi ou mighthave uma mensagem oculta, tem dois
os lados. Um é para o destinatário desejado para ser actualizado que
ele deve tentar desteganizing e decifrar a mensagem, e
o outro é para um possível invasor descobrir ilegal
utiliza de criptografia.

"Steganography deve ser usado com um "furtivo"
criptosistema (chave secreta ou chave pública), em que o
por cyphertext é indistinguível de uma seqüência de bits aleatórios.
Você não gostaria de ter cabeçalhos que poderia ser
usado para confirmar que um desteganized mensagem foi diferente
o ruído aleatório." [Hal Finney, 1993-05-25]
14.7.3. Peter Wayner de "Imitar"
- "Eles codificar uma mensagem secreta dentro de um inofensivo à procura
Arquivo de texto ASCII. Esta é uma das muito poucas vezes
o UNIX ferramentas "lex" e "yacc" tem sido usada em
criptografia, tanto quanto eu sei. Peter Wayner, "Imitar
Funções", CRYPTOLOGIA Volume 16, Número 3, pp. 193-214,
De julho de 1992.[Michael Johnson, sci.cripta, 1994-09-05]
14.7.4. Eu descreveu em 1988 ou 89 e, muitas vezes desde a
Vários anos atrás eu postei a sci.cripta meu "romance" a idéia para
embalagem bits para o essencialmente inaudível "menos
bits significativos" (LSBs) de gravações digitais, tais como
DATs e CDs. Idem para os LSBs em uma imagem de 8 bits ou 24
bits de cor da imagem. Eu já vi esta ideia reinventada
several vezes no sci.cripta e em outros lugares...e eu estou
disposto a apostar que eu não era o primeiro, (então, eu não tenho a pretensão
qualquer crédito).

De uma hora 2 DAT contém cerca de 10 Gbits (2 horas x 3600 s/h
x 2 canais x 16 bits/amostra x 44 K amostras/seg), ou sobre
1.2 Gbytes. Um CD, que contém cerca de metade deste, isto é, cerca de 700
Mbytes. O LSB de um DAT 1/16 de 1.2 Gb, ou 80
Mbytes. Este é um _lot_ de armazenamento!

Uma casa-gravado DAT--e eu uso um Sony D-3 DAT Walkman para
fazer fitas--tem muito barulho na LSB nível de ruído--

a partir do A/D e D/A conversores de ruído do microfone
(se houver), etc.--que os bits são essencialmente aleatórios
a este nível. (Esta é uma sutil, mas importante, do ponto: um
fábrica registradas DAT ou CD terá predeterminado bits
todos os níveis, por exemplo, as autoridades poderiam, em princípio, lugar
quaisquer modificações. Mas casa-gravados, ou dobrados, de DATs vai
é claro que não se sujeita a este tipo de análise.) Alguns
cuidados podem ser tomados para garantir que a estatística
propriedades do sinal de bits se parecem com o que seria
esperado com "ruído" bits, mas isso vai ser menor
obstáculo.

Adobe Photoshop pode ser usado para facilmente colocar mensagem em bits
o "ruído" que domina as coisas no LSB nível.
A resultante GIF, em seguida, pode ser postada na UseNet ou o endereço de e-mail.
Idem para amostras de som, usando as idéias que eu acabei de descrever
(mas, normalmente, necessitando de amostragem do som placas, etc.). Eu
feito algumas experiências ao longo destas linhas.

Isso não significa que nossos problemas estão resolvidos, é claro.
A troca de fitas é complicado e vulneráveis às picadas.
Mas ajuda a apontar a inutilidade e futilidade de tentar
para parar o fluxo de bits.

14.7.5. Stego, outras versões

- Romana Machado Macintosh stego programa está localizado na
compactação de arquivos, /cmp, no sumex-aim@stanford.edu informações
mac os arquivos.
- "Stego é uma ferramenta que permite incorporar dados, e
recuperar dados a partir de Macintosh PICT formato de arquivos, sem
alterar a aparência do arquivo PICT. Embora a sua
o efeito é visualmente indetectáveis, não espera
criptografia de segurança da Stego. Esteja ciente de que qualquer um
com uma cópia da Stego pode recuperar seus dados a partir do seu PICT
arquivo. Stego pode ser usado como um "envelope" para ocultar uma
previously encrypted arquivo de dados em um arquivo PICT, tornando-o
muito menos provável de ser detectado." [Romana Machado, 1993-11-
23]

14.7.6. WNSTORM, Avakov Ray Arachelian

14.7.7. falar sobre isso sendo usado para "marca d'água" images

14.7.8. Criptografia e steganography utilizado para plantar falsas e enganosas
informações nucleares

- "No âmbito de um sub-sub-sub-contrato certa vez, trabalhei em alguns falsos
Desenhos CAD para as armas nucleares, o processo de produção,

plotagem de falsas informações que ainda aparece em livros populares,
alguns dos quais já foi postado aqui....Os documentos foram, em seguida,
criptografados e stegonagraphied de autenticidade. Estávamos
disse que eles foram transformadas solta no mercado para esta
produto em outros países." [John Young, 1994-08-25]
- Bem...
14.7.9. Postscript steganography
- onde a informação é incorporada em espaçamentos, características da fonte
(ângulos, arcos)
- ftp://research.att.com/dist/brassil/infocom94.ps
- o ponto essencial: apenas mais um palheiro para ocultar uma agulha

14.8. Escondendo-se por cyphertext
14.8.1. "Texto cifrado pode ser "uncompressed" para impor desejado
propriedades estatísticas. Um não-adaptativo de primeira ordem
aritmética de descompressão irá gerar primeira ordem, símbolo
frequências que emular, por exemplo, o texto em inglês." [Rick
F. Hoselton, sci.cripta, 1994-07-05]

14.9. "O que são as adulterações de responder ou à prova de violação módulos?"
14.9.1. O mais nome moderno para o que costumava ser chamado de "à prova de adulteração
caixas"
14.9.2. Utilizações:
alarmado casos de exposição, sensível à pressão, etc. (jóias,
arte, etc.)
+ batata frita com camadas extra, fusíveis, abrasivos comounds no
embalagem
- para diminuir a moagem, gravuras, outros depotting ou
decapping métodos
- VLSI Technology Inc. supostamente usa esses métodos em seus
implementação do MYK-78 "Clipper" (EES) chip
- armas nucleares ("Permissive Links de Ação," a la Sandia,
Simmons)
- cartões inteligentes (smartcards) que dão evidências de adulteração, ou que se tornaram
inativos
+ como um exemplo, unidades de disco que apagar dados quando ligar é
puxado, a menos que o código correto for inserido primeiro
- ufa! muito arriscado (falhas de energia e tudo), mas é necessário
por alguns
- como "flash digital de papel"
14.9.3. Ignorando a violação de responder ou à prova de violação tecnologias
- primeiro, você tem que _know_

14.10. Denúncia de irregularidades
14.10.1. Este foi um dos primeiros a proposta de utilização (os meus comentários sobre ele volte para
De 1988, pelo menos), e resultou na criação de
alt.whisteblowers.
- Até agora, nada demais a terra tremer
14.10.2. revelando o segredo agentes de um país, publicando-os
anonimamente para o mundo ampla rede de distribuição....que deveria
agitar as coisas

14.11. Digital Confessionários
14.11.1. religiosa confessionários e consultas mediada pelo digital
links...muito difícil para o governo dos EUA para obter acesso
14.11.2. idem para o cliente-advogado, conversas, sessões com
os psiquiatras e médicos, etc.
14.11.3. (isso não meen estas reuniões são isentos do
lei...testemunha Federais indo depois de contaminados, taxas legais, e
incomodando escritórios de advogados suspeitos de estarem na droga
de negócios)

14.12. Pontas Soltas
14.12.1. Feigenbaum da "Computação com Encriptado Instâncias"
trabalho...links para Eric Hughes do "criptografado livros abertos" idéias.
- mais trabalho necessário, claramente

15. Reputação e Credenciais

15.1. direitos autorais
O CYPHERNOMICON: Cypherpunks FAQ e Mais, Versão 0.666,
1994-09-10, Direitos De Autor Timothy C. De Maio. Todos os direitos reservados.
Veja os detalhes de isenção de responsabilidade. Use seções curtas em "justo
use" disposições, com crédito apropriado, mas não coloque o seu
nome em minhas palavras.

15.2. RESUMO: a Reputação e Credenciais
15.2.1. Pontos Principais
- "um homem da palavra é a sua obrigação"
- reputação matéria
- a expectativa de futuro interação/negócios é crucial
15.2.2. Ligações para Outras Secções
- consulte a secção sobre a Criptografia Anarquia para a qual a reputação matéria
15.2.3. Onde Encontrar Informações Adicionais
- muito pouco publicado neste

- Bruce Benson "A Empresa de Lei"

15.2.4. Diversos Comentários

- este é outro de "transição", capítulo, lançando as bases para Crypto Anarquia

15.3. A Natureza das Reputações

15.3.1. A reivindicação por muitos de nós que "reputação" vai cuidar de muitos problemas em criptografia anárquico mercados é disputada por alguns (nomeadamente Eric Hughes). Para ter certeza, não vai ser trivial questão. Instituições levar anos ou décadas para evoluir.

15.3.2. No entanto, pensar em como usamos muitas vezes reputação: amigos, livros, filmes, restaurantes, etc.

15.3.3. A reputação da empresa e de outras instituições, vai levar tempo para evoluir. Dizendo que "o mercado vai talke o cuidado das coisas" pode ser verdadeiro, mas isso pode levar tempo. A "mão invisível" não necessariamente mover-se rapidamente.

15.3.4. "O que 'reputação' e por que eles são tão importantes?"

- um vago conceito relacionado ao grau de credibilidade, de confiança, etc.

+ "nós sabemos que quando a vemos"

- (desculpem a cop out, mas eu não tenho uma boa definição prático....James Donald diz estudo reputatons é "nominalist de ar quente" [1994-09-02], mas eu acho que é muito importante)

+ óbvia, na vida comum, mas no contexto cyberspatial reputação de sistemas baseados em

- garantia, expectativas
- "o capital de reputação" como reservar ou recomendações da música
- web of trust (é diferente do que apenas a "confiança"---tensor, em vez de escalar)

+ Na verdade é muito comum: como a maioria de nós lidar com nossos amigos, nossos inimigos, os livros que lemos, os restaurantes de nós frequentes, etc.

- nós mentalmente downcheck e upcheck na base de experiência; nós aprendemos
- Há exemplos?
- Eric objeções

15.3.5. "Como está a reputação adquirida, em ruínas, transferência, etc.?"

+ Primeiro, a reputação não são "propriedade" pela pessoa a quem eles são fixados através de outros

+ a álgebra é complicado...talvez Eric Hughes ou um dos outras matemática pura tipos pode ajudar a endireitar a

"cálculo de reputação"
- a reputação não são simétricas: só porque Alice
tenha Bob significa o inverso é tão
- a reputação não são transitivas, que eles são
parcialmente transitiva: se a Alice faz diferença Bob e Bob
tenha Charles, isso pode causar Alice ser um pouco
mais esteemful de Charles.
- um tensor de matrix?
- você pode encontrar um gráfico?
+ Qualquer titular de uma reputação que pode "gastar" alguns de seus
o capital de reputação
- em louvor ou a crítica de outro agente
- nas revisões (acho que de Siskel e Ebert "gastar" alguns dos
a sua reputação de capital no louvor de um filme, e
como o seu próprio reptutations vai para cima e para baixo como um
função de muitas coisas, incluindo especialmente quanto
a visualização do público concorda com eles)

15.3.6. "Eles são à prova de falhas? Todas as perguntas são respondidas?"
- Claro que não.
- E Eric Hughes no passado, disse que o excesso de
importância está sendo investido nessa idéia de reputações,
apesar de muitos ou mesmo a maioria de nós (que comentar sobre o assunto)
claramente pensar de outra forma.
- Em qualquer caso, muito mais estudo é necessário. Hal Finney e eu
tem debatido isso um par de vezes (primeiro em a
Extropians lista e, em seguida, um par ou mais vezes no
Cypherpunks lista), e nós somos a maioria no contrato de que este
a área é muito promissora e é merecedor de muito mais
pensamento-e até mesmo a experimentação. (Um dos meus interesses em
criptografia de simulações, no "protocolo de ecologias," é simular
agentes que jogar jogos que envolvem a reputação da empresa, falsificação,
transferências de reputação, etc.)

15.3.7. Reputação de ter muitos aspectos
+ a negociação de empresa que executa outras pessoas o dinheiro é
provavelmente menos "respeitável" em um sentido importante do que a
empresa comercial em que os parceiros têm a sua própria
fortunas de equitação....ou pelo menos eu sei que que eu tinha confiança!
- (Mas como a garantia de não ser enganado, por um spoof,
uma farsa? Difícil dizer. Talvez a "criptografado livros abertos"
protocolo Eric Hughes está a trabalhar vai ser de uso aqui.)

15.4. A Reputação Da Empresa, Instituições

15.5. Reputação e Sistemas Baseados em Agoric Sistemas Abertos
15.5.1. Evolutiva dos sistemas e mercados de
+ mercados, ordem emergente, Hayek, connectionism
- muitas ideias relacionados...a ordem espontânea, auto-interesse, agentes, etc.
+ uma crítica de "cego racionalismo"
- ou hyperrationalism, que a idéia de um formulário de modelo pode sempre ser encontrado
- ordem pode desenvolver-se mesmo em sistemas anónimos, provding certos tipos de contatos são estabelecidos, determinados coisas
15.5.2. jogos do shell...quem sabe o que?
15.5.3. a chave é que seria o "queimadores" deve nunca sabe quando eles estão na verdade, está sendo testado
- com efeitos devastadores se eles queimam o testador
+ exemplo: como garantir (em algum grau de certeza) que um anônimo banco não é renegging (ou o que)?
- por exemplo, um banco Suíço, que nega o conhecimento de uma conta
- chave é que o banco nunca se sabe quando a retirada é apenas um teste (e estes testes podem ser feitas com freqüência)
- a importância da repetição de negócios
15.5.4. outro chave: repetição de negócio....quando os ganhos a partir da queima de alguém são maiores do que o esperado para o futuro do negócio.....
15.5.5. reputações são o que mantém CA sistemas de degenerar em flamefests
- digital pseudônimos significar uma trilha à esquerda, mate os arquivos podem ser usadas, e as pessoas vão tomar cuidado com o que eles dizem
- e os sistemas não ser realmente anônimo: algumas pessoas vai ver a mesma de outras pessoas, permitindo o desenvolvimento de histórias e continuou medicamentosas (lembre-se de que, nos casos em onde não há futuro interação é exected, a rudeza e a flaming arrasta-se)
+ "Rumormonger" na Apple (e outros) sempre degenera em chamas e crudities, diz Johann Strandberg
- mas isso é o que a reputação será parcialmente compensada
15.5.6. "brilhante tostões" golpe
15.5.7. "reputação float" é a forma como o dinheiro pode ser retirado da valor futuro de uma reputação
15.5.8. Reputação baseada em sistemas e repetir negócios
+ reputações importa...esta é a principal base da nossa economia sistema
- a repetição de negócios....as pessoas a parar de fazer negócios com os eles não confiam, ou quem maltrata-los, ou aqueles que apenas

não parecem ser respeitável
- e mesmo em centralmente controlado sistemas de reputação
a matéria (não pode forçar as pessoas a realizar algumas relações)
- notações de crédito (até mesmo por pseudônimos) a matéria
- custódia de agentes, colagem, etc.
- criminal sistemas ainda dependem de reputação e até mesmo em
honra
- ironicamente, é, muitas vezes, em casos onde não há
restrições na escolha de que as vantagens de reputações
são perdidas, como quando o governo proíbe a discriminação,
limites de escolha, ou se insiste na determinação de quem pode fazer
negócios com quem
+ Repita o negócio é o aspecto mais importante
- granularidade das operações, fluxo de caixa, jogo-teórico
análise das vantagens de "desertores"
- sempre que uma transação tem um valor que é muito grande
(em comparação com o esperado de lucros futuros de operações,
ou na base absoluta), atente
- idealmente, uma série de transações menores são mais
propício para o comércio justo...por exemplo, se um recebe um
má refeição em um restaurante, se evita que o restaurante
o futuro, em vez de demandar (mesmo que se pode afirmar
ter sido "danificado")
- questões de contrato, bem

15.6. A reputação e a Teoria de jogos Evolutiva
15.6.1. jogo do "frango", onde ganhando uma reputação como cara dura, ou rei
da colina, pode cabeça para fora muitos desafios futuros (e, portanto,
ajuda na sobrevivência, reprodução diferencial)

15.7. Reputação Positiva
15.7.1. melhor do que negativo reputação, porque neg repetições pode ser
descartado pelo pseudônimo holdes (neg repetições são como a de permitir uma
cartão de crédito a ser utilizado, em seguida, abandonado com uma dívida sobre ele)
15.7.2. "o capital de reputação"

15.8. Exemplos Práticos
15.8.1. "Existem exemplos concretos de software mediada
sistemas de reputação?"
- crédito de bancos de dados...positivos e negativos reputação
15.8.2. Ausente leis que proíbem forte de criptografia (e tais leis são
- se quase inexequível), será essencialmente
impossível parar anônimo transações e puramente

reputação baseada em sistemas.
- Por exemplo, Pr0duct Cypher e Sue D. Nym será capaz de
utilizar os canais privados de sua própria escolha (possivelmente usando
anônimo piscinas, etc.) para se comunicar e de organizar negócios. Se
alguma forma de dinheiro digital existe, eles vão mesmo ser capaz de
transferir esse dinheiro. (Se não, troca de informações,
seja o que for.)
- Então, as questões levantadas por Hal Finney e outros, expressando
dúvidas sobre a adequação de capital de reputação como um
bloco de construção (e boa preocupações que são, por sinal),
tornou-se discutível. A sociedade não pode parar de querer participantes de
usando a reputação e o anonimato. Este é um dos temas principais da
crypto anarquia: o fato de a convenção pelo disposto
participantes.
+ Se Alice e Bob não se importam que seus física identica
são desconhecidos uns dos outros, por que devemos nos preocupar? Que é, por
a sociedade deve intervir e tentar banir este arranjo?
- assim não usando o "nosso" tribunal sistemas, de modo que não é uma
problema (e a mais longo prazo, PPLs vai tomar o lugar do
tribunais, muitos de nós sentem)
- só se Alice e Bob estão contando com a sociedade, em terceiro
partes para a transação, para fazer determinadas coisas, pode
a sociedade fazer um pedido para ser envolvido
- A principal razão para tentar proibir o anonimato será parar
"bad" de atividades, que é um problema separado; proibição de
"bad" atividade normalmente é inútil, e leva a
estados repressivos. Mas estou divagando.)
15.8.3. Parte da "mudança de fase": pessoas de opt-out de permissão-
deslizamento sociedade através de criptografia forte, fazendo suas próprias decisões
em quem confiar, que para lidar com, o que fazer financeira
acordos com
+ exemplo: agências de notação de crédito que não são rastreáveis, não
prosecutable em qualquer tribunal...as pessoas a lidar com eles apenas se
eles pensam que eles estão obtendo valor para seu dinheiro
- não bobo regras de classificação de crédito de dados pode "apenas" voltar
algumas número arbitrário de anos (7, nos EUA)...não é bobo
regras sobre como determinadas falências "não pode" ser
considerado como o registro é para ser "limpo" se
condições são atendidas, etc.
- sim, todos os dados são considerados....o cliente decide como
o peso dos dados(se um cliente é muito persnickety
sobre o passado caducas contas, ou a inadimplência de muitos anos, no
passado, ele vai encontrar-se nunca de empréstimo de dinheiro, de modo que o

"mão invisível" do livre mercado tenderá a corrigir
tais overzealousnesses)
+ dados paraísos de crédito paraísos, etc. (muitas vezes chamado de "ventos
dados paraísos", como a atual forma de fazer isso seria
localize em Cayman, Ilha de Man, etc.)
- mas é claro que eles podem ser "offshore no ciberespaço"
(anônimo links, etc.)

15.9. Credenciais e Reputação
15.9.1. o debate sobre credenciais vs. reputação
- James Donald, Hal Finney, etc.
- (insira os detalhes do debate aqui)
15.9.2. As credenciais não são tão importantes como muitas pessoas parecem pensar
- "Permisssion escorrega" para vários comportamentos: idade de beber,
a admissão para os cinemas, licenças comerciais, licenças para
unidade de táxis, para ler palmeiras (sim, aqui em Santa Cruz um
deve ter uma leitura de mão de licença, diferente da normal
"licença de negócios")
+ Credenciais, muitas vezes, são inadequadas extensões de
o poder do estado em assuntos que só os pais devem lidar com
- menores de idade bebendo? Não é meu problema! Não force as barras
babás.
- menores de idade, visualização de filmes? Idem, mais ainda.
15.9.3. Provando a posse de alguns credencial

15.10. Fraudes e Falsas Acusações
15.10.1. "E se alguém faz uma falsa acusação?"
- a crença em que uma asserção é um emergente phenomenon
+ de declaração não é igual a prova
- (até mesmo a "prova" é variável, também)
- as falsas declarações, eventualmente, refletir sobre o falso requerente
15.10.2. Fraudes, Esquemas de Ponzi, e Oceania
+ Golpes no ciberespaço são abundantes
- sistemas anónimos vai piorar a situaion em alguns aspectos,
mas, talvez, ajudar de outras maneiras
- certamente, há o risco de perder o eletrônico
dinheiro muito rapidamente e irremediavelmente (é muito longe
uma vez que ele é passado através de vários remetentes)
- conpersons (não posso dizer "vigaristas" mais!) vai estar lá,
muito
+ Muitos de vocês se lembram da propaganda sobre a "Oceania", um
proposta de nação independente, a ser construído em concreto
pontões, ou algo do tipo. As pessoas foram incentivadas a enviar

doações. Aparentemente, a/esquema de fraude em colapso:
+ "Ele saiu para tudo ser uma farsa, na verdade. A chave
as pessoas envolvidas, Eric Kline e Chuck Geshlieder,
supostamente tinha um esquema de definir até onde eles repetidamente pago
se fora de todos os rendimentos." [post anônimo,
altp.privacidade, (reimpressão de Scott A. Kjar post sobre
Compuserve), 1994-07-28]
- ou foi Eric Klein?

15.11. Pontas Soltas
15.11.1. Divulgação selectiva da verdade
- Mais euphemestic de "mentira."
- Considerar como vamos reagir quando alguém nos pergunta sobre algo
consideramos extremamente pessoal, enquanto um amigo ou um ente querido
rotineiramente pode fazer essas perguntas.
- É "pessoal" o real problema? Ou é que entendemos
a verdade é uma mercadoria com valor, para ser dado para
algo em troca?
- Em um extremo, a pessoa que casualmente e consistente
mentiras ganha uma má reputação, qualquer pessoa encontrando-los é
nunca certa, se a verdade está sendo dito. Na outra
extremo, o "sempre honesto" pessoa essencialmente dá muito
muito longe, revelar preferências, planos e idéias, sem
consideração.
- Eu sou tudo para "segredos", e mentiras, quando necessário. Eu acredito em
divulgação selectiva da verdade, porque a verdade
carrega valor e não precisa ser "doado" para qualquer pessoa que
pede.
15.11.2. Crytography permite que redes virtuais para organizar por
criptografia conluio de determinados objetivos. Além de apenas o
padrão de "célula" do sistema, ele permite que arrrangements, planos e
execução.
coleta de dinheiro para ter alguém morto é um exemplo,
apesar de um mau gosto um

16. Crypto Anarquia

16.1. direitos autorais

16.2. RESUMO: Criptografia Anarquia
16.2.1. Pontos Principais
- "...quando você quer quebrar o Estado, tudo parece
um martelo."
- forte de criptografia como o "material de construção" para que o ciberespaço
(fazendo as paredes, as vigas de sustentação, os bloqueios)
16.2.2. Ligações para Outras Secções
- esta seção laços de todas as outras secções juntos
16.2.3. Onde Encontrar Informações Adicionais
- novamente, quase nada escrito sobre isso
- Vinge, Friedman, Rand, etc.
16.2.4. Diversos Comentários
- uma longa seção, possivelmente confuso para muitos

16.3. Introdução
16.3.1. "A revolução não será televisionada. A revolução *o*,
no entanto, ser digitalizado." Bem-vindo ao Novo Submundo Ordem!
(é um termo que foi emprestado do escritor Claire Sterling.)
16.3.2. "Fazer as opiniões aqui expressar os pontos de vista dos Cypherpunks como um todo?"
- Esta secção é controversa. Por isso, ainda mais avisos
do que de costume, sobre o cuidado de não confundir estes
comentários com as crenças de todos, ou mesmo a maioria dos Cypherpunks.
- Na justiça, libertarianismo é, inegavelmente, a mais
representado ideologia na lista, pois é tanta
o Líquido. As razões para isso foram amplamente debatido
ao longo dos anos, mas é um fato. Se outras grandes ideologias
existe, eles são bastante escondidos no Cypherpunks lista.
- Sim, alguns quase-socialista vistas ocasionalmente são apresentados.
Meu amigo Dave Mandl, por exemplo, às vezes tem defendido
uma menos-anarchocapitalist vista (mas eu acho que nossos pontos de vista são
na verdade bastante semelhante...ele só tem um idioma diferente
e pensa que há uma diferença maior do que a sua, na verdade,
é--inserir risonho aqui).
- E vários Cypherpunks que já pensou sobre as questões de
crypto anarquia ter sido perturbado pelas conclusões que
parece inevitável (mercados corporativos de informação,
assassianation fez mais líquido, os dados de paraísos, espionagem
muito mais fácil, e outras tais implicações para ser
explorado mais adiante nesta seção).
- Então, tome esta seção com estas ressalvas.
- E algumas das coisas que eu coisa são inevitáveis, e em muitos

dos casos positivos, vai ser repugnante para alguns. A fim de
bem-estar, o fim dos subsídios do centro da cidade criadores, para
exemplo. O esmagamento do estado de segurança nacional
digital através de espionagem, informação de mercados, e
seletiva assassinatos não são coisas que todo mundo vai
tranquilize-se. Alguns podem até chamá-lo ilegal, sedicioso,
e perigoso. Que assim seja.

16.3.3. "O que são as Ideologias de Cyperpunks?"

+ Eu mencionei isso em uma seção anterior, mas agora que eu estou
discutir "crypto anarquia", em detalhe, é bom recapitular
alguns pontos sobre a ideologia de Cypherpunks.
- uma área repleta de perigos, como muitos Cypherpunks ter
diferentes pontos de vista sobre o que é importante
+ Dois principais focos para Cypherpunks:
- Privacidade pessoal cada vez mais um vigilante da sociedade
- Enfraquecimento de estados e de governos
- De quem falar, mais se parecem a se inclinar em direção a
libertário posição, muitas vezes, explicitamente, portanto, (libertários
muitas vezes são encontrados na Internet, para que esta correlação
não é de surpreender)
+ Socialistas e Communitarians
- Deve falar mais do que eles têm. Dave Mandl é o
só que eu lembro, que é dado um resumo coerente de
seus pontos de vista.
+ O meu ponto de vista Pessoal sobre a Legislação e Ideologia:
- (Também, obviamente, espalhados por toda deste documento).
+ Não-coerção Princípio
- evitar a iniciação de agressão física
- "a cada um o seu" (um "neo-Calvinista" perspectiva de
permitindo que cada pessoa escolher o seu caminho, e não interferir)
- Que eu suporte sem lei que pode ser facilmente evitado.
(As leis de trânsito são um contra-exemplo...eu geralmente concordam
com base as leis de trânsito....)
- E eu suporte sem a lei, eu não iria pessoalmente estar disposto a
fiscalizar e punir. Assassinato, estupro, roubo, etc, mas não
"victimless crimes", não a leis de drogas, e não 99.9998% de
as leis sobre os livros.
- Crypto anarquia é no sentido de um retrocesso para o pré-estado
dias de escolha individual sobre quais as leis a seguir. O
comunidade exercida uma força forte.
- Com uma forte criptografia ("fortaleza de criptografia," na aplicação da lei
termos), apenas um intrusiva de polícia do estado pode parar de pessoas
de acesso "ilegal" de sites, de se comunicar com

outros, do uso "indevido" de serviços, e assim por diante. Para
pegar um exemplo, os "dados de crédito ou não, que mantém qualquer
e todos os registros financeiros--alugar problemas a partir de 1975,
o processo de falência a partir de 1983, acordos de divórcio,
resultados de investigadores privados, etc. Nos EUA,
muitos desses registros "inutilizável": não pode usar dados de crédito
com mais de 7 anos (no âmbito do "Fair credit Reporting
Act"), PI de dados, etc. Mas se eu estou pensando sobre empréstimos
Zé algum dinheiro, como diabos eu posso ser dito que eu não posso
"considerar" o fato de que ele declarou falência em 1980,
correu para fora de suas dívidas no Haiti, em 1989, e está sendo processado
de todos os seus bens por duas ex-mulheres? A resposta é simples:
qualquer lei que diz que eu não estou autorizado a ter em conta
informações que vem o meu caminho é _flawed_ e deve ser
ignorada. Discando para um crédito ainda em Belize é um
abordagem--exceto escutas ainda pode ter-me apanhado.
O ciberespaço permite que muito mais seguro e conveniente
ignora a essas leis.
- (Para aqueles de vocês que pensam que ignora tais leis são
imoral, difícil. Forte de criptografia permite isso. Acostume-se a ele.)

16.3.4. Início da história da criptografia anarquia
+ 1987-8, AMIX, Salin:, Manifesto
- discutido criptografia implicações com Phil Salin: e Gayle
Pergamit, em dezembro de 1987
- com um grupo maior, incluindo Marc Stiegler, Dave Ross,
Jim Bennett, Phil Salin:, etc., em junho de 1988.
- lançado "A Criptografia Anarquista Manifesto", em agosto de 1988.
- Fen LaBalme tinha "Guerillan Informações Net" (GIN), que ele
e eu discutimos em 1988 na Conferência de Hackers
+ ", Da Arcos para Criptografia," de 1987?
- fez pontos semelhantes, mas com algumas diferenças importantes
- TAZ também está sendo escrita neste momento

16.4. A Criptografia Manifesto Anarquista

16.4.1. Inalterado, pois a escrita em meados de 1988, exceto para o meu e-
endereço de correio.
- Há algumas alterações que eu faria, mas...
- Ele foi escrito rapidamente, e em um estilo deliberadamente
imitar o que eu me lembrei do "Manifesto Comunista." (para
irônico razões)
- Ainda., Estou orgulhoso de que há mais de seis anos eu correctamente
vi alguns dos principais pontos que Cypherpunks ajudaram a fazer
acontecer: remetentes, anônimo communictation, reputação-

os sistemas de base, etc.
- Para a história do amor de deus, aqui está ele:
16.4.2.

A Criptografia Manifesto Anarquista

Timothy C. Maio
tcmay@netcom.com

Um fantasma está assombrando o mundo moderno, o espectro de criptografia
a anarquia.

A tecnologia informática está a ponto de fornecer a capacidade de
para os indivíduos e grupos para se comunicar e interagir com
uns aos outros em uma forma totalmente anônima. Duas pessoas podem
trocar mensagens, realizar negócios, e negociar eletrônico
contratos, sem nunca saber o Verdadeiro Nome, ou jurídica
identidade, do outro. As interações nas redes serão
untraceable, através de extensa re-roteamento de pacotes criptografados
e à prova de caixas que implementam a criptografia
protocolos com quase perfeito de garantia contra qualquer
adulteração. Reputação vai ser de importância central, longe
mais importante nas relações que até mesmo os ratings de crédito
hoje. Estes desenvolvimentos irão alterar completamente a natureza do
regulamento do governo, a capacidade fiscal e de controle de
interações econômicas, a capacidade de manter informações
em segredo, e até mesmo alterar a natureza de confiança e de
reputação.

A tecnologia para essa revolução--e certamente será
tanto uma revolução social e econômica--já existia em teoria
durante a última década. Os métodos são baseados em chave pública
criptografia, zero-conhecimento de sistemas interativos de provas, e
vários protocolos de software para interação, autenticação,
e verificação. O foco tem sido, até agora acadêmica
conferências na Europa e EUA, conferências monitorado
de perto pela Agência de Segurança Nacional. Mas só recentemente
tem de redes de computador e computadores pessoais atingido
a velocidade suficiente para fazer as idéias praticamente realizável.
E os próximos dez anos trarão suficiente adicional de velocidade para
faça as idéias economicamente viável e, essencialmente,
imparável. Redes de alta velocidade, ISDN, à prova de adulteração caixas,
cartões inteligentes, satélites de banda Ku, transmissores, multi-MIPS

computadores pessoais e criptografia fichas agora sob
desenvolvimento serão algumas das tecnologias.

O Estado será, naturalmente, tentar diminuir ou interromper a disseminação de
esta tecnologia, citando preocupações de segurança nacional, o uso de
a tecnologia por traficantes, sonegadores e os medos do
sociedade de desintegração. Muitas destas questões serão
válido; criptografia anarquia vai permitir nacional segredos para o comércio
livremente e vai permitir a ilegal e roubo de materiais a serem
negociados. Um anônimo informatizado de mercado ainda vai fazer
possível abominável mercados para assassinatos e extorsão.
Vários penal e os elementos estrangeiros serão usuários ativos do
CryptoNet. Mas isso não vai parar a propagação de criptografia
a anarquia.

Assim como a tecnologia de impressão alterado e reduzido a
o poder das guildas medievais e social, estrutura de poder, então
também cryptologic métodos altera fundamentalmente a natureza
de empresas
e de interferência do governo em transações econômicas.
Combinado com os novos mercados de informação, criptografia anarquia
vai criar um mercado líquido para todos e qualquer material que
pode ser colocado em palavras e imagens. E assim como uma aparentemente
menor invenção como o arame farpado tornou possível a esgrima,
fora de vastas fazendas e fazendas, assim, alterando para sempre o
conceitos de terra e direitos de propriedade na fronteira Oeste, por
também a aparentemente pequena descoberta de um
arcano ramo da matemática que vem a ser o fio clippers
que desmontar o arame farpado, cerca a propriedade intelectual.

Surgir, você não tem nada a perder, mas o seu cercas com arame farpado!

16.5. As mudanças estão Chegando
16.5.1. A tecnologia está a alterar dramaticamente a natureza de
governos.
- Pode soar como newage a tendência, mas forte de criptografia é
"capacitação tecnológica." Ela literalmente dá o poder para
indivíduos. Como Sam Colt, o que os torna iguais.
- "A política nunca deu qualquer uma liberdade duradoura, e ele
nunca será. Nada ganhou através da política será perdido
novamente assim que a sociedade se sente ameaçada. Se mais
Os americanos nunca foram oprimidos pelo governo

(além de um plano anual de assalto) é porque a maioria deles
nunca fiz nada para ameaçar o governo
interesses". [Mike Ingle, 1994-01-01]
+ Tese: Forte de criptografia é uma coisa boa
- ferramenta contra os governos de todos os sabores, esquerda e direita
- liberdade religiosa
- escolha pessoal
16.5.2. Perigos da democracia em geral, e a democracia electrónica em particular
- mob regra, os direitos das minorias ignorado
- muitas coisas obter decidido por votação que não tem nenhum negócio
sendo votada
- "não imposto de mim...", De Tocqueville do aviso
+ a democracia electrónica é ainda pior
- move-se mais do republicana, sistema representativo para
electronc o governo da multidão
- muito rápida de um sistema
- Detweiler do "electrocrasy" (grafia?)...danos no cérebro,
mal pensado
16.5.3. O colapso da democracia é previsto por muitos
+ o "tombamento fator" excedeu, com taxas de tributação em
50% ou mais nos países mais desenvolvidos, com condições de
"tributação sem representação" muito além de qualquer coisa em
América colonial
- com políticos profissionais...e principalmente milionários
a correr para o escritório
- a Cincinato (sp?) abordagem de ir para o governo
apenas por alguns anos, voltando para a fazenda ou
de negócios, é uma piada
+ aumento do nominalismo [defendido por James Donald]
- "Depois de democracia Ateniense auto destruídos, vários
as partes em conflito achei que eles só poderiam ter paz se
eles repudiaram onipotente governo. Eles juntam um
acordo de paz que, em parte, proclamou limites para
o governo, em parte reconhecido inerente limites para o que
era bom que os governos fazem e em parte garantido
de que o governo não ir além do que foi
adequada para que o governo possa fazer, que a maioria não poderia
fazer como o prazer com a minoria, que não de qualquer ato de
o poder era uma lei, essa lei não foi apenas o que o
o governo quis.

Eles não concordam sobre uma constituição, mas aceitou

o respeito de uma constituição não escrita que já existia no
algum sentido.

Um acordo semelhante fundamenta a constituição Americana
(agora extinto) e o inglês declaração de direito (também
extinto)

O problema com tais formal dos acordos de paz é o que
eles só podem ser colocados juntos depois que o governo tem
substancialmente em colapso. Alguns de nós gostaria de tentar outro
possibilidades em caso de queda.

A constituição Americana em colapso por causa da ascensão
de nominalist teorias "A constituição diz que qualquer que seja a
os tribunais dizem que ele diz." [James Donald, 1994-08-31]
- A guerra às Drogas, conspiração encargos, revistas aleatórias,
preparação para situações de emergência de ordens de Operação Vampiro Assassino,
Operação de Trem de Noite, REX-84). As mortes de mais de um
dezenas de repórteres e tipsters durante a última década, muitos dos
- os cobrindo o Iran-Contras história, o tráfico de droga, o
CIA relações...a Fazenda parece ser "inundando" mais e
mais esses arruaceiros na cabeça de março de direção
o fascismo.
+ De Tocqueville do aviso de que a experiência Americana em
a democracia iria durar apenas até os eleitores descobriram que
poderia escolher os bolsos dos outros nas urnas
- um ponto alcançado cerca de 60 anos atrás
- (antes do imposto de renda federal e, em seguida, o "Novo Negócio"
havia sistêmica limitações sobre essa capacidade para o
bolsos dos outros, apesar de populista anseios por
algumas....após o New Deal, e a Grande Sociedade, o
era moderna da fuga de tributação iniciado.)
16.5.4. Depredações do Estado
+ "Discriminação leis"..escolha não permitido
- o clube de strip em LA forçado a instalar acesso cadeira de rodas-
-para os dançarinos!
- idade não é mais permitido ser um fator...mordaça!
+ a democracia de forma desenfreada....piores medos de Fundadores
- votos em tudo...
- controle de armas, convulsões, usando as leis de zoneamento (com FFL
inspeções informantes)
- estado de bem-estar,...Murray, cidades do interior fez pior...roubo
- "moeda de exportação" leis " como é absurdo que os governos

tentativa de controlar o que as pessoas fazem com o seu próprio dinheiro!
16.5.5. As coisas podem piorar, financeiramente (negativo
vista,porém há também razões para ser otimista)
+ um estado de bem-estar que é careening em direção à borda de uma
cliff...escalada de gastos, aumentando constantemente nacional
dívida (com nenhum sinal de que isso nunca vai ser pago para baixo)
- pensões encargos estão a aumentar drasticamente, de acordo com
"O economista", 1994-08.
- o link para crypto é que a gente tinha melhor encontrar formas para
vacinar-se a partir da próxima crise
+ Segurança Social, outros planos de previdência são definidas em 30-40%
de todo o PIB
- muitos promies, as pessoas vivem mais tempo
- orçamento: us $20 trilhões em "responsabilidades"
- cuidados de saúde expectativas... crescente dívida nacional
16.5.6. As fronteiras estão se tornando transparentes os dados...terabytes por dia
estão fluindo através das fronteiras, com milhares de formatos de dados
e praticamente indistinguível de outras mensagens.
Arquivos compactados, divisão de arquivos, de imagens, de sons, de propriedade
formatos de encriptação, etc. Uma vez que pode _almost_ pena ANS, em
a desesperança de seu trabalho.

16.6. A liberdade de expressão e Liberdade--Os Efeitos de Criptografia
16.6.1. "O que a liberdade de expressão está se tornando."
+ Uma maior disposição para o limite de fala, anexando
restrições baseadas em ser "comercial" ou "odeio
a fala."
+ publicidade leis sendo o óbvio exemplo: fumar,
o álcool, etc.
- médicos, advogados, etc.
- sexo, nudez
- mesmo as leis que dizem os outdoors não pode mostrar armas
- Um arrepiante, mas muito sentimento comum na rede é mostrado
por esta citação: "É a liberdade de expressão para vomitar o racismo ,
e steriotypes, apenas, porque lhe falta o intelectual
capacidade para compreender o que , talvez, em algum lugar, há
uma forma diferente de vida, que não é congruente com o seu
pré-concebida de noções?" [Andrew Beckwith, soc.a cultura.eua]
16.6.2. Nós realmente não temos liberdade de expressão
- as leis eleitorais
- publicidade leis
+ "calúnia" e "difamação"
- felizmente, sistemas anónimos vai fazer este simulado

+ permissão necessária...de licenciamento, aprovação, de certificação de
- "qualificações"
- é concedido, Supremes deixaram claro que a política
comentários não podem ser restrito, mas muitas outras áreas
- muitas vezes a distinção envolve "para pagar"
- Talvez você esteja pensando que estas não são realmente exemplos
de censura do governo, apenas de _other crimes_ e
other rights tendo precedência. Assim, os anunciantes não podem
fazer falsas ou enganosas, e não pode anunciar a
perigosos ou, de outra forma não aprovados itens. E eu não posso fazer
diagnósticos médicos, ou dar estruturais e geológicos
o conselho, e assim por diante...uma dúzia de bons exemplos. Mas estes
restrições de castrar a liberdade de expressão, deixando apenas banal
expressão, devidamente cobertas "opiniões pessoais", como
a liberdade de expressão que é permitido...e até que é ofen
sujeito a loucura judiciais e ameaças de ação legal.

