Transmissão Segura de Informações via Internet

O que é Criptografia

- Ciência que usa a Matemática para criptografar e desencriptar dados
- Permite o envio de informação confidencial através de meios de comunicação inseguros, como por exemplo a Internet
- Impede que informações sigilosas sejam lidas por outro que não o destinatário da mensagem
- Arte de escrever mensagens secretas

Terminologia

- Criptografia
  - Palavra de origem grega
    - Kryptos - Escondido
    - Graphia - Escrita
- Criptoanálise
- Processo de se tentar descobrir o conteúdo original de textos cifrados sem a chave

Criptografia

- Utilizada desde os tempos egípcios
- Proteção de comunicação em tempos de guerra
  - Mensagens cifradas de Júlio César
  - Guerra civil americana
  - Enigma na Alemanha
- Diplomacia e política
- *The Adventure of the Dancing Men" (*Sherlock Holmes*)*

Mensagens Cifradas de Júlio Cesar

ABCDEFGHIJKLMNOPQRSTUVWXYZ

rotação de 13 posições

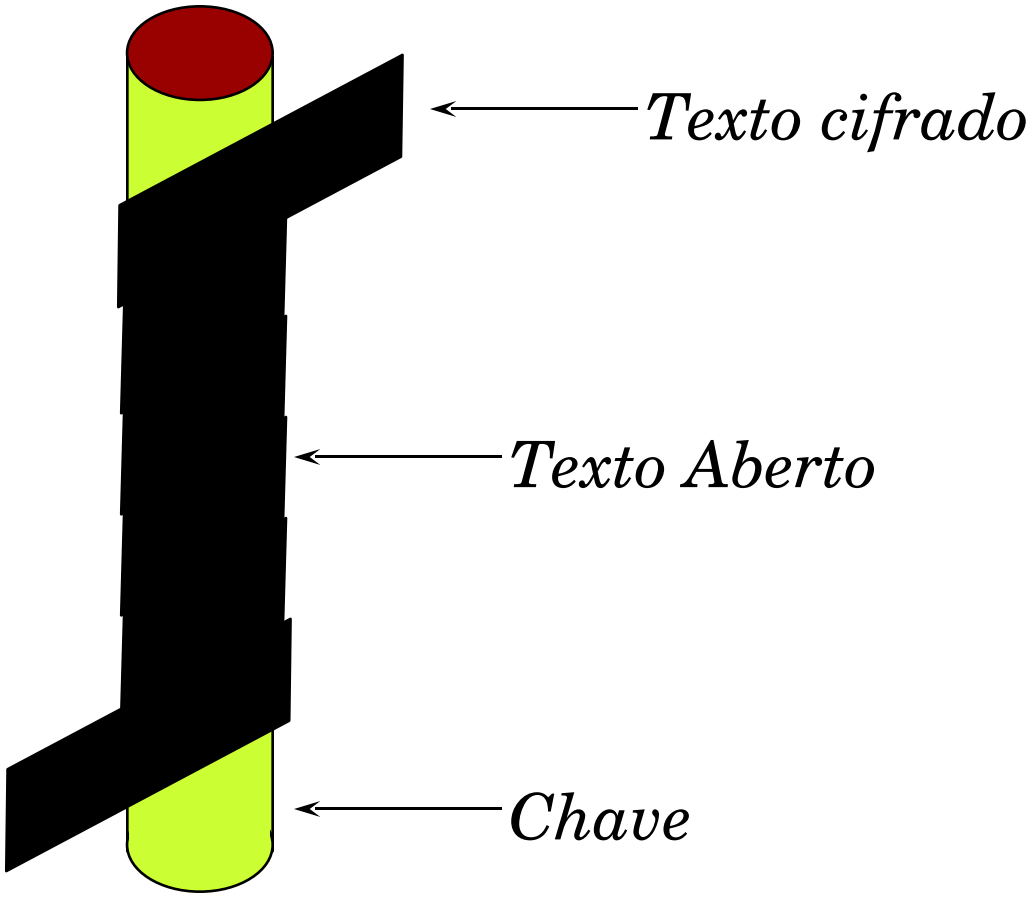
NOPQRSTUVWXYZABCDEFGHIJKLM

THE GOTHS COMETH — *Texto aberto*

