

Conceitos de criptografia

Adaptado de Cristian Moecke (BRy Tecnologia)
Prof. Martín Vigil

Krypto graphos

“Cripto” vem do grego “*kryptos*” e significa oculto, envolto, escondido.

Também do grego, “*graphos*” significa escrever, registrar.

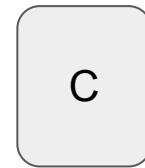
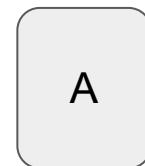
Criptografia: registrar algo de forma oculta...

... mas é muito mais que isto!

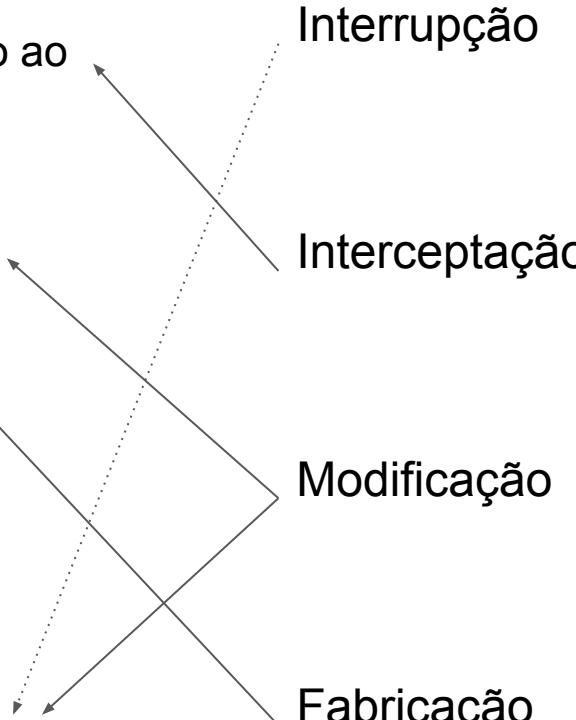


Ameaças de segurança

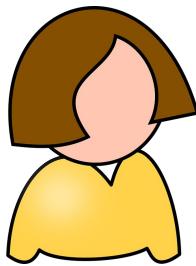
- Interrupção
 - Mensagem de A não chega em B
- Interceptação
 - Mensagem de A para B é capturada por C
- Modificação
 - Mensagem de A para B é modificada por C
- Fabricação
 - C envia mensagem para B como se tivesse vindo de A



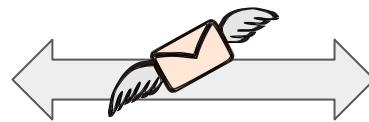
Propriedades alcançadas através de criptografia

- **Sigilo/Confidencialidade**
 - Garantia de que somente o destinatário terá acesso ao conteúdo da mensagem
 - **Integridade**
 - Quem recebe a mensagem consegue identificar se houve alterações no seu conteúdo
 - **Autenticação**
 - Quem recebe a mensagem consegue identificar o remetente
 - **Não recusa ou não repúdio**
 - Quem envia a mensagem não pode negar que a enviou
 - **Irretroatividade – tempestividade**
 - Garantias sobre a existência de uma mensagem em determinada data
- 

Nossos personagens....

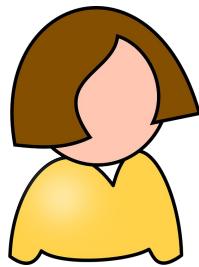


Alice



Bob

Nossos personagens....



Alice



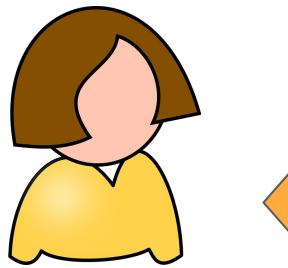
Bob



Eve

*Ameaça:
Interceptação*

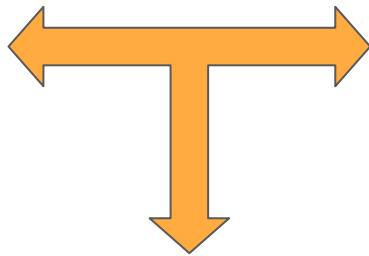
Nossos personagens....



Alice



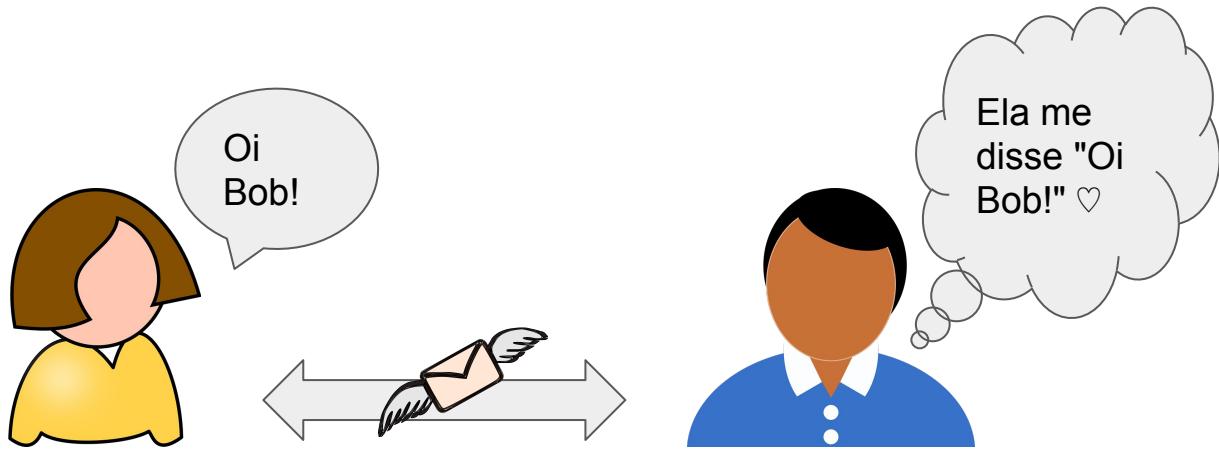
Bob



Mallory

Ameaças:
Interceptação
Interrupção
Modificação
Fabricação

Sigilo ou Confidencialidade



Alice



Eve

Sigilo ou Confidencialidade

iCloud Nude Leaks: 26 Celebrities Affected In The Nude Photo Scandal

BY AMANDA REMLING  ON 09/21/14 AT 1:19 PM



Ashley Madison Hackers Finally Released All the Stolen Data Online

Tuesday, August 18, 2015  Swati Khandelwal

 112  1.9k  3530  544  35  4860



Sigilo ou Confidencialidade

mercado

Hackers roubam dados de 29 mil clientes da corretora XP Investimentos

Joel Silva / Folhapress



Sigilo ou Confidencialidade

The screenshot shows a news article from the 'SAÚDE' section of the Portal Brasil website. The article is titled 'SUS: prontuário eletrônico beneficiará 15 milhões de pacientes'. It discusses the modernization of the healthcare system, mentioning that five thousand basic health units will adopt the new system, providing greater service agility. The article was published by Portal Brasil on September 2, 2015, at 00:00, and last modified on September 3, 2015, at 10:39. The page includes social sharing buttons for Facebook, Twitter, and Google+.

VOCÊ ESTÁ AQUI: PÁGINA INICIAL > SAÚDE > 2015 > 09 > SUS: PRONTUÁRIO ELETRÔNICO BENEFICIARÁ 15 MILHÕES DE PACIENTES

Últimas notícias

Portal Planalto
Blog do Planalto
Navegue por Estados

ASSUNTOS

Cidadania e Justiça
Ciência e Tecnologia
Cultura
Defesa e Segurança

SAÚDE

SUS: prontuário eletrônico beneficiará 15 milhões de pacientes

Modernização

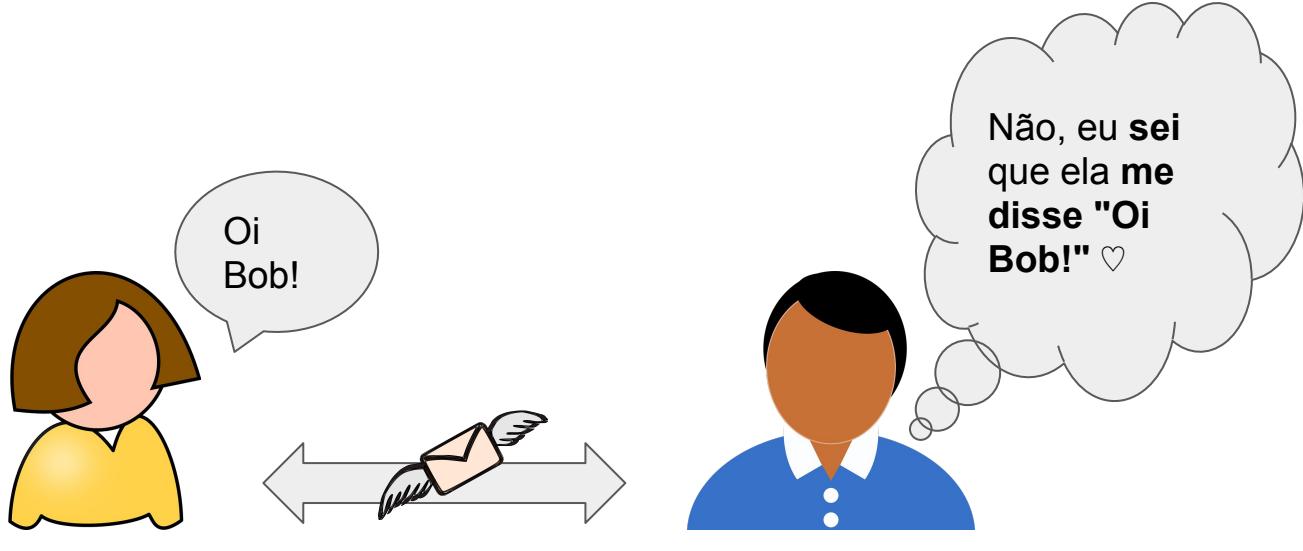
Cinco mil Unidades Básicas de Saúde vão aderir ao novo sistema, dando maior agilidade ao atendimento

por Portal Brasil
Publicado: 02/09/2015 00h00
Última modificação: 03/09/2015 10h39

Curtir 1,7 mil
Tweetar
G+ 3

- Resolução CFM No. 1.821/07
- Manual de Cert. para Sist. de Registro Eletrônico em Saúde (S-RES)
- Criptografar dados de identificação do paciente: recomendado (não mandatório)

