Minicurso Tópicos em Segurança da Informação
Parte 1 - Criptografia

I Workshop de Tecnologia de Redes do POP-BA
Ponto de Presença da RNP na Bahia

Italo Valcy <italo@pop-ba.rnp.br>

20 e 21 de setembro de 2010

Licença de uso e atribuição

Todo o material aqui disponível pode, posteriormente, ser utilizado sobre os termos da:

Creative Commons License:
Atribuição - Uso não comercial - Permanência da Licença

http://creativecommons.org/licenses/by-nc-sa/3.0/

Agenda

- Fundamentos de criptografia
  - Criptografia clássica
  - Criptografia assimétrica
  - Infraestrutura de chaves públicas
- Aplicações práticas
  - SSL – Secure Socket Layer
  - Outras aplicações

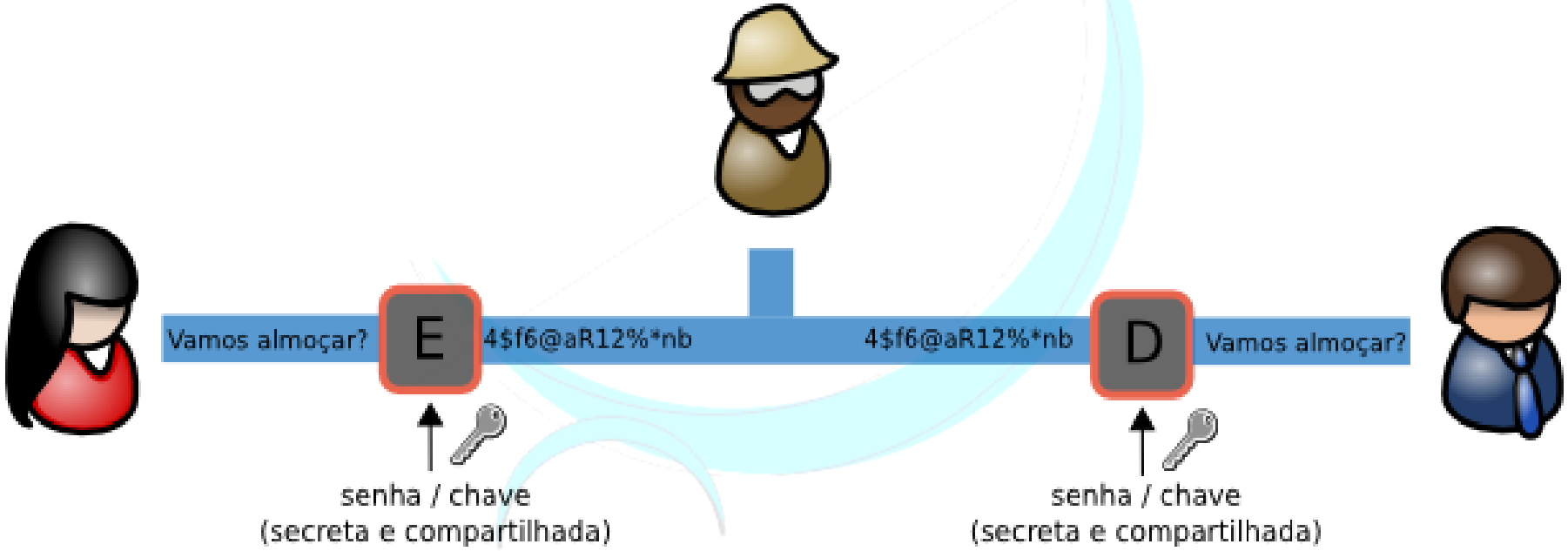
Introdução

- Criptografia
  - Criptografia (kryptós, “escondido”, gráphein, “escrita”)
    - Oculta mensagens de terceiros (legível apenas para o destinatário)
  - Criptoanálise
    - Decodificar mensagem sem conhecer a chave secreta
- Esteganografia
  - Ocultar mensagens dentro de outras

Definições

- Texto claro
  - Texto original, não cifrado
- Texto cifrado
  - Texto ilegível, não compreensível
- Cifrar
  - Transformar texto claro em texto cifrado
- Decifrar
  - Transformar texto cifrado em texto claro
- Chave
  - Conjunto de dados utilizados para cifrar e decifrar

Criptografia



Criptografia Clássica

- Cifradores monolíticos
  - Rearranjo do alfabeto original

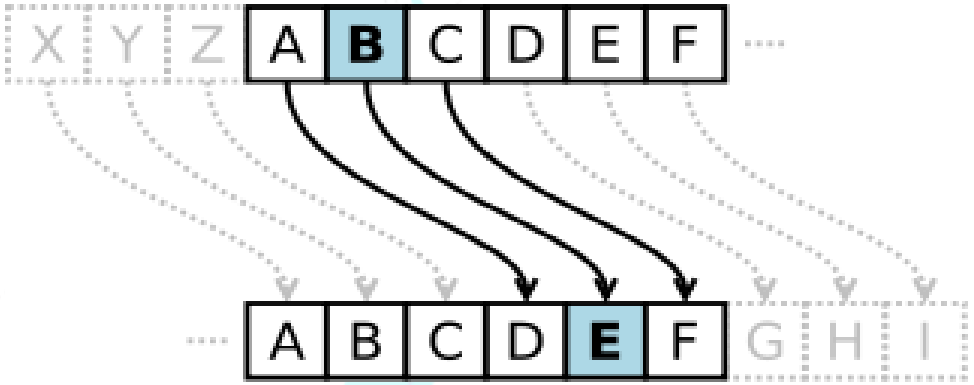
Exemplo

- Alfabeto original: `abcdefghijklmnopqrstuvwxyz`
- Alfabeto cifrado: `JOFPZIDKTMAEGQCSLUVWYXHNBR`