13 — *chave*

FUR TAFUE PAYRFU — *texto cifrado*

Criptografia Simples



Encriptação por Rotação de Chaves

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
BCDEFGHIJKLMNOPQRSTUVWXYZA
CDEFGHIJKLMNOPQRSTUVWXYZAB
DEFGHIJKLMNOPQRSTUVWXYZABC
EFGHIJKLMNOPQRSTUVWXYZABCD
FGHIJKLMNOPQRSTUVWXYZABCDE
GHIJKLMNOPQRSTUVWXYZABCDEF
HIJKLMNOPQRSTUVWXYZABCD...
```

SOUND THE RETREAT — *texto aberto*

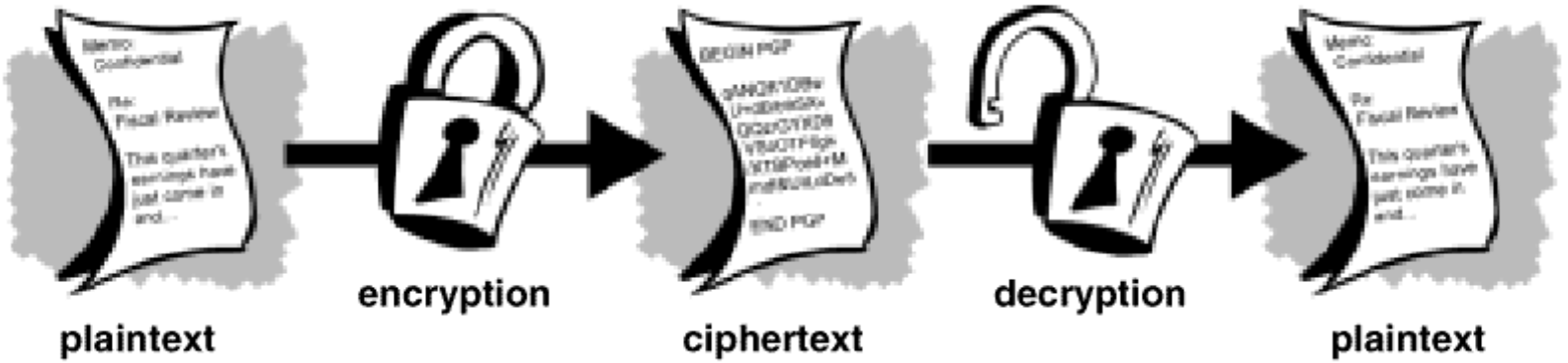
DEADFED — *chave*

VSUPC XKG UEWWEX — *texto cifrado*

Tipos de Sistema Criptográficos

- Simétricos (chaves privadas)
  - utilizam a mesma chave para encriptar e desencriptar a mensagem
  - Inerentemente inseguros - como transportar a chave secreta do remetente para o destinatário sem comprometer sua integridade?
- Assimétricos (chaves públicas)
  - utilizam uma chave pública para a encriptação e uma chave privada para desencriptação

Criptografia Simétrica (Chave Privada)



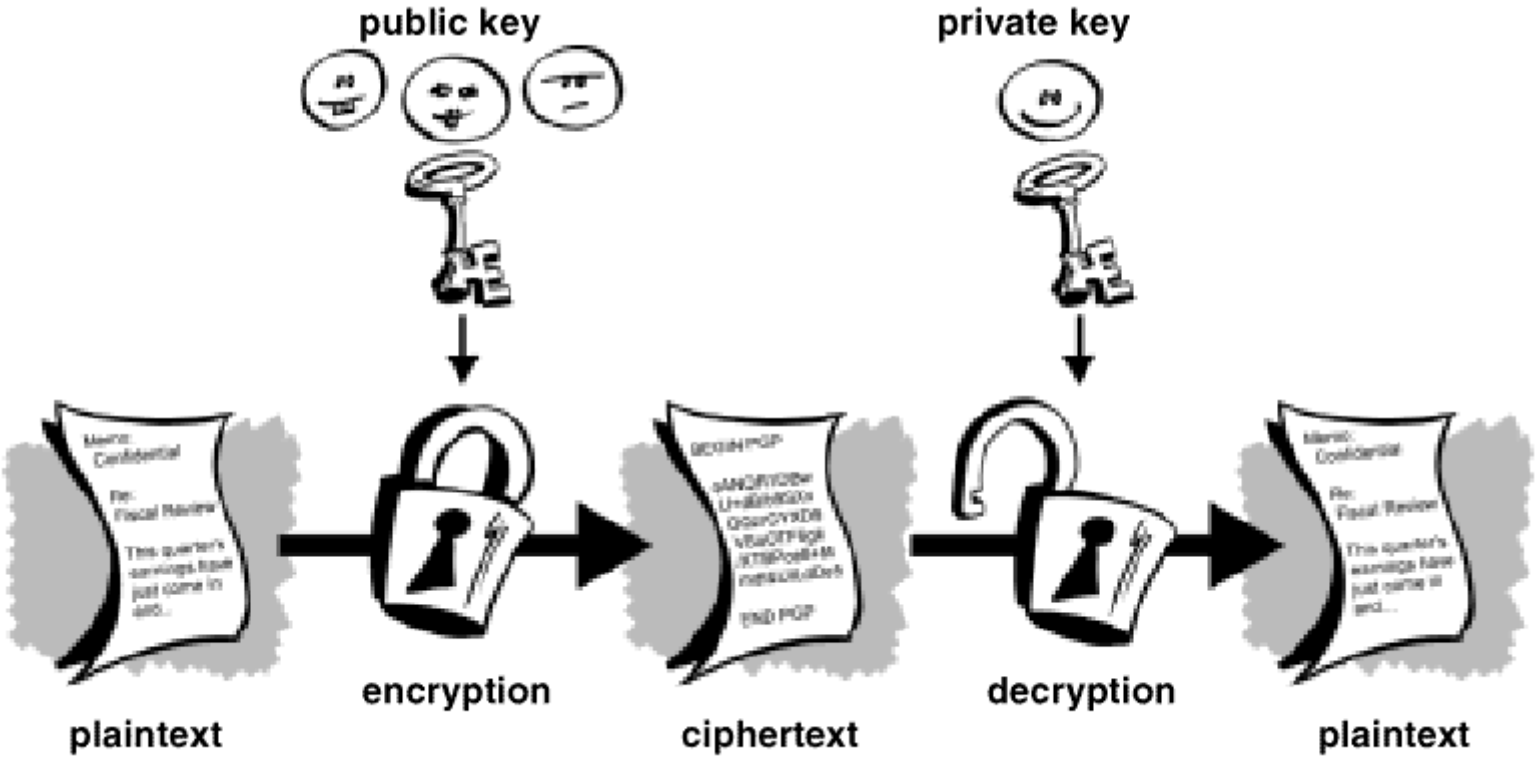
Criptografia Simétrica (Chave Privada)

- Exemplos: *DES, RC4, RC5, IDEA, Skipjack*
