I read every 1990s Cypherpunk email

Here's what you should know

Porter Adams

Cypherpunk Historian, Matter Labs

One quote from ZKsync’s Credo:

The unwavering long-term vision remains: advancing personal freedom for all.

Let us remain resolute in championing digital self-ownership.

Onward.

https://github.com/zksync/credo

I got annoyed

I got annoyed

I read every cypherpunk email

I got annoyed

I read every cypherpunk email

I've picked the best emails that highlight cypherpunk ideas, culture, and world view

I got annoyed

I read every cypherpunk email

I've picked the best emails that highlight cypherpunk ideas, culture, and world view

Read them and learn what the cypherpunks were really like

cryptoanarchy.wiki

Arise, you have nothing to lose but your barbed wire fences!

Subject

```
The perl script, in summary, strips off the mail headers, saving the
Subject: line, rewrites a new header, and appends the body of the
previous message.  Here is the script:

--------- cut here ---------
while (<>) {
        last if /^$/ ;
        $subject = $_ if /^Subject:/ ;
        if (/^Request-Remailing-To:/) {
                chop ;
                s/^.*:// ;
                $addressee = $_ ;
        }
}

#open( OUTPUT, ">foo" ) || die "Cannot open 'foo'." ;
open( OUTPUT, "| /usr/lib/sendmail " . $addressee ) ;
select( OUTPUT ) ;

print "To:" . $addressee . "\n" ;
print "From: nobody\n" ;
print $subject ;
print "Remailed-By: Eric Hughes <hughes@soda.berkeley.edu>\n" ;
print "\n" ;

while (<>) {
} continue {
        print ;
}
--------- cut here ---------
```

Author, Day Month Year

https://mailing-list-archive.cryptoanarchy.wiki/

How to Make an Automated Remailer in Your Copious Spare Time with Easy to Find and Inexpensive Software Tools You May Have Lying Around.

The perl script, in summary, strips off the mail headers, saving the Subject: line, rewrites a new header, and appends the body of the previous message. Here is the script:

```
--------- cut here ---------
while (<>) {
        last if /^$/ ;
        $subject = $_ if /^Subject:/ ;
        if (/^Request-Remailing-To:/) {
                chop ;
                s/^.*:// ;
                $addressee = $_ ;
        }
}

#open( OUTPUT, ">foo" ) || die "Cannot open 'foo'." ;
open( OUTPUT, "| /usr/lib/sendmail " . $addressee ) ;
select( OUTPUT ) ;

print "To:" . $addressee . "\n" ;
print "From: nobody\n" ;
print $subject ;
print "Remailed-By: Eric Hughes <hughes@soda.berkeley.edu>\n" ;
print "\n" ;

while (<>) {
} continue {
        print ;
}
--------- cut here ---------
```

Eric Hughes, Thu, 24 Sep 92

A statement of purpose

I've had a bunch of people ask me about the group and what it's up to. Accordingly, I drafted a small statement of purpose to send to folks.

Please comment.

Eric

Cypherpunks write code. They know that someone has to write code to defend privacy, and since it's their privacy, their going to write it. Cypherpunks publish their code so that their fellow cypherpunks may practice and play with it. Cypherpunks realize that security is not built in a day and are patient with incremental progress.

Cypherpunks don't care if you don't like the software they write. Cypherpunks know that software can't be destroyed. Cypherpunks know that a widely dispersed system can't be shut down.

Cypherpunks will make the networks safe for privacy.

Eric Hughes, Mon, 5 Oct 92

We appear to be entering the long-awaited "Crypto Singularity”

```
* the incredible excitement over these topics at the Hackers
Conference, with the sense that these are no longer just abstract
ideas.

* the interest by several journalists in covering these matters (more
on this if things develop).

* articles in "Scientific American" just in the past
months...David Chaum's work on digital cash, and quantum cryptography.

* the firestorm of comments (over 500) about the proposal to register
cryptographic keys.

All of these point to an accelerating situation. Things may get very
interesting and very sticky in the next several months, which is quite
a bit faster than I'd expected.
```

Timothy C. May, Thu, 12 Nov 92

Thoughts on digital cash

I'd really like to see some sort of digital cash system set up. My feeling is that there would be a stronger demand than most people think for such a thing, even if it weren't anonymous and untraceable and all that. But if it has those features, too, and we do it first, it will get used. And de facto standards are hard to get rid of.

