Criptografia – fundamentos e prática

Italo Valcy <italo@pop-ba.rnp.br>
CERT.Bahia / UFBA

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/

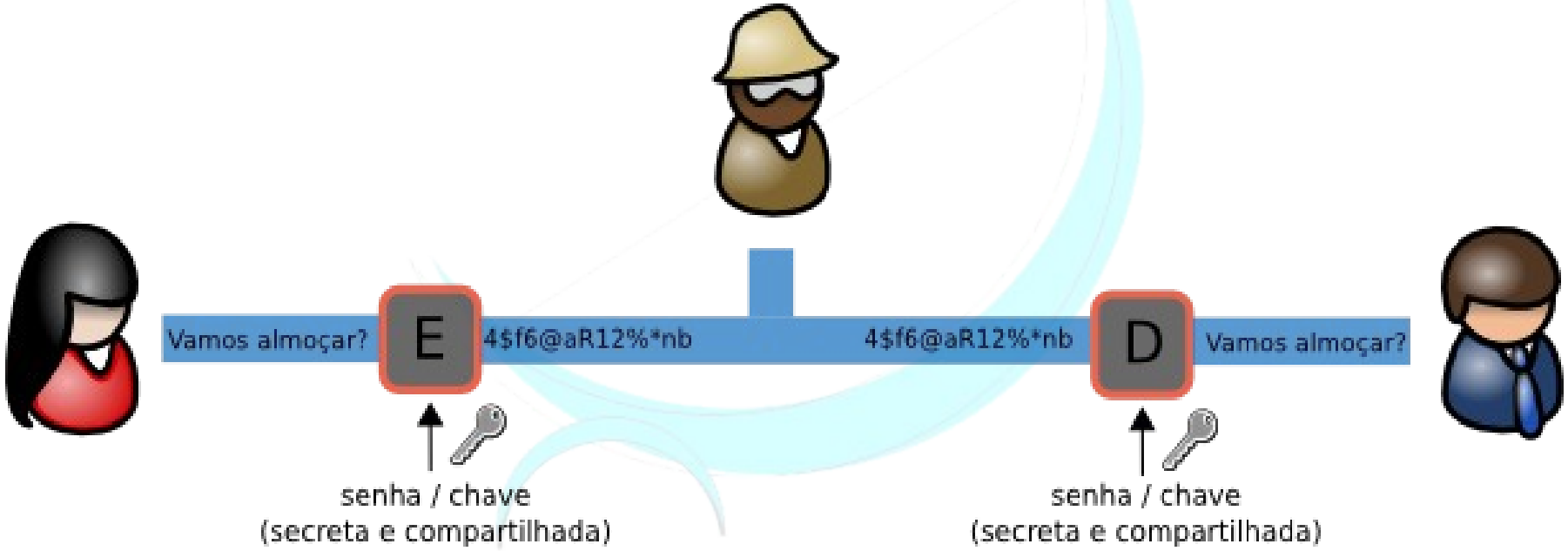
Introdução

- 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

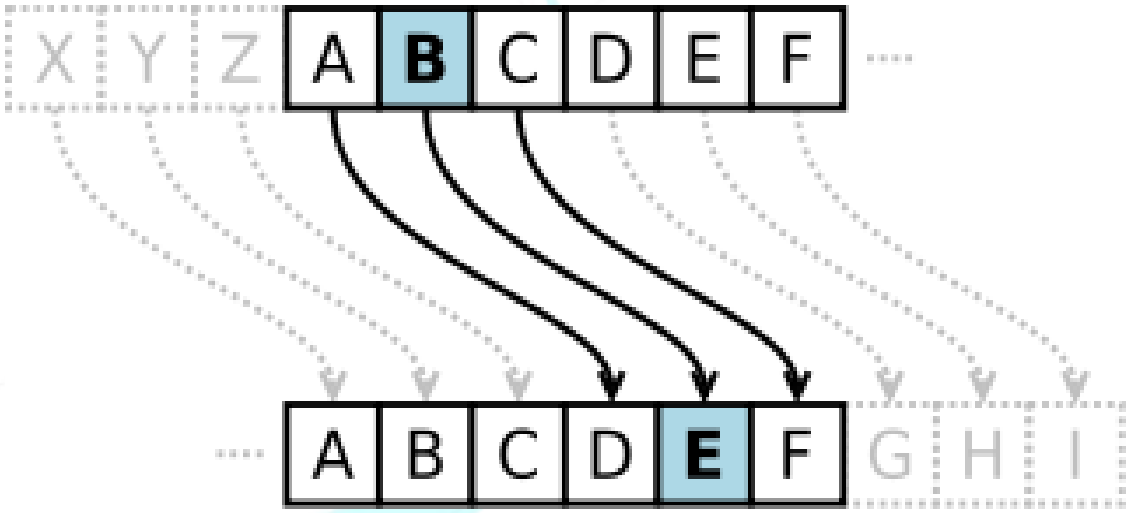
Exemplo

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

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

Criptografia Clássica

- Cifrador de César



Normal: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cifrado: DEFGHIJKLMNOPQRSTUVWXYZABC

Criptografia Moderna

- **Cifradores de blocos**: divide a mensagem em blocos de tamanho fixo (ex: 256 bits)
  - DES, AES, 3DES
- **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?

