AUTENTICAÇÃO
ASSINATURAS DIGITAIS
CERTIFICADOS DIGITAIS

Professor

Edgard Jamhour

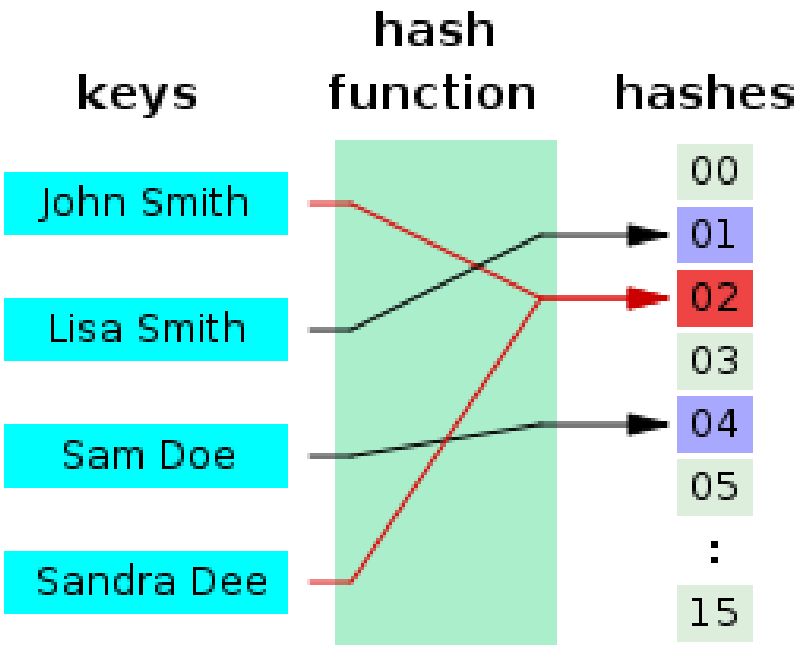
ALGORITMOS DE HASH

Mapeia dados de tamanho variável em códigos de tamanho fixo:

- Digest ou Hashes

Principais aplicações:

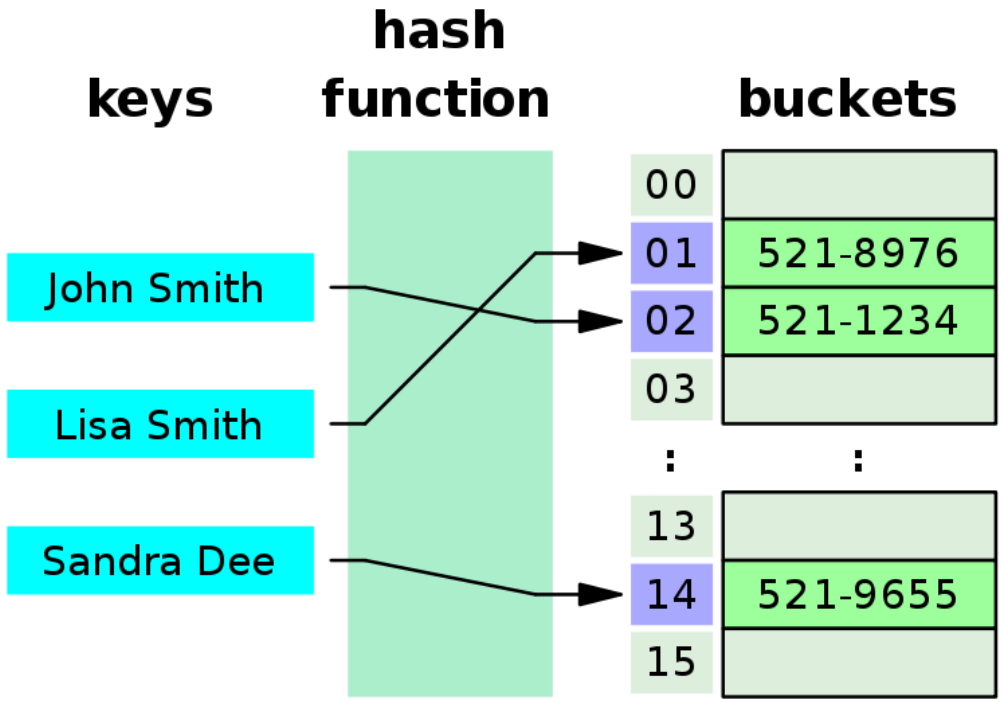
- indexar e localizar rapidamente estruturas de dados
- detectar duplicação de registros em tabelas
- verificar a integridade de dados recebidos pela rede ou potencialmente modificados por vírus



TABELAS HASH = INDEXAÇÃO

A função HASH é muito usada para localizar rapidamente a informação em uma tabela.

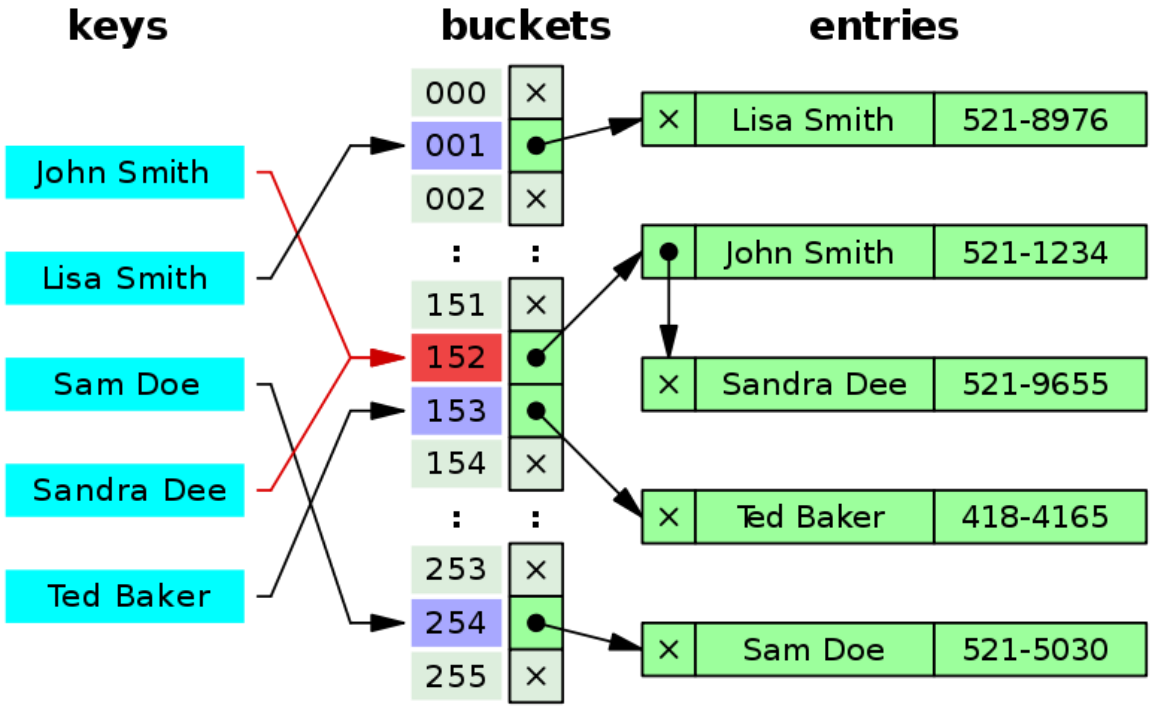
- O HASH calcula a posição (bucket) correspondente ao nome.
- No bucket você encontra informações associadas ao nome, como o telefone.



COLISÃO

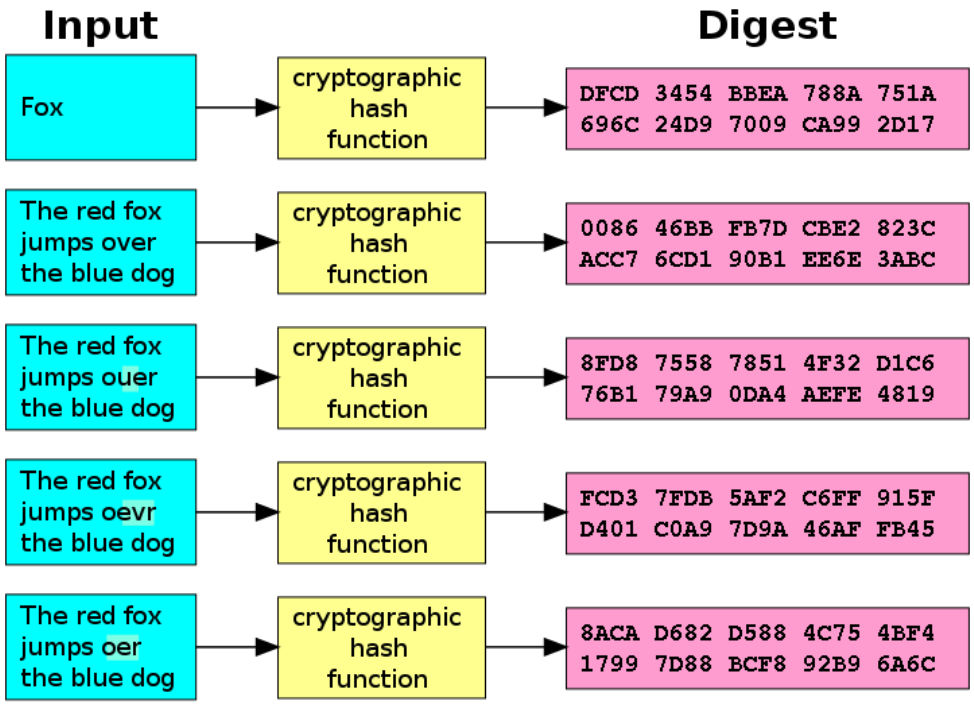
Colisão = mesmo DIGEST é calculado para duas mensagens diferentes.

- Em indexação a colisão pode ser tratada criando uma lista de entradas na mesma posição.
- Em segurança a colisão não pode ocorrer, ou sua ocorrência deve ser muito difícil.