- Vantagens: *rápido, texto cifrado seguro*
- Desvantagens: a chave precisa ser distribuída com antecedência e não pode ser divulgada

Criptografia de Chaves Públicas

- Possibilidade de troca segura de mensagens
- Elimina a necessidade do compartilhamento de chaves secretas entre destinatário e remetente de mensagens
- Apenas as chaves públicas transitam. As chaves privadas não precisam ser transmitidas ou compartilhadas
- Ao contrário da criptografia tradicional, a criptografia de chaves públicas está ao alcance de todos

Criptografia de Chaves Públicas



Encriptação com Chaves Públicas
Principais Características

Características	*Técnica*
•Encriptação/Desencriptação Rápida	Envelopes digitais
•Autenticação Remetente	Assinatura digital
•Verificação da integrida	Resumo da mensagem
•Distribuição segura de chaves públicas	Autoridades Certificadoras

Criptografia forte

- O poder da criptografia é definido pela quantidade de recursos necessários para, a partir de um texto criptografado, se obter o texto original
- Um bilhão de computadores realizando um bilhão de cálculos por segundo não seriam capazes de decifrar um texto cifrado com criptografia forte antes do fim do universo (em 25 milhões de anos)

Encriptação e o Sistema Legal Americano

- O algoritimo RSA é patenteado dentro dos EUA. Esta patente não é reconhecido pela lei internacional de patentes
- Dentro dos EUA é obrigatório o pagamento de licenciamento para usar o algoritmo
- Uso gratuito fora dos EUA
- Chaves fortes de encriptação são classificadas como armamento pela lei de exportação americana
  - É considerado crime a exportação de software com encriptação forte
  - Browsers e servidores são limitados a usar chaves de 40 bits

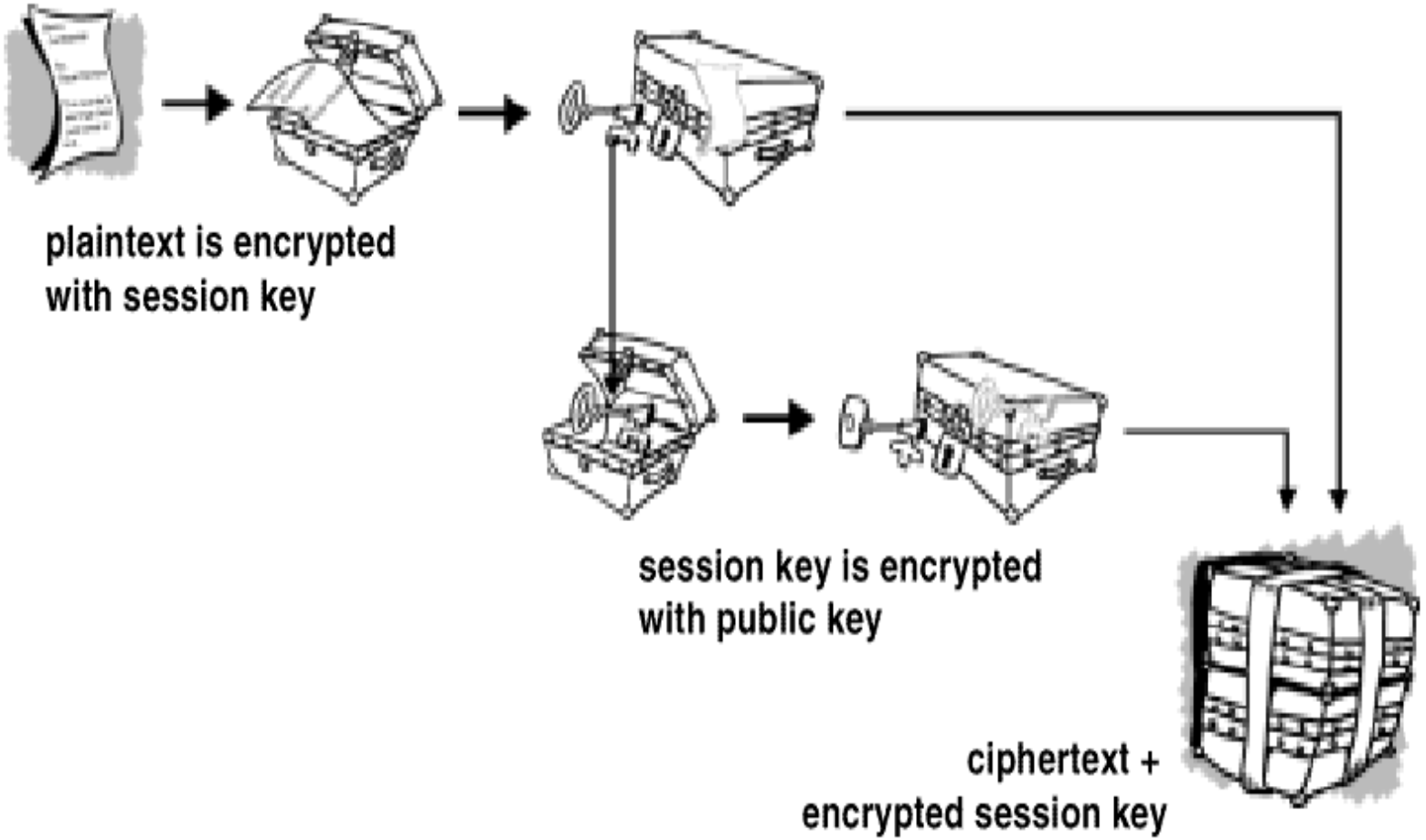
PGP

Pretty Good Privacy

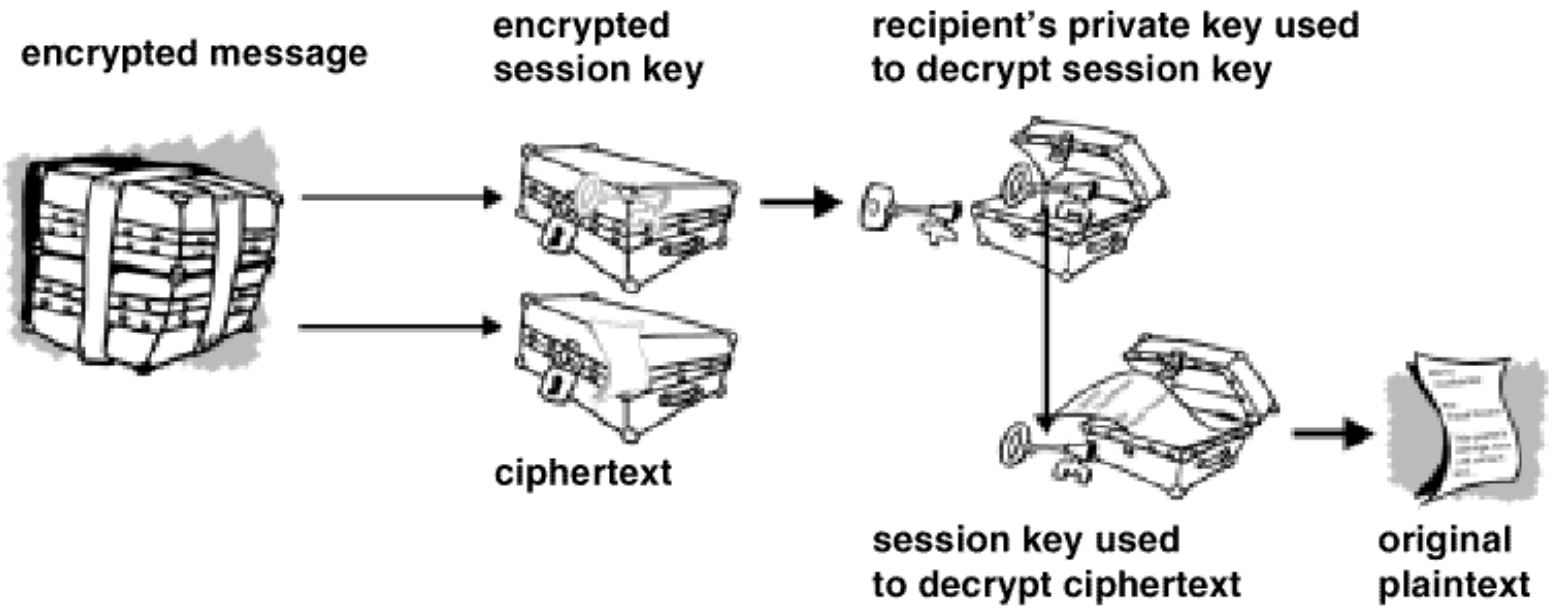
PGP: Pretty Good Privacy

- Desenvolvido por Phil R. Zimmerman
- Combina o melhor da criptografia convencional e de chaves públicas
- Sistema híbrido
- Web of trust
- Disseminado mundialmente

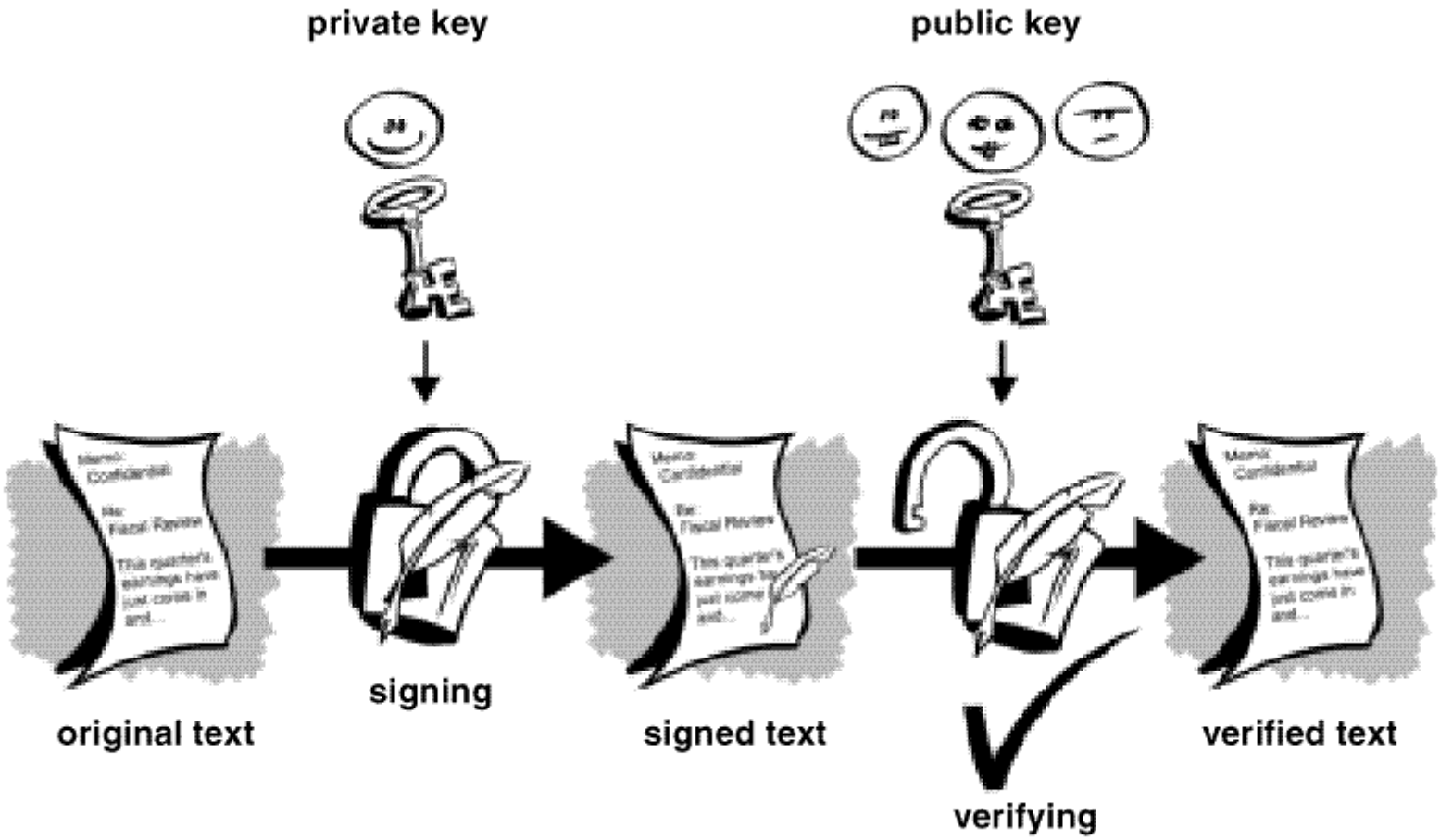
PGP: Encriptação dos Dados



PGP: Desencriptação dos Dados