16.7. A Natureza de Anarchies
Item 16.7.1. Anarquia não significa o caos e a matar
- Como J. Bruce Dawson colocá-lo em uma revisão do Linux no
Setembro, 1994 "Byte" "É a anarquia no seu melhor."
+ Ironicamente, criptografia anarquia não admitir a possibilidade (e
daí probablility) de mais um contrato de homicídios como um
ultimate mecanismo de execução de contratos de outra forma
inaplicável.
- que é que está ocorrendo em drogas e outros crimes
situaions: as partes não podem ir para a polícia ou os tribunais
para a retificação de erros, por isso eles precisam ter o máximo
ameaça de morte ao impor negócios. Isso faz sentido
a partir de uma reputação/teoria dos jogos, do ponto de vista.
16.7.2. Esquerdistas podem ser anarquistas, muito
- Na verdade, essa tende a ser a interpretação popular de
a anarquia. (Além da bomba jogando, anti-Czar anarquistas
do século 19, e a bomba jogando anarquistas de
EUA e, no início deste século.)
+ "Zonas Autónomas temporárias" (TAZ)
- Hakim Bey (pseudónimo de)
- Mondo 2000, livros, (verifique com Dave Mandl, que ajuda a
publicá-los)
16.7.3. Anárquico de desenvolvimento
+ Mercados e comportamentos emergentes vs. planejado de desenvolvimento
- princípios de localidade entram em jogo (os jogadores locais
sabem o que querem e o quanto eles vão pagar por isso)

- central planejadores têm "top-down" perspectivas
- Kevin Kelley e "Fora de Controle" (1994). Além Disso, David
Friedman, do "Tecnologias de Liberdade."
- Um exemplo ouvi falar recentemente foi Carroll College, em
Wisconsin. Em vez da construção de vias e calçadas
todo o recém-construído motivos, a terra foi deixada
nua. Depois de algum tempo, o "emergente caminhos" escolhidos por
alunos e professores foram, então, transformadas em vias pavimentadas,
perfeitamente resolver o problema de pessoas que não utilizam o
"planejada" de ensino. Eu acho que muito da vida funciona este
caminho. Por isso, não o Líquido ("informações caminhos"?).
- anarchies são muito mais comuns do que a maioria das pessoas
acho que...relações pessoais, escolhas na vida, etc.
16.7.4. O sistema financeiro mundial é um bom exemplo: além do
alcance de qualquer governo, mesmo os EUA Novo Mundo
Ordem, o dinheiro se move e fluxos de dúvidas e preocupações aparecem.
Estatizados os governos são impotentes para parar a desvalorização do
suas moedas, com os investidores a mover seus ativos (mesmo as mais leves
move pode ter grandes efeitos marginais).
- "anarquia" não é um termo mais seria aplicável, mas é uma
a anarquia no sentido de que não há nenhuma governantes ("um arco"),
sem comando central da estrutura.

16.8. A Natureza de Criptografia Anarquia
16.8.1. "O que é Criptografia Anarquia?"
+ "Por isso o nome?"
+ parcial de um trocadilho sobre várias coisas"
- "criptografia", que significa "oculto", como usada no termo "criptografia
fascista" (Gore Vidal chamado William F. Buckley este)
- "crypto anarquia", o que significa a anarquia será oculto,
não necessariamente visível
- e, claro, criptologia está centralmente invovled
+ Motivação
- Vernor Vinge de "Nomes Verdadeiros"
- Ayn Rand foi um dos principais motivadores de criptografia
a anarquia. O que ela queria fazer com a tecnologia de materiais
(mirrors mais de Galt Gulch) é _much_ feito mais facilmente
com matemática e tecnologia.
16.8.2. "A anarquia afasta as pessoas...por que não um mais palatável nome?"
- as pessoas não entendem a prazo; se pessoas entenderam a
prazo, poderia ser mais aceitável
- alguns têm sugerido que eu chamo de "digital liberdade", ou
algo do tipo, mas eu prefiro ficar com a menção histórica

16.8.3. Voluntária interações envolvem Schelling pontos, mutuamente acordado pontos de acordo
16.8.4. Crypto anarquia como uma ideologia e não como um plano.
- Sem falsa modéstia, eu acho criptografia anarquia é um dos poucos reais contribuições para a ideologia na memória recente. O noção de indivíduos tornarem-se independentes dos estados ignorando ordinária canais de controle é uma nova. Enquanto tem havido sugestões de presente no género cyberpunk de escrita e áreas relacionadas, (as obras de Vinge especialmente), o tradicional libertário e anarquista movimentos principalmente ignorando as consequências do forte crypto.
- Curiosamente, David Friedman, filho de Milton e autor de "A máquina de Liberdade," tornou-se um convertido às idéias. Pelo menos o suficiente para dar uma palestra em Los Angeles intitula "Crypto Anarquia e o Estado."
- Convencionais ideologia política não conseguiu perceber o grandes mudanças vem ao longo de várias décadas. Focando sem possibilidade de vitória batalhas nas urnas, eles desperdiçar as suas energias; eles junte-se a política processo, mas eles não têm nada para "lidar" com, para que eles perder. O Americano médio, na verdade, _wants_ para escolher bolsos de seus vizinhos (pagar para "livre" de cuidados de saúde, para parar de empresas de lançar-off desnecessários trabalhadores, para trazer mais carne de porco de volta para o local enonomy), pelo que a média de eleitor é altamente improvável que alguma vez votar para um prinicpled Candidato libertário.
- Felizmente, como as pessoas votam tem pouco efeito sobre determinados "chão verdades" que emergem das novas tecnologias e a nova a evolução económica.

16.9. Utiliza de Criptografia Anarquia
16.9.1. Mercados livre das leis locais (digital mercados negros, em menos para os itens que podem ser movidos através do ciberespaço)
16.9.2. Espionagem

16.10. As Implicações-Positivos e Negativos-de Criptografia Anarquia
16.10.1. "Quais são algumas das implicações de criptografia anarquia?"
+ Um retorno aos contratos
- chorões não pode ir lá fora e queixam-se de contratos de
- refere-se a: trabalhadores, condições de trabalho, ações, ferir sentimentos
- com untraceable de comunicação, redes virtuais....

+ De espionagem
+ De espionagem já está mudando dramaticamente.
+ De Steele (ou Steeler?) "fontes abertas"
- coleta de informações a partir de milhares de fontes da Internet
- Bem, essa faca de dois gumes..
+ Vai permitir:
- BlackNet-tipo de solicitações de segredos militares ("Vai
pagar 300.000 dólares para xxxx")
+ Digital Morto Cai
- totalmente seguro, indetectáveis (piscinas, BlackNet modo)
- não há latas de Coca-cola perto da base do carvalho árvores fora da Rota
42
- sem marcas de giz em caixas de correio para sinalizar uma mensagem
pronto
- não "queima" de espiões seguindo-os dead drops
- Não admira que os fantasmas são pirei!
- Forte de criptografia também terá um grande efeito sobre a NSA, CIA,
e FBI habilidades brasileiras, para realizar fiscalização,
e para fazer nacionais e estrangeiros, contra-espionagem
- Isso não é completamente uma coisa grande, como pode ser
some de contra-espionagem trabalho que é útil (eu sou
talvez trair meu remanescentes preconceitos), mas não há
realmente só uma coisa a dizer sobre isso: acostume-se a ele.
Nada menos do que um estado policial totalitário (e
provavelmente não, mesmo que, dada a disseminação do forte
crypto) pode parar a estas tendências.
-
+ Ignorando sanções e boicotes
- Só porque o Bill Clinton não como os governantes de
O Haiti não é razão para mim para honrar o seu "sanções"
- A escolha Individual, que se tornou possível pela forte de criptografia
(untraceable transações, pseudônimos, mercados negros)
+ Informações de Mercados e de Dados Paraísos
- médico
- científicos
- conhecimento corporativo
- dossiês
+ relatórios de crédito
- sem as absurdas regras a limitar o que as pessoas podem armazenar
em seus computadores (por exemplo, se a Alice mantém registros de ir
de volta de mais de 7 anos, blá, blá, podem ser lançados em
prisão por violar o "Fair credit Reporting Act")
- ignorando tais leis

- é verdade, os governos podem tentar forçar a divulgação de
"razões" para todas as decisões (uma tendência popular, onde
mesmo a empregada doméstica não pode ser dispensada sem o
"razões" que é posta em questão!); isto significa que
qualquer pessoa aceder a esses ventos (ou no ciberespaço mesmo...
diferença) bases de dados tem de encontrar alguma razão aceitável
para as acções que toma...não deve ser muito difícil
- (assim como em muitas dessas idéias, a beleza é que o
utilizar de tais serviços é voluntária....)
+ Consultoria
- aumento da liquidez das informações
+ de operações ilegais
+ untraceability e dinheiro digital significa muitos "escuro"
possibilidades
- mercados para os assassinatos
- propriedade roubada
- violação de direitos autorais
+ De espionagem
- informação de mercados (a la AMIX)
- "digital mortos gotas"
- Contas Offshore
- Lavagem de dinheiro
+ Mercados para os Assassinatos
- Este é um dos mais preocupantes implicações de criptografia
a anarquia. Na verdade, ele surge imediatamente para fora do forte,
inquebrável e rastreáveis de comunicação e de alguma forma
de untraceable dinheiro digital. Distrurbing pode ser, mas
as implicações são também interessante considerar...e
inevitável.
- E não todas as implicações são totalmente negativo.
+ deve colocar o temor de Deus políticos
- "O dia do Chacal" electrónicos
- qualquer grupo de interesse que pode (anonimamente) reunir dinheiro
pode ter um político eletrocutado. Positivos e negativos
implicações, é claro.
- A verdade é que algumas pessoas simplesmente precisa matar. Chocante como
isso pode soar para muitos, certamente, todos concordam que
Hitler merecia a morte. O "estado de direito" soa nobre,
mas quando o desprezível pessoas controlam a lei, outros
as medidas são chamados.
- Pessoalmente, eu considero qualquer um que ameace o que eu acho
de como direitos básicos podem precisar matar. Eu sou retidos pela
as repercussões, os perigos. Com mercados líquidos para

de liquidação judicial, as coisas podem mudar drasticamente.

16.10.2. O Lado Negativo de Criptografia Anarquia

+ Comentário:

- Há muito real implicações negativas;

superados no todo, os benefícios. Depois de tudo, livre

discurso tem aspectos negativos. Poronography tem aspectos negativos. (Este

pode não ser muito convincente para muitos....Eu não posso fazer isso aqui-

-a gestalt tem de ser absorvido e considerada.)

+ Abominável mercados

- contrato de assassinatos

- pode coletar o dinheiro anonimamente para ter alguém

desenvolvi...quase ninguém que é controverso, pode gerar

o suficiente "contribuições"

- seqüestro, extorsão

+ De contratos e assassinatos

- "Vai matar por $5000"

+ fornece um mais "líquido" de mercado (pun intended)

- os vendedores e compradores de forma mais eficiente correspondência

- FBI picadas (que são comuns na contratação de bater homens) são

feito quase impossível

- canônico "lado escuro" exemplo--Eric Drexler, quando

disse isso em 1988, foi horrorizado e alegou que eu estava

imoral mesmo continuar a trabalhar sobre as implicações de

criptografia de anarquia!

- feito muito mais fácil a incapacidade para rastreamento de pagamentos, os

a falta de encontros físicos, etc.

+ Potencial de ilegalidade

- corrupção, o abuso, a chantagem

- o cinismo sobre quem pode manipular o sistema

+ De solicitação de Crimes

- untraceably, como vimos

+ Suborno de Funcionários e Influenciar de Eleições

- e o contato direto com os funcionários não é mesmo

necessário...que se alguém "lhe permite ser conhecido" que um

conselho de votos em favor de algum projeto desejado resultará

em contribuições de campanha?

+ Criança molestors, pederasts, e estupradores

- sistema de encriptação de seus próprios diários com PGP (um caso real, diz o

FBI)

- isto levanta a questão da privacidade em toda a sua glória...privacidade

protege a ilegalidade...ele sempre foi e ele sempre será

+ De espionagem é muito mais fácil

- partir a cara assistindo navios partem de um porto para o real

roubo de defesa dos segredos
- trabalho de defesa contra espiões torna-se muito mais
difícil: o fim micropontos e a tinta invisível, que
com o LSB e o método de como que ainda esconde o muito
existência de mensagens criptografadas!
+ Roubo de informações
- a partir de empresas e pessoas singulares
- sociedades como as conhecemos hoje, vai ter que mudar
- a liquidez das informações
- venda de segredos empresariais ou informações pessoais
+ Digilantes e Estrelas Câmaras
- o risco de justiça executando o amok?
+ Alguns assassinos não são reabilitados e precisa ser
eliminados, através de mais de meio direto
+ Preço, Rhode Island, 21, 4 brutais assassinatos
- facadas das crianças, a mãe, o outro
+ para animais como este, linchamentos discreto...
execução...é justificada...
- ou, pelo menos, alguns de nós o considere justificado
- o que eu considero ser uma coisa boa
- isso se relaciona com um tema importante: untraceable
comunicação e mercados significa a capacidade de "opt
fora" da moral convencional
+ Perda de confiança
+ mesmo em famílias, especialmente se o governo oferece
os prémios e recompensas
- lembre-se de Pavel Morozov na URSS, DARE-tipo de programas
(informar no pais)
- mais de 50% de todos os IRS fatos envolvem um cônjuge
informar ao IRS
+ como vai impostos ser afetado pelo aumento do mercado negro?
- uma espécie de curva de Laffer, em que alguns limiar de
tributação disparadores de nojo e esforços para fugir dos impostos
- não está claro o quão grande é o atual economia subterrânea
é....as autoridades estão motivados para o tamanho misstate
(dependendo de sua agenda)
+ Evasão fiscal (não estou defendendo a tributação, apenas apontando
o que mais chamaria de um lado escuro da autoridade de CERTIFICAÇÃO)
+ Pela condução dos negócios secretamente, usando de permuta de sistemas,
moedas alternativas ou sistemas de crédito, etc.
- la a advogados que utilizam AMIX-como sistemas para evitar
sendo tributada em consultas mútuas
+ Por isso ventos

- para que os "produtos" são todos os ventos, mesmo que
muitos ou a maioria dos trabalhadores são teletrabalho ou usando
CA esquemas de
- lembre-se que muitos músicos deixaram a Europa para evitar 90% do imposto de
taxas
+ o "ninho de ovos de" scam: desenho em um montante fixo, não relatada
+ Cenário: Alice vende algo muito valioso-talvez
as especificações sobre um novo produto-para Bob. Ela depósitos a
taxa, que é, digamos, um milhão de dólares, em uma série de
contas. Esta taxa não é relatado para o IRS ou de qualquer
outra coisa.
- a taxa poderia ser em dinheiro ou em uma "promessa"
- em várias contas, ou apenas um
+ de qualquer modo, a idéia é a de que ela agora é pago, digamos,
Us $70.000 por ano durante os próximos 20 anos (o que com
juros), como um "consultor" para a empresa que
representa a sua fundos
- isso, claro, não CA de qualquer forma, apenas alguns
discreto advogados
- e, claro, Alice relatórios de renda para a
IRS-eles nunca desafio contribuinte para "justificar"
trabalho feito (e seria incapaz de "não permitir"
o trabalho, tal como a Alice poderia chamá-lo de um "retentor", ou
como pagar pelo Conselho de Administração funções, ou
qualquer que seja...na prática, é mais fácil chamá-lo de
consultoria)
+ esses golpes estão intimamente relacionadas com semelhante golpes para
lavagem de dinheiro, por exemplo, com a venda de ativos da empresa em
artificialmente baixos (ou altos) preços
- um dono, Charles, poderia vender ativos para uma estrangeira
empresa a preços baixos e, em seguida, ser recompensado em impostos
livre, debaixo da mesa, o dinheiro depositado em uma estrangeira
conta, e estamos de volta para a situação acima
+ Conluio já é comum; métodos de criptografia vai fazer alguma
tais conluios mais fácil
- antiquários em um leilão
+ de espionagem e de negociação nacional segredos (este tem
aspectos positivos bem)
- "informações de mercado" e anônimo de dinheiro digital
- (Esta realização, no final de 1987, foi a inspiração para
as ideias por trás de criptografia anarquia.)
- a desconfiança
- alargamento do fosso entre ricos e pobres, ou quem pode usar

as ferramentas de idade e aqueles que não podem
16.10.3. O Lado Positivo de Criptografia Anarquia
- (outras razões positivas são implicitamente espalhados por todo
este esboço)
+ puro, uma espécie de liberalismo
- aqueles que têm medo de CA pode ficar de fora (não estritamente
verdade, como os efeitos de ondulação)
- uma forma de evitar a erosão da moral, contratos, e
committments (via o papel central que a reputação e a
exclusão de distorcer os governos)
- responsabilidade individual
- proteger sua privacidade ao utilizar hipertexto e ciberespaço
serviços (muitos problemas aqui)
- "é puro" (pmi do perverso que gosta de ver
ideias radicais)
+ Um retorno a 4ª Alteração proteções (ou melhor)
- Sob o sistema atual, se o governo suspeita que um
pessoa de ocultação de bens, de conspiração, de atos ilegais,
de evasão fiscal, etc., eles podem facilmente capturar banco
contas, contas de estoque, barcos, carros, ce. Em particular,
o proprietário tem pouca oportunidade de proteger estes ativos.
- aumento da liquidez nos mercados
+ enfraquecimento dos estados centrais
- perda de receitas fiscais
- redução do controle
- liberdade, liberdade pessoal
- dados paraísos, para ignorar local de leis restritivas
+ Anonymous mercados para assassinatos vai ter algumas boas
aspectos
- a liquidação de políticos e de outros ladrões, o
matar aqueles que ajudaram a communalization
da propriedade privada
- uma terrível swift espada
16.10.4. Vou ficar triste se métodos anônimos permitir untraceable mercados
para assassinatos? Isso depende. Em muitos casos, as pessoas merecem
a morte, aqueles que escaparam da justiça, aqueles que têm quebrado
solene compromisso, etc. Arma agarrando políticos, para
exemplo deve ser morto fora de mão. Anônimo roedores
serviços de remoção será um instrumento de liberdade. O BATF agentes
quem assassinou Randy de Weaver esposa e filho deve ser filmado. Se
os tribunais não fazê-lo, um mercado para a hits vai fazê-lo.
- (Imagine, por um momento, um "anônimo fundo" para recolher o
dinheiro para tal um sucesso. Possibilidades interessantes.)

- "Crypto Estrelas Câmaras," ou o que poderia ser chamado de
"digilantes," podem ser formados em linha, e untraceably, para
mete a justiça para os deixar fora em tecnicalidades. Não
completamente uma coisa ruim.
16.10.5. na interferência em negócios como justificadas pela "sociedade suporta
você" argumentos (e "opt-out)
+ Tem sido tradicionalmente argumentou que a sociedade/governo
tem o direito de regular os negócios, impor regras de
comportamento, etc., por um par de razões:
- "promover o bem-estar geral" (um nebuloso razão)
+ porque o governo constrói a infra-estrutura que faz
companhia
- as estradas, sistemas de transporte, etc. (na verdade, a maioria
são em particular construído...apenas estradas e canal são
publicamente construído, e eles certamente não _have_ para
ser)
- as forças de polícia, os tribunais, a execução dos contratos,
disputas, etc.
- proteção de países estrangeiros, a pauta de negociações,
etc., até a *física* proteção contra
invadindo países
+ Mas com criptografia anarquia, *todos* estas razões desaparecer!
- a sociedade não é "habilitação" da empresa que está sendo transacionado
(depois de tudo, as partes não precisamos necessariamente saber o que
países que o outro é!)
- não, nacionais ou locais, os tribunais estão a ser utilizados, de modo que este conjunto de
razões sai pela janela
- nenhuma ameaça de invasão...ou se existe, não é
algo que os governos podem endereço
+ Assim, em adição à base de ineficácia da proibição do
crypto anarquia--curta da proibição de criptografia--não há
também não é viável argumento para ter os governos interferem na
esses tradicionais motivos.
- (As razões para interferir com base em medos para
o seu próprio futuro e medos sobre desagradáveis e abominável
dos mercados desenvolvidos (partes do corpo, assassinatos,
segredos comerciais, evasão de divisas, etc.) são, naturalmente, ainda
"válido", visto a partir da perspectiva deles, mas os outros
razões não estão.)

16.11. A ética e a Moral de Criptografia Anarquia
16.11.1. "Como você quadrado essas idéias com a democracia?"
- Eu não; democracia correr amok, o cumprimento de

Tocqueville a previsão de que a democracia Americana iria durar
somente até que os Americanos descobriram que poderiam escolher os bolsos
de seus vizinhos nas urnas
- pouca chance de mudar de opinião pública, de educá-las
- crypto anarquia é um movimento do indivíduo de optar, não
de alterações de massa e ação política
16.11.2. "Existe uma responsabilidade moral para garantir que o conjunto de
efeitos de criptografia anarquia são mais favoráveis do que desfavoráveis
antes de promovê-lo?"
- Eu não penso assim, mais do que Thomas Jefferson deve
analisaram as implicações futuras de liberdade antes de
empurrando-a com tanta força.
- Todas as decisões têm implicações. Alguns até custar vidas. Por
não tornar-se médico de trabalho na África Sub-Sahariana, eu
"matou milhares de pessoas"? Certamente eu poderia ter salvo a vida
de milhares de pessoas. Mas eu não matá-los apenas
porque eu escolhi não ser um médico. Da mesma forma, dando
o dinheiro aos famintos camponeses, em Bangladesh, vidas poderiam
inegavelmente, ser "salvo". Mas não dar o dinheiro não
assassinato-los.
- Mas tais ações ou omissões não são o mesmo, em minha mente,
como os actos da comissão. A minha liberdade, através de criptografia anarquia, é
não é um ato de força e de si mesmo.
- Desenvolvimento de uma ideia, não é a mesma agressão.
- Crypto anarquia é de cerca de pessoal de retirada do
do sistema, as "tecnologias de desconexão," de Kevin
Kelly palavras.
16.11.3. "Deve indivíduos têm o poder de decidir o que vai
revelar para os outros, e autoridades?"
- Para muitos ou mesmo a maioria de nós, isso tem uma resposta fácil, e
é axiomatically verdadeiro. Mas outros têm dúvidas, e mais
as pessoas podem ter dúvidas quanto algumas de fácil antecipado
develpoments ocorrer.
- (Por exemplo, os pedófilos usando o muito temido "fortaleza
crypto," terroristas comunicação em inquebrável códigos, tza
evasores, etc. Muitos exemplos.)
- Mas porque algumas pessoas usam criptografia para fazer putativamente mal
as coisas, deve ser dado? Portas fechadas pode
ocultar atos criminosos, mas nós não a proibição de portas fechadas.
16.11.4. "Não há alguns perigos e riscos para deixar as pessoas escolher
e escolher a sua moralidade?"
- (Perguntas sobre o grupo de consenso, as ações do
estado vs. ações do indivíduo, e o "rebanho.)

- De fato, há perigos e riscos. Na privacidade de sua
em casa, o meu vizinho pode ser a operação de uma tortura, do calabouço para
crianças que ele capta. Mas ausente a prova real de
isso, a maioria das nações não sancionada a procura aleatória
de domicílios particulares (nem mesmo a URSS, a medida em que eu
saiba).

16.11.5. "Como um membro de um odiado minoria (crypto anarquistas) eu
ao invés de tomar minhas chances em um mercado aberto do que o risco de oficial
discriminação pelo estado.....Felizmente, a tecnologia que
estão em desenvolvimento permitirá que todos os que se preocupa com a recusar
participar deste coercitiva distribuição de poder." [Duncan
Frissell, 1994-09-08]

16.11.6. "Há tecnologias que devem ser "parado" antes mesmo de
eles são implantados?"

- Caixa de Pandora, "coisas que o Homem não deveria saber", etc.
- Ela costumava ser que a minha resposta foi, principalmente, um claro "Não", com
nuclear e armas biológicas como a única clara exceção.
Mas os recentes acontecimentos envolvendo a tecla de custódia de ter me causou
repensar as coisas.
- Imagine uma empresa que está a desenvolver casa de vigilância
câmeras...talvez por assaltante de prevenção, segurança infantil,
etc. Os pais podem monitorar Junior no teto câmeras montadas
que não pode ser facilmente adulterado ou desligado, sem
o envio de alarmes. Tudo muito bem.
- Agora, imagine que os ganchos são colocados para estes sistemas de câmera para
enviar as imagens capturadas para um escritório central. Novamente, não
necessariamente uma má idéia, os turistas podem querer a sua segurança
empresa monitorar suas casas, etc.
- O perigo é que um repressivas do governo poderia fazer a
obrigatório do processo....de que outra forma para pegar sexual desvia,
criança molestors, os cultivadores de maconha, os falsificadores, e o
como?
- Som implausível, inaceitável, certo? Bem, key escrow é
uma forma deste.
- O Perigo. Que OS vendedores colocam esses SKE sistemas
lugar sem proteção adequada contra tecla de caução a ser
tornou-se obrigatório em alguma data futura.

16.11.7. "Não crypto anarquia permitir algumas pessoas para fazer coisas ruins?"

- Certo, então o que mais há de novo? Quartos privativos permite plotters para
trama de conspirações. Etc.
- Não parece muito simplista, mas a maioria das coisas que pensamos
como direitos básicos, permitir que várias ilegal, de mau gosto, ou
ruim as coisas para ir em frente. Parte do acordo que fazemos.

- "Claro, você pode impedir que o contrato de assassinatos exigindo
todos carregam governo "caucionada" gravações para
gravar todas as suas conversas e obrigando-os a manter um
diário em todos os momentos alibing suas todas as suas atividades.
Isso também torna muito mais fácil para carimbar a criança
a pornografia, o plutónio contrabando, e a discriminação social
contra o politicamente correto". [James Donald, 1994-09-
09]

16.12. Problemas práticos com Criptografia Anarquia
16.12.1. "O que se "bandidos" usar criptografia inquebrável?"
- O que se criminosos em potencial podem ter fechaduras
suas portas? O que se estupradores em potencial pode comprar pornografia?
O que se....
- Esses são todos os homens de palha usado em várias formas ao longo de
a história por tiranos para o controle de suas populações. O
"sheepocracies" do moderno chamado era democrática são
a votação fora suas antigas liberdades em favor de berço para
túmulo de segurança e de segurança.
- O mais recente tack é propor limites de privacidade para ajudar a
pegar criminosos, pedófilo, terroristas, e o pai rapers.
Deus nos ajude se isso vier a acontecer. Mas Cypherpunks não
esperar a hora de Deus, eles escrever código!
16.12.2. Lidar com o "Abominável " Mercados"
- como os mercados para assassinatos e extorsão
+ Possibilidades:
+ proteção física, física capure
- tornar arriscado
- (por outro lado, sniping é fácil)
+ "inundação" de ofertas
- "dar um número" (o que significa: entrar em linha)
- atacar reputações
- Eu concordo que o mais pensamento é necessário, análise mais aprofundada
- Algumas pessoas têm até apontou os benefícios de matar
fora dezenas de milhares de políticos corruptos, narcóticos,
e os policiais que executaram fascista, colectivista
políticas para muito tempo. Assassinato mercados podem fazer isso
muito mais prático.
16.12.3. "Como é *fraude* tratadas com criptografia anarquia?"
- Quando os autores ainda não pode ser identificado.
- Um dos mais interessantes problemas.
- Em primeiro lugar, a reputação da empresa em questão. Repita o negócio não é garantia.
É sempre melhor não ter muito em jogo em qualquer

única transação.
16.12.4. "Como sabemos que a criptografia anarquia vai funcionar? Como sabemos que ele não vai levar o mundo para a barbárie, a guerra nuclear, e o terror?"
- Nós não sabemos, é claro. Nós nunca pode.
- No entanto, as coisas já estão bem ruins. Olhar para a Bósnia, Ruanda, e uma centena de outros hellholes e ponto de fulgor, em todo o mundo. Olhar para os arsenais nucleares dos superpoderes, e olha que inicia as guerras. Em quase todos os casos, o estatismo é a culpa. Os estados têm matou uma centena de milhões ou mais de pessoas neste século sozinho, pense Hitler, Stalin, Mao e Pol Pot-meio forçado fome de todo províncias, a liquidação dos camponeses, matando dos intelectuais, e a massa exterminations de religiosos e grupos étnicos. É difícil imaginar criptografia causando anarquia tudo o que bad!
- Crypto anarquia é um cyberspatially mediada pessoal do curso de ação; por si só, envolve ações tais como o terrorismo nuclear ou de chantagem. Apenas um poderia tão facilmente perguntar, "Será que a liberdade de levar a chantagem nuclear, armas de negociação, e a pedofilia?" A resposta é a mesma: talvez, mas então o que?
16.12.5. É verdade que a criptografia anarquia não é para todos. Alguns vão ser muito incompetente para preparar-se para proteger-se, e vai quer um protetor. Outros terão pobres sentido para os negócios.
16.12.6. "Mas o que vai acontecer com os pobres e as pessoas de bem-estar se crypto anarquia realmente consegue?"
- "Então?"
- Muitos de nós gostaria de ver isso como uma coisa boa. Não apenas para Calvinista-Randite razões, mas também porque poderia quebrar o ciclo de dependência que realmente fez coisas pior para as classes menos favorecidas da América (pelo menos). Ver Charles Murray "Perdendo Terreno" para mais sobre isso.
- E lembre-se de que um colapso do sistema tributário significa mais dinheiro deixado nas mãos do ex-contribuintes, e, portanto, sobra mais para a verdadeira caridade (para aqueles que realmente não podem ajudar a si mesmos).

16.13. Mercado Negro
16.13.1. "Por que alguém iria usar preto mercados?"
+ quando as vantagens de fazer isso e desvantagens
- incluindo a chance de ser pego e o consequências

- (Como as chances de queda, isto sugere um aumento na
punição gravidade)
- as empresas tendem a fugir de mercados ilegais,
a menos que...
+ Anonymous mercados para produtos médicos
- para reduzir a responsabilidade, local éticos e religiosos leis
- Exemplo: ao Vivo de vacinas contra a AIDS...considerado muito arriscado para qualquer
empresa a introduzir, devido à incapacidade de obter ligação
isenção de responsabilidade (mesmo para "plenamente informado" pacientes
que cara provável morte)
- mercados em partes do corpo...
16.13.2. Criptografia de anarquia abre algumas possibilidades interessantes para a
conluio em negócios financeiros, para o insider trading, etc.
- Eu não estou afirmando que isso vai significar riquezas instantâneas, como
os mercados são bastante eficiente (*) e "insiders", muitas vezes não
fazer o bem no mercado. (* Alguns argumentam que o relaxamento de leis
contra insider trading vai fazer ainda, para uma mais justa
mercado...eu concordo com isso.)
- O que eu estou afirmando é a SEC e FinCEN computadores serão
trabalhando horas extras para tentar manter-se com o novo
possibilidades de criptografia de anarquia abre. Untraceable dinheiro, como
em contas bancárias no exterior que pode-se enviar anônimo
instruções de negociação para (ou para), significa "insider trading"
simplesmente não pode ser parado...tudo o que acontece é que insiders
ver as suas contas bancárias aumento (na medida em que ganhar
por causa do "insider trading" ...como eu disse, uma discutível
ponto).
- Preço de sinalização, de um la a companhia aérea caso de alguns anos atrás
(o que, você não será surpreendido ao ouvir, eu não tenho problemas
com), vai ser mais fácil. Untraceable de comunicação, virtual
reuniões, etc.
16.13.3. Mercados De Informação
- a la "informações de corretagem," mas mediada
criptograficamente
- lembre-se de 1981 mercado de mísseis Exocet de códigos (França,
Argentina-depois de relevância quando um Exocet afundou um Britânico
navio)
16.13.4. Preto Mercados, Economias Informais, Leis De Exportação
+ Transfronteiriças de fluxo de dados, questões legais
+ complexo..leis, direitos de autor, de "soberania nacional"
- por exemplo, Filipinas exigiu-a-claro transmissões
durante o empréstimo ao banco renegociações ... e várias latina
Os países da américa proibir transmissões criptografadas.

+ Exportação, Tecnologia E Exportação, Controle De Exportação
- Lei De Controle De Exportação
- Escritório de Munições (como em "Munições Lei", por volta de 1918)
+ exportação de alguns de criptografia engrenagem mudou de Departamento. do Estado, Escritório de Munições, para o Dept. de Comércio
- Mercadoria Lista de Controle, permite-s/w que é livremente disponível para o público a ser exportado sem adicionais papelada
- Munições usado para ser stickier sobre exportação (alguns dizer, de modo justificado, paranoid)
- Mercadoria Jurisdição pedido, para ver se o produto para exportação cai em Estado ou do Comércio regulamentos
- A negociação com o Inimigo Agir
- Exocet códigos--mercado negro de venda de fichas emasculado

16.13.5. O contrabando e o mercado Negro

+ Preto Mercados na URSS e Outros Ex-Bloco do Leste Nações
+ um grande problema, porque os mecanismos normais de graça mercados-leis de propriedade, lojas, mercados de ações, duro moedas, etc.-não foi no lugar
- na Rússia, nunca existiu realmente
+ Papel de "Máfia"
- diversas relacionadas com a família grupos (que é como o comércio começa-se sempre, através de contactos e ligações de família e lealdade, até que as corporações e as suas próprias estruturas de confiança e lealdade pode evoluir)
+ como a Máfia na Rússia funciona
- propina para "perder" materiais, mesmo todo trainloads
- o mercado negro da moeda (dólares favorecido)
+ Isso pode provocar um grande descontentamento na Rússia
- como privilegiados, muitos deles ex-oficiais Comunistas, estão melhor preparados para fazer a transição para o capitalismo
+ aqueles em fábrica de postos de trabalho, em matéria de pensões, etc., não tem a renda disponível para tirar partido das novas oportunidades
- A américa tinha a dupla vantagem de uma fronteira que as pessoas queriam mover para (Turner, ética Protestante, etc.) e um grande crescimento era (industrialização)
- além disso, não houve exposição a outros países vastamente melhor qualidade de vida
+ Contrabando na CEE
+ o sonho de pauta livre de fronteiras, tem dado lugar a a realidade de uma complexa teia de leis que ditam o que é

o politicamente correto e o que não é:
- animais de hormônios de crescimento
- adoçantes artificiais são limitadas após 1-93 para uma pequena
lista de aprovados alimentos, e o Britânico está encontrando
que o seu querido "cocktail de camarão com sabor de batatas fritas"
são para ser banido (para exportar para CEE ou completamente?)
porque eles são feitos com sacarina ou aspartame
- "Europeu de conteúdo" em programas de televisão e filmes podem limitar
Produções americanas...como com o Canadá, esta não é uma
grande simplificação das liberdades básicas?
+ isso pode levar a um novo tipo de contrabando no "politicamente
incorreto" itens
- pode-se argumentar que este já é o caso com a proibição de
sobre drogas, peles de animais, marfim, etc. (tão tediosamente
argumentou Brin)
- lembre-se Turgut Ozal refrescante comentários sobre afrouxando
até na fronteira restrições
+ quanto mais itens forem declarados bootleg, o contrabando vai
aumento...politicamente incorreto contrabando (peles, marfim,
racista e sexista literatura)
+ o ponto sobre sexista e racista literatura sendo
contrabando é dizer: esse tipo de literatura (livros, revistas)
pode não ser formalmente proibidos, por que seria uma violação da
Primeira Alteração, mas ainda podem ser importados de forma anônima
(contrabando) e distribuídos como se fossem banidos (!) para
a razão de evitar os "danos" de pessoas que
afirmam que foram vítimas, agredido, etc. como resultado
da literatura!
+ para evitar processos judiciais ou reivindicações de danos para escrever,
edição, distribuição ou venda de "danos" materiais
é ainda outra razão para sistemas anónimos a surgir:
as pessoas envolvidas no processo procurará imunizar
- se a partir de várias ato ilícito extracontratual que são
o entupimento dos tribunais
- produtores, distribuidores, diretores, escritores, e até mesmo
atores de x-rated ou de outra forma "inaceitável"
o material pode ter a proteção de anônimo
sistemas
- imagine fibra óptica e a proliferação de vídeos
e talk-shows....bluenoses e os promotores irão usar
"forum shopping" para bloquear o acesso, para julgar o
produtores, etc.
+ De países do terceiro Mundo pode declarar que a "soberania nacional

sobre os recursos genéticos" e, assim, bloquear a livre exportação
e o uso da planta - animal e derivados e outras drogas
produtos
- mesmo quando apenas uma única planta
- royalties, impostos, taxas, licenças, a ser pago ao local
bancos de genes
- estes bancos de genes seriam os únicos permitidos a fazer
genética de catalogação
- o problema é, naturalmente, um de execução
+ tecnologia, programas de
- cenário: muitos programas úteis são preços para
corporações (como quartos de hotel, passagens aéreas,
etc.), e sensível ao preço, os consumidores não vão pagar r $800
para um programa que irá usar, ocasionalmente, para moer a prazo
artigos e igreja newsletters
+ Cenário: Anônimo doador de órgãos bancos
+ por exemplo, uma forma de "mercado" raros tipos de sangue, ou seja,
sem expondo uma auto forçada, doação ou outros
sanções
- "forçado doação" envolve as ações ajuizadas pelo
potencial destinatário
- no momento de oferecer, pelo menos...o que acontece quando a
negócio é consumado é outro domínio
- e uma forma de evitar que um número crescente de governo
picadas
+ o aborto e direitos das mulheres de metro...uma esperança
aliado (meio geralmente antiliberty movimento de mulheres)
- RU-486, de metro clínicas de aborto (porque muitos
clínicas têm sido firebombed, boicotou para fora da existência,
corte de fornecimentos e serviços)
+ Ilegal de estrangeiros e imigração
- "O Boxer Barreira", usado para selar as barreiras...Barbara Boxer
quer a militar e a guarda nacional para o controle ilegal
a imigração, por isso seria justiça poética de fato, se este
o programa tem o nome dela
16.13.6. O Crime organizado e Cryptoanarchy
+ Como e Por que
+ onde quer que o dinheiro é para ser feita, algumas no submundo vai
naturalmente, o interesse de
- empréstimo sharking, jogos de números, etc.
+ eles podem se envolver na configuração de metro bancos,
usando a autoridade de CERTIFICAÇÃO protocolos
- jogos do shell, o anonimato

- tal Máfia envolvimento em um subterrâneo sistema monetário
o que realmente pode espalhar as técnicas
+ mas, em seguida, ambos os lados podem ser de lobby com a Máfia
- o CA defende a fazer um pacto com o diabo
- e o governo quer que o Mob para ajudar a erradicar a
métodos
+ Programas Específicos
+ Identidades Falsas
- no mundo informatizado dos anos 90, mesmo a Multidão (que
geralmente evite cartões de crédito, números de segurança social,
etc.) vai ter de lidar com a facilidade de seus movimentos
pode ser rastreada
+ de modo que o Mob irá envolver-se em Identificações falsas
- como mencionado por Koontz
- A Lavagem de dinheiro, naturalmente
+ mas alguns no governo veja alguns dos principais freelance
oportunidades em CA e começar a usá-lo (isso prejudica
o controle de autoridade de CERTIFICAÇÃO e, na verdade, espalha-lo, porque o
o governo está a trabalhar no cross purposes)
- análogo à forma como o governo da utilização do comércio de drogas
sistemas de difundir as técnicas
16.13.7. "Digital Custódia" contas para mutuamente suspeitos, partes,
especialmente em operações ilegais
- droga, promoções, informações de corretagem, informações, etc.
+ Mas por que será que a custódia de entidade é de confiança?
+ reputações
- a sua empresa é confiável garantia titular, não
dela, destruindo sua reputação de suborno ou ameaça
+ anonimato significa conivência empresa não sabe quem é
"queima" se tentar fazer isso
- eles nunca sabe quando eles mesmos estão sendo testados
por algum serviço
- e o potencial bribers não vai saber quem contactar,
embora o e-mail pode ser dirigida para a garantia da empresa
com bastante facilidade,
16.13.8. As empresas privadas são, muitas vezes, os aliados do governo com
relação ao mercado negro (cinza ou mercados)
- eles vêem descontrolada comércio como cortar seus monopólio
poderes
- uma forma de limitar a concorrência

16.14. Lavagem de dinheiro e Evasão Fiscais
16.14.1. Desesperança de controlar a lavagem de dinheiro

+ Eu vejo todo esse aumento moneylaundering como um incrivelmente
a esperança de tendência, que vai de malha bem com o uso de
criptografia
- por que deveria exportação de moeda ser limitado?
- o que há de errado com a evasão fiscal, de qualquer maneira?
- corromper, afeta todas as transações
- grandes quantidades de dinheiro que flui
- 2000 bancos na Rússia, principalmente a lavagem de dinheiro
+ as pessoas e países são tão carente de moeda forte que
a maioria dos bancos fora dos EUA terão todo o prazer em receber esse dinheiro
- não há recursos naturais em muitos desses países
- impossível controlar
- sendo apresentado como "lucros vs. diretores," mas eu acho que
este é manifestamente equivocada
+ Jeffery Robinson, "O Landrymen," entrevista a CNN, 6-24-
94
- "mais perto da anarquia" (yeah!)
- impossível controlar
- dezenas de novos países, carente de moeda forte, tem
autonomia para definir políticas de bancos (e da maioria dos Europeus
países fecham os olhos para a maioria dos anti-
as disposições de lavagem)
16.14.2. Impostos e Criptografia
- além de vacância, existem também problemas de registros de impostos,
imposto sobre vendas, recibos, etc.
+ esta é outra razão pela qual o governo pode exigir o acesso a
ciberespaço:
- para garantir o cumprimento da lei, la um inviolável dinheiro
registar
- evitar-a-tabela de transações
- suborno, do lado de pagamentos, etc.
- Nota: é improvável que o acesso aos registros iria parar
qualquer fraude ou a evasão fiscal. Eu só estou citando razões para eles
para tentar ter acesso.
- Eu nunca disse que o sistema de impostos entrará em colapso total,
ou durante a noite, ou sem uma luta. As coisas levam tempo.
+ o cumprimento das obrigações fiscais taxas de cair
+ o tecido já desfazia em muitos países, onde
oficial de um padrão de vida abaixo do _apparent_
padrão de vida (por exemplo, a Itália).
- a evasão fiscal uma coisa importante
- dinheiro atravessa a fronteira para a Suíça e
Áustria

- Frissell figuras
- relatórios de imprensa
+ Imposto de problemas, e como o forte de criptografia torna mais difícil e mais difícil impor
- escondendo de renda, mercados internacionais, consultores, complexamente estruturados de transações

16.14.3. A Fuga De Capitais

- "A questão importante para Cypherpunks é como devemos responder a esta aparentemente inevitável o aumento da mobilidade de de capital. Não representam uma ameaça à privacidade? Se for assim, vamos escrever código para combater a ameaça. Não nos oferecem qualquer ferramentas que pode usar para combater os esforços dos estados-nação, para tira nossa privacidade? Se for assim, vamos escrever o código para tomar a vantagem dessas ferramentas." [Sandy Sandfort, Declínio e A queda, de 1994--06-19]

16.14.4. Lavagem de dinheiro e de Metro de Bancos

+ uma grande quantidade de dinheiro está se tornando disponível sob a tabela: a partir de skimming, a partir de evasão fiscal, e a partir ilegal atividades de todos os tipos
- pode ser visto como parte da internacionalização de todos os empresas: por exemplo, o Paquistanês de trabalho que possam colocaram alguns rupees em alguns locais do banco de depósitos com o BCCI, em Karachi, a obtenção de um maior rendimento e também aumentando o "multiplicador" (como estes rupees de obter quaresma muitas vezes)
- é o que aconteceu nos EUA há muitos anos
- isso vai acelerar à medida que os governos tentar obter mais impostos a partir de suas mais sofisticadas e técnicas de contribuintes,de por exemplo, maneiras inteligentes para ocultar rendimentos serão buscadas
+ BCCI, Lavagem de Dinheiro, Bancos da Frente, a CIA, o Crime Organizado
+ Lavagem De Dinheiro

A Cidade de nova York é o principal clearinghouse, Federal Reserva de Nova York, supervisiona este
- Fedwire sistema
- trilhões de dólares passar através deste sistema, o diário
+ Como a lavagem de dinheiro pode trabalhar (de um labirinto de técnicas)
- um milhão de dólares para ser lavado
- agente de fios que, talvez, junto com o de outros fundos, para Panamá ou para algum outro país
- banco no Panamá pode emitir para quem apresenta a letra adequada
- diversas maneiras para que ele se mova para a Europa, a ser emitido como portadora de estoque, etc.