HASH CRIPTOGRÁFICO

Uma função de hash precisa atender a certas propriedades para ser aplicável em criptografia:



(SHA1 – efeito avalanche)

1. determinística
2. rápida
3. inversão inviável
4. efeito avalanche
5. achar colisões inviável

EXERCÍCIO 1:

Implemente uma função que soma os valores ASCII dos caracteres em uma STRING.

Para esta função indique quais propriedades são satisfeitas:

1. determinística (S/N)
2. rápida (S/N)
3. inversão inviável (S/N)
4. efeito avalanche (S/N)
5. achar colisões inviável (S/N)

Qual a sua conclusão? Essa função pode ser usada como HASH criptográfico?

EXERCÍCIO 2:

Repita o teste usando uma função de HASH padronizada:

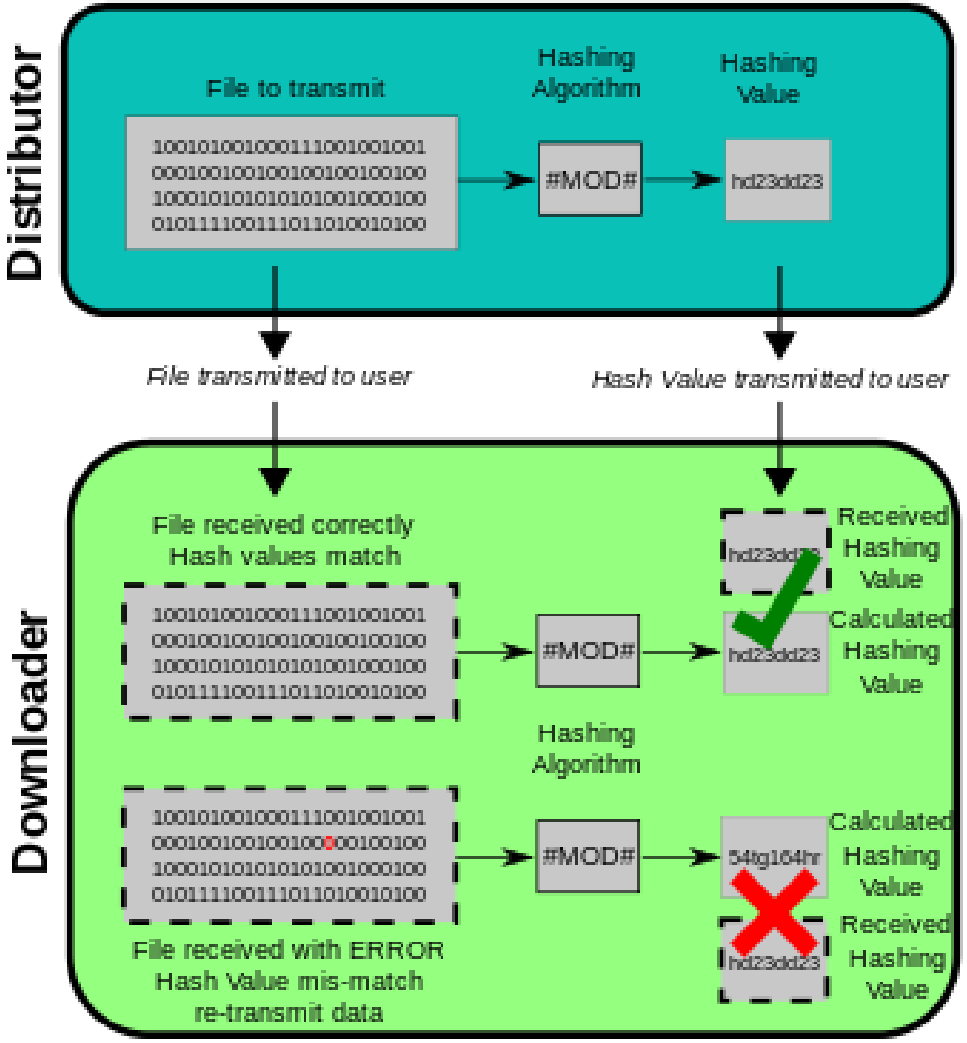
```
import hashlib
m = hashlib.md5()
m.update(b’1234')
m.hexdigest()
```

Qual a sua conclusão? Quais das 5 propriedades de HASH criptográfico esse algoritmo satisfaz?

Quantos bits tem o código HASH do MD5?

APLICAÇÃO DE FUNÇÕES HASH

Verificação de **integridade** de distribuições de software e mensagens transmitidas.



QUIZ 1:

Suponha que um usuário fez o download de um programa no site da Microsoft. Que tipo de segurança o HASH fornece ao usuário? Justifique se a resposta for considerada FALSA.

A. O HASH garante que o arquivo recebido não tem vírus.

B. O HASH garante que o arquivo veio realmente da Microsoft.

C. O HASH detecta erros causados pela perda de dados que possam ocorrer durante o download.

D. O HASH protege contra ataques do tipo Man-In-The-Middle, que interceptem e alterem o arquivo em trânsito.

EXEMPLO: MD5 (MESSAGE DIGEST V5)

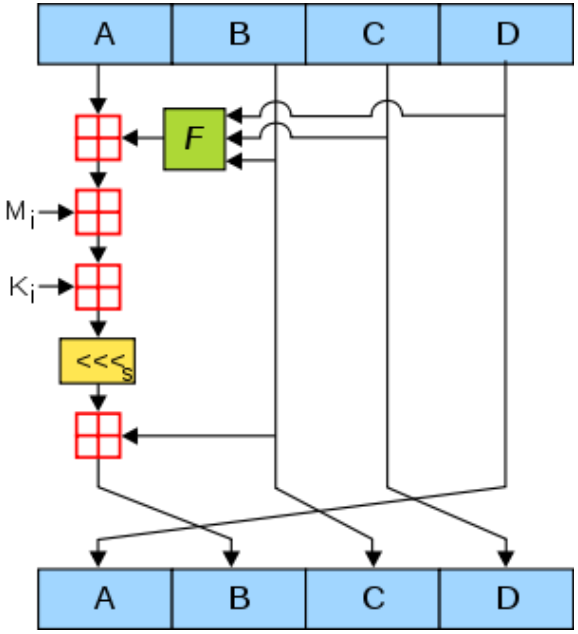
conteúdo informativo

Projetado por Ronald Rivest, 1991 (RFC 1321)

Gera **Digests** de 128 bits.

A mensagem original é fragmentada em blocos de 512 bits (16x32)

Para mensagens não múltiplo de 512 é feito **padding** no bloco final: 100...0 + tamanho original (64 bits)



A, B, C, D: Bloco inicial fixo de 128 bits dividido em partes de 32 bits:

M_i Parte de 32 bits da mensagem original (16 partes)
K_i Constante diferente para cada operação
S Quantidade de bits deslocados (varia a cada operação)

Cada bloco é processado em 4 rounds, usando funções **F diferentes** a cada vez:

$$F(B,C,D) = (B \wedge C) \vee (\neg B \wedge D)$$
$$G(B,C,D) = (B \wedge D) \vee (C \wedge \neg D)$$
$$H(B,C,D) = B \oplus C \oplus D$$
$$I(B,C,D) = C \oplus (B \vee \neg D)$$

Cada round consiste de 16 operação, cada uma com uma parte de 32 bits M_i da mensagem original

SHA (SECURE HASH ALGORITHM)

Existem muitas variantes do SHA, e eles são agrupados em quatro famílias

- SHA-1 e SHA-2: criados pela NSA (National Security Agency)
- SHA-3: Non-NSA competition

SHA-0: não é usado

SHA-1: hashes de 160 bits

SHA-2: resolve potenciais vulnerabilidades do SHA-1

- SHA-256, SHA-512
- SHA-224, SHA-384: versões truncadas de 256 e 512

SHA-3: (previamente conhecido como Keccak)

- Hashes de mesmo tamanho que SHA-2 (224, 256, 384 e 512)

CASOS DE USO DO HASH EM SEGURANÇA

Verificação de integridade de arquivos executáveis

- Arquivos executáveis não devem ser modificados
- Se você calcular o HASH de um arquivo saudável ele será diferente de um HASH de um arquivo contaminado com VIRUS.

Verificação de integridade de arquivos de sistemas

- Um software malicioso do tipo Rootkits pode esconder sua atuação (não aparecer como um processo).
- Contudo, o arquivo contaminado do sistema que está lançado o Rootkit pode ser detectado por HASH.

Usado por HIDS e Antivirus

- Alguns antivírus e HIDS (Host Intrusion Detection System) monitoram a integridade de arquivos calculando o HASH do arquivo saudável e vendo se foram modificados.

Algoritmo integrante de assinaturas digitais de chave pública e HMAC

- Assinaturas digitais protegem a integridade durante a comunicação.

HMAC (HASH-BASED MESSAGE AUTHENTICATION CODE)

HMAC é um tipo de ASSINATURA DIGITAL

HMAC é uma função HASH que autentica uma mensagem concatenada com uma chave secreta

HMAC provê **integridade** e **autenticidade**, porque se a identidade do transmissor será validada pelo uso da chave secreta

Como a chave secreta não é usada para criptografia, a operação é **muito rápida**

Adicionado pelo **TLS** e pelo **IPsec** aos pacotes transmitidos para garantia de integridade e autenticidade.