- Texto original: `tricolor paulista`
- Texto cifrado: `WUTFCECU SJYETVWJ`

Criptografia Clássica

- Cifrador de César



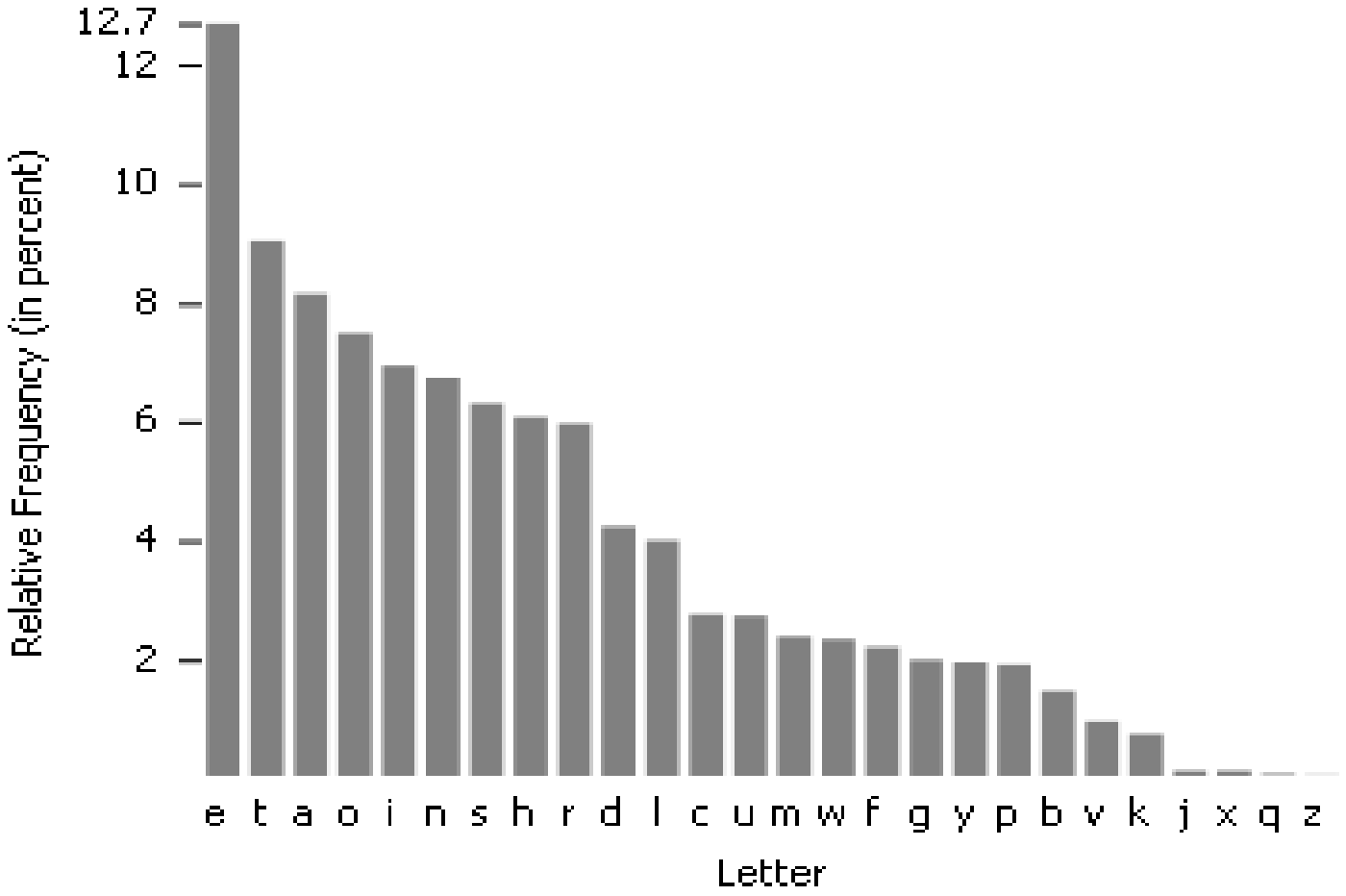
Normal: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cifrado: DEFGHIJKLMNOPQRSTUVWXYZABC

E(x) = (x + 3) mod 26
D(x) = (x – 3) mod 26

Criptografia Clássica - Ataques

- Surgimento da criptoanálise
  - Decifrar a mensagem sem conhecer a chave
- Surgiu para quebrar a cifra de substituição monoalfabética
- Análise de frequência
  - Contar a frequência dos caracteres no texto
  - Digramas
  - Trigramas

Tabela de frequências



Criptografia Clássica

- Cifradores polialfabéticos
  - Mais de um alfabeto cifrado

Exemplo

- Alfabeto original: `abcdefghijklmnopqrstuvwxyz`
- Alfabeto cifrado 1: `JOFPZIDKTMAEGQCSLUVWYXHNBR`
- Alfabeto cifrado 2: `PKBFLRIJEQTMYOAVHDCUXGSNZW`

- Texto original: `hello`
- Texto cifrado: `KLEMC`

Criptografia Clássica

- Vigenère

	a	**b**	**c**	**d**	**...**	**z**
a	A	B	C	D	...	Z
b	B	C	D	E	...	A
c	C	D	E	F	...	B
.	**.**	**.**	**.**	**.**	**...**	**.**
z	Z	A	B	C	...	Y

Exemplo:

- Texto claro: `bazar`
- Chave: `chave`
- Cifrado: `DHZVV`

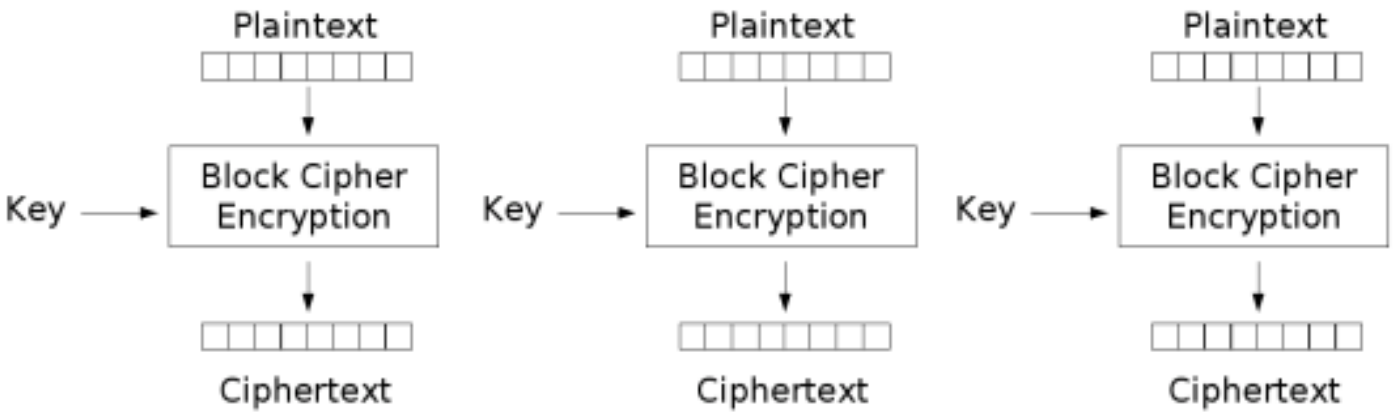
Criptografia Clássica

- Máquina Enigma
  - 1918 – Alemanha
  - 3 rotores
  - Utilizada pelos nazistas durante a II guerra mundial

http://www.youtube.com/watch?v=YhVjgYr26lo

Criptografia Moderna

- **Cifradores de blocos**: divide a mensagem em blocos de tamanho fixo (ex: 128 bits)
  - DES, AES



Electronic Codebook (ECB) mode encryption

Criptografia Moderna

- **Cifradores de fluxo**: cifra cada digito do texto plano por vez
  - RC4

Criptografia Simétrica

Como distribuir as chaves de maneira segura?