- 1968, ventos fundos mútuos, Bernie Kornfield
+ CIA prefere muitas vezes os bancos com conexões de Mob
- porque Mob bancos já têm a segurança necessária
e o anonimato
- e estão dispostos a trabalhar com a Empresa de forma que
bancos convencionais não podem ser
+ ligações voltar para OSS e da Máfia na Itália e Sicília, e
para o comércio de heroína no SUDESTE da Ásia
- Inteligência Naval fez um trato na 2ª guerra mundial com a Máfia,
wherby Meyer Lansky iria proteger as docas contra
greves (provavelmente em troca de um "corte"), se
Lucky Luciano seria lançado no final da guerra
(ele foi)
- Operação de inferno: a Máfia assistido as tropas Aliadas em
Sicília
- "Corse"
+ Luciano ajudou em 1947 para reabrir Marselha quando
Comunista grevistas tinha desligá-lo
- continuando o padrão de cooperação iniciados no
a guerra
- estabelecendo assim a Conexão francesa!
- Nugan Hand Bank
+ BCCI e o Bank of America favorecido pela CIA
- Russbacher diz B de Um abençoado tampa
+ nós quase certamente irá descobrir que o BCCI foi o
principal banco utilizado, com os laços para o Bank of America
escritórios em Viena
+ O Bank of America tem admitiu ter tido início
os laços com o BCCI no início da década de 1970, mas afirma
romperam os laços
- no entanto, Russbacher diz que a CIA usou B de Um
sua preferência, o banco, na Europa, especialmente desde que
ele tinha laços com empresas como a IBM, que foram usadas
como capas para seus covert ops
- Viena foi um privilegiado de branqueamento de capitais do centro para a CIA,
especialmente através do Banco da América
+ um redemoinho de papel frentes, escondendo os fluxos de reguladores
e os investidores
- "nomeados", usado para esconder os verdadeiros proprietários e verdadeiro atividades
- várias nações têm de sigilo bancário leis, criando o
"véu" que não pode ser furada
+ CIA sabia sobre todos os voos para a América do Sul (e
provavelmente em outros lugares também)

- admitiu Thomas Polgar, um alto ex-CIA oficial, em
testemunho sobre 9-19-91
- isso indica que a CIA sabia sobre os braços negócios, o
tráfico de droga, e a vários outros esquemas e fraudes
+ Anterior CIA-Banco Escândalos (Nugan Hand e o Castelo de Banco)
+ Nugan Hand Bank, Austrália
+ Frank Nugan, em Sydney, na Austrália, morreu em 1980
+ aparente suicídio, mas claramente manipuladas
- Mercedes, rifle, sem impressões digitais, posição
tudo errado
- provas de que ele tinha uma mudança de coração-foi
a oração diária, a la Charles Colson-e foi
pensando sobre a obtenção de fora do negócio
+ configurar Nugan Hand Bank, em 1973
- os serviços de private banking, livre de impostos depósitos em
Jacarés
+ usado por agentes da CIA, tanto para operações da Agência e
para sua própria lama/fundos de aposentadoria
- CIA vários tipos em folha de pagamento (listados seus
endereços como o mesmo que o Ar da América)
- William Colby a Bordo, e foi um advogado
+ ligações com o crime organizado, por exemplo, Santo Trafficante,
Jr.
- Flórida, a heroína, links para o assassinato de JFK
- trafficante era conhecido como "o Cobra" e tratados
muitas transações para a CIA
+ de branqueamento de capitais para os países Asiáticos, os traficantes de droga
+ Triângulo de ouro: N-H mesmo tinha ramificações em GT
- e filial em Chiang Mai, na Tailândia
- links para traficantes de armas, como Edwin P. Wilson
+ EUA as autoridades recusaram-se a cooperar com
investigações
- e quando a informação foi lançado, ele foi apagado com
um "B-1" observe, implicando nacional de segurança
implicações
+ de investigações pelo Australian Bureau Federal de
Entorpecentes foram frustrados-agentes transferidos e
Secretaria desfez logo em seguida
- semelhante a "não foda com a gente" mensagem enviada para
FBI e pela CIA, DEA
+ N-H do Banco tinha uma estreita relação de trabalho com o Australiano
Inteligência de segurança da Organização (ASIO)
- NSA aproveitado conversas pelo telefone (especulativa) de

Nugan que indicado ASIO conluio com N-H do Banco
no comércio de drogas
+ Pine Gap facilidade, perto de Alice Springs (NSA, NRO)
- P. M. Gough Whitlam críticas de Pine Gap levou a
CIA-ASIO conspiração para destruir a Whitlam do gov.
- De novembro de 1975 queda instigado com escutas e
falsificações
+ Nugan Hand Bank também estava envolvido com a "Força-Tarefa
157," uma Inteligência Naval operação secreta, dado
a tampa nome de "Furar Morgan" (um bom nome?)
- informou a Henry Kissinger
- lembre-se ponto de menor importância que a Marinha é, muitas vezes, o preferido
serviço da elite dominante (o real preppies)
+ e George Bush filho, George W. Bush, estava envolvido
com Nugan Hand:
- vinculada ao William Quasha, que tratou N-H lida em
Filipinas
+ donos da Harken Energy Corp., baseada no Texas empresa
que comprou de G. W. Bush, empresa de petróleo "Espectro de 7" em
1986
- depois tem de perfuração offshore direitos do Bahrein
petróleo-com G. W. Bush no Conselho de Administração
- isso poderia ser um outro link para a Crise do Golfo?
+ Castelo Banco, Bahamas, Paul E. Helliwell
+ OSS (China). CIA
- Mitch WerBell, Branco especialista russo em
assassinato, silenciadores, trabalhou para ele na China
- Howard Hunt trabalhou para ele
- após a 2ª guerra mundial, configurar Mar de Abastecimento Inc., CIA frente em Miami
+ vinculada à Resorts Internacionais
- escritório de advocacia de Helliwell, Melrose e DeWolf
- emprestou dinheiro para Bahamas P. M. Lynden Pindling em
troca de prorrogação da licença de jogo
+ Robert Vesco, Bebe Rebozo, e Howard Hughes
- em contraste com a "Leste do Estabelecimento," estes
foram Nixon insiders
- ligações com o ex-agente da CIA Robert Maheu (que trabalhou
para Hughes); onvolved withTrafficante, CIA enredo para
matar Castro, e as possíveis ligações para JFK
assassinato
- Vesco ativa no comércio de drogas
+ também envolvido na compra de terras para a Walt Disney
Mundo

- De 27.000 hectares perto de Orlando
- Castelo Banco foi uma CIA eletroduto
+ Operação Tradewinds, IRS sonda de banco de fluxos de dinheiro
- final dos anos 60
- investigação de "placa de bronze" as empresas, em Jacarés,
Bahamas
+ Enredo Cenário: Operação Tradewinds descobriu muitos
UltraBlack operações, forçando-os a recuar e
cavar mais fundo, sacrificar várias centenas de milhões de
- por volta de 1977 (Castelo Banco encerrado)
+ World Finance Corporation (WFC)
+ começou em 1971, em Coral Gables
- o primeiro conhecido como República Corporação Nacional
- Walter Surrey, ex-OSS, como Helliwell do Castelo
Banco, ajudaram a incorporá-lo
+ De negócios
- explorada fluxos de caixa na Flórida
- dadas com a CIA, Vesco, Santo Trafficante, Jr.
- também tenho de empréstimo depósitos de Árabes
- links para Narodny Banco, a união Soviética banco que também
pagar agentes
+ relacionadas com a empresa foi o Domínio Mortgage Company,
localizado no mesmo endereço WFC
- vinculada ao fluxo de narcóticos em Las Vegas
- e para Trafficante, Jr.
- malas de dinheiro lavado de Las Vegas para
Miami
- Jefferson de Poupança e Empréstimo Associação, Texas
+ Guilermo Hern&#65533;bernardo hernández Cartaya, ex-Havana banqueiro, Cubana
exílio, foi chefe figura
- veterano da Baía dos Porcos (provavelmente CIA contatos)
- investigados: R. Jerônimo Sanford, Miami assistente
O procurador dos EUA
- Dade County Crime Organizado Secretaria também envolvidos na
a investigação de 1978
- Rewald e a sua banca de negócios
- BCCI foi um sucessor para esse banco
+ CIA e da DEA Links para Comércio de Drogas
- o ex-agentes e traficantes de drogas foram frequentemente
recrutados pela DEA e da CIA para executar as suas próprias interações
a operação, às vezes com motivações políticas
- Carlos Hern&#65533;bernardo hernández recrutados por BNDD (Departamento de Narcóticos
e drogas Perigosas, antecessor da DEA) para formar uma

esquadrão da morte para assassinar outros traficantes de drogas
+ ligações possíveis de traficantes de drogas para
UltraBlack/Testemunho De Programa De Segurança
- agentes na Flórida, o corretor da bolsa de valores de matar em 1987
- Selo foi traído pela DEA e da CIA, a permissão para ser
mortos pelos Colombianos
+ Rebeldes afegãos, os Braços do irão (e Iraque), a CIA, o Paquistão
- havia uma banca e braços-execução de rede centralizado
em Karachi, a casa do BCCI, para os vários braços negócios
envolvendo rebeldes Afegãos
- Karachi, Islamabad, outras cidades
+ Tráfico De Influência, Agentes
- la a muitos altos advogados contratados pela BCCI (Clark
Clifford, Frank Manckiewicz ortografia [?]
+ ilustra novamente o básico corruptability de um
centralizado de comando da economia, onde os reguladores e
os legisladores são, muitas vezes, nos bolsos dos corruptos
empresas
- claramente alguns escândalos e perdas ocorrem em livre
mercados, mas pelo menos o mercado livre não será
backup com o governo de coerção
+ Por que a CIA está Envolvida em Tantos negocios escusos?
+ capa ideal para operações secretas
- fora de auditoria canais
- links para o submundo
+ agentes fornecer para suas próprias aposentadorias, seus próprios
negociação particular, e a suavização de seus ninhos
- a liberdade de interferência
- a ganância
+ lida como a de Noriega, no qual CIA-suporte
os ditadores e os agentes de sua própria pródigo
estilos de vida\
- e o BCCI-Noriega links acredita-se que
contribuiu para a CIA falta de vontade para a pergunta
as atividades do BCCI (na verdade, da Justiça
Departamento)
+ O papel dos Bancos no Iraque e a Guerra do Golfo, o Iraque-Gate, Escândalos
- Export Import Bank (Ex-Im), CCC
- implicado no armamento do Iraque
- Banco Lavorzo Nazionale ortografia [?]
+ CIA estava usando BNL arranjar us $5 bilhões em transferências, a braço
O iraque, para garantir a igualdade de tratamento com Iran
- porque BNL não pergunte de onde ele veio

- território federal de empréstimos garantidos usado para financiar covert ops
+ a privatização de covert ops, pela CIA e NSA
- deniability
- eles subcontratadas a lei de quebra de
- o lado mais obscuro do capitalismo fez o trabalho real
- mas os bandidos aprenderam rapidamente quanto eles
poderia roubar...provavelmente 75% do dinheiro roubado
- a fraude de seguros...aviões é permitido para ser roubado, então
enviado ao Contrário, com Ollie Norte argumentando que
ninguém estava realmente machucado por todo esse processo
+ ironicamente, ricos Kuwaitis estavam ativos no financiamento
"instant bancos", por lavagem de dinheiro e armas
transações, por exemplo, várias Ilhas do Canal)
- Ahmad Al Babtain Grupo de Empresas, Ltd., um
Antilhas holandesas corporation
- Inslaw caso se encaixa com esta imagem
+ Reserva Federal e S não têm o Poder de "Peirce a
Véu" sobre Bancos Estrangeiros
- como Morgenthau caso em Manhattan desenvolve
- um conhecido problema
+ Mas devemos ser tão surpreso?
- ainda não bancos sempre financiados guerras e armas comerciantes?
- e que alguns deles não falhou?
- olhe para os Rothschilds
- o que é surpreendente é que muitas pessoas sabiam o que é
estava fazendo, que seu negócio era, e que era mesmo
apelidado de "Bancos de Bandidos e Criminosos Internacionais"
+ Utilizando agentes de software para a lavagem de dinheiro e outros
atos ilegais
+ esses agentes atuam como semi-autônomas de programas que são um
alguns passos além do simples algortihms
- não é de todo claro que esses agentes podem fazer
muito para executar carteira, porque nada realmente
funciona
- uso real poderia ser digital "recortes": a transferência de
riqueza para outros agentes (também controlado de longe, como
marionetes)
- a vantagem é que elas podem ser programadas para executar
operações que são, talvez, ilegal, mas sem
rastreabilidade
+ Informações corretores como os lavadores de dinheiro (os dois são
intimamente relacionados)
- o aumento de AMIX estilo mercados de informação e Sterling-

estilo de dados "paraísos" irá fornecer novos caminhos para o dinheiro
de capitais e asset-ocultar
+ informações é intrinsecamente difícil de valor, difícil colocar
uma etiqueta de preço (isso varia de acordo com as necessidades do
compradores)
- o que significa que os fluxos transnacionais de inforamation
não podem ser avaliados com precisão (atribuído um valor em dinheiro)
- está intimamente relacionada com a idéia de informal
consultoria e nontaxable natureza
- caixas de papelão cheia de dinheiro, gravado e amarrado, mas
ainda estourando aberto
- ginásio sacos de transporte relativamente pequenas quantidades de skim: um
meros cem mil em us $100s
+ L. A. se tornando um foco maior parte do dinheiro
- proximidade com o México, grandes comunidades de imigrantes
- auto-estradas e de fácil acesso
+ centenas de pistas de pouso, dezenas de portos
- que Costa Leste parece ter ainda mais, de modo que este
não parece ser uma razão convincente
- Condado de Ventura e de Santa Barbara
16.14.5. Privado Moedas, Desnacionalização de Dinheiro
- Lysander Spooner defendeu essas moedas
- e "desnacionalização" de dinheiro é um tema quente
+ é efeito, alternativas ao normal moeda já existe
- cupons de passageiro frequente cupons, etc.
+ de telefone de cartões e cupons (amplamente utilizada na Ásia e
partes da Europa)
- ironicamente, EUA tiveram na sua maioria, optaram por cartões de crédito,
o que são totalmente rastreáveis e oferecer um mínimo de privacidade,
enquanto outras nações têm abraçado o anonimato do
o seu tipo de cartões...e isso parece estar levando
para a cabine de pedágio sistemas que estão sendo planejadas
- permuta de redes
- pique as marcas (na Ásia)
+ "reputação" e favores
- se Al dá Bob alguns conselhos, isso é tributável? (fazer
advogados que falar entre si, o relatório
operações/ od claro que não, e ainda, esta é
efectivamente uma transacção de troca ou o resultado de um vencedor
presente)
+ sofisticado alternativas financeiras para o dólar
- diversos instrumentos
- contratos de futuros, contratos forward, etc.

- "informação" (mais do que apenas favorece)
+ obras de arte e similares itens físicos
- não é um mercado líquido, mas para altos rolos, de uma maneira fácil
a transferência de centenas de milhões de dólares (mesmo com
o desconto de valores de um item roubado, e não todos os
itens vai ser roubado...muitas pessoas vai ser muito cuidadoso
nunca viaje com arte roubada)
- diamantes, pedras preciosas têm sido uma forma de transportáveis
riqueza
+ obras de arte não precisa ser declarado no máximo (?) fronteiras
- isso pode mudar com o tempo

16.14.6. Esquemas De Evasão Fiscal

- omissão de receita, por exemplo, bancos como o BCCI, obviamente,
não relatar o que eles ou os seus clientes estavam fazendo para o
várias autoridades fiscais (ou outra pessoa)
- proveitos diferidos, dos fundos fiduciários discutidos aqui
(onde o pagamento é diferido e algum tipo de confiança é usado
para pagar pequenas quantias por ano)
+ De ativos-Esconde, Pagamentos Ilegais, Suborno e Evasão Fiscal
Os fundos Podem Ser Protegido em um "Fundo de pensões"
+ por exemplo, um político ou informações de ladrão, talvez um Intel
funcionário que vende algo para us $1 milhão-pode comprar ações de uma
crypto-fundo que garante, em seguida, ele é contratado por uma sucessão
de empresas de consultoria para anual de consultoria ou até mesmo só...
colocado em um "retentor" de, digamos, us $100 mil em um ano
+ IRS pode vir a ter dúvidas sobre tais serviços, mas
a menos que o governo de passos e exigências detalhadas
inspeção do trabalho real feito-e mesmo então, eu acho que
isso seria impossível e/ou ilegais, tais
arranjos parece ser infalível
+ por que não pode o governo da demanda a prova de trabalho?
- que julga o valor de um funcionário?
- dos conselhos, dos relatórios gerados, ou do
valor de ter um consultor "no retentor"?
- esse tipo de interferência devastar muitas investido
interesses
+ impostos e outras vantagens destes "crypto anuidades"
- só de imposto pago sobre o rendimento anual, não sobre o nódulo
soma
- as autoridades não estão alertados para a súbita recepção de
de um montante fixo (um ex-oficial de inteligência que recebe
um pagamento de us $1 M virá sob suspeita, exatamente
como seria um político)

- e o pagamento de um montante fixo pode muito bem despertar suspeitas
e ser considerado evidência de alguma atividade criminosa
+ original quantia está protegido de confisco
por governos, pela consideração em pensão alimentícia ou
matéria de falência, etc.
- a tal "consultoria anuidades" podem ser adquiridos apenas
de modo a isolar os rendimentos de pensão alimentícia,
falência, etc.
- como de costume, eu não estou defendendo essas etapas como moral ou
como bom para o clima de negócios do mundo, só
como conseqüência inevitável de muitas tendências atuais
evolução técnica e
+ o "jogo shell" é usado para proteger os fundos
- com periódicos, levantamentos ou transferências
- observe que todo esse esquema pode muito bem ser feito por
advogados e agentes de hoje, apesar de poderem ser intimada
ou, de outra forma incentivados a blab
+ pode até não ser ilegal para um consultor para tomar o seu
taxa durante um período de muitos anos
+ o IRS pode reivindicar o "valor actual", como um
quantia fixa, mas outras pessoas já fazem coisas como esta
- a realeza de fluxos (e ninguém reivindica um autor deve
concordo com o IRS para algum valor estimado do presente
stream)
- percentagens do valor bruto da (e o gosto)
- engenheiros e outros profissionais são muitas vezes mantidos em
folhas de pagamento não tanto pelas instantânea
como as conquistas de seu passado e projetadas
conquistas-estamos a tratar de futuras realizações
em um montante fixo forma?
+ IRS e outros podem tentar inspecionar os termos da
de emprego ou contrato de consultoria, mas estes parece muito
invasiva e incômoda
+ faz o governo de um terceiro em todas as
as negociações, exigindo agentes estar presente em todos os
fala ou, pelo menos, para ler e compreender todas as
a papelada
- e, ainda assim, pode haver reivindicações que o
o governo não siga as ofertas
- não há tempo ou mão-de-obra para lidar com todas essas
coisas
- e a invasão da privacidade é extrema!
+ Cenário: o Fincen-tipo de agências de maio de lidar com o

crescente ameaça de CA-tipo de sistemas (e criptografia
geral), envolvendo o governo ostensivamente
negociação particular
- análogo ao imposto de vendas e da contabilidade
arranjos (onde gov. é um terceiro para todos
transações)
+ ou EEOC, raça e sexo discimination casos
- vai transcrições e gravações de todos os trabalhos de
as entrevistas passam a ser exigidas?
- a "imposição"da trilha
- OSHA, poluição, etc.
+ software de cópia de leis (mais ao ponto):
o governo parece ter o poder de introduzir um
de negócios para ver se cópias ilegais estão em uso; este
pode requerer um mandado de
+ quanto tempo antes de vários tipos de software são
banido?
- com o argumento de que alguns tipos de
software são análogas às lockpicks e outros
proibida assaltante ferramentas
- "utilizado para facillitate a cópia ilegal de
o software protegido"
+ a ameaça de criptografia para a segurança nacional como
bem como para a lavagem de dinheiro e ilícitos
pagamentos possibilidades pode causar o governo
para colocar restrições sobre o uso de criptografia
software para nada a não ser aprovada usa
(e-mail externo, etc.)
- e mesmo esses usos podem, naturalmente, ser subvertido
- e técnicas de criptografia não são realmente necessários: advogados
e outras discreto agentes será suficiente
+ além disso, as empresas têm uma quantidade razoável de lattitude
na definição de políticas de reforma e benefícios, e assim o
métodos que descrevi para abrigar a renda atual de maio
tornar-se mais comuns
+ embora possa haver alguns ressalva de que, se os benefícios
exceeed alguma porcentagem de sua renda anual, levando-se em
anos de trabalho, que esses benefícios são tributados em alguns
punative forma
- e.g.., uma empresa que paga R $100 por ano para um
críticas técnicas pessoa para um ano de trabalho e, em seguida,
paga-lhe $60K de um ano para os próximos dez anos, poderia
ser razoavelmente acredita-se ter definido um sistema de

ajudá-lo a evitar o pagamento de impostos em uma grande quantia de pagamento
+ De ativos de se esconder, para evitar apreensão em falências, ações judiciais
+ por exemplo, os fundos colocados em contas que são secretos, ou em
sistemas/esquemas em que o activo-hider tem o controle
de algum tipo (direito de voto, consultoria, etc.)
- este é obscura: o que eu estou pensando é algum tipo de
acordo em que Albert é contratado por Bob como um "conselheiro"
em matéria financeira, mas Bob dinheiro vem
Albert e assim o quid pro quo é que Bob vai demorar
Albert conselhos....portanto, o efetivo de capitais e
protecção
+ Também pode ser utilizado para criar "multi-camadas" sistemas de moeda,
por exemplo, onde relatou as transações são alguns fração de
valores reais
- suponha que estamos de acordo para lidar em algum artificialmente baixos
valor: eletricistas e encanadores, pode negociar com cada
outros em us $5 por hora, enquanto usando o metro
contas, na verdade, o comércio em mais realista níveis
+ governo (IRS) tem leis sobre o "valor justo", mas como
poderiam estas leis sejam aplicadas para tais ativos intangíveis, como
software?
- se eu vender um programa de software por us $5000, pode o
o governo declarar que este é mais ou underpriced?
- da mesma forma, se um encanador cobra us $5 por hora, pode o
governo, suspeitando de que a evasão fiscal, forçá-lo a
cobrar mais?
- mais uma vez, a natureza da tributação em nosso mundo cada vez mais
muitos dimensionada economia parece exigir grandes
invasões de privacidade

16.14.7. "Desnacionalização de Dinheiro"

- como com o antigo SF espera de "créditos"
+ cf. os livros sobre a desestatização do dinheiro, e a idéia
de competir moedas
- dinheiro digital podem ser expressos de diversas
moedas, o que torna a ideia de competir moedas
mais prático
- de certa forma, isso já existe
+ o dinheiro duro advogados (erros de ouro) estão a perder a sua
a fé, como eles vêem dinheiro se movendo e nunca realmente
o desembarque em qualquer "rígido" formulário de
- claro, é fundamental que os governos e os grupos de
não têm a capacidade para imprimir mais dinheiro
- redes internacionais provavelmente irá denominar

transações em tudo o que moedas são mais estáveis e
menos inflacionária (ou menos imprevisível inflacionária)

16.15. Propriedade Intelectual
16.15.1. Conceitos de propriedade, vai ter que mudar
- propriedade intelectual; a execução é tornar-se problemático
- quando os ladrões não ser pego
16.15.2. Propriedade intelectual debate
- incluir o meu comentário sobre ondas
+ trabalho em pagamento, para os itens...Brad Cox, Pedro Sprague, etc.
- Superdistribution, com medidor de uso
- propertarian
- muitos problemas

16.16. Mercados para o Contrato de Assassinatos, Extorsão, etc.
16.16.1. Nota: Este é suficientemente importante tópico que merece
seu próprio título. Há material sobre este espalhados ao redor
este documento, material eu vou recolher quando eu chegar em um
chance.
16.16.2. Este tópico veio várias vezes em seguida, Extropians de discussão
lista, onde David Friedman (autor de "A máquina de
Liberdade" e filho do vencedor do Prêmio Nobel, Milton Friedman) e
Robin Hanson debatido isso comigo.
16.16.3. Doug Cutrell resumiu as dúvidas de muitos, quando ele escreveu:
- "...a disponibilidade de proteger efetivamente o anonimato, forte
criptografia, e rastreáveis de dinheiro digital pode permitir
contrato de matar para ser abertamente realizado o negócio. Para
exemplo, um anônimo postagem de notícias anuncia uma chave pública
o que é para ser usado para codificar um contrato de matar ordem, ao longo
com o pagamento digital. A pessoa que coloca o
contrato precisa somente de forma anônima lugar a mensagem criptografada
no alt.o teste. Talvez seja mesmo possível fazê-lo
impossível dizer que a mensagem foi criptografada com a
contract killer de chave pública (o assassino teria que
tentativa de decodificação de todos da mesma forma codificada mensagens
alt.teste, mas que pode ser bastante viável). Assim, ele poderia
ser completamente livre de risco para qualquer pessoa o lugar de um contrato de
ninguém." [Doug Cutrell, 1994-09-09]
16.16.4. Abominável mercados
- contrato de assassinatos
- pode coletar o dinheiro anonimamente para ter alguém
desenvolvi...quase ninguém que é controverso, pode gerar
o suficiente "contribuições"

- seqüestro, extorsão
16.16.5. Lidar com Essas Coisas:
+ nunca link físico de IDENTIFICAÇÃO com pseudônimos! (eles não vão matar se eles não sabem quem são)
- e mesmo se um pseudônimo é ligado, certifique-se de que o seu registros financeiros não são vinculados
- confiar em ninguém
- aumento da segurança física...fazer o esforço de matar muito mais potencialmente perigoso
- ataques de congestionamento..dizer extorsionários para "sair da linha" por trás de todos os outros extorsionários
+ de anunciar ao mundo que não se paga extorsionários conjunto de... protocolo para garantir que este
- sim, alguns vão morrer como resultado deste
- console-se com o fato de que, embora alguns podem morrer, menos estão morrendo como resultado de patrocínio estatal, guerras e o terrorismo (historicamente um maior assassino de contrato assassinatos!)

16.17. Persistente Instituições
16.17.1. Forte de criptografia torna possível a criação de instituições que pode persistir por longos períodos de tempo, talvez para séculos.
tais instituições já existem: igrejas (Católicos da várias ordens), universidades, etc.
16.17.2. todos esses "persistente" (serviços digitais de bancos, garantia serviços de reputação, servidores, etc.) exigem muito melhor proteções contra quedas de serviço, apreensões por parte dos governos, desastres naturais, e até mesmo o colapso financeiro do que a maioria das existente serviços de computadores-uma oportunidade para que os ventos de caução-como serviços
- manter um banco de dados distribuído, com incondicional privacidade, etc.
+ novamente, é imperativo que garantia as empresas exigem que todos os material colocado para ser criptografada
- para protegê-los contra ações judiciais e reivindicações por autoridades (que roubou informações, que eles censurado material, que eles são um espionagem eletroduto, etc.)
16.17.3. Serviços De Garantia
+ Digital "Escrow" contas para mutuamente suspeitos, partes, especialmente em operações ilegais
- droga, promoções, informações de corretagem, informações privilegiadas,

etc.
+ Mas por que será que a custódia de entidade é de confiança?
+ reputações
- a sua empresa é confiável garantia titular, não
dela, destruindo sua reputação de suborno ou
ameaça
+ anonimato significa conivência empresa não sabe quem é
"queima" se tentar fazer isso
- eles nunca sabe quando eles mesmos estão sendo testados
por algum serviço
- e o potencial bribers não vai saber quem contactar,
embora o e-mail pode ser dirigida para a garantia da empresa
com bastante facilidade,
- como a colagem de agências
- chave é que essas entidades têm a ganhar muito pouco
roubar dos seus clientes, e muito a perder (depende
de qualquer relação de única transação para o tamanho do mercado total)
- útil para os mercados negros e transacções ilegais (um
de terceiros confiável que ambos os lados podem confiança, ainda que não
completamente)
16.17.4. Reputação Baseada Em Sistemas De
+ De Rating de crédito de Serviços que são Imunes a Intromissão e
Ações judiciais
+ digital com pseudónimos, a verdadeira classificação de crédito de bases de dados
pode ser desenvolvido
- com nenhum dos "5 anos de expirações" (quero dizer, quem são
você para me dizer que não devo segurá-la contra uma pessoa que
os registros mostram que ele declara Capítulo 7 a cada 5 anos ou
então?...tal é a informação, e não pode ser
declarado ilegal, apesar de as questões políticas que são
envolvidos)
+ isto provavelmente poderia ser feito hoje, o uso de ventos de dados
os bancos, mas, então, pode desenvolver injunções contra
uso por empresas nos estados unidos
- como isso poderia ser aplicada? picadas? o aprisionamento?
+ "pode ser que a concessão de crédito a entidades será
forçado a usar fórmulas rígidas para as suas decisões,
com uma trilha de auditoria completa disponível para o
requerente
- se qualquer um "critério" ou juízo é permitido, em seguida,
estes ilegais ou ventos entradas podem ser usados
relacionados com a "revolução" e outros informal
mecanismos de sinalização

- lembre-se que Prop. 103 tentou ignorar normal
leis da economia
+ AMIX-como serviços irá oferecer várias abordagens aqui
+ variando de crédito convencionais de bases de dados, embora
com menores custos de entrada (por exemplo, um cidadão privado
poderiam lançar um "pedidos de falência" da base de dados, utilizando
de registros públicos, sem prazo de expiração, são apenas
relatar a verdade, por exemplo, que o zé pediu
falência pessoal em 1987
- isso leva a algumas das ideias estranhas envolvendo
obrigatória a reconfiguração da verdade, como quando "de crédito
os registos são eliminados" (expurgado do que? a partir do meu
pessoal bases de dados? a partir de registros públicos
e que agora estou a vender o acesso a?)
+ pode haver argumentos de que a "registros públicos" são
direitos autorais ou outra propriedade de alguém e, portanto,
não pode ser vendido
- livro de telefone caso (no entanto, as Supremes realizada
que o "ato criativo" foi específicos
arranjo)
- um truque pode ser um Habitat-como sistema, onde alguns dos
os registros são "históricos"
- para ventos de bases de dados
+ Resenhas De Livros, Críticas De Música
- às vezes com pseudônimos para proteger os autores de
retaliação ou mesmo ações judiciais
+ "O que devo comprar?" serviços " a la Consumer Reports
- novamente, proteção contra ações judiciais
16.17.5. Criptografia de Bancos e o "Jogo de aparências" como uma Metáfora Central
+ Central metáfora: o Jogo Shell
- descrição do convencional shell de jogo (e de alguns
alusões ao con artistas na esquina de uma rua-a mão é
mais rápido do que o olho)
+ como entrar em uma sala cheia de caixas de depósito seguro, com
não há vigilância e não há maneira de monitorar a atividade na
caixas....e o usuário pode comprar novas caixas de forma anônima,
transferência de conteúdos entre as caixas
- só desligar todo o sistema e forçar todos
as caixas de abrir faria qualquer coisa-e esta seria a "piscina"
todo o conteúdo (a menos que uma lei foi aprovada dizendo:
as pessoas poderiam "declarar" o conteúdo antes de alguns
dias....)
+ o shell de sistema de jogo pode ser "testado"-através do teste de

serviços, por suspeita de indivíduos, qualquer que seja muito baixo
custo dividindo alguns soma entre muitas contas e
verificando que o dinheiro ainda está lá (recuperando ou
descontá-los em)
- e lembre-se de que as contas são anônimos e são
indistinguíveis, de modo que o dinheiro não pode ser apreendida
sem repercussão
+ esta é, naturalmente, a forma como os bancos e similares reputação-
em todas as instituições têm sempre (ou quase) trabalhou
- pessoas de confiança, os bancos não para roubar seu dinheiro
verificar durante algum período de tempo que o seu dinheiro foi
não desaparecendo
- e por basear-se em alguns senso comum, as idéias de que o
banco de negócios básico a noção de que um banco
existe continuar no negócio e ganhar mais dinheiro
mais alguns longo prazo período por ser confiável do que ele
gostaria de fazer um one-shot imitação)
+ Numeradas de contas
- lembre-se de que a Suíça tem se curvou para o internacional
a pressão e agora é limitar (ou eliminar) numerada
contas (embora outros países ainda estão permitindo que alguns
formulário de tais contas, especialmente Lichtenstein e
Luxemburgo)
+ com criptografia números, ainda mais segurança
- "você perder seu número, difícil"
- mas o dinheiro tem de existir, de alguma forma, em algum momento?
+ opções para a forma física do dinheiro
+ contas de acções de um fundo público investido
- ações de agir como "votos" para a distribuição de
receitas
- dividendos são pagos à conta de (e enviada onde)
- um resumo, nebulosas idéia: várias camadas de dinheiro,
como desigual de direitos de voto de estoque...
+ poderia até mesmo ser físico depósitos
- talvez, até mesmo, manipulado pelo manuseio automático
sistemas (apesar de que isso é muito inseguro)
- o Bennett-Ross proposta Global para os Serviços de Dados
essencialmente, a forma inicial da presente
16.17.6. cryonicists vai buscar "crypto-relações de confiança" para proteger seus ativos
+ novamente, o "crypto" parte não é realmente necessário, dado que
de confiança advogados e sistemas similares
- mas o crypto parte-dinheiro digital-mais automatiza o
sistema, permitindo que pequenas e transações mais seguras

(sobrecarga é menor, permitindo que mais dispersões e
difusão)
- e elimina humano link
- de modo a proteger melhor contra intimações, ameaças, etc.
+ e para ajudar a financiar as "persistentes instituições" que vai fundo
pesquisa e protegê-los em suspensão
- eles podem também colocar os seus fundos em "politicamente correto"
a longo prazo, os fundos-que pode ou não exercer uma postive
ifluence no sentido que desejar, o que com a lei de
consequências não intencionais e todos os
opl
+ muitas avenidas para a lavagem de dinheiro persistente
instituições
+ dummy corporações (ou até mesmo real corporações)
- com longo prazo de consultoria arranjos
- "shell jogo" votação
+ como as pessoas começam a acreditar que eles podem possivelmente ser
revivido em algum tempo futuro, eles vão começar a se preocupar com
proteger os seus activos correntes
+ lembranças do "Por que Chamá-Los de Volta do Céu?"
- preocupações sobre a estabilidade financeira, sobre o confisco
de riqueza, etc.
- não será o substituto formas de imortalidade-a investidura fo
museus, universidades, etc.-ser como aceitável pessoas...
vai querer a coisa real
+ Investimentos que podem sobreviver atuais instituições
- compras de obras de arte (uma la de Bill Gates, que é na verdade um
possibel modelo para este tipo de comportamento)
direitos de obras famosas, com disposição para o direito autoral
validades, etc. (é por isso que a posse física é
preferível)
- shell de jogos, de curso de redes de reputação baseado em
contas)
- Jim Bennett relata que Saul Kent é como a criação de
as coisas em Lichtenstein para Alcor (que é o que eu sugeri
para Keith Henson vários anos atrás)

16.18. Crime organizado: as Tríades, Yakuza, Máfia, etc.
16.18.1. "O Novo Submundo Ordem"
+ Claire Sterling "Ladrão do Mundo"
- (Sterling é bem conhecido por sua visão conservadora sobre
as questões políticas, tendo escrito o polêmico "O
Terror Conexão", que, basicamente, indeferiu o papel de

a CIA e outras agências dos EUA em promover o terrorismo.
"Ladrão do Mundo" continua a postura alarmista, mas tem
alguns detalhes suculentos de qualquer maneira.)
- ela defende a aplicação da lei mais
+ mas foi a policiais corruptos estados da Alemanha Nazista,
Sovet Rússia, etc., que deu tantas oportunidades para
moderno corrupção
- e CIA -, etc. comércio de drogas, Guerra Fria desculpas, e
estado de segurança nacional renúncias
+ no FSU, a Máfia russa é o principal beneficiário
de privatização...só eles tinham o dinheiro e o
conexões para fazer as compras (ameaçando-a de que não
Mob licitantes, matando-os, etc.)
- como alguém colocado, o primeiro do mundo completo
criminal estadual
16.18.2. "É o mundo do crime interessado em criptografia? Eles poderiam ser
os primeiros que adotaram as técnicas avançadas?"
- o uso precoce: BBS/Compuserve mensagens, flash digital de papel,
códigos
- a lavagem de dinheiro, anstalts, bancos
- Tríades, pique marcas
- Mesmo que este uso parece inevitável, é, provavelmente, deve ser
cuidado aqui. Tanto porque a clientela para o nosso conselho de maio de
ser violento, e idem para a aplicação da lei. A conspiração
e RICO leis podem ser o suficiente para obter qualquer pessoa que aconselha, tais
pessoas em grandes problemas. (Claro, aconselhamento e consultoria
pode acontecer através do mesmo indetectáveis tecnologia!)
16.18.3. criptografia fornece alguns esquemas para obter mais seguro de drogas
distribuição
- células, morto cai, segura transferências para contas no exterior
- comunicação via piscinas, ou remetentes
- muito dinheiro é geralmente o problema...
- "siga o dinheiro" (FinCEN)
- não há moral, escrúpulos...quase todas as drogas são menos perigosos do que
o álcool é...que droga era muito popular para proibir
- essa droga de cenário é consistente com a Tríade/Mob
cenário

16.19. Em Particular Produzido Lei Policêntrica Lei, O Anarco-Capitalismo
16.19.1. "minha casa, minhas regras"
16.19.2. a la David Friedman
16.19.3. mercados de leis, a Lei do Comerciante
- empresas, outras organizações têm seus próprios locais

normas legais
- Extropians teve muito debate sobre isso, e vários concorrentes
códigos legais (como um experimento...não muito sucesso, para
várias razões)
- "Snow Crash"
16.19.4. os Cypherpunks grupo é em si um bom exemplo:
- algumas regras locais (local para o grupo)
- alguns constrangimentos por máquina host (ambiente de sapo,
soda)
+ mas é uma lista sobre "lei dos Estados Unidos"?
- com membros em dezenas de países?
somente quando o externo leis estão envolvidos (se um de nós
ameaçou um outro, e, mesmo assim este é duvidoso) o
as leis externas....
- negligência benigna, por necessidade
16.19.5. Eu não tenho absolutamente nenhuma fé na lei quando se trata de
cyberspatial questões outras questões, também).
- especialmente vis-a-vis as coisas como o acesso remoto a arquivos, um
la AA BBS caso
- "a lei é um cu"
- patch de uma área, outro quebras de
- O que então? A tecnologia. Remetentes, criptografia
16.19.6. Contratos e Criptografia
+ "Como os contratos devem ser aplicadas em criptografia anarquia
situações?"
- Uma pergunta-chave, e uma que faz com que muitas pessoas
pergunta se crypto anarquia pode funcionar em tudo.
+ Primeiro, pense em quantas situações são _already_
essencialmente, fora do âmbito da lei...e ainda no
que algo semelhante a "contratos" são executória,
embora não através do processo legal.
- amigos, relacionamentos
+ preferências pessoais em alimentos, livros, filmes, etc.
- que "o recurso" tenho em casos onde uma refeição
é satisfatória? Não vai voltar para o restaurante
geralmente é o melhor recurso (isso também é uma dica
sobre a importância da "expectativa de futuro
de negócios" como um meio de lidar com tais coisas).
- Nestes casos, a lei não está diretamente envolvido. No
de fato, a lei não está envolvido em _most_ humanos (e
nãohumanos!) interações.
+ As Principais Abordagens:
+ Reputações.