Marc

Marc Horowitz, Sun, 29 Nov 92

Digital banking, file formats, etc.

```
This is a run through of Hal Finney's summary of the bank protocol.
Here is what I envision the digital bank working like, with rough
sketches of file formats, conspicuously similar to the remailer's
:-):

1) Alice chooses x, r
   Alice computes B = r^3 * f(x) mod n
   Alice sends the following message to the bank via an anonymous
remailer

    ::
    withdraw
    <account name>
    <B = r^3 * f(x) mod n>
    Reply-To: <an anonymous remailer>
    <remailing request to Alice encrypted with appropriate remailer
public key>
```

Karl L. Barrus, Wed, 2 Dec 92

Electronic money legality

The question came up here some time ago as to whether it would be legal to issue electronic money, or regular money, for that matter. I got a couple of books out of the library to try to learn something of the history of private bank notes.

George Selgin's book, The Theory of Free Banking, is a call to return to a situation of competitive note issue, where each bank would print its own "money" and people would use all these different monies freely according to their preferences. Regardless of the pros and cons of this idea, he does mention the legal situation briefly in footnote 7 of chapter 11:

"Strictly speaking, issue of bank notes by commercial banks is not presently illegal; however, such issue must still meet the bond-deposit requirements

Hal Finney, Thu, 14 Jan 93

RE: White House letter

I think to start off and get attention and respect from the big white house we should simply send our stance on encryption and why it shouldn't be regulated.. I think this is the common goal among all the cypherpunks on this list [that is except the NSA folks who are listening in |-]].

I think, for now, we just want to let people know that there IS a specific group of individuals who are willing to protest for their right to privacy [you are, aren't you?] and follow up with suggestions to specific issues in later messages to the White House. and YES we should definately send all our public keys along with the message.. basically telling the government that we DO enjoy extreme privacy in part of our lives and would like to see it extended to all forms of communication.
TTFN!

DrZaphod

DrZaphod, Thu, 4 Feb 93

RE: A Modest Proposal

Nonetheless, I will never desire censorship for its own sake and I will also fight to remove the conditions which make censorship exigent in the first place.

The problem is, who decides what is exigent? We can either answer that question, or change the world so that we never need ask it.

I decline to respond to the essay by Mr. D. Lewdud.

Eric

Timothy C. May, Mon, 1 Mar 93

White House encryption idea

Well, this all sounds fine and dandy, but...

1) They are not passing out the algorithym, and I dont trust ANYONE to tell me its secure. I am not a cryptographer, so it wouldn't help any if they gave the code to me, but it just being out there for public perusal helps me to think it IS secure. I trust no payola.

treason@gnu, Fri, 16 Apr 93

Re: Is Rush Limbaugh giving Clinton sh*t about wiretap chip?

```
>> WEll i work for a mojor airline and I would be happy to get you his homne
>> mailing address if he has a frequent flyer number.

Excuse me?  Are you completely missing the point here?  We're fighting
for *PRIVACY*.  Misusing your position at whatever airline you work
for and broadcasting someone's home address over a mailing list of
people he's never heard of is completely antithetical to what we are
trying to do.

                Marc
```

Marc Horowitz, Sun, 2 May 93

Re: Digital Cash

```
>>>Then DC is actually backed by "legal" currency?  Then, what's to keep
>>>someone from opening a digital bank, and takeing the money and runing?

Nothing.  Just like the First National City Bank of New York or Bank Leu,
Zurich.  You should deal with someone with a rep and perhaps a history.
Obviously the risk of fraud would be greater with a digital cash issuer
completely unconnected to an existing financial institution.
```

Duncan Frissell, Thu, 17 Jun 93

Radical Paranoia?

I'm having a philisophical problem reguarding when to sign someone else's public key.