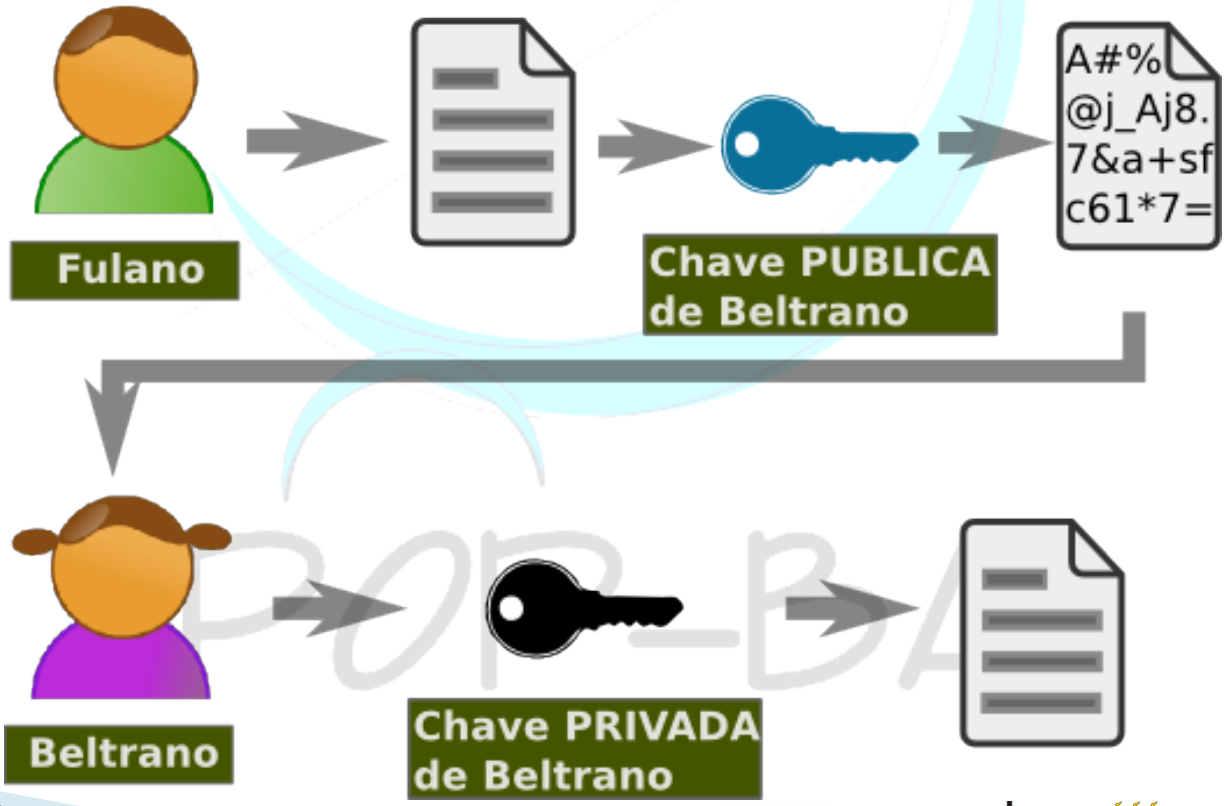
Como verificar se a mensagem não foi modificada?

Como ter certeza que a mensagem foi realmente enviada por quem diz ter enviado?

Criptografia Assimétrica

- Par de chaves
  - ***Pública e Privada***

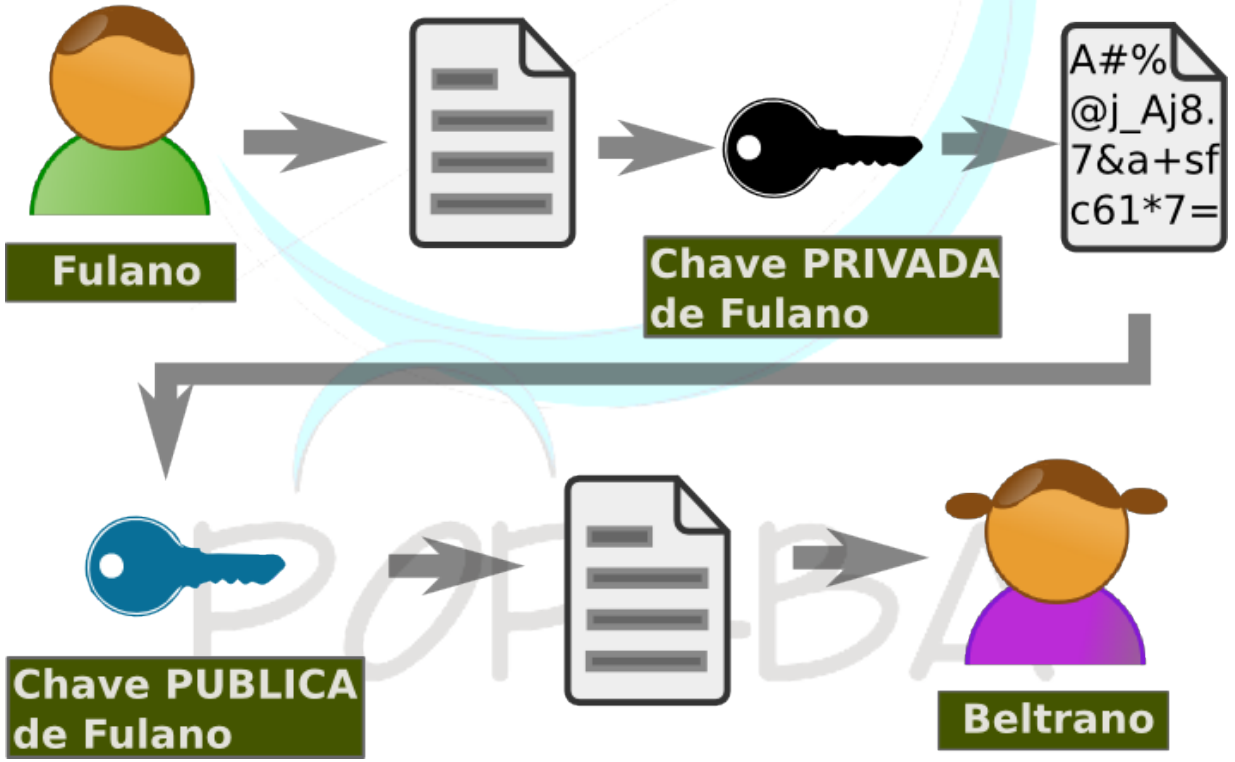
Confidencialidade



Criptografia Assimétrica

- Par de chaves
  - ***Pública e Privada***

Autenticidade



Criptografia Assimétrica

- Diffie Hellman, 1976
- Principais algoritmos:
  - RSA (Rivest, Shamir e Adleman, 1977)
  - DSA (NSA)

