Entendendo a criptografia e como ela pode ser usada na prática

Italo Valcy <italovalcy@ufba.br>
Universidade Federal da Bahia
CERT.Bahia – PoP-BA/RNP

STI Superintendência de Tecnologia da Informação | UFBA

POP-BA

Conceitos iniciais

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

Conceitos iniciais

- 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

Papel da criptografia na segurança da informação

Confidencialidade
(Privacidade)

Integridade

Irretratabilidade
(não repúdio)

Autenticidade

Papel da criptografia na segurança da informação

- Criptografia **não é a única forma de assegurar** todos os princípios da segurança da informação
- Criptografia **não resolve todos os problemas** de segurança da informação
- Criptografia **não é a prova de falhas**, sobretudo se implementada incorretamente
  - Criptografia caseira

Criptografia clássica

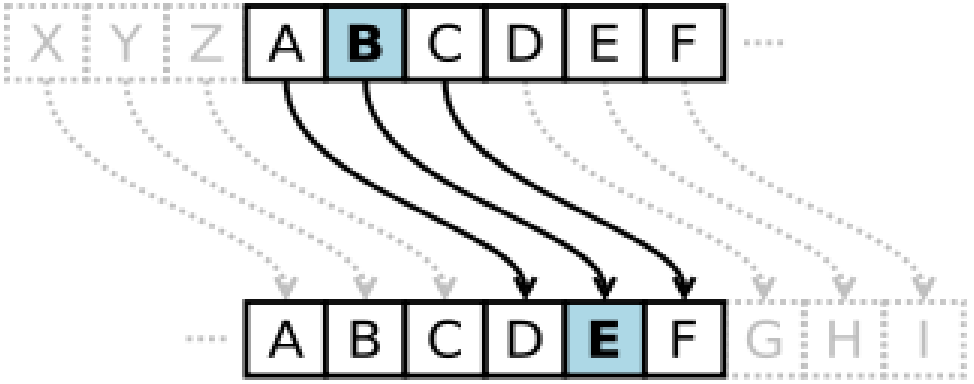
- Cifradores monolíticos
  - Rearranjo do alfabeto original