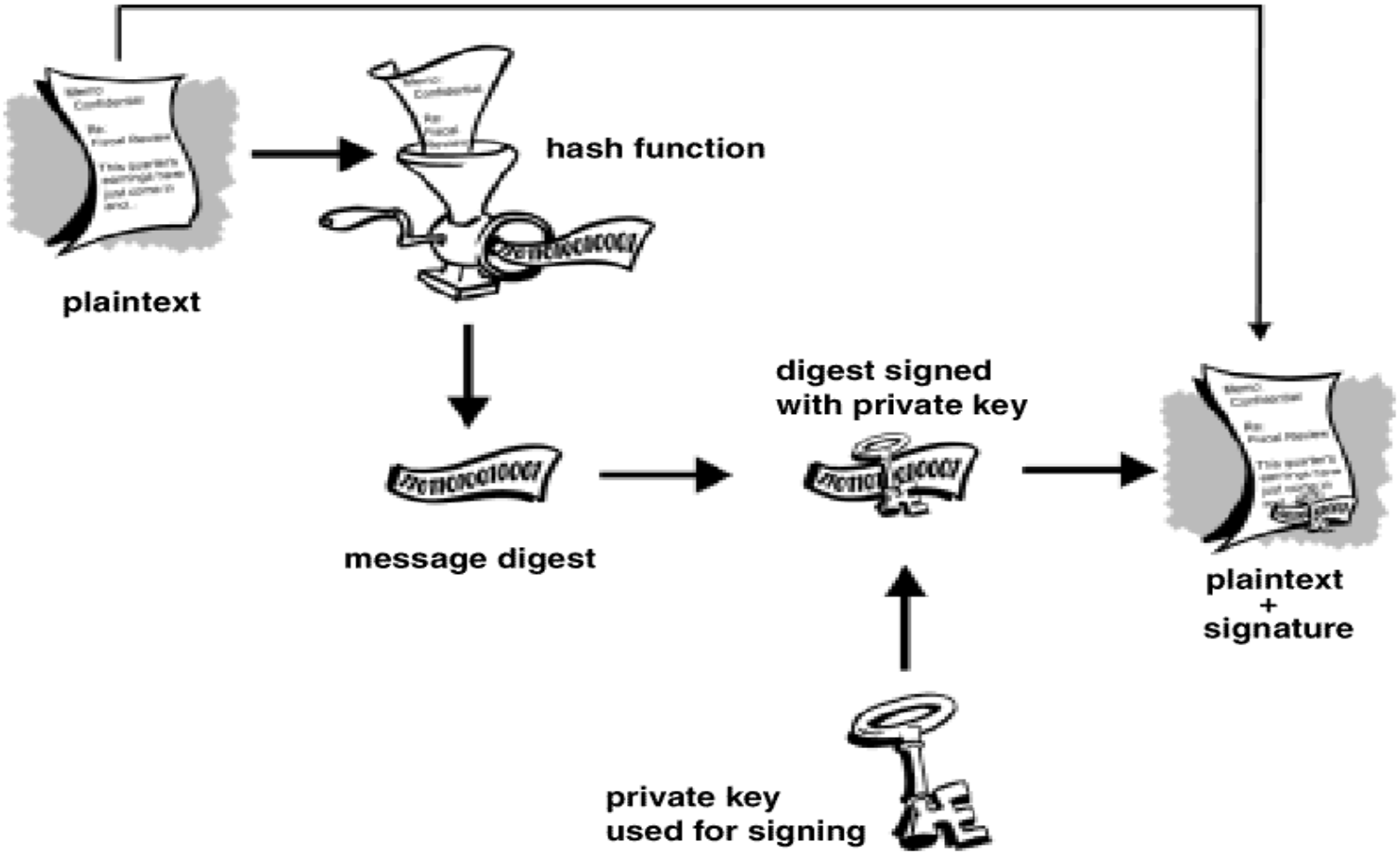
Assinaturas Digitais



Assinaturas Digitais

- Verificação da autenticidade da origem da informação
- Integridade da informação
- Garante o não repúdio de mensagens
- Praticamente impossíveis de serem falsificadas
- Autenticam não apenas a origem da informação como também o seu conteúdo

Funções Hash



Certificados Digitais

- Dados que funcionam de forma semelhante a certificados físicos
- Informação que é incluída juntamente com chave pública que serve para verificar se uma chave é genuína ou válida
- São usados para impedir que a chave de uma pessoa seja substituída por outra
- Simplificam a tarefa de se estabelecer se uma chave realmente pertence ao seu dono

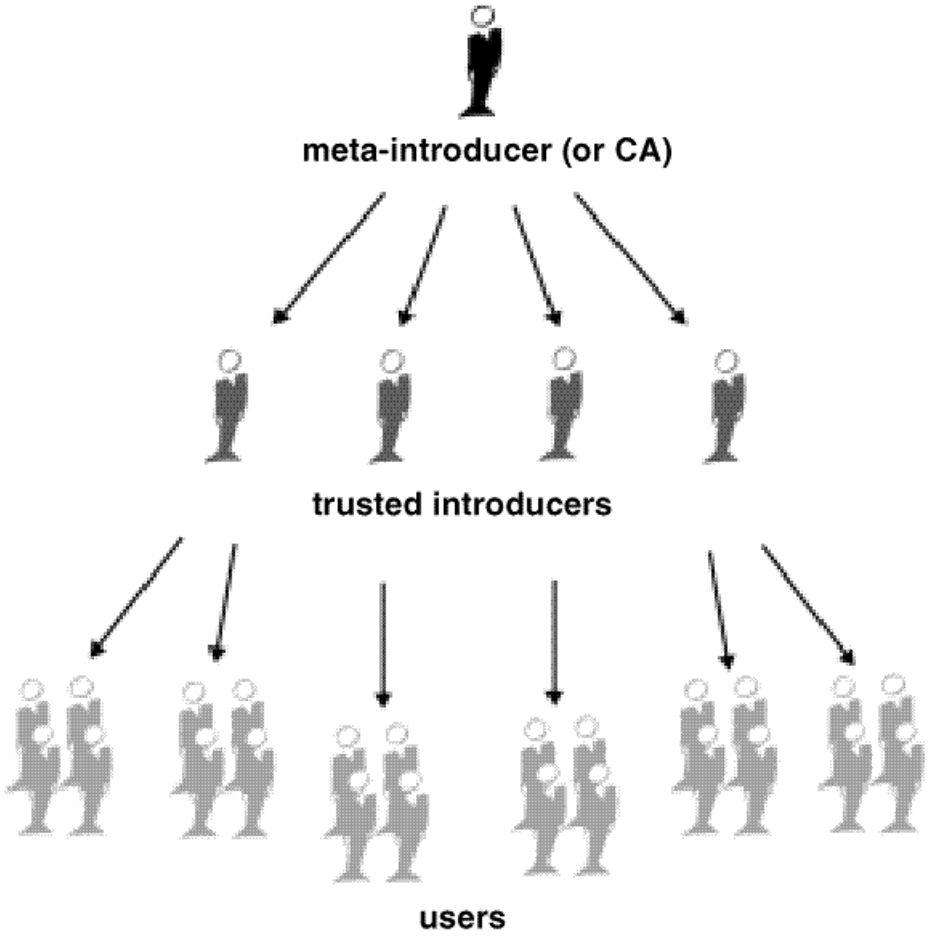
Certificados Digitais

- Um certificado digital consiste de três elementos:
  - Uma chave pública
  - Informação do Certificado (informações sobre o usuário como nome, identidade e outros)
  - Uma ou mais assinaturas digitais

Validade e Confiança

- Validade é a confiança de que a chave pública realmente pertença ao seu dono declarado