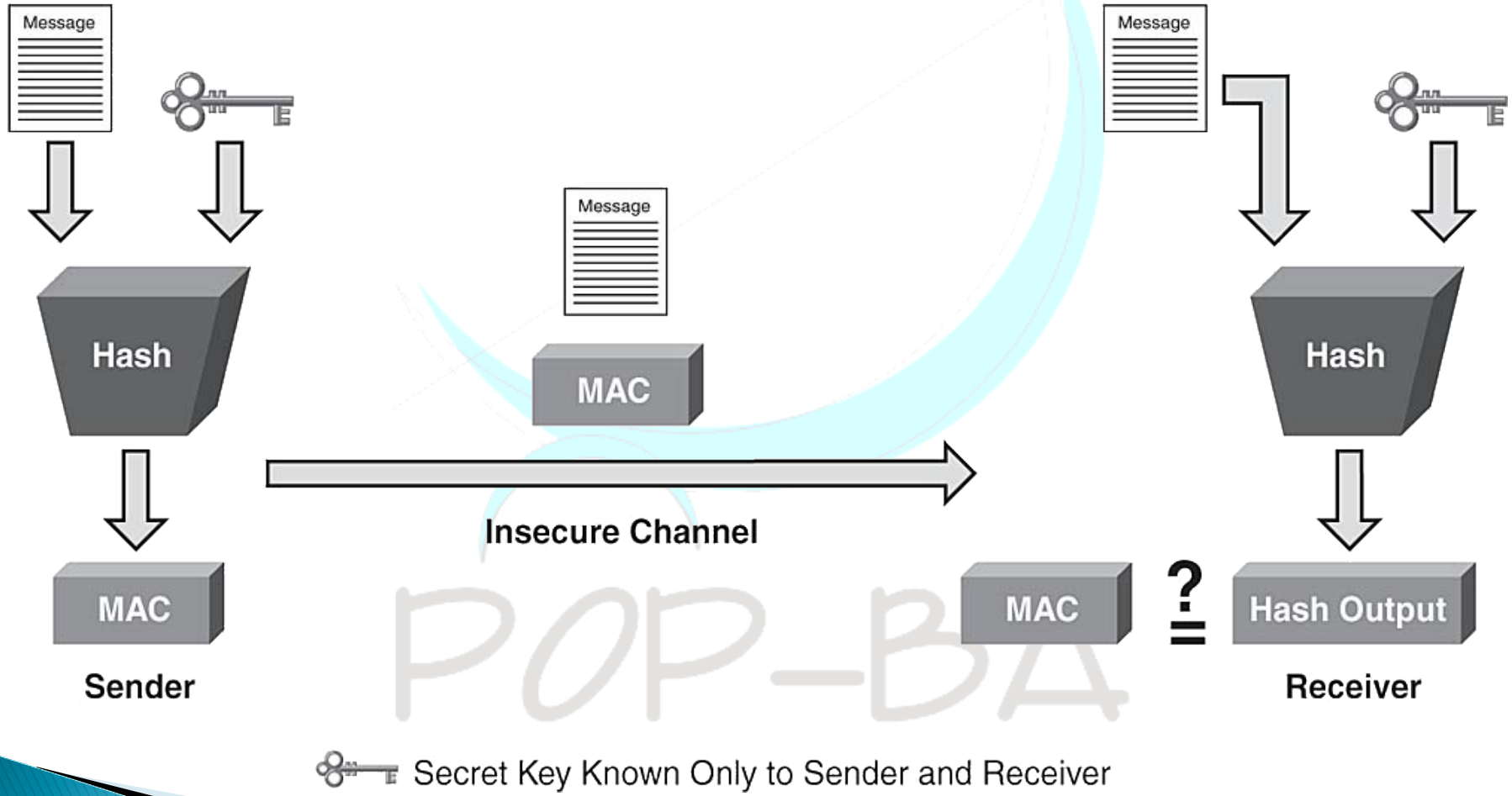
Funções hash

- Procedimento ou função matemática para transformar um conjunto de dados em um outro conjunto de tamanho fixo (resumo criptográfico)
- Propriedades
  - Impossível obter a mensagem original a partir do resumo criptográfico
  - Difícil colisão

Assinatura digital

- *Análogo digital* do conceito de *assinatura de um documento*.
- Permite:
  - Integridade
  - Autenticidade
  - Não repúdio

Assinatura digital



Problemas à vista: colisão de hash

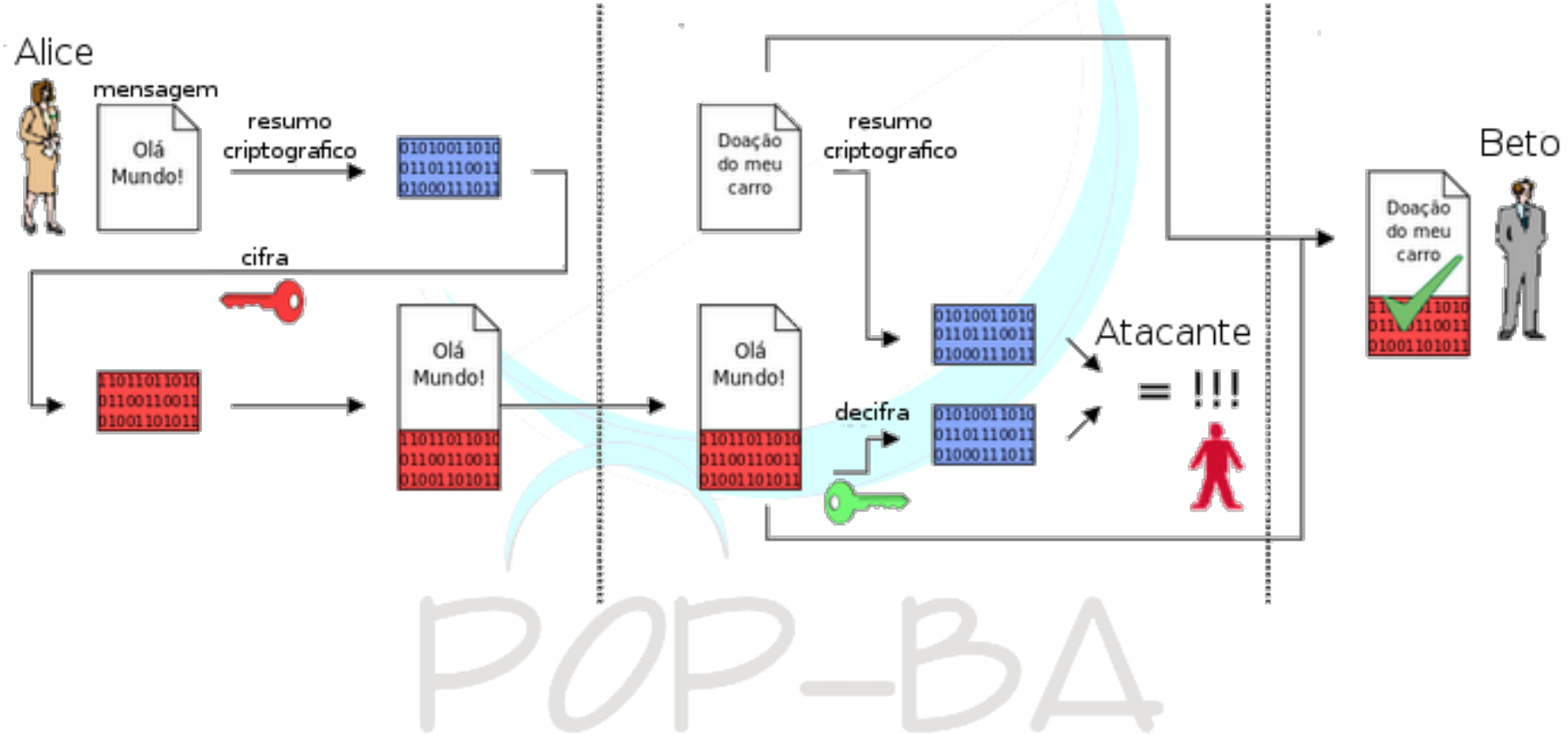
- O hash tem tamanho fixo. Então existe um número **finito** de “hashes”
- Existem **infinitas** mensagens...
- Logo:

Mais de uma mensagem tem o mesmo hash

=

Colisão de hash

Colisão de hash



Colisão de hash

Calma, calma, não criemos pânico...

