Introdução à Segurança de Informações

Prof. Valdeir Romão
Ciências da Computação

1º semestre de 2021

Roteiro

- Proteção da informação
- Técnicas para proteção do conteúdo da informação
- Aplicações
- Conclusões

Roteiro

- **Proteção da Informação**
- Técnicas para proteção do conteúdo da informação
- Aplicações
- Conclusões

Acesso à Informação é...

- Cultura
- Cidadania
- Desenvolvimento
- ... Poder

 Imprescindível para a vida social.

Informação deve ser protegida...

... em vários níveis da atividade humana:

- **Pessoal**
  - **Privacidade, confidencialidade, anonimato**
- **Social**
  - **Comércio, propriedade intelectual, mídia**

Político-administrativo

- **Responsabilização, segredos estratégicos**

Corporativo-Industrial

- **Patentes, comércio, estratégia**

Informação e Internet

- Todos esses aspectos da segurança da informação são anteriores à expansão espetacular do uso dos computadores, suas redes de interconexão e telecomunicações.
- Esses avanços técnicos amplificaram a importância da informação e evidentemente as preocupações com a sua proteção.
- Estamos só no começo.

Informação na era Internet

Características

- Abundância e variedade
- Acessibilidade imediata e barata
- Grande vulnerabilidade nos muitos pontos de acesso distribuídos
- Facilidade de reprodução
- Facilidade de modificação
- Facilidade de fabricação

Ataques à integridade

- Fáceis, baratos e remotos
- Variedade de formas e poder computacional
- Possibilidade de esforços distribuídos organizados à distância. Casos recentes:
  - negação de serviço na Web
  - roubo de ciclos
  - PCC ☹
  - ...

Onde estão as vulnerabilidades?

Em todo lugar:

- Informações de qualquer tipo, dados ou programas, armazenadas em processadores, memória primária ou secundária, on-line ou off-line.
- Informações em trânsito em conexões com ou sem fio.

Exemplo - Comércio Eletrônico

- Ataques ao **software do servidor** incluem roubo de informações, alteração de contas, alteração de código para obtenção de vantagens.
- Ataques ao **software do cliente** incluem modificação de código, acesso ao cache do browser.
- Ataques ao **sistema operacional** do servidor ou cliente visam acesso não autorizado a arquivos, instalação de vírus, entre outros.

Exemplo - Comércio Eletrônico

- Ataques à **transação de pagamento** podem ocorrer em vários níveis:
  - manipulação de pacotes TCP/IP
  - protocolos de conexão
  - protocolos de sistemas de pagamento, carteiras eletrônicas. Vão desde a modificação não autorizada de protocolos até a exploração de fraquezas conceituais que permitam a negação posterior de ordens de pagamento, entre outros.

Exemplo - Computação Móvel

- Novas ameaças se configuram
  - Código móvel carrega informações sensíveis e fica à mercê dos servidores onde se instala. Entre essas informações estão registros de transações passadas, futuras e chaves.
  - Os servidores também estão expostos a agentes maliciosos. Agentes devem ser autenticados e sua computação isolada em ambientes protegidos, com interfaces bem definidas.

Quem são os perpetradores?

- Grande parte dos ataques vem de dentro das organizações e freqüentemente dispensam a aplicação de técnicas sofisticadas de invasão de sistemas.
- Outra classe de ataques, mais divulgados, são feitos por entidades externas, entre os quais estão os chamados *hackers* e *crackers*.

Quem são os perpetradores?

Assim, medidas para garantir a integridade de sistemas de informações devem ter caráter **técnico**, na forma de algoritmos e protocolos de segurança, e **político**, na forma de procedimentos sistemáticos para atribuição de responsabilidades, distribuição de informações sensíveis, controle de acesso, entre outros.

Nosso objetivo - I

Nesta palestra trataremos apenas dos aspectos técnicos para o provimento de requisitos de segurança.

Serão descritos métodos para proteção da informação, principalmente aquela em trânsito por redes de computadores.

Veremos fundamentos, técnicas, protocolos e seu emprego em algumas aplicações típicas de ambientes computacionais distribuídos modernos.

Requisitos básicos de segurança

- **Confidencialidade ou sigilo:** Informação deve ser acessível apenas a autorizados.
- **Autenticidade:** Certeza da origem e conteúdo da informação.
- **Integridade:** Garantia de que a informação não tenha sido alterada indevidamente.
- **Não-repúdio:** Garantia de que o originador da informação não possa negar sua autoria.

Serviços de segurança

O provimento desses requisitos se dá através de serviços básicos que, combinados, formam serviços de segurança mais específicos como **validação, identificação, certificação, autorização, revogação, emissão de recibos e anonimato,** entre outros.

Segurança (do funcionamento)

Existe uma classe de problemas de segurança relacionados com o funcionamento correto dos sistemas e seus programas. O termo em inglês para essa área é *safety*, em vez de *security*, como é o nosso caso.

A área de *safety* trata da disponibilidade de sistemas, sua tolerância a falhas e confiabilidade.

A integração das técnicas de *safety* e *security* é considerada muito promissora para a construção de sistemas confiáveis e seguros (*dependable*).

Ataques

Ameaças à segurança de informações são multi-facetadas, multi-localizadas e nem sempre detectáveis prontamente. As precauções contra essas ameaças vão desde a prevenção, passando pela detecção até, quando possível, o restabelecimento do funcionamento do sistema após um ataque.

De forma muito geral, ataques classificam-se em **passivos** e **ativos**.

Ataques passivos

Limitam-se à escuta e cópia de informações e análise de tráfego. Fica ameaçada apenas a confidencialidade.

- Medidas de segurança limitam-se à prevenção, já que é muito difícil detectar um espião numa rede, principalmente uma rede aberta como a Internet.

Ataques ativos

- **Replicação e/ou alteração de informações legítimas**
- **Confecção de mensagens em nome de terceiros**
- **Personificação (falsificação da identidade) de terceiros, com objetivo de obter acesso a serviços**
- **Negação de responsabilidade da autoria de informações**
- **Acesso a serviços por meios sub-reptícios**
- **Desestabilização e interrupção ilegítima de serviços**

Ataques ativos

Precauções contra ataques ativos usam todo tipo de ferramentas disponíveis, desde a **prevenção**, por meio de técnicas criptográficas, a **detecção**, pelo monitoramento constante, até a **recuperação** de informações ou o **restabelecimento** do funcionamento dos sistemas atacados, por meio de técnicas de tolerância a falhas e outras.

Defesas

Praticamente todos os métodos e técnicas para a proteção dos requisitos da segurança de informações utilizam a ciência da **Criptografia.**

Embutidas em protocolos nos diversos níveis de processamento e comunicações, técnicas criptográficas tornaram-se uma ferramenta indispensável na construção de sistemas de software e hardware seguros e confiáveis.

Isso não quer dizer que a Criptografia prescinda de uma boa política de segurança e outros cuidados.

Nosso Objetivo - II

Exemplificar como técnicas criptográficas são empregadas em duas aplicações modernas:

- correio eletrônico - PGP
- segurança de conexões na Web - SSL

Veremos fundamentos, primitivas básicas, protocolos e seu uso nas aplicações.