- as reputações são importantes, não são levemente para ser
considerado
- A Repetição De Negócios.
- Serviços De Garantia.
+ O "direito dos contratos" (e o dever de as respeitar, para
não tente alterar o contrato após os fatos) é um
crucial bloco de construção.
- Imagine uma sociedade em que os contratos são válidos. Este
permite que aqueles que estão dispostos a assinar contratos de definição de limites
negligência para ficar mais barato de cuidados de saúde, enquanto que aqueles que
não vai assinar tais contratos são livres para sue--mas de
claro, tem que pagar mais para os cuidados de saúde. Nada é de graça,
e frívola malversação de processos tem aumentado
os custos operacionais. (Lembre-se que o "psíquico", que alegou que
seus poderes psíquicos foram perdidos depois de uma tomografia. Um júri
concedeu-lhe milhões de dólares. Cf. Peter Huber livros
sobre as leis de responsabilidade.)
- Imagine, agora, uma sociedade em que nunca é claro se um
o contrato é válido, ou seja, os tribunais de anulação ou
alteração de um contrato. Isso distorce a análise acima, e
assim, os hospitais, por exemplo, tem que construir em segurança
margens e almofadas.
+ De criptografia pode ajudar criando depósito em garantia ou de colagem de contas realizada
por terceiros--rastreáveis para os outros-partes--que
atuar como agentes de ligação para conclusão dos contratos.
Tais arranjos não pode ser permitido. Por exemplo, um
o hospital, que tentou lidar com uma ligação
agência e pediu que os clientes também lidar com eles,
poderiam enfrentar sanções.
- "Seguro de cartões de crédito" são um exemplo atual: a pessoa paga
uma reserva de valor maior que o limite do cartão (talvez 110%).
A razão para isso não é a obtenção de crédito","
obviamente, mas para ser capaz de ordenar os itens por telefone, ou
para evitar o transporte de dinheiro. (O benefício é, portanto, no
channel de comércio).
16.19.7. O ostracismo, a Expulsão em Particular Produzido Lei
+ Voluntária e discricionário eletrônico comunidades também
admitir a possibilidade de fácil de banimento ou ostracismo
(grupo selecionado matar arquivos). De curso, a execução é
geralmente difícil, por exemplo, não há nada para parar
indivíduos de continuar a comunicar com o
ostracismo indivíduo, utilizando métodos seguros.
- Eu posso imaginar regimes em que o software key escrow é

usado, mas estes parecem muito complicado e intrusiva.
- A capacidade dos indivíduos, e mesmo subgrupos, para impedir
o ostracismo não é uma coisa ruim.
-
- "Em um mundo online, seria muito mais fácil para impor
eliminação seletiva ou o ostracismo que na vida real.
Filtragem de agentes pode olhar para certificados de aceite
agências de aplicação antes de deixar mensagens através de. Cada
usuário pode ter um conjunto de agências que foram compatível
com seus princípios, e outro conjunto de "foras-da-lei". Você
pode até mesmo acabar com o efeito de várias "lógico
sub-redes" de pessoas que se comunicam uns com os outros, mas não
fora de sua sub-rede. Algumas redes podem respeito intelectual
propriedade, outros não, e assim por diante." [Hal Finney, 1994-08-21]
16.19.8. Os Governos, Cyberspaces, PPLs
- Debate periodicamente irrompe na Lista sobre este tópico.
- Não pode ser cobertos aqui em detalhe suficiente.
- Friedman, Benson, Stephenson de "Snow Crash", etc.
16.19.9. O direito de recurso nos tribunais com criptografia mediada por sistemas de
isolados dos tribunais
- PPLs são essenciais
- a reputação da empresa, o compromisso, a mediação (crypto-mediada mediação?)
16.19.10. Fraude
- não exatamente raro na não-crypto mundo!
- novos sabores contras, provavelmente vai surgir
- anônimo contas bloqueadas, debate com Hal Finney sobre isso
problema, etc.
16.19.11. PPLs, policêntrica lei

16.20. Libertaria no Ciberespaço
16.20.1. o que é
16.20.2. paralelos para a Oceania, de Galt Gulch
16.20.3. A privacidade nas comunicações altera a natureza de conectividade
- comunidades virtuais, invisível para as pessoas de fora
- verdadeiramente uma criptografia cabal
- isso é o que assusta os legisladores mais...as pessoas podem
optar por sair do mainstream sistema de governo, pelo menos
em parte (e, provavelmente, cada vez mais)

16.21. O ciberespaço, espaços privados, o cumprimento de regras e tecnologia
16.21.1. Considerar a "lei" abordagem baseada em
- um grupo de discussão que não quer homens envolvidos ("protegida
espaço para womyn")

- então, a demanda do sistema de direito civil impor suas regras
- exemplo prático: sysadmins yank contas quando
"impróprio posts" são feitas
- a C&S de spam é um exemplo
- Nota: A rede como actualmente constituído é repleta de
confusão sobre quem é dono de que, sobre o que são públicos e
o que são recursos privados, e sobre o que as coisas são
permitido. Se zé envia Suzy Creamcheese um "indesejados"
letra, é este "abuso" ou "harassement"? É roubo
Suzy recursos? (Na minha opinião, claro que não, mas eu
concordo que as coisas são confusas.)
16.21.2. A abordagem tecnológica:
- espaços criados por criptografia...unbreachable paredes
+ exemplo: uma lista de discussão com os controles na associação
- pode requerer a nomeação e atestar por outros
- apresentação de alguns credencial (assinado por alguém), por exemplo,
de femaleness
- como você vai pagar pára de spam
16.21.3. Este é um exemplo concreto de como a criptografia funciona como uma espécie de
material de construção
- e por que o governo limitações sobre a criptografia prejudicar aqueles que
querem proteger os seus espaços próprios
- uma lista de discussão privada é um espaço privado, inacessível ao
aqueles que estão fora
- "Há boas abordagens de engenharia que pode forçar dados
para comportar-se. Muitos deles envolvem a criptografia. Nossa
governo restrições sobre a criptografia limite de nossa capacidade para
construir a confiança de sistemas de computador. Precisamos de uma forte criptografia para
engenharia básica razões." [Kent Borg", Argumentando Crypto:
A Abordagem Da Engenharia," 1994-06-29]
16.21.4. Comunidades virtuais-o Uso de Redes Virtuais para Evitar
Governo
- que é, as alternativas para a criação de novos países (como o
Minerva projeto)
- o Assassino de culto, uma seita religiosa nas montanhas da Síria, Iraque,
Afeganistão, etc. tinha uma rede de correios na montanha
fastnessess
- pirata comunidades, redes de postos de comércio e de rega
buracos, isenta-se apenas por alguns anos-a partir das leis da
potências imperiais
16.21.5. Estes espaços privados, como a tecnologia torna mais
"habitável" (não quero dizer, em um sentido integral, para que não me enviem
notas sobre como "você não pode comer ciberespaço"), tornar-se completo

funcionou "espaços" que estão fora do alcance da
governos. Uma nova fronteira, intocável por fora, coercitiva
governos.
- Vinge de "Nomes Verdadeiros" feita em tempo real
16.21.6. "O fato de as coisas realmente desenvolver neste "ciberespaço" que tantos
de nos falar?"
- "Você não pode comer ciberespaço!' é o ponto feito. Eu
argumentam, no entanto, que resumo mundos têm sido sempre com
nós, nas formas de comércio, a reputação, os amigos, etc.
E isso vai continuar.
- Algumas pessoas opuseram-se às vezes sobre-
entusiasta afirma que as economias e a sociedade vai
florescer mediada por computador cyberspaces. De forma resumida,
a objeção é: "Você não pode comer o ciberespaço." Significado
que os lucros e ganhos feitos no ciberespaço deve ser convertido
do mundo real lucros e ganhos.
- Em "Snow Crash", essa foi feita para ser difícil...Hiro
Protagonista era muito rico no Multiverso, mas viveu
em um contêiner de carga no LAX no "mundo real". Uma multa
a novela, mas essa idéia é screwy.
+ Existem muitas formas de transferência de riqueza para os "real"
mundo:
+ todas as várias lavagem de dinheiro, esquemas de
- dinheiro em contas no exterior, acessível para férias,
visitas, etc.
- falsos pedidos de compra
- o meu favorito: o Ciberespaço, Inc. contrata um como um
"consultor" (IRS não pode e não demanda prova de
o trabalho que está sendo feito, a natureza do trabalho, uma
qualificações para executar o trabalho, etc....Na verdade,
muitos consultores são contratados "no retentor," apenas para ser
disponível deve a necessidade surgir.)
- informações-venda
- investimentos
-
16.21.7. Protocolos para esta está longe de ser completa
- dinheiro, identidade, paredes, estruturas
- um monte de trabalho de base é necessário (embora as pessoas vão persegui-lo
localmente, não depois que o trabalho está terminado...por isso soluções
provavelmente emergente)

16.22. Dados Paraísos
16.22.1. "O que são dados paraísos?"

+ Lugares onde os dados podem ser ocultos ou protegidos contra legal
a ação.
- Sterling, "Ilhas na Rede", 1988
+ Experiências médicas, aconselhamento jurídico, pornografia, armas
- a reputação da empresa, lista de médicos, advogados, alugar vagabundos,
registros de crédito, privado olhos
- O que fazer sobre a pressão crescente para a proibição de certos tipos
de pesquisa?
- Um dos poderosos usos do forte de criptografia é a criação
de revistas, web sites, listas de discussão, etc., que são
"indetectáveis." Estas são algumas vezes chamados de dados "paraísos"
embora esse termo, como o usado por Bruce Sterling em "Ilhas
a Net" (1988), tende a sugerir lugares específicos, como o
Ilhas Cayman que as empresas podem usar para armazenar dados. Eu
preferem a ênfase em "cypherspace."
- "Vale a pena notar que, privada de dados "paraísos" de todos os tipos
são abundantes, especialmente para as matérias financeiras, e a maioria não são
sujeitos à regulamentação governamental....Alguns bancos têm
os departamentos de pesquisa que são mais velhos e mais abrangente
de crédito relatórios agências. Favorecido os clientes podem usar
- los para avaliação de negociação particular....Grandes escritórios de advocacia
manter bancos de dados que se aproximam as dos bancos, e eles
crescer com cada caso, através de adições de privada
pesquisadores pago por sucessivas clientes....Segurança
profissionais, como Wackenhut e Kroll, também o mercado
frutos de importantes coleções de dados....Para estes add
aqueles de seguro, de colagem, de investimento, de empresas financeiras
e o gosto que ajudam a fazer ou quebrar negócios."
[John Young, 1994-09-07]

16.22.2. "Pode haver leis sobre o que pode ser feito com os dados?"
- Normativo de leis ("eles não deveriam manter tais registros e, portanto,
nós vamos proibir-lhes") não funciona em uma era de forte de criptografia
e de privacidade. Na verdade, alguns de nós dados de suporte paraísos
precisamente para ter registros de, digamos, doenças terminais, de modo
nós não vamos emprestar o dinheiro para Joe-que-tem-AIDS. Ele não pode ser
"justo" para Joe, mas é o meu dinheiro. (A mesma idéia, no uso de
ventos ou cryptospatial dados paraísos para ignorar o
absurdo no "Fair credit Reporting Act" que foras-da-lei
a manutenção de certos tipos de fatos sobre crédito
os candidatos, tais como os que declararam falência de 10 anos
atrás, ou que eles partiram de uma cadeia de inadimplência, na Alemanha, em
a década de 1970, etc.)

16.22.3. Redes clandestinas, Piratas de Pesquisa e Informações

Contrabando
+ O Compartilhamento do Conhecimento Proibido
- mesmo se o conhecimento não é proibido, muitos
as pessoas apreciam a idéia de tráfico proibido
+ Alguns exemplos modernos
+ drogas e cultivo de maconha
- medicamentos para o prolongamento da vida, a AIDS tratamentos
- ilegal de drogas para uso recreativo
+ bootleg de investigação médica, AIDS e tratamentos de câncer,
etc.
- por exemplo, de auto-ajuda grupos de usuários que aconselhar sobre
tratamentos, alternativas, etc.
+ lockpicking e similares de segurança evasão
técnicas
- lembre-se que a posse de lockpicks pode ser ilegal
- o que acontece com os manuais? (note que a maioria dos catálogos de ter um
disclaimer: "Esses materiais são para a educação
meramente informativo, ...")
- defesa de questões relacionadas a: limitações em debate
as questões de segurança nacional pode resultar em "anônimo
fóruns"
+ BTW, o trabalho recente em caranguejo, conchas e outros rígido conchas
produziu ainda mais forte armadura!
- isso pode ser alguns da pesquisa genética que é
altamente classificado e é vendido em anônimo redes
+ Alquimistas e a busca pela imortalidade
+ teoria de que o "Avô de todos os cultos" (expressão minha)
iniciado há cerca de 4500 a. C.
- tanto o Egito e a Babilônia/Suméria
+ ancestral dos Gnósticos, os Sufis, Illuminati, etc.
- O místico Sufi Gurdjieff dizia que ele era um membro
de um culto místico formado na Babilônia cerca de 4500
B. C.
- aranha, venom?
+ Especulação: um grupo ou de um culto voltado para a vida
extensão, para a busca de imortalidade-talvez
um link para O Épico de Gilgamesh.
+ A lenda de Gilgamesh
- Gilgamesh, acadiano tábuas de pedra em
Nínive
- fez uma jornada para encontrar Utnapihstim, sobrevivente de
Dilúvio babilônico e possuidor de um segredo de
a imortalidade (uma planta que iria renovar a juventude)

- mas Gilgamesh perdeu a planta para uma serpente
+ Egípcios
- obviamente, os Egípcios tinham o maior interesse em
extensão da vida útil e/ou imortalidade
+ Osíris, Deus da Ressurreição e da Vida Eterna
- também o Escuro Companheiro de Serius (acredita-se
ser uma estrela de nêutrons?)
- eles dedicado enorme fração de riqueza para as pirâmides,
embalsamamento, etc. (mirra ou incenso de
cidade do deserto moderna Omã, descobriu com
shuttle imaging radar)
+ "pirâmide de poder": o papel no Grande Selo, sinal de
Illuminati, e de teorias sobre a energia cósmica,
formas geométricas, etc.
- e lembre-trabalho em significados numerológicos
da Grande Pirâmide dimensões
-
+ Cristianismo Primitivo
- foco na ressurreição de Jesus Cristo
+ Busca pela imortalidade é um personagem importante
motivação ou tema
+ indiscutivelmente para todas as pessoas: através de crianças,
realizações, com duração de acções, ou ainda "uma boa
vida"
- "Viva uma vida boa não é um substituto para a vida
para sempre"
- mas alguns procuram explicitamente
- "Milhões vivo hoje nunca vai morrer." (ecos do
passado cultos religiosos....As Testemunhas de jeová?)
- proibido pela Igreja (a Inquisição)
+ pesquisa, tal como ela foi, foi mantido vivo por segredo
ordens que comunicavam secretamente e no código e que
foram muito seletiva sobre a associação
- classes de associação para proteger contra descoberta
(o espião moderno sistema de célula)
vermelho - arenques concebido para desviar a atenção de
+ tudo isso se encaixa a estrutura de grupos como o
Os maçons, Maçons, Illuminati, rosa-cruz, e outros
mística grupos
- com membros como John Dee, astrólogo da corte da Rainha
Elizabeth
+ um gênio do escritor-cientista como Goethe foi, provavelmente, um
membro deste grupo

- Faust foi sua mensagem de luta
- com a Idade do Racionalismo, o místico, mumbo-jumbo
aspectos da alquimia, a pesquisa foi considerada passar&#65533;,
e grupos como Crowleys O. T. O. tornou-se puramente mística
showmanship
+ mas a necessidade de manter o segredo foi agora no financeiro
arena, com vastos recursos corporativos, laboratórios de p & D, e
bancos necessário
- assim, o papel do Morgans, Rothschilds, etc. no
estas conspirações
+ e modernas redes de computadores irá fornecer a próxima
passo, a próxima vez que o sistema de pesquisa
- financiados de forma anônima
- anônimo sistemas significa que os pesquisadores podem publicar
resultados controversos áreas (lembre-se de que
cryobiologists não se atreve a mencionar a criónica, para que eles
ser expulso da American Cryobiology xxx)
+ Bootleg de Investigação Médica (e a Criónica)
+ Criónica de Investigação e Tratamentos Anti-envelhecimento
+ O uso de Nazista Dados
a hipotermia experiências no campo de concentração de Dachau
+ Anti-envelhecimento medicamentos e tratamentos
- a fonte da juventude, etc.
- muitos FDA restrições, é claro
- México
+ Suíça
- fetal bezerro de células?
- sangue alterar ou reciclagem?
+ Ilegal Experiências
- relatórios de oxigênio hiperbárico pode ajudar a revitalização de
pacientes de puro-morte em acidentes de congelamento
+ Preto Mercados de Medicamentos, Tratamentos Médicos
+ RU-486, as proibições ele
- anti-aborto inimigos
- fácil de sintetizar
- AGORA tem indicado planos para distribuir esta droga
si, para criar redes (assim, a criação de
de facto aliados do libertário orientada para os usuários)
+ Bancos De Órgãos
+ o estabelecimento de um lucro para os doadores de órgãos
- pode ser a única forma de gerar doações suficiente,
mesmo entre os mortos
- alguns estão a ser feitos planos para tais motivos,

especialmente para motivar as famílias de morrer
pacientes
- questões éticas
+ o que sobre a colheita do que ainda é vivo?
- libertários gostaria de dizer: OK, se o consentimento informado foi
dado
- o rico pode ir para o exterior clínicas
+ De pacientes com AIDS unindo através de quadros de avisos para compartilhar
tratamento idéias, auto-ajuda, etc.
- com a compra de viagens para o México e em outros lugares
- as autoridades irão tentar deter tais BBSs (no que
motivos, se não o dinheiro está mudando de mãos?)
+ Os médicos podem participar de metro de redes de investigação
para proteger a sua própria reputação e estatuto profissional
- para escapar de AMA ou outras organizações profissionais e
sua restritivas de códigos de ética
+ ou judiciais, e a publicidade negativa
- alguns grupos, os "Anjos da guarda" de futuro,
procurar expor aqueles que eles acham que estão cometendo
crimes: abortistas (apesar de legal), etc.
- "politicamente incorreto" de investigação, tais como a vitamina
a terapia, a longevidade de investigação, a criónica
- cirurgia de implante de mama pode ser forçada no mercado negro
(e, talvez, os médicos que, mais tarde, descobrir provas de tais
as operações poderão ser obrigados a comunicar tais operações)
+ Volta de Questões de Testes e Bibliotecas de Documentos
- já existentes, mas imagine com um AMIX-como frontend?
+ De diferentes tipos de redes irão surgir, não todos eles
igualmente acessível
+ o equivalente para o de drogas e de armas, as redes não
o ganho de entrada, só por perguntar em torno de um bit
- a credibilidade, a reputação", fazendo com que seus ossos"
- essas redes não estão abertos para a pessoa casual
+ Algumas Redes Podem Ser Para o Suporte do Exterior
Pesquisadores
+ que enfrentam restrições sobre a sua pesquisa
- por exemplo, os países que a proibição do controle de nascimento poderá proibir
pesquisadores da comunicação com outros pesquisadores
+ suponha dos EUA, os pesquisadores estão ameaçados com
sanções-perda de suas licenças, censura, mesmo
procuradoria-se participarem de RU-486 experiências?
- lembre-se da AIDS drogas bootleg ensaios em SF, c. 1990
- ou para ignorar restrições de exportação

- cenário: várias anônimo quadros de avisos são definidas
-e, em seguida, fechado pelas autoridades-para facillitate
anônimo conexões (tanto como "anonymous FTP")
+ De grupos confrontados com debilitantes ações judiciais "ir
metro"
- Act A Up! e a Terra em Primeiro lugar! tem não identificável central
escritório que pode ser processado, desligar, etc.
- e a Operação de Resgate tem feito a mesma coisa

16.22.4. Ilegal De Dados

- histórico de crédito que viole alguma lei atual sobre
registros
- bootleg de investigação médica
- roubo de dados (por exemplo, a partir de concorrentes....um GDS sistema poderia
permitir consultas remotas de um banco de dados, quase "oracular,"
sem os dados roubados estar em uma jurisdição dos EUA)
- clientes no U. K ou a Suécia, que está proibido de
compilar bases de dados em que os indivíduos podem escolher para guardar o
dados de ventos e, em seguida, acessá-lo de forma discreta (outro motivo
criptografia e ZKIPS deve ser oferecido)

16.22.5. "a Suíça de dados"

- Brussells supostamente aumenta menos de sobrancelhas
Listenstaine, Luxemburgo, Suíça, etc.
- Ilhas Cayman, outras pequenas nações veja as possibilidades

16.22.6. Mercados de informação pode ter para mover ventos, devido à
de licenciamento e outras restrições

- assim como corretoras e corretores de seguros de são licenciados,
o governo pode insistir para que informações revendedores ser
licenciado (passar de ano, ser sujeitas a auditorias e regulamentos)

16.23. Minar Governos--Colapso do Estado

16.23.1. "É legal para defender a derrubada de governos ou a
a quebra de leis?"

- Embora muitos Cypherpunks não são radicais, muitos outros de
nós somos, e nós, muitas vezes, defendem "o colapso dos governos" e
outras coisas tais como esquemas de lavagem de dinheiro, evasão de divisas,
novos métodos de espionagem, informação de mercados, dados
paraísos, etc. Este rasises preocupações evidentes sobre a legalidade.
- Primeiro, tenho que falar, principalmente dos EUA questões...as leis
da Rússia ou Japão ou o que pode ser completamente diferente.
Desculpe para os EUA centrada no foco deste FAQ, mas que
do jeito que está. O Líquido começou aqui, e ainda é
predominantemente aqui, e as leis dos estados unidos estão sendo
propagada em todo o mundo como parte da Nova Ordem Mundial

e o colapso da outra superpotência.
- É legal para defender a substituição de um governo? No
os estados unidos, é o básico do processo político (embora os cínicos
pode-se argumentar que ambas as partes representam o mesmo que regem
a filosofia). Defendendo a *derrube violento* dos EUA
o governo aparentemente é ilegal, apesar de que eu não cite em
isso.
+ É legal para defender a atos ilícitos em geral? Certamente
muito da liberdade de expressão é precisamente este: discutindo a droga
usar, por boicotes, etc.
+ FEP gopher site tem isso em um "defensor da Lei,
Brandenburg v. Ohio. ":
- "Em 1969 caso de Brandemburgo v. Ohio, o Supremo
Tribunal derrubou a condenação de uma Ku Klux Klan
membro sob um criminoso sindicalismo lei e estabelecido
um novo padrão: o Discurso não pode ser suprimido ou
punidos, a menos que ele se destina a produzir iminente
sem lei de ação", e é " provável para produzir tais
ação". Caso contrário, a Primeira Emenda protege mesmo
o discurso que defende a violência. O teste é de Brandemburgo
a lei hoje. "
16.23.2. Espionagem e Subversão dos Governos Será
Revolucionada pela Forte de Criptografia
- (Eu acho que eles ver o que nós vemos, também, e este é um
a motivação para a tentativa de limitar o uso de forte
crypto. Além de algumas das mais convencionais razões.)
+ Digital morto cai, irá revolucionar espionagem
+ spies e seus controladores podem se comunicar de forma segura,
de forma relativamente rápida, sem medo de estarem sendo observados, a sua
gotas comprometida, etc.
- não há mais cantos de árvores, sem mais as marcas de giz no
caixas de correio para o sinal de uma queda para ser feito
+ este deve estar pirando a comunidade de inteligência!
- mais informações sobre por que a oposição a criptografia é tão
forte
+ Célula Baseada em Sistemas Convencionais e Sistemas de Proteção
+ Células são uma forma padrão para limitar os danos da exposição
- o padrão é 3-pessoa célula, tão comum no
primeiros dias de espionagem Soviética nos EUA
- mas sistemas de computador podem permitir novos tipos de células, com
mais complicado protocolos e mais segurança
+ Manter arquivos para proteção é um outro padrão
método de proteção

+ e com forte criptografia, esses arquivos podem ser mantidos
criptografados e em locais não visíveis (por exemplo, postado
em quadros de avisos ou outros lugares, com apenas o
chave necessária em um momento posterior para abrir)
- a la "arquivos binários" a idéia, em que ficheiros encriptados
estão amplamente disponíveis por algum tempo antes de a chave é
distribuído (portanto, tornando-se muito difícil para os governos
para interromper a distribuição dos arquivos raw)
16.23.3. "Xº Coluna" (X = criptografada)
- A eventual necessidade de utilização de criptografia forte como uma ferramenta para
lutar contra o estado.
+ ajudando a minar o estado usando denunciantes e
anônimo mercados de informação para vazamento de informações
- o 63,451 pessoas falsas identidades na WitSec
programa de...fuga de seus nomes, assista ao ser eletrocutado por
vingativo inimigos, e assistir o governo se contorcer
- o leilão dos detalhes de 1967, Inspector-Geral do
relatório da CIA assassinatos
16.23.4. use clandestinos, célula-base de sistemas podem permitir um pequeno
grupo para usar o "cupim" métodos para destruir a sociedade, para
destruir um estado que tornou-se demasiado repressivo (soa como
EUA-me)
sistemas criptografados, anônimo, piscinas, etc., permitir que verdadeiramente
seguro cell-based systems (esta é, aliás, um dos
preocupações de muitos países têm sobre "permitindo" criptografia
para ser usado...e eles estão certos sobre o perigo!)
a subversão de fascista ou socialista governos, minando
os chamados governos democráticos
16.23.5. "Por que não o governo simplesmente proibir tais métodos de encriptação?"
+ This sempre foi o Problema Número Um!
- criado por Stiegler, Drexler, Salin:, e vários outros
(e, na verdade, levantadas por alguns como uma objeção à minha mesmo
ao abordar estas questões, a saber, que a ação, em seguida, pode ser
levado para a cabeça fora do mundo que eu descrever)
+ Tipos de Proibições sobre Criptografia e Sigilo
- Proibição de Utilização Privada de Criptografia
- Proibição de Armazenar e Encaminhar Nós
- Proibição e Tokens de Autenticação ZKIPS
- Requisito para a divulgação pública de todas as transações
+ Notícias recentes (3-6-92, mesmo dia em que Michaelangelo e
Cortador de grama Homem) que o governo está propondo uma sobretaxa
em empresas de telecomunicações e serviços de longa distância para pagar novas
equipamentos necessários para a toque de celulares!

- S. 266 e facturas relacionadas com a
- esta foi a argumentar em termos de parar os traficantes de drogas e
outros criminosos
- mas, como o governo pretende lidar com os
várias formas fo usuário final de criptografia ou "confusão"
(a confusão que vai vir de compressão,
packetizing, simples de criptografia de arquivo, etc.)
+ Tipos de Argumentos Contra Tais Proibições
- Os "Direitos Constitucionais" Argumentos
+ "É Tarde Demais" Argumentos
- PCs já estão amplamente espalhados, a execução de dezenas de
a compressão e encriptação de programas...é muito
final de insistir "em claro" transmissões, qualquer que seja
pode ser (é código de programa distinguível de
mensagens criptografadas? Não.)
criptografado por fax, modem geralmente (embora com algumas
restrições)
- as LANs sem fios, pacotes, rádio, IV, do texto comprimido e
imagens, etc....tudo vai derrotar qualquer esforços curtos de
a polícia de intervenção do estado (que ainda pode acontecer)
+ A "Briga Dentro da NSA" Argumentos
- COMSEC vs. PROD
+ Afetará os direitos de privacidade das empresas
- e há muita evidência de que as empresas estão em
fato a ser espiado, por governos estrangeiros, pelos
NSA, etc.
+ Eles Vão Tentar Proibir Tais Técnicas de Criptografia
+ Picadas (talvez usando vírus e bombas lógicas)
- ou "de bário", para rastrear o código
+ De responsabilidade Legal para empresas que permitem que os funcionários usem
tais métodos
- talvez, até mesmo, no seu próprio tempo, através da suposição de que
os funcionários que usam software ilegal métodos em suas próprias
tempo são, talvez, correios ou agentes para a sua
corporações (um tênue ponto)
16.23.6. "Como as massas, ser convertido?"
- Provavelmente não. As coisas apenas acontecem, assim como o
as massas não foram convertidas em questões do mundo financeiro
mercados de instrumentos derivativos, e um monte de semelhante
coisas.
- Crypto anarquia é, sobretudo, uma abordagem pessoal
retirada de evitação. Massa consenso não é necessário
(a menos que o estado de polícia opção é fechar).

- Não pense em termos de venda de criptografia anarquia para Joe Média. Só usá-lo.

16.23.7. Como as coisas parecem estar piorando, vis-a-vis a criação de um estado policial nos EUA-pode ser uma boa coisa que anônimo assassinato mercados vai ser possível. Pode ajudar a nivelar o campo de jogo, como os Federais tiveram seus bater as equipes por muitos anos (juntamente com suas casas seguras, forjado credenciais, alojamento endereços, cut-outs, e outros accouterments da inteligência de estado).

- (Eu não vou entrar em conspirações aqui, mas é o seguinte termos podem desencadear algumas memórias: Gehlen Org, Wackenhut, McKee Equipe, Danny Casolaro, Cabazon Índios, Gander falhar, Iraque braços negócios, Pan Am 103, Bridegrooms de Morte, francês Conexão, Fascista Terceira Posição, Phoenix Programa, Bebe Rebozo, Marex, Otto Skorzeny, Nixon, P-2, Klaus Barbie, etc.)

- A abundância de provas de mau comportamento em grande escalas, as agências de inteligência, as forças policiais, e os estados em de modo geral. O poder absoluto corrompeu absolutamente.

- Eu certamente não estou defendendo o assassinato de Congressrodents e outros burocratas, apenas observando que esta nuvem pode ter um forro de prata.

16.24. Depositários e Reputação

16.24.1. De custódia de Agentes como uma forma de lidar com contrato renegging

- Na linha de compensação tem o perigo implícito em todos os negociações que Alice vai entregar o dinheiro, Bob irá verificar que autorizou, em hisaccount (nos antigos termos, Bob teria de esperar palavra que sua conta bancária Suíça acaba de ser creditado) e, em seguida, Bob vai conseguir concluir o seu fim de a barganha. Se a transação é verdadeiramente anônimo, sobre linhas de computador, então é claro que Bob simplesmente trava-se o seu modem e a ligação é interrompida. Esta situação é tão antiga como tempo, e sempre envolveu outros protocolos em que a confiança, a repetição de negócios, etc., são factores. Ou conivência de agentes.

- Muito antes de a "custódia" de Clipper, verdadeira garantia foi planejado. De caução como garantia de agentes. Ou colagem de agentes.

- Alice e Bob querem a realização de uma transação. Nem confia os outros;
de fato, eles são desconhecidos uns dos outros. Nas etapas "de Ester Garantia De Serviço." Ela é _also utraceable_, mas tem estabeleceu uma assinado digitalmente presença e um bom reputação pela sua imparcialidade. Seu negócio está sendo um garantia

agente, como uma ligação de agência, e não na "queima" de qualquer
festa. (A matemática isso é interessante: enquanto a
os lucros a serem obtidos a partir de qualquer pequeno conjunto de transações é
menos do que seu "capital de reputação," é no seu interesse
abrir mão de lucros a partir da queima e ser honesto. É
também é possível marcar que Esther não pode lucrar
a queima de tanto Alice quanto Bob ou de ambos, ou seja, por
devidamente criptografar o caucionadas coisas.)
- Alice pode colocar sua parte da transação em conivência com
Ester, Bob pode fazer o mesmo, e, em seguida, Ester pode lançamento
os itens para as partes quando as condições forem atendidas, quando ambos
as partes concordam, quando o julgamento de algum tipo ocorre, etc.
(Há uma dúzia de problemas aqui, é claro, sobre como as controvérsias
são liquidada, sobre a qual as partes certificar-se de que
Ester tem os itens, ela diz que tem, etc.)
16.24.2. Utilização dos serviços de garantia como um substute para o governo
+ como no submundo ofertas, acordos internacionais, etc.
- "Máquinas de Liberdade" (Friedman), "A Empresa de
Lei" (Benson)
- "É importante ter em atenção, em qualquer caso, que o uso de terceiros-
festa de caução como um substituto para a regulamentação do Governo foi
uma característica do Norte da europa, semi-anarchies de
A islândia e a Irlanda, que tem informado moderno libertário
pensamento." [Duncan Frissell, 1994-08-30]
16.24.3. Várias pessoas levantaram a questão de alguém em um
anônimo transação simplesmente tomar o dinheiro e não
executar o serviço (ou o outro lado). Este é o lugar onde
intermediaries entram em cena, assim como no real
worl (títulos, de custódia de agentes, etc.).
16.24.4. Alice e Bob gostaria de conduzir um anônimo transação; cada
é desconhecido para o outro (sem conhecimento físico, não pseudônimo
reputação de conhecimento). Estes "mutuamente suspeitos, os agentes," em
Anos 1960 e 70 da era da ciência da computação linguagem, deve organizar
métodos para a realização de negócios, enquanto não confiar nos outros.
16.24.5. Vários protocolos criptográficos têm sido desenvolvidos para tais
coisas como "pouco compromisso" (útil em jogar poker a
telefone, por exemplo). Eu não sei de que os progressos realizados na
a granularidade do anônimo transações, embora. (Embora o
protocolo de criptografia de blocos de construção em níveis inferiores, tais
como pouco compromisso e blobs--irá, provavelmente, ser usado
eventualmente, em níveis mais elevados, em mercados.)
16.24.6. Eu acredito que não há evidência de que nós podemos encurtar o ciclo de
empréstimo noncryptographic protocolos (uma heresia para os puristas!) e

adaptação. A reputação da empresa, por exemplo. E de custódia de agentes (um
forma de reputação, em que o "valor" de uma ligação de entidade
ou escrow agent reside na capital de reputação).
16.24.7. se uma única garantia de agente é suspeito de ser indigno de confiança,
(em uma capital de reputação sentido), então pode usar _multiple_
escrows
- com vários protocolos, contrapartidas
- n-out-of-m de voto esquemas, onde n custódia de agentes de m
são necessárias para concluir uma transação
- difícil de compromisso a todos eles, especialmente se eles não têm
idéia se eles estão sendo "legitimamente subornados" ou apenas
pingado por uma reputação de classificação de serviço
- Palpite: o trabalho de Chaum, Bos, e o Pfaltzmanns no DC-
as redes podem ser directamente aplicável aqui...problemas de conluio,
conjuntos de colluders, detecção de colisão, etc.

16.25. Previsões vs. Implicações
16.25.1. "Como sabemos que a criptografia anarquia 'o trabalho', para que o
direito de instituições de emergir, de que os erros serão concertados,
etc.?"
- Nós não sabemos. Algumas coisas são certas. Só o tempo dirá.
Estas são questões emergentes, onde a evolução
determinar o resultado. Como em outras áreas, as formas de
soluções terão tempo para evoluir.
- (Os Fundadores não poderia ter previsto de forma corporativa
lei levaria, mas como um exemplo.)
16.25.2. Meu pensamento sobre a criptografia anarquia não é tanto como _prediction_
exame de tendências e as implicações de certas coisas.
Assim como vigas de aço dizer certas coisas para o desenho de
edifícios, assim também acontece com criptografia inquebrável dizer certas coisas
para a concepção de sistemas sociais e econômicos.
16.25.3. Várias tecnologias estão envolvidos:
- Criptografia inquebrável
- Untraceable comunicação
- Unforgeable assinaturas
16.25.4. (Nota: Sim, às vezes é perigoso dizer "inquebrável,"
"indetectáveis", e "unforgeable." Os puristas abster-se de tais termos.
Todos os criptografia é a economia, até mesmo de informação, teoricamente,
seguro de criptografia (por exemplo, subornar alguém para lhe dar a chave, quebra de
e roubar, etc.). E computacionalmente seguro de criptografia--
como RSA, IDÉIA, etc.--pode, em *princípio* - bruta-forçado.
Na realidade, os custos podem ser exhorbitantly
de alta...talvez mais energia do que a que está disponível em todo o

o universo seria necessário. Essencialmente, essas coisas
como inquebrável, untraceable, e unforgeable como se pode
imaginar.)
16.25.5. "Forte materiais de construção" implica certas coisas. Rodovias,
pontes, motores a jato, etc. Da mesma forma, para o forte de criptografia, que
a forma exata das coisas que se constroem ainda é desconhecida.
Mas muito claramente de algumas incríveis novas estruturas serão construídas
este caminho.
16.25.6. O ciberespaço, paredes, tijolos e argamassa...
16.25.7. "Será forte criptografia ter o efeito principal de proteção atual
liberdades, ou vai criar novas liberdades e novas situações?"
- Há um campo que acredita, principalmente, que o forte de criptografia vai
assegurar que os actuais liberdades sejam preservadas, mas que esta
não vai mudar as coisas materialmente, as Comunicações poderão ser
privado, diários podem ser garantidas a segurança do computador será
avançado, etc.
- De outro acampamento--de que eu sou um vocal porta-voz--acredita
que qualitativamente diferentes tipos de transacções, será
tornou-se possível. Além disso, é claro, para a obtenção de
liberdades que o primeiro acampamento de coisas é o efeito principal.
+ Esses efeitos são specultative, mas provavelmente incluem:
- aumento da ocultação de bens através de untraceable bancário
sistemas
- mercados de serviços ilegais
- aumento da espionagem
- dados paraísos
16.25.8. "Com todo o cripto-anarquia transações de ser anônimo?"
- Não, várias partes vão negociar arranjos diferentes.
Tudo é uma questão de economia, de cumprimento de prazos, etc.
Alguns, alguns não. O fundamental é que a decisão
para revelar a identidade vai ser apenas outro mutuamente negociados
questão. (Pense em gastar dinheiro em uma loja. O proprietário da loja
pode _want_ para saber o que seus clientes estão, mas ele ainda vai
ter dinheiro e permanecer na ignorância, na maioria dos casos. A menos que uma
governo passos e distorce o mercado, exigindo
aprovações de compras e registros de identidades-pensar
armas aqui.)
- Por exemplo, os locais não pode emprestar-me dinheiro, se eu estou
anónimo para eles, mas eles têm um "gancho" em mim se eles
sabe quem eu sou. (Aspectos do anonimato pode ainda ser utilizado,
como os sistemas que não deixam de papel ou computador trilha
apontando para eles ou para mim, para evitar picadas.)
- "Execução" no metro de mercados, para que o

legal convencional remédios são impossíveis, é, muitas vezes, por
meio de força física: quebrando pernas e até mesmo matar
welshers.
- (Pessoalmente, eu não tenho problemas com isso. A Multidão não pode
ligar para a polícia local, por isso tem que se impor suas ofertas
próprio caminho. Se você não pode pagar, não joga.)

16.26. Como Criptografia Anarquia Será Travada
16.26.1. O Ataque Direto: Restrições de Criptografia
+ "Por que não o governo simplesmente proibir tais métodos de encriptação?"
+ Esse sempre foi o Problema Número Um!
- criado por Stiegler, Drexler, Salin:, e vários outros
(e, na verdade, levantadas por alguns como uma objeção à minha mesmo
ao abordar estas questões, a saber, que a ação pode, em seguida,
ser levado para a cabeça fora do mundo que eu descrever)
+ Tipos de Proibições sobre Criptografia e Sigilo
- Proibição de Utilização Privada de Criptografia
- Proibição de Armazenar e Encaminhar Nós
- Proibição e Tokens de Autenticação ZKIPS
- Requisito para a divulgação pública de todas as transações
+ Notícias recentes (3-6-92, mesmo dia em que Michaelangelo e
Cortador de grama Homem) que o governo está propondo uma sobretaxa
em empresas de telecomunicações e serviços de longa distância para pagar novas
equipamentos necessários para a toque de celulares!
- S. 266 e facturas relacionadas com a
- esta foi a argumentar em termos de parar os traficantes de drogas e
outros criminosos
- mas, como o governo pretende lidar com os
várias formas fo usuário final de criptografia ou "confusão"
(a confusão que vai vir de compressão,
packetizing, simples de criptografia de arquivo, etc.)
+ Tipos de Argumentos Contra Tais Proibições
- Os "Direitos Constitucionais" Argumentos
+ "É Tarde Demais" Argumentos
- PCs já estão amplamente espalhados, a execução de dezenas de
a compressão e encriptação de programas...é muito
final de insistir "em claro" transmissões, qualquer que seja
pode ser (é código de programa distinguível de
mensagens criptografadas? Não.)
criptografado por fax, modem geralmente (embora com algumas
restrições)
- as LANs sem fios, pacotes, rádio, IV, do texto comprimido
e imagens, etc....tudo vai derrotar qualquer esforços curto

a polícia de intervenção do estado (que ainda pode acontecer)
+ A "Briga Dentro da NSA" Argumentos
- COMSEC vs. PROD
+ Afetará os direitos de privacidade das empresas
- e há muita evidência de que as empresas estão em
fato a ser espiado, por governos estrangeiros, pelos
NSA, etc.
+ Eles Vão Tentar Proibir Tais Técnicas de Criptografia
+ Picadas (talvez usando vírus e bombas lógicas)
- ou "de bário", para rastrear o código
+ De responsabilidade Legal para as empresas que permitem que os funcionários
o uso de tais métodos
- talvez, até mesmo, no seu próprio tempo, através da assunção
que os funcionários que usam software ilegal métodos
seu próprio tempo são, talvez, correios ou agentes para
suas corporações (um tênue ponto)
- restrições: o uso de códigos e cifras
+ há muito tempo tem sido certas restrições sobre o uso de
criptografia
- criptografia através de ondas de rádio é ilegal (a menos que a chave é
fornecido para o governo, como com o código Morse)
+ em tempo de guerra, muitas restrições (por todos os governos)
- quem encriptar são, ipso facto, culpado e são fotografadas
sumariamente, em muitos lugares
- mesmo hoje em dia, o uso de criptografia perto de uma base militar ou
dentro de um contratante de defesa poderia violar as leis
+ S. 266 e projetos semelhantes para mandato "alçapões"
+ exceto que isso vai ser difícil para a polícia e até mesmo para
detectar
- tantas maneiras de ocultar mensagens
- muito comuns de compactação, a soma de verificação, etc.
+ Chave De Registro De Trilha De Balão
- cite Denning da proposta, e a minha própria lançamentos

16.26.2. Outro Ataque Direto: Eliminação de Dinheiro

+ a idéia de que a eliminação do dinheiro, com os cartões de crédito
substituir o dinheiro, irá reduzir mercado negro
- "uma pessoa, uma IDENTIFICAÇÃO" (objetivo de muitos internacional
as organizações de padrões)
- eliminação de dinheiro pode vir a ser amarrado para o
chave de registro de idéias...o governo torna-se um terceiro
em todas as transações
+ um dos favoritos dos teóricos da conspiração
- de forma extrema: o número da Besta tatuado em nós

(crédito, números, etc.)
- trocas de moeda (rumores sobre as Redes sobre o iminente
lembro de notas, ostensivamente para lavar ilícitos
ganhos e fazer a contrafação mais fácil)
+ mas também é algo que os governos gostam de fazer, às vezes, classificação
de recordar-nos quem está realmente no comando
- Alemanha, um par de vezes
- França, no final dos anos 1950
- várias outras desvalorizações de moeda e reformas
+ Parcial passos já foram feitas
- as transações em dinheiro superiores a um valor de us$10.000, neste
o tempo, apesar de "suspeitos" sub-$10K transações devem ser
relatou-são proibidos
+ grande denominação contas foram retirados de
circulação
- utilizado no tráfico de droga, o argumento
- Massachussetts exigiu que os bancos viram todos os
registros de conta, SS números, saldos, etc.
+ "Se o que você está fazendo é legal, por que você precisa de dinheiro para
ele?"
- parte da antiga American dicotomia: de privacidade versus "o Que
você tem a esconder?"
+ Mas por que a proibição de cash não funciona
+ se existe uma necessidade, mercados negros irão surgir
- i.é., o normal tradeoff entre risco e recompensa:
pode haver alguns "descontos" no valor, mas cah
ainda circulam
+ muitos outros canais: títulos e valores mobiliários, segredos, bens
+ a negociação de ouro ou de prata, nem de que são
proibida qualquer por mais tempo, a negociação em segredos, como o
o governo parar com isto?
- arte a ser utilizada para a transferência de dinheiro entre internacional
fronteiras (evita Aduaneiro)
- "consideração" dado, a la esquema para ocultar rendimentos
+ total de vigilância?
- ele não funciona mesmo na Rússia
- por outro lado, a Rússia não possui o "ponto de venda"
infra-estrutura para impor um sistema sem dinheiro
16.26.3. Outro Ataque Direto: o Controle do Governo de Criptografia,
Redes e Acesso à rede.
- a la antigo Sino Sistema de monopólio, o que limita o que pode
ser conectado a uma linha telefônica
+ o governo pode assumir o controle de redes em vários

formas:
+ FCC-tipo de restrições, embora seja difícil ver como um
rede privada, a propriedade privada, poderia ser restrito
- como ele não está usando parte do público "espectro"
- mas ele é duro para construir um muito interessante de rede que
fica em propriedade privada....e assim que ele cruza
propriedade pública, BINGO!
+ "Dados nacionais de Estrada" poderia ser tão fortemente subsidiado
que alternativas definham (por um tempo)
- o Al Gore propostas para uma financiados pelo governo federal, do sistema de
(e sua esposa, Basculante, é claro, um líder da
censura asa)
- e então, o governo pode reivindicar o direito e o dever de
definir o "tráfego" leis: protocolos, tipos de criptografia
permitido, etc.
- principais patentes, a la RSA (se na verdade do gov. é um silencioso
parceiro na RSA Data Security)
16.26.4. Um Ataque Indireto: Insistindo que todas as transações econômicas
ser "revelados" ("Full Disclosure Sociedade" cenário)
+ isso soa Orwelliano, mas o óbvio precedente é que
as empresas devem manter registros de todas as transações financeiras.
(e até alguns outros registros, para ver se eles estão conspirando
ou manipular algo)
- para o rendimento e o imposto sobre vendas razões
- e OSHA inspeções, INS de invasões, etc.
+ não existe actualmente nenhum requisito de que todas as transações
ser totalmente documentado com o identica de todas as partes,
exceto em alguns casos como armas de fogo compras, mas este
poderia mudar
- especialmente como transações eletrônicas tornam-se mais
comum: a receita federal pode, algum dia, insistem em tais registros,
talvez até mesmo insistindo em escrowing de tais registros, ou
time-stamping
+ isso vai doer pequenas empresas, devido ao custo de entrada de
e a sobrecarga de tais sistemas, mas as grandes empresas
provavelmente suporte-lo (depois de alguns resmungando)
- um grande negócio, sempre vê a burocracia como um dos seus
vantagens competitivas
+ e indivíduos não foram incomodados pela receita federal em menor
pessoal de operações, de que a web está a apertar:
1099s são muitas vezes necessário (quando exceder alguns pagamentos
quantidade, tais como us $500)
- pequena escala de transações de permuta