EXEMPLO DE HMAC

- h = função de hashing (MD5 ou SHA1)
- k = chave secreta
- ipad = 0x363636 ... 3636
- opad = 0x5c5c5 ... c5c5c

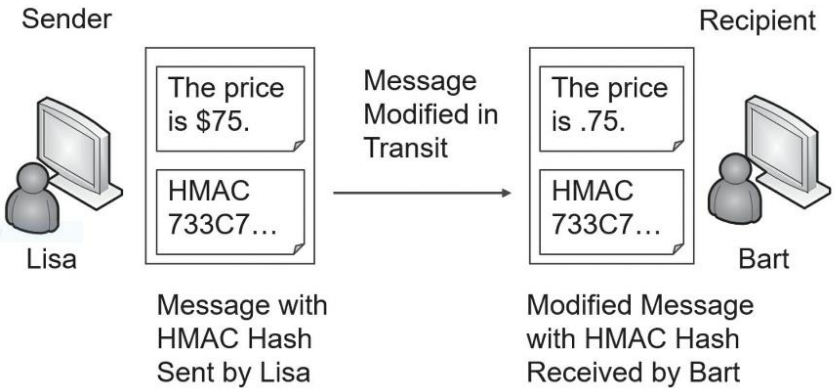
$$\mathrm{HMAC}_K(m) = h\left((K \oplus \mathrm{opad}) \| h\left((K \oplus \mathrm{ipad}) \| m \right) \right),$$

TRANSMISSÃO DE MENSAGENS COM HMAC

Funções HASH não oferece segurança na transmissão de mensagens

A segurança existe apenas se houver um segredo entre as partes para ser usado como prova de identidade.

```
redes@ubuntu:~$ echo password | openssl md5
(stdin)= 286755fad04869ca523320acce0dc6a4
redes@ubuntu:~$ echo password | openssl md5 -hmac 1234
(stdin)= 1fd3928ce25eb44133e89c487010d6cc
redes@ubuntu:~$ echo password | openssl md5 -hmac 1235
(stdin)= 10da927667f97e896e4064bf85d737cd
redes@ubuntu:~$
```



QUIZ 2:

Suponha que Alice enviou uma mensagem para Bob, e que no final da mensagem tem um código HASH. Que tipo de segurança esse HASH fornece? Indique todas que aplicarem.

A. O HASH garante que o arquivo veio realmente da Alice.

B. O HASH detecta erros causados pela perda de dados que possam ocorrer durante a transmissão.

C. O HASH protege contra ataques do tipo Man-In-The-Middle, que interceptem e alterem a mensagem em trânsito.

D. O HASH garante que apenas Bob irá receber a mensagem.

QUIZ 3:

Suponha que Alice enviou uma mensagem para Bob, e que no final da mensagem tem uma assinatura HMAC. Que tipo de segurança esse HMAC fornece? Indique todas que aplicarem.

A. O HMAC garante que o arquivo veio realmente da Alice.

B. O HMAC detecta erros causados pela perda de dados que possam ocorrer durante a transmissão.

C. O HMAC protege contra ataques do tipo Man-In-The-Middle, que interceptem e alterem a mensagem em trânsito.

D. O HMAC garante que apenas Bob irá receber a mensagem.

RIPEMD (RACE INTEGRITY EVALUATION MESSAGE DIGEST)

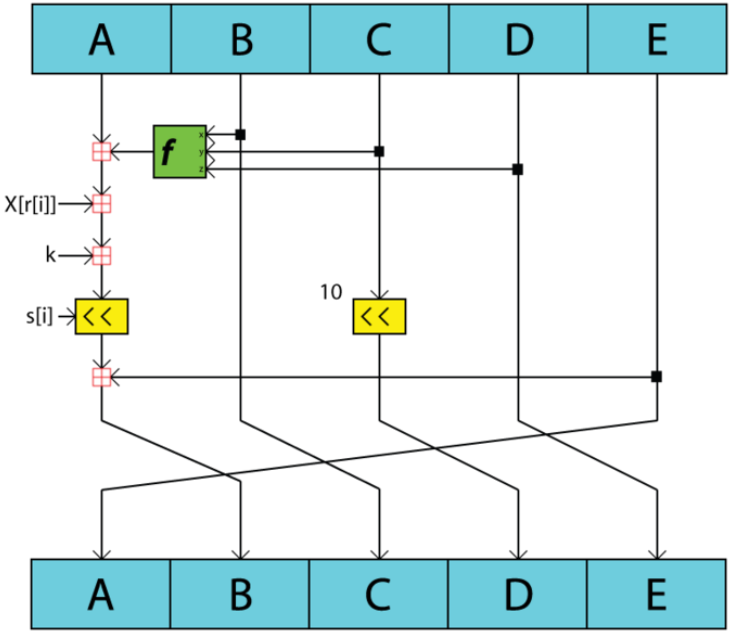
conteúdo informativo

Família de Cryptographic Hash Functions desenvolvidas a partir de 1992.

- RIPEMD, RIPEMD-128, RIPEMD-160, RIPEMD-256 e RIPEMD-320

Menos popular que SHA-X

- Usado em bitcoin e outras criptomoedas



Exemplo: RIPEMD 160
Mensagem processada em blocos de 512 bits
- Usa constantes k diferentes e funções lineares diferentes em múltiplas interações de sub-blocos

HASHING PASSWORDS

conteúdo informativo

PASSWORDS não são salvos diretamente em arquivos, mas sim o seu código HASH.

- Assim, se o arquivo for roubado, a senha do usuário continuará protegida.

Para evitar ataques do tipo **Rainbow**, uma técnica denominada **SALT** é utilizada

Ataques do tipo **Rainbow** consistem em consultar bancos de dados gigantescos com o HASH das palavras mais comuns **já calculadas**.

SALT é uma técnica para fortalecer a senha do usuário sem que ele precise decorar um palavra muito complexa.

Antes de calcular o HASH de um password, alguns caracteres ou bits randômicos são adicionados automaticamente a senha.

- Usando essa técnica, mesmo uma senha simples como ‘dog’ vai gerar um HASH complexo ‘dog$%&’ que não será encontrado em nenhuma tabela de Rainbow.

CONCEITOS DE AUTENTICAÇÃO

Identificação:

- requerer uma identidade (e.g. username)

Autenticação:

- provar a identidade apresentando algum tipo de credencial
  - passwords, smart cards, biometrics
- autenticação é parte do controle de acesso
- não é limitado a usuários
  - inclui serviços, processos, servidores, estações de trabalho, dispositivos de rede

AAA: Authentication, Authorization and Accouting

- Autorizar = dar acesso a um recurso baseado na prova de identidade
- Accounting = registrar o acesso a recursos em logs

AUTENTICAÇÃO COMBINADA = MULTI-FATORES

Autenticação básica: um fator (*fator* ou *type*)

Autenticação forte: dois ou mais fatores

- password + PIN (personal identification number)
  - algo que sabe = não é multifator
- password + smart card ou token USB
  - + algo que possui
- password + impressão digital (*fingerprint*)
  - + algo que é
- password + localização
  - + onde está
- password + gestos em uma tela touch
  - + algo que faz

COMPLEXIDADE DO PASSWORD

Senha forte:

- comprimento suficiente
- não incluir palavras de dicionário, nome, ou atributos do usuário
- complexidade: combinar ao menos 3 de 4 tipos de caracteres
  - maiúscula (26), minúscula (26), números (10) e caracteres especiais (32)

KEYSPACE

- C^N onde:
  - C é o número de caracteres possíveis
  - N é o tamanho da senha
- Password Cracker:
  - 20 bilhões de senhas por segundo em um computador desktop
- Exemplo: Password com 6 caracteres
  - Apenas minúsculas: 308 milhões de possibilidades
  - Todos os tipos de caracteres: 53 quintilhões

ORIENTAÇÕES SOBRE PASSWORDS

Passwords excessivamento complexos são menos seguros

- 4%kiE1NsB*: o usuário vai escrever o password ao invés de memorizar

Exemplos de passwords fortes: PASSPHRASES

- IL0veSecurity+, IL0veThi$BOOk, IWi11P@$$

COMPLEX = mix de diferentes tipos de caracteres

STRONG = mix de caracteres diferentes com tamanho suficiente

POLÍTICAS SOBRE PASSWORDS

Password Expiration

- 45 ou 90 dias

Password Recovery

- Problema: Hacker liga ao helpdesk e pede para resetar o password do CEO
- Tem que ser SELF-SERVICE
  - usar email ou smartfone cadastrado
  - incluir prova de identidade
  - após o reset o password precisa ser temporário (expira após o primeiro uso)
  - passwords expirados não podem ser utilizados
    - alguns sistemas lembram de até 24 passwords

QUIZ: COMPTIA

Desenvolvedores de uma organização criaram uma aplicação para o time de vendas, mas os usuários estão usando a senha 1234 para se autenticar na aplicação, o que viola a política de segurança da instituição. Qual é a melhor resposta que a equipe de segurança deve dar a esse problema?

A. Nada. Senhas fortes não são necessárias em aplicações.

B. Modificar a política de segurança para aceitar essa senha.

C. Documentar isso como uma exceção na documentação da aplicação.

D. Orientar o gerente de desenvolvedores de aplicações para que a aplicação atenda a política de senhas da organização.

QUIZ: COMPTIA

A política de uma organização orienta o seguinte sobre as senhas:
- Expira após 30 dias
- Tamanho mínimo de 14 caracteres
- Deve incluir maiúsculas, minúsculas números e caracteres especiais.
- Deve diferente das 5 últimas utilizadas

Uma análise no log no servidor de autenticação mostra que usuários estão mantendo a mesma senha por mais de 30 dias. Como isso pode ser resolvido?