Obviously, if you watch someone generate a key, and they physicaly hand you a copy of it, you should sign it. Fortunately, life has been this good to me about 5 times. But what if life isn't so good?

Lets say someone emails me a key and the return address matches that of the address in the key. Do I assume no one is spoofing me? You have to admit that this is possible albeit unlikely. What good is key certification if it only "probably valid?" I've noticed that many of the keys on the server are signed with the same person's key. I doubt that these people have had physical contact with each of the people who's key that they've signed. Am I just being paranoid, or is there a valid issue here? I welcome any of your comments.

J. Michael Diehl, Sun, 11 Jul 93

Secure voice software issues

But there are some problems yet to be solved. I'm rapidly coming to the conclusion that the only way around the SLIP/PPP modem buffer/delay problems is to speak raw synchronous data to the modems, even to the point of implementing V.42bis and HDLC in the host computer instead of using the modem's implementation.

Phil

Phil Karn, Thu, 12 Aug 93

Re: Digital warfare

We may also see the creation of `virtual governments' in which the geographical location of an individual is irrelevant to his choice of government, and perhaps for the first time in history the individual can choose freely among all those that exist, to that which best suits his preferences, and the so-called `social contract' between the citizen and his government is actually made *explicit* for the first time. This will all happen on some levels.

But only the silly, pale bureacrats in the NSA attribute the Collapse of the World and the Plague of the BoogieMen to the advent and proliferation of strong cryptography. Cryptography is not synonymous with tax evasion, terrorism, or utter chaos. It is simply as neutral, powerful, and liberating as communication itself. In fact, for the first time we are beginning to realize what `communication' truly entails.

L. Detweiler, Fri, 10 Sep 93

Re: Cypherpunk Cause

If there is no cypherpunks cause or movement, please let me know. Being able to interact with people who believe in the cypherpunks cause is the only reason I subscribe to this list and if there is no cause, I would like to unsubscribe and spend my time elsewhere. Can we have a simple survey of the list? If you believe there is a cypherpunks cause and you believe in it, please post a short note to that effect to the list. Anyone who is interested can keep count. I suppose to be fair, you should also post a note if you believe there is no cause.

Don Henson

>
> If there is no cypherpunks cause or movement, please let me know

What the hell are you talking about?

From owner-cypherpunks Fri Oct 8 23:37:20 1993

Paul Ferguson, Fri, 8 Oct 93

LD’s last flame of me

CPs,

I did not want to poin-blankly address some of the comments that LD made about me in his last post, but I feel it necessary. I won't say he's insane or deranged, since i know it does no good. I won't say that he is raving or frothing at the mouth, since it does no good either.

I will say that I am doing my best to uphold what I believe in, and that I will not stand for the public slander of my name and reputation all across the net. If you want to slam me, L.Detweiler, please slam me in private email, since very few people put great weight on your post, at least not lately.

- -nate sammons

Nate Sammons, Thu, 25 Nov 93

Love lost

It appears I have made quite a pest of myself on this mailing list, and that everyone hates me, and curses me as Satan, particularly at the delight and encouragement of your leaders. In fact, a long time ago, before it became clear I was such an unstable jerk and paranoid lunatic out to get people who betray me, in fact around the time of the PGP subpoenas, in which I had continually sent out some of my most masterful and brilliant postings, when I still had a respectable reputation, despite that P.Metzger was continually attacking and dogging me in the most vicious way a human being (at least, I think he

L. Detweiler, Sun, 5 Dec 93

Psychobabble

```
Nick Szabo (szabo@netcom.com) wrote:

: No, Mr.
: Detweiler, I'm not "pseudospoofing",

How do you explain your statements I analyzed in RISKS 15.27, where you
posted to cypherpunks promoting your sophisticated pseudospoofing techniques?
Multiple posting sites, countermeasures and contempt for `opponents' who
attempt to determine whether your tentacles are who they claim to be.

Frankly, I think you are a baldfaced liar. Are you intellectually challenged
or am I going to have to go root up all the archives to prove it?

You cryptoanarchists are so arrogant. it will be your downfall.
```

Anon (probably L.Detweiler), Sun, 5 Dec 93

Who is L. Detweiler?