+ mas a natureza da autoridade de CERTIFICAÇÃO é que muitas transações podem ser financeira e parece ser outra coisa (como o transferência de músicas ou imagens, ou até mesmo a escrita do letras)
- é por isso que uma cúspide está chegando: divulgação completa é um rota, a proteção da privacidade é outro
+ o governo pode citar os perigos de um "bom rapaz rede" (literalmente) que promulga racistas, sexistas e ableist discriminação através de redes de computadores
- por exemplo, que as novas redes são "sub-representando as pessoas de cor"
- e como pode cotas de ser aplicada em um anônimo sistema?
- propostas na Califórnia (7-92) de que os consultores do arquivo mensal de instruções, tem-se imposto retida, etc.
- uma estratégia para o IRS: exigir que todos os usuários de uma rede ter um "número de IDENTIFICAÇÃO de contribuinte" para todas as transações, de modo que a evasão fiscal pode ser verificado

16.26.5. Tenta desacreditar a reputação baseada em sistemas por engano, a fraude, a falta de pagamento, etc.
- ataques deliberados sobre a reputação de serviços a o governo não quer ver
- não pode ser o governo de operações de sabotagem empresas, para prejudicar os esforços antes de começar
- análogo ao "mail-bombing" anônimo reenvio de e-mails

16.26.6. Licenciamento de desenvolvedores de software podem ser um método utilizado para tente controlar a disseminação de sistemas anónimos e mercados de informação
- por exigência de uma "licença de negócios" ligados a qualquer e todas as blocos de código
+ implementado através de assinaturas digitais, a la de assinatura de código protocolos mencionados por Bob Baldwin como um meio de reduzir alçapões, sabotagem e outras modificações por espiões, hackers, etc.
- propostas para exigir que todos os blocos de código para ser assinado, após o Sililcon Vale do caso em meados dos anos 80, onde espião/sabotador foi a diversas s/w empresas e metido com o código
- "selos" de algum grupo, como "Escritores de Software Laboratórios," formal com as especificações exigidas, o código-fonte fornecido para um guardião confiável, etc.
+ tal licenciamento e inspeção também vai servir para aprisionar os atuais jogadores (Microsoft irá amá-lo) e fazer a competição externa de software mais difícil

- a menos que a concorrência estrangeira é "sancionada" eg,
Microsoft abre um código facilidade na Índia
16.26.7. RICO-como a apreensão de computadores e sistemas de bbs
- picada de operações e configurações
- Steve Jackson Games é exemplo óbvio
- para material ilegal (porno, interações defesa, eletrônica
dinheiro, etc.) fluindo através de seus sistemas
- mesmo quando sysop pode provar que ele não sabia atos ilegais foram
sendo cometido em seu sistema (precedentes são os iates
apreendidas porque uma barata foi encontrado)
+ estas crises podem ocorrer mesmo quando o julgamento é nunca realizada
- por exemplo, a "apreensão administrativa" de automóveis em Portland
a prostituição casos
- e apreensões em penalidades civis, onde o
padrões de prova são muito mais baixos
+ em alguns casos, um simples investigação do FBI é o suficiente para obter
funcionários demitidos, locatários expulso, IRS auditorias iniciadas
+ relatos de que uma mulher em Geórgia, que postou algumas "ULs"
(não consta da lista de números?) foi despedido pela sua empresa, após o
FBI envolveu-se, disse ao seu senhorio, de que sua concessão foi
não sendo estendidos, e assim por diante
- "Nós não caminhão com espias"
- o IRS de auditoria não ser ostensivamente para o assédio, mas
para a "causa provável" (ou qualquer que seja o termo que eles usam) que o imposto
a vacância, a comunicação, mesmo que a lavagem de dinheiro pode
ser envolvido
16.26.8. Ilegalidade da Digital Pseudônimos e Credentialling
+ pode echoe equivocada controvérsia sobre ID de Chamador
- equivocada, porque o livre mercado, a solução é clara: permitir
aqueles que desejam ocultar o seu número-estupro e agressão
os números de suporte, policiais, detetives, ou mesmo apenas
cidadãos solicitar serviços ou o que-fazer
- e que aqueles que se recusam a lidar com esses anônimos
os chamadores também fazê-lo (uma simples o suficiente de programação de
máquinas de atendimento e telefones)
- por exemplo, para evitar que os menores e os criminosos de usar o
sistemas, "nomes verdadeiros" pode ser necessário, com pesadas multas e
confiscos de equipamentos e ativos para ninguém que a falha
para cumprir (ou é pego em picadas e configurações)
+ menores de idade podem ficar separados de partes do ciberespaço por
obrigatório "idade de credenciamento" ("cartão")
- isso poderia ser uma grande ameaça para tais livre e aberta
sistemas com várias abas ao longo menores de registo em

para a Internet e vendo X-rated imagens (porém mal
processado) ou leitura picantes material em alt.sexo
- pode haver algum governo humor insistir que apenas
"nomes verdadeiros" ser utilizado, para facillitate tal verificação da idade
(Fiat-Shamir passaportes, documentos, número da Besta?)
+ o governo poderá argumentar que o digital pseudônimos são
presumivelmente considerada parte de uma conspiração, um
penal empresarial, a evasão fiscal, etc.
- o velho "o que você tem a esconder" teoria
- intimamente relacionada com a questão de saber se a Identificações falsas podem ser
usado mesmo quando não há crimes estão sendo cometidos (que é,
pode Joe Média de representar a si mesmo por que não é sua Verdadeira
Nome?)
- defensores das liberdades civis podem lutar contra esta proibição, argumentando que
Os americanos não são obrigados a apresentar "papéis" para
autoridades, a menos que directamente sob a suspeita de um crime
(nunca mente a vadiagem leis, que têm a vista)
16.26.9. Anônimo sistemas pode ser restringida sob o fundamento de que eles
constituem uma perturbação da ordem pública
- ou que promovem o crime, espionagem, etc.
+ especialmente depois de algumas bem conhecidas abusos
- possivelmente, instigada pelo governo?
- os operadores podem ter para postar títulos que efetivamente a unidade
o negócio deles
16.26.10. As empresas podem ser efetivamente proibido de contratar consultores
ou subcontratados como indivíduos
+ o problema prático: a confusão de imposto e o benefício leis
tornar os indivíduos incapazes de lidar com as montanhas de formas
que tem que ser arquivado
- assim, efetivamente preços indivíduos de fora deste mercado
+ a lei de imposto sobre o lado: lembre que a alteração no estado de
consultores de alguns anos atrás...isso pode ser estendido ainda mais
- uma estratégia para o IRS: exigir que todos os computadores da rede
os usuários tenham um "número de IDENTIFICAÇÃO de contribuinte" para todos os
transações, de modo que a evasão fiscal pode ser verificado
- não é claro como isso difere do ponto acima, mas eu
sentir mais essa pressão vai ser aplicada (após
de todas, a maioria das corporações tendem a ver independentes
contratados como mais negativa do que positiva)
- essa pode ser uma agenda, já que as empresas estabelecidas:
eles vêem consultores e free lancers como ladrões e
velhacos, roubar seus segredos e divulgando a coroa
jóias (para punningly mistura de algumas metáforas)

- e como as redes discutido aqui, facilitar a utilização de
consultores, mais motivos para limitar-los
16.26.11. Não podem ser chamadas para a U. N. o controle do mundo bancário
sistema, na esteira do BCCI e semelhantes escândalos
"para peirce o véu" em mãos
- chamadas para um fim ao sigilo bancário,
- falar sobre negar o acesso ao dinheiro centros de Nova York
(mas será que isso empurre o negócio offshore, em paralelo, para
o mercado de Eurodólares?)
+ motivações e métodos
- lembre-se da UNESCO tentativa de alguns anos volta a credencial
repórteres, ostensivamente para evitar o caos e o "injusto"
relatório...bem, o BCCI e armas nucleares de negócios
revestimento pode revigorar os esforços de
"credentiallers"
+ a URSS e outros países a entrar no mundo da comunidade
pode sentir uma oportunidade para a formação de
"conselhos de administração", esses tipos de bancos e
empresas podem usar a ideia em U. N.
- como uma espécie de Banco Mundial ou o FMI, com ainda mais poder
para intervir e assumir o controle de outros bancos, e com
o Bloco Leste e URSS ter lugares!
16.26.12. "Segurança nacional"
- se a situação se torna grave o suficiente, uma la com um full-blown
crypto anarquia do sistema, pode não o governo tomar a
passo de declarar um tipo de emergência nacional?
- existem disposições: "401 de Emergência" e a FEMA planos
- claro, a URSS tentou intitiate medidas de emergência
e falhou
- lembre-se que um dos principais objetivos da criptografia anarquia é o que os
sistemas descritos aqui vai ser tão amplamente implantado como ser
essenciais ou críticos para a economia global, qualquer tentativa...
para "puxar o plug" também vai matar a economia
16.26.13. Pode autoridades forçar a divulgação de uma chave?
+ sobre o "Sim" do lado:
+ é mesmo, dizem alguns, como forçar a combinação de um cofre
que contenham informações ou bens roubados
- mas alguns dizem-e um tribunal pode ter decidido sobre isso-que
o seguro pode sempre ser cortados e abertos, e assim, a questão é
principalmente simulado
- ao forçá-chave divulgação é compelido testemunho
- e pode-se sempre alegar ter esquecido a chave
- por exemplo, o que acontece quando um suspeito simplesmente amêijoas até?

- mas as autoridades podem rotineiramente demanda de cooperação em
investigações, pode aproveitar os registros, etc.
+ sobre o "Não" lado:
- não pode forçar um suspeito para falar, seja sobre onde ele se escondeu
o saque ou onde sua sequestrar a vítima está escondido
- praticamente falando, alguém sob acusação não pode ser
forçado a revelar banco Suíço contas....isso parece
para ser diretamente análoga a uma chave criptográfica
- assim, a chave para abrir uma conta, parece ser a
mesma coisa
- um memorizado chave não pode ser forçado, diz alguém com FEP
ou CPSR
- no balanço, parece claro que a divulgação do
chaves de criptografia não pode ser forçado (embora a prática
penalidade para a não-divulgação pode ser grave)
- mas este não foi realmente testado, tanto quanto eu sei
- e muitas pessoas dizem que essa cooperação pode ser
exigiu...

16.27. Como Criptografia Anarquia Defende A Luta De Volta
16.27.1. Ignorando as restrições comerciais de criptografia de pacotes
não fazê-los "comercial"
- domínio público
- distribuída gratuitamente
- depois de tudo, os algoritmos básicos são simples e realmente não
merecem a proteção de patentes: o dinheiro não vai ser feita pelo
origens de código, mas sim pelo próprio provedores de
(serviços para a transmissão e armazenamento de pacotes)
16.27.2. Ruído e sinais são muitas vezes indistinguíveis
- como com o LSB sinal de áudio abordagem...a menos que o
governo proíbe gravações ao vivo ou gravações digitais
sistemas de...
16.27.3. Timed-release arquivos (usando criptografia) será utilizado para ocultar
arquivos, para garantir que os governos não podem remover material que eles
não gosto
- mais fácil dizer do que fazer
16.27.4. Abordagens jurídicas deverão também ser tidas em: fundamental
questões constitucionais
- a privacidade, a liberdade de expressão, liberdade de associação,
16.27.5. O Plano Mestre para Lutar contra as Restrições no Criptografia
+ "Gênio saiu da garrafa" estratégia: implementar criptografia amplamente
- entrelaçada com as religiões, jogos, grupos de informantes,
e outros usos que não pode facilmente ser encerrado

- espalhados entre muitas outras atividades
- A atenção da mídia: de mídia para relatório no valor de
criptografia, privacidade, etc.
+ De difusão, confusão, e refusion
- Difundir o uso por dispersão em torno de
- Confundir o problema através de falsas religiões, jogos, outros usos
- Recusar-se a cooperar com o governo
- A liberdade de expressão argumentos: chamar as discussões liberdade de expressão
e forçando o governo a provar que a liberdade de expressão é
na verdade, uma transação econômica
+ ligações com religiões, sociedades, etc.
- reuniões privadas protegida
- sistemas de votação

16.28. Coisas que Podem Esconder a Existência de Criptografia Anarquia
16.28.1. em primeiro lugar, a incrível largura de banda, os bits
deslocamento de todo o mundo de redes...fitas estão sendo trocados,
PCs chamar outros PCs, uma variedade de dados e compressão
formatos, ISDN, a transmissão sem fio, etc.
16.28.2. nos próximos anos, o tráfego de rede irá saltar de um mil
dobra, o que com o digital, fax, telefones celulares e computadores,
ISDN, cabo de fibra óptica, e de maior velocidade de modems
- e estas ligações serão de todos os tipos: local, particular,
corporativa, empresarial, comercial, bootleg (não registrado),
rádio celular, etc.
16.28.3. empresas e pequenos grupos têm suas próprias privadas
LANs) e redes com grande largura de banda, e com pouco
perspectivas de que o governo pode polícia-los-não pode haver
lei que exige que a comunicação interna seja legível pelo
governo!
- e as revelações que o Ultra Black tem sido usado para ler
mensagens e usar a informação será mais uma prova de que
empresas que precisam adotar segurança muito forte
medidas
+ e "parcerias" pode ser espalhados por todo o país, e
mesmo internacionalmente, e tem grande lattitude na definição de
seus próprios canais de comunicação e sistemas de criptografia
- lembre-se que a Cargill caso
- e lembre-se também de que o governo pode reprimir
estes sistemas
16.28.4. AMIX-como serviços, novos serviços, a realidade virtual (para jogos,
entretenimento, ou apenas como um lugar de fazer negócio), etc.
+ muitos usuários criptografar seus links para VR servidores, com um

agente de descriptografia na outra extremidade, de modo que suas atividades (personagens, fantasias, compras, etc.) não pode ser monitoradas e registradas
+ isso vai aumentar ainda mais a largura de banda do criptografados dados e vai complicar ainda mais o trabalho da NSA e agências similares
- tenta forçar "em claro" links serão condenados pela confusão de PC normas, utilitários de compressão, celulares, modems, e afins...não haverá "texto puro", que pode ser obrigatória

16.28.5. steganography

+ em geral, impossível saber se uma mensagem contém outros encypted mensagens
- exceto na picadas e configurações, o que pode ser considerado ilegal,
+ LSB método, e variantes
+ LSB de DAT, DCC, MD, etc., ou até mesmo sound bites (pedaços de samples de sons negociados em quadros de avisos)
- especialmente ao vivo ou analógico-apelidado de cópias (o ruído andar de um típico consumidor da classe mike é muito maior que o LSB de DAT)
+ de imagens, o Adobe Photoshop, imagens, obras de arte, etc.
+ imaginar uma "Galeria de Arte Online" que é usado para armazenar mensagens, ou uma "Galeria de Fotos" que os participantes do post suas melhores fotos, a oferta para venda
- Sturges caso
- LSB método
+ recebe em alguns teóricos picuinhas sobre o verdadeiro natureza do ruído, especialmente se a toda a LSB canal característica do "real ruído"
- mas reduzindo a largura de banda de certa forma, o ruído perfil pode ser feito essencialmente imita real ruído
- e um de 2 GB DAT produz 130 MB de LSB, o que é muito de margem!
+ o que poderia o governo fazer?
- picadas e configurações de captura e afugentar potenciais usuários
- uma tentativa de limitar a ampla utilização de digital dados-impossível!
+ um requisito para aprovadas pelo governo, "composição"?
- isso seria um pesadelo de execução
+ e só iria fazer com que o sistema seja movida para superior bits

- e com bastante correção de erro, mesmo audível
composição de cores do sinal não iria acabar com o
criptografados sinal
+ variantes: justificação de texto, seleção de palavra
- largura de banda tende a ser baixa
mas em Três Dias do Condor
+ de realidade virtual de arte pode permitir privado
comunicações
- pense no que pode ser criptografada em tais imagens digitais!
- e o usuário tem total privacidade e é capaz de manipular a
imagens e bancos de dados localmente
16.28.6. no sentido de que estas outras coisas, tais como os governos
redes próprias de casas seguras, falsas identidades, e bootleg
pagamentos de salários, tendem a ocultar qualquer outro tipo de sistemas que emergem
+ porque os investigadores podem pensar que já tropeçou ainda
outra operação de inteligência, ou aguilhão, ou o que quer que
- isso rotineiramente aleijados investigações sigilosas
- cenário: os criminosos ainda flutuar rumores de que outra agência
está a fazer uma operação....?
16.28.7. Governo de Operações que se Assemelham Cryptoanarchy vai
Confundir os Problemas
- diversas confidenciais redes que já existem, operado por
Estado, departamento de defesa, o de serviços, etc.
+ Programa de Proteção a testemunhas (ou Testemunha de Realocação de Programa)
- Identificações falsas, documentos, transcrições
- mesmo que o dinheiro dado a eles (e os valores parecem ser
minimizou na imprensa e em t.v., com uma súbita onda
da mostra sobre o quão mal eles fazem no meio do meio
América-soa como uma plantadas história para mim)
- cooperação com empresas e escolas para ajudar
neste aspecto
+ Pagamentos de salários dos informantes, agentes não-oficiais
- como agentes de lugar dentro de empreiteiras
- grande quantidade de dicas de autônomos, cidadãos estrangeiros,
etc.
- operadores de casas seguras (como a Sra Furbershaw)
+ Redes da CIA-financiado bancos, para diversos fins
- a la Nugan-Mão de Banco BCCI, etc.
- Primeiro-Americana, do Banco de Atlanta, Centrust de Poupança, etc.
- esses bancos e S&Ls atuam como condutores para controverso ou
operações secretas, para estacionamento temporário de fundos, para
a banca de lucros, e até mesmo para o privado
fundos de aposentadoria de agentes (um piscou-na prática)

+ Confidenciais redes através de linhas de computador
- por exemplo, criptografados teleconferência de Bacanas, PFIAB, etc.
+ estes irão aumentar, por muitas razões
- preocupações sobre o terrorismo
- exigências de tempo limite de viagens (especialmente para
grupos de não-tempo integral membros da comissão)
- esses suspeitas de operações do governo vai impedir
investigação
16.28.8. Tráfego Criptografado Irá Aumentar Dramaticamente A
- de todos os tipos
- mails, imagens, propostas, aparelhos de fax, etc.
- a aceitação de um P-K sistema de correio irá fazer amplo uso de
criptografia quase automático (embora alguns fração, talvez,
a maioria, não se incomodam mesmo)
+ pode até haver razões legais para a encriptação para aumentar:
- requisitos de registros de empregados de ser protegidas, que
registros médicos de ser protegidas, etc.
- "homem prudente" regras sobre o roubo de informações (poderia
significa que os arquivos são encriptados, exceto quando
trabalhou em)
- assinaturas digitais
- ecos do COMSEC vs. SIGINT (ou PROD) debate, onde
COMSEC quer ver mais de criptografia (para proteger-Americana
a indústria contra os Soviéticos e comercial de espionagem)
+ Venda de "Anónimo-Mails"?
- usando RSA
+ evitar a RSA e a P-K patente pântano
- pode vender pacotes de one-time pads
+ sem a efetiva garantia de segurança, mas adequada para
muitos fins simples
+ especialmente se os compradores trocá-los com outros
- mas como garantir que não são mantidas cópias?
- a idéia é permitir que uma espécie de "Democracia de Parede"
+ pré-pago "moedas" comprou anonimamente
- como com o Japonês cartões de telefone
- ou as várias pedágio eletrônico tokens a ser
desenvolvido
16.28.9. Jogos, de Religiões, de Consulta Jurídica e de Outras "Cobre" para
a Introdução e Proliferação de Criptografia Anarquia
- não ser claro o que é real criptografia e o que é jogo
jogar
- imagine um jogo chamado "Cryptoanarchy"!
+ Comentário sobre estes "Cobre"

- alguns desses vai ser bastante legítimo, outros serão
deliberadamente configurar como capas para a propagação da autoridade de CERTIFICAÇÃO
métodos
- talvez subsidiados apenas para aumentar o tráfego (e
tráfego criptografado já é esperado um aumento para um
variedade de razões)
- as pessoas têm diferentes razões para querer anonimato
+ Jogos
+ "Habitat"estilo de jogos e sistemas
- com "pegas" que são muito mais seguros do que em
presente (lembre-se do Chip comentários)
+ comportamentos que estão estreitamente semelhante ao do mundo real ilegal
comportamentos:
- uma área de ladrões
- um jogo de espionagem
- uma "democracia de parede", em que tudo pode ser postado
anonimamente, e lida por todos os
+ MUDs (Multi-user Domains, Multi-User Dungeons)
- lotes de interesse aqui
- tópico de discussão em um especial Cypherpunks reunião,
início de 1994.
+ interativo role-playing games irá fornecer cobertura para o
expansão dos sistemas: pseudônimos vai ter muito mais
a proteção que eles têm agora
- apesar de vários métodos podem existir para "marcar" uma transação
(a la de bário), especialmente quando grandes quantidades de largura de banda
envolvidos, para análise (por exemplo, "Dark Dante" é
identificados pela anexação de bits específicos para a sequência)
+ De lidar com Bário Traçadores
- código tem permissão para ferver em uma máquina para fora do local
algum tempo (e com o girar do relógio do sistema)
- mutações adicionados
+ Mundos Partilhados
- autores, artistas, jogo-os jogadores, etc. pode adicionar estes
mundos
- ligações de hipertexto, baseado na reputação de sistemas
+ a hipótese de um "Nomes Verdadeiros" jogo em redes, com base
explicitly no Vinge do trabalho
- talvez a partir de uma roupa como Steve Jackson Games, criador de
similar jogos de rpg
- variável-resolução gráfica (a la Habitat)
- realidade virtual capacidades
+ um jogo como o "Habitat" pode ser usado como um Labirinto virtual,

além disso, para confundir a linha entre a realidade e a fantasia
- e isso pode fornecer uma grande quantidade de largura de banda para cobrir
- o Smalltalk "Cryptoids" a idéia é relacionado a isso...ele
parece uma simulação ou um jogo, mas pode ser usado por
"outsiders"
+ Religiões
+ um quase ironclad sistema de liberdades, que _some_
existem limites de
- por exemplo, uma igreja que usa a sua organização para o transporte de
drogas ou executar uma operação de apostas seria encerrado
rapidamente (lembre-se que a droga igreja?)
- e chamadas para imposto de quebra de limitações (que projeto de lei de
Direitos não diz nada sobre)
- ainda assim, será _very_ difícil para os EUA.
governo interferir com as comunicações de um
"religião".
+ "ConfessionNet"
+ um hipotético anônimo sistema que permite confissões
para ser ouvida, com todos os privilégios de privacidade
normal confissões ter
- sucessores de 900 números?
+ praticamente ironclad proteções contra governo
interferência
- "O congresso não fará nenhuma lei..."
+ mas os governos podem tentar restringir quem pode fazer isso, uma
la as restrições nos anos 70 e 80 em "instant
Reverendos"
- Kirby J. Hensley da Univeral Vida da Igreja
- diversas IRS restrições, estabelecer de forma eficiente
duas classes de religiões: aqueles de anterioridade e
dado isenções fiscais e semelhantes, e aqueles que foram
considerado inválido, de alguma forma,
+ Cenário: Um Scientology-como o culto usando a autoridade de CERTIFICAÇÃO como o seu
chefe
sistema de comunicações?
- níveis de iniciação mesma como um sistema de célula de
- "compensação"
- Nova era lixo: Mestres Ascensionados, células, o dinheiro flui
e para trás
- blackballing
+ Digital Namoro
- o "namoro" seção de jornais, atualmente, requer
o jornal, para fornecer o anonimato (até que as partes

acordar para atender)
- o que sobre AMIX ou serviços similares?
- um sistema totalmente digital pode permitir a auto-organização de sistemas de
+ veja como funciona:
- Alice quer conhecer um homem. Ela escreve de um típico anúncio
"SWF procura SWM por diversão e passeios na praia..."
- Alice coloca-la especialmente selecionada de chave pública, que
é efetivamente o seu único nome. Este é, provavelmente, um
horário de lidar, unlinkable para ela de qualquer maneira.
- Ela criptografa todo o pacote e o envia através de um
remailing cadeia (ou DC-Net) para eventual lançamento no
lugar público.
- Todos podem fazer o download a área relevante (as mensagens podem
ser classificado por tipo, ou organizados em grupos de interesse),
com ninguém mais saber quais as mensagens que eles estão
leitura.
- Bob lê a sua mensagem e decide repond. Ele
digitaliza uma foto de si mesmo e inclui alguns outros
informações, mas não é seu nome real. Ele também pega uma chave pública
para Alice para se comunicar com ele.
- Bob criptografa tudo isso com a chave pública de Alice
(mas lembre-se de que ele não tem nenhuma maneira de saber o que ela
realmente é).
- Bob envia esta mensagem através de um remailing cadeia
fica lançada como uma mensagem criptografada dirigida ao
chave pública de Alice. Novamente, alguns organização pode
reduzir a largura de banda total (por exemplo, uma área para
"Respostas").
- Alice verifica as respostas e downloads de um grupo de
mensagens que inclui o que ela pode ver-e só ela
pode ver!-é endereçada a ela.
- Este tenha estabelecido uma comunicação de duas-vias caminho
entre Alice e Bob, sem nenhum deles saber
que o outro é ou onde eles vivem. (O negócio
sobre as fotos é claro que não contribuem para a
o anonimato, mas é consistente com o "Namoro"
modo).
- Se Alice e Bob deseja conhecer a pessoa que ele é, então, fácil
para que eles possam comunicar real, números de telefone e o
gosta.
+ Por que isso é interessante?
- estabelece um papel para sistemas anónimos
- poderia aumentar a largura de banda de tais mensagens

+ De Serviços jurídicos (Legítimos, isto é, nem mesmo o bootleg
coisas)
+ protegidos pelo advogado-cliente privilégios, mas vários Barra
Associações podem colocar limites sobre o uso de redes
- mas se visto a forma como telefones, parece improvável que
As barras podem fazer muito para limitar o uso de computador
redes
- e suponha que um Nolo de Imprensa-publicação do tipo de empreendimento começou
até nas Redes? (publicação de auto-ajuda info em
pseudônimos)
- ou o golpe para evitar o pagamento de impostos por incorporar como uma
empresa ou organização sem fins lucrativos?
+ Sistemas De Votação
- com e sem anonimato
+ Conselho de Administração-tipo de votação
- com credenciais, senhas, e (talvez) o anonimato
(sob certas condições)
+ Blackballing e Associações
- geralmente anônimo
- blackballing pode ser ilegal estes dias (de preocupações sobre a
racismo, sexismo, etc.)
- cf. Salomaa para a discussão da indistinguibilidade de
blackballing de votação por maioria
+ Consumidor Classificações e Avaliações
- por exemplo, não pode ser "garantido anônimo" avaliação
sistemas de software e outros de alta tecnologia itens (Joe
Bluecollar não vai mexer com computadores e complicado
sistemas de votação)
+ Politicamente Ativo Grupos Podem Ter Votação Anônima
- para votar no grupo de políticas, procedimentos, liderança
- ou sobre o boicote lista (lembre-se a idéia do PC-Card
que não permite politicamente incorreto compras)
+ isso pode ser para se proteger de ações judiciais (SLAPP)
e hostilidades do governo
- elas têm medo do governo infiltrados irá obter os nomes
de eleitores e como eles votaram
+ Oficial Para As Eleições
- embora isso seja improvável que o mal-alfabetizados
maioria
- os inevitáveis casos de fraude terá ampla exposição e
assustar as pessoas e os políticos até mais
- pouco provável na próxima década
+ Diário De Arbitragem

- alguns jornais, como o Diário da Criptologia,
apropriadamente, já estão usando em papel
versões deste
+ Xanadu-como os sistemas podem ser early adopters
- há, naturalmente, razões para o oposto:
avançado usado de reputações
- mas, em alguns casos, o anonimato pode ser preferido
+ De Groupware
- comentário anônimo (sistemas de imagem digital blackboard
anônimo observações, mostrando-se)
- esses sistemas são promovidos para incentivar a calma e ter
uma voz igual
- mas eles também fornecem um outro caminho para anônimos e/ou
reputação baseada em sistemas de
+ Psicológico Consultas
- vai exigir o licenciamento de conselheiros, de curso de
(sob as leis dos estados unidos)
- o que acontece se as pessoas chamam de ventos conselheiros?
+ e várias limitações sobre a privacidade dos registros de existir
- Tarisoff ortografia [?]
- intimações
- manter registros necessários
+ pode ser usado por vários "politicamente correto" grupos de
- as mulheres vítimas de violência
- as crianças vítimas de abuso
- talvez em conjunto com a RU-486-tipo de problemas,
um terreno comum pode ser estabelecido (um novo tipo de
Underground Railroad)
+ Assessoria em Medicina (la AIDS, RU 486)
- o anonimato necessário para proteger contra ações judiciais e apreensão
- AGORA e outros grupos feministas poderia usar criptografia anarquia
métodos para reduzir os riscos para as organizações
+ Anonymous Dica De Linhas, Serviços De Comunicação De Irregularidades
+ por exemplo, um jornal pode configurar um sistema de recompensa,
usando a criptografia equivalente do "papel rasgado" chave
- onde o informante tem para a rasgada "chave"
- mesmo algo como o James Randi/Yuri Geller caso
revela que "anônimo críticos" podem se tornar mais comuns
+ corporativa e contratante de defesa dos denunciantes poderão buscar
proteção através de métodos de criptografia
- uma "Garganta Profunda", que usa placas de boletim para comunicar
com o DS?
+ isso supõe muito mais ampla utilização de computadores e modems

"média" de pessoas...e eu duvido "Prodígio"-tipo de sistemas de
irá dar suporte a essas atividades!
- mas não pode ser barato, sistemas baseados em vídeo do jogo
máquinas, uma la a proposta de Nintendo computadores
ambientalistas configurar estes denunciante linhas, para
pessoas para denunciar extração ilegal de madeira, pulverização, etc.
+ On-Line, "Instantâneo" Sociedades
+ de empresas de fachada, devidamente constituída em Delaware ou
onde quer (talvez até mesmo sites estrangeiros) são "vendidos" para
os participantes que pretendam criar uma empresa para cobrir
suas atividades
- para que AMIX-como as taxas são parte do "interno
de contabilidade"
+ Anonymous escrita colaborativa e crítica
- semelhante a votação anônima
16.28.10. Comprimido de tráfego, da mesma forma aumentar
- e muitos de compressão algortithms vai oferecer alguma forma de
criptografia como um brinde
- e vai ser difícil de decifrar, com base apenas na pura
volume
- arquivos terão, pelo menos, ser descompactado antes de palavra-chave
as pesquisas podem ser feitas (apesar de que pode haver atalhos)

16.29. A Vinda De Mudança De Fase
16.29.1. "É melhor esperança de que a forte cypto, barato telecomunicações e livre
os mercados podem proporcionar a organização de base para um funcional
a sociedade, pois é claro que a coerção como uma organização de
princípio já não é o que costumava ser." [Duncan Frissell, em
sua sig, 4-13-94]
16.29.2. "O que é a "inevitabilidade" argumento?"
- Muitas vezes feita por mim (Tim de Maio), Duncan Frissell, de Areia
Sandfort, e Perry Metzger (com algumas reviravoltas). E Hal
Finney assume problema com certos aspectos e contribui
críticas incisivas.
+ Motivos:
- fronteiras, tornando-se mais transparente para o fluxo de dados
- a criptografia não é detectável/pode ser interrompida
- instrumentos financeiros derivativos, dinheiro deslocamento em
fronteiras
- transnacionalismo
- máquinas de dinheiro, transferência bancária
- permanente "turistas"
- Fronteiras estão se tornando totalmente transparente para grandes volumes de dados

fluxos. O rápido exportação de criptografia, mas é um exemplo irônico
desta. Mosaid, ftp, gopher, lince...todos atravessam fronteiras
de uma forma fluida e quase untraceably. Ele é, provavelmente, muito tarde para
parar estes sistemas, curto de "puxar a ficha de rede" na Net,
e esta puxando o plugue é simplesmente demasiado caro para
considerar. (Se a Polícia realmente descobrir a longo
gama de implicações dessas coisas, eles podem tentar mas...
provavelmente não.)

16.29.3. "O que é a "criptografia de mudança de fase"?"

- Normalmente sou cético em relação a alegações de que uma "singularidade" é
vinda (nanotecnologia sendo o lugar de costume, este é
alegou, la Vinge), mas "fase alterações" são mais
plausível. O efeito de baixo impressão foi uma fase
a mudança, alterando a conectividade da sociedade e do
a dispersão do conhecimento em uma forma que pode ser melhor descrito
como uma mudança de fase. Os efeitos do forte de criptografia, e o
relacionados com as ideias de dinheiro digital, anônimo, mercados, etc. são
provavelmente semelhante.
- transição
- tombamento de fatores, o nojo pelo povo, a fuga de tributação
+ "efeito de leverage"
- o que Kelly chamado de "o fax efeito"
- crypto usar se espalha, feito mais popular pelo uso comum
- pode nucleate em um pequeno grupo...não precisa de massa
aceitação

16.29.4. "Pode criptografia anarquia ser interrompido?"

+ Um objetivo é obter de criptografia amplamente suficiente implantado que
não pode ser interrompido
- para o ponto de não retorno, onde o custo de retirada
ou a proibição de uma tecnologia é simplesmente demasiado alta (não sempre uma
guaranteee)
- O único recurso é um estado policial, no qual casas e
as empresas estão aleatoriamente entrou e procurou, em que
criptografia é ilegal e vigorosamente processados, em
que escutas, vigilância por vídeo e outras formas de
vigilância são utilizados de forma agressiva, e, talvez,
a muito a posse de computadores e modems é restrito.
- Nada menos do que esses policiais do estado tática permitirá o
o desenvolvimento das idéias aqui discutidas. Até certo ponto.
Mas o suficiente para desencadear o processo de transição para uma maioria de criptografia
anárquico situação.
- Isso não significa que todos, ou mesmo a maioria, usará criptografia
anarquia.)

16.29.5. Não precisa ser um universal ou mesmo tendência popular
- mesmo se restrito a uma minoria, podem ser muito influentes
- George Soros, o Quantum fund, os bancos centrais, Espanha, grã-Bretanha, Alemanha
- e uma minoria tendência pode afetar outros
16.29.6. "As fronteiras nacionais estão apenas speedbumps digital auto-estrada."
16.29.7. "Não crypto anarquia tem que ser um movimento de massa para o sucesso?"
- Dado que apenas uma pequena fração agora está ciente de que o implicações....
+ Precedentes para a "vanguarda" movimentos
+ alta finança, em geral, é uma coisa de elite
- Eurodollars, swaps de taxa de juro, etc....não exatamente
Joe Média...e ainda de extrema importância (George
Soros tem afetado banco central Europeu (política)
- contrabando é, em geral, uma massa de coisa
- etc.
+ Assim, os usuários de criptografia anárquico, ferramentas e instrumentos
pode ter um efeito fora de proporção para os seus números
- os outros vão começar a usar
- ressentimento por o "otários" vai construir
- os serviços próprios-os dados paraísos crédito
registros, a espionagem mercados--naturalmente terá um
efeito real
16.29.8. Forte de criptografia não significa o fim de aplicação da lei
- "...de criptografia não é de forma alguma um escudo mágico para
os criminosos. Ele elimina, talvez, um caminho pelo qual
os crimes podem ser descobertas. No entanto, é certamente
não é o caso de que alguém que coloca um abrir anônimo
contrato por um assassinato em um fórum aberto, é fazê-lo "risco
livre". Há *abundância* formas ela pode ser encontrada fora.
Da mesma forma, grandes sociedades secretas que nefariously minar
o mundo livre através de criptografia são tão vulnerável como nunca
as motivações de seus próprios membros para expor a
grupos em um double-cross." [Mike McNally, 1994-09-09]

16h30. Pontas Soltas
16.30.1. os governos podem tentar proibir o uso de criptografia em qualquer
sistema de transmissão, não importa o quão baixo o poder, por causa de um
perceber que todas elas podem ser usadas para criptografia anarquia
e espionagem
- é uma batalha perdida, é claro, que com a LANs sem fios de
vários sabores, celulares, modems, a capacidade de ocultar

informações, e apenas o enorme aumento na largura de banda
16.30.2. "tontines"
- Eric Hughes escreveu algumas coisas sobre isso em 1992 [tentar obter ele]
- Italiano pseudo-acordos de seguros
- "digital tontines"?
16.30.3. Mesmo no mercado anarchies, há momentos em que de cima para baixo, imposto conjunto de comportamentos desejáveis. No entanto, em vez de sendo imposta pela ameaça de violência, o próprio mercado impõe um padrão.
- Por exemplo, o sistema operativo Macintosh, com comandos padronizados que os desenvolvedores de programa são "incentivados" a usar. Desvios obviamente são permitidos, mas o mercado tende a punir tais desvios. (Isto tem sido útil para evitar modal de software, onde a mesma seqüência de teclas pode salvar uma arquivo em um programa e eliminá-lo no outro. Infelizmente, o a complexidade de software moderna ultrapassou o Mac OS sistema de Comando-Opção Y, muitas vezes, diferentes coisas em diferentes programas.)
- Padrões de mercado são uma noncoercive contra o caos total.
16.30.4. Claro, nada impede que pessoas de contratação financeiro consultores, advogados, e até mesmo "Protetores" para protegê-las do o predations dos outros. As viúvas e os órfãos poderia escolher conservadores, conservadores, enquanto os jovens turcos poderia escolher ir sozinho.
16.30.5. quem pode tolerar criptografia anarquia
- Não é muito diferente da forma como as coisas foram, no passado. Contrapartidas. Olhe para o Número Um. Cuidado com óleo de cobra.
16.30.6. Local de aplicação de regras, em vez de regras globais
+ por exemplo, a inundação de Usenet com publicidade e cartas em cadeia
+ duas abordagens principais
- proibição de tais coisas, ou conjunto de quotas, global de uso aceitável políticas, etc. (ou usar o direito penal para processar e pegar danos)
- local carrriers decidir o que vai e não vai levar, e quanto eles vão cobrar
- é o antigo racionamento vs. preço de mercado argumento
16.30.7. A localidade é um conceito poderoso
- auto-responsabilidade
- quem melhor para tomar decisões do que aqueles afetados?
- maior feedback loops
- evita em grande escala governos

+ Nonlocally-sistemas organizados, muitas vezes, resultam em chamadas para parar
"devoradores" de recursos, e o general rancor e inveja
+ consumo de água é o melhor exemplo: alguém já viu
"desperdiçar" de água, independentemente de suas conservações
em outro lugar ou há prioridades, é castigado e repreendido.
Às vezes, a água polícia é chamada.
- os custos envolvidos (talvez alguns tostões a pena de
de água, para lavar um carro ou água de rosas) são, muitas vezes,
trivial...enquanto isso, bilhões de acre-pés de água
vendido muito abaixo do custo para os agricultores que cultivam culturas de monção
como o arroz no deserto da Califórnia
- esta hipocrisia é alto na minha lista de razões por que é grátis
os mercados são moralmente preferível ao racionamento de base
sistemas

17. O Futuro

17.1. direitos autorais
O CYPHERNOMICON: Cypherpunks FAQ e Mais, Versão 0.666,
1994-09-10, Direitos De Autor Timothy C. De Maio. Todos os direitos reservados.
Veja os detalhes de isenção de responsabilidade. Use seções curtas em "justo
use" disposições, com crédito apropriado, mas não coloque o seu
nome em minhas palavras.

17.2. RESUMO: O Futuro
17.2.1. Pontos Principais
- onde as coisas estão indo provavelmente
17.2.2. Ligações para Outras Secções
17.2.3. Onde Encontrar Informações Adicionais
17.2.4. Diversos Comentários

17.3. Progresso Necessário
17.3.1. "Por ter a maioria das coisas Cypherpunks falar sobre *não* * *
aconteceu?"
+ Exceto para remetentes e básicos de criptografia, alguns dos principais
ideias falado por tanto tempo ter visto qualquer tipo
de realização. Há muitas razões:
R. Difícil de alcançar. Tanto Karl Kleinpaste e Eric
Hughes simples implementadas a primeira geração de remetentes em uma
questão de _days_, mas "dinheiro digital" e "aptical
foddering", por exemplo, não são tão
simples e direto. (Estou, é claro, não tirar nada
a partir de Kleinpaste, Hughes, Helsingius, Finney, etc., apenas

observando que redirecionando mensagens de correio-e até mesmo
a implementação de PGP e coisas como atraso, dosagem, etc.,
em remetentes--é muito mais fácil conceitualmente do que DC-Redes
e o como.
B. Protocolos são confusos, difíceis de implementar. Apenas uma pequena
fração do "crypto primitivos" discutido na Criptografia
Conferências, ou em vários criptografia livros, foram
percebi como runnable código. Blocos de construção como "pouco
compromisso" não têm mesmo--do meu conhecimento--sido
adequadamente compreendido como código reutilizável. (Com certeza vários
grupos, tais como Chaum, tem de paralelepípedos-coisas
como o pouco empenho....Eu só não acho que há um
o consenso quanto à forma, e isso tem limitado o
capacidade de nonspecialists para usar esses "objetos".)
C. confusão Semântica bem. Embora seja bastante claro o que
"criptografar" ou "remailing" significa, apenas que é um
digital "banco"? Ou uma "reputação do servidor"?
D. Interoperablity é problemático. Muitas plataformas, muitas
sistemas operacionais, muitos idiomas. Novamente, remetentes e
criptografia de trabalho, porque há de facto comum mais baixo
denominador para eles: o simples bloco de texto, usado em e-
mail, editores, entrada e saída de programas, etc. Que
é, todos nós, principalmente, saber exatamente o que um bloco de texto ASCII
é, e programas de criptografia são esperados para saber como
acessar e manipular tais blocos. Isto explica em parte
o sucesso do PGP em várias plataformas--blocos de texto são
o elemento básico. Idem para Cypherpunks remialers, que
operar nos blocos de texto encontrado na maioria dos sistemas de email.
A situação torna-se muito mais sombria para coisas como
dinheiro digital, que não são autônomos de objetos e são
muitas vezes multi-festa de protocolos envolvendo atrasos de tempo,
processamento off-line, etc.
E. Falta de um económica motivo. Temos nesta lista não estão sendo
paga para o desenvolvimento de qualquer coisa, não são assistidos por qualquer pessoa, e
não tem o apoio financeiro de empresas para
nos ajudar. Uma vez que hoje "desenvolvimento de software"
é, na verdade, _deal-making_ e _standards negotiation_, nós
são deixados de fora de muitas coisas.

17.4. Direções Futuras
17.4.1. "Quais são algumas direções futuras?"
17.4.2. O Futuro da Lista
+ "O que pode ser feito sobre essas situações?"