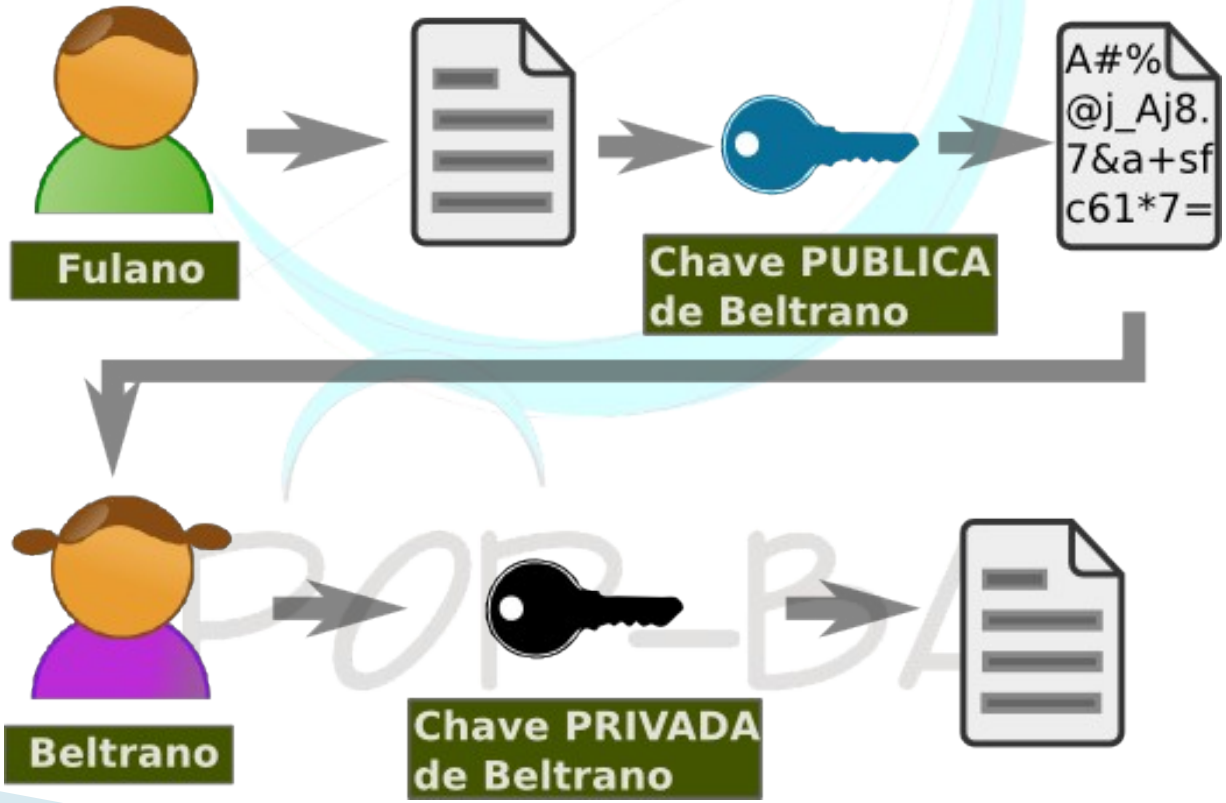
Criptografia Assimétrica

- Baseado no par de chaves: pública e privada
  - Chaves públicas são divulgadas abertamente
  - Chaves privadas devem ser mantidas em segredo
- Uma função matemática relaciona as duas
  - Não é possível obter a chave privada a partir da pública!
- Provê:
  - Confidencialidade das mensagens
  - Autenticação do remetente
  - Verificação de integridade
  - Não repudio