He joined the Cypherpunks list about a year ago and showed great enthusiasm and energy, volunteering to write the FAQ on "Anonymity on the Internet" and "Privacy and Anonymity." He put this out very

He asked to be removed from the Cypherunks list, and was, but continued to post to it (blindly). He created his own group, the "Cypherwonks" list, with a fascist list of rules and regulations about true identities, the evils of pseudospoofing, etc. I gather from reports that it is now moribund. (I didn't join, for obvious reasons,

Timothy C. May, Tue, 11 Jan 94

Who is T.C.May?

First, reports of my insanity are greatly exaggerated. They seemed to have originated with P.Metzger. At first I was just writing `rants' and these became labelled as `insane' as a simple progression in terms that paralleled the Cypherpunk desperation at my tenacity.

Mr. May, when he sees editorial cartoons in the newspaper, probably likewise considers them `forgeries'. He is incapable of understanding the distinction of truth and satire, having, like the rest of the CA psychopunks, stoned himself for years on lies.

L. Detweiler, Thu, 13 Jan 94

Blacknet worries

Blacknet could remove most of this risk. With near-perfect anonymity and digital cash, a tidy side income could be created for anyone with access to classified information. There would be no need for risky physical meetings. The money could be spent on a few nice extras to make life more comfortable, without fear of it being traced.

Hal Finney, Sun, 20 Feb 94

Re: Digital Cash

```
Hal Finney writes:

> The other issue, which I know less about, is the possibility of cryptograph-
> ically strong obfuscated code.  Mike Duvos first mentioned this.  You could
> have an algorithm running on your own computer and have it be impossible to
> determine what it is doing, or (presumably) to effectively alter the internals
> of the algorithm.
```

```
The similarities with zero knowledge work are apparent (in zero
knowledge interactive proof systems, one proves one knows something
without actually shwoing what one knows).

This may not be exactly what Hal was thinking of, but it's a starting
point.
```

Timothy C. May, Sat, 26 Mar 94

nsa digital cash?

ok, so the nsa looked at commercial cryptography and said, `we need to control it'. and out pops clipper (quite an ugly baby, eh?)

this makes me wonder. i bet that they see that announcement by visa for `digital cash' and go crazy. they are already thinking of how to put clipper into a nationwide digital cash system, don't you think?

this brings up some serious issues. i doubt it will be long before there are some official government agencies developing the official u.s. digital cash system. in fact, it wouldn't surprise me if there are divisions in the nsa dedicated to doing it *this moment*.

tmp@netcom.com, Tue, 5 Apr 94

Cypherpunks Goals: Bad debate drives out good debate

While I'm not predicting the imminent death of the Cypherpunks list, it seems clear we have to stop the slide into inconsequential chatter and paranoid speculation.

Cypherpunks write code. Or at least they work on ways to *make things happen*. They don't fall into the trap both the Marxists and the Libertarians have fallen into, of idly discussing theory and hoping that somehow the glorious future will arrive. Cyperpunks understand that the genie of strong crypto is out of the bottle and that a relatively small number of people working on new tools and capabilities can produce a phase shift of immense proportions in the world.

There's work to be done, and I know of no other groups even one tenth as prepared as we are to do this work.

Let us get on with it.

--Tim May

Timothy C. May, Wed, 11 May 94

Delayed self-decrypting message

I have a need to give several people an information file that is secured until a given date. Think of an embargoed press release for a model.

Can I do this with crypto technology? Is there a way I can send out a file and perhaps a tool such that the file can be decrypted only after a given date?

++PLS

Paul Schauble, Fri, 10 Jun 94

Re: Counting bits

```
Both Sun C and GCC on a Sun SPARC system running 4.1.3 produced this code
for each bit-count line (-O4 optimization used):

L77042:
        andcc   %o0,2,%g0               ; AND the bit
        bne,a   L77044                  ; branch/anull if zero
        inc     %o5                     ; increment bitcount
L77044:

This, I believe, is as optimized as it is possible to get on a uniprocessor
machine.
```

Ian Farquhar, Wed, 6 Jul 94

Remailer chaining results

I've done some calculations on the mixing properties of Chaum-style networks and gotten some interesting results.