- Que é, dado que os Cypherpunks lista, muitas vezes, contém o material sensível (ver acima), e dado que o atual lista de membros pode ser acessado por..... o que pode ser feito?
- Mover servidor central para a não-localidade dos EUA
- Ou "ciberespaço" (rede distribuída, com nenhuma central servidor...como FidoNet)
- assinantes podem usar pseudônimos, recortes, remetentes

17.4.3. O que se encriptação é ilegal?

- pode uuencode (e semelhantes), para, pelo menos, abrandar o filtro de programas um pouco (isso é mal de segurança através de obscuridade, mas....)
- metro movimentos?
- vai Cypherpunks ser arredondado?

17.4.4. "Deve Cypherpunks ser mais organizado, mais como o CPSR, FEP, e ÉPICO?"

- Esses grupos em grande parte, são grupos de lobby, com uma equipe de funcionários em Washington apoiado pela associação de doações de milhares ou dezenas de milhares de sócios representativos. Eles executar um serviço valioso, claro.
- Mas esse não é o nosso modelo, nem podem plausivelmente ser. Estávamos formado como um grupo ad hoc para explorar crypto, foram apelidados de "Cypherpunks", e desde então atuou como um techno-grasssroots a anarquia. Sem funcionários, sem dívidas, sem eleições, sem regras oficiais e regulamentos, e não de liderança, além do que é fornecido pelo poder do discurso (e uma pequena quantidade de "palavra final" fornecida pela lista mantenedor Eric Hughes e a máquina proprietário, John Gilmore, com o apoio de Hugo Daniel).
- Se a gente quer um grupo de pressão, com advogados em Washington, eles devem se juntar a FEP e/ou CPSR.
- E nós preencher um nicho que não tentar preencher.

17.4.5. Difícil Definir Direções

- a anarquia...nenhum controle centralizado
- emergente interesses
- todo mundo tem alguma machado para moer, algumas conjunto temporário de prioridades
- pouca motivação econômica (e a maioria tem outros trabalhos)

17.4.6. O Coração e a Alma de Cypherpunks?

+ Objetivos Concorrentes:
+ De Privacidade Pessoal
- PGP, integração com e-mails
- educação
+ Redução do Poder de Instituições

- whistelblowers grupo
-
- Crypto Anarquia
+ Propósitos Comuns
+ Espalhando forte de criptografia e ferramentas de conhecimento
- PGP
+ De luta governo restrições e regulamentos
- Clipper/Skipjack luta foi um unificador experiência
+ De explorar novas direções na criptologia
- digital misturas, dinheiro digital, a votação

17.4.7. Direções Possíveis

+ De criptografia, Ferramentas...torná-los onipresente "suficiente" para que o gênio não pode ser colocado de volta na garrafa
- pode se preocupar com a política, mais tarde (socialistas vs. anarchocapitalists, etc.) (Embora socialistas faria bem para pensar cuidadosamente sobre as implicações de untraceable comunicações, dinheiro digital, e em todo o mundo redes de consultores e trabalhadores-e o que isso faz para a coleta de impostos e a despesa social programas--antes de eles trabalham com os libertários e anarchocapitalists para traga a Criptografia Millenium.)
+ Educação
- educar as massas sobre criptografia
- fóruns públicos
- este foi escolhido pelo Cambridge/MIT grupo como sua de interesse especial
+ Lobby
- conversando com assessores do Congresso e comissão de funcionários, participando de audiências, para apresentação de resumos na proposta legislação
- coordenar com o FEP, CPSR, ACLU, etc.
- este foi escolhido pelo grupo de Washington como seus especiais o interesse, que é, forçosamente, adequado (Califórnia. grupo é simplesmente muito longe)
- Desafios Legais
+ mistura do legal e ilegal
- use ferramentas legais e ilegais ferramentas
- reversão de posições
- inscrever-se ilegais os usuários como clientes...ajuda espalhou-se em estes canais (mostrado para ser quase incontrolável)

17.4.8. Objetivos (como eu vê-los)

+ Obter o forte de criptografia implantado na forma a ser imparável, unrecallable

- "disparar e esquecer" crypto
- gênio fora da garrafa
- Em atenção que essa situação _not_ necessariamente que ser crypto
widely implantado, no entanto, que é geralmente uma boa idéia.
Isso pode significar a propagação chave de sites de fora dos EUA com
forte de criptografia de ferramentas, com remetentes, e com os outros
acouterments.
+ Monkeywrench ameaças à liberdade de criptografia.
- sabotagem económica de quem use estatizante contratos para
impedir a liberdade (por exemplo, partes da AT&T)
+ direto sabotagem
- um dia, vírus, HERF, etc.
17.4.9. Uma Visão do Futuro
- encriptada, seguro, untraceable de comunicações
- centenas de remetentes, em muitos países
- entrelaçada com tráfego normal, assegurando que qualquer tentativa de
para revogar, crypto também teria um efeito dramático em
negócios
- dados paraísos, de crédito, inquilinos, etc.
- informação de mercados
- capacidade para guerras é dificultado
- EUA é frenético, como o seu controle sobre o mundo solta...Pax
Americana morre
17.4.10. Conceitos-chave são a maneira de lidar com a complexidade da criptografia
- O pântano de protocolos, sistemas e resultados é melhor
analisados, eu acho que, por não perder de vista o básico
"primitivas", as coisas sobre a identidade, a segurança,a
autenticação, etc. que fazer de criptografia, sistemas de trabalho, a forma
eles fazem.
+ Axioma de sistemas, com teoremas e entradas que podem ser retirados a partir do
axiomas
- com alternativa axiomas dando o equivalente a "não-
Euclidiana e geometrias" (em um sentido, a remoção física
identidade postulado, e substituí-lo com o "a chave é
a identidade de" postulado dá um novo cenário de
medicamentosas, implicações e estruturas).
- (Mercados, referências locais, voluntários de transações, etc.)
- (ecologias, predadores, defensores, etc.)
- (teoria dos jogos, economia, etc..)

17.5. Líquido do Futuro
17.5.1. "Que papel, se houver, serão MUDs, MOOs e Realidades Virtuais
jogar?"

- "Nomes Verdadeiros," "Snow Crash", "Shockwave Rider"
- Habitat, serviços on-line
+ a interação é muito além de apenas canônico "texto
mensagens" que, como sistemas de Telefonia Digital são projetados
para lidar com
- onde está o nexo da mensagem?
- o que sobre conferências espalhados por todo o mundo, em
várias jurisdições?
- crypto = cola, argamassa, blocos de construção
- "quartos" = privadas locais; problemas de controle de acesso
- A menos que os policiais são colocados para esses vários "quartos", através de uma
a tecnologia, nós mal podemos imaginar hoje (agentes?), ele vai
ser essencialmente impossível controlar o que acontece nesses
quartos e lugares. Muitos graus de liberdade, muitas
caminhos para o exchange.
- cyberspaces, Lamas, comunidades virtuais, de direito privado,
intocável pelo físico governos
17.5.2. baseadas em palavras-chave
- pode ser falsificada, incluindo dicionários
17.5.3. cavar sig de base (baseado na reputação)
17.5.4. piscinas e anônimo áreas podem ser explicitamente suportada
17.5.5. melhores leitores de notícias, telas, filtros de
17.5.6. Opções
- "mudar de tecidos"
- ATM
- Intel flexível de malha de interconexões, iWARP, etc.
tudo isso vai fazer para um aumento exponencial no
graus de liberdade para o reenvio de e-mails redes (labirintos). No
chip remailing é esentially o que é necessário para Chaum do
misturas. ATM quanta (pacotes) são a próxima meta para
remetentes.
17.5.7. "Quais os limites na Net estão sendo propostos?"
- NII
+ Realização de transportadores responsáveis pelos conteúdos
- por exemplo, processando Compuserve ou Netcom
- muitas vezes feito com placas de boletim
- "Temos que fazer algo!"
+ Jornais estão reclamando sobre os Quatro Cavaleiros do
Infocalypse:
- os terroristas, pedófilos, traficantes de drogas e dinheiro
os lavadores de
+ "L. A. Times", opina:
- "Os Designers da nova era da Informação foram inspirados por

nobres sonhos de livre fluxo de dados global
libertadora força, uma verdadeira democratização do agente. Infelizmente,
os bandidos e arrasta-se também subiu a bordo. O
chegou a hora para muito mais rigorosas de segurança do computador.
Afinal, os bancos aprenderam a colocar bloqueios em seus cofres."
["L. A. Vezes," editorial, 1994-07-13]

17.6. Os Efeitos do Forte de Criptografia na Sociedade
17.6.1. "Qual será o impacto do forte de criptografia, em última instância, sobre
o tecido social?"
- É difícil saber com certeza.
+ Esses efeitos parecem prováveis:
- Fome de governo de receitas tributárias, com concommitant
efeitos sobre o bem-estar, gastos, etc.
- aumenta em espioage
- problemas de confiança
17.6.2. As revelações de vigilância e de controlo dos cidadãos
e as corporações servem para aumentar o uso de
criptografia, em primeiro lugar, as pessoas com algo a esconder, e
em seguida, por outros. Cypherpunks já estão ajudando a espalhar
a palavra de estas situações.
- um efeito bola de neve
- e várias agências do governo-se usar
criptografia para proteger seus arquivos e seus arquivos de privacidade
17.6.3. As pessoas que fazem escolhas morais individuais
- as pessoas vão fazer as suas próprias escolhas, como o que revelar,
o que eles acham que vai ajudar a paz mundial, ou a futuro, ou
os golfinhos, ou o que quer que
- e este será um mercado líquido, não apenas almas gritando
no deserto
- claro que não, tudo vai ser revelado, mas o "mosaico
efeito" garante que, principalmente, a verdade vai surgir
- cada governo o pior medo, que é assuntos
decidir por si mesmos o que é secreto, o que não é, o que pode
ser dito para estrangeiros, etc.

17.7. Novas Ferramentas de Software e Quadros de Programação
17.7.1. Softwares necessários
- Drop-in de criptografia módulos são uma necessidade para o desenvolvimento. Como V.
Bontchev diz, "seria bom se a criptografia de disco
software permitiu que o usuário conectar seus próprios módulos.
Desta forma, todo mundo pode usar tudo o que eles confiam - MDC/SHA,
MDC/MD5, DES, IDEA, qualquer que seja." [V. B., sci.cripta, 1994-07-

01]
+ Robustez
- Segurança e robustez são, muitas vezes em desacordo
- Arquivos que são apagados na primeira dica de intrusão
(flash digital de papel), reenvio de e-mails de sites que ir para baixo no
primeiros sinais de problemas, e o arquivo de sistemas de transmissão
que dividir arquivos em várias partes--qualquer um dos que
pode ser perdido, destruindo assim toda a transmissão--são
não exatamente modelos de robustez.
- Correção de erro normalmente funciona diminuindo a entropia
através de redundância, o que é ruim para crypto.
- O militar usa elaborado (e caro) sistemas de
garantir que os sistemas não ir para baixo, teclas não são perdidas,
etc. A maioria dos usuários casuais de criptografia não estão dispostos a tomar
estes passos.
- E então chaves são perdidas, as senhas são esquecidos (ou são
escritas em Post-its e gravadas para terminais),
e remetentes são tomadas quando os operadores de ir em
férias. Tudo muito esquisito e não-robusto.
Veja como é esquisito entrega de correio é!
+ Um desafio é criar sistemas que são:
- robusto
- não muito complicado e trabalhoso para usar
- onde a redundância de não comprometer a segurança
+ De criptografia workbench
- Um uso excessivo do termo, talvez, mas um que capta a
metáfora de um grande conjunto de ferramentas, modelos de programação
aids, etc.
+ QKS e "Agentes Kit de Construção" (em desenvolvimento)
- junto com Dylan, DylanAgents, Telescript, e, provavelmente,
várias outras tentativas para desenvolver agente de kits de ferramentas
- Henry Strickland está usando "tcl" (uma espécie de script
a linguagem, como o "perl") como base.
+ Crise de Software
- ferramentas, linguagens, estruturas, ambientes, objetos,
bibliotecas de classes, métodos, agentes, exatidão,
robustez, evolução, desenvolvimento de protótipos
+ Ligações entre a crise de software de criptografia e
- sistemas complexos, complicado protocolos
- preço por ser "errado" pode ser muito alto, se é
um aeroporto que não pode abrir no tempo (Denver), ou uma
digital banco que tem seus ativos drenado em segundos
- os agentes, os objetos são esperava ser o "balas de prata"

+ A necessidade de uma melhor software de metodologias
- "balas de prata"
- falhas, erros, falhas, métodos
- comprovadamente correto projetos? (la Viper)
- Costuma-se dizer que muito melhor metodologias são
necessário para _real tempo programming_, devido ao tempo de
a criticidade e (provavelmente) a dificuldade de fazer
realista testes. Mas, certamente, o mesmo deve ser dito
de _financial programming_, a la bancário e
digicash esquemas que nos interessam muito.
- "um aspecto do software que mais torna o
esquisito indústria é que é incomum para
profissionais para estudar o trabalho dos outros. Programadores
não leia bons programas. Designers não estudo
projetos pendentes. As consequências ... não, basta olhar
para si mesmo. [Cameron Laird, comp.software-eng, 1994-
08-30]
+ De Software Grandes Construções
- A crise de software torna-se particularmente agudo quando
os grandes sistemas são construídos, tais como--para aplicar este
Cypherpunks problemas--quando o dinheiro digital e sistemas de
as economias são construídas.
17.7.2. Object-oriented ferramentas
+ Enquanto tres moda, alguns muito real de ganhos estão sendo relatados;
mais do que apenas um modismo, especialmente quando combinado com
outras ferramentas:
- quadros, kits de ferramentas
+ linguagens dinâmicas
- maior flexibilidade do que com a estática, fortemente tipados
langueages (mas também menos segurança, geralmente)
- OpenStep, Visual Age, Visual Basic, Dylan, Telescript (mais
agent-oriented), Lisp, Smalltalk, etc
17.7.3. Protocolo Ecologias
- Simulações comportamentais dos agentes digitais de dinheiro, falsificação,
etc.
- o mundo em que Alice e Bob e seus criptografia amigos
ao vivo
- a defesa, o ataque, falsificação, roubo de identidade, roubo de
- elementos que são criptograficamente forte (como o D-H-chave
bolsas de valores), mas combinadas de modos complexos, que tem quase a
para ser simuladas para encontrar pontos fracos
- "meio-out" em vez de "cima para baixo" (convencional, formal)
ou "bottom-up" (emergente, UMA-VIDA)

- como Eurisko (Lenat), exceto orientada para o domínio da
agentes financeiros
17.7.4. O uso de agentes autônomos (escravos?)
- "Um avançado ambiente de telecomunicações oferece um número
maneiras de proteger-se contra os problemas envolvidos
para lidar com o anônimo entidades em uma situação em que
não há monopólio do Governo.....Quando um PABX encontra
que uma chamada não está passando por um determinado tempo
operadora, ele muda automaticamente para o outro.
É fácil imaginar uma agentes inteligentes testes
vários tipos de transação conclusões e comutação
vendedores quando uma falha. Profissional de damas pode fornecer
informações sobre o fornecedor de estado para o pagamento de uma taxa. Depois de tudo, nós não
cuidado se uma empresa que estamos a lidar com alterações, se a sua
o serviço é afetado." [Duncan Frissell, 1994-08-30]
17.7.5. Ferramentas
+ "De línguas dentro de línguas" é uma forma padrão para ir para
implementar abstrações
- "Design Intermediários Línguas" (IDLs)
- conceitos abstratos tais como "motores" e "futuros"
- Lisp e Scheme tem sido favorecido idiomas para esta
- outros idiomas: Smalltalk, Dylan
+ Para criptografia, este parece ser o caso: abstrações
representados como classes ou objetos
- com programação em seguida, a seletiva subclassificação
- e, por vezes, gener
+ "tipo de verificação" de criptografia objetos é necessário
- para garantir o cumprimento de protocolos, com formas esperado, etc.
- verifique as mensagens para o formulário, remoção de sigs, etc. (análogo
para a verificação de uma carta antes de enviar para a adequada
endereçamento, para carimbo, vedação, etc.)
- muito do nonrobustness de correio e de criptografia vem do
os problemas com a manipulação de exceção--coisas que um ser humano
envolvidos podem ser capazes de resolver, em correio convencional sistemas
- "letra morta departamento"?
- Nota: No "Crypto Anarquia Jogo" jogamos em
Setembro, 1992, muitos selada mensagens foram descartadas por
sendo na forma errada, faltando a taxa de reenvio de e-mails que
o reenvio de e-mails necessários, etc. Concedido, os seres humanos fazem
bastante pobre mantenedores de restrições complexas....um monte

de as pessoas continuaram a se esquecendo de fazer o que era necessário. Um grande momento foi tido por todos.

17.7.6. "O que o framework de programação recursos são necessários?"

- O que se segue são definitivamente o meu opnions, ainda mais a minha própria opiniões que a maior parte do que eu escrevi. Muitas pessoas vão discordar.

+ Necessários:

- Flexibilidade de excesso de velocidade
- Prototipagem rápida, para adicionar novas funcionalidades
- Evolutiva abordagens
- Robustez (comprovadamente correto seria bom, mas...)

17.7.7. Frameworks, Ferramentas, Recursos

- Quase todo o trabalho de vanguarda em sistemas operacionais, a partir de "mutuamente suspeitos, cooperando processos" para "deadlock" a "persistência", mostrar-se em criptografia áreas que estão considerando-se.

+ De Software da Net vs. Software para Acessar a Net

- A Net--é atual forma adequada?
- Software para Acessar a Net

+ OpenDoc e OLE

- componentes trabalhando juntos, em cima de vários operacional sistemas, no topo de várias plataformas de hardware

+ Objeto Persistente Lojas

- provavelmente será necessário para os sistemas de prevemos
- robusto, de modo que um é "dinheiro" não evaporar quando um o sistema é reinicializado!
- questões interessantes aqui...
- CORBA. OpenDoc, OLE II, do SOM, da SILVA, da pedra preciosa, etc.

+ Quadros De Programação

- Linguagens dinâmicas pode ser muito útil quando os detalhes são difusa, quando as idéias necessidade de exploração (este não é um chamada para nondeterminism, para aleatórios futzing volta, mas um o reconhecimento de que o preciso, fortemente tipados abordagem de alguns idiomas podem ser menos útil do que um rico, exploratório ambiente. Isso se encaixa com a "ecologia" ponto de vista.

-

+ Conectividade

- precisa ser mais robusto, não escamosa a forma atual de e-mail é
- apertos de mão, agentes, robusto conexões
- ATM, SONET, agentes, etc....a "Rede do Futuro"

17.8. A complexidade
17.8.1. As areias movediças de modernos sistemas complexos
- muita sujeira, detalhe...mudar..relacionados para o "software
crise"...a flexibilidade de modernos sistemas de software
promove a mudança freqüente de características e comportamentos,
assim, jogando a placa de cozinhar com as tentativas de outros para compreender o
estrutura...a evolução em ação
- os seres humanos que usam esses sistemas se esqueça de como os comandos funcionam,
onde as coisas estão guardadas, como cancelar a subscrição, a partir de listas,
etc. (Este é apenas um motivo a várias sub-listas de nossa
lista raramente chegado muito tráfego: as pessoas usam o que eles
são mais acostumados a usar, e esqueça o resto.)
- computador (agentes de scripts, programas) que utilizam estes sistemas
muitas vezes, "de quebra" quando o sistema subjacente a alterações. Um bom
exemplo disso são o reenvio de e-mails de sites e scripts para o uso de
- os. Como reenvio de e-mails de sites de ir para cima e para baixo, como chaves de mudança, como
outros as coisas mudam, os scripts tem que mudar para acompanhar o ritmo.
- Este documento é outro exemplo. Espalhados por todo
são referências a sites, programas, fontes, etc. Como o tempo
passa, mais e mais deles (inevitavelmente) tornar-se
obsoleto. (A minha esperança é que o suficiente dos ponteiros vai
ponto para o ainda-existem coisas assim, como fazer os ponteiros
continuam sendo úteis. E eu vou tentar atualizar/corrigir o mau ponteiros.)
17.8.2. "Fora de Controle"
- Kevin Kelly livro
- incapacidade para ter um controle preciso, e como este é
consistente com a evolução, propriedades emergentes, limites de
modelos formais
- crypto, graus de liberdade
+ imagine redes do futuro próximo
- aumento de dez vezes em sites, usuários, domínios
- Comutação ATM tecidos..granularidade das operações
mudanças...de convergência da informática e das comunicações...
+ computação distribuída (que, a propósito, que, certamente, precisa
criptografia de segurança!)
- Joule, Digital Rota Da Seda
- agentes, etc.
+ não pode controlar a distribuição de informações
+ Como com a Ação Amador BBS caso, o acesso não pode ser controlada.
- "A existência de gateways e servidores proxy significa que

não há nenhuma maneira eficaz para determinar onde qualquer
a informação que você disponibilizar vai eventualmente acabar.
Alguém, digamos, Tennessee, pode facilmente chegar a um FTP
site na Califórnia por meio de um proxy na Suíça.
Até mesmo informações detalhadas sobre o tipo de
informação é considerada contrabando em cada
jurisdição do mundo não vai ajudar, a menos que todos os
gateway no mundo tem e usa-lo bem."
[Stephen R. Savitzky, comp.org.fep.falar, 1994-08-08]

17.8.3. Uma fértil união da criptologia, teoria dos jogos, economia, e ecologia

+ de criptografia tem muito tempo ignorado economia, exceto perifericamente, como um problema de engenharia (quanto tempo de encriptação demora, etc.)
- em particular, as áreas de reputação, risco, etc. não foi tratado como idéia central...talvez adequada para algoritmo matemático de trabalho
- mas a economia é crucial para os sistemas a serem planejado...de dinheiro digital, dados paraísos, remetentes, etc.
+ por que o dinheiro funciona tão bem...localidade de referência, imediata compensação de transações, as forças de cálculos para baixo para as unidades relevantes
- reduz reclamações, "ele me fez fazer isso" argumentos que...
é, aumenta a auto-responsabilidade...contrapartidas
+ teoria do jogo
+ maduro para o tratamento de "Alice e Bob" tipos de situações, em que os agentes com diferentes agendas de são interagir e competir
- "desertar", como no Dilema do Prisioneiro
- pagamento de salários as matrizes para vários comportamentos
- teoria de jogos evolutiva
- evolutivo de aprendizagem, algoritmos genéticos/programmming
- protocolo de ecologias

17.9. Criptografia Padrões De

17.9.1. A importância das normas

- um papel crítico
+ Parte de padrões de validação, suites de teste, etc.
- validação dos recursos e a segurança de um reenvio de e-mails, através de pings, testes, testes de desempenho, fiabilidade, etc.
- assim, a imposição de um negativo bater aqueles que falham
+ Existem muitas maneiras de fazer isso de padrões de teste
- relatórios de mercado (como com comercial de chips, software)

- "selo de aprovação" (especialmente conveniente digital
sigs)

17.10. Criptografia De Pesquisa
17.10.1. A pesquisa acadêmica continua a aumentar
17.10.2. "Qual é o futuro da criptografia?"
- Prever o futuro é notoriamente difícil. A IBM não
acho que muitos computadores jamais seria vendido, Western Union
passada a chance de comprar a Campainha do telefone patentes. E
assim por diante. O futuro é sempre nublado, o passado é sempre
claro e óbvio.
- Nós vamos saber em 30 anos, o que do nosso cypherpunkish e
cryptoanarchist previsões aconteceu--e o que não.
17.10.3. As cifras são um pouco como nós...a seqüência correta de movimentos
desata-os, a sequência errada, apenas os torna mais emaranhada.
("Nó teoria" está a tornar-se um tema quente em matemática e física
(trabalho de Vaughn Jones, a teoria das cordas, etc.) e eu suspeito
existem algumas ligações entre o nó teoria e criptografia.)
17.10.4. Teoria dos jogos, a reputação da empresa, criptografia -- muito a ser feito aqui
- é um elo, uma área não coberta acadêmica criptologia
investigação
distribuídos, modelos de confiança, o conluio, a cooperação,
evolutiva da teoria dos jogos, ecologia, sistemas de
17.10.5. Áreas mais avançadas, novas abordagens
+ alguns têm sugerido quasigroups latina, praças, finito
autômatos, etc. Quasigroups são importantes na IDÉIA de
cifra, e em algumas DES de trabalho. (Eu não vou especular furher
sobre uma área que não há quase nada sobre....Eu tinha ouvido falar de
semigroups, mas não quasigroups.)
- "O "Bloco de Mistura de Transformar" a tecnologia que eu tenho
vindo a promover no sci.cripta para grande parte da primavera e
o verão é um quadrado latino de tecnologia. (Esta foi a parte da
o meu "Grande Bloco DES", que eventualmente produzidos
o "Cercado DES" cifra como um possível DES
atualização.)....Cada uma das equações em um Bloco de Mistura
Transformação é a equação de um quadrado latino. O
várias equações de tal transformação, juntos, representam
ortogonal latina quadrados. [Terry Ritter, sci.cripta, 1994-
08-15]
+ Mas o que sobre para a chave pública utiliza? Aqui está algo Perry
Metzger executou através de:
- ""Finte de Autômatos, latino-matrizes, e a Criptografia" por Tao
Renji, Institute of Software, Academia Sinica, em Pequim.

Este (ainda não publicado) documento aborda vários
fascinante tópicos, incluindo alguns muito rápido de chave pública
métodos -- infelizmente, em muito pouco detalhe. Espero que
uma versão publicada vai aparecer logo..." [P. M.,
sci.cripta, 1994-08-14]

17.10.6. Comentários sobre a criptografia do estado da arte de hoje, contra o que é provável estar vindo

- Perry Metzger comentários sobre os atuais dificuldades de ordem prática:
"...pode a diferença entre "criptografia pode ser transformadora
quando a tecnologia amadurece" e "crypto é maduro agora" ser
que unobvious?....Um dos motivos que eu estou envolvido com o
IETF IPSP esforço é porque a criptografia coisas tem que ser
transparente antes que ele vai ser realmente
útil-em sua forma atual, é apenas lixo. Espero que,
versões posteriores do PGP também interface bem com o novo
padrões desenvolvidos para um sistema integrado de seguro mensagem
o tipo de corpo em MIME. (PGP também requer algum tipo de escalonável
e inversa mapable keyid sistema -- o atual keyids são
não vamos permitir que servidores de chaves para a escala de uma distribuição de
maneira.) Sim, eu vi os scripts do shell e o resto, e
eles realmente necessitam de muito esforço para a maioria das pessoas-e
na melhor das hipóteses, depois de ter as coisas configurado, agora você pode com segurança
ler alguns e-mail em alguns sites. Eu sei que para mim,
uma vez que eu ler um grande fração do meu e-mail durante o trabalho
clientes, onde eu enfaticamente não confiar no hardware,
cada mensagem criptografada significa uma grande inconveniência,
independentemente." [Perry Metzger, 1994-08-25]

17.11. Crypto Armagedom? Cryptageddon?

17.11.1. "Haverá um "Waco no ciberespaço"?"

- enquanto alguns de nós são muito vocais aqui, e são, provavelmente,
conhecido para as autoridades, este não é geralmente o caso.
Muitos dos usuários do forte de criptografia será discreto e
não vai dar aparências de ser de código-utilizando
crypto anarquista cultistas.

17.11.2. Ataques vir

- "Você vai ver essas pessoas atacando remetentes anônimos,
criptografia, psuedonymous contas, e outras ferramentas de
a coerção-a liberdade de expressão e de intercâmbio de informações sobre
a net, ironicamente, muitas vezes, em nome da promoção
"o comércio". Você vai ouvi-los discurso e sobre a rave
"bandidos" e "terroristas", como se eles ainda tinham um bom

pista sobre as leis de milhares de jurisdições
atravessado pela Internet, e como se suas próprias tentativas de
para habilitar a coerção têm qualquer semelhança com a prática de
o terrorismo. O assustador coisa é, eles realmente acha que eles
ter uma boa idéia sobre o que as leis devem ser, e
eles estão perfeitamente dispostos a enfiá-lo goela,
independentemente da grande diversidade da cultura, intelectual,
político, e parecer jurídico sobre o planeta."
[<an50@desert.hacktic.nl> (Ninguém), libtech-l@netcom.com,
1994-06-08]
+ por que eu não estou otimistas sobre Federais
- matar Randy de Weaver esposa e filho a partir de uma distância,
após forjadas armas encargos
- queima viva a Koresh composto, por acusações falsas
de Satanismo, abuso de crianças, e a mulher, insultuosa
- apreensão de barcos, carros, etc., em "suspeita" de
o envolvimento com drogas

17.12. "O Futuro é Tão Brilhante, eu Tenho roupas de Tons"
17.12.1. Apesar de, ocasionalmente, sombrias previsões, as coisas parecem
muito bom.Não há garantias, é claro, mas as tendências que estão
favorável. Não há razão para o descanso, porém.
17.12.2. Duncan Frissell coloca desta forma:
- "O comércio é o caminho para cima. A riqueza é caminho para cima. Viagem internacional
é caminho para cima. A migração é caminho para cima. Recurso preços são os
o mais baixo na história humana. Os custos de comunicação são a forma
para baixo. Eletrônica custos são a maneira para baixo. Estamos em um zero ou
negativo de inflação. A quantidade e a qualidade
de bens e serviços oferecidos nos mercados em
tempo alto. A porcentagem de países liderado
por ditadores é o mais baixo que jamais esteve.

"O que tudo isto significa é que políticos filosofias que
depende de força de braços para empurrar pessoas para dentro de uma linha
cada vez mais a deixar de funcionar. As pessoas ricas com escolhas,
quando forçadas, tendem a alterar seus investimentos e
negócios em um ambiente de formulário ou para mover para um
ambiente mais amistoso. A escolha é real. Se escolhas
existem, eles serão feitos. Uma cada vez maior proporção de
pessoas do mundo vai ser "rico" em riqueza e escolha como a
passar dos anos.

"Apenas uma filosofia política que depende o não coagida

a cooperação de pessoas muito diferentes, tem uma chance de
funcionamento no futuro." [Duncan Frissell, 1994-09-09]

17.13. "Vai criptografia realmente trazer o Milênio?"
17.13.1. Sim. E gatos irá mover-se com cães, Snapple de chuva a partir de
o céu, e P será mostrado desigual para NP.
17.13.2. Sério, as implicações do forte de privacidade, de
cyberspatial economias, e das fronteiras, tornando-se transparente
são enormes. A maneira com que os governos fazer o negócio já está
mudando, e isso vai mudar as coisas ainda mais drasticamente.
A forma precisa pode ser imprevisível, mas certos estados finais
são relativamente fáceis de prever, em traços gerais.
17.13.3. "Como sabemos as implicações de criptografia são o que eu tenho
alegou?"
- Não podemos saber o futuro.
- Impressão, estradas, eletrificação
17.13.4. "Quando isso tudo acontecer? Quando vai forte de criptografia realmente
começam a ter um grande efeito sobre a economia?"
+ Etapas:
- A Era Pré-Histórica. Antes de 1975. NSA e outras
órgãos de inteligência e de controladas mais de criptografia de trabalho.
Criptografia visto como um hobby. DES apenas começando a ser
implantado por bancos e instituições financeiras.
- A Investigação Era. 1975-1992. Grande interesse no público
chave de identificação, em vários protocolos. Início de várias
"Crypto" conferências. Trabalhar em dinheiro digital, DC-Redes,
registro de data e hora, etc.
- O Ativismo Era. 1992--?? (provavelmente, 1998). PGP 2.0
lançado. Cypherpunks formado. Clipper anunciou--atende
tempestade de protestos. FEP, CPSR, ÉPICO, outros grupos.
"Wired" começa publicação. Digital Telelphony, outros
contas. Várias tentativas para iniciar a criptografia de empresas de são
feito...a maioria fundador.
- A Era De Transição. Depois de cerca de 1999. As empresas.
Dinheiro Digital necessário para transacções Líquidas. Redes e
computadores rápido o suficiente para permitir que mais protocolos robustos. Imposto
paraísos florescer. "Novo Submundo Ordem" (crédito para Claire
Sterling) floresce.
- Ainda é cedo para se esperar que o ambiente atual--
tecnológica e regulamentar--será benéfico para o
tipo do forte de criptografia nós somos a favor. Muitas peças são
faltando. Mais alguns avanços são necessários. Um pouco mais
falhas também são necessários (gulp!) para mostrar melhor como não

prosseguir.
17.13.5. "Mas criptografia anarquia realmente acontecer?"
- Para uma crescente medida, ele já está acontecendo. Olhar para o
os chamados mercados ilegais, os fluxos de dinheiro da droga em torno de
o mundo, a transferência de bilhões de dólares de um dia na
mera "chop marks," e o próspero comércio de itens proibidos.
- "Cinza e preto, o capitalismo já é uma grande componente de
internacional fluxos de caixa....Uma vez adequado amigável
o software está disponível, a internet accellerate este
tendência que já se verifica....Crypto anarquia é meramente a
aplicação de modernas ferramentas para auxiliar secreta do capitalismo."
[James Donald, 1994-08-29]
- Existem argumentos de que uma Grande Repressão está chegando, que
os governos encerrar mercados ilegais, vai parar
forte de criptografia, força economias subterrâneas
acima do solo. Isso é duvidoso--tentou-se para o passado
há várias décadas (ou mais). Proibição meramente feita crime
mais organizado; idem para a Guerra em (Alguns) de Drogas.
17.13.6. "Tem o ponto de não retorno foi passada no forte de criptografia?"
- Na verdade, eu acho que nos EUA pelo menos, o ponto de
passadas décadas atrás, possivelmente, um século ou mais atrás, e
que qualquer esperança de controlar forte de criptografia e privado
comunicação evaporado há muito tempo. Abusos cometidos pelo FBI em
escutas telefônicas Americanos, e os relatórios de monitoramento da ANS
comunicação interna não obstante, é
essencialmente.....

17.14. Pontas Soltas
17.14.1. firewalls virtuais, perímetros, deslize-tipo de túneis criptografados,
um fim de break-ins,
17.14.2. "Que tipo de criptografia será usada com o ATM?"
- (ATM = Modo de Transferência Assíncrono, não Automated Teller
Máquina)
- alguns relatórios que a ANS é a elaboração de normas para ATM
17.14.3. As formas das coisas futuras, que talvez....(leis de outros países)
+ A índia tem uma taxa de agendamento para BBS operadores, por exemplo, eles têm
para pagar us $50.000 por ano para operar em uma placa de boletim! (Este
soa como a lenda urbana sobre a FCC planejamento de um modem
imposto, mas talvez seja verdade.)
- "O Fórum de Direitos Eletrônico de Expressão (FREE) tem
foi formado na Índia, como um órgão dedicado a estender
direitos fundamentais para a eletrônica de domínio....LIVRE deve
a sua criação para um ataque a uma Indiana de transmissão de dados pelo Indiano

o governo, na forma de exorbitantes taxas de licença (um
mínimo de Rs. 1,5 milhões = US$50,000 cada ano para um BBS,
muito mais por e-mail)." [amehta@doe.ernet.in (Dr. Arun
Mehta), encaminhado por Phil Agre, comp.org.cpsr.falar, 1994-
08-31]
- para mais informações: ftp.eff.org
/pub/FEP/Política/Mundo/Índia/LIVRE
17.14.4. Ciberespaço terá a melhor proteção
- para garantir a fraude e a contrafacção é reduzida (lembre-se
Habitat de problemas com as pessoas a descobrir as brechas)

18. Pontas soltas e Tópicos Diversos

18.1. direitos autorais
O CYPHERNOMICON: Cypherpunks FAQ e Mais, Versão 0.666,
1994-09-10, Direitos De Autor Timothy C. De Maio. Todos os direitos reservados.
Veja os detalhes de isenção de responsabilidade. Use seções curtas em "justo
use" disposições, com crédito apropriado, mas não coloque o seu
nome em minhas palavras.

18.2. RESUMO: Pontas Soltas e Tópicos Diversos
18.2.1. Pontos Principais
18.2.2. Ligações para Outras Secções
18.2.3. Onde Encontrar Informações Adicionais
18.2.4. Diversos Comentários
- Eu odeio ter uma seção como esta, mas há apenas alguns
coisas que não parecem se encaixar perfeitamente em outro lugar
- espero que você encontrou este tópicos com o seu editor de pesquisa
ferramentas

18.3. Criptografia Quântica
18.3.1. "O que é criptografia quântica?"
+ Dois principais sabores:
+ canais seguros que exploram o Princípio da Incerteza
+ Brassard, Bennett, de fibra óptica, distâncias curtas,
detecta tocar
+ Criptografia quântica
- bits podem ser trocados-embora com bastante baixos
as eficiências através de um canal
- com a detecção de toques, através da mudança de
duas polarizações
+ Stephen Wiesner escreveu uma 1970 papel, metade de uma década
antes de o P-K de trabalho, que delineou-não

publicado até muito mais tarde
- se especular que a NSA sabia sobre isso e
anulada a publicação
+ fatoração de números usando um estranho Mundo, Muitos
interpretação
- Shor
+ dá atenção à minha paródia sobre Russos
- Eu nunca soube que eu bater tão perto da marca!
18.3.2. "O que sobre _quantum cryptography_?"
+ Explorando o Princípio da Incerteza de fazer untappable
as linhas de comunicação. (Mais precisamente, aproveitado linhas de dar
indicação de ter sido aproveitado.)
- Bennett e Brassard
- fraco flashes de luz em um cabo de fibra óptica utilizados;
fótons polarizados
- Alice e Bob ir através de um protocolo que envolve
escolhendo Linear ou Polarização Circular (LP CP); não pode
ser simultaneamente medidas...
-
- Não poderão ser importantes para um longo período de tempo.
- Uma ferramenta adicional, ou crypto primitivo bloco de construção.

18.4. Caótico De Criptografia
18.4.1. o oscilador esquema foi interrompida em Criptografia '94

18.5. Redes neurais e AI Criptográfica
18.5.1. "O que sobre redes neurais e AI em criptografia?"
De uso limitado, pelo menos em quebrar as cifras modernas. Marvin
Minsky uma vez disse que se você não entender como resolver
um problema, a adição de aleatoriedade geralmente não ajuda.
- A forma do espaço de solução é muito alta, muito mal
adequado para escalada ou dividir-e-conquistar métodos
+ Redes neurais não são susceptíveis de fazer o bem com as cifras modernas
(por exemplo, RSA, IDEA, DES, etc.), principalmente por causa da forma
do espaço de solução. Em vez de "colinas e
vales" que as redes neurais (e métodos relacionados, tais como
algoritmos genéticos, simulated annealing, etc.) fazer o bem,
o espaço de solução para as cifras modernas oferece muito pouco em
a maneira de "aprender" oportunidades: você tem o
solução (a chave), ou não.

Acho que de uma agulha, do pé de uma planície...um ou NN
qualquer outro-hill climber poderia andar por anos e nunca

encontrá-lo. Bem-concebido, as cifras modernas como o RSA e a IDÉIA
parecem admitir nenhuma análise com base no "não randômico"
propriedades. Se alguém tiver encontrado atalhos para o factoring
módulo de elasticidade na RSA, por exemplo, eles não o permitir.

Suspeito que há utiliza em aspectos periféricos, tais como
a adivinhação de senhas (quando as pessoas não pegou de alta
a entropia senhas, mas em vez de ter usado nomes familiares).
Ou em análise de tráfego. Aqueles que arrebentar em lotes do tráfego
pode muito bem estar usando redes neurais, processamento de sinais customizados,
etc. para "preparar" o tráfego capturado por mais
análise. Uma aposta segura, na verdade.

Mas o movimento moderno criptologia é, definitivamente, longe de
usar qualquer coisa com "estrutura" que pode ser aprendido. Coloque
de outra maneira, as redes neurais e trabalho bem estruturado
ambientes onde há algo para _learn), mas não
na alta entropia, aparentemente aleatórios mundo da criptografados
dados.
+ AI pode ser útil em outras áreas
- protocolo de geração de
- SIGINT
18.5.2. Evolutiva ou Programação Genética
- a la Holland, Koza
- RNGs

18.6. Diversos Avançados De Criptografia Ideias
18.6.1. "Por ter comprovadamente "NP-completo" problemas não encontrados usa em
criptografia?"
- Um dos grandes Mistérios não Resolvidos! Ou o Santo Graal,
se você vai.
- O problema é que tem comprovadamente o disco rígido (ou NP-completo, para ser
mais preciso) problemas não foram usados? (Factoring não é
conhecido NP-completo...especialistas pode corrigir meu fraseado aqui
se eu estou misstating coisas.)
- Seria bom se um comprovadamente problema difícil, como o
domino ladrilhos problema, ou 3SAT, ou outras coisas fora de
Garey e Johnson, o livro de NP-Completude pode ser usado.
Isso aumentaria a confiança em cifras ainda mais.
18.6.2. "Pode autômatos celulares, como Conway "Jogo da Vida", a ser usado
para criptografia?"
- Stephen Wolfram proposta de utilização de autômatos celulares para
crytography alguns anos atrás; a sua coleção de ensaios sobre a

autômatos celulares contém pelo menos uma menção. Muitos
as pessoas suspeitas de que o 1D CAs não eram mais fortes do que linear
feedback shift registers (LFSRs), e eu recally de ouvir um
alguns anos atrás de que alguém provou 1D CAs (e talvez
todas as autoridades de certificação?) são equivalentes a LFSRs, que têm sido utilizados em
criptografia por muitos anos.
- Wolfram do livro "Teoria e Aplicações de Celulares
Autômatos," De 1986, O Mundo Científico. Diversos trabalhos sobre a utilização de
CAs para a sequência aleatória de geração. P. Bardell mostrou
in1990 que o CAs produzir as saídas de LFSRs.) Wolfram também
tem um papel de "Criptografia com autômatos celulares," em
Proc. CRYPTO 85.
- Intuitivamente, a ideia de uma autoridade de CERTIFICAÇÃO parece atraente para "one-way
funções," pelas razões mencionadas. Mas o que é a
"alçapão", que dá a chave de seu titular um atalho para reverter
o processo? (Criptografia de chave pública precisa de um alçapão 1-forma
cortaram o funtion que é fácil reverter se alguém tem o direito
informações).