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

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

Criptografia clássica

- Cifrador de César



- Normal: ABCDEFGHIJKLMNOPQRSTUVWXYZ
- Cifrado: DEFGHIJKLMNOPQRSTUVWXYZABC

$E(x) = (x + 3) \bmod 26$

$D(x) = (x – 3) \bmod 26$

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`

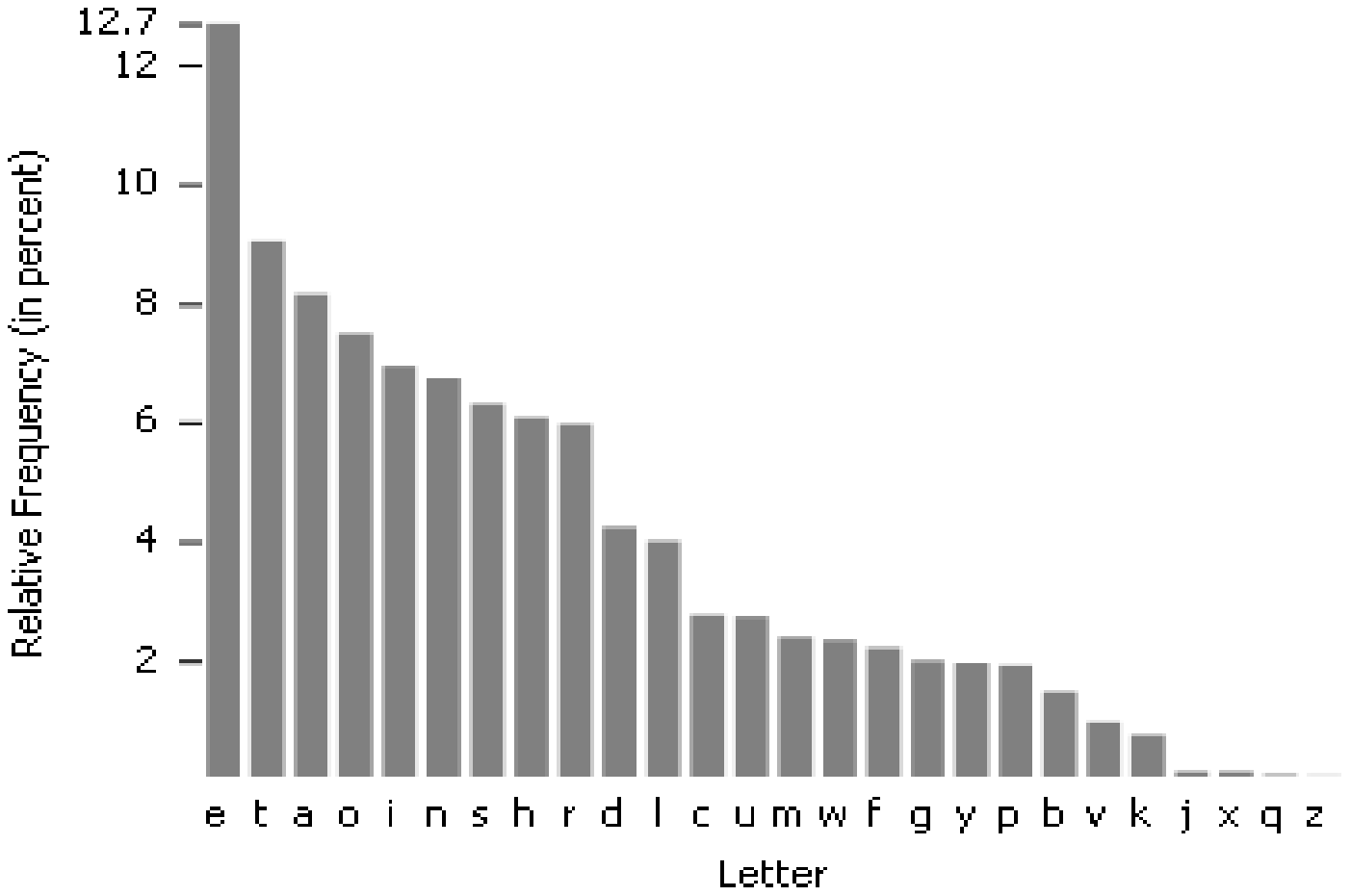
Criptografia clássica

- 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

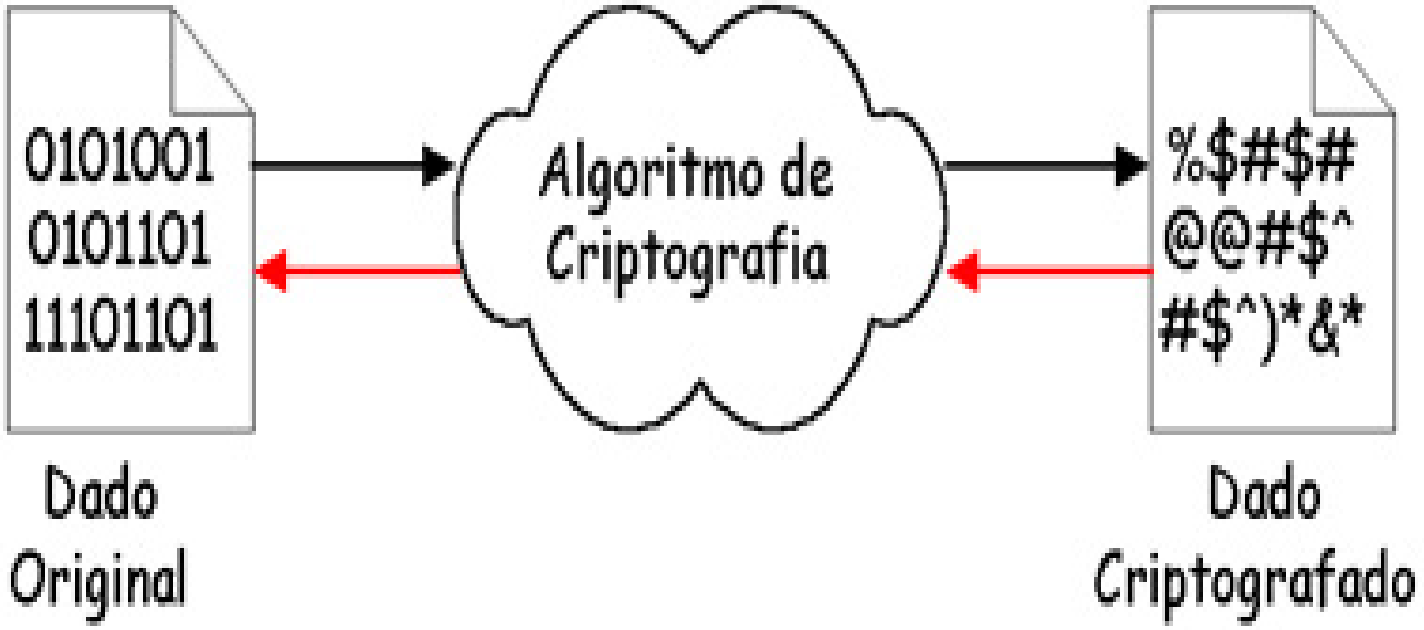
Exemplo:
- Texto claro: `bazar`
- Chave: `chave`
- Cifrado: `DHZVV`

Criptoanálise – Tabela de Frequências



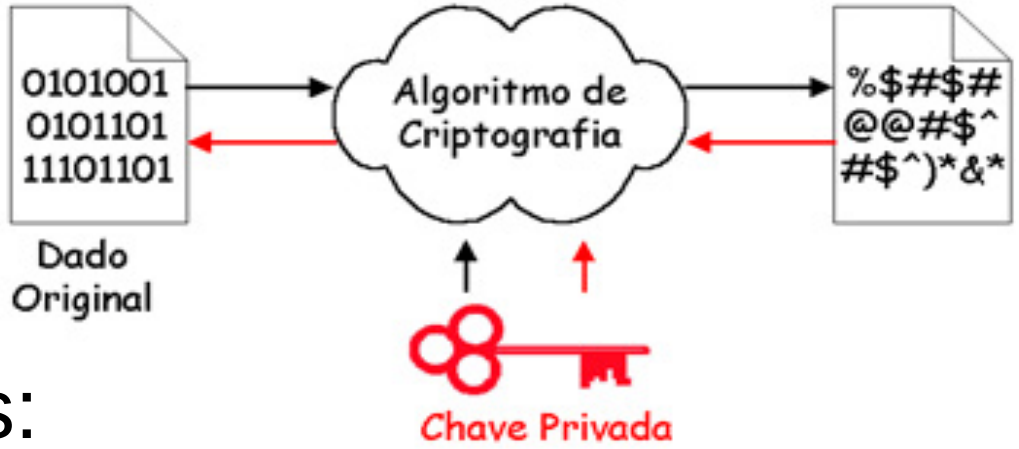
Procedimentos criptográficos

- Os procedimentos de cifrar (E) e decifrar (D) são obtidos através de um **algoritmo (público)** e uma **chave secreta**.



Criptografia simétrica

- Utiliza uma **chave compartilhada** entre o emissor e receptor para cifrar e decifrar a mensagem



- Algoritmos conhecidos:
  - DES / 3DES
  - AES (192, 256 ou 512 bits)
  - Blowfish/Twofish (448 bits)