- *É possível? Sim... mas uma boa função hash tem as seguintes características:*
  - É difícil, tendo *h(m)*, achar *m*
  - É difícil, tendo *m1*, achar *m2* tal que *h(m1)=h(m2)*
- Mais difícil que encontrar uma colisão, é encontrar uma **colisão "útil"**.

Quanto tempo você quer que a assinatura digital continue válida?

Criptografia Assimétrica

~~*Como distribuir as chaves de maneira segura?*~~

~~*Como verificar se a mensagem não foi modificada?*~~

~~*Como ter certeza que a mensagem foi realmente enviada por quem diz ter enviado?*~~

Como vincular uma chave à informação de seu detentor?

Criptografia Assimétrica

Como vincular uma chave à informação de seu detentor?

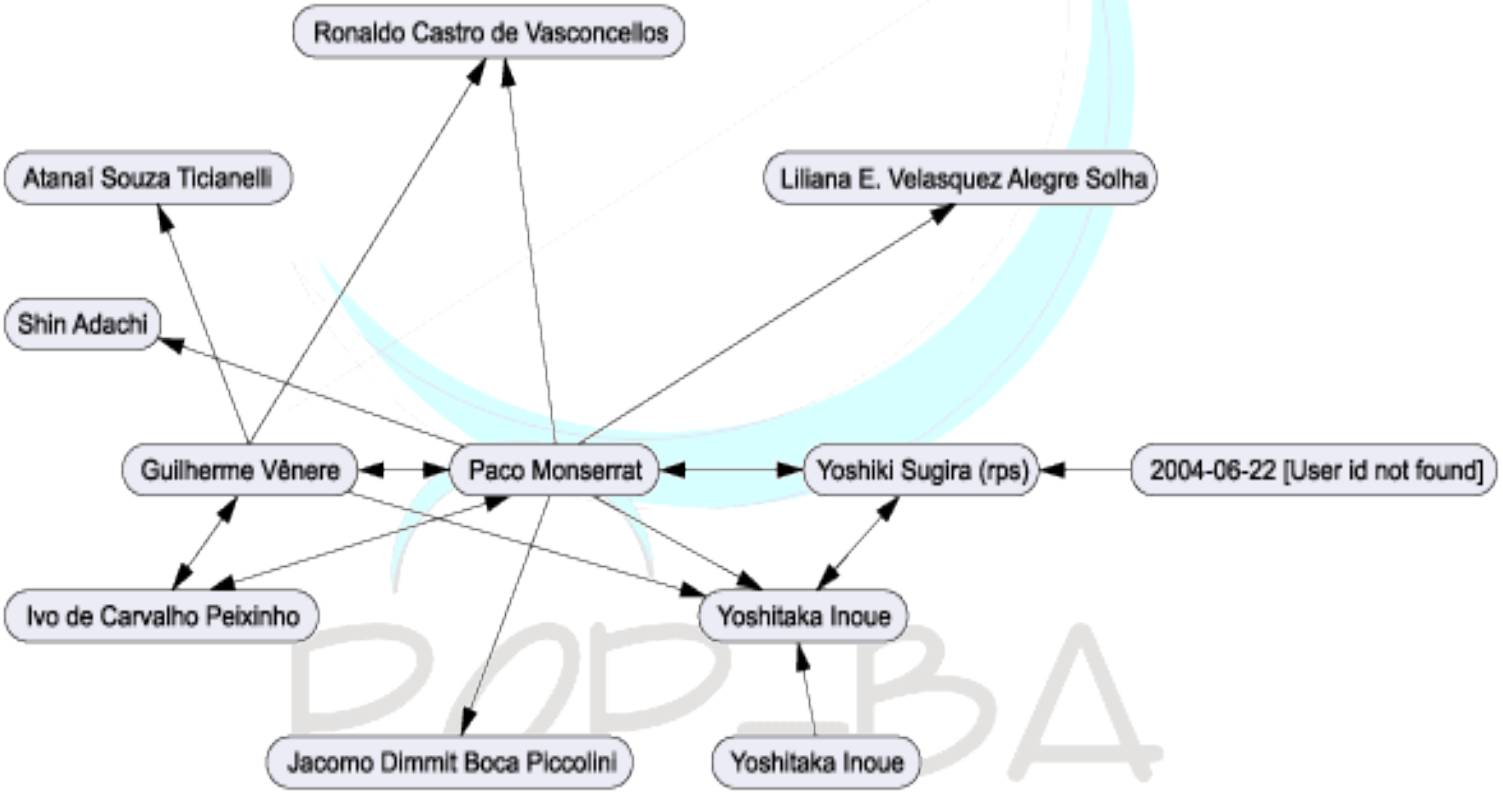
- Alternativas
  - Utilização de uma autoridade certificadora
  - Web-of-trust

Criptografia Assimétrica

- Web-of-trust
  - A confiança vai sendo estabelecida através de uma rede de transitividade
  - Publicação da chave em um servidor
  - Assinatura de pessoas que confiam na chave

Criptografia Assimétrica

- Web-of-trust



Retirado de http://www.rnp.br/cais/keyserver

Criptografia Assimétrica

- Web-of-trust
  - Servidores de chave
    - http://www.rnp.br/keyserver
    - http://pgp.mit.edu
    - ...
  - Festas de assinatura de chave

Certificados Digitais

- Objeto puramente digital
- Contém informações do detentor da chave privada
- Criado por uma entidade confiável
- Possível delimitar as suas possíveis aplicações
- Fácil determinar se foi violado
- Possível verificar seu estado atual

Lista de Certificados Revogados

- Necessidade de tornar um certificado inválido
  - Impossível apagar todas as cópias existentes de um certificado
- Objeto puramente digital
- Motivos para revogação
  - Modificação de um certificado
  - Comprometimento da chave privada
  - Encerramento do uso