Criptografia Assimétrica

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

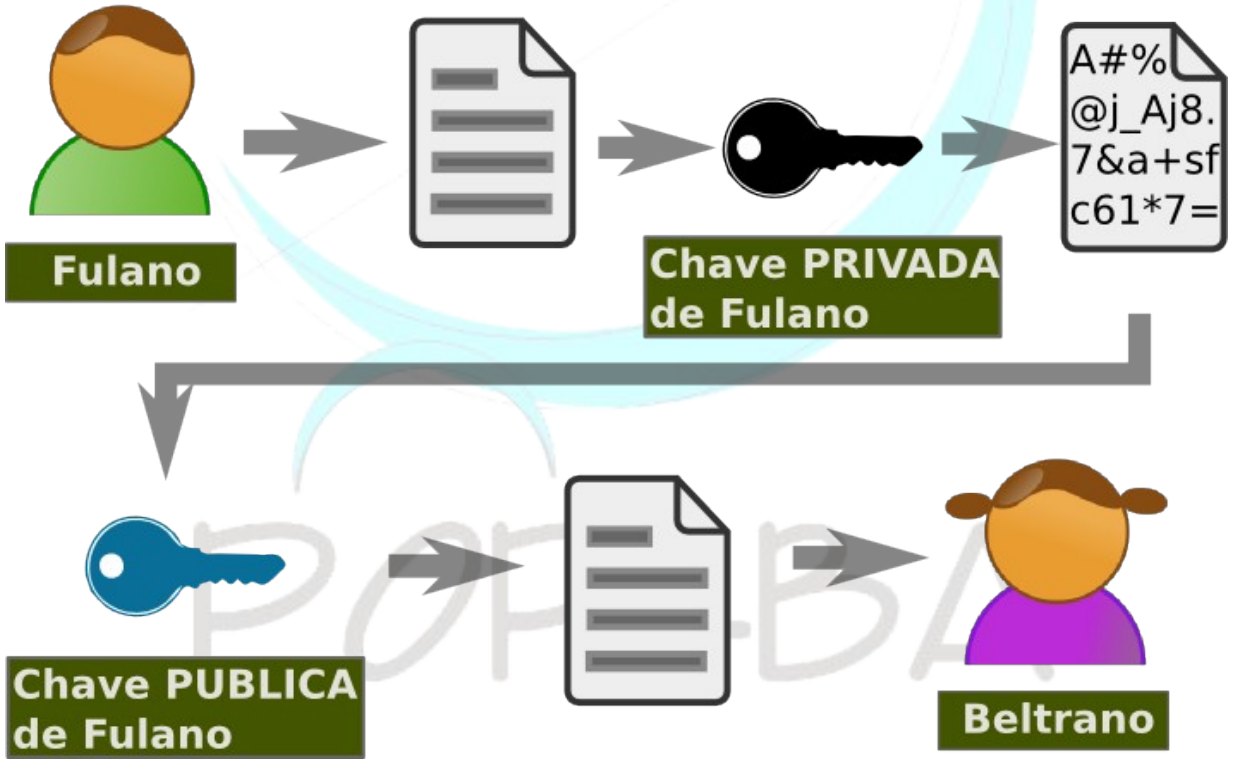
Confidencialidade



Criptografia Assimétrica

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

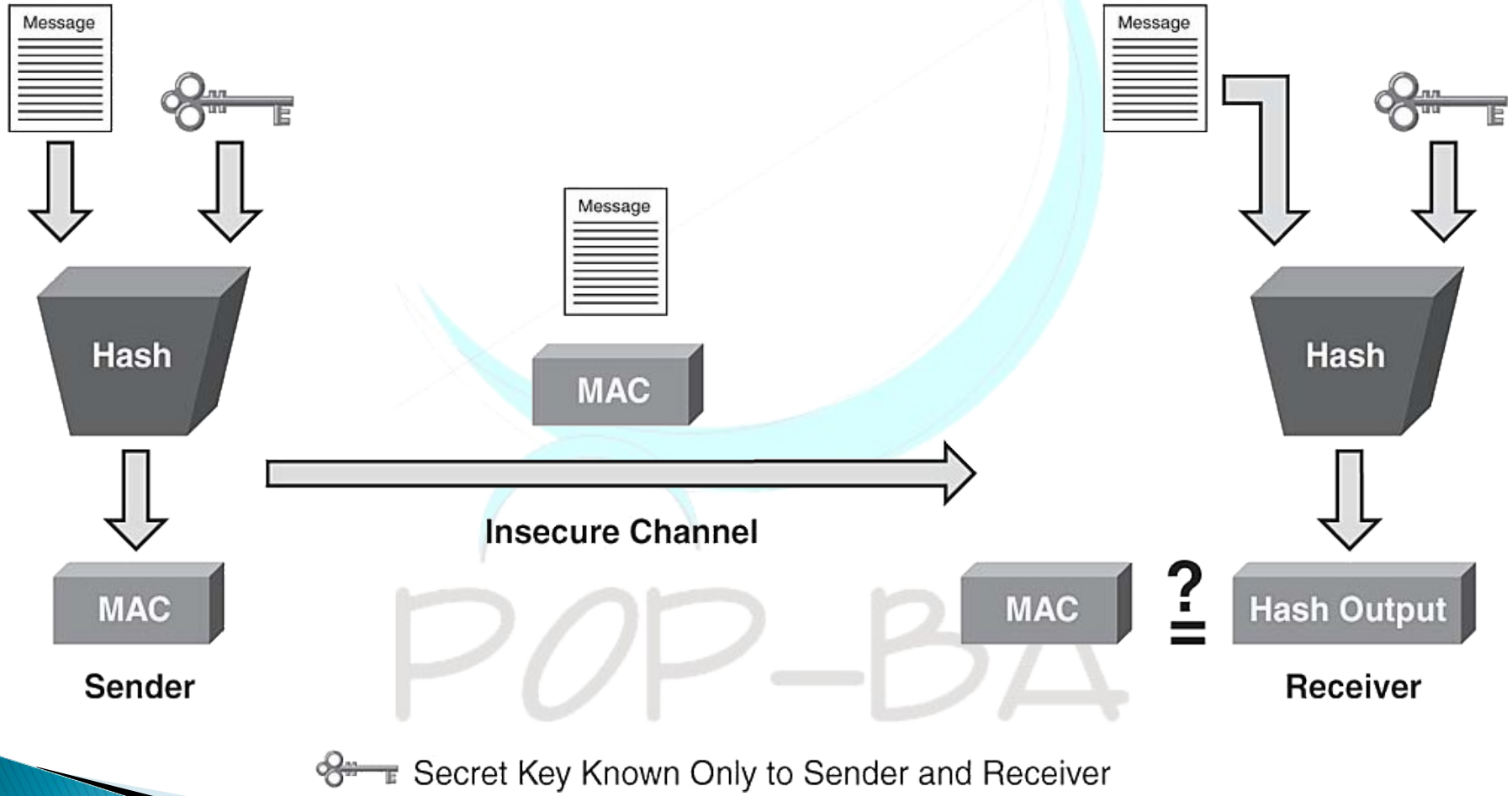
Autenticidade



Assinatura digital

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

Assinatura digital



PGP (Pretty Good Privacy)

- Software que implementa criptografia assimétrica (um dos primeiros), escrito por Phil Zimmermann
- Originalmente era freeware, mas agora é proprietário da Symantec
  - http://www.symantec.com/encryption
- Deu origem ao padrão OpenPGP (RFC 4880)
  - http://www.openpgp.org/

GPG – GnuPG

- Implementação livre do OpenPGP, distribuído sobre GPL
  - GNU Privacy Guard
- É base para diversas outras ferramentas de criptografia assimétrica
- Por ser amplamente usado, confunde-se com o conceito (não adequado):
  - Chaves GPG
  - Assinatura GPG
  - ...