Roteiro

- Proteção da Informação
- **Técnicas (criptográficas) para proteção do conteúdo da informação**
- Aplicações
- Conclusões

Criptografia Clássica x Moderna

Criptografia clássica era assunto secreto de diplomatas e militares; e um passatempo fascinante. Referências excelentes são:

The Codebreakers: ... from ancient times to the Internet, de David Kahn. O mais completo relato da história da criptografia desde tempos imemoriais até o presente.

The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, de Simon Singh. Outro relato agradável e moderno.

Codebreakers: the inside story of Bletchley Park. Depoimentos pessoais de vários integrantes da equipe de criptoanalistas ingleses na Segunda Guerra.

Criptografia Clássica x Moderna

- Criptografia moderna é uma ciência eminentemente pública, com possibilidades imensas de aplicação.
- Deixou de ser sinônimo de ciframento, para tornar-se o conjunto de algoritmos e técnicas matemáticas sobre as quais repousam métodos e protocolos destinados ao provimento dos requisitos da segurança da informação.

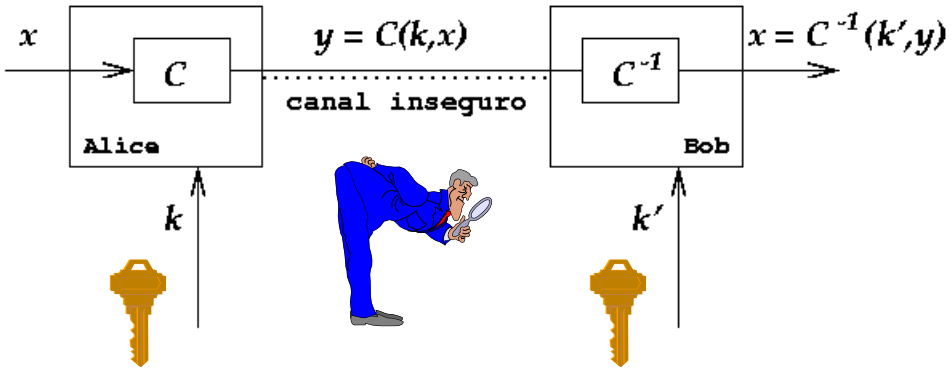
As Ferramentas Fundamentais

- Funções **unidirecionais** (em inglês, *one-way functions*) são o bloco básico para a construção de algoritmos de ciframento, assinaturas e hashing criptográfico.
- Protocolos criptográficos combinam esses algoritmos de diferentes formas, para satisfazer os diferentes requisitos da segurança de informações.

As Ferramentas Fundamentais

- Para obtermos ciframento e deciframento, é necessário que seja possível inverter uma função unidirecional, com a ajuda da chave de deciframento.
- Tais funções são as **unidirecionais com alçapão.** Em inglês, *trapdoor one-way functions*.

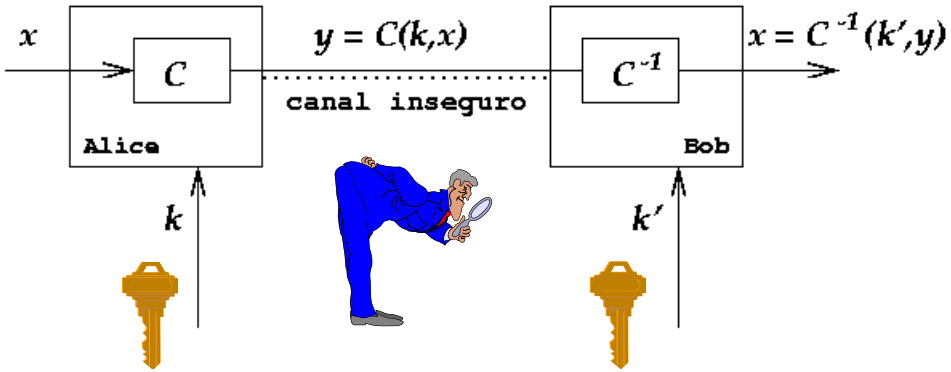
Sistema Criptográfico Clássico



- $k = k'$ secretas e combinadas por comunicação pessoal.
- Algoritmos C e C^{-1} eram simples

$\Rightarrow$ Totalmente inadequados para ambientes modernos

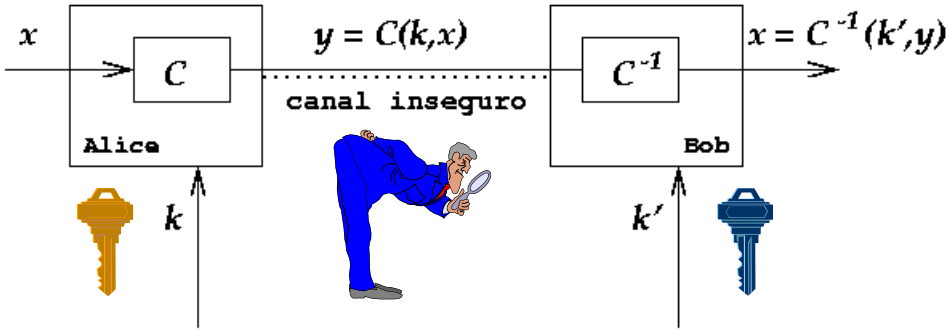
Sistema Moderno Simétrico



- $k = k'$ secretas e pré-combinadas em segredo
- Sistema é seguro desde que:
  - chaves sejam grandes (≥ 128 bits) ⇒ muitas chaves
  - C e C^{-1} sejam difíceis de inverter, **unidirecionais**
- Persiste o problema do estabelecimento da chave k

Sistema Moderno Assimétrico

Solução para o estabelecimento da chave - I



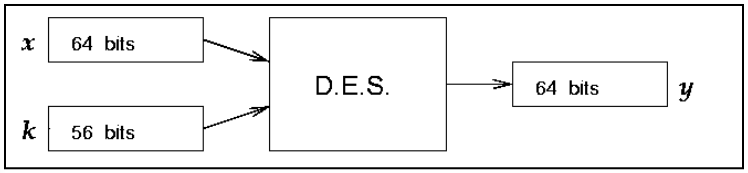
- *k* é a chave **pública** e *k'* é a chave privada (de Bob)
- Sistema é seguro desde que:
  - *k'* seja grande (≥ 180 bits), difícil de obter a partir de *k*
  - *C* e C^{-1} **unidirecionais**
  - *k* seja obtida de forma certificada

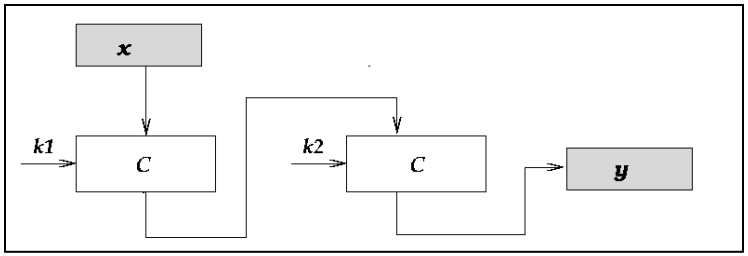
Simétricos x Assimétricos

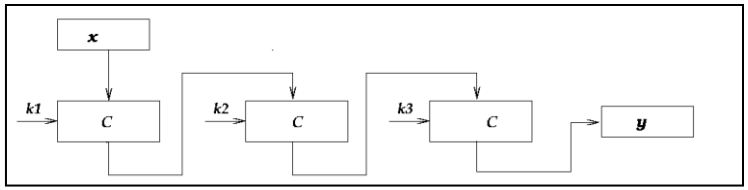
- Algoritmos simétricos
  - rápidos e facilmente implementáveis
  - chaves são relativamente pequenas
  - problema das chaves: n^2 e difíceis de distribuir
- Algoritmos assimétricos
  - lentos e de implementação intrincada
  - chaves são maiores
  - n chaves apenas e a distribuição é simples

Misture os dois!