Integridade



Integridade

Bloomberg

News

Quick

Markets

Personal Finance

Tech

U.S. Politics

Sustainability

Digital Health Records' Risks Emerge as Deaths Blamed on Systems

Save

By Jordan Robertson · Jun 25, 2013 6:01 PM GMT+0200 · 115 Comments

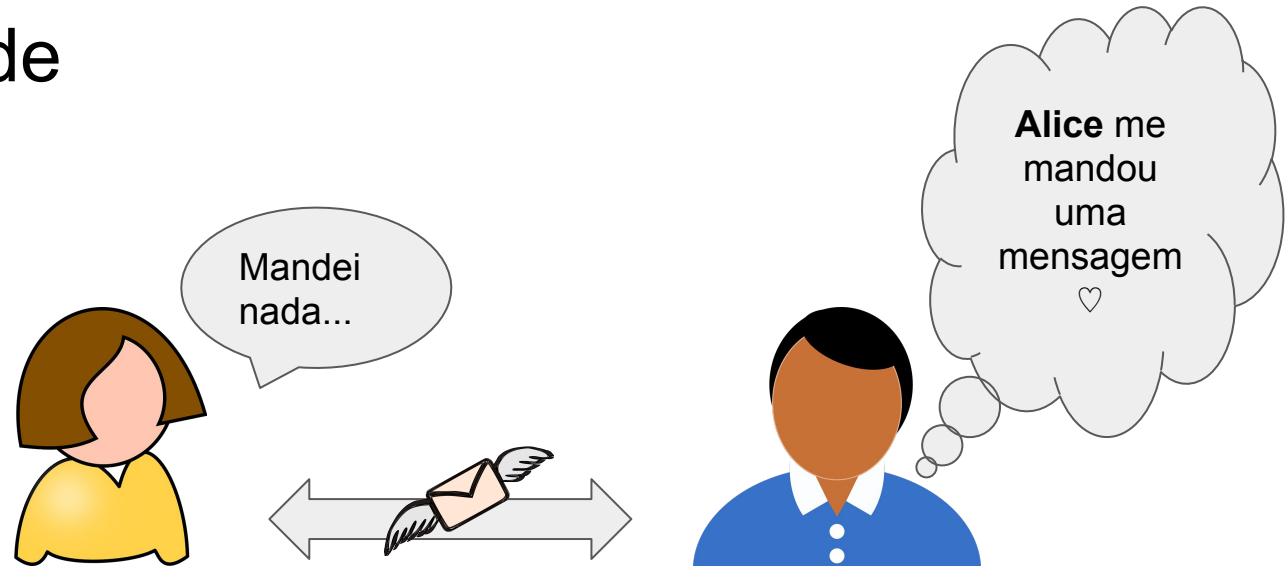
Email

Print

Integridade



Autenticidade



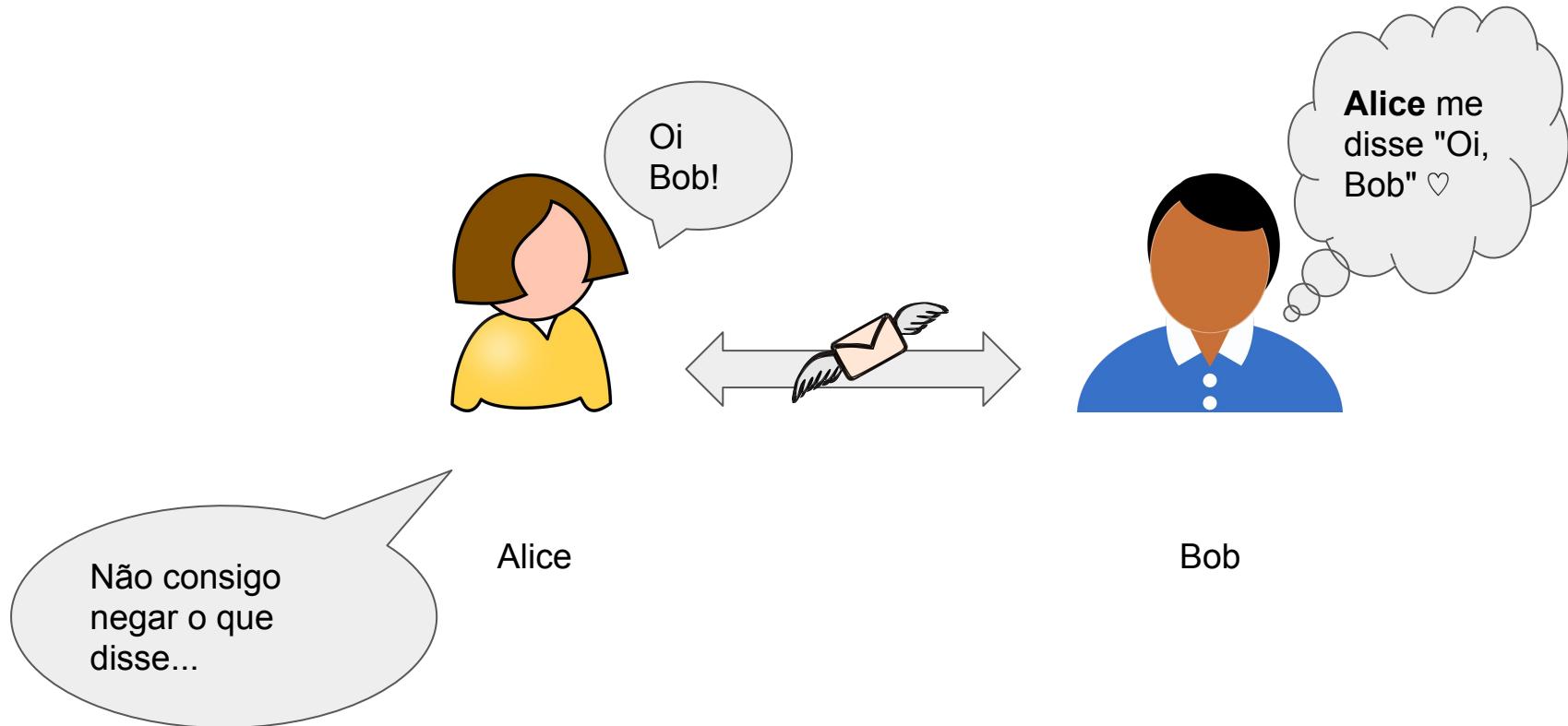
Alice

Bob

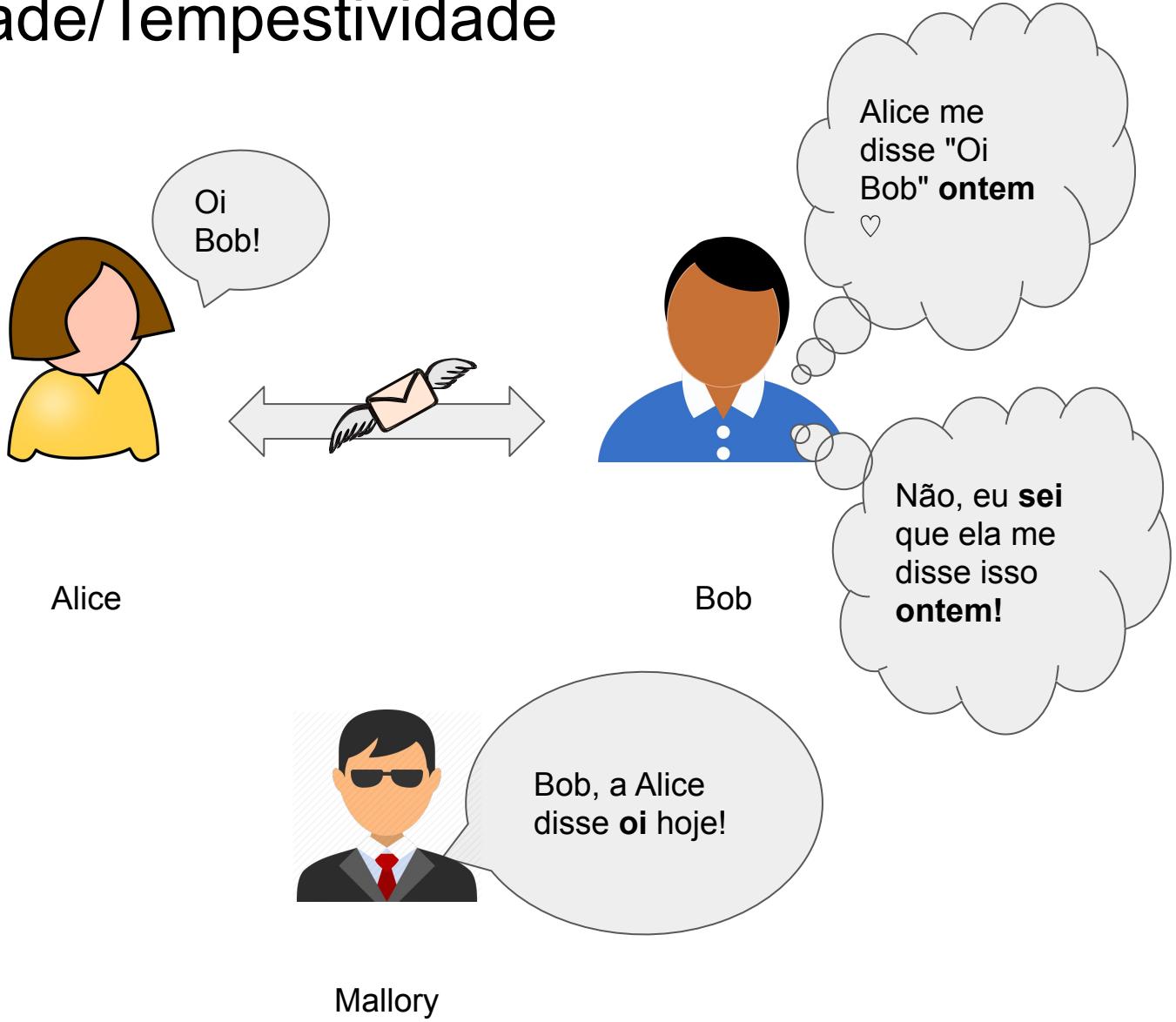


Mallory

Não repúdio



Irretroatividade/Tempestividade



Onde criptografia é comumente usada?

- Comunicação segura
 - Web (https - SSL/TLS), wireless (WPA, GSM, Bluetooth, etc.)
- Proteção de dados
 - EFS, TrueCrypt, BitLocker, etc.
- Proteção de conteúdo
 - DVD (CSS), Blu-ray (AACS)
- Autenticação

Comunicação Segura

Consiste em:

- Acordo de chave: Estabelecer uma chave secreta compartilhada
- Transporte: Transmitir dados usando a chave secreta com garantia de integridade e confidencialidade

Exemplo: SSL/TLS - Protocolo amplamente utilizado para confidencialidade e autenticação de comunicações

Princípios básicos de criptografia

- Problema matemático/computacional difícil
- Modelo de ameaça claro
- Não é a solução para tudo
- Se usar errado, não adianta **nada!**



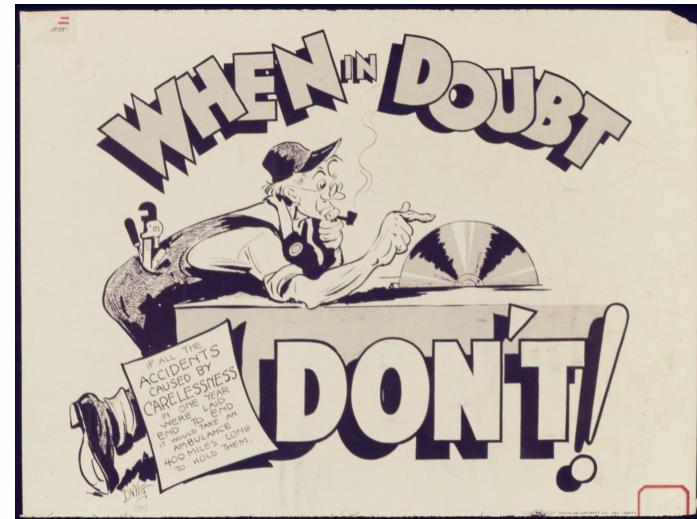
A lição mais importante...

Não implemente seu próprio algoritmo ou protocolo!

Use os amplamente difundidos e avaliados publicamente!

Use cada algoritmo e protocolo apenas para aquilo que eles foram desenvolvidos!

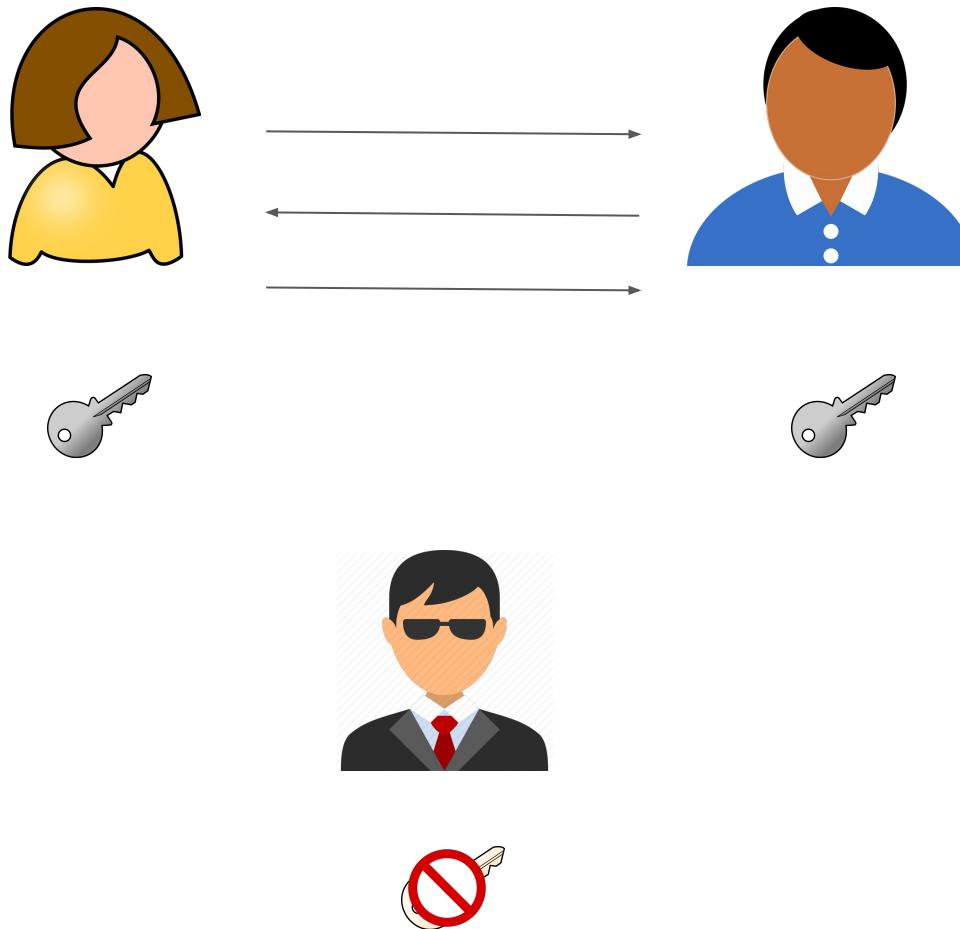
A única coisa secreta é chamada de *chave*!