Recall that in a Chaum-type remailer network users use nested encryption and remailing instructions to set up a chain or "cascade" of remailers. Each remailer strips off the encryption envelope and sees the address of the next remailer in the chain or, for the final remailer, the ultimate destination. All messages are the same size and carry no distinguishing features. We assume that the opponent is monitoring all messages traffic into and out of all remailers on the net but can't see what is happening within each remailer.

Let's take a concrete example and suppose there are four remailers. Everyone sets up a chain of 2 remailers, chosen at random from these four. A batch of messages is received by each remailer, which strips off the envelope and sends them on to the next remailer in the chain, where they are mixed with the other messages which chose that remailer as the 2nd in the chain, then sent out to their ultimate destinations. This model is a little artificial in that we are assuming a certain amount of synchrony of the operation of the various remailers for simplicity. (Note that for this four-node network there are twelve possible two-node chains where the nodes are different.)

There are three measures that I am interested in: bandwidth used (the less the better); message mixing (the more the better); and immunity to subversion (the more the better). For bandwidth we can measure the flow through the remailer. Due to the symmetry of the situation, the inflow and outflow are equal and the same for all remailers. Message flows per remailer are the sum of the flow into the remailer from outside (the user messages), plus all flows into the remailer from the other remailers. Mixing can be measured by a probability distribution over the outgoing messages which represents how likely they are to be a given incoming message. For simplicity this can be expressed simply as the number M of messages which are equally likely to be the original (in an earlier message I used entropy which is a log measure of the same thing). I am thinking of measuring immunity to subversion in terms of how much mixing is lost by a certain number of "failed" (that is, subverted) nodes. Some networks are vulnerable to "single point failures", where a single subverted node destroys all the anonymity. A more robust network would require multiple failures for this to happen. However, it turns out that even in a multiple-failure network a single-point failure may reveal some information about the messages, which we can express as a loss in mixing.

Let the total message bandwidth into the network be N packets per time unit. Due to symmetry, each node will receive N/4 packets. With the chains as defined above, the other three nodes will all be equally likely to be the 2nd in the chain, so N/12 packets are sent to each of them. Simultaneously, N/12 packets come to this node from each of the others. This is a total internode bandwidth of N/4 in each direction per node, or N total per direction. Add this internode bandwidth to the user-link bandwidth of N per direction and we get 2N total, or N/2 per node.

At the beginning of each chain, we have N/4 packets come in and get mixed as each node. As the packets go out, they are sent to the other three remailers, and when they leave they may be any of the output of those three. Thus they are equally likely to be any of 3N/4 of the packets, and this is the amount of mixing we have.

If one of the two nodes in your remailer chain is compromised, it provides no effective mixing. This means that your message is only mixed at one node, where it is combined as part of a batch of N/4, so that is the degree of mixing you have with a single failure. If both remailers are compromised then of course you have no mixing, which we would write as a factor of 1 in uncertainty increase.

This can also be expressed in terms of a percentage compromise of the network. If 1 node is compromised, which can be represented as p=.25, then the six of the twelve remailer paths which use that node will have single-point failures with the concomitant reduction in mixing. In other words, half of the messages will have the full 3N/4 mixing while half have N/4. With p=.50, two nodes are compromised. Two paths are safe, eight have single failures, and two have double-failures. So we have 1/6 of the messages with 3N/4, 2/3 with N/4, and 1/6 with only 1 mixing. With p=.75, three nodes compromised, there are no safe paths; half have single failures and half have double. So 1/2 the messages have mixing of N/4 and half have 1. And of course with p=1 all messages are compromised with mixing factor 1.

Let me just go on and extend this analysis in one way. In the discussion of the chains, we have assumed that the two nodes in the chain would be different. Logically though one could have chains where both nodes were the same. Let us compare this network with the one we just did.