Infraestrutura de Chaves Públicas - ICP

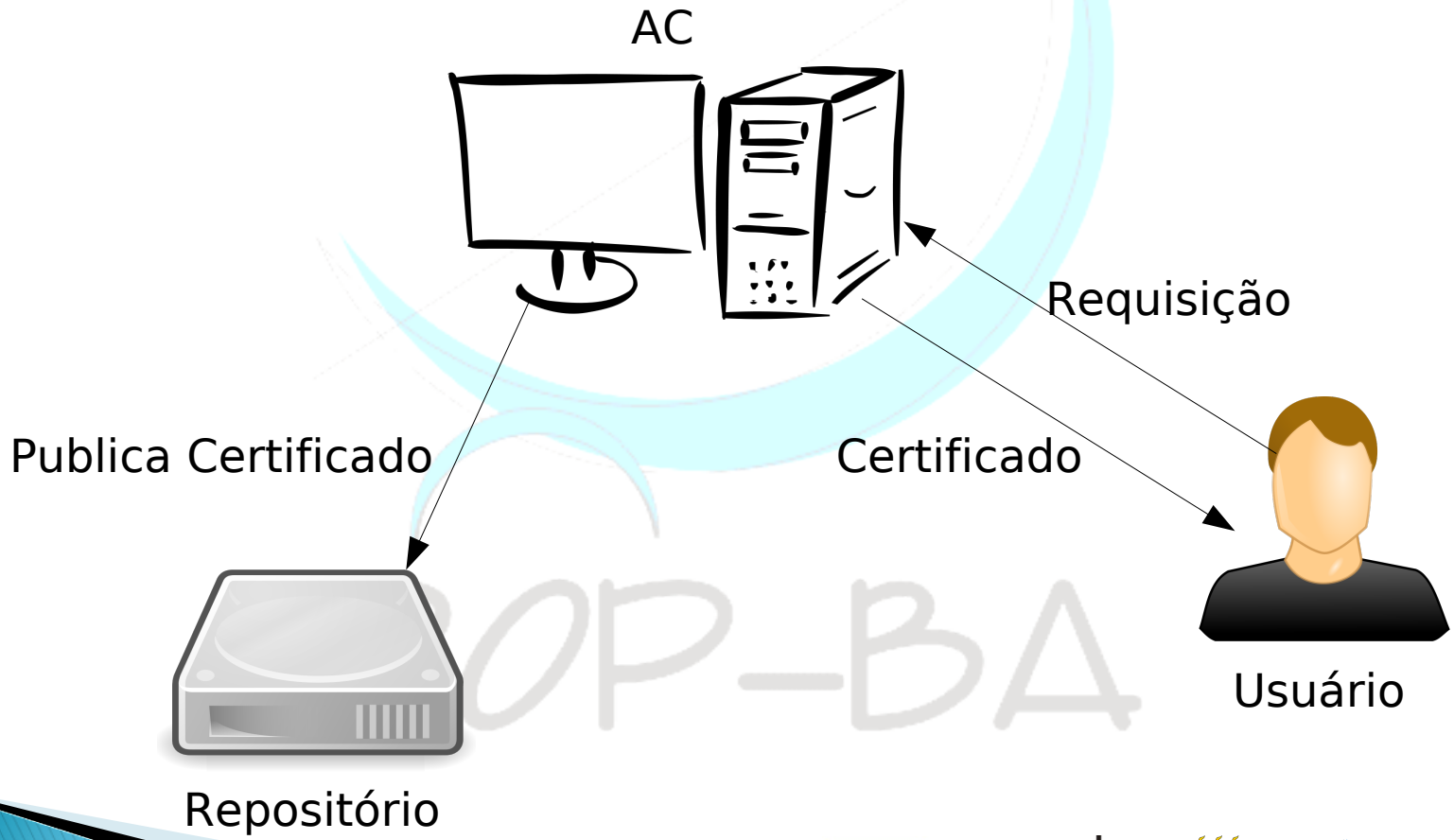
- Objetivo: Facilitar o uso de criptografia de chaves públicas
- Principais componentes
  - Autoridades Certificadoras
  - Autoridades de Registro
  - Repositório

Autoridades Certificadoras

- Responsáveis por:
  - Emissão de certificados digitais
  - Emissão de listas de certificados revogados
  - Gerenciamento das informações dos certificados
  - Verificação dos dados das requisições
  - Delegar Tarefas

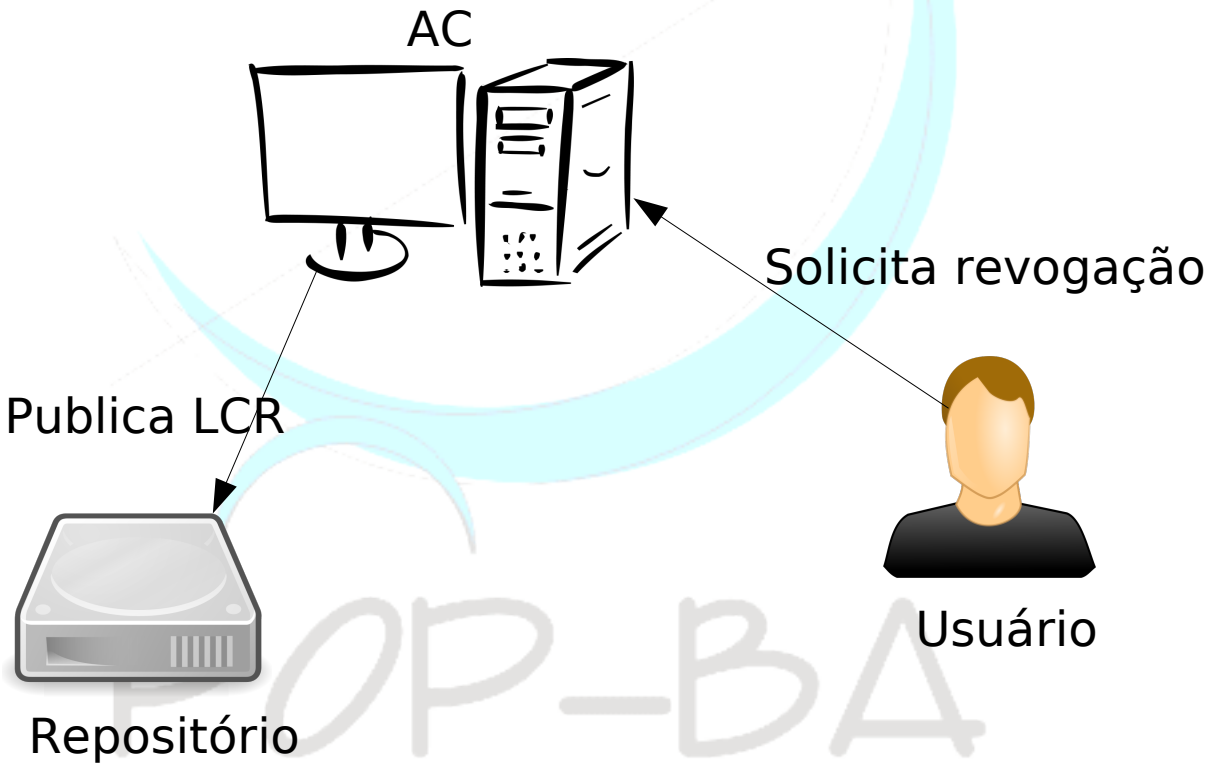
Autoridades Certificadoras

Emissão de certificados



Autoridades Certificadoras

Emissão da lista de certificados revogados



Certificados Digitais

- Por que confiar?
  - Certificado contém informações do detentor da chave privada
  - Emitido por uma entidade confiável
  - Dados são verificados
  - ICPs são auditadas