18.7. Vírus e Criptografia
18.7.1. "O que é a conexão entre Cypherpunks e vírus?"
- Como, dewd, é tão kool.
- Beavis 'n Butthead usar o PGP (na verdade, Eric Hughes proposta
em um ponto que sugerimos uma criptografia de tie-in para o
escritores)
- Só há conexão periférica.
- O vírus pode ser transmitido com remetentes anônimos, mas o digital
as assinaturas podem ser utilizados para proteger o software. Assinado
software, sem mods permitido.
18.7.2. "O que sobre a "criptografia de vírus," como KOH?"
- (Um pouco longe, mas o problema vem de cima.)
- Alguém perguntou sobre isso no sci.cripta e Vesselin
Bontchev disse: "Este tema tem sido debatido até a morte em
alt.segurança.pgp, quando alguém postou KOH, mesmo sem um
aviso que ele não é um vírus.....Ambos os vírus, de fato, usar o
A IDÉIA de codificação - o mesmo que é utilizado tanto por SecureDevice
e SecureDrive. No entanto, os vírus representam algum significativa
as ameaças à integridade dos seus dados, exatamente por causa de
a sua replicação viral significa.....Além disso, se você adquirir por
viral significa, você não receba o doumentation e um
utilitário, os quais são essenciais para o uso adequado
do produto - assim, provando mais uma vez que a sua viral
capacidades são desnecessários e prejudiciais. Além disso, o vírus

não vem na origem, o que significa que ele poderia ter
alguns escondidos backdoors ou, simplesmente, falhas de segurança, e você
não temos nenhuma maneira de verificar isso ou para corrigi-los. Por último, em alguns
casos, o vírus pode destruir informações valiosas durante
seu processo de replicação."
- "Em resumo, não usá-los. Você vai ganhar nada mais
usando
autônomo programas de criptografia, e você vai expor o seu
dados
a integridade de riscos significativos. Os vírus são
completamente inútil
e mesmo prejudicial; eles foram criados com o único
a razão para
perdoar as atividades ilícitas dos criadores de vírus, por
alegando que
vírus de computador pode ser "útil"." [Vesselin Bontchev,
sci.cripta, 1994-08-31]

18.7.3. "O que sobre vírus? Existem laços de criptografia e
Cypherpunks temas?"
- Qualquer ligação direta que qualquer um de nós ver claramente. Ocasionalmente, um
vírus fã vê os "punks" nome e acha que estamos envolvidos
escrito vírus. (Na verdade, algumas pessoas na lista tem
vírus de experiência.)
- Criptografia pode proteger contra vírus, por ter o código-assinado.
E a confiança na auto-responsabilidade e a auto-protecção
está em contraste com a abordagem jurídica, que tende a não
funciona muito bem para a proteção contra vírus (pelo encoberto natureza de
muitos vírus).

18.7.4. "O que interessa fazer Cypherpunks tem vírus?"
- Não muito, embora o tema vem periodicamente.
- Alguma sobreposição das comunidades envolvidas.
- E há algum vírus métodos que usam formas de
criptografia.
- Também, assinaturas digitais em código pode ser utilizado para garantir que
código não foi modificado desde que foi lançado pela
autor original.

18.8. Ganhar Dinheiro na Criptografia

18.8.1. "Como eu posso ganhar dinheiro na criptografia?"
- crypto especialistas são contratados por empresas de software
+ start up de empresas
- um caminho difícil
- não claro que, mesmo Phil Zimmermann fez dinheiro

- e mesmo RSADSI está diante de um desafio (não passou
público, não uma vaca de dinheiro, etc.)
- Pode haver um crescimento explosivo--a mudança de fase que muitas vezes eu
falar--e muitas oportunidades vão surgir. Mas, tendo
dito isto, continuo a não ver o óbvio oportunidades de direito
agora. E começando uma empresa de esperança e de ideologia,
em vez de suprir um mercado real ou empurrando real
tecnologia (market pull versus tecnologia push argumento) parecem
equivocado.

18.9. A Net
18.9.1. Limitações do actual líquido
- interoperabilidade
+ subsidiada, não como você vai pagar
- faz spam inevitável, não alocar recursos para
aqueles que querem eles, o mais
- isso vai exigir digicash em melhor forma do que a maioria
os usuários agora têm acesso a
- sysadmins ficar preocupado
- criptografia, às vezes, banido
- comuns estado de portador não é claro
- geral cruftiness de Líquido ("morte iminente da Usenet
previsto")

18.10. Coação Muda, Morto O Homem Muda
18.10.1. "O que cerca "coação" códigos adicionais de segurança?"
- Onde um inofensivo decrytion pode ser feito, ou um alarme enviada.
+ Exemplos
- envio de alarme, como uma em que o contador botão de alarme
- desencriptação de um banco, o número do cartão para um menor valor de conta
- dois conjuntos de livros (não é estritamente uma "coação" do código, a menos que
você exibir o IRS como causadora de coação)
- alarmes associados, como em células
- " Se ter separado do mecanismo de autenticação que é utilizado
sob coação, é uma idéia muito boa que alguns sistemas existentes
já
empregar.... A partir de um sistemas de ponto de vista, é difícil
descobrir exatamente como o sistema deve responder quando ele
reconhece uma coação de autenticação....O seguro dentro do
Máquinas ATM usado por BayBanks (Boston em Massa) pode ser aberto
com duas combinações. Uma combinação envia um alarme para
o banco, através de uma linha telefónica separada (não utilizado para
realizar a transação em caixa eletrônico). O alarme do telefone de linha também é

conectado a um convencional pânico mudar." [Bob Baldwin,
Coação Senhas/ / Pinos/Combinações, 1993-11-18]

18.10.2. Coação muda, homem morto, interruptores, etc.

+ "Digital, flash paper," pode ser acionado para apagar arquivos, etc.
- (BATF e DEA raiders pode ter meios sofisticados de a desabilitação de computadores)
+ Coação códigos..."apagar meus arquivos," maneiras de não dar esrowed informação adequada, a menos que o código é dado, etc.
+ "Não vai liberar se eu estou sob acusação"
- questões interessantes sobre o segredo acusações, sobre a publicidade de tais casos, o acesso aos autos por ventos computadores, etc.

18.10.3. Pessoal de segurança para discos, morto o homem muda

+ Ouvi dizer que algumas BBS operadores de instalar o homem morto parâmetros de perto as portas para os quartos, contendo a respectiva sistemas de...entrando no quarto sem lançar o interruptor faz com que algumas medidas a serem tomadas
- apagar um disco, o "dumping" um disco de RAM (uma forma perigosa para armazenamento de dados, dada a falhas de energia, macio erros, reinicia, etc.)

18.11. Pode Criptografia de ser Detectado?

18.11.1. "As mensagens podem ser digitalizados e disponibilizados para a encriptação?"

- Se a criptografia produz _markers_ ou outras indicações, em seguida, é claro. "BEGIN PGP" é um muito claro beacon. (Tais marcadores auxilia na descriptografia pelo destinatário, mas não são essencial. "Stealth" versões do PGP e outros criptografia programas-como o S-Ferramentas para ms-DOS--não tenho essa marcadores.)
- Se a criptografia produz "aleatório procurando" coisas, então entropia e outras medidas de testes estatísticos podem ou não ser capaz de detectar essas mensagens de forma confiável. Depende do que não-mensagens criptografadas parecer, e como o algoritmo funciona.
+ Steganography:
tomada de mensagens de aparência normal
- dobrando th ebits com outros aleatórios-como bits, tais como na baixa-ordem de bits de imagens ou arquivos de som
- A preocupação de ordem prática depende de um político local meio ambiente. Em muitos países, a mera suspeita de usar crypto poderia pôr um perigo real.

18.12. Assistentes Digitais pessoais, Newton, etc.

18.12.1. "Há de criptografia usa para coisas como Newtons?"
- Provavelmente. Eventualmente. Carteiras digitais, portáteis chave
titulares, agentes locais de acesso, etc.
+ Enquanto isso, alguns programas de criptografia de existir. Aqui está um:
- -> nCrypt, a criptografia forte para aplicação
Newton:
-> ftp.sumex-aim.stanford.edu/info-mac/nwt/utils/n-crypt-
lite.hqx

18.13. Segurança Física
18.13.1. "Pode fibra óptica cabos de ser tocado?"
+ Sim. A luz pode escapar da fibra em curvas, e "perto-
campo" tocando teoricamente, é possível, pelo menos em
condições de laboratório. Medidas activas de perfuração a cabo
escudos e tocar as fibras também são possíveis.
- "O Fed quer um custo eficaz, F/O toque rapidamente em. Minha empresa foi
aproximou-se para desenvolver um sistema, pode ser feito, mas não
hotéis baratos, como fio de cobre de tocar." [
domonkos@access.digex.net (andy domonkos),
comp.org.fep.falar, 1994-06-29]
- De Los Alamos tecnologia? 1990?

18.14. Atacando Os Governos
18.14.1. "cupins" (rumores, psy-ops), que podem comprometer os governos,
seguido por "torpedos" (ataque direto)
18.14.2. RESÍDUOS (Guerra Contra o Forte, resistente a Adulterações de Criptografia).

18.15. Cypherpunks A Lista De Problemas
18.15.1. muito ruído na lista?
- "De todas as listas que eu estou inscrito, este é o único
que eu leia
todas artigo no. Até mesmo o "ruído" dos artigos. Seres humanos
sendo que
eles são, o ruído é necessária para ajudar a decidir a direção
do
do grupo. Além disso, para aqueles de nós que estão apenas começando no
nossa jornada
através de criptografia-submundo precisa de ruído para ajudar
familiarizar
- nos com a forma como a criptografia funciona. Eu aprendi mais do
o informal
divagações do que eu colhi de todas as formais e/ou
matemática

lançamentos para a data." [Patrick E. Hykkonen, 5-25-93]

18.16. Resistente A Adulterações Módulos
18.16.1. TRMs, afirma que "Picbuster" processador pode ser localmente
substituído com centrou-ou dirigida UV (OTP)
18.16.2. resistente a adulterações módulos de ter algumas desvantagens, como bem
- caixas registradoras para assegurar a conformidade com todas as
imposto sobre vendas, imposto sobre o valor acrescentado (IVA), e o racionamento de regras; um
resistente a adulterações do módulo de registo de dinheiro poderia ser o
mecanismo de execução para um estado de segurança nacional.
- "observadores"

18.17. Mais Profundas Conexões
18.17.1. Em vários lugares que eu já referido "conexões profundas" entre
coisas como criptografia, dinheiro, teoria de jogos evolutiva
ecologias, motivações humanas, e a natureza do direito. Por este
Quero dizer que há mais profunda, princípios unificadores. Princípios
envolvendo a localidade, a identidade e a divulgação do conhecimento. Um
bom exemplo: a profunda justiça de "cortar-e-escolha" protocolos-
-Eu vi menção a isso na teoria de jogo tesxts, mas não
muita discussão de outros protocolos similares.
18.17.2. Por exemplo, abaixo do nível da teoria e algoritmos
na criptologia encontra-se um nível de lidar com a "identidade"," prova","
"conluio" e outros conceitos fundamentais, conceitos que podem
quase ser tratada independente do acual algoritmos
(apesar de que a realização concreta da chave pública métodos tomou
esta fora do âmbito abstracto de filosofia e fez
importante analisar). E estes conceitos abstratos estão ligado
para outros campos, como economia, psicologia humana, a lei,
e evolutiva da teoria dos jogos (o estudo da evoluiu estratégias
em multi-agent systems, por exemplo, os seres humanos, interagindo e
a negociação com cada um dos outros).
18.17.3. Eu acredito que há questões importantes sobre o porquê de as coisas funcionam
a maneira de fazer a este nível. Para ser concreto, por fazer ameaças
de coerção física criar distorções no mercado e que
efeitos isso tem? Ou, o que é a natureza de emergente
comportamento baseado na reputação de sistemas? (A combinatiion de
criptografia e a economia é uma área fértil, mal tocou
acadêmico criptologia comunidade). Qual é a localidade é
importante, e o que isso significa para o digital cash? Por que
regulamento geralmente produzem _more_ crime?
18.17.4. Criptografia e idéias relacionados de reputação, identidade e

teias de confiança introduziu um novo ângulo em econômico
matéria. Eu suspeito que há um par de Prêmios Nobel em
Economia para aqueles que integrar estes conceitos importantes.

18.18. Ponta Solta Pontas Soltas
18.18.1. Quais as principais questões que são...uma coisa difícil de analisar
- untraceablility como uma base de construir, o que tem importantes implicações
+ muitas vezes, pode perguntar quais seriam as implicações se, dizer:
- invisibilidade existia
- untraceability existia
- Por "difícil analisar", quero dizer que as coisas são, muitas vezes,
coflated, misturados. É a "reputação" que
importa, ou o "anonimato"? O "untraceability" ou o
"dinheiro digital"?
18.18.2. Preço de sinalização nos posts...para mais informações
+ Quando um artigo é publicado, e não há mais completa
informações disponíveis em outros lugares por ftp, gopher, mosaic,
etc., então, como é que este ser assinalado sem, na verdade,
publicidade de forma destacada?
- por que não um código, tal como o "Geek código" assim, muitas pessoas colocam
em sua sigs? O código pode ser analisado através de um leitor, e
usado para ir buscar automaticamente as informações, pagar por ele,
etc. (Agentes que podem ser criados em leitores de notícias.)
18.18.3. "O que deve Cypherpunks suporte para "cabo" ou "set-top box"
padrões?
- Advertências: Minhas opiniões, oferecido apenas para ajudar a enquadrar o
o debate. E muitos de nós, rejeitam a idéia de governo-
mandato "normas" para o meu fraseado aqui não é para
implicam o apoio de tais normas.
+ Principais alternativas:
+ Set-top box, com t.v. como o núcleo de acesso a "informações
auto-estrada."
+ Problemas:
- número limitado de canais, mesmo se "500 canais"
- faz t.v. o foco, perde algumas outras capacidades
- poucos consumidores terão aparelhos de televisão com o
capacidades de resolução que mesmo computador atual
os monitores têm (há razões para isso: tamanho da
monitores (relacionada com a distância de visualização), NTSC
restrições de idade de televisores, etc.)
+ De comutação de pacotes do cabo, como na ATM ou mesmo SONET
(Synchronous Optical network), a Rede de acesso
+ Vantagens:

- A televisão é apenas um dos mais de comutação de pacotes
de transmissão, não usando a largura de banda
+ Proposta Radical: Completa desregulamentação
+ deixe o cabo de fornecedores-especialmente de fibras ópticas,
que são pequenos e discretos--leigos fibras para qualquer casa
eles podem negociar o acesso a
- por exemplo, transportando linhas telefônicas, elétricas
cabos, etc. (para remover a objeção sobre feio
novos postes ou cabos a ser amarrado...não deve ser uma
problema com fibra ótica)
- deixem o mercado decidir...deixe que os clientes decidam
+ Na minha opinião, o governo padrões são uma péssima ideia aqui.
Com certeza, NTSC foi um padrão eficaz, mas provavelmente seria
surgiram sem o envolvimento do governo. Idem para
Ethernet e um zilhão de outras normas. Não há necessidade de
envolvimento do governo.
- Claro, quando a indústria de grupos se reúnem para discutir
normas, espera-se que as leis antitruste não será
invocada.
18.18.4. ponto de menor importância: a importância do "Mas não é escala?" é, muitas vezes, exagerado
- em muitos casos, é muito mais importante para simplesmente chegar
algo implantado do que ele é preocupar-se com antecedência sobre como
ele vai quebrar se muitas pessoas usá-lo (por exemplo, MacDonald
preocupar-se em 1955 sobre scalabilty de seus negócios).
- Redes de reenvio de e-mails, por exemplo, não pode dimensionar especialmente
bem, na sua forma actual...mas quem se importa? Fazê-los
usado permitam uma maior requinte.

19. Anexos

19.1. direitos autorais

19.2. RESUMO: Apêndices
19.2.1. Pontos Principais
19.2.2. Ligações para Outras Secções
19.2.3. Onde Encontrar Informações Adicionais
19.2.4. Diversos Comentários

- Este ainda está em construção.
- Desorganizado!!!
- Os URLs devem ser verificados

19.3. Apêndice -- os Sites, Endereços URL/Web Sites, Etc.
19.3.1. certifique-se de obter soda endereço direto!!! [usar clones]
- Eu recebi o meu da soda.csua.berkeley.edu
os menus são: /pub/cypherpunks/pgp/pgp26

19.3.2. Como usar esta seção
+ comentário sobre URLs que estão sendo apenas um instantâneo...
- use responder a Sherry Mayo aqui
19.3.3. Geral de Criptografia e Cypherpunks Sites
- sci.cripta de arquivo: ftp para anon ftp.wimsey.bc.ca:/pub/crypto
[Mark Henderson]
+ ftp://soda.berkeley.edu/pub/cypherpunks/Home.html [tem
provavelmente foi alterado para soda.csua.edu site]
- ftp://ftp.u.washington.edu/public/phantom/cpunk/README.ht
ml
- ftp://furmint.nectar.cs.cmu.edu/security/cypheressay/what-
é-cypherpunk.html [Vincent Cate, 1994-07-03]
- ftp://wiretap.spies.com/Gov/World/usa.con
- http://www.quadralay.com/www/Crypt/Crypt.html
- http://cs.indiana.edu/ripem/dir.html
- diversos. artigo sobre criptografia:
http://www.quadralay.com/www/Crypt/Crypt.html
- ftp.wimsey.bc.ca:/pub/crypto tem REDOC III, Loki91, SHS e
HAVAL (Mark Henderson, markh@vanbc.wimsey.com, 4-17-94,
sci.cripta>
+ Alguns objetos. sites ftp para verificar:
- soda.berkeley.edu
- ftp.informatik.uni-hamburg.de
- ripem.msu.edu
- garbo.uwasa.fi
- wimsey.bc.autoridade de certificação
- espírito.dsi.unimi.ele
- http://rsa.com
- PC Expo embalagem do disco para ftp.wimsey.bc.ca [Avakov Ray
Arachelian, 1994-07-05]
+ PC Expo disco
- ftp.wimsey.bc.ca
/pub/crypto/software/dist/US_or_Canada_only_XXXXXXXX/pcxp
o/pcxpo.zip

- "O site FTP ripem.msu.edu tem um monte de criptografia coisas."
[Marcos Riordan, 1994-07-08]
+ URL para "applied Cryptography"arquivos relacionados
- http://www.openmarket.com/info/cryptography/applied_crypt
ography.html
19.3.4. PGP Informações e Sites
+ http://www.mantis.co.uk/pgp/pgp.html
- informações sobre onde encontrar PGP
+ pgpinfo@mantis.co.uk
- enviar qualquer e-mail para este site e receber uma lista de trás do PGP
sites
- PGP informações: ftp.netcom.com em /pub/gbe e em /pub/qwerty
- mais PGP:
ftp:csn.org//mpj/I_will_not_export/crypto_???????/pgp
<Michael Paul Johnson, mpj@csn.org, Colorado Catacumbas, de 4 a 8
94>
- Para fora dos EUA fontes de PGP: enviar email em branco para
pgpinfo@louva-a-deus.co.reino unido
+ Sherry Mayo, um cripto pesquisador, na Austrália, é também
fazendo versões disponíveis:
- "PGP2.6ui está disponível (espero eu!) no meu experimental WWW
server, aponte seu navegador
http://rschp2.anu.edu.au:8080/crypt.html eu sou novo para
WWW coisa então deixe-me saber se você tem alguma probs
o download. Disponível no servidor é:
PGP2.6ui de origem para máquinas unix
Executável da versão para PC de PGP 2.6 interface do usuário
Executável para MacPGP 2.3" [Sherry Mayo,
falar.política.crypto, 1994-09-06]
19.3.5. Servidores De Chaves
+ pgp-public-keys@demon.co.uk
- AJUDA na linha de assunto para obter mais informações sobre como
para usar
- pgp-public-keys@jpunix.com
+ pgp-public-keys@pgp.iastate.edu
- `ajuda" no assunto, para obter uma lista de servidores de chaves
[Michael Graff <explorer@iastate.edu> alt.segurança.pgp,
1994-07-04]
19.3.6. Reenvio De E-Mails De Sites
- Para mostrar active remetentes: dedo remailer@soda.berkeley.edu
19.3.7. E-Mail-para-Usenet gateways:
+ group.name@paris.ics.uci.edu
- group.name@cs.dal.ca

- group.name@ug.cs.dal.ca
- <compilado por Matthew J. Ghio, 4-18-94>
19.3.8. De Informação Do Governo
+ Califórnia Informação Legislativa
- "Você está convidado a procurar a nova edição da minha lista de
Internet com ligação directa e fontes de Califórnia governo
informações no URL:
www.cpsr.org/cpsr/states/california/cal_gov_info_FAQ.html
"[Chris Mays, comp.org.cpsr.falar, 1994-07-01]

+ NSA Informações
- Pode entrar na NSA/NCSC/NIST lista de discussão enviando para:
- csrc.nist.gov:/pub/nistpubs
19.3.9. Clipper Informações
+ http://www.mantis.co.uk/~mateus/
- algumas boas Clipper artigos e testemunho
19.3.10. Outros
+ ftp://furmint.nectar.cs.cmu.edu/security/README.html#taxes
- Vincent Cate
- http://www.acns.nwu.edu/surfpunk/
+ As Leis De Exportação
- "FEP membro do Conselho de administração e a Cygnus Support co-fundador João
Gilmore, tem de configurar uma página da World Wide Web em criptografia
problemas de exportação, incluindo informações sobre como solicitar
exportação, desembaraço, exchages com o Departamento de Comércio. na exportação
de licenciamento, documentos legais sobre problemas de rede no
com relação à exportação de tecnologia e de criptografia, e muito mais.
O URL é: http://www.cygnus.com/~gnu/export.html"
[Stanton McCandlish, mech@eff.org, 1994-04-21]
+ Inteiros grandes bibliotecas de matemática
- ripem.msu.edu <Marca Riordan, mrr@scss3.cl.msu.edu, de 4 a 8
94, sci.cripta>
- ftp:csn.org//mpj <Michael Paul Johnson, 4-8-94,
sci.cripta>
+ Phrack
arquivado em ftp.netsys.com
+ Bruce Sterling comentários em PCP
+ Bruce Sterling do discurso feito pelo "Computadores,
A liberdade e a Privacidade IV"
- conferência , Mar. 26 de 1994, em Chicago, estão agora on-line em
FEP:
- ftp://ftp.eff.org/pub/Publications/Bruce_Sterling/cfp_9
4_sterling.fala

- http://www.eff.org/pub/Publications/Bruce_Sterling/cfp_
94_sterling.fala
- gopher://gopher.fep.org/11/Publicações/Bruce_Sterling/
cfp_94_sterling.fala
- gopher.eff.org, 1/Publicações/Bruce_Sterling,
cfp_94_sterling.fala
- (fonte: Stanton McCandlish * mech@eff.org, 3-31-94)
19.3.11. Crypto artigos
- ftp.cs.uow.edu.au
pub/papers
- (quantum, outros, Siberry, etc.)
19.3.12. CPSR URL
- CPSR URL: http://www.cpsr.org/home

19.4. Apêndice -- Glossário
19.4.1. **Comentários**
- Nota de lançamento: lamento que eu ainda não tive tempo de adicionar muitos
novas entradas aqui. Há um monte de termos especializados, e
Eu provavelmente poderia ter dobrado o número de entradas aqui.
- Muito mais trabalho é necessário aqui. Na verdade, eu debatidas em um
ponto de fazer as perguntas frequentes, em vez disso, em uma espécie de "Encycopedia
Cypherpunkia," com uma mistura de curtos e longos artigos sobre
cada uma das centenas de tópicos. Tal organização seria
sofrer as desvantagens encontradas em quase todos os
lexicographically-organizado funciona: a confusão do
conceitos.
- Muitas dessas entradas foram compilados por um longo divulgação
no primeiro Cypherpunks reunião, setembro, 1992. Erros
estão obviamente presentes. Vou tentar corrigi-los
quando eu puder.
- Schneier "applied Cryptography" é claro, um excelente
lugar para procurar por termos, usos especiais, etc.
19.4.2. agoric sistemas-aberto, mercado livre, sistemas em que
voluntária transações são centrais.
19.4.3. Alice e Bob -- crypographic protocolos são muitas vezes feitas
mais claro, considerando as partes A e B, ou Alice e Bob,
executando algum protocolo. Eva o intruso, são Paulo
provador, e Vic o verificador são comuns stand-se em nomes.
19.4.4. ANDOS -- tudo ou nada revelação de segredos.
19.4.5. anônimo credencial -- uma credencial que defende algum direito
ou privilege ou fato, sem revelar a identidade do
titular. Isso é diferente de CA carteiras de motorista.
19.4.6. assymmetric cifra -- mesmo que criptosistema de chave pública.

19.4.7. autenticação-o processo de verificação de identidade ou
credencial, para se assegurar de que você disse que você era.
19.4.8. segurança biométrica -- um tipo de autenticação usando
impressões digitais, retina, exames, palma ou outros
físico/biológico assinaturas de um indivíduo.
19.4.9. pouco compromisso -- por exemplo, lançando uma moeda e, em seguida,
comprometendo-se a
o valor, sem ser capaz de alterar o resultado. O de blob
é uma primitiva criptográfica para esta.
19.4.10. BlackNet -- um regime experimental concebido por T. Maio
sublinhado a natureza das informações anônimas mercados. "Qualquer
e todos os" segredos podem ser oferecidos para venda através do anônimo
e-mails e mensagem de piscinas. O experimento foi transmitida através de
reenvio de e-mails para os Cypherpunks lista (não Pode) e daí para
várias dezenas de grupos da Usenet por Detweiler. As autoridades estão a
disse estar investigando-a.
19.4.11. cegueira, cego assinaturas -- Uma assinatura que o signatário
não lembro de ter feito. Um cego assinatura é sempre um
cooperativa de protocolo e o receptor da assinatura
fornece o signatário com a cegueira de informações.
19.4.12. blob -- criptografia equivalente a uma caixa fechada. Um
criptografia primitivo para pouco compromisso, com o
propriedades que um blobs podem representar um 0 ou um 1, o que os outros
não é possível dizer estar procurando se se trata de um 0 ou um 1, que o
criador do blob pode "abrir" o blob para revelar o
conteúdo, e que não blob, pode tanto ser um 1 e um 0. Um
exemplo disso é uma invertida de moeda coberto por uma mão.
19.4.13. BnD --
19.4.14. Capstone --
19.4.15. canal -- o caminho através do qual as mensagens são transmitidas.
Os canais podem ser seguro ou inseguro, e pode ter
os bisbilhoteiros (ou inimigos, ou desreguladores, etc.) que alter
mensagens, inserir e excluir mensagens, etc. Criptografia é
os meios pelos quais a comunicação através de canais inseguros são
protegido.
19.4.16. escolhido ataque de texto simples -- um ataque onde o criptoanalista
pode escolher o texto simples para ser cifrada, por exemplo, quando
a posse de um enciphering máquina ou algoritmo é no
a posse do criptoanalista.
19.4.17. cifra-um segredo formulário de redação, usando substituição ou
transposição de caracteres ou símbolos. (Do árabe "sifr,"
o significado de "nada".)
19.4.18. texto cifrado -- o plaintext depois que ele foi encriptado.

19.4.19. Clipper -- o infame Clipper chip
19.4.20. código -- um restrito criptosistema de onde as palavras ou letras de uma mensagem de são substituídas por outras palavras escolhidas a partir de um livro de códigos. Não faz parte do moderno criptologia, mas ainda útil.
19.4.21. moeda flippping -- um importante criptografia primitivo, ou do protocolo, em que o equivalente a jogar uma moeda boa é possível. Implementado com bolhas.
19.4.22. conluio -- em que vários participantes cooperam para deduzir a identidade de um remetente ou destinatário, ou para quebrar a cifra. Mais criptosistemas são sensíveis a algumas formas de conluio. Muito do trabalho sobre a implementação da DC Redes, por exemplo, consiste em assegurar que os colluders não conseguir isolar mensagem remetentes e, assim, rastreamento de origens e destinos de email.
19.4.23. Aplicações de comint --
19.4.24. computacionalmente seguro -- onde uma cifra não pode ser quebrado com disponibilidade de recursos do computador, mas, na teoria, pode ser quebrado com bastante recursos do computador. Contraste com incondicionalmente segura.
19.4.25. contramedida -- algo que você faz para impedir que um atacante
19.4.26. credencial -- fatos ou afirmações a respeito de alguma entidade. Para exemplo, as classificações de crédito, passaportes, reputação, status do imposto, registos de seguro, etc. Sob o sistema atual, estes as credenciais são cada vez mais sendo cruzada. Cego as assinaturas podem ser usados para criar credenciais anônimas.
19.4.27. credencial clearinghouse -- bancos, agências de crédito, as companhias de seguros, os departamentos de polícia, etc., que se correlacionam registros e decidir o status dos registros.
19.4.28. criptanálise -- métodos para atacar e quebrar cifras e relacionadas com sistemas criptográficos. Cifragem pode ser quebrada, tráfego podem ser analisados, e as senhas podem ser quebrado. Os computadores são essenciais.
19.4.29. crypto anarquia -- o sistema econômico e político, após o implantação de criptografia, rastreáveis e-mail, digital pseudônimos, criptografia de voto, e de dinheiro digital. Um trocadilho "criptografia", que significa "escondido", e como quando Gore Vidal chamado William F. Buckley um "crypto fascista."
19.4.30. criptografia-outro nome para criptografialogy.
19.4.31. criptologia-a ciência e o estudo de escrever, enviar, receber e decifrar mensagens secretas. Inclui autenticação, assinatura digital, a ocultação de mensagens (steganography), criptoanálise, e vários outros campos.
19.4.32. ciberespaço-eletrônico de domínio, as Redes, o computador-gerado espaços. Alguns dizem que é a "realidade consensual"

descrito em "Neuromancer." Outros dizem que é o telefone
do sistema. Outros têm trabalho a fazer.

19.4.33. DC protocolo, ou DC-Net -- o jantar métodos de criptografia de protocolo.
DC-Redes de usar vários participantes se comunicar com o controlador de domínio
o protocolo.

19.4.34. DES -- o Padrão de Criptografia de Dados, proposto em 1977 pelo
National Bureau of Standards (agora NIST), com a assistência de
a Agência de Segurança Nacional. Com base no "Lúcifer" cifra
desenvolvido por Horst Feistel na IBM, DES é uma chave secreta
criptosistema ciclos de blocos de 64 bits de dados por meio de
várias permutações com uma chave de 56 bits controlar a
de roteamento. "Difusão" e "confusão" são combinados para formar um
cifra que ainda não foi cryptanalyzed (ver "DES,
Segurança"). DES está em uso para transferências interbancárias, como um
cifra dentro de vários RSA-sistemas de base, e está disponível
para PCs.

19.4.35. DES, Segurança de -- muitos têm especulado que a NSA colocado
um alçapão (ou backdoor) em DES para permitir que ele leia DES-
mensagens criptografadas. Isso não foi provado. Ele é conhecido
que o original de Lúcifer algoritmo utilizado uma chave de 128 bits e
que este comprimento de chave foi reduzida para 64 bits (56 bits mais 8
bits de paridade), ths, tornando exaustiva pesquisa muito mais fácil (para
agora, como é conhecido, pesquisa de força bruta não foi feito, apesar de
ela deve ser viável hoje). Shamir e Bihan ter usado um
a técnica chamada de "a criptanálise diferencial" para reduzir o
busca exaustiva necessários para o escolhido ataques de texto simples (mas
sem importar para o comum DES).

19.4.36. a criptanálise diferencial -- o Shamir-Biham técnica para
cryptanalyzing DES. Com um escolhido ataque de texto simples, eles
reduziu-se o número de chaves DES de que deve ser julgado a partir de cerca de
2^56 a cerca de 2^47 ou menos. Note, no entanto, que raramente pode um
atacante montar um escolhido ataque de texto simples em DES sistemas.

19.4.37. dinheiro digital, digital de dinheiro-Protocolos para transferência de
valor, monetária ou outra, por via electrónica. Dinheiro Digital
geralmente refere-se a sistemas que são anônimos. Dinheiro Digital
os sistemas podem ser usadas para implementar qualquer quantidade que é
conservados, tais como pontos, massa, dólares, etc. Há
muitas variações de dinheiro digital sistemas, desde VISA
números para cegos assinado digital moedas. Um tópico muito grande
para uma única entrada de glossário.

19.4.38. digital pseudônimo -- basicamente, um "crypto identidade." Uma maneira
para os indivíduos para configurar as contas com várias organizações
sem revelar mais informações do que eles desejam. Os usuários podem

tem vários digital pseudônimos, alguns usado apenas uma vez, alguns utilizada durante muitos anos. Idealmente, o pseudônimo pode ser vinculado somente a vontade do titular. Na mais simples forma, uma chave pública pode servir como uma digital pseudônimo e precisa não estar vinculado a uma identidade física.

19.4.39. assinatura digital -- Análoga à assinatura autógrafa em um documento. Uma modificação de uma mensagem que só o assinante pode fazer, mas que todos podem se reconhecer. Pode ser usado legalmente ao contrato à distância.

19.4.40. digital de registro de data e hora -- a função de um cartório digital público, no qual alguns mensagem (uma música, roteiro, laboratório de notebook, contrato, etc.) é marcado com um tempo que não pode (facilmente) ser forjado.

19.4.41. jantar métodos de criptografia de protocolo (aka DC protocolo, DC redes) -- untraceable sistema de envio de mensagem inventado por David Chaum. Nomeado após o "jantar dos filósofos" problema no ciência da computação, os participantes formam circuitos e passar mensagens de tal forma que a origem não pode ser deduzido, restrição de conluio. No nível mais simples, os dois participantes compartilhar uma chave entre eles. Um deles envia algumas real mensagem por bit a bit ORing exclusivo a mensagem com a chave, enquanto a outra apenas envia a chave em si. Real mensagem de este par de participantes é obtido por XORing as duas saídas. No entanto, uma vez que ninguém, mas o par sabe o a chave do original, a mensagem não pode ser atribuída a qualquer um dos participantes.

19.4.42. logaritmo discreto problema -- dado inteiros a, n, e x, encontrar algum inteiro m tal que um^m mod n = x, se m existe. A exponenciação Modular, a um^m mod n parte, é simples (e de finalidade especial fichas estão disponíveis), mas o problema inverso é que se acredita ser muito difícil, em de modo geral. Assim, é conjeturado que a exponenciação modular é uma função unidirecional.

19.4.43. DSS, Padrão de Assinatura Digital -- o mais recente NIST (National Instituto de Padrões e Tecnologia, sucessor do RN) padrão para assinaturas digitais. Com base no El Gamal cifra, alguns o consideram fraco e pobre substituto para o RSA-com base esquemas de assinatura.

19.4.44. a espionagem, ou passivo escutas telefônicas -- interceptando mensagens sem detecção. As ondas de rádio podem ser interceptadas, linhas de telefone pode ser aproveitado, e os computadores, poderá ter de RF emissões detectadas. Ainda de fibra óptica pode ser aproveitado.

19.4.45. Caucionada Encryption Standard (EES) -- nome atual para o

chave do sistema de custódia conhecida também como Clipper, Clímax, Skipjack, etc.

19.4.46. factoring-Alguns números grandes são difíceis de fator. Ele é conjeturado que não há viável--por exemplo,"fácil," menos de exponencial no tamanho do número-- factoring métodos. É também um problema em aberto se o RSA pode ser quebrado mais facilmente que considerando o módulo de elasticidade (por exemplo, a chave pública pode revelar informações que simplifica o problema).
Curiosamente, apesar de factoring é acreditado para ser "duro", ele não se sabe se é na classe de problemas NP-difíceis.
Professor Janek inventou uma factoring dispositivo, mas ele é acredita-se ser de ficção.

19.4.47. HUMINT --

19.4.48. informações teórico-segurança -- "inquebrável" de segurança, em que nenhuma quantidade de criptoanálise pode quebrar uma cifra ou do sistema. Uma vez almofadas são um exemplo (desde que as almofadas são não perdeu nem roubado, nem utilizadas mais de uma vez, é claro). Mesmo como incondicionalmente segura.

19.4.49. chave -- um pedaço de informações necessárias para se cifran ou decifrar uma mensagem. As chaves podem ser roubado, comprado, perdidos, etc., assim como com teclas físicas.

19.4.50. troca de chave, ou a chave de distribuição, o processo de compartilhamento de um chave com alguma outra entidade, no caso de cifras simétricas, ou de distribuição de uma chave pública em uma cifra assimétrica. Um grande problema é que as teclas de ser trocadas de forma confiável e sem compromisso. Diffie e Hellman concebido como uma regime, com base no logaritmo discreto problema.

19.4.51. known-plaintext attack -- um segurança de uma cifra onde texto sem formatação-texto cifrado pares são conhecidos. Este ataque pesquisas para um desconhecido chave. O contraste com os escolhidos de texto sem formatação o ataque, onde o criptoanalista pode também escolher o plaintext para ser cifrada.

19.4.52. ouvir mensagens -- a NSA e outras agências de inteligência manutenção de sites para a intercepção de rádio, telefone e comunicações via satélite. E assim por diante. Muitos sites têm sido identificados (cf. Bamford), e muitos mais sites suspeitos.

19.4.53. mail, untraceable -- um sistema para envio e recebimento de email sem rastreabilidade ou relevância. Recepção de correio anônima pode ser feito com a transmissão do correio em de forma criptografada. Apenas o destinatário pretendido (cuja identidade, ou do nome verdadeiro, pode ser desconhecido para o remetente) pode capazes de decifrar a mensagem. Enviar email anonimamente, aparentemente, requer a mistura ou o uso do jantar criptógrafos (DC)

o protocolo.

19.4.54. Mensagem Piscina

19.4.55. mínimos de provas -- outro nome para conhecimento zero provas, favorecido por Chaum.

19.4.56. misturas -- David Chaum termo de uma caixa que executa o função de mistura, ou decorrelating, de entrada e de saída mensagens de correio eletrônico. A caixa também retira o exterior envelope (i.é., descriptografa com a sua chave privada) e remails a mensagem para o endereço no envelope interior. Tamper-resistente módulos podem ser utilizados para evitar a fraude e forçado a divulgação do mapeamento entre a entrada e saída de e-mail. Uma sequência de muitos remailings efetivamente faz o rastreamento enviar e receber impossível. Contraste isso com o versão do software, a DC protocolo. O "remetentes", desenvolvido por Cypherpunks são uma aproximação de um Chaumian mistura.

19.4.57. a exponenciação modular -- elevar um número inteiro para o poder de outro número inteiro, o modulo algum inteiro. Para números inteiros a, n, e m, um^m mod n. Por exemplo, 5^3 mod 100 = 25. Modular a exponenciação pode ser feito rapidamente, com uma sequência de pouco muda e acrescenta, e a finalidade especial de chips foram projetado. Ver também o logaritmo discreto.

19.4.58. Agência de Segurança nacional (NSA) -- a maior inteligência a agência, responsável por fazer e quebrar cifras, para a intercepção de comunicações, e para garantir a segurança da EUA computadores. Com sede em Fort Meade, Maryland, com muitas ouvir mensagens de todo o mundo. A ANS fundos criptografia de pesquisa e aconselha outras agências sobre criptografia matéria. A ANS, uma vez que, obviamente, tinha o mundo levando estudando criptografia, mas isso pode não ser o caso.

19.4.59. negativa de credencial -- uma credencial que você possui que você não quero ninguém para saber, por exemplo, uma falência depósito. Uma versão formal de uma reputação negativa.

19.4.60. NP-completo -- uma grande classe de problemas difíceis. "NP" significa não determinístico em tempo polinomial, uma classe de problemas de pensamento, em geral, não têm viável algoritmos para a sua solução. Um problema é "completo" se qualquer outro NP problema pode ser reduzido ao problema. Muitos importantes combinatória e algébrica problemas NP-completos: o problema do caixeiro viajante, o Hamiltoniano do ciclo de problema, o gráfico isomorfismo problema, o problema de palavras, e e em.

19.4.61. oblivious transfer -- uma primitiva criptográfica que envolve o probablistic de transmissão de bits. O remetente não

saber se os bits recebidos.
19.4.62. one-time pad-uma seqüência de caracteres de selecionados aleatoriamente bits ou símbolos
o que é combinado com uma mensagem de texto sem formatação para produzir o
cifrado. Esta combinação pode estar mudando algumas letras
quantidade, exclusivo lógico-Vermelho, etc.). O destinatário, que
também possui uma cópia de um time pad, pode facilmente recuperar os
texto sem formatação. Desde que o pad é utilizado apenas uma vez e, em seguida,
destruído, e não está disponível para um intruso, o
o sistema é perfeitamente seguro, por exemplo, é a informação-
teoricamente seguro. De distribuição de chaves (pad) é
obviamente, uma preocupação de ordem prática, mas considere a unidade de CD-ROM.
19.4.63. função unidirecional -- uma função que é fácil calcular em
uma direção, mas difíceis de encontrar qualquer inverso para, por exemplo, modular
a exponenciação, onde o problema inverso é conhecido como o
logaritmo discreto problema. Comparar o caso especial de armadilha
porta de funções unidirecionais. Um exemplo de uma operação unidirecional
é a multiplicação: é fácil multiplicar dois números primos
de 100 dígitos para produzir 200 dígitos do número, mas difícil
fator que 200 dígitos.
19.4.64. P ?=? NP-Certamente o mais importante problema sem solução
na teoria da complexidade. Se P = NP, então criptografia como sabemos
isso hoje não existe. Se P = NP, todos os problemas NP são
"fácil".
19.4.65. preenchimento -- o envio de mensagens extras para confundir os bisbilhoteiros
e para derrotar a análise de tráfego. Também a adição de bits aleatórios para
uma mensagem a ser cifrada.
19.4.66. PGP
19.4.67. texto simples -- também chamado de texto, o texto que está a ser
cifrado.
19.4.68. Piscina
19.4.69. PGP (Pretty Good Privacy) -- Phillip Zimmerman
a implementação do RSA, recentemente atualizado para a versão 2.0, com
componentes mais robustos e vários novos recursos. RSA Data
Segurança ameaçou PZ então ele não funciona mais sobre ele.
A versão 2.0 foi escrito por um consórcio de fora dos EUA hackers.
19.4.70. primeiro-números inteiros sem fatores outros que
si e o 1. O número de primos é ilimitada. Sobre
1% dos 100 dígito decimal números são primos. Desde lá
são cerca de 10^70 partículas no universo, há cerca de
10^23 100 dígitos primes para cada partícula no
universo!
19.4.71. probabalistic criptografia -- um esquema de Goldwasser, Micali,

e Blum, que permite que múltiplos textos cifrados para o mesmo
texto sem formatação, isto é, qualquer texto simples pode ter muitos
textos cifrados se a cifra é repetido. Isso protege
contra certos tipos de conhecidos ataques de texto cifrado em RSA.

19.4.72. provas de identidade, comprovando que você é, a sua verdadeira
nome, ou a sua identidade digital. Em geral, a posse de
tecla direita é prova suficiente (guarda a sua chave!). Alguns trabalhos
tem sido feito "é-uma-pessoa" credentialling agências, usando
o chamado Fiat-Shamir protocolo...pense nisso como uma forma
a questão unforgeable de passaportes digitais. A prova física de
identidade pode ser feito com segurança biométrica métodos. Zero
conhecimento, provas de identidade não revela nada além do fato de o
que a identidade é como alegado. Isto tem óbvias usa para
computador de acesso, senhas, etc.

19.4.73. protocolo-um procedimento formal para a resolução de algum problema.
Moderno criptologia é principalmente sobre o estudo de protocolos para
muitos problemas, tais como moeda-inversão de bit de compromisso (blobs),
provas de conhecimento zero de refeições, métodos de criptografia, e assim por diante.

19.4.74. chave pública -- a chave distribuído publicamente para potenciais
mensagem-os remetentes. Ele pode ser publicado em uma lista telefônica-como
diretório ou de outra forma de envio. Uma preocupação importante é a validade
esta chave pública para a proteção contra falsificação ou
representação.

19.4.75. criptosistema de chave pública -- o moderno avanço na
criptologia, projetado por Diffie e Hellman, com
contribuições de vários outros. Usa a porta da armadilha de uma forma
funções, de modo que a criptografia pode ser feito por qualquer pessoa com
o acesso ao "chave pública", mas a descodificação pode ser feita apenas por
o detentor da "chave privada." Abrange a chave pública
criptografia, assinaturas digitais, digital, dinheiro, e muitas outras
protocolos e aplicações.