A. Criar uma regra que a senha não pode ser alterada por 7 dias.

B. Mudar o histórico de senhas para 10.

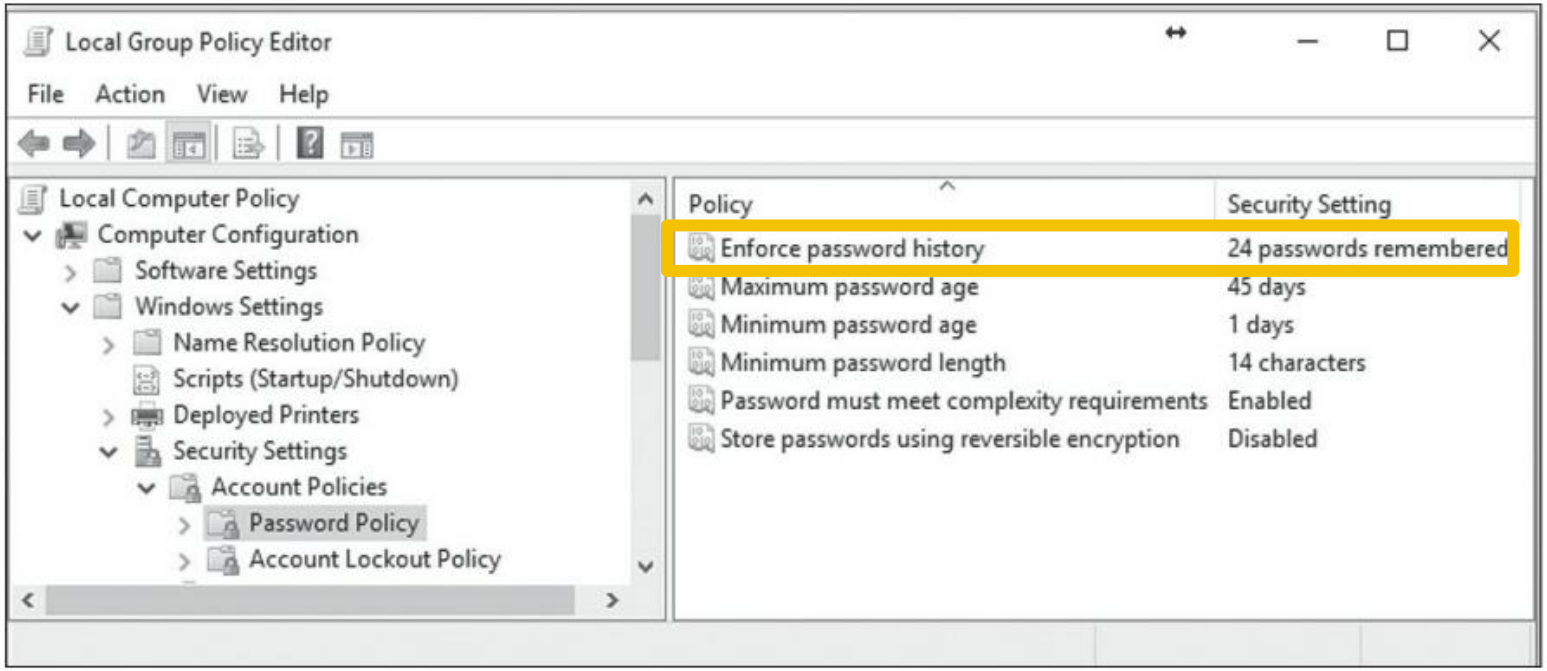
C. Aumentar a complexidade das senhas.

D. Mudar o tempo de expiração para 60 dias.

GPO: GROUP POLICY

Em redes Windows, a política de senhas é feita no Active Directory:

- Aplicar a política a vários usuários e computadores em um domínio
- Contas de usuários e computadores são organizados em OU (Organizational Units)
- Uma GPO pode ser aplicada a uma OU
  - exemplo: trocar a senha de administrador local de todos os computadores do domínio)



BOAS PRÁTICAS:

Políticas de Travamento de Contas (Account Lockout Policies)

- Evita ataques de dicionário e força bruta
- Parâmetros da políticas;
  - Account Lockout Threshold: número máximo de erros de password
  - Account Lockout Duration: tempo que a conta fica suspensa
    - 0 = unlock manual pelo administrador

Trocar a senha default

- Não apenas trocar a senha do administrador, mas também o login
- Manter um login “dummy”: administrator

FATOR: ALGO QUE VOCÊ TEM (SOMETHING YOU HAVE)

Smart Cards

- Cartões com microchip e certificado embutidos
  - Contém a chave privada do usuário
  - O sistema de autenticação contém a chave pública
- Provê autenticação baseada em certificado (ver PKI)
- Pode ser usado com assinaturas digitais e criptografia de dados

Podem suportar autenticação de fator duplo (PIN ou senha)

Smart cards que incluem foto

- CAC (Common Access Card)
  - smart card usado pelo U.S. Department of Defense
  - além do certificado, inclui a foto do usuário e outras informações que podem ser lidas
- PIV(Personal Identity Verification)
  - smart card usado pelas U.S. federal agencies

FATOR: ALGO QUE VOCÊ TEM (CONTINUAÇÃO ...)

Hardware Tokens ou Key Fobs

- Gera um one-time-password
- O número muda periodicamente (60s)
- O número é sincronizado com um servidor

HOTP e TOTP (open source standards)

- HOTP: HMAC-based One-Time Password
  - contador + chave secreta
  - valores de 6 a 8 dígitos válidos até serem usados
- TOTP: Time-based One-Time Password
  - expira tipicamente após 30 segundos

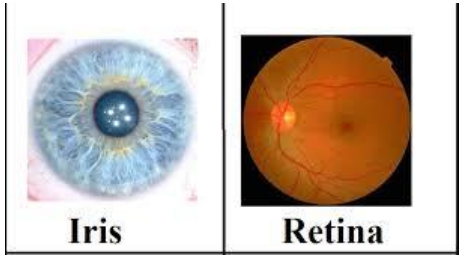
FACTOR: ALGO QUE VOCÊ É (SOMETHING YOU ARE)

Usa informações biométricas para autenticação

- forma mais forte de autenticação
- passwords são a forma mais fraca

Tipos:

- Fingerprint scanner
- Retina scanner
  - analisa padrões dos vasos sanguíneos do fundo do olho
- Iris scanner
  - analisa padrões da íris em volta da pupila do olho
  - funciona até 25 centímetros de distância
- Voice recognition
  - exemplo: Siri da Apple
- Facial recognition
  - exemplo: serviços de reconhecimento de face do Windows Hello



ver comparação

ERROS DE BIOMETRIA

FRR: False Rejection Rate

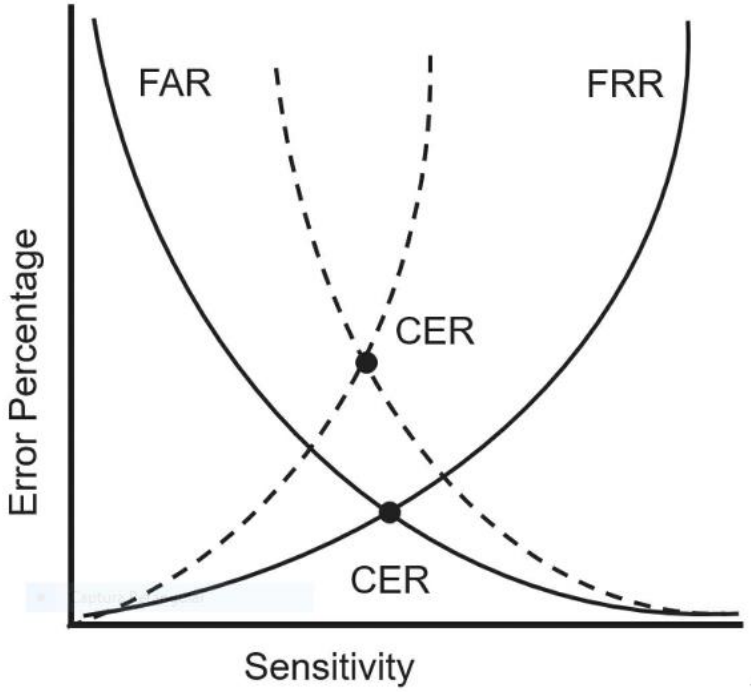
FAR: False Acceptance Rate

Sensitividade:

- parâmetro configurável
- determina o nível de threshold

CER: Crossover Error Rate

- ponto onde FAR = FRR
- quanto menor o CER, mais a acurácia do sistema



QUIZ: COMPTIA

Sua organização está planejando implementar recursos de acesso remoto. A gerência deseja uma autenticação forte e deseja garantir que as senhas expirem após um intervalo de tempo predefinido. Qual das opções a seguir atende MELHOR a esse requisito?

A. HTOP.

B. TOTP.

C. CAC.

D. GPO no Active Directory.

QUIZ: COMPTIA

Sua organização decidiu implementar uma solução biométrica para autenticação. Um dos objetivos é garantir que o sistema biométrico seja altamente preciso. Qual das opções a seguir fornece a MELHOR indicação de precisão com o sistema biométrico?

A. Menor FRR

B. Maior FAR

C. Menor CER

D. Maior CER

FATOR: ONDE VOCÊ ESTÁ (SOMEWHERE YOU ARE)

Fatores usados para localização

- IP: país, região, estado, cidade e, as vezes, código postal
- Pode ser mascarado com VPN
- Em redes locais pode ser substituído pelo nome do computador ou MAC

Onde você está + Biometria

- Método mais forte de identificação
- Método mais difícil de ser falsificado

OBS. Métodos de Biometria:

- Mais fortes:
  - Retina (violação de privacidade) e íris (mais usado)
- Mais flexível:
  - Reconhecimento facial (melhor com luz infravermelha)

FATOR: ALGO QUE VOCÊ FAZ (SOMETHING YOU DO)

Ações (gestos) em uma tela touch screen

Exemplos:

- Passwords baseados em figuras (Windows 10)
  - Clicar em pontos de uma figura pré-definida
  - Desenhar linhas com o dedo
  - Desenhar um circulo em volta de uma parte da figura
- Medição dinâmica de apertos de tecla (keystroke)
  - Mede velocidade, tempo de contato e tempo de movimento