Aplicações de criptografia

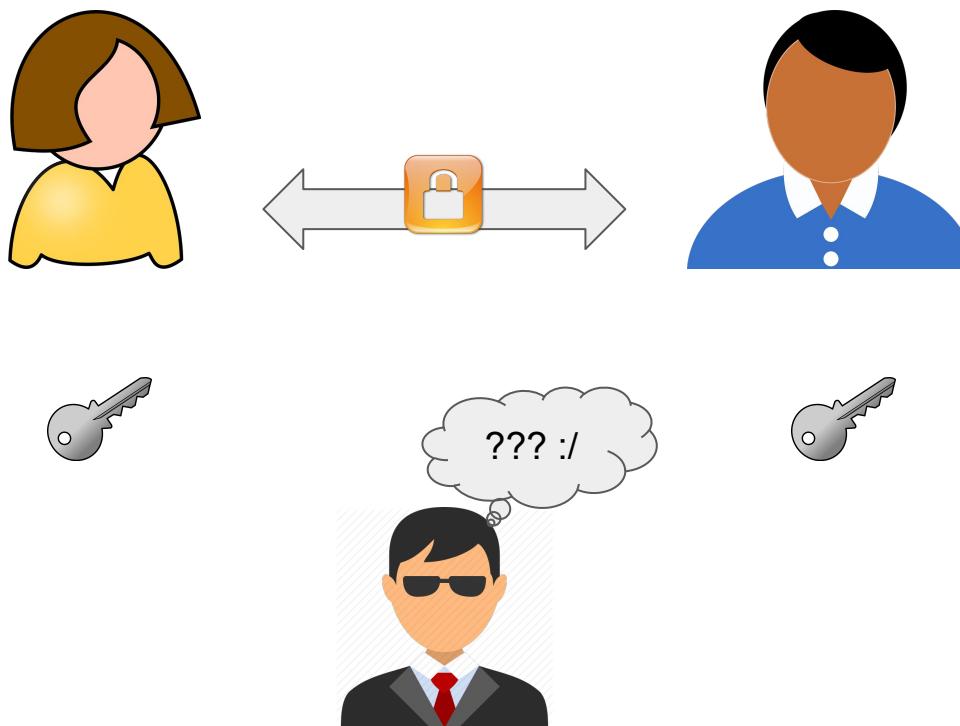
Core: Comunicação Segura

Acordo de chaves



Core: Comunicação segura

Transporte



Com integridade, autenticidade, confidencialidade

Assinatura Digital

No papel eu faço a *mesma* assinatura em todos documentos.

A handwritten signature in black ink, appearing identical across four instances.

A handwritten signature in black ink, appearing identical across four instances.

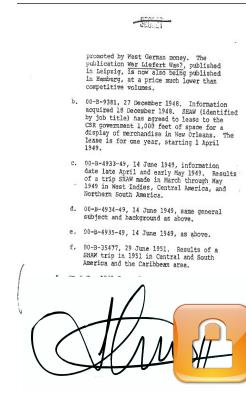
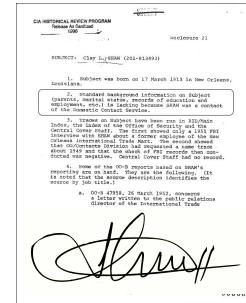
A handwritten signature in black ink, appearing identical across four instances.

A handwritten signature in black ink, appearing identical across four instances.

Como traduzir isso para o mundo digital, onde bits podem ser copiados?

Faça a assinatura ser uma função que tem como entrada o documento assinado

Documento diferente, assinatura diferente:



produced by West German agency. The publication was transferred to published in Leipzig. It is now also held in published in London, and is sold in much lower than competitive volumes.

b. 00-9-9381, 27 December 1948. Information dated 27 December 1948. SWU Identified by Job title has agreed to supply the CIC government 1,000 feet of space for a data processing center. The contract will last for one year, starting 1 April 1949.

c. 00-9-933-49, 14 June 1948. Information date late April and early May 1948. Results - 1948 in West Indies, Central America, and Northern South America.

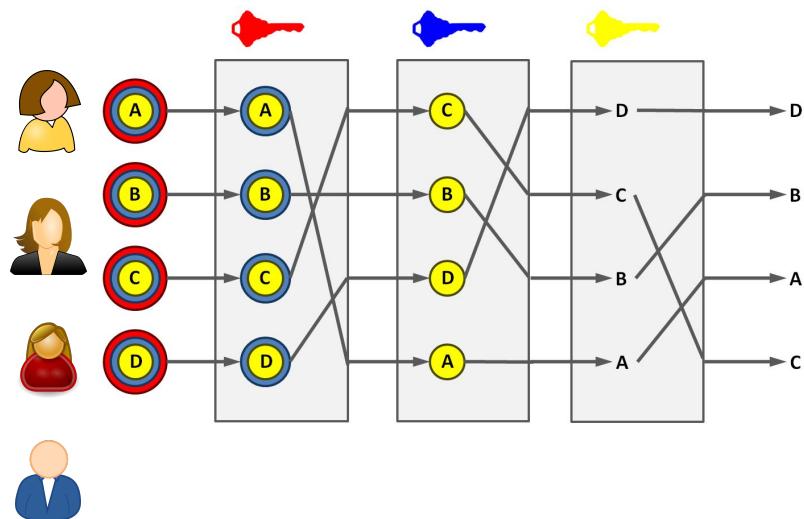
d. 00-9-933-49, 14 June 1948, same general subject and background as above.

e. 00-9-933-49, 14 June 1948, as above.

f. 00-9-933-49, 29 June 1948. Details of a survey trip in 1941 in Central and South America and the Caribbean area.

Comunicações anônimas

Mix-net



Dinheiro virtual anônimo

Suponha que Alice tenha um real virtual e queira gastá-lo através de um protocolo anônimo.

Como evitar que dinheiro virtual anônimo seja re-usado?

Aparentemente há um conflito entre anonimidade e o reuso.

Mas é possível resolver com criptografia!



Eleições

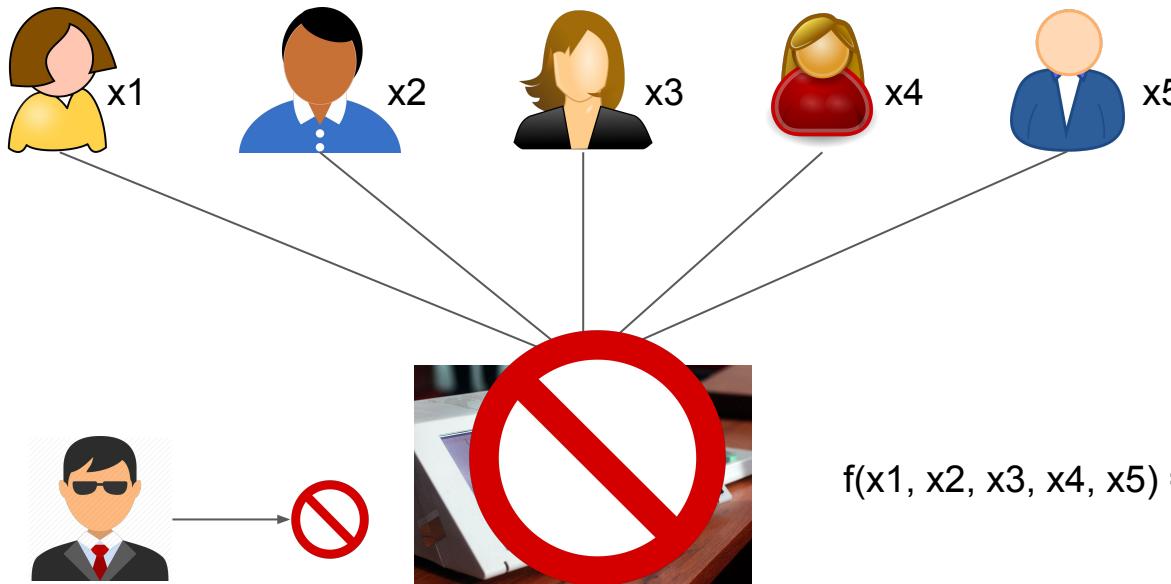
Problema: Como contar o total de votos em cada opção, sem que:

- os votos individuais sejam revelados
- os votos sejam manipulados
- pessoas não autorizadas votem, ou votantes votem mais de uma vez

Problema análogo: leilão/pregão

- objetivo é descobrir maior/menor lance sem revelar nada sobre os outros lances;

Eleições

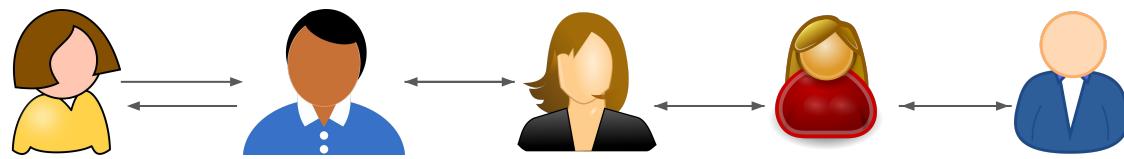
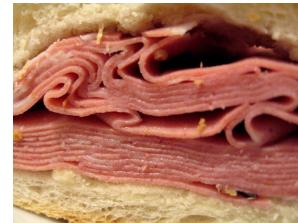


Computação multiparty segura

Teorema: O que pode ser feito com uma autoridade confiável também pode ser feito sem ela.

Como? Protocolo criptográfico onde as partes falam entre si e ao final chegam a um resultado homologado por todos - sem revelar seus segredos.

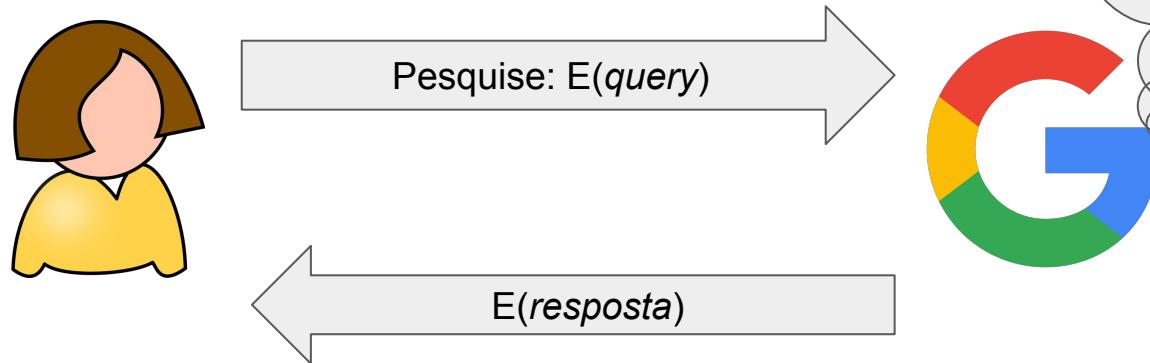
Eleições



$$f(x_1, x_2, x_3, x_4, x_5) = ???$$

“Mágicas criptográficas”

Computação em nuvem sem revelar o conteúdo



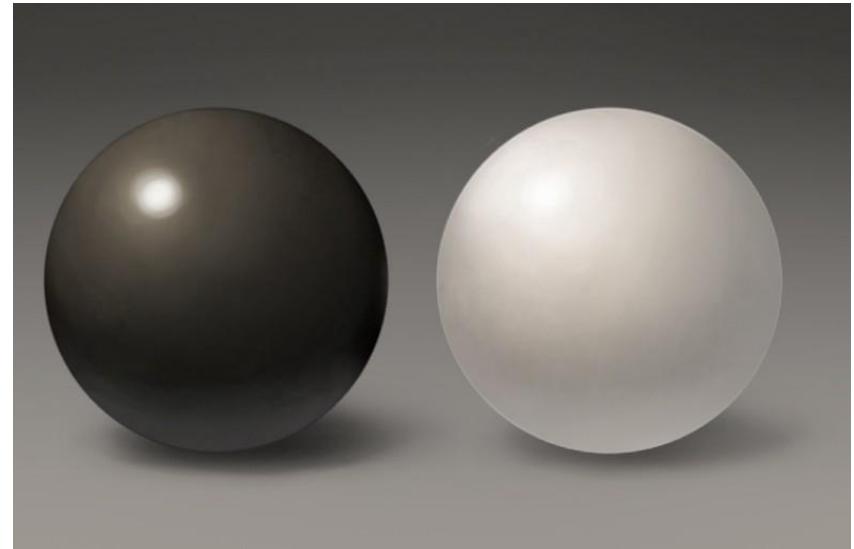
E agora, como
vou exibir
propagandas sem
saber o que Alice
buscou? :(

Possível? SIM!