  - Assinatura de chaves públicas
  - Certification Authorities (CA)
  - Servidor de Certificados

Apresentadores



Estabelecimento de Confiança

- Apresentadores: Meta e Confiáveis
- Modelos de confiança
  - Direta
  - Hierárquica
  - Rede (Web of Trust)

PGP: Níveis de Confiança

- Níveis de Confiança
  - Completa
  - Parcial
  - Nenhuma
- Níveis de Validade
  - Válido
  - Parcialmente válido
  - Inválido

Particionamento de Chaves

- Permite que uma chave privada seja dividida entre várias pessoas
- Útil em situações onde mais de uma pessoa precisa responder em nome de sua empresa
- Número mínimo de partes para tornar a chave válida
- Reconstituição da chave através da rede

PGP: Proteção de Dados

- Encriptação de partes do conteúdo do disco rígido
- Arquivos realmente apagados
- Plug-ins para uso com correio eletrônico
- Limpeza do espaço livre

Integração com Correio Eletrônico

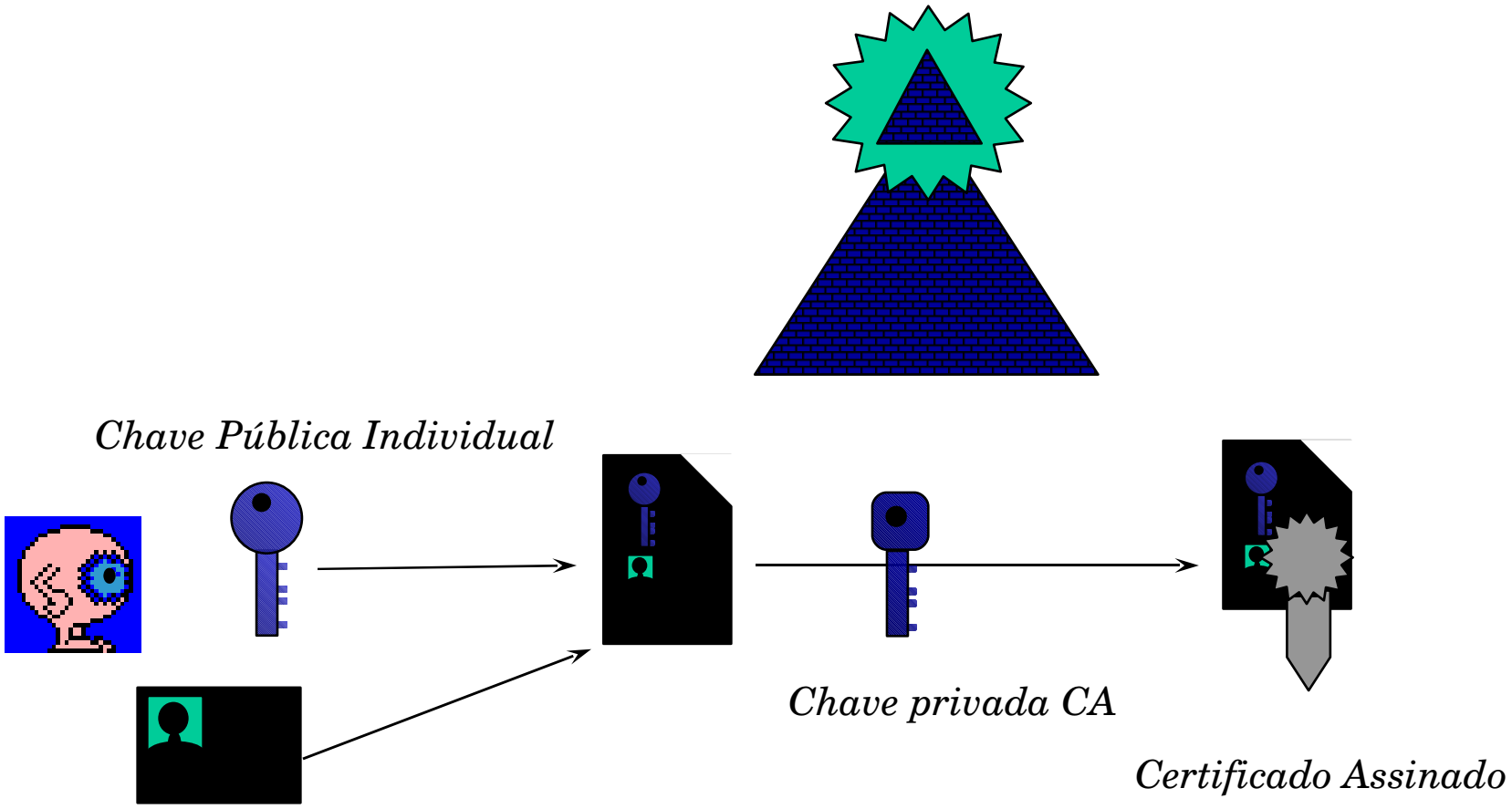
- Email tradicional é como um cartão postal escrito a lápis