AUTENTICAÇÃO DUAL FACTOR E MULTIFACTOR

Multifactor

- Dois ou mais métodos de autenticação diferentes

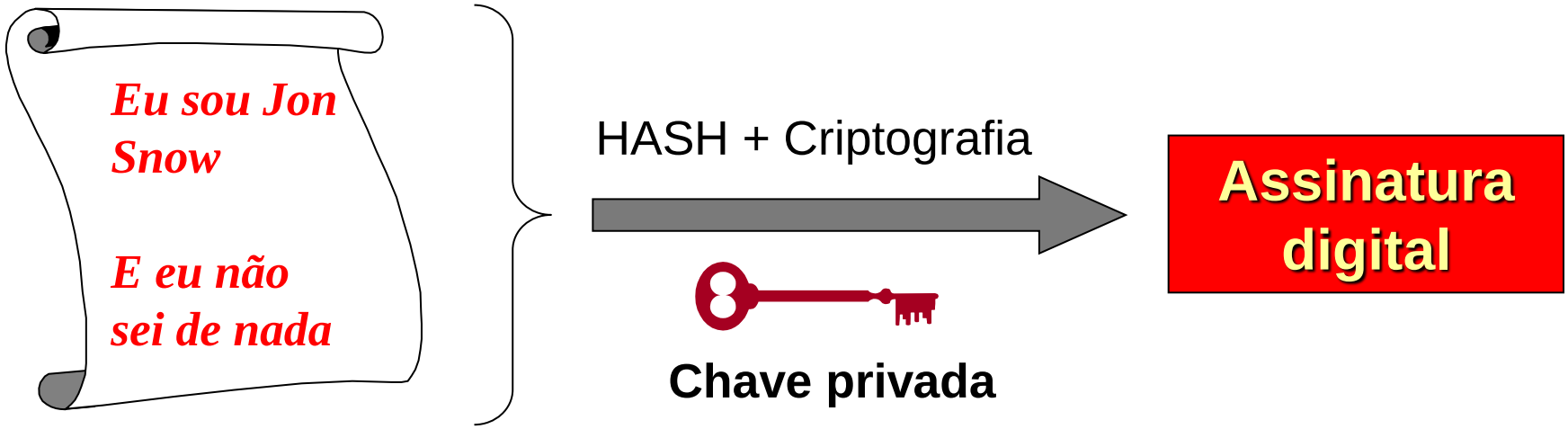
PIN + Password = single authentication factor

Thumbprint + Retina Scan = single authentication factor

ASSINATURA DIGITAL COM CRIPTOGRAFIA ASSIMÉTRICA

AUTENTICAÇÂO DO TIPO ALGO QUE VOCÊ TEM ...

ASSINATURA DIGITAL COM CRIPTOGRAFIA ASSIMÉTRICA



Permite ao receptor verificar a integridade e autenticidade da mensagem:

- **Integridade**: a mensagem não recebida é igual aquela gerada.
- **Autenticidade**: a origem (identidade do autor) é comprovada.
- **Non-Repudiation**: quem executa uma ação não pode negar sua autoria

ASSINATURA DIGITAL COM CRIPTOGRAFIA ASSIMÉTRICA

Função Hash

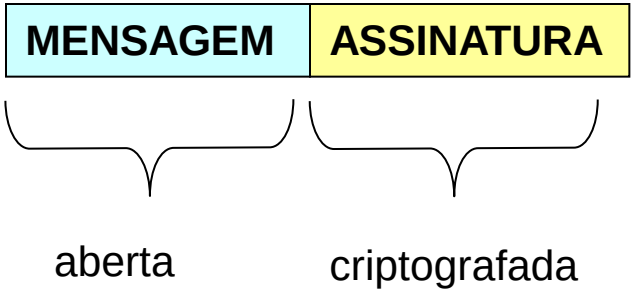
DIGEST

F18901B

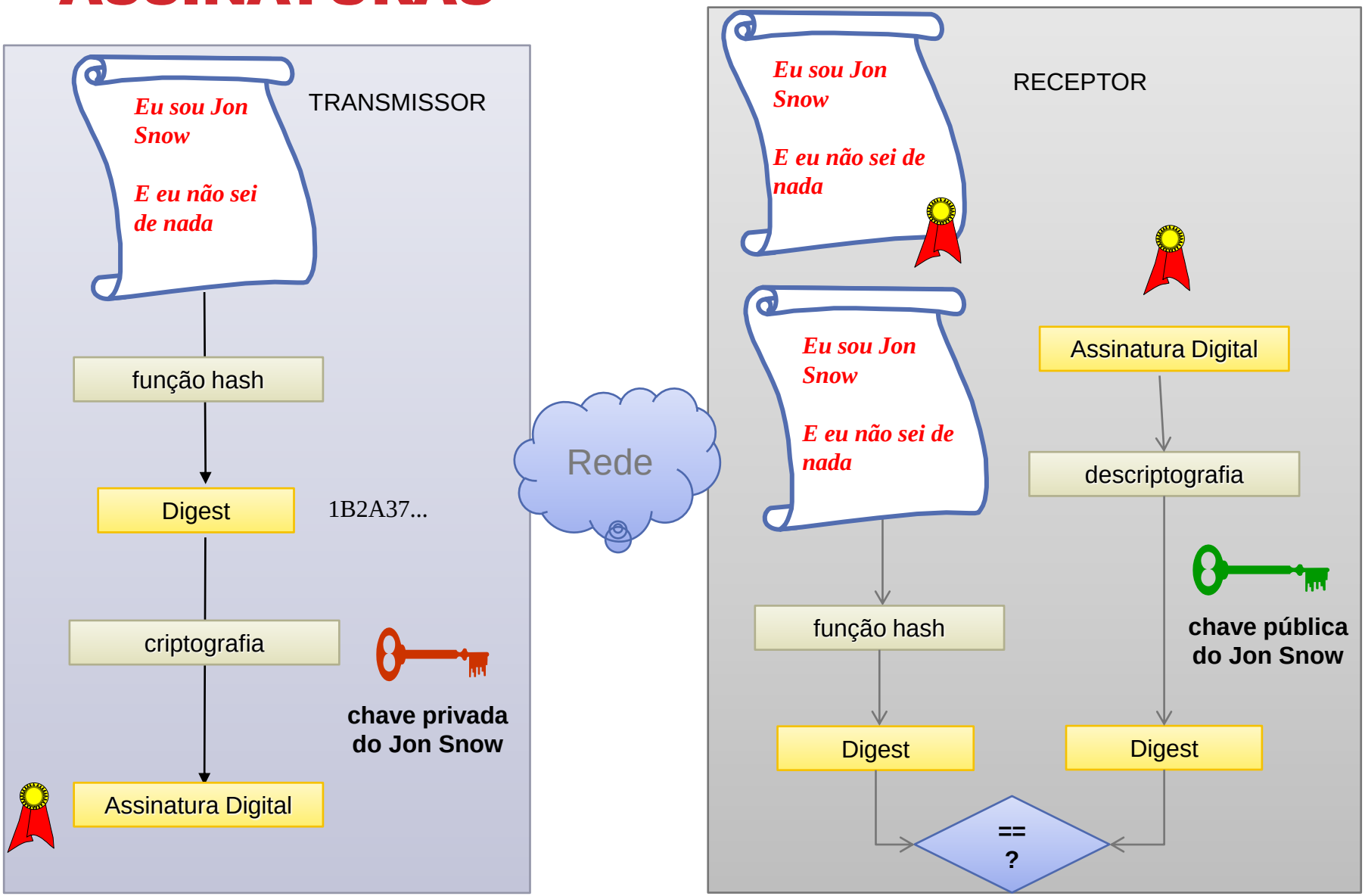
Chave Privada do Autor

ASSINATURA DIGITAL

Mensagem com Assinatura Digital



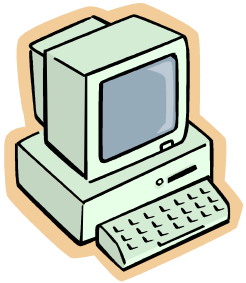
GERAÇÃO E VALIDAÇÃO DAS ASSINATURAS

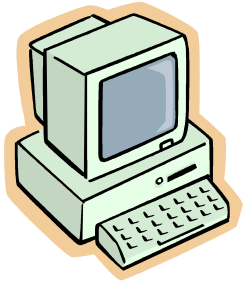


VERIFICAÇÃO DA ASSINATURA DIGITAL

Transmissor (A)

Receptor (B)





MENSAGEM	ASSINATURA DIGITAL

CHAVE PRIVADA DE A

CHAVE PÚBLICA DE A

O receptor precisa ter a chave pública do transmissor para verificar a assinatura.

QUIZ 4:

Suponha que Alice enviou uma mensagem para Bob, e que no final da mensagem tem uma assinatura digital com chave privada. O que Bob precisa conhecer para ter certeza que a mensagem veio da Alice?

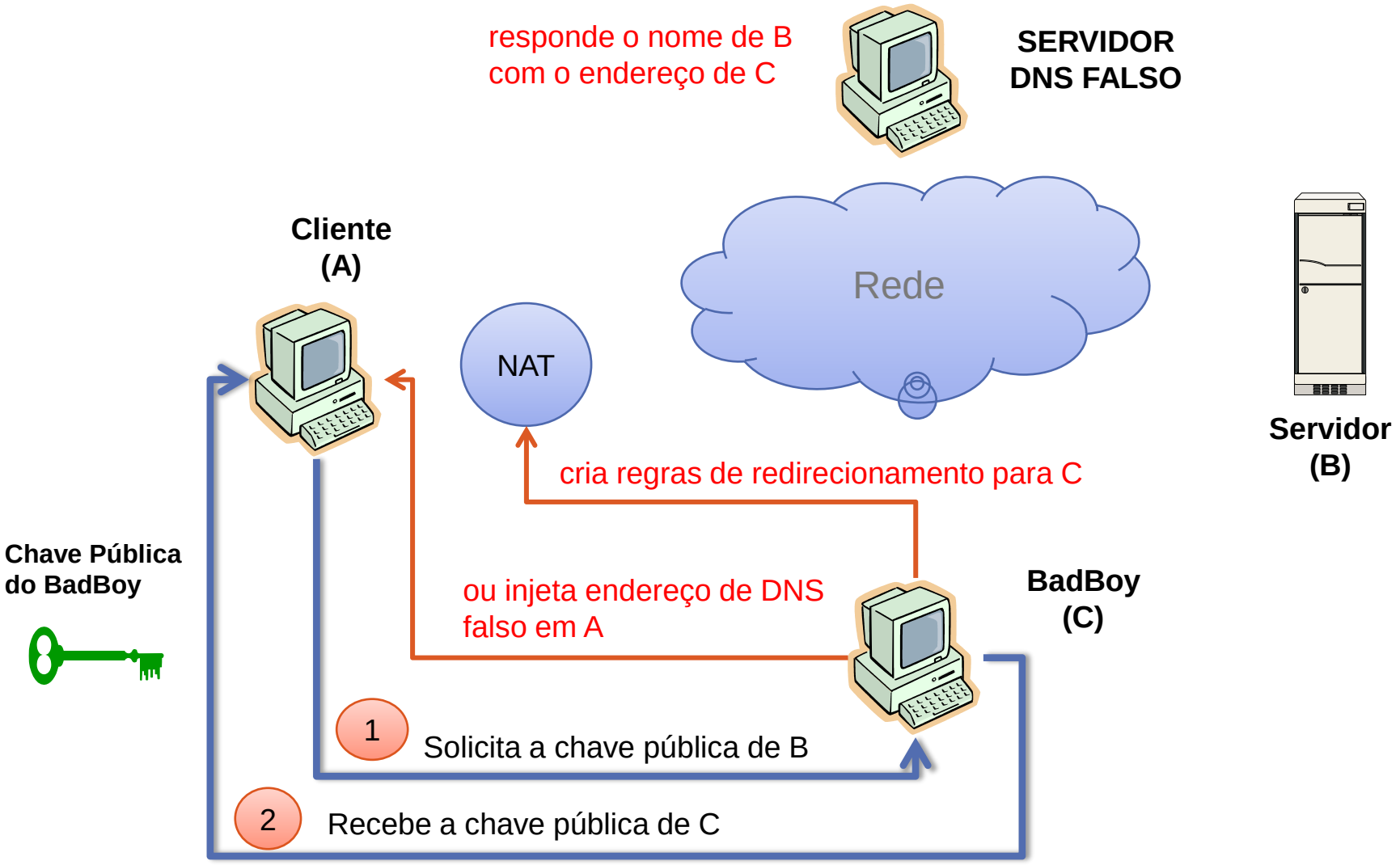
A. Ele precisa conhecer a chave pública da Alice e essa chave pode ser transmitida pela rede.