There are now 16 possible chains. Total bandwidth is somewhat less (since we don't count the messages which stay in one remailer). Now only 3/4 of the messages from each node need to get exchanged. Per node, there will be N/4 messages to users and 3N/16 messages to other nodes, for a total of 7N/16 per node or 7N/4 total (above the 7's were 8's). Mixing is actually improved; there is no limitation on which input messages might map to which output ones, so we have full N-fold mixing (compared to 3N/4 above). With single-point failure mixing is again N/4 as above.

The failure behavior is quite different. With p=.25, 1 of the 16 paths is totally compromised, 6 of the 16 have single failures for N/4 mixing, and 9 of the 16 have no failures for N mixing. With p=.50, 4/16 of the paths have mixing 1, 8/16 have mixing N/4, and 4/16 have mixing N. With p=.75, 9/16 have mixing 1, 6/16 have N/4, and 1/16 have N.

It's not clear what measure is useful to compare these failure situations. A double-point failure seems much worse than a single one. I wonder whether taking a geometric mean (which would be equivalent to taking the arithmetic mean of the entropies) would be valid. If we did that for the p=.25 case, we get average mixing of .59N^(15/16) for the self-chain network, and .27N for the network where all chains are two different nodes. For N less than about 250,000 packets per (network-wide) batch the self-chain network provides superior average mixing in the p=.25 case by this measure.

Sparing the math, for p=.50 the self-chain network is superior for batch sizes smaller than 29 packets, and for p=.75 the self-chain network is only superior for batch sizes smaller than 16 packets. This suggests that if the network is likely to be mostly safe then the extra mixing allowed by same-node chains is worth the small increased risk of exposure. But as the chance of encountering bad nodes rises it becomes unwise to take this chance.

Here is a quick summary of the extension of these results to larger numbers of remailers and longer chains. Let there be R remailers and let the chain length be K. Let the number of message packets per batch (network wide) again be N. (I will neglect the differences between same-node chains and different-node chains as they are generally small effects on the order of 1/R.)

Bandwidth per node is approximately KN/R. Network wide it is therefore NK. Adding remailer hops increases network bandwidth loads directly in proportion to the number of hops. Mixing is approximately N for K=2 and up, which is the maximum possible. For K=1 mixing is N/R.

Fault tolerance is interesting. A K-length cascade is invulnerable to up to K-2 failures! At K-1 the mixing decreases from N to N/R, a significant decrease. And with K failures of course the mixing drops to 1. I was surprised how robust these networks are. The reason is that with even K-2 compromised remailers in a K-length cascade there still remains a safe length 2 cascade, and as we saw above that provides N-fold mixing.

This provides some guidelines on the choice of K. First, K should clearly be at least 2. The increase from K=1 to K=2 increases mixing from N/R to N, a considerable increase. Secondly, K should probably be at least 3. This will provide full mixing even if you are unlucky enough to choose a compromised remailer. Beyond this, you can calculate that with a chain length of K and probability p of a compromised node, the expected number of compromised nodes in your chain is Kp. This suggests that you should choose K large enough that Kp is well below K-2. If you estimate p=.50, for example, you might choose K=8. The binomial theorem states that the chance of x failures out of K nodes where the probability of each failure is p is (p^x)*((1-p)^(k-x))*k!/x!(k-x)!. In this example, the chance of 7 failures out of 8 is about 3% and the chances of 8/8 is about .5% for a total risk of 3.5% that you won't be fully protected.

Now, how many people read this far? ;-)

Hal

Hal Finney, Mon, 8 Aug 94

Social punishment 3/3: reputation systems

One problem with such a wildfire reputation system is it can be _too_ effective. Once ostracized, the decentralized system makes it very difficult for someone to rejoin society, to have his/her 'reformation' recognized. The channels in traditional societies include lots of 'good work' and recommendation by 'good citizens' such as the priest etc. The other is a new identity.

This is a strong case for universal pseudonymity - BAN TRUE NAMES - which, together with strong voluntary reputation and social punishment systems can form the basis for cyberspatial order.

Rishab Aiyer Ghosh, Fri, 9 Sep 94

On Feistel Networks, S-Boxes, and Block Cipher Design

Choosing good S-boxes is not an easy task, and there are many competing ideas on how to do it. Four general approaches can be identified:

Choose randomly: It is clear that small random S-boxes are insecure, but large random S-boxes may be good enough. Random S-boxes with 8 or more inputs are quite strong. And even more strength is added if the S-boxes are both random and key-dependent. IDEA uses both large and key-dependent S-boxes.