Mas ainda apenas para aplicações extremamente mais simples!

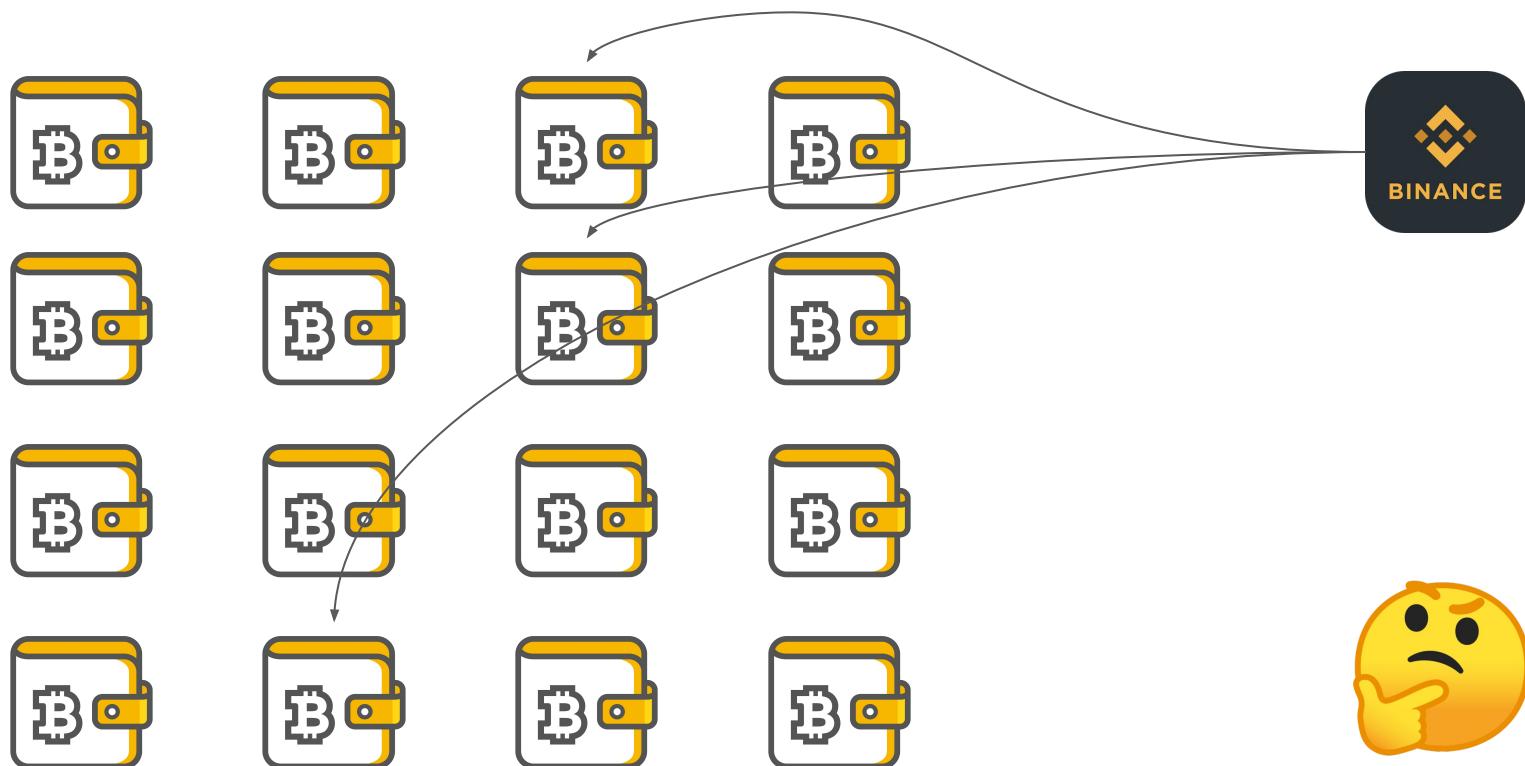
Zero knowledge Proofs

Provar a alguém que você conhece a solução de um problema, sem revelá-la



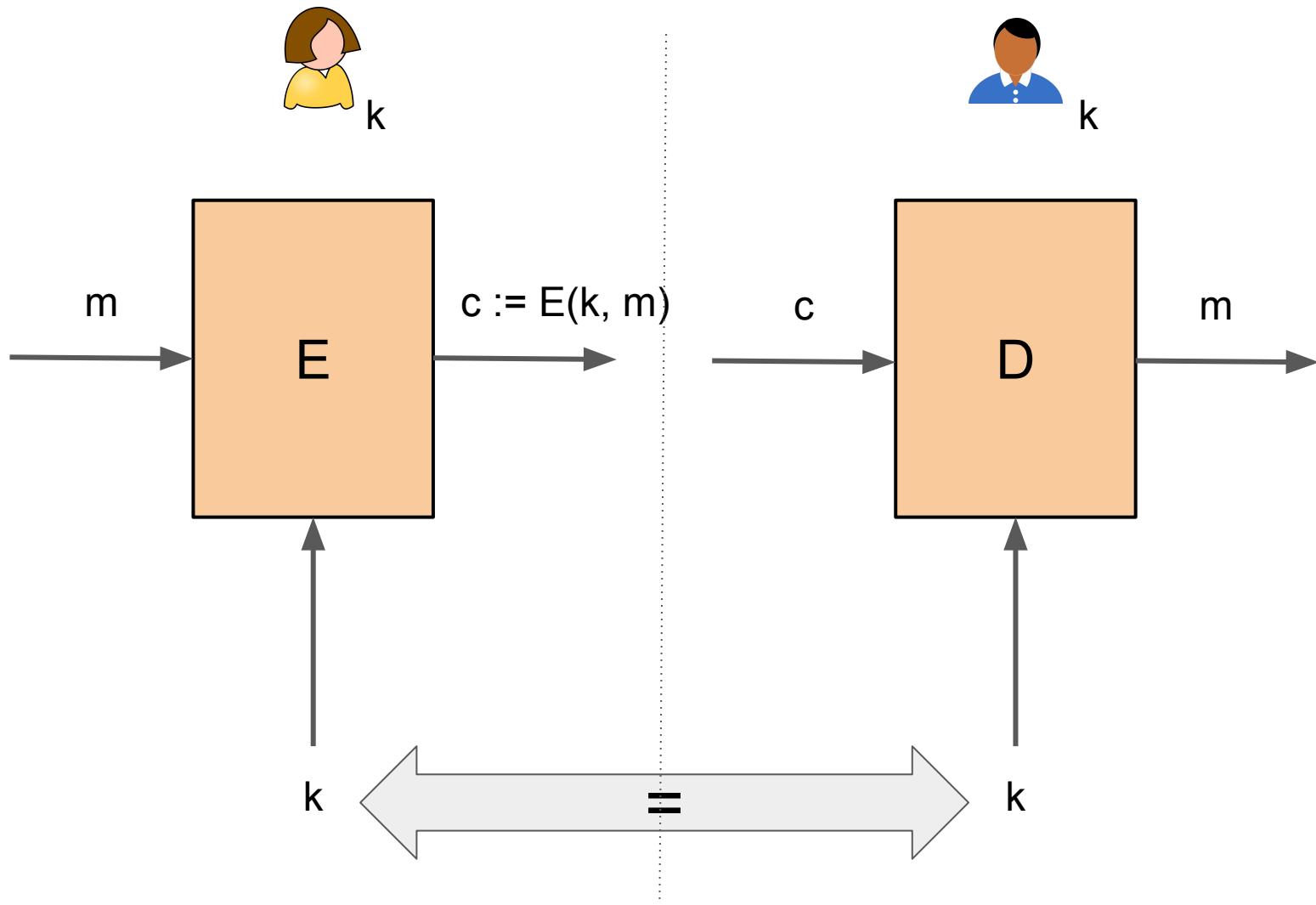
Zero knowledge Proofs

Provar que você tem $n > 0$ bitcoins em suas carteiras sem revelá-las



Cifradores simétricos (como garantir sigilo)

Cifragem simétrica: notação

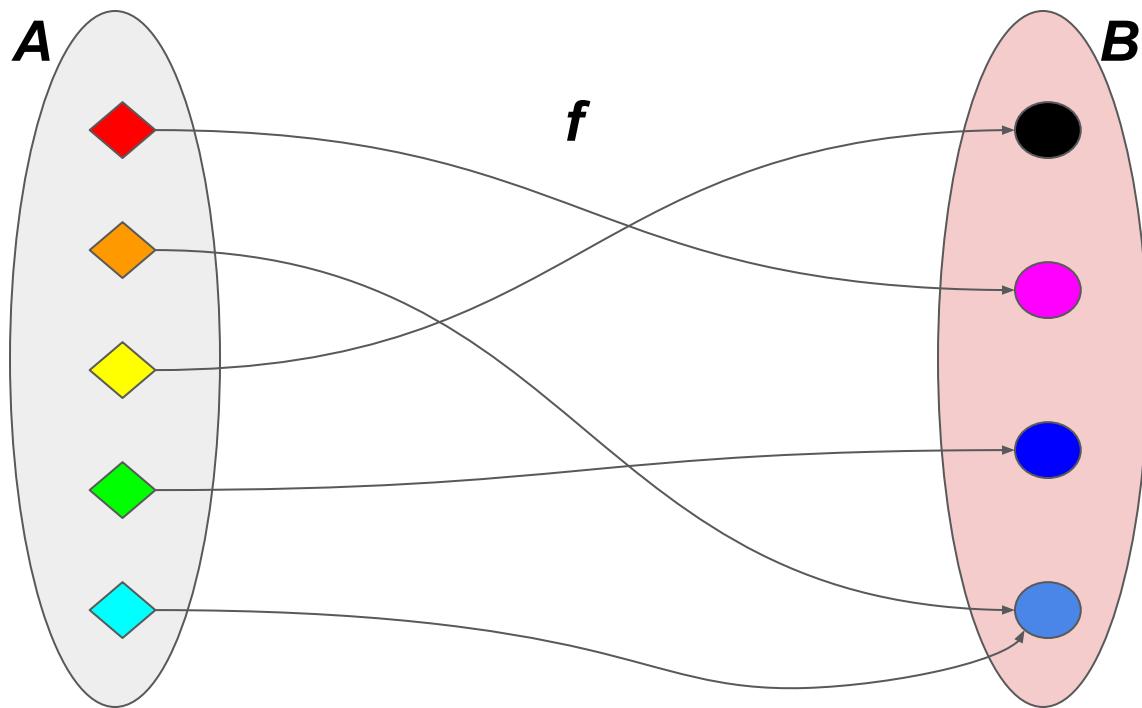


Algoritmos de cifragem simétrica

- Data Encryption Standard (DES)
 - Chaves de 56 bits (+8 de paridade)
 - Hoje inseguro
- Advanced Encryption Standard (padronizado pelo NIST)
 - Chaves de 128, 192 e 256 bits

Funções Hash (Resumo Criptográfico)