B. Ele precisa conhecer a chave pública da Alice e a chave não pode ser transmitida pela rede.

C. Ele precisa ter a chave privada da Alice, salva previamente em seu computador.

D. Ele não precisa de nenhuma informação adicional, pois a assinatura contém todas as informações necessárias para sua validação.

COMO TER CERTEZA QUE A CHAVE PÚBLICA ESTÁ CORRETA?



MODELOS DE AUTENTICAÇÃO

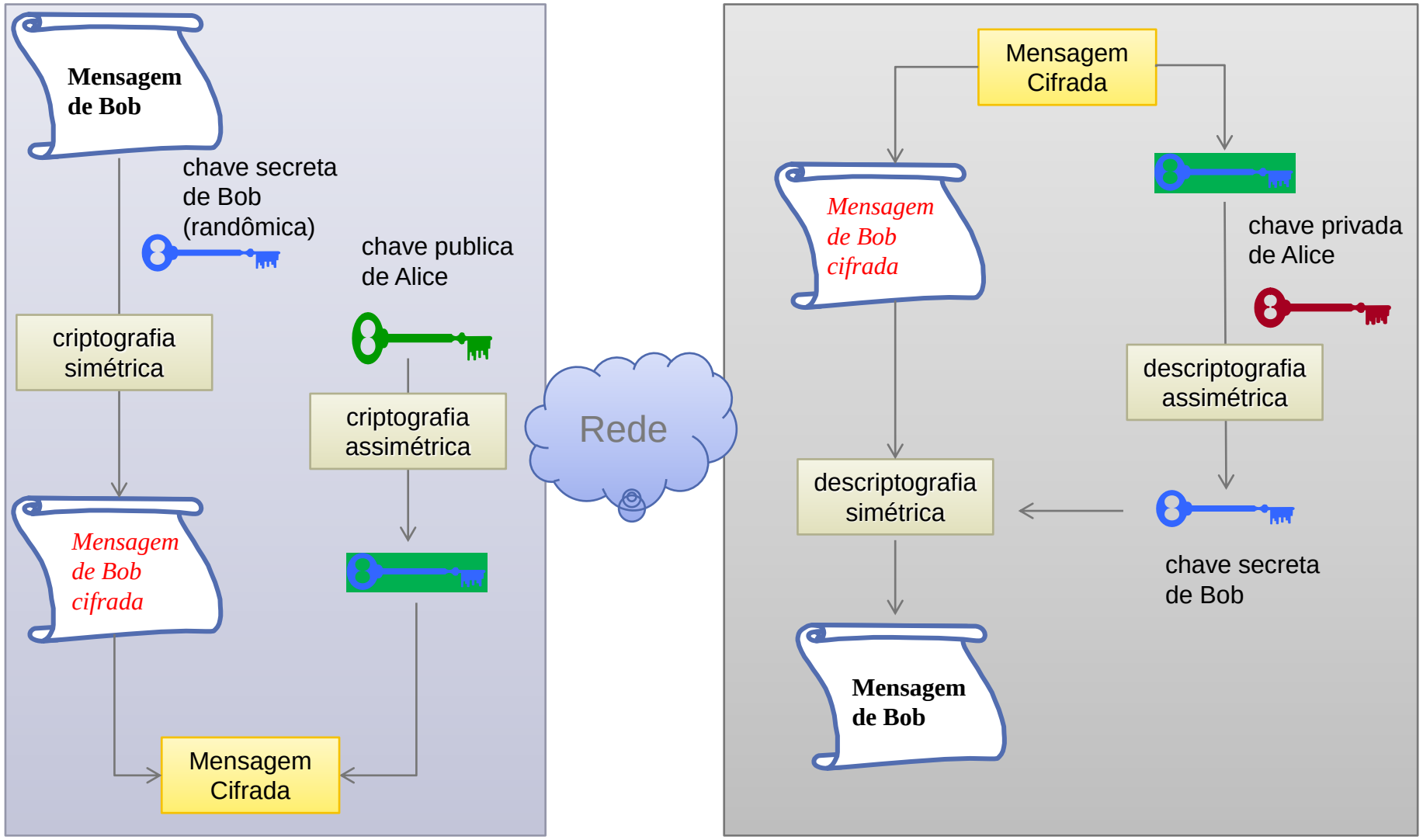
WOT: Web of Trust

- **Modelo descentralizado de confiança**
- PGP (**Pretty Good Privacy**)
- Phil Zimmermann em 1991

PKI: Public Key Infrastructure

- **Modelo centralizado e hierárquico de confiança**
- Certificados X509 usados em SSL/TLS
- Versão original 1988 (para redes X500)
- Versão para uso na Internet: RFC 5280
  - Usualmente referida como **PKIX**

PGP: PRETTY GOOD PRIVACY

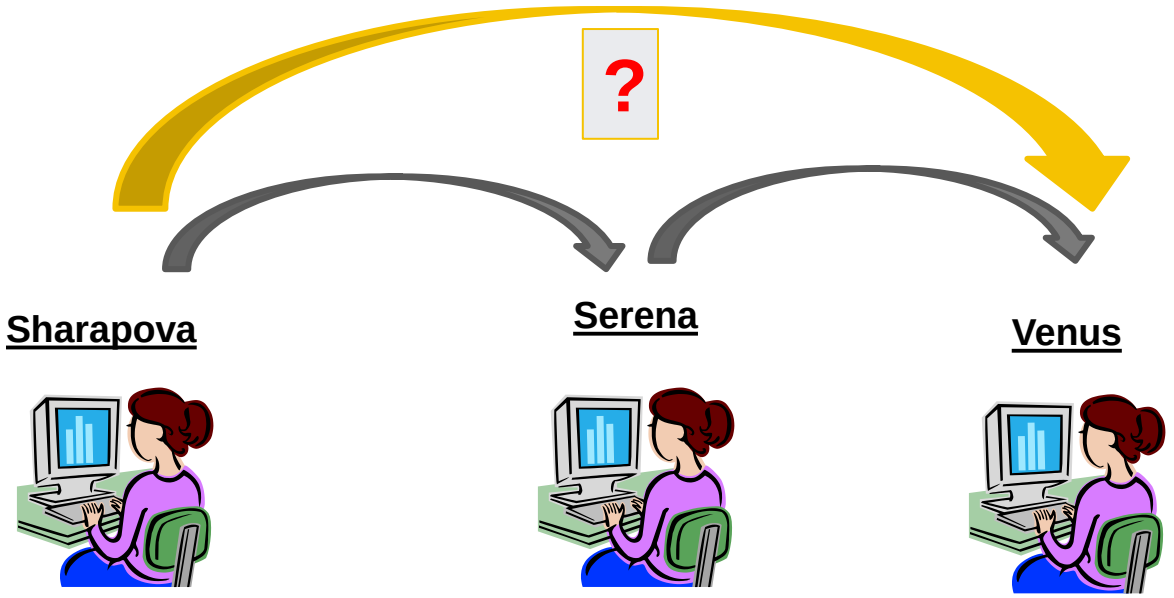


WEB OF TRUST

Considere o exemplo a seguir:

- Sharapova já tem a chave pública da Serena
- Serena já tem a chave pública da Venus

Como a Sharapova pode obter a chave pública da Venus de um modo seguro pela rede?



OBS: CONFIAR é já ter a ***chave pública***

WEB OF TRUST

Sharapova pode receber a chave da Venus pela Serena

Chave pública da Venus	Essa chave pertence a Venus	Assinado Serena

A assinatura é feita com a chave privada da Serena

Sharapova

confia na Serena

Serena

confia na Venus

Venus

Sharapova consegue validar a assinatura pois já tem a chave pública da Serena

OBS: CONFIAR é já ter a ***chave pública***

WEB OF TRUST & PATH SERVERS

COMO SHARAPOVA PODE VALIDAR A MENSAGEM DE MARTINA?

1

Mensagem assinada com a **chave *privada*** *de Martina*

Sharapova

confia na Serena

Serena

confia na Venus

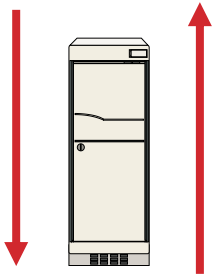
Venus

confia na Martina

Martina

2

Se eu conheco a serena, qual o **menor caminho** até a Martina?



Serena - Venus - Martina

3

PATH Server

QUIZ 5:

No exemplo com PATH server, o que a Sharapova precisa fazer para validar mensagem da Martina? Ordene os passos corretamente. Alguns passos podem não ser necessários ou estarem incorretos.