Choose and test: Some ciphers generate random S-boxes and then test them for the requisite properties. See [ADA90] for an example of this approach.

Man-made: This technique uses little mathematics; S-boxes are generated using more intuitive techniques. Bart Preneel stated that "...theoretically interesting criteria are not sufficient [for choosing Boolean functions for S-boxes]..." and that "...ad hoc design criteria are required" [PRE93].

Math-made: Generating S-boxes according to mathematical principles so that they have proven security against differential and linear cryptanalysis, and good diffusive properties. See [NYB94A] for an excellent example of this approach.

Bruce Schneier, Sun, 2 Oct 94

Cell Phones Security - NOT!

Well, as one who owns an AOR 1000 radio frequency scanner that can receive any and all cell phone conversations, I would have to say you have no security unless you use some kind of voice encryption. In order to make you can feel warm and safe, the manufacture or importation of scanners with cell phone capability was outlawed by congress earlier this year, which means that I can still listen to your call with my existing scanner while you feel protected. I bought guns with high capacity magazines this year after they were banned also. I wish I had enough money to buy a good assault rifle before they're all over priced (they'll never be all gone, just over priced.)

Conrad Walton

Conrad Walton, Tue, 22 Nov 94

Tim May is RIGHT!!!

I'm sorry I can't say so under my real name, but I *vehemently agree* with Tim May about the authoritarian, heavy handed, generally outrageous egotism of Eric Hughes of recent. This is REALLY UPSETTING. Eric should be ASHAMED OF HIMSELF for strutting around like a peacock. he is EMBODYING THE DICTATORIAL APPROACH HE CLAIMS TO DEFY VIA CYPHERPUNK PHILOSOPHY. this is truly the most HYPOCRITICAL AND EGOMANIACAL action I have seen by anyone in recent times on this list.

Tim May will leave the list? GOOD FOR YOU, TIM. Get the hell out of here. Eric Hughes may have had some good ideas ONCE UPON A TIME but hasn't kept up his end of the bargain of the cypherpunk agenda for a LONG, LONG TIME. just a WASHED-UP HAS BEEN, who defies the very ideals that he claims to espouse in the most dictatorial manner possible.

nobody@c2.org, Thu, 1 Dec 94

The Value of Anonymity

In an information-age society without extremely strong privacy protections, the chief factor which makes the difference between winners and losers may be how much information each of us has on others, and how much they have on us. Given this degree of economic and social motivation, it is easy to imagine the sort of panopticon which will soon arise on the Internet (and its descendants), unless the strongest possible protections are adopted. (And it is equally easy to imagine who the biggest winners and losers will be.)

mkj@october.ducktown.org, Sat, 7 Jan 95

The Value of Anonymity

Now that I've just spent some time compiling and playing with Matt's ESM program, it seems almost perfectly suited for prototyping Pipe-Net since you can use it to do nested encryption. All that's needed is to hack it so that it implements link encryption (i.e., send a constant stream of random data in between keypresses).

I wonder if Matt has the time and interest do this... If not then I guess I can try, but I've never done real crypto programming before...

Wei Dai

Wei Dai, Wed, 8 Feb 95

A Chronology on crypto bans

Attempts to ban encprytion 1977-1995

1977-1980 NSA Director Inman calls crypto born secret. Should be restricted. Attempts to use Invention Secrecy Act of 1951 to patent inventions by academic researchers. Attempts to use export control laws to limit scientific discussion.
NSA Threates NSF over grants for crypto studies.

1981 American Council on Education committee recommends voluntary submissions of cryto papers to NSA

1984 National Security Decision Directive 145. Gave NSA authority over all govt crypto and computer security development.

1986 NSTISSP. Attempted to extend NSDD-145 to private sector. USe to justify visits to LEXIS/NEXIS, Dialog, public libraries etc.