Ferramentas GPG

- Linux:
  - GPG – Command Line (backend para demais)
  - Frontends: Seahorse, Kgpg, etc
  - Enigmail
- MAC OSX:
  - GPG Suite (GPG Keychain, GPG Services)
- Windows:
  - GPG 4 Win
  - Enigmail (Mozilla)

Passos para utilização

- Criação de chave pública/privada
- Envio/disponibilização da sua chave pública
- Importação da chave de outros usuários
  - Configuração de servidor de chaves (?)
- Assinatura de chaves
- Obter lista de chaves revogadas
- Criptografar arquivos, pastas, e-mails
- Eventualmente... gerar chave de revogação

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?

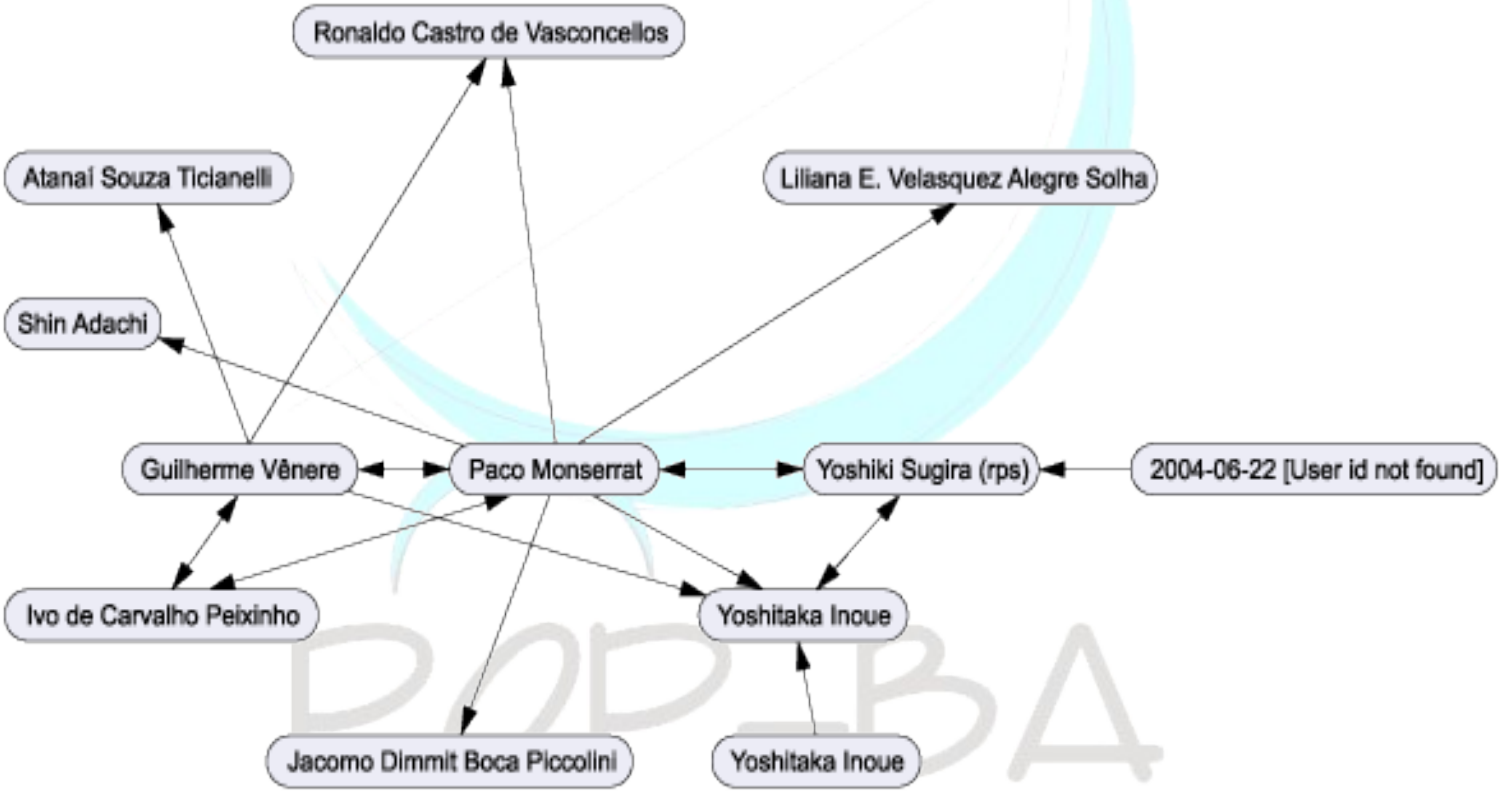
- Alternativas
  - Web-of-trust
  - Autoridades certificadoras