Simétrico I - o DES



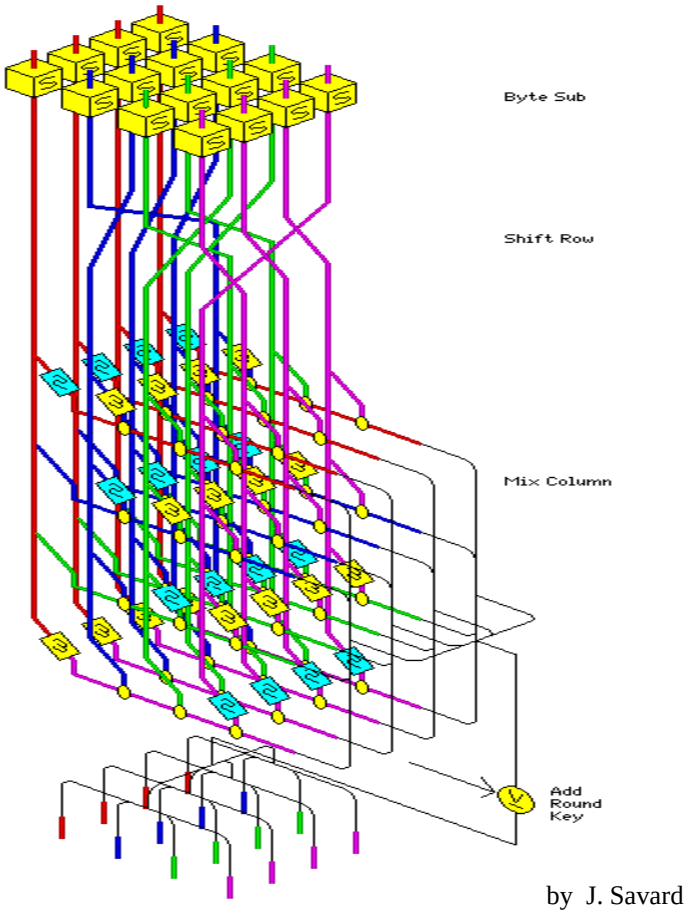




DES - Data Encryption Standard

- Marco da criptografia moderna
- Nunca foi quebrado
- Padrão do governo americano na década de 70
- Ciframento em blocos de 64bits
- Chaves de 56 bits
- Ainda o mais usado, mas já foi superado pela velocidade do hardware na forma simples
- Muito usado com ciframento duplo ou triplo

Simétrico II - o AES

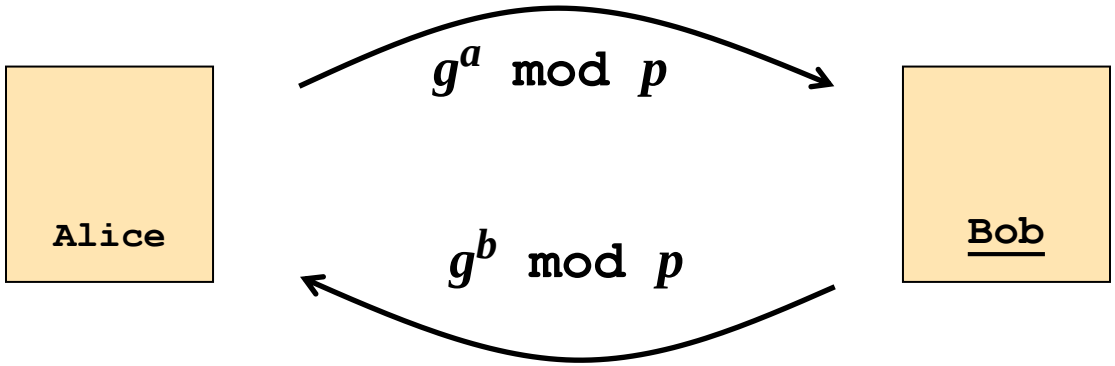


AES - Advanced Encryption Std.

- Recentemente definido como o padrão FIPS (E.U.A.) substituto do DES p/ info não-classificada
- Resultou da cooperação de 4 anos entre governo, indústria e universidades que culminou num processo de seleção finalizado em outubro de 2000
- Chaves e blocos de 128, 192 e 256 bits
- Operações são simples, até 13 rodadas da operação ilustrada

Método de Diffie-Hellman

Solução para o estabelecimento da chave - II



- os valores *a* e *b* são secretos, exceto para Alice e Bob, respectivamente
- *g* e *p* são parâmetros públicos
- Alice e Bob calculam a informação secreta

$$g^{ab} \bmod p$$

Assimétricos I - o RSA

- Chave Pública é (e,n)
- Chave Privada é d
- $n = p \times q$, p e q primos secretos
- $e \times d \equiv 1 \bmod (p-1)(q-1)$

Ciframento de x

$$y = x^{e} \bmod n$$

Deciframento de y

$$x = y^{d} \bmod n$$

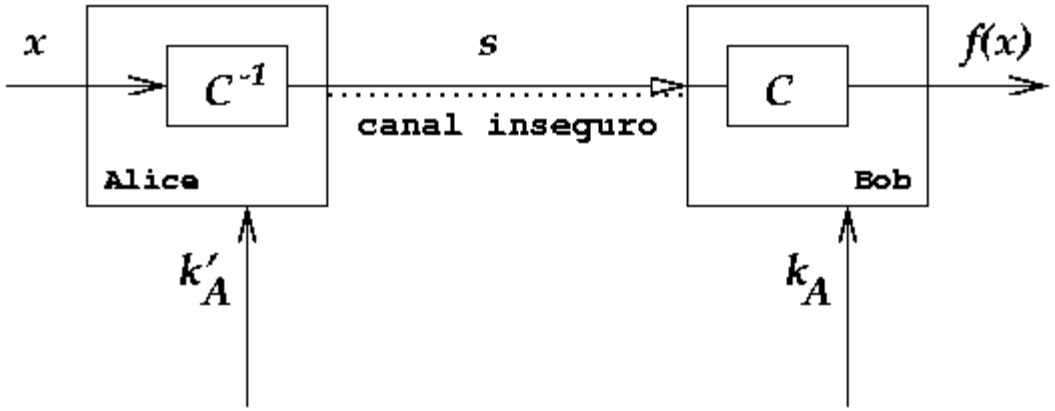
- O mais popular dos sistemas assimétricos. Proposto em 1977 por Rivest, Shamir e Adleman.
- Baseia sua força na dificuldade de se fatorar números grandes eficientemente.