ICP-Brasil

Conjunto de entidades, padrões técnicos e regulamentados, elaborados para suportar um sistema criptográfico com base em certificados digitais

- MP 2.200-2, de 2001-08-24
- Exemplos de ACs credenciadas
  - Caixa Econômica Federal
  - CertiSign
  - Serasa
  - Serpro
  - Receita Federal

ICP-Brasil

- Exemplos de uso:
  - Sistema de Pagamento Brasileiro (SPB)
  - Autenticação
  - Tramitação e assinatura eletrônica de documentos oficiais
  - Assinatura de Contratos
  - Assinatura de documentos
  - Internet banking
  - Automação de processos no Poder Jurídico
  - Declaração de Imposto de Renda

ICPEDU

- Proposta
  - Implantação de uma ICP para emissão de certificados aplicados em autenticação, assinatura digital e sigilo, dentro do ambiente das IFES e UPs
  - Pode emitir certificados digitais gratuitamente
  - Facilita e confere segurança a atividades internas
  - Sistema hierárquico de confiança
  - Utilizada para transações em aplicações acadêmicas e de pesquisa
  - Não possui validade legal

Objetivos da ICPEDU

Esforço da Rede Nacional de Ensino e Pesquisa (RNP) para viabilizar a implementação de uma Infraestrutura de chaves públicas acadêmica.

- Objetivos
  - Uso acadêmico
  - Autenticação
  - Desenvolver cultura em certificação digital
  - Treinamento
  - Pesquisa
  - Aplicações

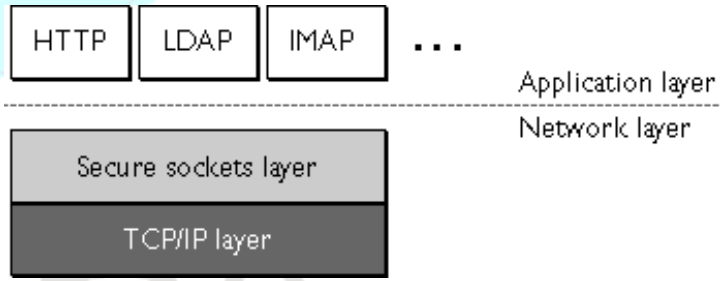
Aplicações práticas

Secure Socket Layer

- Histórico
  - Criado em 1995 pela Netscape
  - Versão atualizada SSLv3
  - Versão padronizada pelo IETF: TLS (RFC5246 – v1.2)
- Motivação
  - Atender demandas por conexão mais seguras na Internet;
- Objetivo
  - Prover serviços de autenticação do servidor, comunicação secreta e integridade dos dados;
  - Tornou-se um padrão é utilizado até hoje para prover conexões seguras;

Secure Socket Layer

- O protocolo SSL executa sobre os protocolos TCP/IP e abaixo de procolos de alto nível (HTTP, IMAP, LDAP).
- Provê os seguintes serviços para comunicações na Internet:
  - Autenticação do servidor
  - Autenticação do cliente
  - Conexão encriptada



Secure Socket Layer

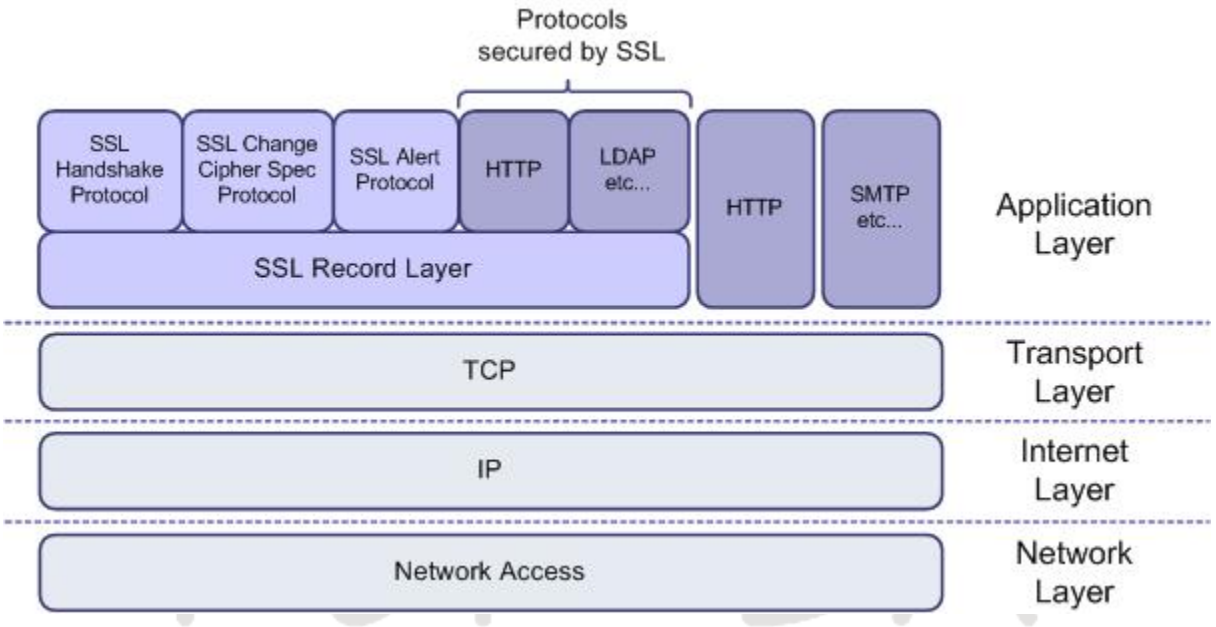
- Criptografia SSL: segurança *versus* desempenho
  - Definição da chave secreta: Cript. Assimétrica
  - Criptografia dos dados: Cript. Simétrica

Secure Socket Layer

- SSL: Record Protocol + Handshake Protocol + Alerts Protocol + Change CipherSpec Protocol
  - ***Record Protocol***: define o formato usado na transmissão dos dados
  - ***Handshake Protocol***: definição dos parâmetros necessário ao estabelecimento da conexão SSL
  - ***Alerts Protocol***: define as mensagens de erro (*fatal* e *warning*)
  - ***Change CipherSpec Protocol***: Sinaliza o fim do handshake e inicia a comunicação criptogafada