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

Infraestrutura de Chaves Públicas - ICP

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

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

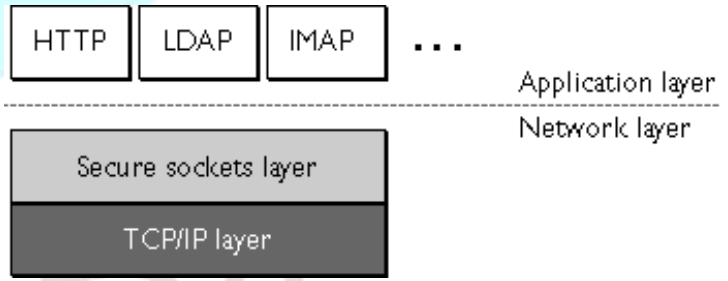
Aplicações práticas

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



Outras aplicações

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

Comunicação Off-the-Record (OTR)

Qual o problema com PGP?

- O que acontece quando a chave privada é perdida/roubada?
  - Computador comprometido
  - Computador roubado

- Todo o material criptografado pode ser lido!
  - Decifrar mensagens do passado
  - Conhecer seu conteúdo
  - Conhecer sua origem (com prova matemática)

Isso é realmente seguro?

Qual o problema com PGP?

- O software criou bastante vestígio...
  - Chaves que decifram dados enviados pela internet a qualquer tempo
  - Assinaturas com não repúdio
- No fundo, “Alice depende das ações de Bob”
- Na vida real:
  - É ilegal gravar conversas sem notificação
  - Ilegal grampear linhas telefones em autorização judicial
- E na internet?