Criptografia simétrica

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

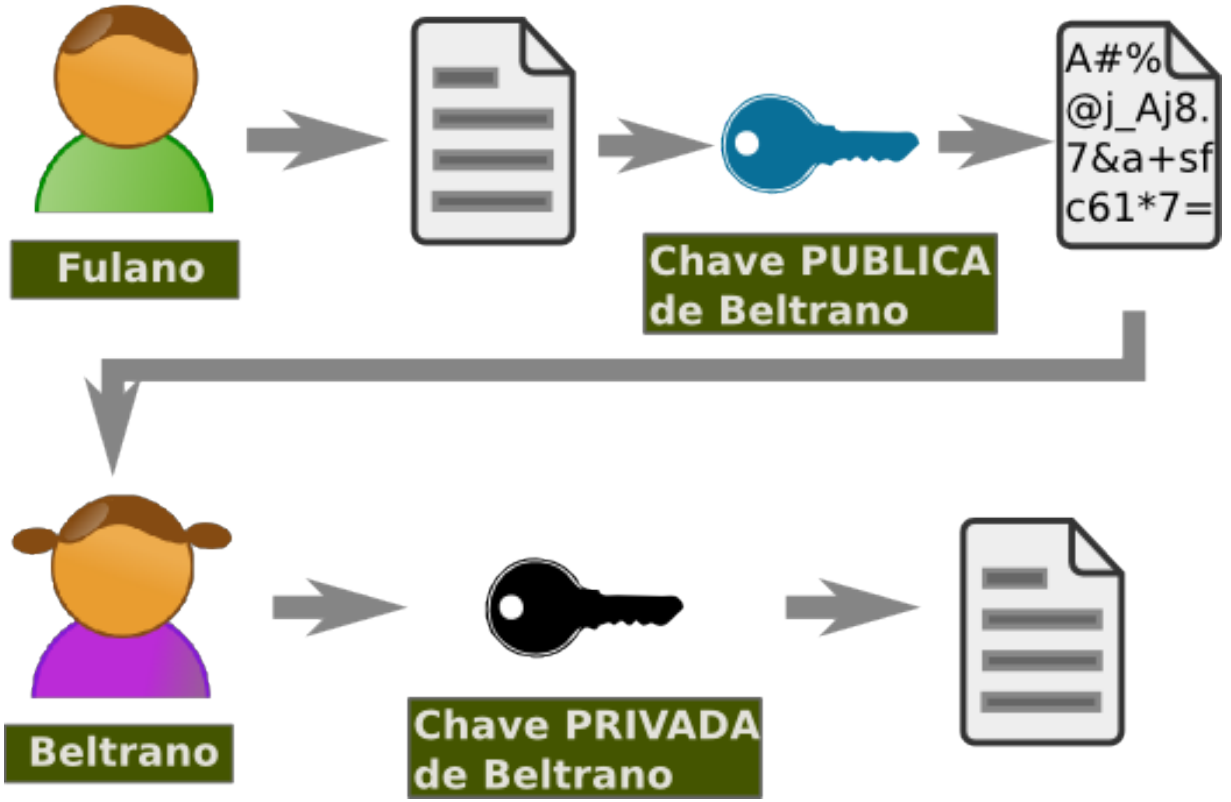
*Como verificar se a mensagem não foi **modificada?***

*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

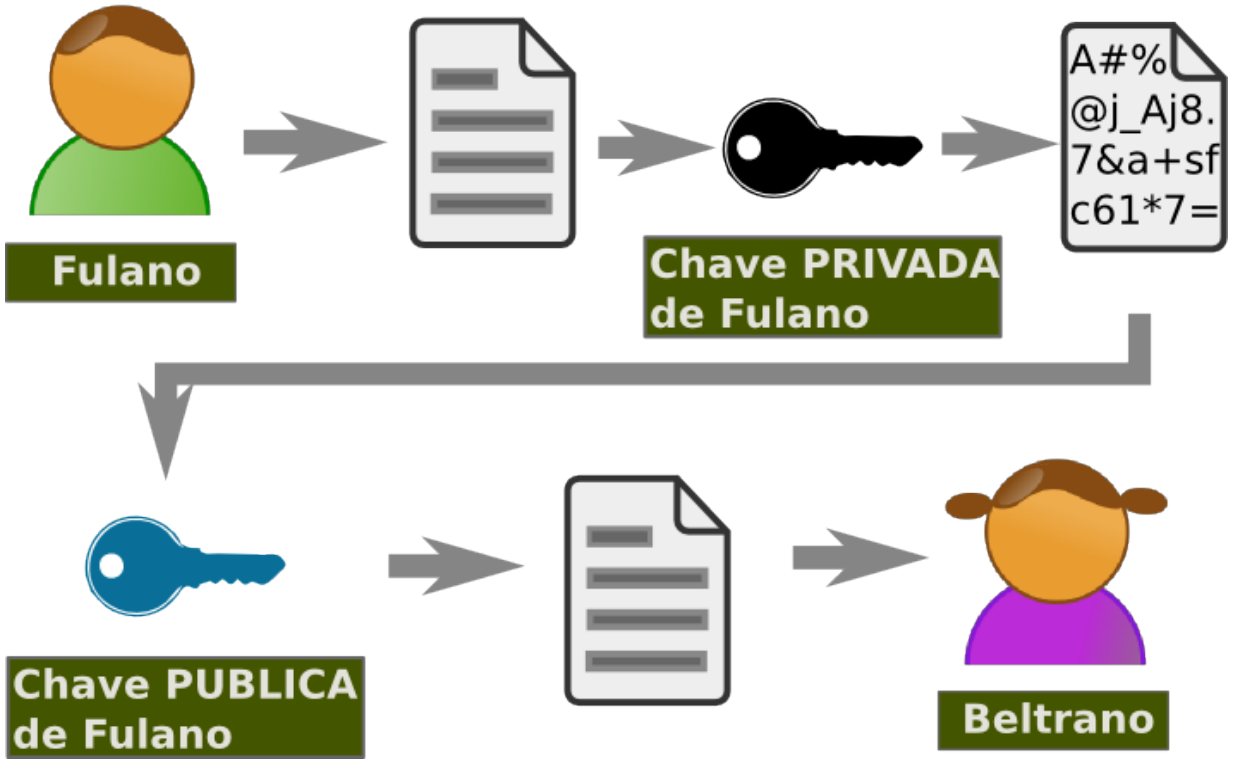
Confidencialidade



Criptografia assimétrica

- Baseado no par de chaves: pública e privada
  - **Chaves públicas** são divulgadas abertamente
  - **Chaves privadas** devem ser mantidas em segredo