Como garantir integridade

$f : A \rightarrow B$ 

Exemplo

- $A = \text{conjuntos dos CPFs}$
- $B = \text{conjuntos dos nomes dos contribuintes}$

$$f : A \rightarrow B$$

Exemplo

- $A, B = \text{conjuntos dos números inteiros}$
- $f(x) = 2x$, onde $x \in A$ e $f(x) \in B$

$$f : A \rightarrow B$$

Não é exemplo

- A = conjunto dos nomes dos contribuintes
- B = conjunto dos CPFs

João da Silva -> 034.234.678-90

João da Silva -> 234.680.224.71

$$f : A \xrightarrow{\text{NOT}} B$$

Uma função de hash H

- A = conjunto de todas as sequências de bits (infinitos elementos)
- B = conjunto de todas as sequências de $n > 0$ bits (2^n elementos)

$$H : A \rightarrow B$$

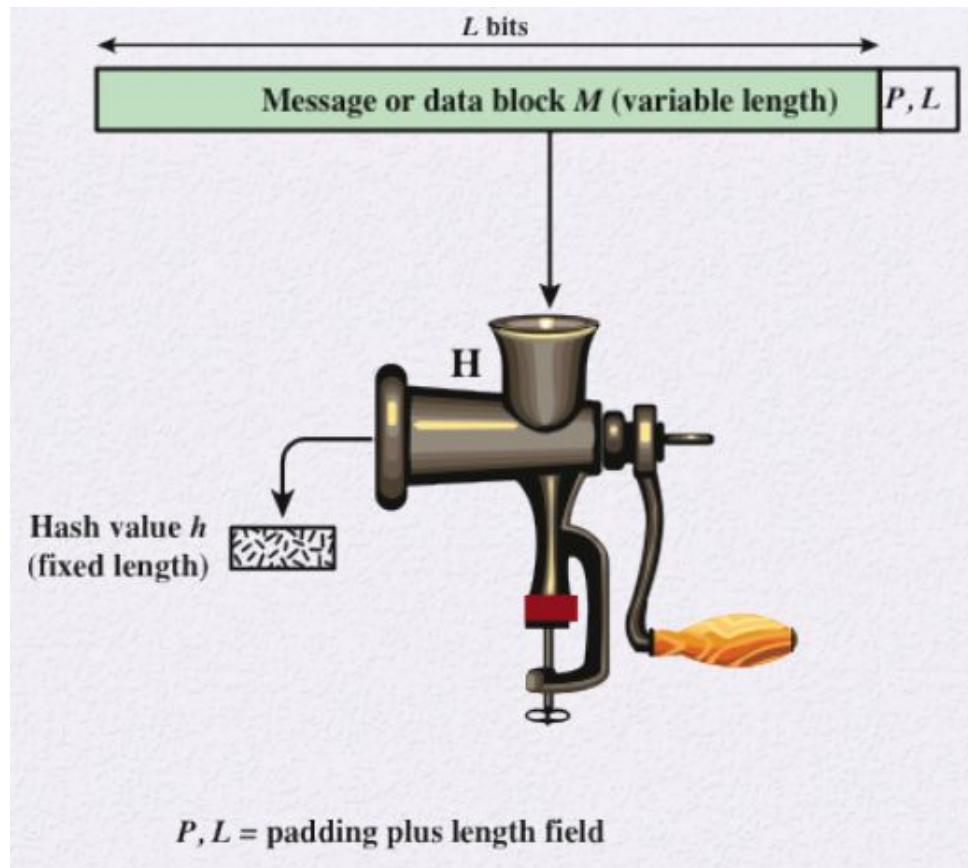
Exemplo: função de hash SHA256

- A = conjunto de todas as sequências de bits (infinitos elementos)
- B = conjunto de todas as sequências de 256 bits (2^{256} elementos)



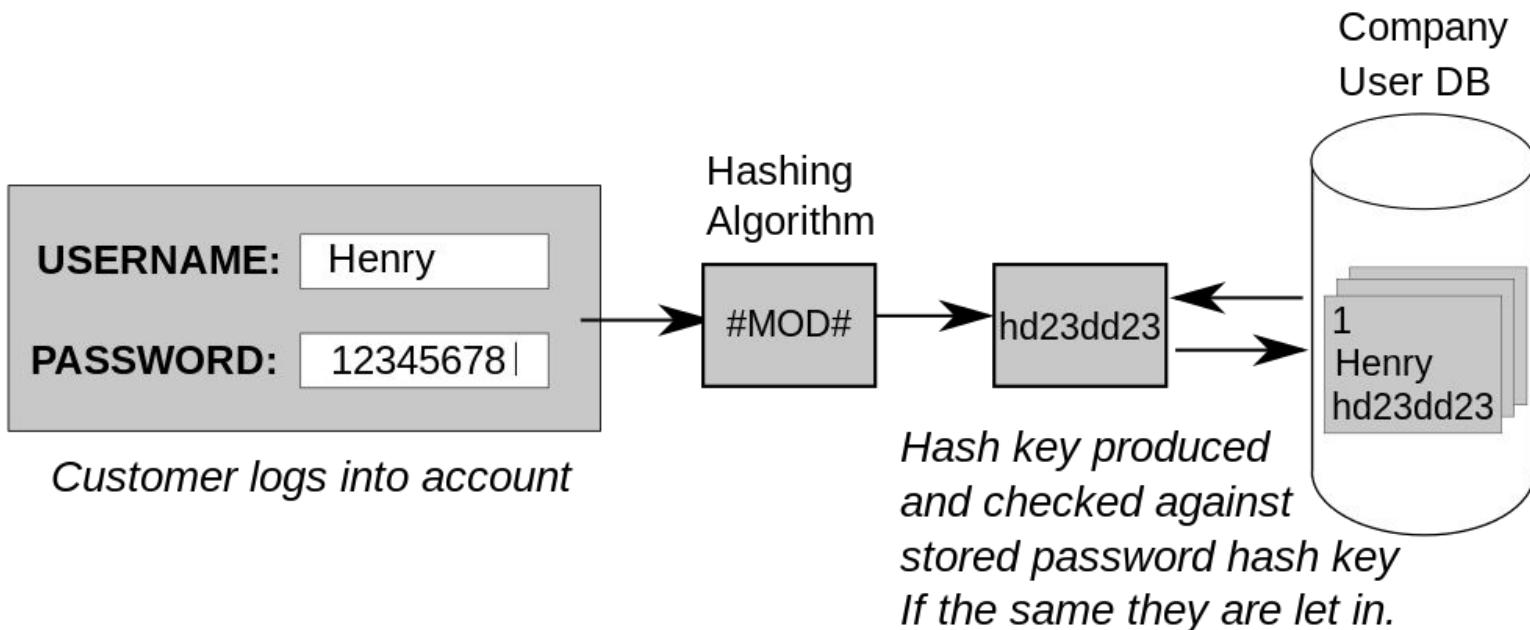
Hash = 0a 04 e5 71 2a c8 e3 dc 1c f0 f9 26 57 57 f1 ab 28 ca f9 42

Função de hash produz um "resumo" ou "impressão digital" do dado de entrada



Uma função H de hash ou resumo criptográfico

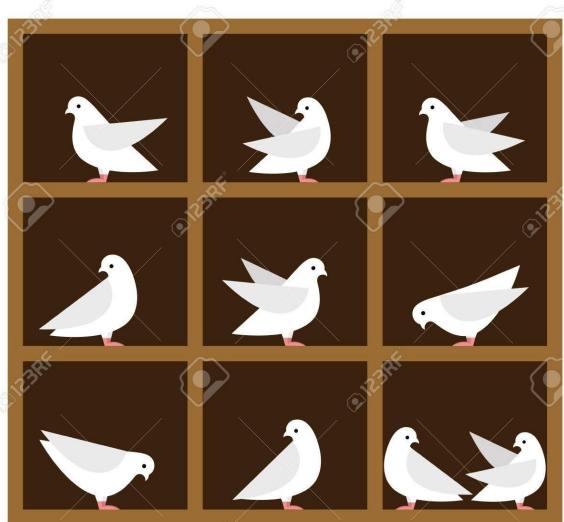
- Resistência a pré-imagem: dado $H(x)$, é *muito difícil* descobrir x



A contém mais elementos que B

- A = conjunto de todas as sequências de bits (infinitos elementos)
- B = conjunto de todas as sequências de bits de tamanho $n > 0$ (2^n elementos)

$$H : A \rightarrow B$$



Uma função H de hash ou resumo criptográfico

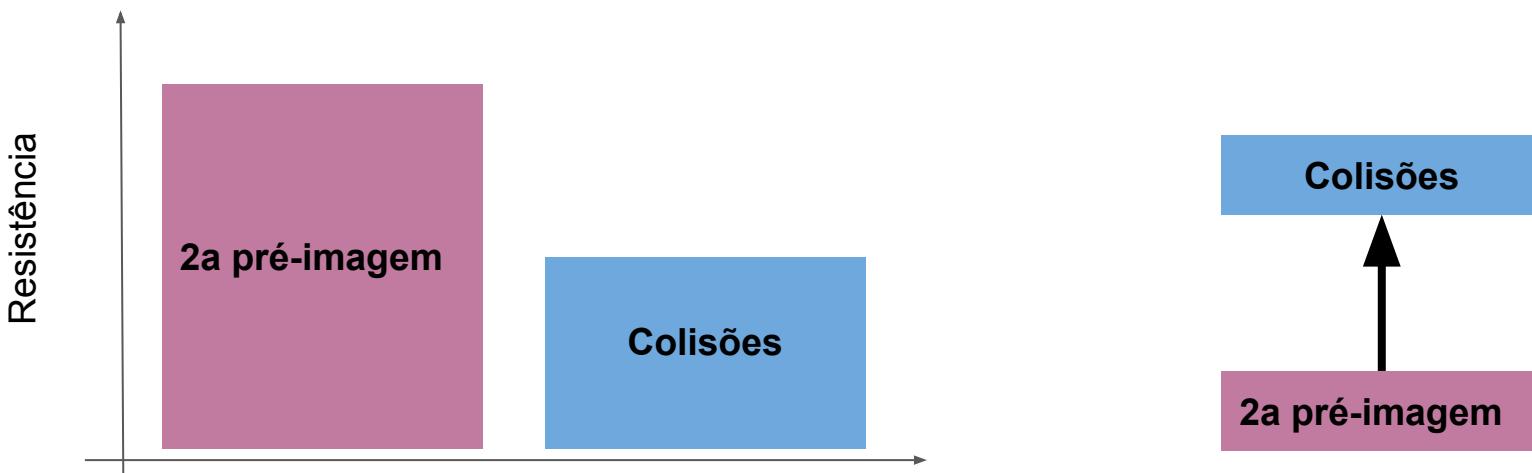
- Resistência a pré-imagem: dado $H(x)$ é *muito difícil* descobrir x
- Resistência a 2^a pré-imagem: dados x e $H(x)$ é *muito difícil* descobrir $y \neq x$ tal que $H(x)=H(y)$
- Resistência a colisões: é *muito difícil* encontrar quaisquer $x \neq y$ tal que $H(x)=H(y)$



Uma função H de hash ou resumo criptográfico

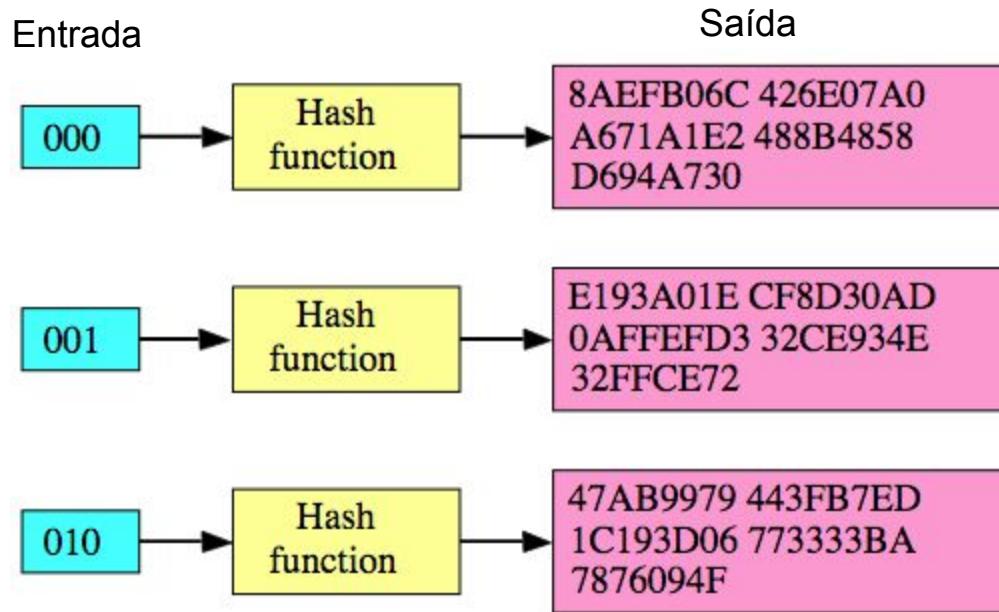
- Resistência a 2^a pré-imagem: dados x e H(x) é *muito difícil* descobrir y≠x tal que H(x)=H(y)
- Resistência a colisões: é *muito difícil* encontrar **qualsquer** x≠y tal que H(x)=H(y)