Como usar OTR

- OTR baseai-se em:
  - Perfect Forward Secrecy
  - Repudable Authentication

Perfect Forward Secrecy

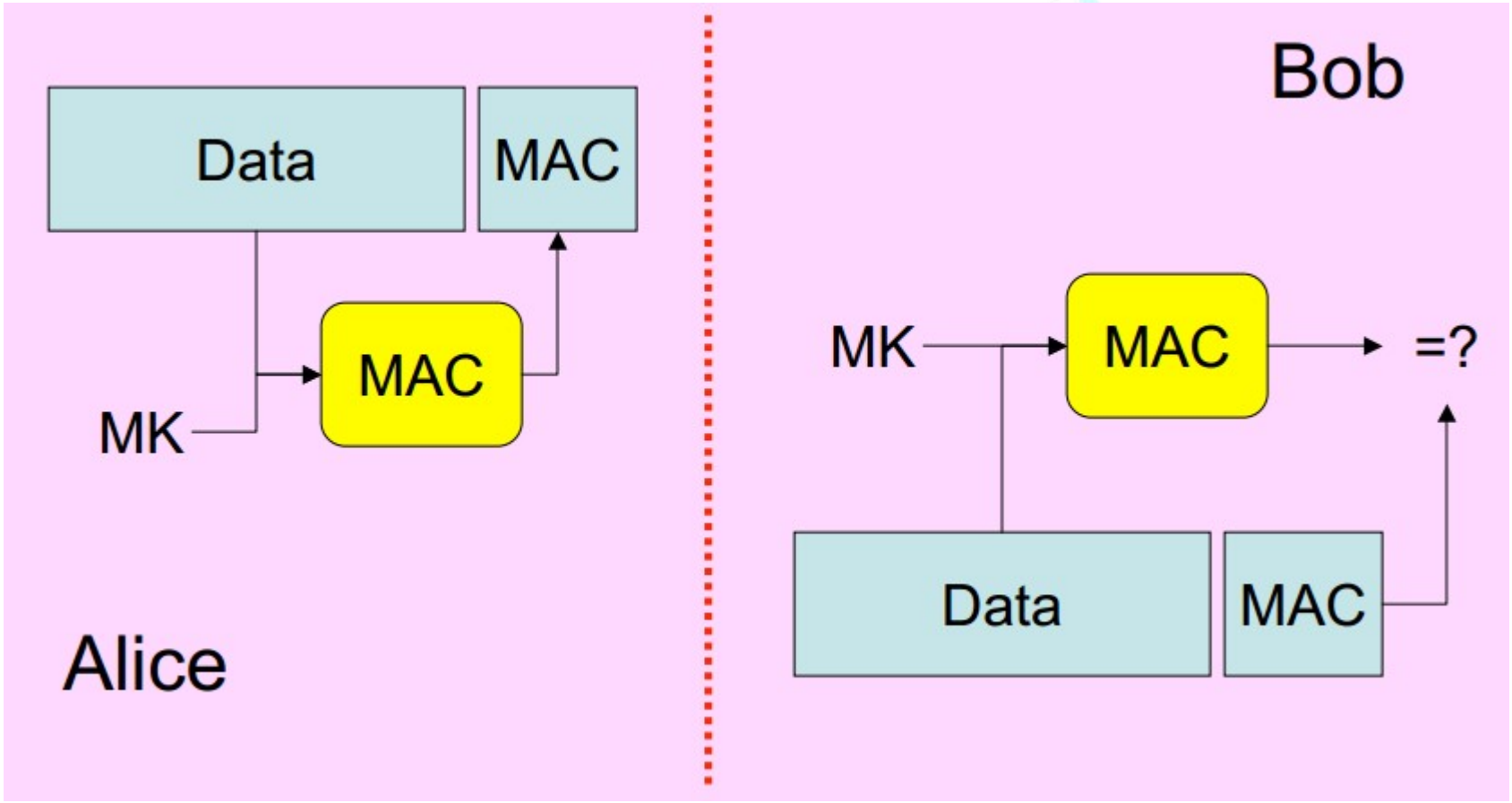
- Premissa: Vazamento de chaves futuras não devem comprometer dados anteriores

- Faz uso de chaves criptográficas de **curta validade**
- Descarta as chaves após seu uso
  - Remove da memória
- Utiliza chaves de **longa validade** apenas para **distribuição** das chaves de curta validade

Autenticação Repudiável

- Não repudio é importante para contratos, mas é **desnecessário para conversas**
- Ainda assim, autenticação é importante
  - Previne ataques de personificação
- Usar MACs (Message Authentication Codes)

OTR funcionamento



OTR - Ferramentas

- Ferramentas de IM (Pidgin, Adium) IRC (BitlBee)
  - Qualquer provedor XMPP
  - Facebook, Gtalk, etc
  - Requer que ambas as partes ativem
  - Não suportado por clientes IM web
- Apache2 + OpenSSL + PFS
  - Basta selecionar a suite de cifragem correta

Conclusões

- Criptografia é importante para melhorar a segurança de sistemas de informação e comunicação
- Existem diversas aplicações que fazem uso de criptografia
  - SSL, VPN, DNSSEC, OTR, E-mail seguro, hash de senha, etc
- A criptografia também tem falhas
  - Colisão de hash, falhas em implementações específicas
- Cuidado com “criptografia caseira”
- Use criptografia sempre que possível!

Dúvidas?