Autenticidade

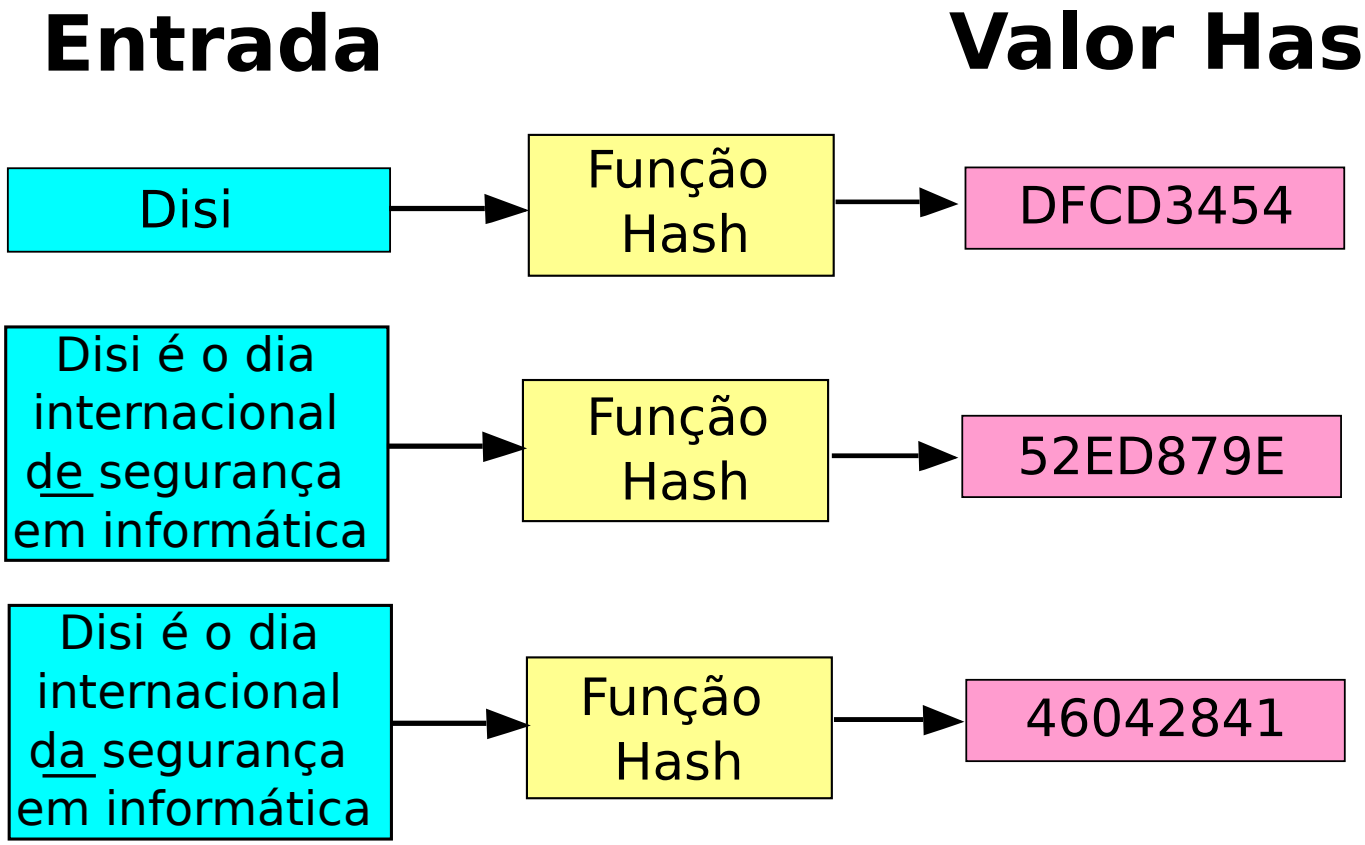


Criptografia assimétrica

- Principais algoritmos
  - RSA (Rivest, Shamir e Adleman, 1977)
  - Diffie-Hellman
  - DSA de curvas elípticas
  - El Gamal

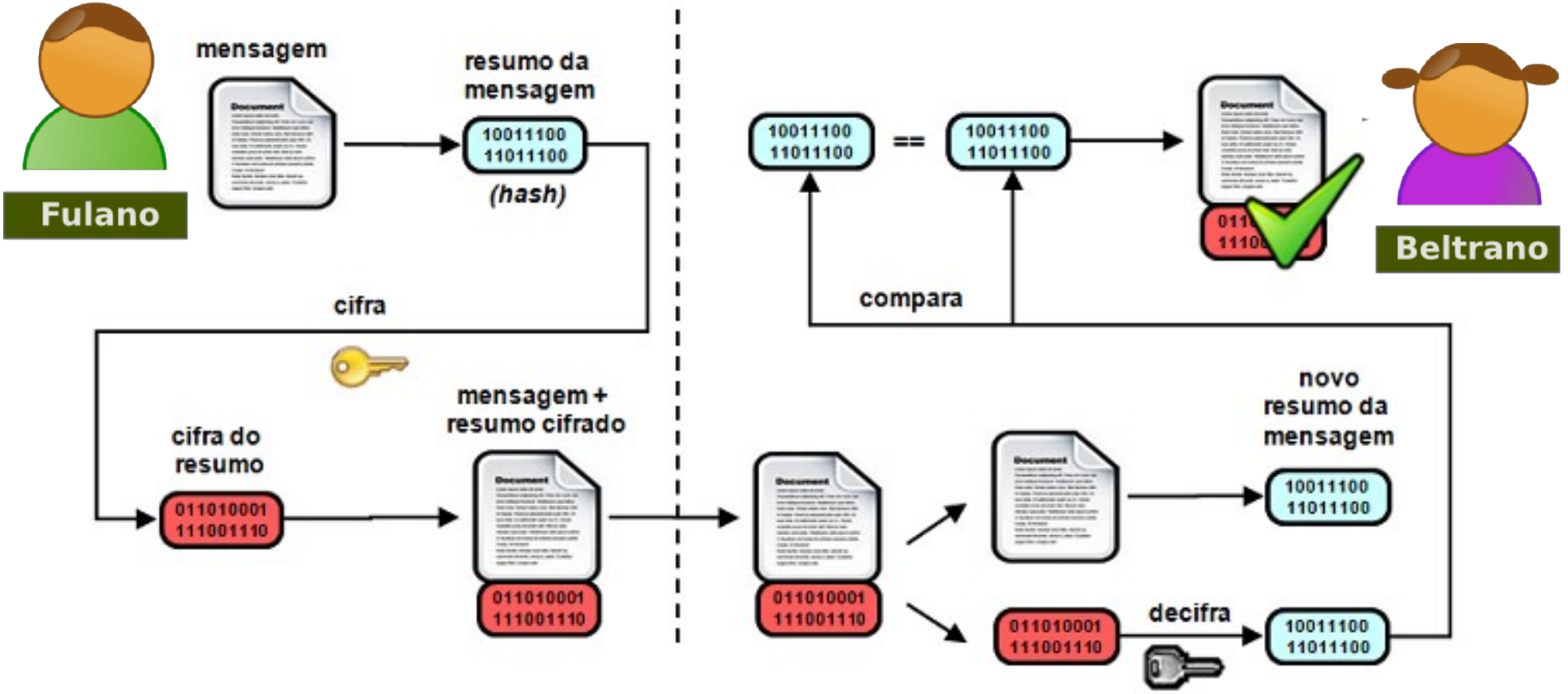
Funções de hash

- Resumo criptográfico de uma mensagem de tamanho variável



Assinatura Digital

- Assinatura digital != assinatura eletrônica
- Propriedades: integridade, autenticidade, não repúdio



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?