- Integração com Outlook Express, Eudora, Outlook 98
- Utilização também com outras ferramentas através do Clipboard
- Visualizador Seguro (TEMPEST)

Segurança naWeb

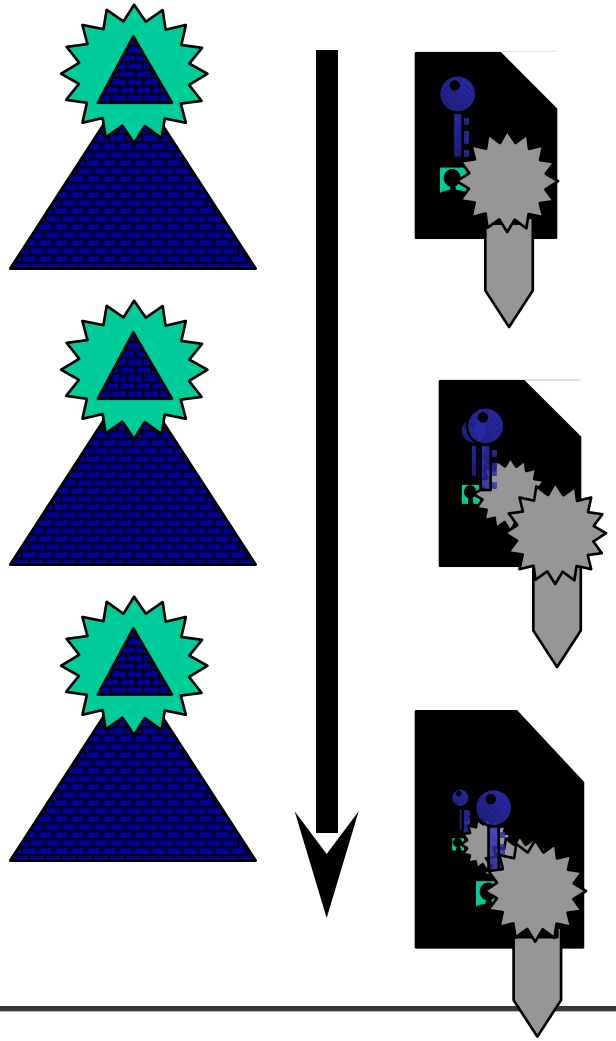
Criptografia de Chaves Públicas na Web

- Secure Socket Layer (SSL)
  - Netscape Communications Corporation
- Secure HTTP (SHTTP)
  - Commerce Net

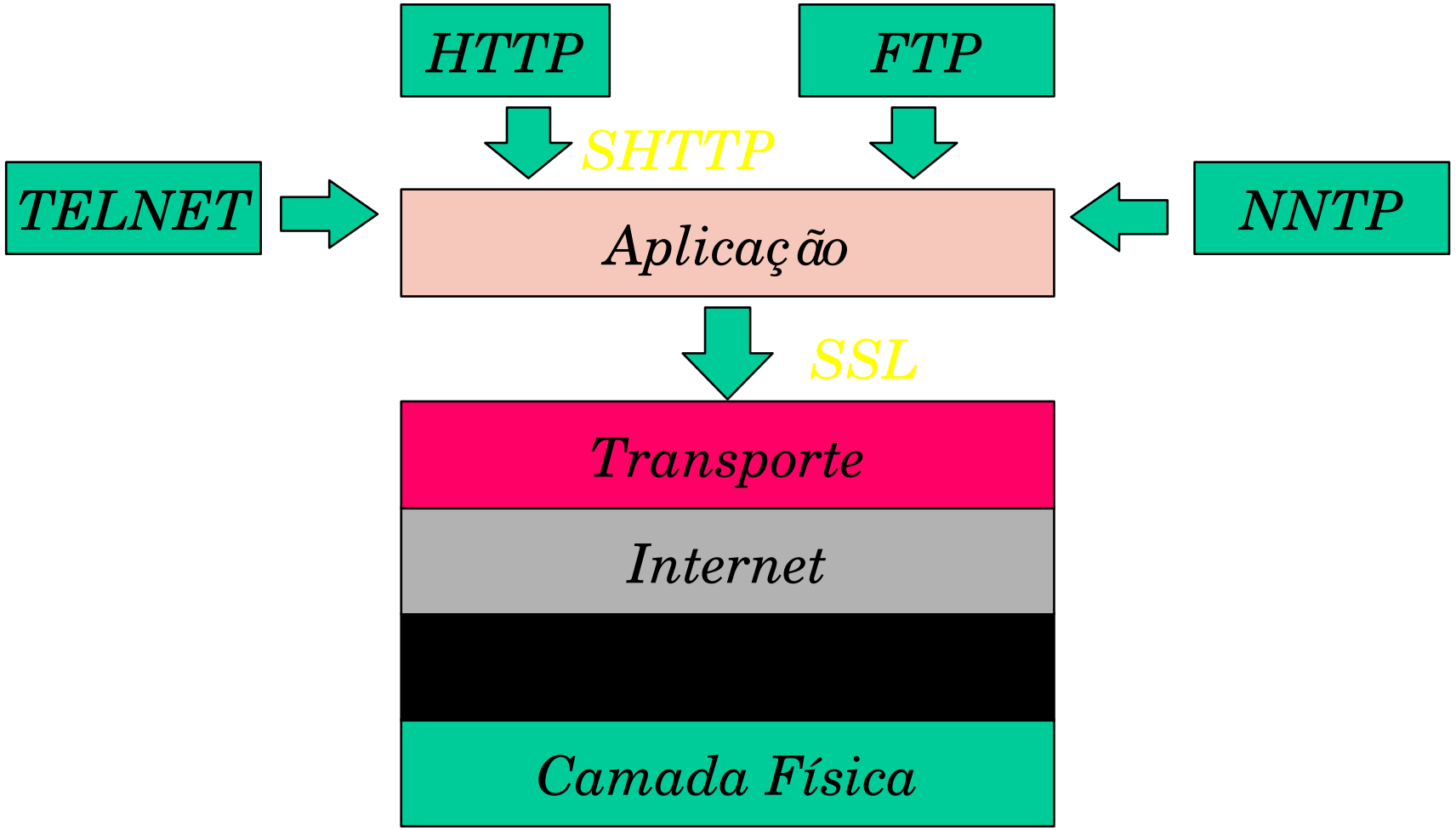
Autoridades Certificadoras (Certifying Authorities)



Hierarquia de Confiança



SSL and SHTTP



Servidores Seguros

- Netscape Commerce Server
- Microsoft Internet Information Server
- WebSite Professional
- Quarterdeck/WebSTAR Professional
- OpenMarket Secure Server
- Apache SSL
- e muitos outros ...

Servidores Seguros: Custos

- Software Servidor
  - Necessária licença empresa RSA Data Security
  - Gratuita para uso não comercial
  - $200-$1000 for uso comercial
  - Exportação para fora dos EUA proibida
- Certificado do Servidor
  - $290 para certificado inicial
  - $95 para cada servidor adicional
  - $75 taxa anual de renovação

Certificado Assinado