19.4.76. criptografia de chave pública-o uso de modernas cryptologic
métodos para fornecida mensagem de segurança e autenticação. O
Algoritmo RSA é o mais amplamente utilizado formulário de chave pública
criptografia, embora outros sistemas existentes. A chave pública pode ser
livremente publicado, por exemplo, na lista telefônica-como diretórios, enquanto
a chave privada correspondente está muito bem guardado.

19.4.77. chave pública patentes -- M. I. T. e Stanford, devido ao trabalho
de Rivest, Shamir, Adleman, Diffie, Hellman e Merkle,
formado Chave Pública de Parceiros para licenciar os mais diversos públicos-chave,
assinatura digital RSA e patentes. Essas patentes, concedidas em
o início da década de 1980, expirar no entre 1998 e 2002. PKP tem
licenciado RSA Data Security Inc., de Redwood City, CA, que

alças de vendas, etc.

19.4.78. criptografia quântica-um sistema baseado em mecânica quântica princípios. Os bisbilhoteiros alterar o estado quântico do sistema e, portanto, são detectados. Desenvolvido por Brassard e Bennett, apenas pequenas demonstrações laboratoriais foram feitas.

19.4.79. remetentes -- versões de software de Chaum a "mistura" para o envio de untraceable mail. Vários recursos são necessários para fazer isso: estudo randomizado, a fim de reenvio, a criptografia em cada fase (escolhido antecipadamente pelo remetente, conhecer a cadeia de remetentes), preenchimento de tamanhos de mensagem. O primeiro foi reenvio de e-mails escrito por E. Hughes em perl, e cerca de uma dúzia ou assim são ativa agora, com diferentes conjuntos de recursos.

19.4.80. reputação -- a trilha de positivo e de negativo as associações e os juízos, que alguma entidade acumula. Crédito classificações, credenciais acadêmicas e confiabilidade são todos exemplos. Digital pseudônimo acumularão essas reputação credenciais baseado em ações, opiniões de outras pessoas, etc. No crypto anarquia, reputações e agoric sistemas de suma importância. Há muitos fascinante problemas de como a reputação baseada em sistemas de trabalho, como as credenciais podem ser comprados e vendidos, e assim por diante.

19.4.81. RSA -- o principal público do algoritmo de criptografia de chave, desenvolvido pela Ron Rivest, Adi Shamir, e Kenneth Adleman. Ele explora o dificuldade de fatoração de grandes números para criar uma chave privada e a chave pública. Inventado em 1978, ele continua a ser o núcleo de modernos sistemas de chave pública. Geralmente é muito mais lento do que O DES, mas a finalidade especial de exponenciação modular chips provavelmente acelerá-lo. Um esquema popular para a velocidade é usar o RSA para transmitir as chaves de sessão e, em seguida, uma alta velocidade de codificação, como DES para a real mensagem de texto.

- Descrição-Que p e q grandes primos, normalmente com mais de 100 dígitos. Seja n = pq e encontrar alguns e tais que e é relativamente primo a (p - 1)(q - 1). O conjunto de números p, q, e e é a chave privada RSA. O conjunto de números n e e formas de chave pública (lembre-se de que o conhecimento não é n suficiente para facilmente encontrar p e q...o factoring problema).

Uma mensagem M é criptografada através do cálculo de M^e mod n. O proprietário a chave privada pode decifrar a mensagem criptografada explorando teoria resultados, como se segue. Um número inteiro d é calculado de tal forma que ed =1 (mod (p - 1)(q - 1)). Euler provou um teorema que M^(ed) = M mod n e assim, M^(ed) mod n = M. Isto significa que, em algum sentido, os números inteiros e e d são "inversos" um do outro. [Se isso não está claro, por favor, consulte

um dos muitos textos e artigos sobre a chave pública
criptografia.]

19.4.82. criptosistema de chave secreta -- Um sistema que utiliza a mesma chave para criptografar e descriptografar o tráfego em cada extremidade de uma comunicação o link. Também chamado de simétrico ou de um sistema de chave. Contraste com o criptosistema de chave pública.

19.4.83. SIGINT --

19.4.84. smart cards-um chip de computador incorporado em cartão de crédito. Eles pode levar dinheiro, credenciais, chaves de criptografia, etc. Normalmente estes são construídos com algum grau de resistência a violações. Smart cartões pode executar parte de um cripto transação, ou todo ele. Realização de parte dela pode significar verificar os cálculos de um mais poderoso do computador, por exemplo, de um em um caixa eletrônico.

19.4.85. falsificação, ou mascaramento -- posando como outro usuário. Usado para roubar senhas, modificar arquivos, e roubando o dinheiro. Assinaturas digitais e outros métodos de autenticação são útil para evitar que isso. As chaves públicas devem ser validados e protegidos para assegurar que outros não subsititute seus próprios as chaves públicas das quais os usuários podem, em seguida, involuntariamente usar.

19.4.86. steganography -- uma parte da criptologia lidar com a esconder mensagens de e obscurecendo o que é o envio e recebimento de mensagens. Mensagem de tráfego é muitas vezes acolchoado para reduzir os sinais que caso contrário, iria vir de um súbito início de mensagens. "Coberto de escrita."

19.4.87. cifra simétrica -- mesmo que criptosistema de chave privada.

19.4.88. de violação de responder módulos, inviolável módulos (TRMs) -- caixas fechadas ou módulos que são difíceis de abrir, exigindo ampla sondagem e, geralmente, deixando amplas evidências de que o violação ocorreu. Várias técnicas de proteção são usados, tais como, especiais de um metal ou de óxido de camadas de batata frita, armored revestimentos, incorporado fibras ópticas, e de outras medidas destinadas a frustrar análise. Popularmente chamado de "à prova de adulteração caixas." Usa inclui: cartões inteligentes, armas nucleares iniciadores, chaves criptográficas de titulares de, caixas eletrônicos, etc.

19.4.89. a adulteração, ou active escutas telefônicas -- intefering com mensagens e, possivelmente modificando-os. Isso pode comprometer os dados segurança, ajudar a quebrar cifras, etc. Consulte também de falsificação.

19.4.90. Tessera

19.4.91. token-cerca de representação, tais como cartões de IDENTIFICAÇÃO, de metrô tokens, dinheiro, etc., que indica a posse de alguns propriedade ou valor.

19.4.92. análise de tráfego -- determinar quem está a enviar ou a receber mensagens de análise de pacotes, a frequência de pacotes, etc. Um

parte da steganography. Geralmente tratadas com o tráfego de preenchimento.
19.4.93. análise de tráfego -- identificar as características de uma mensagem
(tais como, remetente, ou o destino) monitorando o tráfego.
Remetentes e criptografia de ajuda para a folha de tráfego analysys.
19.4.94. as regras de transmissão -- os protocolos para determinar quem pode
enviar mensagens em um controlador de domínio do protocolo, e quando. Estas regras são
necessária para evitar a colisão e deliberada de interferência do
canais.
19.4.95. mensagens de trap -- dummy mensagens em DC Redes que são utilizados para
pegar jammers e perturbadores. As mensagens contêm nenhum privado
informações e são publicados em um blob de antemão de modo que
a mensagem de trap pode mais tarde ser aberta para revelar o disruptor.
(Existem muitas estratégias para explorar aqui.)
19.4.96. armadilha de-porta-Em criptografia, um pedaço de informações secretas
que permite que o titular de uma chave privada para inverter normalmente
difícil de inverter a função.
19.4.97. armadilha-porta de uma maneira funções -- funções que são de fácil
computação em avançar e direção inversa, mas para
que a divulgação de um algoritmo para calcular a função de
na direção não fornece informações sobre como
para calcular a função, no sentido inverso. Mais simplesmente
colocar, trap-porta de uma maneira funções são um caminho para todos, mas a
titular de informações secretas. O algoritmo RSA é o
exemplo mais conhecido de uma função.
19.4.98. incondicional de segurança -- mesmo que informação teórica-
de segurança, que é, inquebrável, exceto por perda ou roubo dos
chave.
19.4.99. incondicionalmente segura, onde nenhuma quantidade de interceptado
texto cifrado é suficiente para permitir a codificação para ser quebrado, como
com o uso de uma almofada de um tempo de codificação. Contraste com
computacionalmente seguro.
19.4.100. URLs
19.4.101. de votação, de criptografia -- Vários esquemas têm sido desenvolvidos
por anônimo, untraceable de voto. Votação esquemas deve ter
várias propriedades: a privacidade dos votos, a segurança do voto
(sem votos múltiplos), robustez contra ruptura por jammer
ou desreguladores, verificabilidade (eleitor tem confiança no
resultados), e a eficiência.
19.4.102. Denunciantes
19.4.103. provas de conhecimento zero -- provas em que o não conhecimento do
prova real é transmitida. Peggy o Provador demonstra a
Sid o Cético que ela é, de fato, na posse de alguns
parte do conhecimento sem, na verdade, revelando que

conhecimento. Isso é útil para o acesso a computadores, porque
os bisbilhoteiros ou desonesto sysops não pode roubar o conhecimento
dado. Também chamado mínimos de provas. Útil para
provando a posse de alguma propriedade, ou de credenciais, tais como
idade ou estado de voto, sem revelar informações pessoais.

19.5. Apêndice -- Resumo da Criptografia Versões
19.5.1. DOS e Windows
- SecureDevice
+ SecureDrive
- "Secdrv13d é a versão mais recente. Houve um unupdated
.arquivo exe no pacote que tinha de ser corrigido. Do
arquivo readme: Se você achou este arquivo dentro FPART13D.ZIP,
esta é uma atualização e correção de bugs para o FPART utilitário de
SecureDrive Versão 1.3 d,
- Edgar Swank envolvidos?
+ SecureDevice
- Versões Principais:
- Funções:
- Principais Autores:
- Principais Plataformas:
+ Onde Encontrar:
- ftp://ftp.csn.org/mpj/I_will_not_export/crypto_???????/
secdrv/secdev.arj
Ver ftp://ftp.csn.org/mpj/README.MPJ para o ???????
- Pontos fortes:
- Pontos fracos:
+ Notas:
- A propósito, eu não sou o único que fica SecureDrive
e SecureDevice confuso. Atente para isto.
+ SFS
- "Um MS-DOS-based pacote de criptografia de disco rígido. É
implementado como um driver de dispositivo e criptografa um todo
partição (por exemplo, não é um arquivo ou um diretório). Ele usa o
MDC/SHA cifra. ... Ele está disponível a partir Grabo
(garbo.uwasa.fi:/pc/crypt/sfs110.zip, eu acho), e também
a partir de nosso site de ftp: ftp.informatik.uni-
oportunidades de hotéis de hamburgo.de:/pub/virus/crypt/disk/sfs110.zip gostaria de
recomendo o Garbo site, porque a nossa é um pouco lento."
[Vesselin Bontchev, alt.segurança.pgp, 1994-09-05]
- Em comparação com SecureDrive, os usuários relatam que, para ser mais rápido,
melhor destaque, tem uma interface do Windows, é um dispositivo de
driver, e é robusto. As desvantagens são que ele

atualmente não é fornecido com o código-fonte e usa um mais
obscuro de codificação.
- "SFS (Secure sistema de arquivos) é um conjunto de programas que
criar e gerenciar um número de volumes de disco criptografada, e
é executado em ms-DOS e do Windows. Cada volume é apresentado como
um DOS normal de unidade, mas de todos os dados armazenados nele é encryped
no nível individual-nível de setor....SFS 1.1 é um
versão de manutenção que corrige alguns pequenos problemas no
1.0, e adiciona uma série de funcionalidades sugeridas pelos usuários.
Mais detalhes sobre as alterações são dadas no arquivo leia-me."
[Peter Gutmann, sci.cripta, 1994-08-25]
- "a partir de garbo.uwasa.fi gratuito e de todos os seus sites espelhos em todo o mundo
como o /pc/crypt/sfs110.zip."
+ WinCrypt.
- "WinCrypt é muito bom SE você manter o seu texto criptografado
a menos que o comprimento de sua senha, E SE você
gerar sua senha aleatoriamente, E SE você só usar cada
senha uma VEZ. :-)" [Michael Paul Johnson, sci.cripta,
1994-07-08]
+ Ganhar PGP
+ parece haver dois idêntico programas:
- WinPGP, por Christopher w. Geib
+ WinPGP, por Timothy M. Janke e Geoffrey C. Grabow
- ftp WinPGP 1.0
carvalho.oakland.edu//pub/msdos/windows3/WinPGP10.ZIP
- Até que isso seja esclarecido...
+ PGPShell
- "PGPShell v3.2 já foi lançado e está disponível em
estes sites: (EUA)
carvalho.oakland.edu:/pub/msdos/security/pgpshe32.zip
(Euro)
ftp.demon.co.uk:/simtel20/msdos/security/pgpshe32.zip
[still@rintintin.Colorado.EDU (Johannes Kepler), 1994-07-
07]
+ PGS
- ftp.informatik.uni-
oportunidades de hotéis de hamburgo.de:/pub/virus/crypt/pgp/shells/pgs099b.zip
- "Eu só carregado a correção do bug de PGS (v0.99b) em alguns FTP-
sites:
wuarchive.wustl.edu:/pub/msdos_uploads/pgs/pgs099b.zip
rzsun2.informatik.uni-oportunidades de hotéis de hamburgo.de:/pub/vírus/crypt/pgp/...
(Uploaded apenas ele, deve ser em poucos dias)
carvalho.oakland.edu:/SimTel/msdos/security/pgs099b.zip (Apenas

carregou-o, deverá ser em poucos dias)

[Eelco Cramer <crame001@hio.tem.nhl.nl>, 1994-06-27]
+ DOS criptografia de disco utilitários
+ Vários livre ou quase livre utilitários estão disponíveis:
- ftp.informatik.uni-hamburg.de:/pub/virus/crypt/disk/
[Vesselin Vladimirov Bontchev, como de 1994-08]
+ Norton "Diskreet" é fraco e essencialmente inútil
- usa DES fraca (BCE) de modo...é, provavelmente, a "serpente
óleo" que Zimmermann escreve sobre sua docs. SFS docs
dizem que é ainda pior do que isso.
+ PGS
- "PÁGS v0.99c está lá fora!

Esta nova versão do PÁGS suporta 8 bytes keyid s.
Esta versão irá ser capaz de executar em um OS/2, DOS,.

PGS v0.99c está disponível no seguinte site:
wuarchive.wustl.edu:/pub/msdos_uploads/pgs/pgs099c.zip"
[ER CRAMER <crame001@hio.tem.nhl.nl>, 1994-07-08]

+ Programa:
- Versões Principais:
- Funções:
- Principais Autores:
- Principais Plataformas:
- Onde Encontrar:
- Pontos fortes:
- Pontos fracos:
- Notas:

19.5.2. OS/2

19.5.3. Amiga

+ Programa: PGPAmiga, Amiga, PGP
+ Versões principais: 2.3.4, PGP 2.6
- "Amiga equivalente de PGP 2.6 interface do usuário é chamado PGP
2.3.3" [desconhecido comentarista]
- Funções:
- Principais Autores:
- Principais Plataformas:
- Onde Encontrar:
- Pontos fortes:
- Pontos fracos:

- Notas: a Situação é confusa. 2.3.3 não é equivalente
para PGP 2.6 interface do usuário.
19.5.4. Unix
- NeXTStep
- Sol 4.3
- Solaris
- PS
- SGI
+ deslize
- Metzger: João Ioannidis " swIPe pacote, e foi
não apenas anunciou
mas liberado. Phil tem feito um pacote semelhante para KA9Q
e foi um dos
19.5.5. SFS ?
- "Um MS-DOS-based pacote de criptografia de disco rígido. É
implementado como um driver de dispositivo e criptografa um todo
partição (por exemplo, não é um arquivo ou um diretório). Ele usa o
MDC/SHA cifra. ... Ele está disponível a partir Grabo
(garbo.uwasa.fi:/pc/crypt/sfs110.zip, eu acho), e também
a partir de nosso site de ftp: ftp.informatik.uni-
oportunidades de hotéis de hamburgo.de:/pub/virus/crypt/disk/sfs110.zip gostaria de
recomendo o Garbo site, porque a nossa é um pouco lento."
[Vesselin Bontchev, alt.segurança.pgp, 1994-09-05]
19.5.6. Macintosh
+ mais sobre MacPGP
- A partir de: phinely@uhunix.uhcc.Hawaii.Edu (Pedro Hinely)
Assunto: Re: MacPGP 2.6 interface do usuário não funciona
Message-ID: <CsI3wr.I3B@news.Hawaii.Edu>
Remetente: news@news.Hawaii.Edu
Organização: Universidade do Havaí
Referências: <m0qJqLD-001JKsC@sunforest.mantis.co.uk>
Data: Quarta-feira, 6 de Julho de 1994, 04:17:15 GMT
Linhas: 9

No artigo <m0qJqLD-001JKsC@sunforest.mantis.co.uk>
mateus@stallman.louva-a-deus.co.reino unido (mateus em casa), escreve:
>Bem, eu baixei o rumor de MacPGP 2.6 interface do usuário, mas, infelizmente,
ele bombas de fora
>imediatamente com um endereço de erro quando eu tento executá-lo.

MacPGP 2.6 interface funciona no meu Quadra 605.
MacBinary processo não consegue processar nomes de caminho >63
caracteres, mas a longo

um encriptar ficheiros na área de trabalho, ele não é muito de
um problema.
- A partir de: warlord@MIT.EDU (Derek Atkins)
Grupos de notícias: alt.segurança.pgp
Assunto: Re: Quando haverá uma correção de bug para MacPGP?
Followup-To: alt.segurança.pgp
Data: 6 de Julho de 1994, 10:19:13 GMT
Organização: Instituto de Tecnologia de Massachusetts
Linhas: 19
Message-ID: <WARLORD.94Jul6061917@toxicwaste.mit.edu>
Referências: <AWILSON-020794082446@ts7-57.upenn.edu>
NNTP Anfitrião de registo: toxicwaste.media.mit.edu
Em resposta a: AWILSON@DRUNIVAC.DREW.EDU's mensagem do 2 de Julho
1994 12:25:14 GMT

No artigo <AWILSON-020794082446@ts7-57.upenn.edu>
AWILSON@DRUNIVAC.DREW.EDU (AL WILSON) escreve:

Quando haverá uma correção de bug para MacPGP (1.1.1)? Eu sou
não reclamando, eu
sabemos que o software é livre. Eu só quero começar
utiliza-lo para
comunicações o mais cedo possível.

Há ainda uma série de bugs que precisam
ser
fixo, mas a esperança é a de fazer uma correção de bugs de lançamento no
perto
futuro. Eu não sei quando é que vai ser, mas
espero que
ele vai ser Real, Logo Agora (TM).
- Data: Wed, 6 De Julho De 1994, 10:42:08 -0700
A partir de: tcmay (Timothy C. de Maio)
Para: tcmay
Assunto: (fwd) Re: Qual é a diferença entre 2.6 &
2.6 interface do usuário?
Grupos de notícias: alt.segurança.pgp
Organização: NETCOM Na linha de Serviços de Comunicação (408
261-4700 convidado)
Status: S

Xref: netcom.com alt.segurança.pgp:16979
Caminho: netcom.com!netcomsv!decwrl!lll-

winken.llnl.gov!sol.ctr.columbia.edu!howland.reston.a ans.n
et!pipex!lyra.csx.cam.ac.reino unido!iwj10
A partir de: iwj10@cus.cam.ac.uk (Ian Jackson)
Grupos de notícias: alt.segurança.pgp
Assunto: Re: Qual é a diferença entre 2.6 e 2.6 interface do usuário?
Data: Quarta-feira, 6 de Julho de 1994, 10:14:24 GMT
Organização: Linux Ilimitada
Linhas: 55
ID de mensagem:
<1994Jul6.101424.9203.chiark.ijackson@nyx.cs.du.edu>
Referências: <CsE3CC.Gqz@crash.cts.com>
<RATINOX.94Jul3221136@delphi.ccs.neu.edu>
NNTP de Host de Postagem: bootes.cus.cam.ac.reino unido
Resumo: o Uso 2.6 interface do usuário :-).
Cedente: iwj10@bootes.cus.cam.ac.uk

-----BEGIN PGP MENSAGEM ASSINADA-----

No artigo <RATINOX.94Jul3221136@delphi.ccs.neu.edu>,
De Aço inoxidável Rat <ratinox@ccs.neu.edu> escreveu:
>Ed Dantes <edantes@crash.cts.com> escreve [citar
normalizou - iwj]:
>> linha de assunto diz tudo.
>
>PGP 2.6 é distribuído a partir do MIT e está legalmente disponível
para EUA e Canadá
>moradores. Ele usa a RSAREF biblioteca. Ele possui um código que
vai impedir
>interoperação com versões anteriores de PGP.
>
>PGP 2.6 interface do usuário é uma versão modificada do PGP 2.3 um que
funções quase
>idêntico ao MIT PGP 2.6, sem o "aleijado"código de
do MIT PGP 2.6. Ele
>está legalmente disponível fora os EUA e o Canadá apenas.

Isto é falso. PGP 2.6 interface de usuário está disponível para EUA e Canadá
residentes.
É definitivamente legal para tais pessoas para fazer o download do PGP
2.6 interface do usuário e o estudo
isso.

No entanto, RSADSI alegação de que *o uso* PGP 2.6 interface do usuário NOS eua

e Canadá
viola suas patentes do algoritmo RSA e em público
chave
criptografia em geral. Outras pessoas (como eu)
acredito que
essas patentes não iria ficar até se testado no tribunal, e
que, em qualquer
caso os danos recuperáveis seria zero.

Você também pode gostar de saber que os formatos de saída
gerado pelo 2.6 interface do usuário
e o MIT-2.6 são idênticos, de modo que, se você escolher usar
2.6 interface do usuário do Norte
América ninguém será capaz de dizer a diferença.

Infelizmente, esses problemas de patentes tem causado muitos
América Do Norte
Sites FTP para parar de realizar 2.3 e 2.6 interface do usuário, por medo de
cometer
contributivas violação.

Se você gostaria de analisar PGP 2.3 a 2.6 ou ui, eles são
disponível em
muitos sites de FTP. Tente
o preto.boi.ac.reino unido:/src/segurança
ftp.demônio.co.reino unido:/pub/pgp
ftp.dsi.unimi.ele:/pub/security/crypt/PGP
ftp.funet.fi gratuito:/pub/cripta
para acionadores de partida. Olhar para as postagens regulares aqui no
alt.segurança.pgp para outros sites.

-----BEGIN PGP SIGNATURE-----
Versão: 2.6

iQCVAgUBLhqD48MWjroj9a3bAQH9VgQAqovcvxqjlhnfvskfr82m5808h
6GKY5RW
SZ1/YLmshlDEMgeab4pSLSz+lDvsox2KFxQkP7O3oWYnswXcdr4FdLBu/
TXU+IQw
E4r/jY/IXSupP97Lxj9BB73TkJlHVmrqgoPQG2Nszj60cbe/LsiGs5uMn
CSESypH
c0Y8FnR64gc=
=Pejo
-----END PGP SIGNATURE-----

--
Ian Jackson, em casa <ijackson@nyx.cs.du.edu> ou
<iwj10@cus.cam.ac.uk>
+44 223 575512 Escoerea no IRC.
http://www.cl.cam.ac.uk/users/iwj10/
2 Lexington Fechar, Cambridge, CB4 3LS, Inglaterra. Urgente:
<iwj@cam-orl.co.uk>

--
.....
.....
Timothy C. Maio | Crypto Anarquia: criptografia,
dinheiro digital,
tcmay@netcom.com anônimo | redes digitais
pseudônimos, zero
408-688-5409 | conhecimento, reputação,
informação de mercados,
W. A. S. T. E.: Aptos, CA | preto mercados, o colapso da
governos.
De consumo de Energia superior: 2^859433 | Chave Pública: PGP e MailSafe
disponível.
"As fronteiras nacionais estão apenas de redutores de velocidade nas informações
auto-estrada."

+ CurveEncrypt, para Mac
- "Curva de Criptografar 1.1, a IDÉIA de criptografia para o Macintosh é
agora disponível.....Curva de Criptografar é um freeware de arrastar-e-
queda de criptografia de aplicações para o Macintosh. Ele usa
A IDÉIA de codificação-modo de realimentação com uma de 255 caracteres passar
frase, criptografa os dados e bifurcações de recursos de
arquivos, e irá encriptar o conteúdo de uma pasta ou
volume em uma única operação. O código fonte é fornecido,
natch. CE é o Sistema 7....(Observe que este programa tem
nada a ver com a curva elíptica
métodos de encriptação, apenas para que ninguém fica confuso...)" [
"W. Kinney" <kinney@bogart.Colorado.EDU>, 1994-07-08]
- "Sites Ftp:

ripem.msu.edu:pub/crypt/outros/curva-criptografar-ideia-para-mac/
Este é um produto de exportação controlado site ftp: leitura

pub/crypt/GETTING_ACCESS para
informações.

ftp.a csn.org:/mpj/I_will_not_export/crypto_???????/curve_e
ncrypt/
a csn.org é também de exportação controlada: leitura /mpj/README para
os caracteres
para substituir ???????." ["W. Kinney"
<kinney@bogart.Colorado.EDU>, 1994-07-08]
+ RIPEM no Macintosh
- Carl Ellison diz: "eu só usei RIPEM AOL -- mas
deve ser o mesmo....Eu executado em um Mac, gerando o
blindados arquivo e, em seguida, usar o AOL, "colar de arquivo" opção
no menu Arquivo para incluir o arquivo criptografado no
o corpo da mensagem.....Em outra direção, eu tenho que
use Selecionar Tudo e Copiar para tirá-lo do AOL mail, Cole
para obtê-lo em um editor. A partir daí eu posso arquivo e
dar a esse arquivo para PGP ou RIPEM.....BBEDIT no Mac tem
bom apoio para RIPEM. Eu gostaria de saber como escrever
BBEDIT extensões para Mac PGP bem." [C. E., 1994-07-
06]
+ URL para Stego (Macintosh)
- http://www.nitv.net/~mech/Romana/stego.html
19.5.7. Newton
19.5.8. Atari
19.5.9. VMS
19.5.10. IBM VM/etc.
19.5.11. Diversos
19.5.12. Divisão de ficheiro de utilitários
+ Vários existe.
- XSPLIT
- cryptosplit, Ray Cromwell
- sombra

19.6. Apêndice -- Referências
19.6.1. a importância das bibliotecas
- "O uso de uma biblioteca. É um lugar com um monte de papel
periódicos e livros de papel. Materiais de biblioteca on-line não,
a maioria, mas ainda é onde a maioria do mundo codificado
o conhecimento é armazenado. Se você não gosta de papel, resistente.
Essa é a maneira como o mundo está agora." [Eric Hughes, 1994-
04-07]
19.6.2. Livros

- Bamford, James, "The Puzzle Palace," De 1982. O seminal
de referência a NSA.
- N. Koblitz, "Um curso de teoria dos números e criptografia",
QA3.G7NO.114. Muito técnico, com ênfase na elī
funções.
+ D. Galês, "Códigos e Criptografia", Oxford Science
Publicações, 1988, Eric Hughes especialmente
recomenda isso.
- Z103.W461988
- D. E. Denning, "Criptografia e Segurança de Dados", de 1982,
Addison-Wesley, 1982, QA76.9.A25D46. Um clássico, se um pouco
datada de, introdução, por parte da mulher, que mais tarde tornou-se o chefe
torcedor do Clipper.
+ G. Brassard, "Moderno Criptologia: a tutorial", Lecture Notes
no Computador
- Ciência 325, Springer de 1988, QA76.L4V.325 Um pouco magro
livro que é uma jóia. Seções por David Chaum.
- Vinge, V., "Verdadeiros Nomes", De 1981. Um romance sobre o digital
pseudônimos e ciberespaço.
- Cartão de Orson Scott, "Ender do Jogo", 1985-6. Romance sobre crianças
quem adotar digital pseudônimos para o debate político.
- G. J. Simmons,"Contemporânea Criptologia", IEEE Press, 1992,
QA76.9.A25C6678. Uma coletânea de artigos escritos por conhecidos
especialistas. Surpreendentemente, nenhuma discussão sobre dinheiro digital. Gus
Simmons projetado "Permissiva Links de Ação" para armas nucleares, em
Sandia.

19.6.3. sci.cripta

arquivado em ripem.msu.edu e rpub.cl.msu.edu
-
+ A criptografia anon arquivo ftp no
wimsey.bc.ac:/pub/crypto
- foi movido para ftp.wimsey.bc.ca

19.6.4. criptografia-faq

- em cerca de 10 peças, colocar para fora pela Cripta Cabal (vários
Cypherpunks sobre ele)
- rtfm.mit.edu em /pub/usenet/news.respostas/criptografia-
faq/parte[xx]
+ postado a cada 21 dias para o sci.cripta, falar.política.crypto,
- sci.respostas, notícias.respostas

19.6.5. RSA FAQ

- Paulo Farias, RSA Laboratories
- FTP anônimo da rsa.com:/pub/faq
- rtfm.mit.edu, /pub/usenet/news.respostas/criptografia-faq/rsa

19.6.6. Computadores, a Liberdade e a Privacidade de Conferência
- Computadores seguinte, a Liberdade e a Privacidade Conferência será
De Março De 1995, Em São Francisco
19.6.7. Várias computador de segurança de documentos, publicações e programas de
pode ser encontrado em cert.org.
- ftp anônimo para ele e olhar em /pub. /pub/info ainda tem
a ANS "Livro de Laranja." (Não é um segredo, obviamente. Qualquer pessoa pode
obter a NSA/NCSC lista de correio e obter uma enorme pilha de
documentos enviados a eles, com os novos que chegam a cada
várias semanas.)
- ou tentar ftp.win.tue.nl /pub/security
19.6.8. Clipper informações pela Internet
- ftp.cpsr.org
- ftp.eff.org

19.7. Glossário Itens
19.7.1. mensagem de piscinas --
19.7.2. piscinas-veja "mensagem de piscinas."
19.7.3. tampa de tráfego --
19.7.4. estofamento-veja "mensagem de preenchimento."
19.7.5. mensagem preenchimento --
19.7.6. latência --
19.7.7. BlackNet -- uma experiência em mercados de informação, utilizando
anônimo mensagem de piscinas para a troca de instruções e
itens. Tim Poderá experiência de guerrilha ontologia.
19.7.8. ILF-Informações da Frente de Libertação. Distribui direitos autorais
material através de remetentes, de forma anônima. Outra experiência
guerrilha ontologia.
19.7.9. mistura digital --
19.7.10. FinCEN -- Crimes Financeiros De Aplicação De Rede.
19.7.11. nome verdadeiro -- de fato, o nome físico. Tomadas de Vernor
Vinge do romance com o mesmo nome.
19.7.12. misture --
19.7.13. TEMPESTADE --
19.7.14. OTP --
19.7.15. Cifra de Vernam --
19.7.16. detweiler -- verbo, a reclamar e a delirar com tentáculos que são
destruindo um a sanidade através de criptografia pensamento anarquista
o controle. Nomeado após L. Detweiler. "Ele é apenas detweilering."
19.7.17. reenvio de e-mails --
19.7.18. --Stego
19.7.19. incipits -- mensagem de indicadores ou tags (relaciona-se com a stego)
19.7.20. coação código -- uma segunda chave que pode descriptografar uma mensagem para

algo inofensivo. Poderia ser útil para cartões de banco, bem
como para evitar a incriminação. Uma forma de segurança através de
obscuridade, e não é amplamente usado.

19.8. Um comentário sobre versões de software, sites ftp, instruções, etc.
19.8.1. Eu lamento que eu não possa ser concluída em todas as versões, plataformas
suporte, sites para obter instruções,
incompatibilidades, etc. Francamente, eu estou afogando-se em relatórios de
novas versões, questões sobre o uso, etc. A maioria destes
versões eu não tenho conhecimento direto de, não tenho experiência
com e sem a apreciação do sutil incompatibilites
envolvidos.
19.8.2. Há outros que têm-se concentrado em fornecer
data de relatórios sobre o que está disponível. Alguns deles são"
- site
19.8.3. Leitura sci.cripta, alt.segurança.pgp e grupos relacionados, para um
poucas semanas e olhando para programas de interesse para a própria
situação deve dar mais recentes e resultados atuais.
As coisas estão se movendo rapidamente, por isso, se está interessado em
"AmigaPGP", por exemplo, então o lugar certo para o
versões mais recentes, é nos grupos que acabamos de mencionar, ou em grupos de
e ftp sites específicos para a Amiga. (Tenha cuidado para que
sabotado falsificado ou versões não são usados, como em todos os criptografia.
"Joe AmigaPGP" pode precisar de um olhar mais atento.)

20. Leia-me

20.1. direitos autorais
O CYPHERNOMICON: Cypherpunks FAQ e Mais, Versão 0.666,
1994-09-10, Direitos De Autor Timothy C. De Maio. Todos os direitos reservados.
Veja os detalhes de isenção de responsabilidade. Use seções curtas em "justo
use" disposições, com crédito apropriado, mas não coloque o seu
nome em minhas palavras.

20.2. LEIA-ME--BREVE VERSÃO
20.2.1. Direitos De Autor Timothy C. De Maio. Todos os direitos reservados. Para o que é
a pena.
20.2.2. Desculpas antecipadamente para a mistura de estilos (estrutura de tópicos, bala,
texto, ensaios), por fragmentos incompletos e seções. Este
FAQ é já demasiado longo e detalhado, e a escrita
adequado conjuntivo material, apresentações, resumos, etc.
não está nos cartões em breve. Ir com o fluxo, use o
texto ferramentas de busca, e lidar com ele.

20.2.3. Substantivo correções de boas-vindas, sofismas menos bem-vindo, e debate ideológico ainda menos bem-vindo. Correções para desatualizado informações, especialmente sobre ponteiros para informações, será o mais apreciado.

20.3. Copyright Comentários

20.3.1. Pode parecer ilógico para um Cypherpunk afirmar algum tipo de direitos de autor. Talvez. Mas a minha principal preocupação é a facilidade com o que as pessoas podem mudar a legenda documentos como os seus próprios, por vezes, após a adição de algumas palavras aqui e ali.

20.3.2. Sim, eu usei as palavras de outros lugares, para fazer pontos melhor do que eu senti minhas próprias palavras, para poupar tempo, e para dar aos leitores uma voz diferente de falar sobre problemas. Eu creditado cotações com um "[Joe Foobar, local, data] atribuição, geralmente no final da citação. Se um lugar é não listado, é o Cypherpunks própria lista. O autor e a data deve ser suficiente para (um dia) recuperar a origem texto. A propósito, eu usei aspas como eles pareciam adequadas, e não declarações de que os pontos cotados são necessariamente original para o autor, que pode ter lembrou-los a partir de em outro lugar-ou que a data listada é a origem data para o ponto. Tenho algo como 80 megabytes de Cypherpunks posts, então eu não poderia fazer uma escavação arqueológica para a primeira menção de uma ideia.

20.3.3. As pessoas podem citar este FAQ em "fair use" provisões, por exemplo, um parágrafo ou dois, com créditos. Nada mais do que um alguns parágrafos constitui violação de direitos autorais, como eu compreendê-lo.

20.3.4 reunião. Devo desistir de manter este FAQ e/ou deve outros se envolver, então o normal, co-autoria e a herança de regime vai ser possível.

20.3.5. A Web. WWW e Mosaico de oferecer incrível novas oportunidades para documentos on-line. Na verdade, é provável que este FAQ será disponível como um documento da Web. Minha preocupação, no entanto, é que o integridade e autoria de ser mantida. Assim, dividindo-se o documento em centenas de pequenos pedaços, sem autoria anexado, não seria legal. Também, minha intenção manter este documento com o meu poderosas ferramentas de estrutura de tópicos (Symantec, o "MAIS" em um Macintosh) e, assim, qualquer pessoa que "congela" o documento e usa-lo como base para os links, ponteiros, etc., vai ser deixado para trás como mods são feitos.

20.4. Algumas Palavras sobre o Estilo

20.4.1. Algumas seções são em forma de estrutura de tópicos
- como este
- com fragmentos de ideias e de pontos
- com frases incompletas
- e com listas de pontos que são, obviamente, apenas começando
pontos para mais completas análises
20.4.2. Outras seções estão escritos no mais completo ensaio de formulário, como
razoavelmente auto-contido análises de algum ponto ou tópico.
Como este. Alguns destes ensaios foram retirados directamente do
as postagens que eu fiz para a lista ou para o sci.cripta, e não
atribuição H (desde que eu escrevi as coisas...as cotações dos outros
são creditados).
20.4.3. Os estilos podem confronto, mas eu simplesmente não tenho a centenas de
horas para percorrer e para "regularizar" tudo para uma
estilo coerente. O estilo de estrutura de tópicos permite que mais pontos,
rugas, refutações, e elaborações para ser levadas facilmente
(se não sempre elegantemente). Espero que mais leitores possam entender
isso e aprender a lidar com isso.
20.4.4. É claro que há lugares onde os pontos são apenas
muito fragmentária, muito outlinish, para as pessoas a fazer sentido.
Eu já tentei limpá-las o máximo que posso, mas não vai
sempre ser alguns lugares onde a idéia parecia claro para mim o
tempo (talvez não), mas que não é apresentado de forma clara para
outros. Eu vou continuar tentando ferro estas torções no futuro
versões.
20.4.5. Comentário sobre estilo
- Em muitos casos eu unidas duas ou mais blocos de idéias em uma
seção, resultando, em muitos casos, em incompatível escrita
estilos, tempos, etc. Peço desculpa, mas eu só não tenho o
muitas dezenas de horas pode demorar para passar e
"regularizar" as coisas, para escrever mais graciosa transição
parágrafos, etc. Eu senti que era mais importante para obter a
idéias e idéia fragmentos para fora do que para polir a escrita.
(Ensaios escritos a partir do zero, e na ordem, são geralmente
mais graciosa do que são concatenações de idéias, fatos,
ponteiros, etc.)
- Os leitores também não deve supor que um "recheadas"de
seção, composta de relativamente parágrafos completos, é qualquer
mais importante do que uma seção que ainda é maioritariamente composto
de curto one-liners.
- Referências a Criptografia Revistas, Livros. Quase todos secção
neste documento _could have_ uma ou mais referências para
artigos e papers em Criptografia Processos, em

Schneier livro, ou o que seja. Desculpe, mas eu não posso fazer isso.
Talvez um dia, quando verdadeiro hipertexto chega e é prontamente
utilizável (não me enviem e-mail sobre HTML, ou Xanadu, etc.)
este tipo de referência cruzada será feito. Notas de rodapé
iria trabalhar hoje, mas são distração em documentos on-line.
E muito trabalho, dado que esta não se destina a ser um
acadêmicos tese.
- Eu também resisti ao impulso para incluídas citações ou
as seções a partir de outras perguntas frequentes, nomeadamente o sci.cripta e rsadsi
Perguntas frequentes. Não adianta copiar as suas coisas, mesmo com
crédito apropriado. Os leitores já devem ter esses documentos,
do curso.

20.4.6. sofisma

- A qualquer momento que você diga algo para 500-700 pessoas, esperar
tem um monte de sofismas. As pessoas vão ter problema com
phrasings, com opções de definições, com fatos, etc.
A precisão é importante, mas, às vezes, o sofisma conjuntos
fora uma reação em cadeia de correções, countercorrections,
refutações, e eu gostaria de ter a colocá-lo de forma diferente"s. É tudo
um pouco exagerado às vezes. Minha esperança para este FAQ é que
erros graves são (naturalmente), corrigida, mas que a Lista
não se atolar em infinitas tergiversações sobre tais menor
questões como estilo e fraseado.

20.5. Como Localizar Informações

20.5.1. Este FAQ é muito longo, o que torna a busca por perguntas específicas
problemática. Como é a vida--mais curto FAQ são, naturalmente, mais fácil
para navegar, mas não pode tratar de questões importantes.

20.5.2. Uma versão completa deste documento está disponível, bem como o capítulo-
por-capítulo versões (para reduzir o download de esforços para
algumas pessoas). Ferramentas de pesquisa dentro de editores de texto são uma forma de
encontrar tópicos. Futuras versões deste FAQ podem ser paginados e
em seguida, indexados (mas talvez não).

20.5.3. Eu aconselho usar ferramentas de pesquisa em editores e processadores de texto para
encontrar seções de interesse. Este é provavelmente mais rápido do que de qualquer maneira
consulta de um índice gerado por mim (que eu não
gerado, e provavelmente nunca será).

20.6. Meus Pontos De Vista

20.6.1. Este FAQ, ou o que se chama, é mais do que apenas um
a simples inclusão de perguntas freqüentes e de menor
comum denominador respostas. Esta deve ser clara, apenas o
tamanho sozinho. Eu não faço nenhum pedido de desculpas por ter escrito o documento eu

queria escrever. Outros são livres para escrever o FAQ eles
prefiro ler. Você está recebendo o que você paga.
20.6.2. Minhas opiniões são muito fortes em algumas áreas. Eu tentei
apresentar alguns dissidentes argumentos em casos onde eu acho
Cypherpunks são realmente um pouco dividido, tal como no reenvio de e-mails
estratégias e o gosto. Nos casos em que eu acho que não há nenhuma
credível dissidência, tais como na sabedoria de Clipper, eu fiz
nenhuma tentativa para ser justo. Meu libertário, mesmo anarquistas, pontos de vista
certamente virá através de. De qualquer lidar com isso, ou não leia o
documento. Eu tenho que ser honesto sobre isso.

20.7. Mais detalhada de isenção de responsabilidade
20.7.1. Este detalhada de isenção de responsabilidade é, provavelmente não é bom na maioria dos tribunais
nos EUA, os contratos de ter sido expulso se a favor da
nominalismo, mas aqui é assim mesmo. Pelo menos ninguém pode reclamar
eles foram enganados em pensar que eu estava dando-lhes warranteed,
garantido conselhos.
20.7.2. Timothy C. Pode renuncia a quaisquer garantias relativas à
este documento, seja expressa ou implícita, incluindo, sem
limitação, quaisquer garantias implícitas de comercialização ou
adequação para uma finalidade específica. Tim Podem não ser responsabiliza
por quaisquer danos especiais, acidentais, consequenciais, indirectos ou
semelhante danos por perda de negócios, acusação, por qualquer
o crime, prisão, tortura, ou por qualquer outro motivo, mesmo se
Tim Pode ou um agente de sua tenha sido avisada da
possibilidade de tais danos. Em nenhum evento deve a Tim Pode ser
responsável por quaisquer danos, independentemente da forma de reclamação.
A pessoa que está lendo ou usando o documento assume todos os riscos
a qualidade e a adequação do documento. Legalidade da
a leitura ou a posse deste documento em uma jurisdição que não é
a responsabilidade da Tim de Maio.
20.7.3. As opiniões expressas podem ou não representar a visão da
Tim Pode, e certamente podem não representar a opinião dos outros
Cypherpunks. Certas idéias, são explorados que, se
implementado, seria ilegal várias extensões mais
países no mundo. Pense nestas explorações de ideias
como apenas isso.

20.8. Eu decidi lançar este antes da RSA patentes correr para fora...