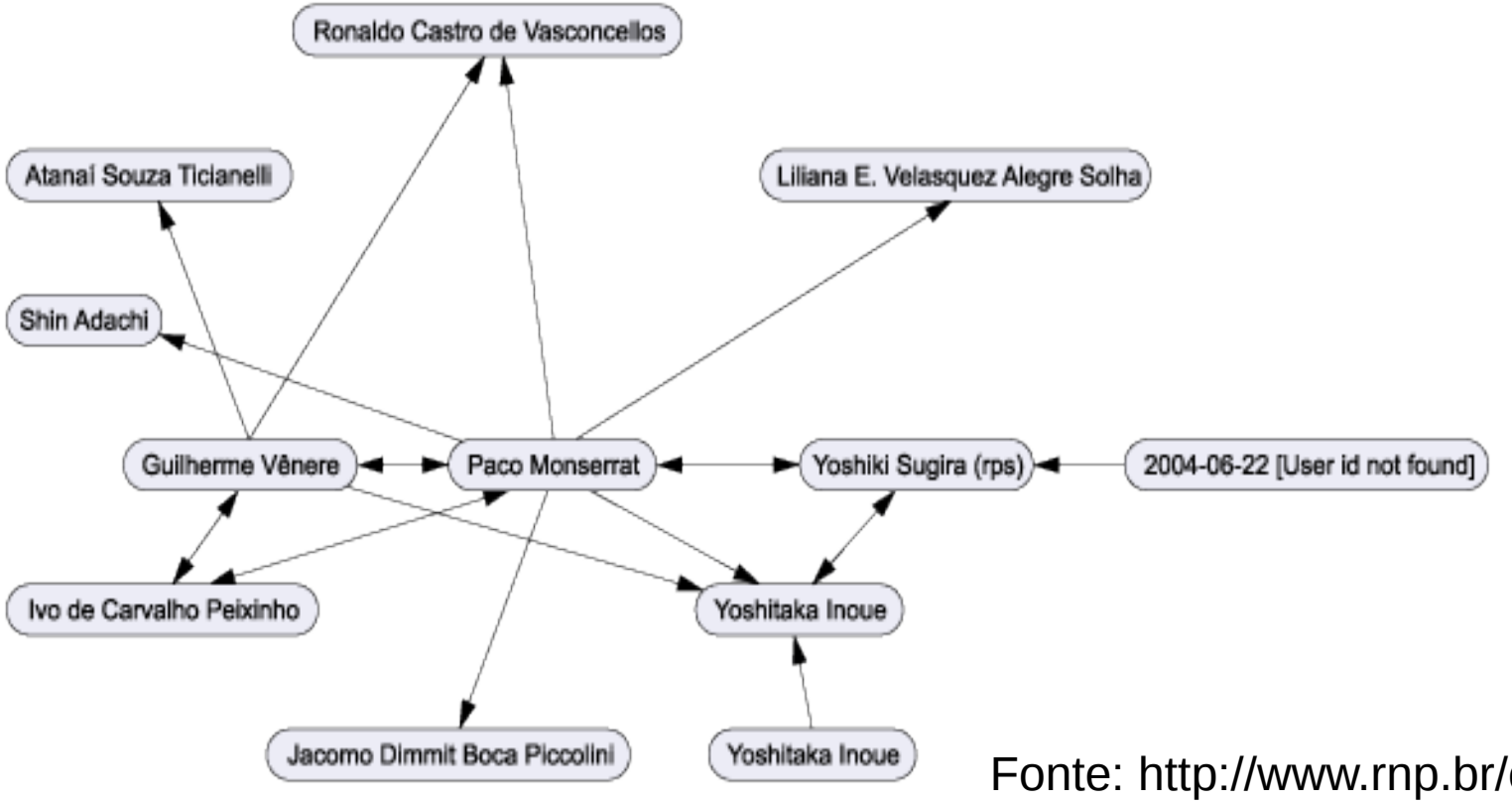
Criptografia assimétrica

Como vincular uma chave à informação de seu detentor?

- Alternativas:
  - Autoridades Certificadoras
  - Teia de confiança (Web-of-Trust)