Resistência a colisão implica resistência a 2^a pré-imagem

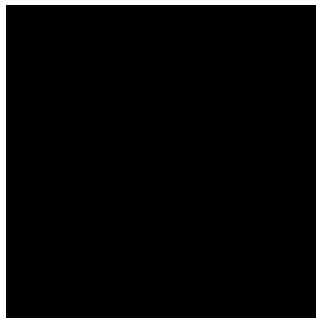


Uma função H de hash ou resumo criptográfico

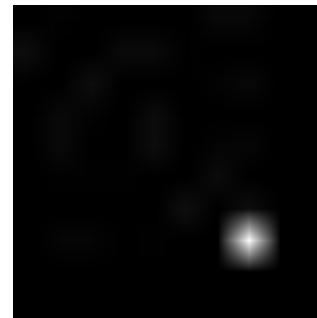
- Resistência a pré-imagem: dado $H(x)$ é *muito difícil* descobrir x
- Resistência a 2^a pré-imagem: dados x e $H(x)$ é *muito difícil* descobrir $y \neq x$ tal que $H(x) = H(y)$
- Resistência a colisão: É *muito difícil* encontrar quaisquer $x \neq y$ tal que $H(x) = H(y)$
- Efeito avalanche: geralmente, mesmo que x seja parecido com y , $H(x)$ difere muito de $H(y)$



Comparando arquivos de imagem de 10x10 pixels



Antes



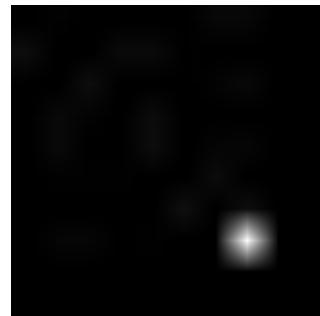
Depois

9362cbcfc6b5cf7fc25129162582a1b040de1e15d

41238f83b360914dbcca4ae973bf59ad874e6473

Comparando arquivos de imagem de 10x10 pixels

Antes



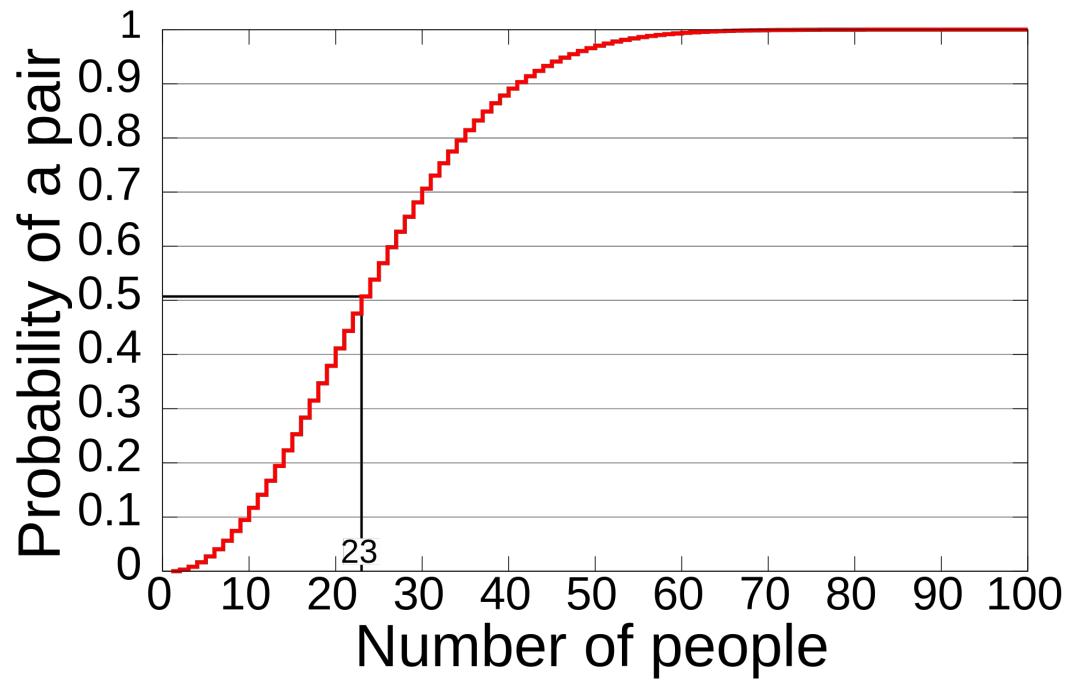
Depois

9362cbcfc6b5cf7fc25129162582a1b040de1e15d

41238f83b360914dbcca4ae973bf59ad874e6473

Problemas das funções de hash criptográfico

"Paradoxo" do aniversário



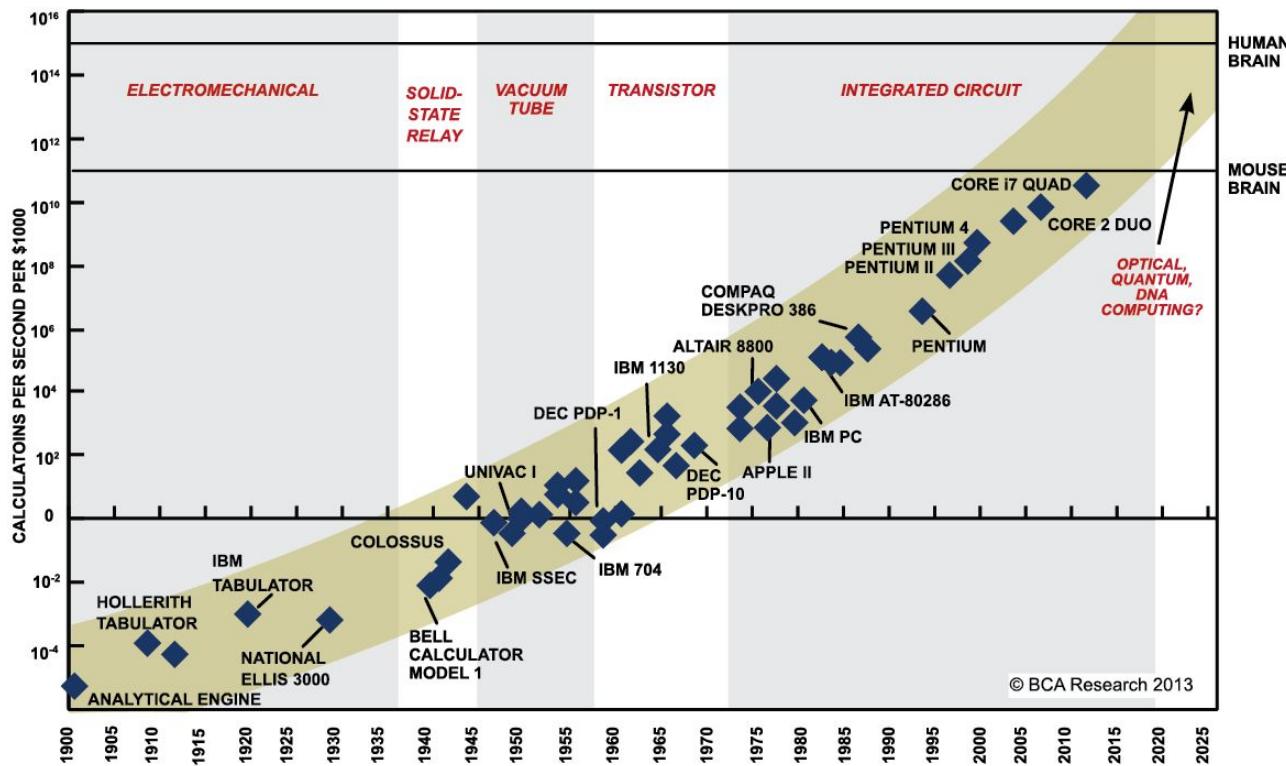
Ataque de colisão

- $|m|$ variável, $|H(\cdot)|$ fixo \rightarrow se $|m| > |H(\cdot)|$, então há colisão!
- Deve ser difícil encontrar x e y quaisquer tal que $H(x) = H(y)$
- Resistência a colisão não significa que não existem colisões
- *Paradoxo do aniversário*: necessário calcular $2^{n/2}$ mensagens para encontrar colisão
- Ataque: achar colisão < paradoxo do aniversário

É muito difícil encontrar colisão... difícil quanto?

- Estimativa (paradoxo do aniversário): $2^{n/2}$ tentativas
- Tentativas de colisão para SHA256 : $2^{256/2} = 3.4028237e+38$
- CPU 2,7 GHz Intel Core i7: 18 SHA256 por segundo
- Tempo para encontrar colisão: $5.9946017e+29$ anos

É preciso considerar projeções de...

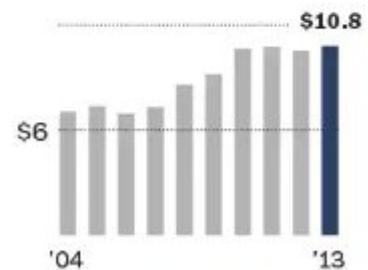


Poder computacional



National Security Agency

Protect the government's information systems and intercept foreign signals intelligence information.



Orçamento institucional

Funções de hash não são seguras para sempre



253dd04e87492e4fc3471de5e776bc3d

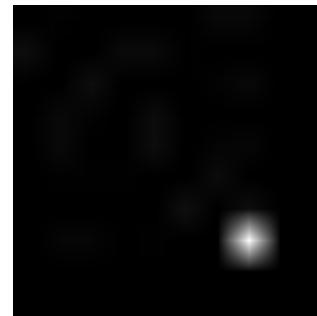
253dd04e87492e4fc3471de5e776bc3d

Adotar novas e seguras funções

O hash calculado é autêntico?

Antes

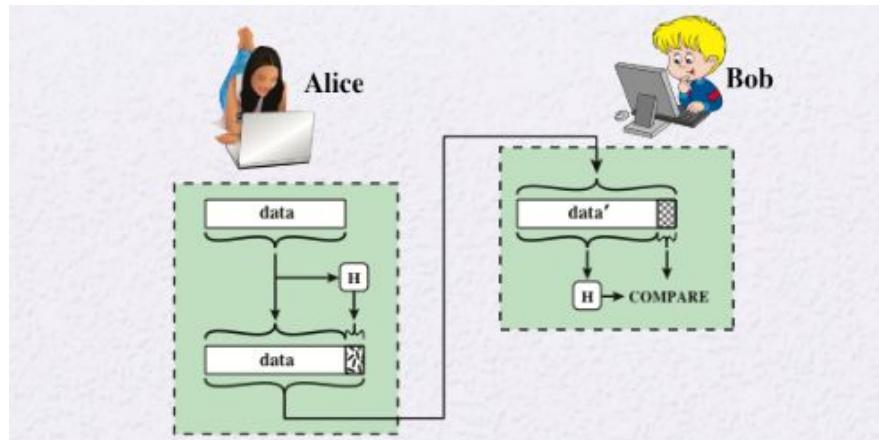
9362cbcf6b5cf7fc25129162582a1b040de1e15d



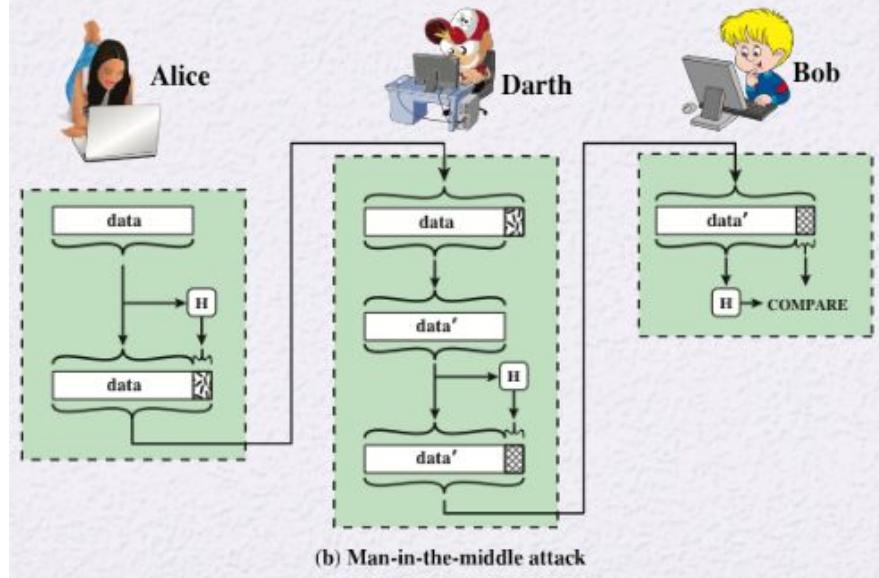
Depois

41238f83b360914dbcca4ae973bf59ad874e6473

O hash calculado é autêntico?