A. Ele precisa obter a chave pública da Martina assinada com a chave pública da Venus .

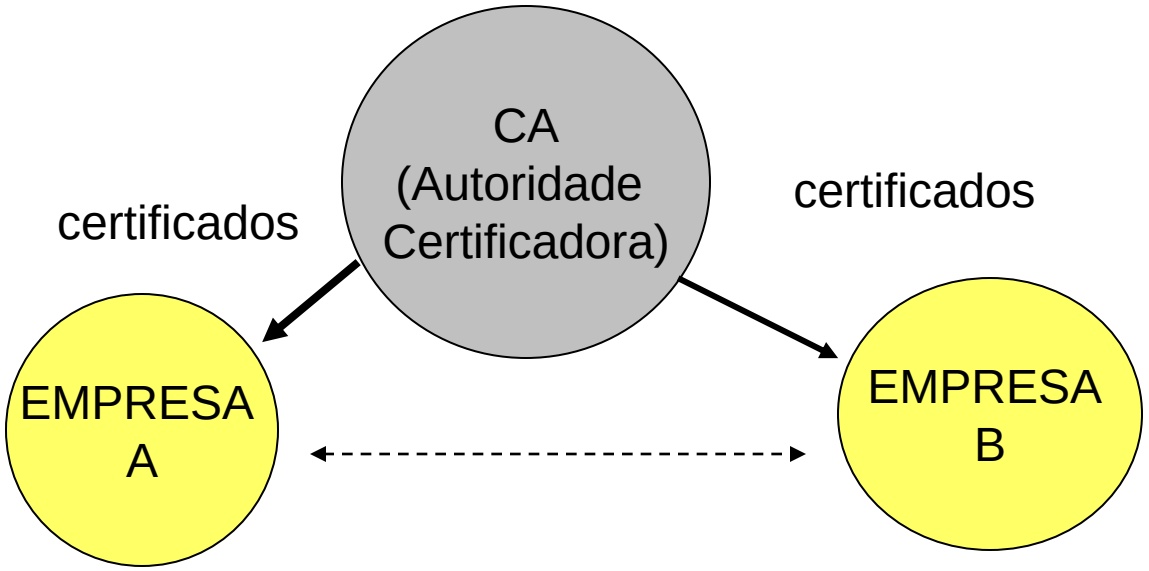
B. Ela precisa obter a chave pública da Venus assinada pela Serena.

C. Ela precisa obter a chave pública da Serena assinada pela Venus.

D. Ela precisa obter a chave pública da Martina assinada pela Serena.

PKI (PUBLIC KEY INFRASTRUCTURE)

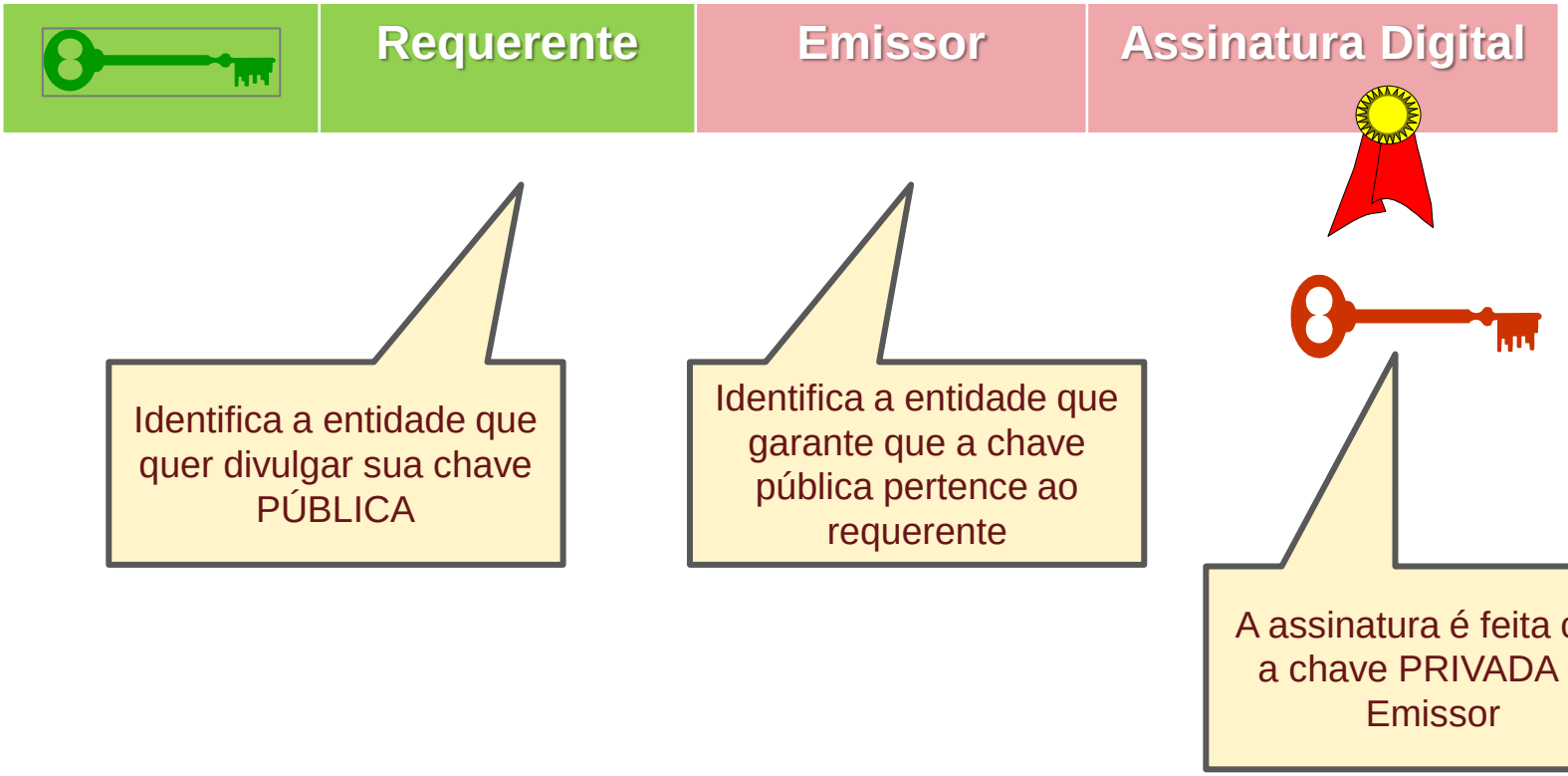
O termo PKI (Infraestrutura de chave pública) é utilizado para descrever o conjunto de elementos necessários para implementar um mecanismo de **certificação** por chave pública.



CERTIFICADO DIGITAL

É uma estrutura que associa uma chave pública ao seu proprietário

O certificado é emitido por alguém em quem você confia (isto é, já tem a chave pública)



EMISSOR = AUTORIDADE CERTIFICADORA

Autoridade Certificadora
(Verisign, Certisign, Etc.)

C.A.
(Certification Authority)

CHAVE
PRIVADA

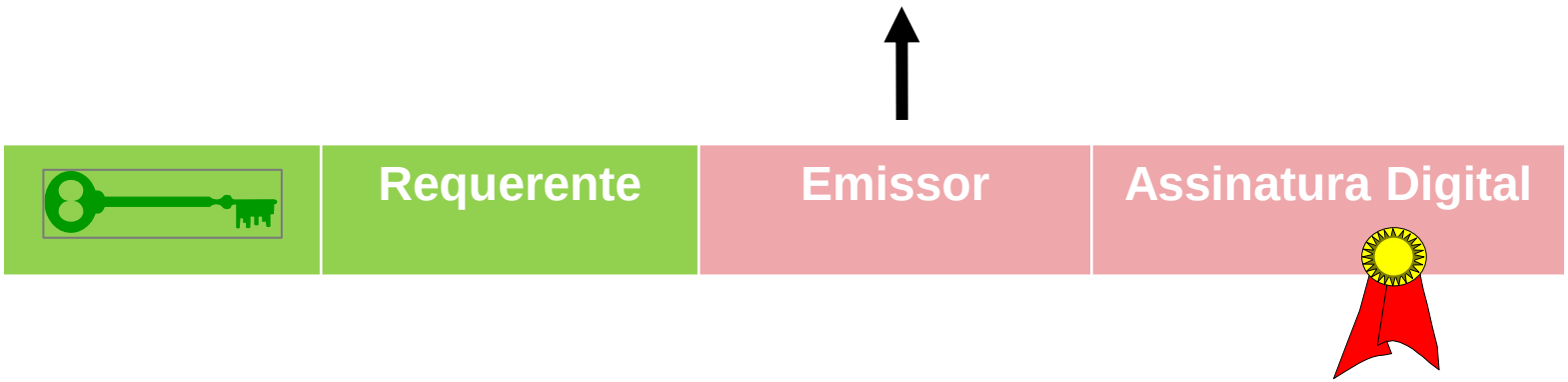
Chave pública
(e.g., Banco do Brasil)

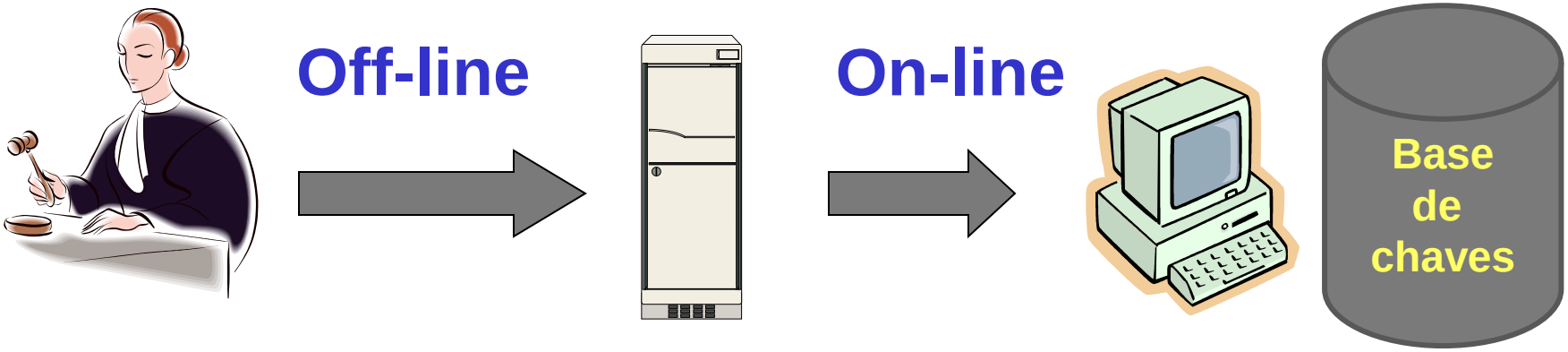
www.bancodobrasil.com.br
Banco do Brasil S.A.
Brasilia, DF, Brasil

www.verisign.com
Verisign, Inc.