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



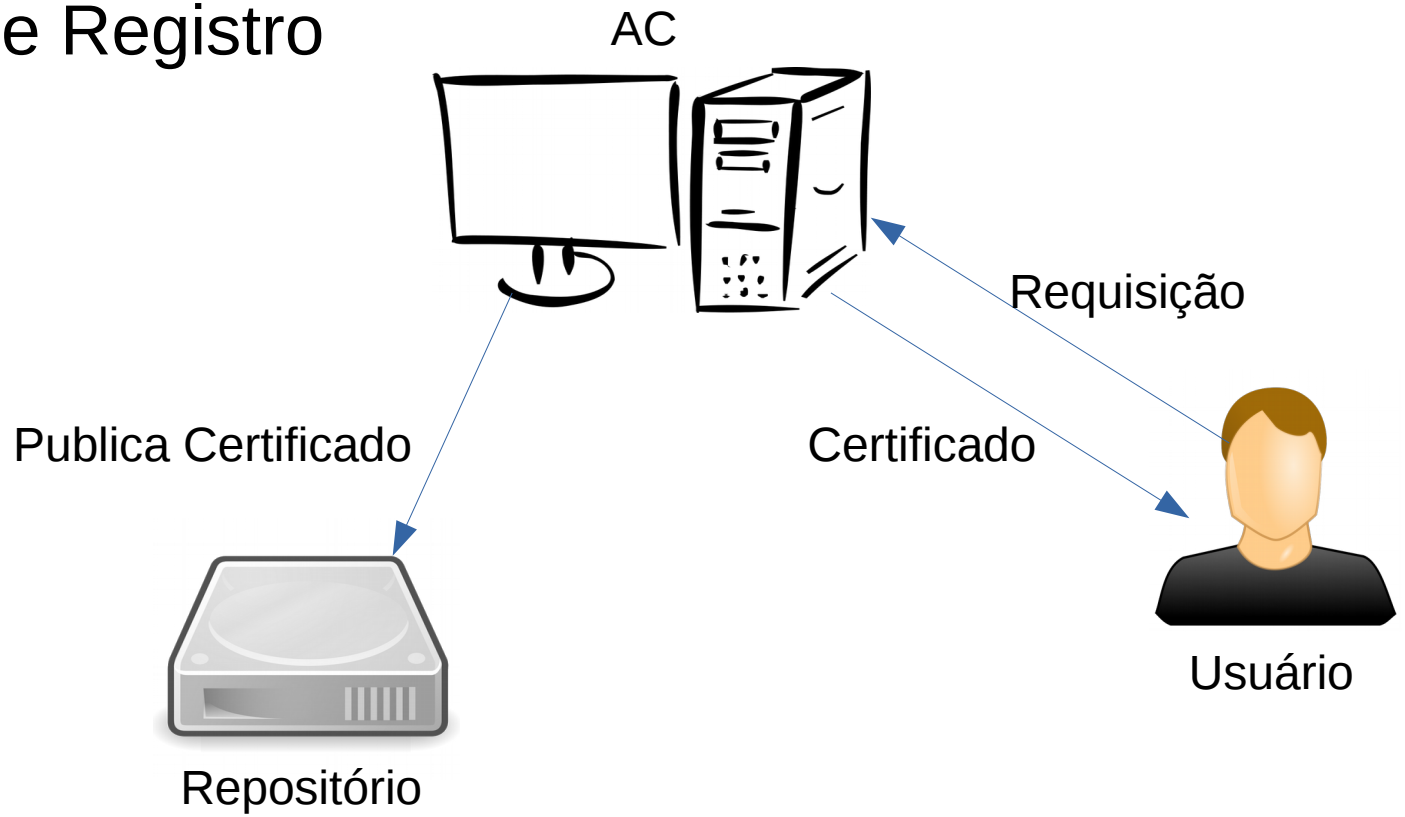
Fonte: http://www.rnp.br/cais/keyserver

Certificado Digital

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

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:
  - 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

A Infraestrutura de Chaves Públicas para Ensino e Pesquisa (ICPEdu) é o serviço oferecido pela RNP para a emissão de certificados digitais e chaves de segurança.

- Assinatura digital;
- Sigilo e Autenticação;
- Proteção das transações na Internet (HTTPS);
- Emissão de certificados digitais (Pessoas e Serviços);
- Credibilidade nos processos administrativos.

Fonte: https://www.rnp.br/servicos/servicos-avancados/icpedu

Aplicações

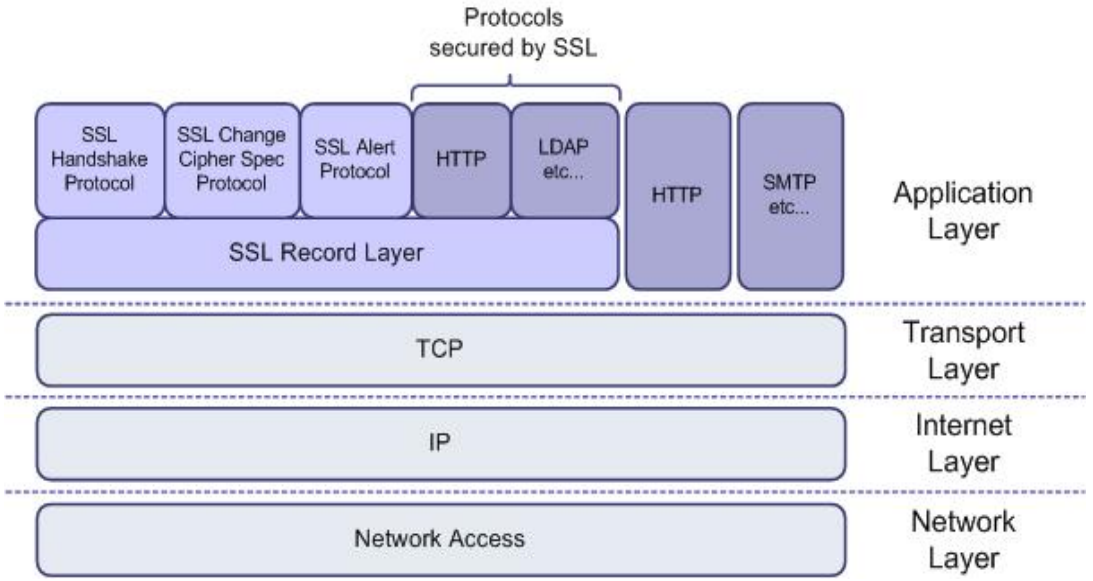
- Comunicação em rede
- E-comerce
- Moeda virtual
- Armazenamento de arquivos e dados pessoais
- Tramitação de processos eletrônicos
- Autenticação de entidades

Comunicação em rede

- Camada de enlace
  - Padrão IEEE 802.11i (WPA/WPA2)
  - Padrão IEEE 802.1AE (MAC Sec)
- Camada de Rede
  - Protocolo IPSec
- Camada de transporte
  - SSL/TLS
- Camada de aplicação
  - S/MIME
  - VPN
  - DNSSEC

SSL/TLS

- Protocolo que provê confidencialidade e integridade de dados entre duas aplicações que comuniquem em canal inseguro.
  - HTTPS, SMTPS, LDAPS, FTPS
- Método híbrido: assimétrica + simétrica