(a) Use of hash function to check data integrity



(b) Man-in-the-middle attack

PRNG

Geradores de Números Pseudo-Aleatórios

- Utilizados para:
 - Geração de chaves
 - Geração de parâmetros
 - Controle de sessão (*nonce*)
- Aleatoriedade
 - Distribuição uniforme → fácil
 - Independência → difícil

Como assim, “pseudo”?

- Não pode surgir aleatoriedade de um sistema determinístico (computador comum)
- É possível "ler" fenômenos que sejam aleatórios - mas custa tempo para acumulá-los em quantidade suficiente
- PRNGs tem como entrada *sementes* e produzem um resultado que tenha características estatísticas aleatórias, apesar de determinístico
 - Executar um PRNG com a mesma semente (*seed*) gera o mesmo número aleatório!
- Semente deve ser obtida de fontes aleatórias
 - Conjunto de dados de sensores
 - Movimento do mouse
 - Etc.

```
int getRandomNumber()
{
    return 4; // chosen by fair dice roll.
              // guaranteed to be random.
}
```

Entropia

Medida de desordem e randomicidade em um sistema

Calcanhar de aquiles de muitas implementações

*nix: /dev/random x /dev/urandom

Casos famosos...

Debian 2008: Código comentado removeu entropia do seed

Java 2013: Nonce fraco no SecureRandom

Playstation 2010: Nonce repetido permitiu roubo de chave da Sony

NIST 2013: Backdoor no PRNG pela NSA



O caso da urna brasileira

Uso do horário da zerésima como *seed* do PRNG que embaralha os votos da urna.



Um horário, além de ser um péssimo *seed*, é informação pública e impressa em relatório da urna!

Teste TSE 2012 - Prof. Diego Aranha - Registro Digital de Voto

Teste TSE 2014 - Mídia de Ajuste de Hora (ADH) também tinha falha de *seed* fraco para PRNG

Criptografia assimétrica

Como garantir autenticidade

Assinatura de próprio punho



Apenas você consegue
criar assinaturas
(muito difícil de forjar)

 **CARTÓRIO DINIZ**
REGISTRO DE FIRMAS

NOME: EVALDO PINTO
Nacionalidade: BRASILEIRO Estado Civil: SOLTEIRO
Profissão: ADVOGADO Fone:
Residência: AV. PRESIDENTE VARGAS, 2623 - CASTANHAL

Assinatura: 
Documento Identidade: 2816 - OAB - PA,
CPF N°: 234.584.299-72.

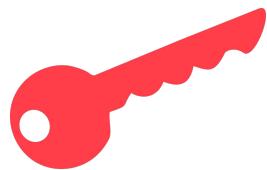

Belém 29/06/2011

Vide Verso

Todos podem verificar
suas assinaturas

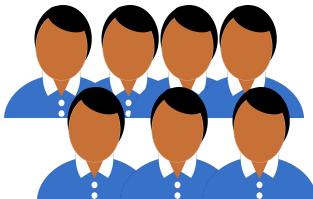
Esquema de criptografia assimétrica

Chave privada



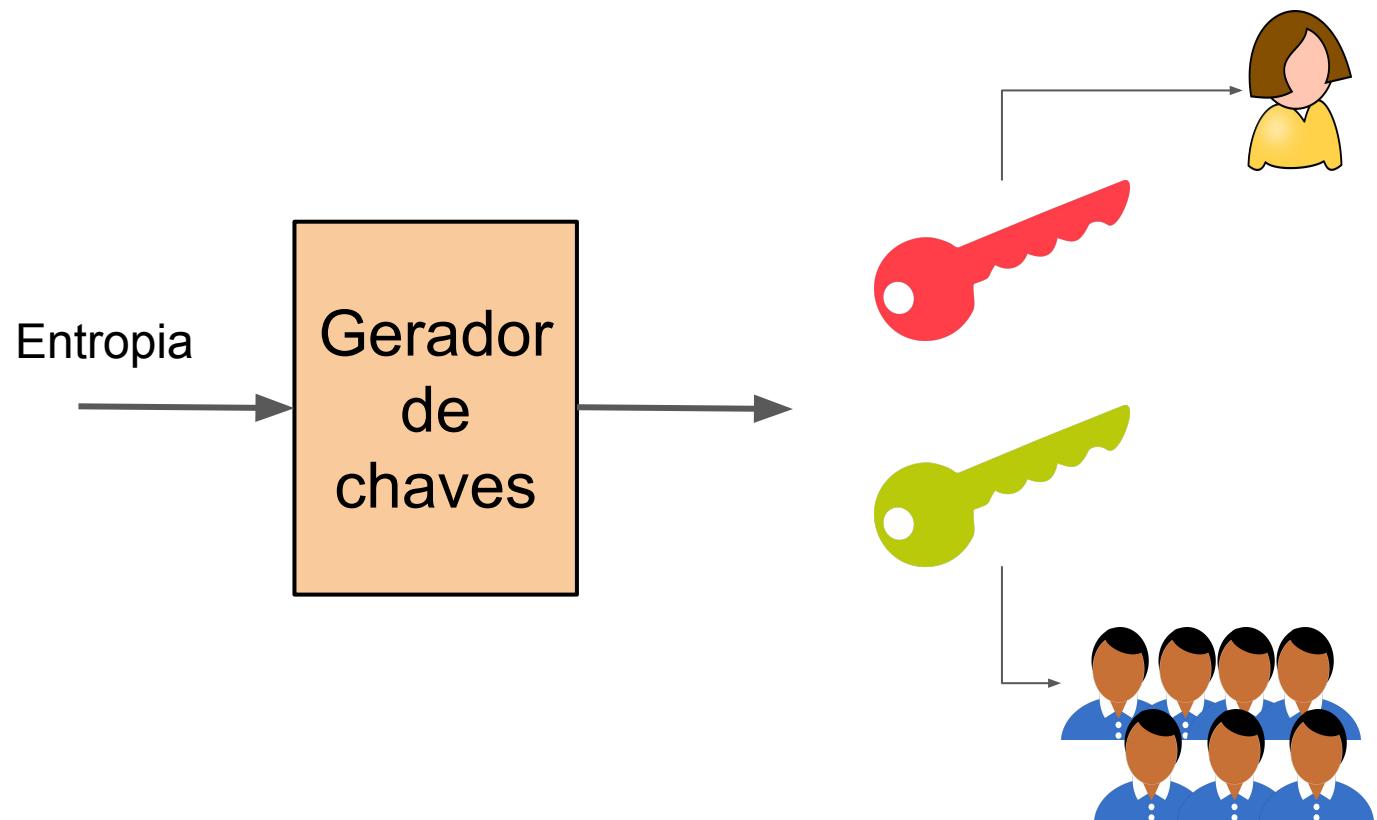
Apenas você sabe a chave
para criar assinaturas
(muito difícil de forjar)

Chave pública

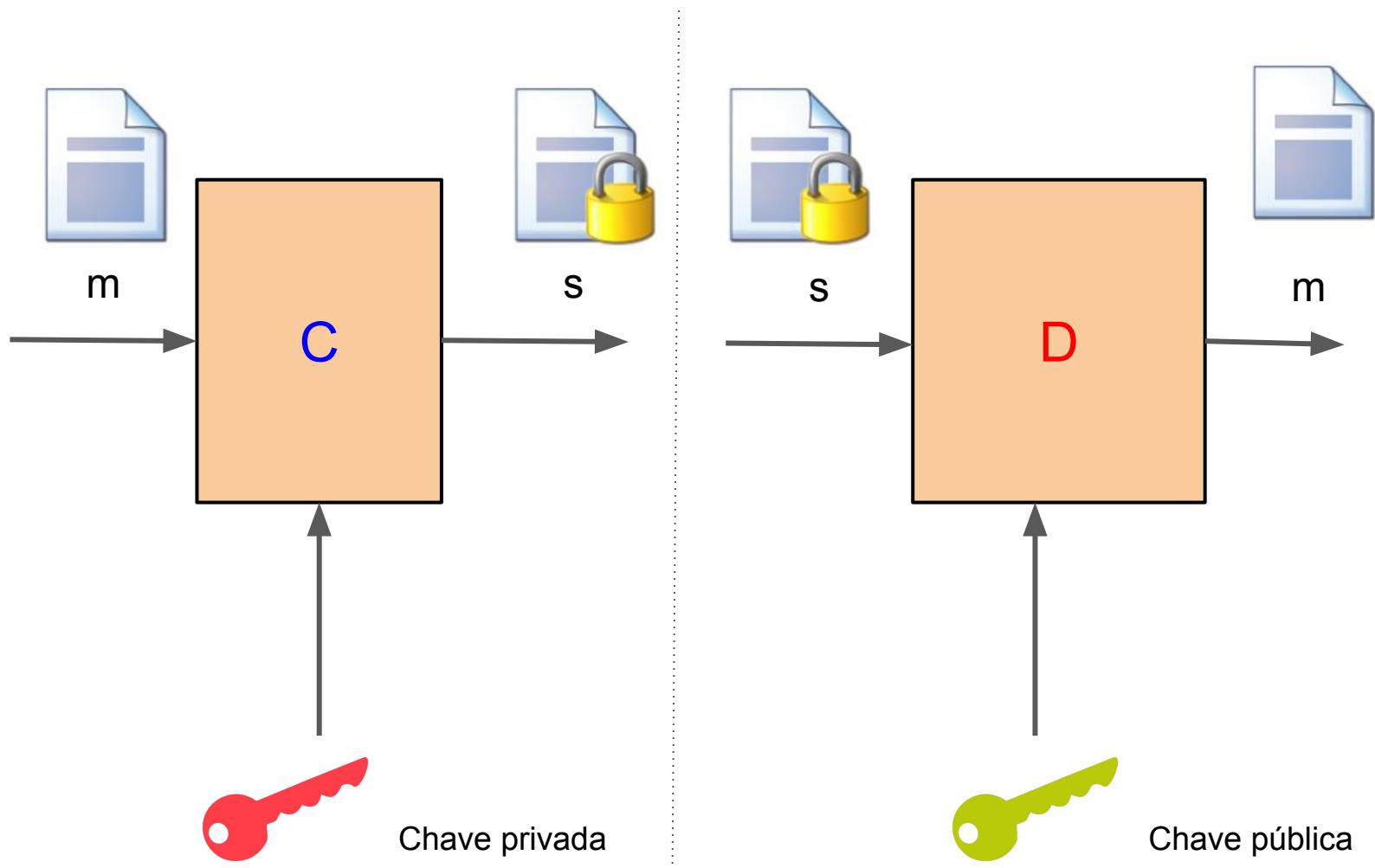


Todos podem usá-la para
verificar suas assinaturas

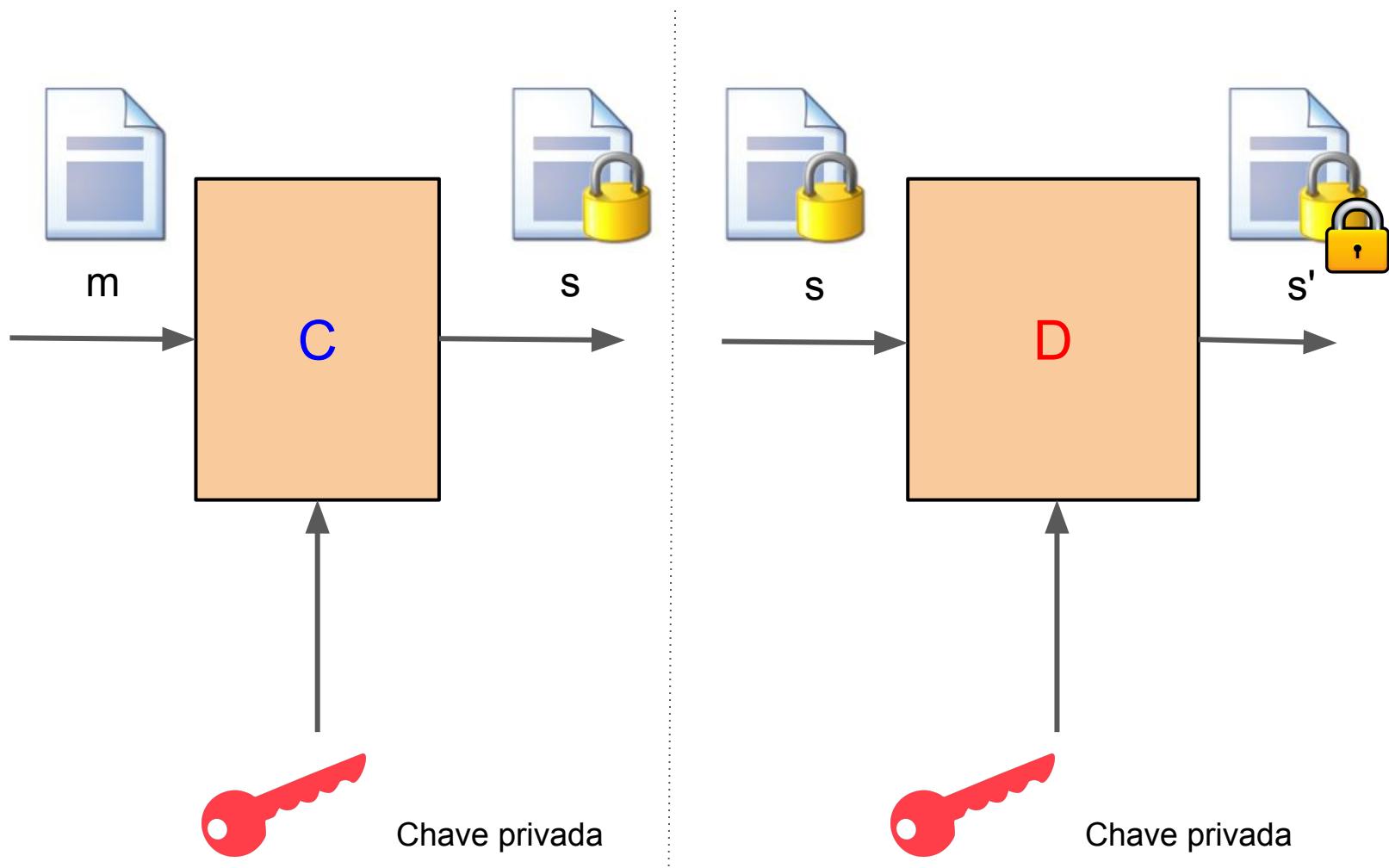
Esquema de cript. assimétrica: gerador de chaves