Assimétricos II - Curvas Elípticas

- Sistemas baseados em curvas elípticas extraem sua força da dificuldade de se calcular o logaritmo discreto em uma estrutura algébrica especial: o grupo de pontos com coordenadas inteiras de uma certa família de curvas cúbicas em duas variáveis, chamadas de curvas elípticas.
- Os melhores algoritmos para resolver este problema são menos eficientes do que os melhores algoritmos para fatoração de inteiros, para números da mesma magnitude.
- Estes sistemas, com chaves de 180 bits, têm robustez equivalente a sistemas RSA com chaves de 1000 bits. São preferíveis em ambientes restritos computacionalmente.

Assinaturas Digitais

- Sistemas assimétricos trouxeram consigo também a possibilidade das assinaturas digitais.



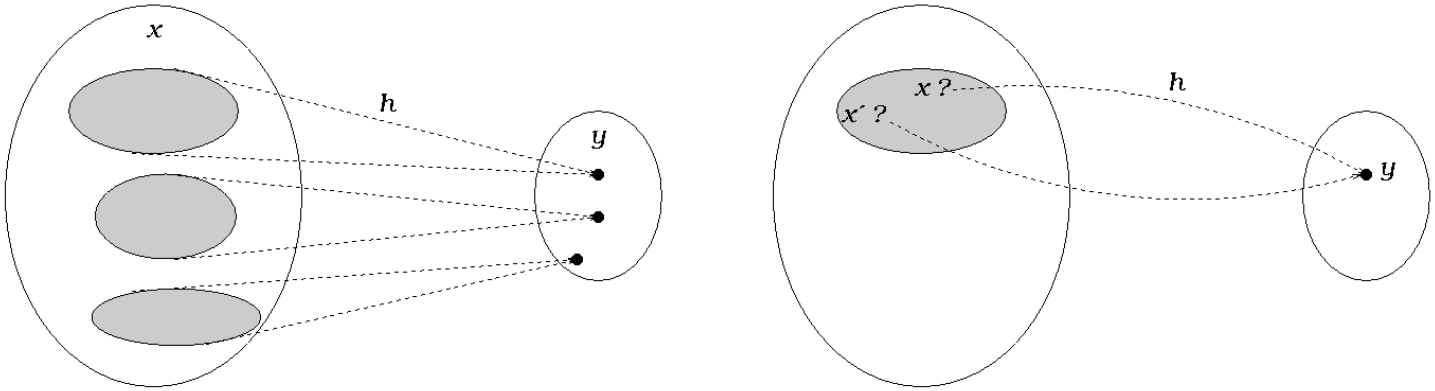
Alice assina a mensagem ***x*** usando sua chave privada k'_A e Bob verifica a assinatura ***s*** com k_A.

Hashing Criptográfico

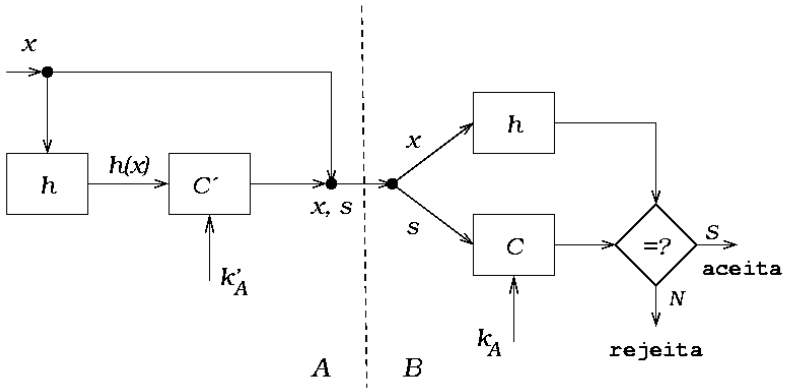
$$h : X \rightarrow Y$$

- x tem tamanho aribitrário e $h(x)$ tem tamanho fixo

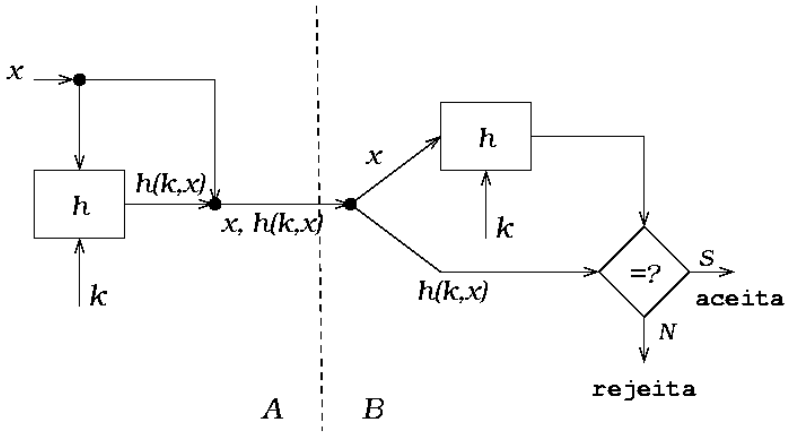
  $\Rightarrow$ colisões são inevitáveis.
- São unidirecionais e resistentes a colisões



Hashing - Utilidade

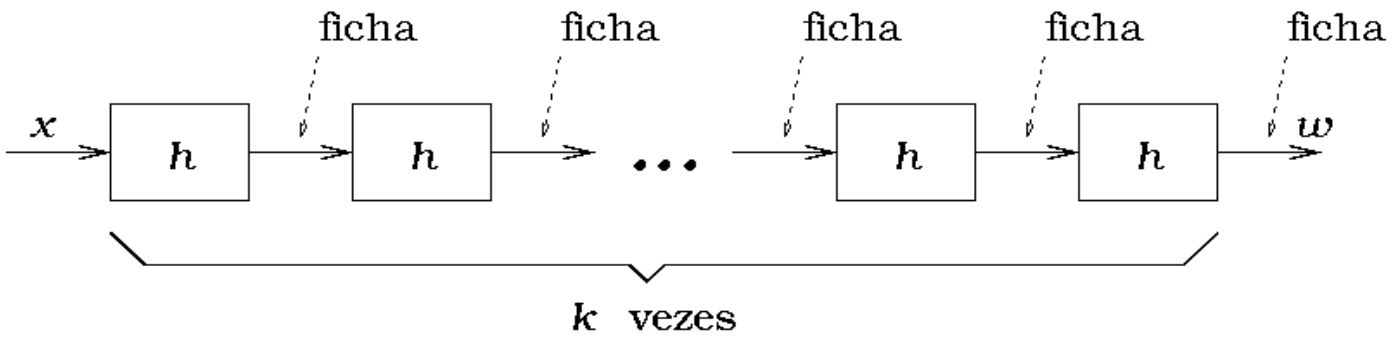


- **Compressão de assinaturas** assinar x ou $h(x)$ é equivalente pelas propriedades da função h. Mas $h(x)$ é muito mais compacta.