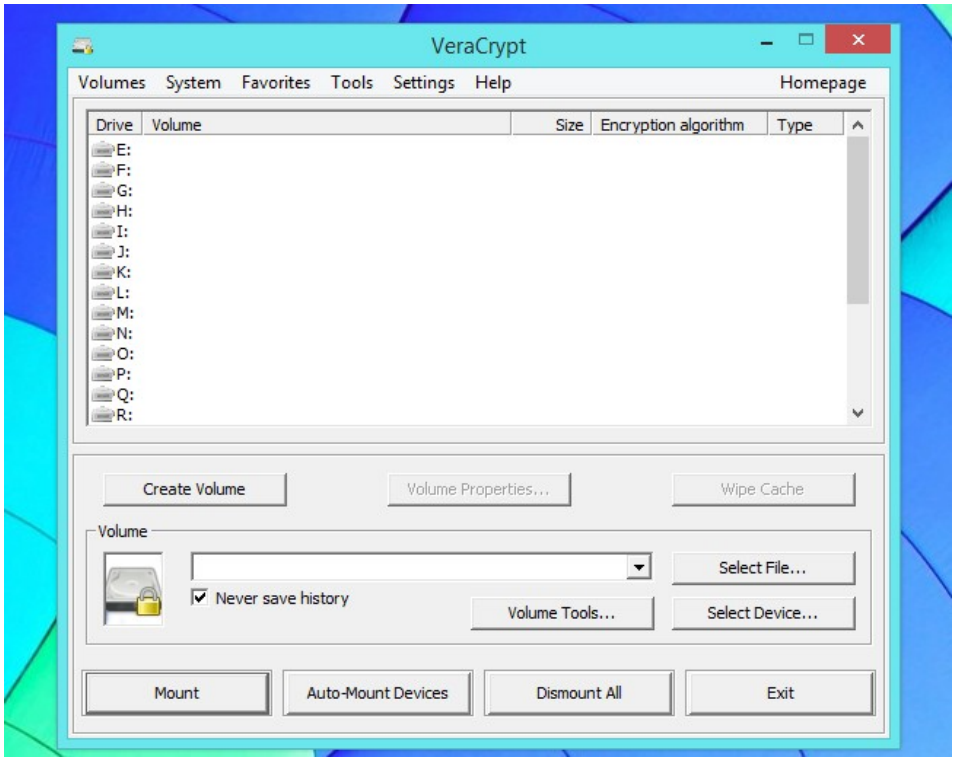
Perfect Forward Secrecy

- Premissa: Vazamento de chaves 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

Criptografia de arquivos

- Como armazenar arquivos pessoais de forma segura?
  - Proteção contra roubos, acesso indevido, serviços de nuvem, etc.



Tramitação de processos eletrônicos

- RNP tem trabalhado em parceria com Universidades em pilotos do ICPEDU Pessoa

Sistema	Módulos Testados (100% de compatibilidade)
SUAP	• Protocolo Eletrônico • Documento Eletrônico

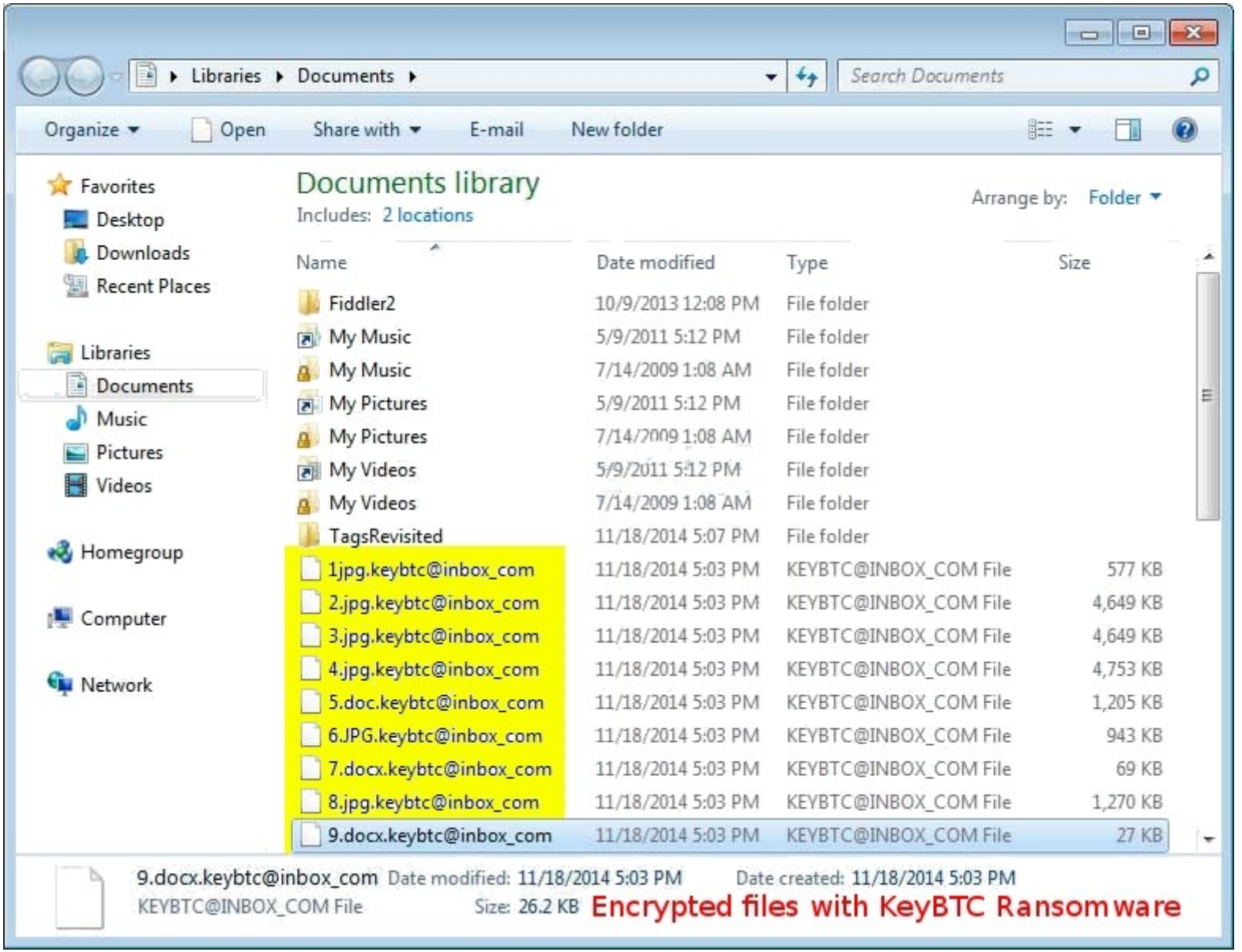
SIG	• SIPAC
	  • Patrimônio
	  • Administração
	  • Contratos