```
          Signed by the Certification Authority nicknamed:
                    RSA Data Security, Inc.
                     Serial No.: 0000000839194656
                  Organization : The Capricorn Organization
              Organization Unit :
                         E-Mail : lstein@capricorn.org
                    Common Name : www.capricorn.org
                     Valid From : Sun, Aug 04, 1996  21:37:36
                     Expires On : Fri, Aug 09, 1997  21:37:36
                       Location : Boston
                    State/Prov. : Massachusetts
                        Country : US
 Certificate Fingerprint (MD5) : 4b5573480dce5a676bbca43f22936c66
                  Certificate (PEM format):

-----BEGIN CERTIFICATE-----
MIIB6TCCAVICBDIFGCAwDQYJKoZIhvcNAQEEBQAwOTEcMBoGA1UEChMTWGNlcnQg
U29mdHdhcmUgSW5jLjEZMBcGA1UECxMQSW50ZXJuZXQgRGVtbyBDQTAeFw05NjA4
MDQyMTM3MzZaFw05NjA4MDkyMTM3MzZaMHcxCzAJBgNVBAYTAlVTMRYwFAYDVQQI
Ew1NYXNzYWNodXNldHRzMQ8wDQYDVQQHEwZCb3N0b24xIzAhBgNVBAoTGlRoZSBD
YXByaWNvcm4gT3JnYW5pemF0aW9uMRowGAYDVQQDExF3d3cuY2Fwcmljb3JuLm9y
ZzBnMA0GCSqGSIb3DQEBAQUAA1YAMFMCTADIuscTHRXfooKtE6Zt3QkOe9kgTCWL
DnUa8qhliklh0sKckHI+1LvITlIUXLXmWy3Pl93LlGZDYGB/ZrRACuuWLCQ2qwLk
7UtS2m0CAwEAATANBgkqhkiG9w0BAQQFAAOBgQB0+0aVrufX07MMlfnvO/W5s/jY
eD6AA6G2Q/72+/LptZGBL89E5fEJm0UV0cpVMTOc2KNjCZO0SpSqXdwKl2v5PVCF
VL5aIQLrTwMY/Gqu7XNGdNg9bfIraJfRmdBdLGYAlaMrrBmlu75lStrHtY8esJMM
UsgldxmB4HRsYtWfOA==
-----END CERTIFICATE-----
```

Falhas Detectadas SSL

- Dois incidentes bastante divulgados em 1995
- A chave de 40 bits usada em versões de software para exportação é vulnerável a ataques
  - Redes de estações de trabalho conseguem quebrar o código em algumas semanas de trabalho
  - Hardware especializado (possivelmente) pode realizar o mesmo em algumas horas
- Problema de implementação
  - A versão 2.0 do Navegador da Netscape usava chaves aleatórias previsíveis para gerar as chaves secretas
  - Mensagens quebradas em apenas alguns minutos em uma estação de trabalho convencional

Bibliografia

- An Introduction to Cryptography
Network Associates
http://www.nai.com
- PGP Windows 95, 98 and NT
User´s Guidehttp://www.nai.com
- Computer Security Basics
Deborah Russel and G.T. Gangemi Sr.O´Reilly and Associates

URLs

- Protocolo SSL
  - http://home.netscape.com/newsref/std/SSL.html
- Protocolo SHTTP
  - http://www.eit.com/projects/s-http/
- Verisign
  - http://www.verisign.com/
- RSA Data Security
  - http://www.rsa.com/