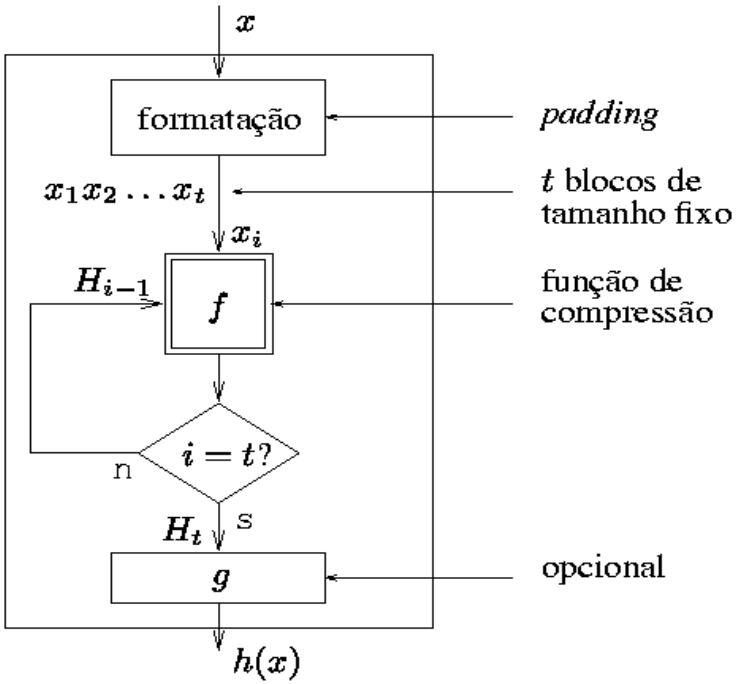
- **Gerar códigos de autenticação** a posse da chave secreta k apenas por A e B garante autenticação mútua.

Hashing - Outros Usos



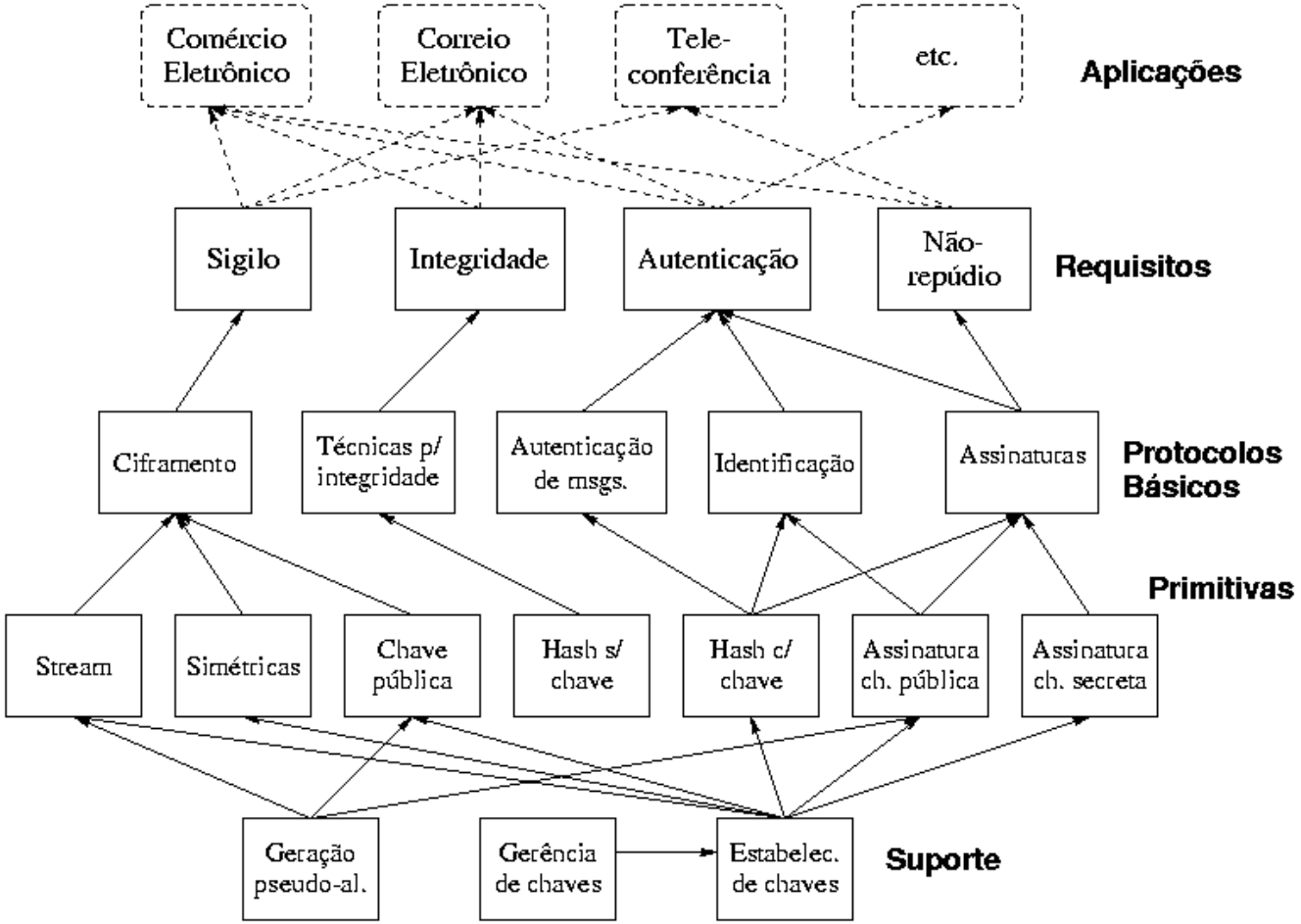
- **Simulação de "tokens".** Cada uma das *k* fichas tem valor fixo e são gastas do fim, *w*, para o começo, *x*.
- Comprador envia inicialmente *w* ao vendedor e gasta fichas enviando valores anteriores.

Hashing - Construção



- Várias funções populares usam este esquema, entre elas MD-5, SHA-1.
- Função de compressão é baseada em um algoritmo simétrico de ciframento ou num algoritmo dedicado.