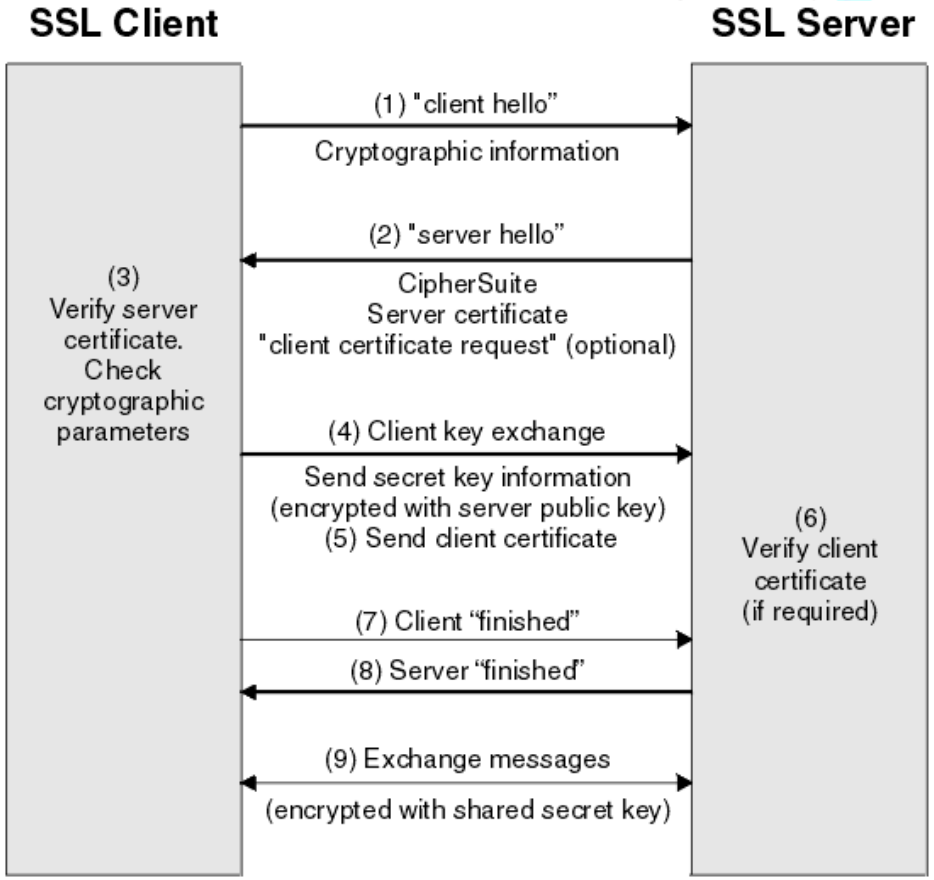
Secure Socket Layer

- SSL: Record Protocol + Handshake Protocol + Alerts Protocol + Change CipherSpec Protocol



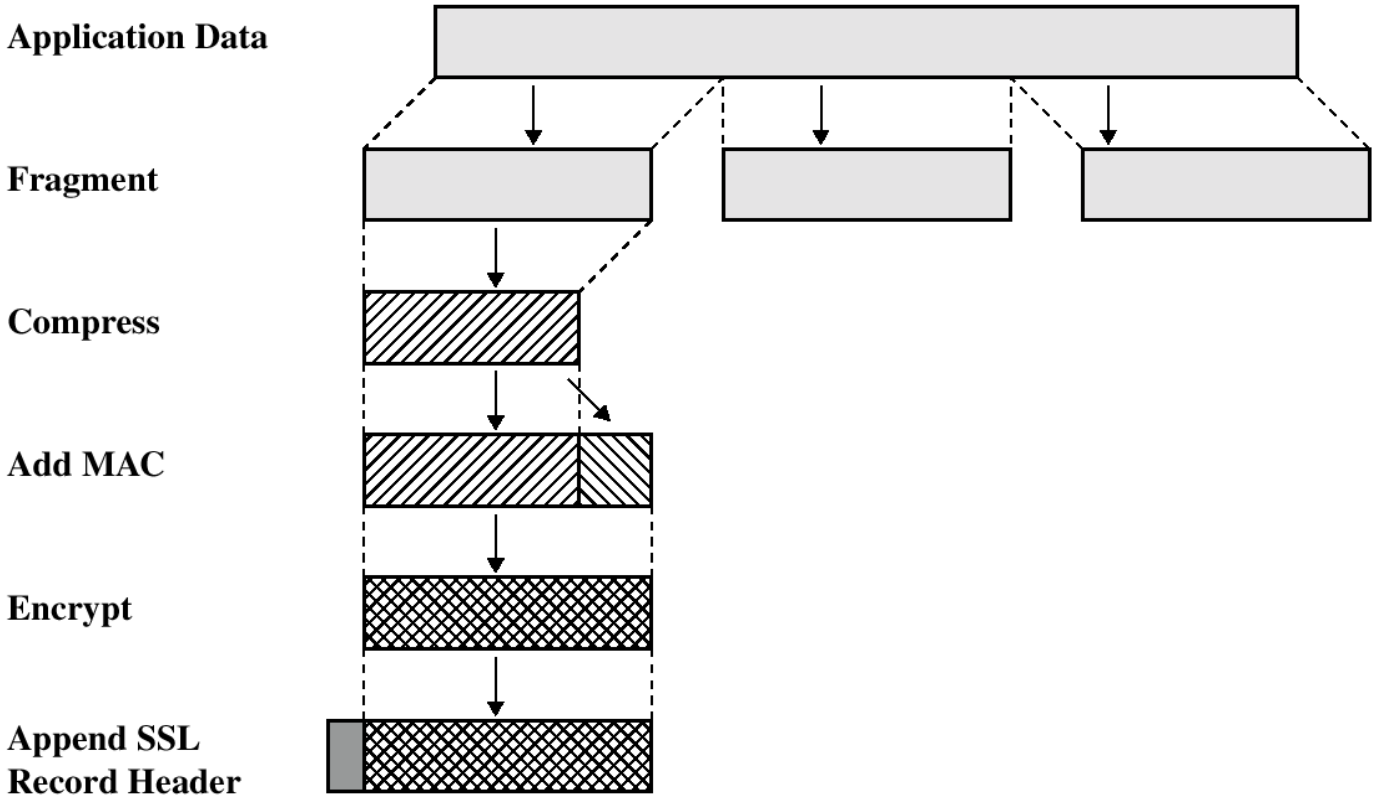
Secure Socket Layer

- SSL Handshake Protocol



Secure Socket Layer

- SSL Record Protocol



Secure Socket Layer

- Aplicações
  - Qualquer comunicação de aplicação baseada em TCP (LDAP, IMAP, POP, etc.)
  - Uso mais comum: HTTP + SSL == HTTPS
    - HTTPS (Secure HTTP) – porta 443 invés da porta 80

Secure Socket Layer

- SSL no Apache
  - Habilitar o ***mod_ssl***
  - Obter/criar o certificado
  - Configurar um *VirtualHost* com SSL habilitado
  - (opcional) Verificar a confiabilidade da CA nos clientes

Secure Socket Layer

- ***Prática***: Configurar SSL no apache (ver roteiro de prática – prática 01)

Outras aplicações

- VPN – Virtual Private Network
- DNSSEC – Extensão de Segurança do DNS
- Assinatura/Criptografia de e-mails
- Autenticação
- Assinatura de documentos

Dúvidas?