1987 Congress passes Computer Security Act. Gives crypto authority to NIST.

1989 NIST signs MOU with NSA giving back authority to NSA. NIST starts development of new public key system to do both signatures and key exchange.

1990 After pressure by NSA. NIST adopts El Gamal for signatures only. NSA secreatly designs "algorithm on a chip" for key exchange. FBI, NSA and NIST also begin "National Cryptgraphic Review".

1991 FBI asks Senator Joseph Biden to introduce "Sense of Congress" to recommend backdoors in all encpryption, telephone systems. Provision removed after public outcry. Later evolves into digital telephony proposal
October 1991, NSA, FBI, CIA meet to discuss possible legislation on encryption.

1992 NIST memo - "FBI working on draft legislation to control and liscense all cryptography"

1993 Clipper Proposal introduced. Interagency working group formed by Presidential Review Directive 27. According to NSA memo on IWG "FBI proposed legislation to authorize the FCC to regulate common carriers, PBX operators, and manufacturers of encryption devices available for use in the US to ensure such systems and devices are compatable with law enforcement electronic surveillance interests....the interagency working group revied proposed legislation and concluded that ....legislation to authorize regulation of encryption product manufacturers would be considerably more difficult [than passing the digital telephone proposal] and required further study." 6 options were discussed including prohobiting all other encprytion besides Clipper. The other five have been classified "top secret".

Dave

Dave Banisar, Sun, 16 Jul 95

Crypto = Competitive Advantage?

Crypto could be the next big wave of IPOs, with "Verisign" and "RSADSI" both rumored to be offered. Some of the digital commerce companies may be next.

It seems that anything involving the Internet, the Web, and digital commerce is really, really hot.

--Timothy C. May, President, Bank of the Web

Timothy C. May, Wed, 9 Aug 95

Re: Fiat Shamir Zero Knowledge Test

```
>Can someon point me to a net description of
>the "Fiat Shamir Zero Knowledge Test" used
>in the RCA DirecTV smart cards.
>

The standard text on this is the paper "How To Prove Yourself" by Fiat and
Shamir. I'll try and dig up the name of the ftp site I found it on but in
the meantime here is a rough description.

The access control system for RCA DirecTv was developed by News Datacom.
They, News Datacom, also developed the security for the VideoCrypt system
```

John McCormac, Fri, 1 Sep 95

Crypto hardware summary

Here is a summary of my points on this subject to date, for those who haven't been following this discussion:

- Using coprocessors of any sort to achieve speed in cryptography operations is probably not justified for end users; it is almost always justified for servers with a high volume of transactions requiring public key authentication or encryption.

- People running cryptography-based transaction clients on their PCs are going to learn, one way or another, that having valuable secret keys on their hard disks is not a great idea. This, not speed, is the primary motivation for consumer-oriented cryptography hardware. People want their keys and financial transactions on secure, removable, non-mechanical media. Products that provide this are just starting to come on the market, notably from National Semiconductor and Telequip.

Douglas Barnes, Sun, 1 Oct 95

Cypherpunk FAQ

Hi, I'm new to the list, so please don't flame me too badly if this is a dumb question. At least restrict the flames to private email where no one else can hear me scream. :>

I downloaded the Cypherpunk FAQ from the Cypherpunk Website. When I decompressed it, all it contained were the words "Yoo hoo, anybody home?" Has the FAQ been corrupted or is this an in-joke?

Also, the Privacy FAQ states it was written by L. Detweiler. Is this THE L. Detweiler? If so, why is it in the archives?

Thanks for helping me out.

Cassiel

Cassiel, Wed, 15 Nov 1995

Re: Housewarming/birthday party

```
>      The price of condo living: There is no guest parking in the complex,
>      and the party must end by 10pm.  Please help us get along with our new
                ^^^^^                  ^^^^
>      neighbors by respecting the condo rules.  Thanks!
>

Thats not a party. Thats an after-school tupperware get-together.

Cheers,
```

Julian Assange, Sat, 30 Dec 1995

Now you've seen the cypherpunk emails

What should you do with this information?

Thank you!

Porter Adams

Matter Labs

Twitter: portport255

Matter Labs is hiring Protocol Engineers