Todos os pedaços



Roteiro

- Proteção da Informação
- Técnicas para proteção do conteúdo da informação
- **Aplicações**
- Conclusões

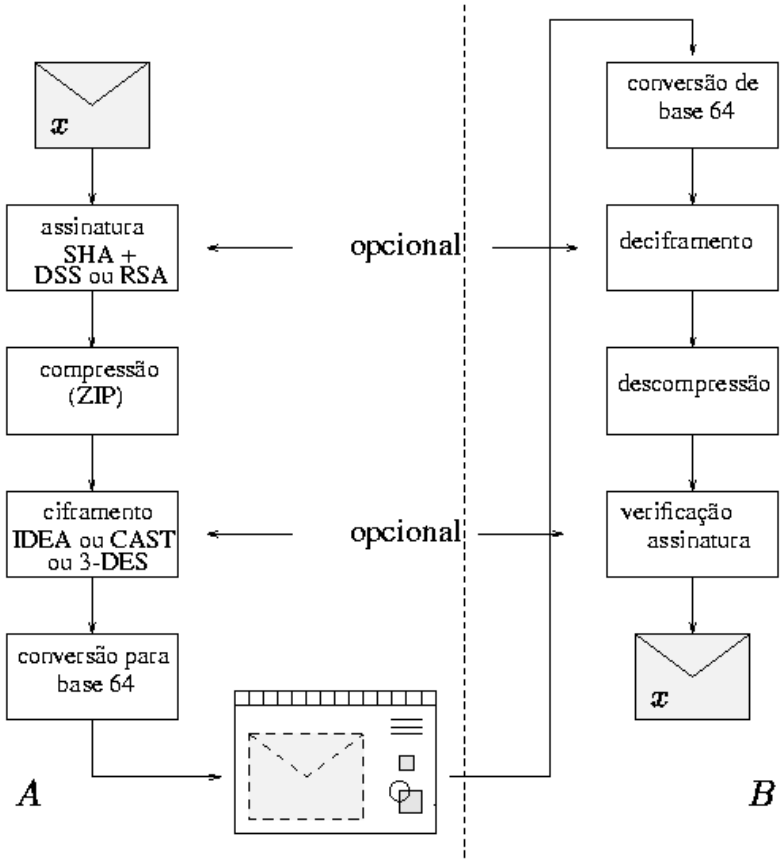
PGP (Pretty Good Privacy)

- Phil Zimmermann criou o PGP: um sistema público, barato e de código aberto.
- Bem implementado, flexível e com toda a estrutura criptográfica necessária.
- Preferido para uso individual. S/MIME, uma versão segura do formato MIME, é recomendado para sistemas corporativos.

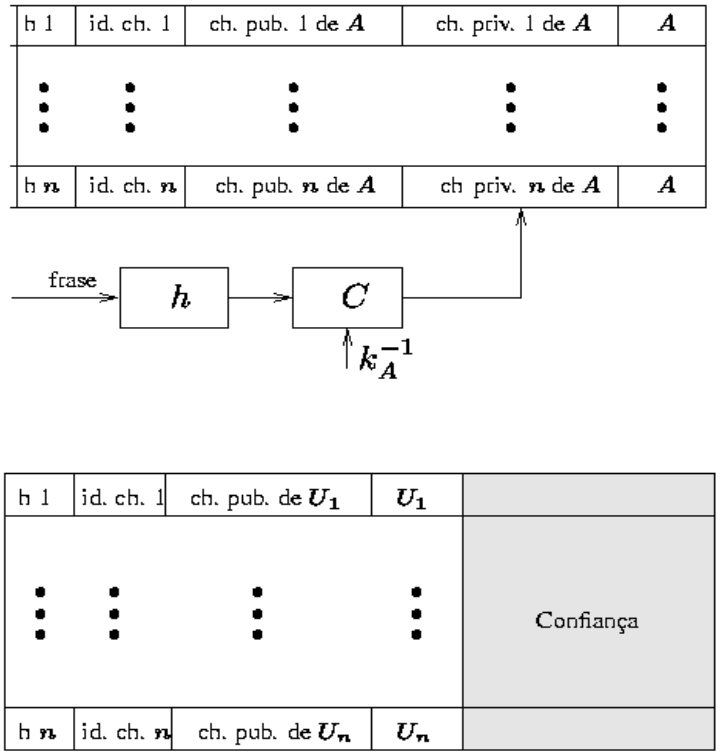
PGP - Serviços

- Confidencialidade
- Autenticação via assinaturas
- Geração de chaves
- Gerenciamento de chaves - chaveiros
- Compressão
- Fragmentação
- Empacotamento em BASE-64

PGP - Esquema Geral



Chaveiros do PGP



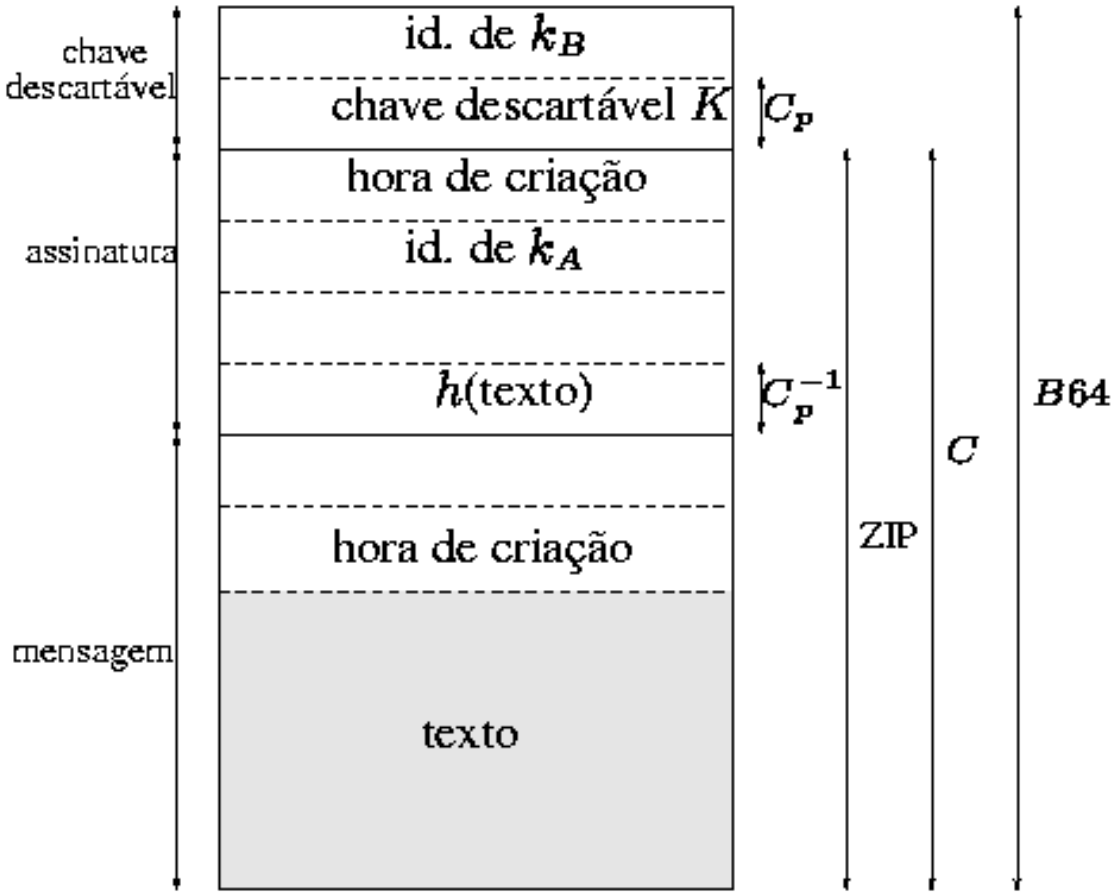
- **Chaveiro privado** contém os vários pares de chaves públicas e privadas do usuário. Chaves privadas são cifradas usando uma passphrase.
- **Chaveiro público** contém todas as chaves públicas conhecidas pelo usuário, juntamente com o grau de confiança em cada uma.