ESTRATÉGIAS DE CERTIFICAÇÃO

www.verisign.com





www.google.com

O software que recebe o certificado (por exemplo, o browser) deve possuir a chave pública da autoridade certificadora.

QUIZ 6:

Como o navegador Web obtém a chave pública da Autoridade Certificadora (CA)?

A. A chave pública da CA vem junto com o certificado do Requerente.

B. O navegador Web envia o certificado do Requerente para CA validar, assim não precisa da chave pública da CA .

C. Assim que obtém o certificado, ele consulta a CA para obter sua chave publica.

D. A chave pública da CA precisa estar previamente armazenada no computador.

PADRÃO X509

O padrão que define o formato dos certificados é denominado X509

- Identifica o Requerente e o Emissor usando **Distinguished Names**.

Distinguished Name: conjunto de atributos que define uma entidade de forma única

DN Field	Abbrev.	Description	Example
Common Name	CN	Name being certified	CN=Joe Average
Organization or Company	O	Name is associated with this organization	O=Snake Oil, Ltd.
Organizational Unit	OU	Name is associated with this organization unit, such as a department	OU=Research Institute
City/Locality	L	Name is located in this City	L=Snake City
State/Province	ST	Name is located in this State/Province	ST=Desert
Country	C	Name is located in this Country (ISO code)	C=XZ

EXEMPLO: CERTIFICADOS X509

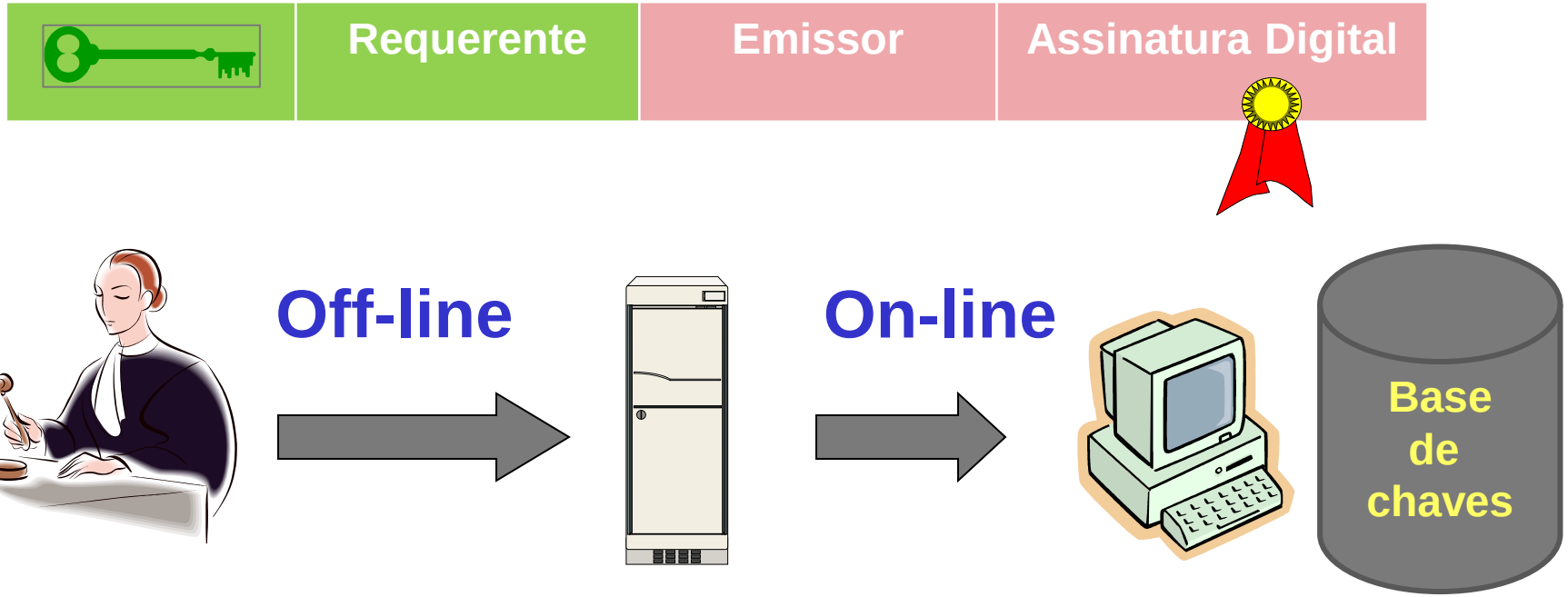
Campo	Exemplo
Versão	v3
Número de Série	3b 5b 9d 41 f0 00 b6 e4 95 c3 fc 84 24 41 37 f7
Algoritmo de Assinatura	sha256RSA (sha256WithRSAEncryption)
Algoritmo de Hash	sha256
Emissor	CN = GeoTrust SHA256 SSL CA, O = GeoTrust Inc., C = US
Validade	de domingo, 16 de outubro de 2016 21:00:00 até terça-feira, 17 de outubro de 2017 20:59:59
Requerente	CN = conteudo2.uol.com.br, OU = Universo Online AS, O = Universo Online AS, L = Sao Paulo, S = Sao Paulo, C = BR
Chave Pública	RSA (2048) .... muitos e muitos bytes ...
Lista de Revogação:	URL=http://gj.symcb.com/gj.crl
Assinatura Digital	67 30 f1 f0 07 72 f6 99 d1 14 a1 dc 98 31 84 49 a9 e9 98 cf

PROBLEMA: COMO ESCALAR O PKI?

Existem centenas de países no mundo, cada um com um idioma diferente.

O que acontece se você acessar um site na China ou na Arábia Saudita?

Será que o seu navegador Web tem a chave pública das CAs desses países em sua base de chaves?



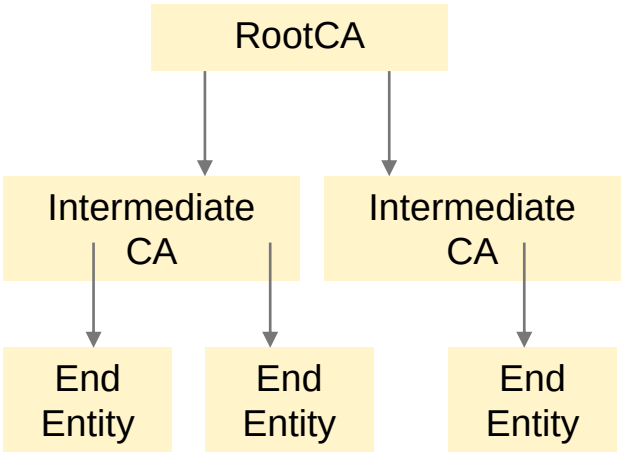
MODELO DE CONFIANÇA HIERÁRQUICO

O modelo Hierárquico é a forma mais comum de modelo de confiança

O modelo Hierárquico é centralizado (em oposição ao WOT)

Nesse modelo, uma entidade **Trusted** emite certificados para CAs intermediárias.

Os certificados para entidades finais (servidores, pessoas, etc.) são emitidos pelas autoridades intermediárias.



TIPOS DE CERTIFICADOS

- **Certificado Root**
  - Auto assinado
  - Representa uma Autoridades Certificadoras (CA)
  - Validado com sua própria chave pública
  - O certificado precisa estar previamente armazenado

- **Certificados Intermediários**
  - Assinado por um certificado Root ou Intermediário
  - Representa uma Autoridade Certificadora (CA)
  - Usado para assinar o certificado da Entidade Final
  - O certificado não precisa estar previamente armazenado

- **Certificados de Entidade Final**
  - Assinado com um certificado Root ou Intermediário
  - Usado para identificar Servidores HTTP e outros serviços
  - O certificado não precisa estar previamente armazenado

CADEIA DE CERTIFICAÇÃO

Certificados Intermediários são usados para:

- Escalabilidade no processo de geração de certificados
- Redução do risco de exposição da chave privada do Root
- Redução dos certificados comprometidos em caso de exposição da chave privada

Cadeia completa transmitida ao cliente (Apenas o root é opcional)

Entidade Final
Subject: www.uol.com.br
Issuer: RapidSSL SSHA56

C.A. Intermediária
Subject: RapidSSL SHA256 Issuer: GeoTrust Global

C.A. Root
Subject: GeoTrust Global
Issuer: GeoTrust Global

C.A. Root
Subject: GeoTrust Global
Issuer: GeoTrust Global

C.A. Intermediária
Subject: RapidSSL SHA256
Issuer: GeoTrust Global

Entidade Final
Subject: www.uol.com.br
Issuer: RapidSSL SSHA56

REVOGAÇÃO DE CERTIFICADOS

- De acordo com a **RFC 5280**: **PKIX**

- Certificados são identificados por **números de série**
  - **Unicos** para cada C.A.

- **CRL: Certificate Revogation List**
  - Lista de certificados revogados assinados pela CA e disponível publicamente em um repositório
  - Certificados são identificados pelo seu “numero de série”

- **CRLs** são atualizadas periodicamente pela CA

- **Clientes** fazem verificação periódica das CRLs

CONCLUSÃO

Criptografia Simétrica

- Chaves de pelo menos 128 bits
- Rápido
- Usado para proteção de dados

Criptografia Assimétrica

- Chaves de pelo menos 2048 bits
- Lento
- Usado no processo de negociação de chaves