SIG	• SIGAA*
	• Sistema de Gestão e Geração de Documentos • Processo Eletrônico no SPA
Gedoc	• Assinatura de Documentos
SEI	• Aderência está sendo negociada com MPOG

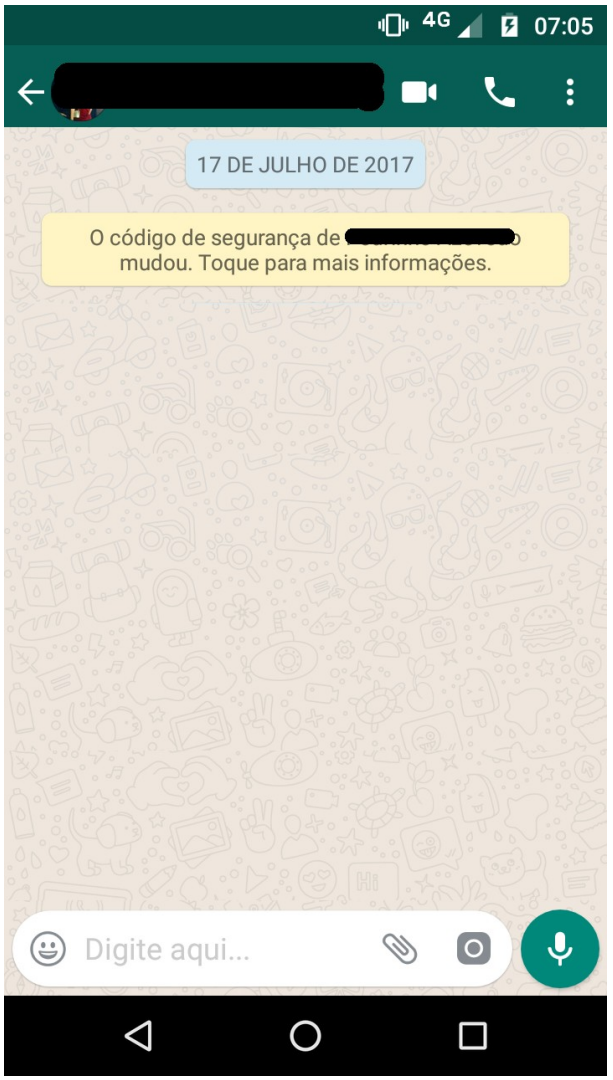
Ataques contra sistemas criptográficos

- Força bruta / Dicionário
  - Tentativa de quebra de valores de chaves
- Seleção de texto cifrado
  - Decifrar trechos conhecidos da mensagem para descobrir a chave
- Acumulo de material criptográfico
- Análise de frequência
- Ataques de regressão
  - NULL Cypher, WPA2

Ransomware


Libraries ▸ Documents ▸
Search Documents
Organize
Open
Share with
E-mail
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Homegroup
Computer
Network
Documents library
Includes: 2 locations
Arrange by: Folder
Name
Date modified
Type
Size
Fiddler2 10/9/2013 12:08 PM File folder
My Music 5/9/2011 5:12 PM File folder
My Music 7/14/2009 1:08 AM File folder
My Pictures 5/9/2011 5:12 PM File folder
My Pictures 7/14/2009 1:08 AM File folder
My Videos 5/9/2011 5:12 PM File folder
My Videos 7/14/2009 1:08 AM File folder
TagsRevisited 11/18/2014 5:07 PM File folder
1jpg.keybtc@inbox_com 11/18/2014 5:03 PM KEYBTC@INBOX_COM File 577 KB
2.jpg.keybtc@inbox_com 11/18/2014 5:03 PM KEYBTC@INBOX_COM File 4,649 KB
3.jpg.keybtc@inbox_com 11/18/2014 5:03 PM KEYBTC@INBOX_COM File 4,649 KB
4.jpg.keybtc@inbox_com 11/18/2014 5:03 PM KEYBTC@INBOX_COM File 4,753 KB
5.doc.keybtc@inbox_com 11/18/2014 5:03 PM KEYBTC@INBOX_COM File 1,205 KB
6.JPG.keybtc@inbox_com 11/18/2014 5:03 PM KEYBTC@INBOX_COM File 943 KB
7.docx.keybtc@inbox_com 11/18/2014 5:03 PM KEYBTC@INBOX_COM File 69 KB
8.jpg.keybtc@inbox_com 11/18/2014 5:03 PM KEYBTC@INBOX_COM File 1,270 KB
9.docx.keybtc@inbox_com 11/18/2014 5:03 PM KEYBTC@INBOX_COM File 27 KB
9.docx.keybtc@inbox_com Date modified: 11/18/2014 5:03 PM Date created: 11/18/2014 5:03 PM
KEYBTC@INBOX_COM File Size: 26.2 KB
Encrypted files with KeyBTC Ransomware

Criptografia e investigações criminais



T PAGSEGURO CURSOS UOL RESOLVE UOL BUSCA E-MAIL CONTA UOL

Bate-papo Notícias Carros Economia Folha Esporte Entretenimento TV e famosos Jogos Estilo Educação Vi

WhatsApp: Audiência do STF vira debate sobre legitimidade das comunicações criptografadas

cristinadeluca
03/06/2017 14h14

15/04/2016 09h14 - Atualizado em 15/04/2016 09h14

Apple e FBI irão ao Congresso se enfrentar novamente por criptografia

Representantes da empresa e da polícia darão depoimento para deputados. Eles tratarão do pedido não cumprido para Apple desbloquear iPhone.

Conclusões

- Uso de criptografia incorpora importantes requisitos de segurança: confidencialidade, integridade, autenticidade, irretratabilidade
- Criptografia não resolve todos os problemas
  - Backup
  - Redundância
  - Diversidade de defesa
- Importante ter cuidado com uso de criptografia
  - Criptografia caseira
  - Legitimidade de uso ou não uso de criptografia

Entendendo a criptografia e como ela pode ser usada na prática

Italo Valcy <italovalcy@ufba.br>
Universidade Federal da Bahia
CERT.Bahia – PoP-BA/RNP

STI Superintendência de Tecnologia da Informação | UFBA

POP-BA