PGP - confiança e certificação

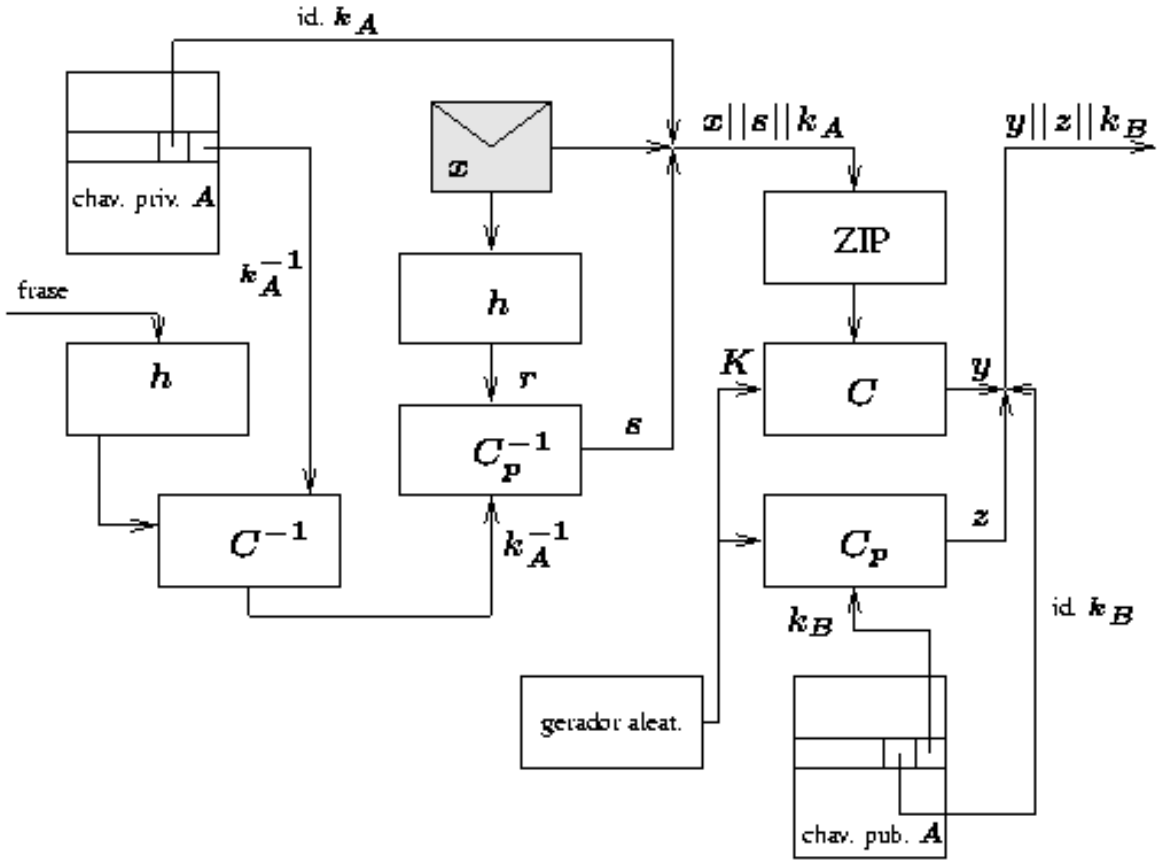
- Dispensa o uso de autoridades certificadoras.
- Constrói a própria rede de confiança de forma gradual e unilateral.
- O nível de confiança (KL) numa chave pública baseia-se na própria confiança do usuário (OT) e na confiança de terceiros, representadas pelas assinaturas S_{u1}, S_{u2} etc

KL	OT	$S_{u_1}, S_{u_2} \ldots$	$S^t_{u_1}, S^t_{u_2} \ldots$

PGP - Formato das mensagens



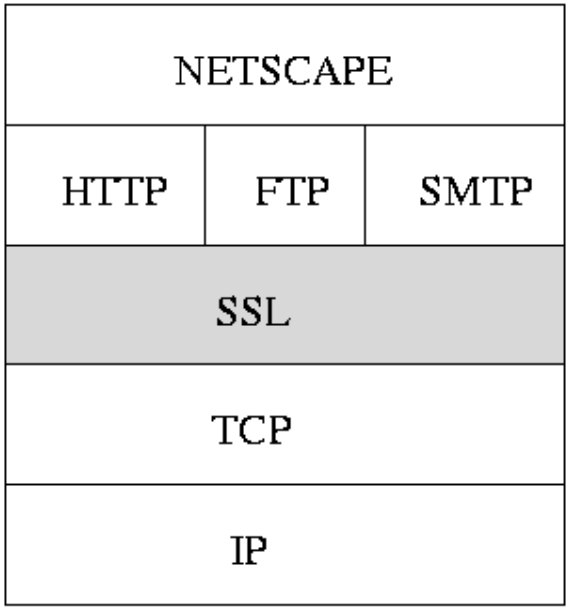
PGP - Esquema Detalhado

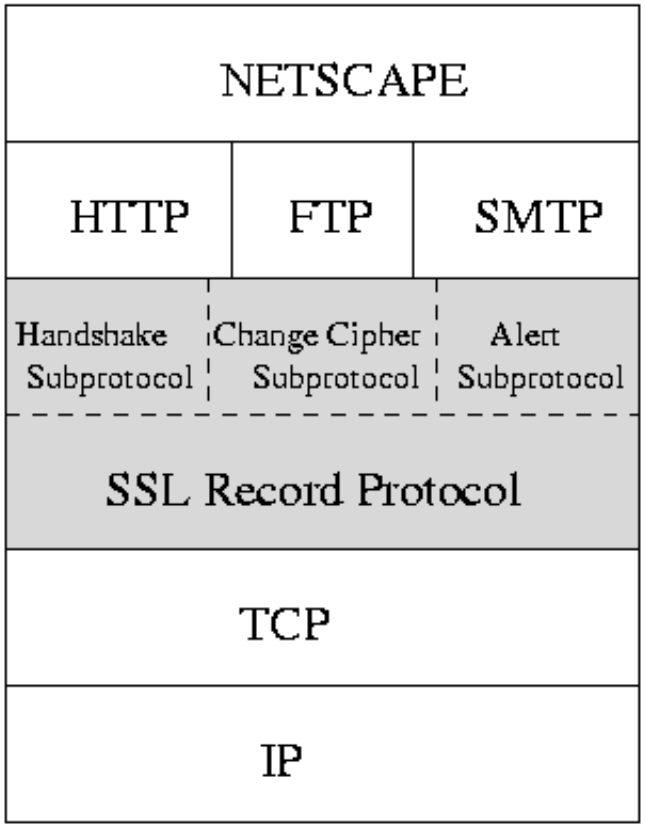


SSL (Secure Socket Layer)

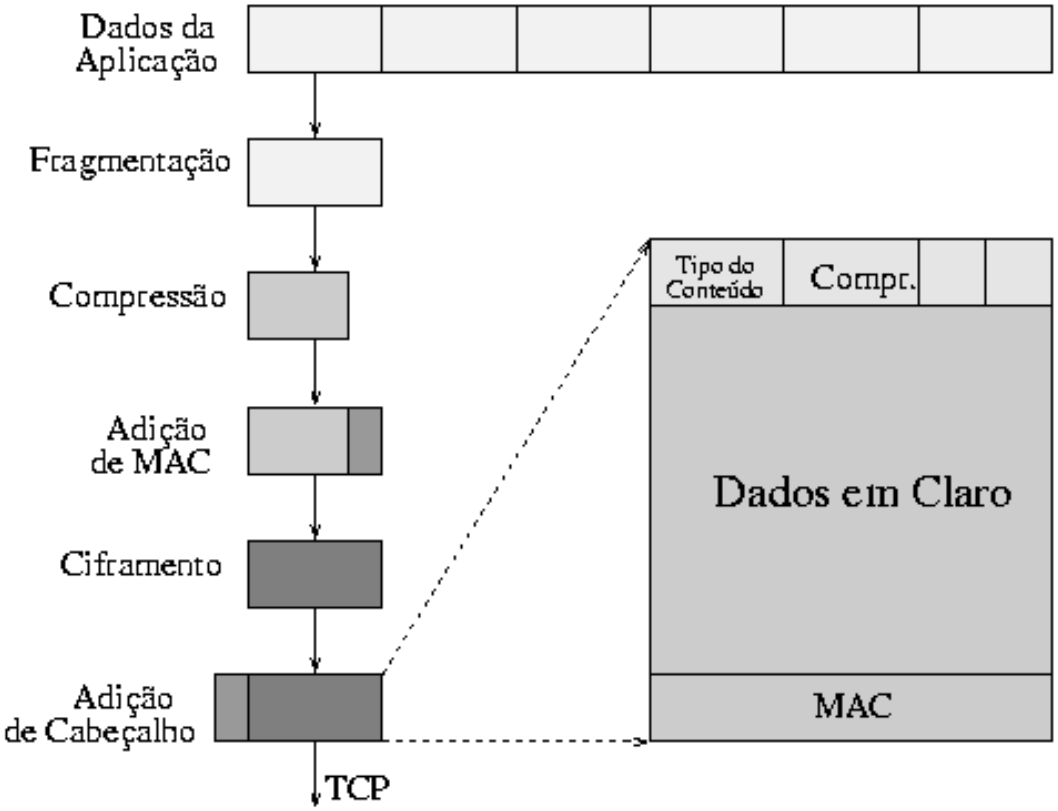
- Camada entre TCP/IP e aplicações destinada a possibilitar conexões seguras.
- Uma vez abertas conexões, algoritmos e chaves são negociados entre cliente e servidor.
- Provê sigilo e autenticação de dados.
- Pode ser instalado como parte da suíte TCP/IP ou como parte de aplicações.

SSL - Localização

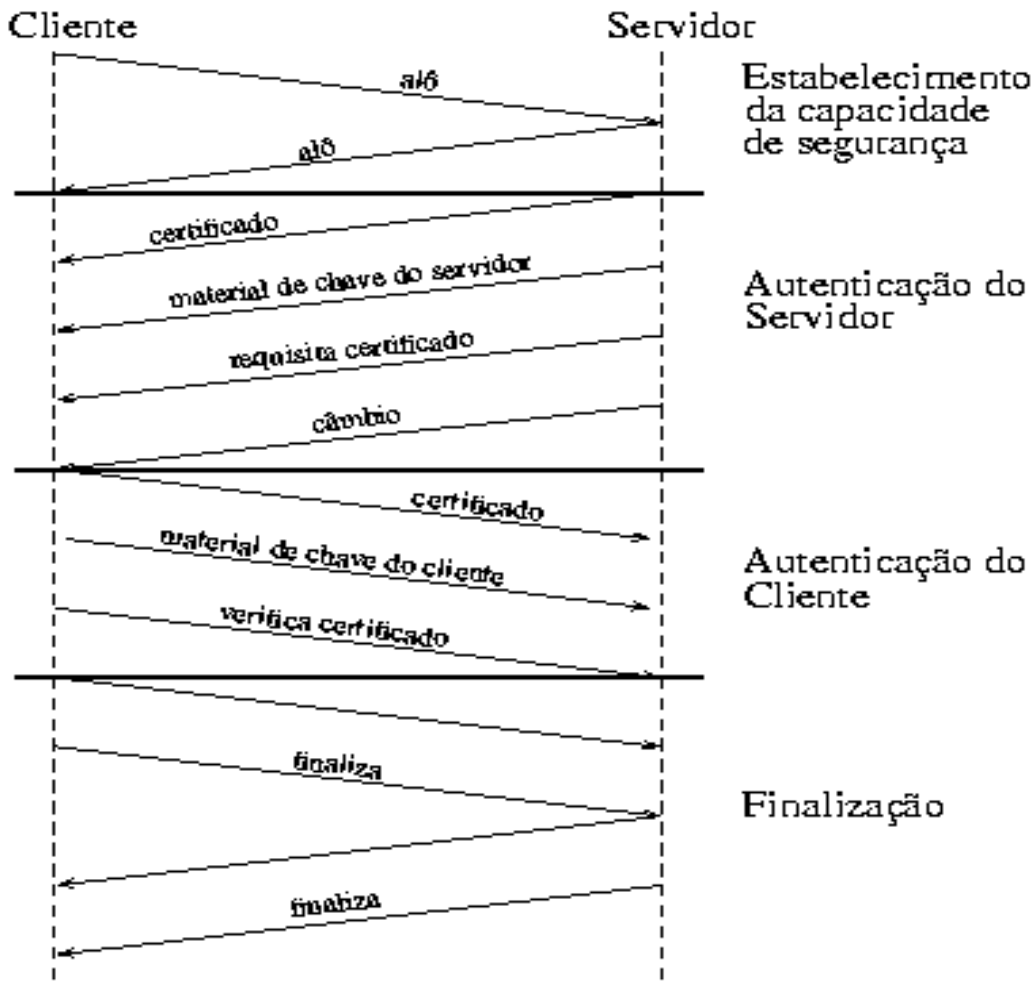




SSL - Record Protocol



SSL - Handshake



Roteiro

- Proteção da Informação
- Técnicas para proteção do conteúdo da informação
- Aplicações
- **Conclusões**

Um resumo das defesas

- PGP, S/MIME: correio eletrônico seguro
- SET: comércio eletrônico seguro
- SSL - TLS: conexões WWW seguras
- SSH: login remoto seguro
- IPSec: conexões IP seguras
- Firewalls: proteção de sub-redes
- Kerberos: infra-estrutura para autenticação em redes
- PKI’s ou IPC’s: infra-estrutura de chaves criptográficas
- IDS: Monitoramento para detecção de intrusão
- Hardware seguro

Conclusões

- Criptografia é a resposta técnica para a maioria dos desafios.
- O uso correto destas técnicas é fundamental
- Não dispensam o uso de outras práticas e disciplinas de segurança.
- Pode ser uma arma quando mal usada. Questões como registro público de chaves e restrição ao uso deverão ser temas de política governamental no futuro próximo.