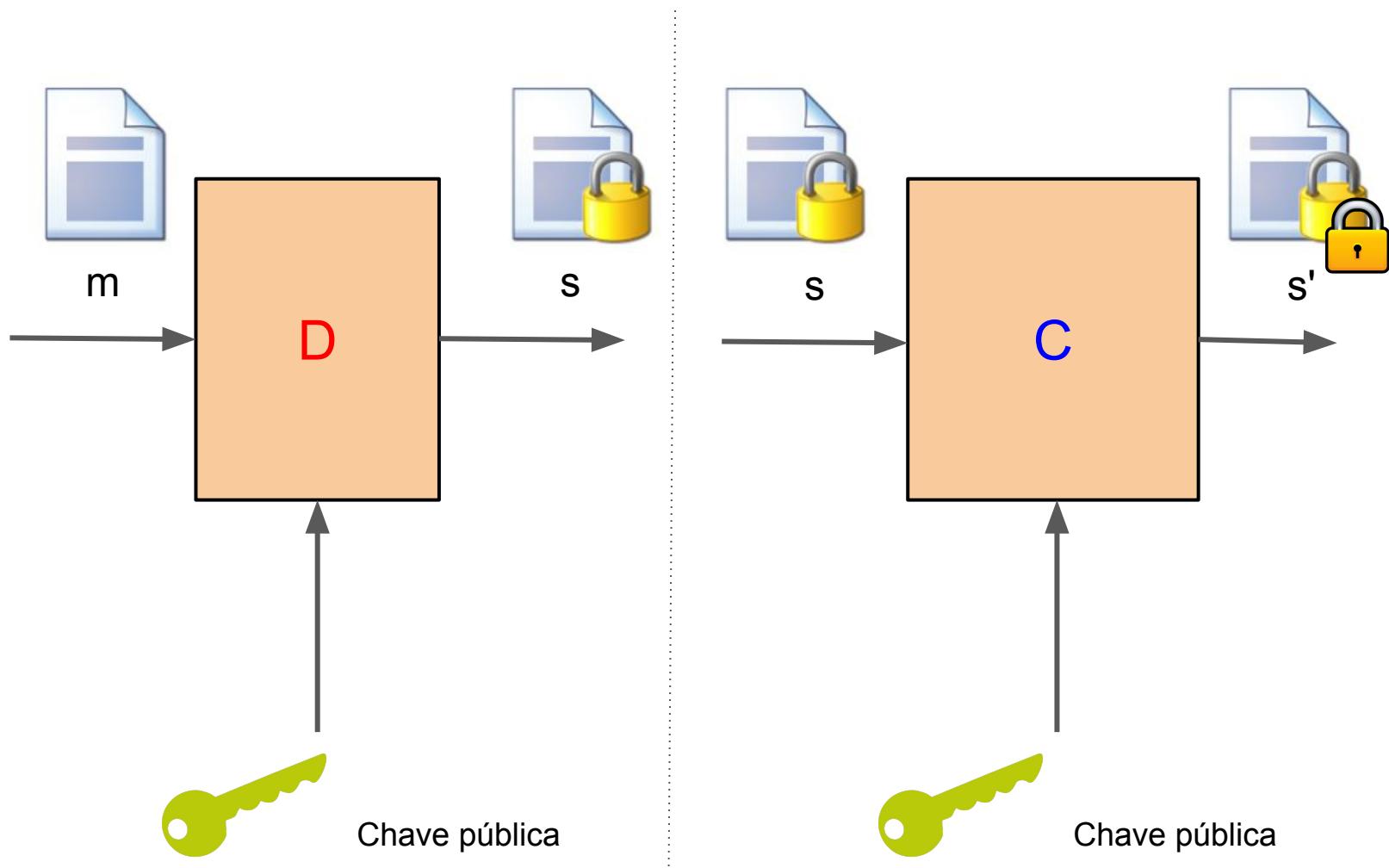
Esquema de cript. assimétrica: **cifrador** e **decifrador**



A mesma chave que cifra não decifra

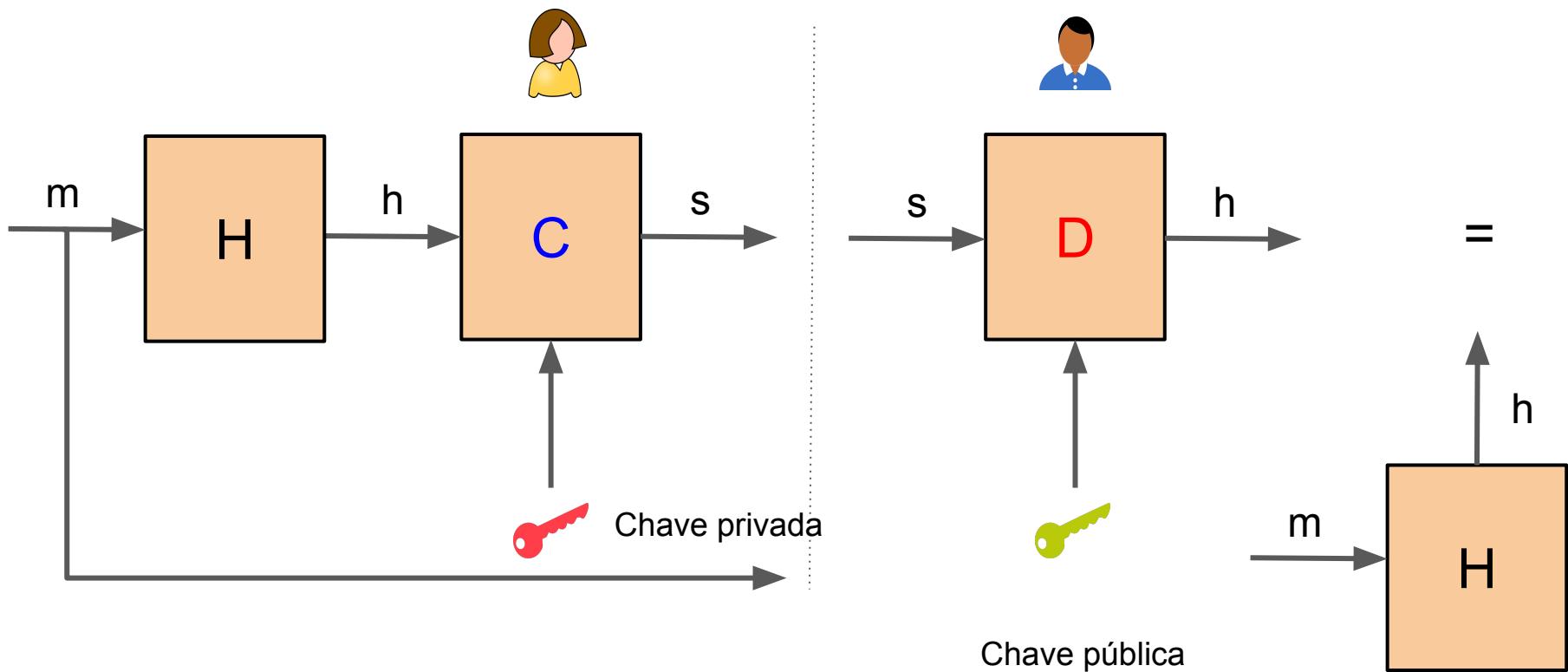


A mesma chave que cifra não decifra



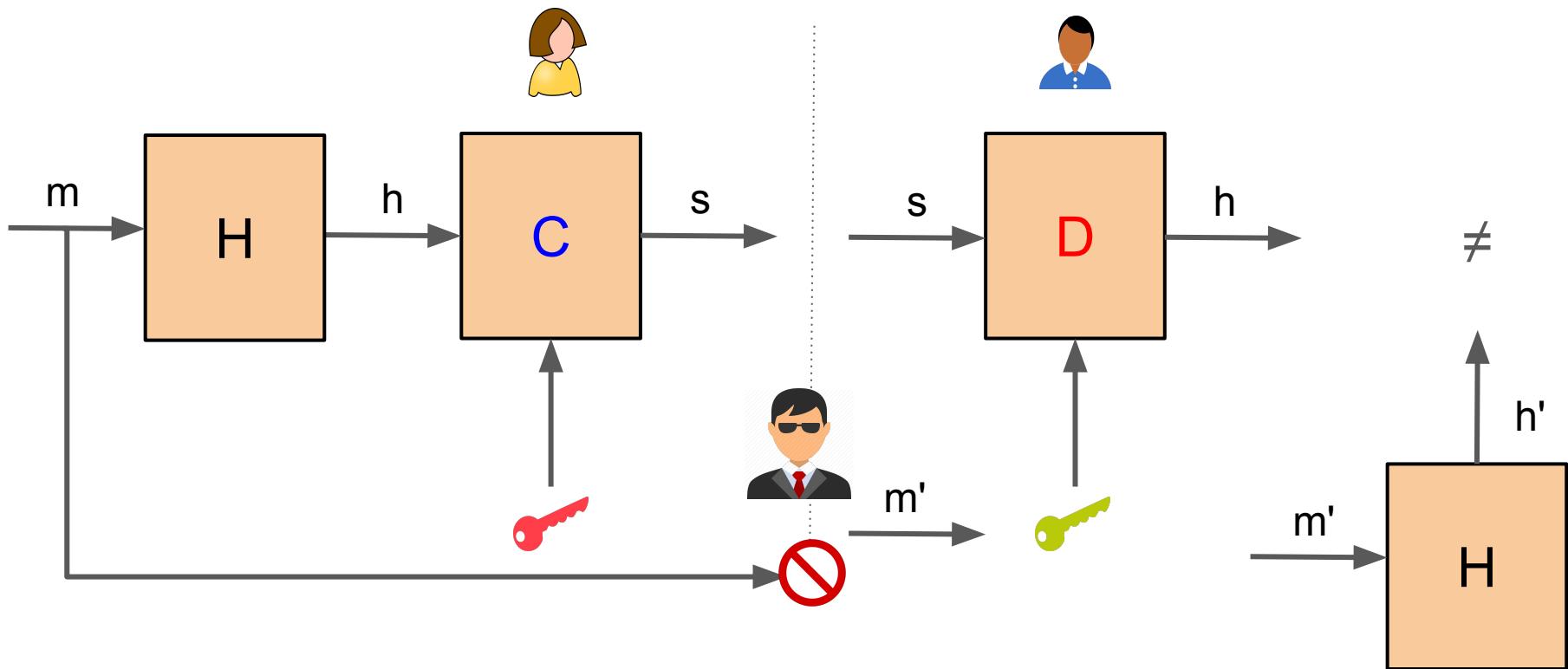
Assinatura digital: função hash + cript. assimétrica

- Assinatura digital: ao assinar *hash*, está se assinando um identificador único do documento



Assinatura Digital: hash resistente a colisão

- Mallory não consegue encontrar $m' \neq m$ que tenha mesma assinatura (*hash*)

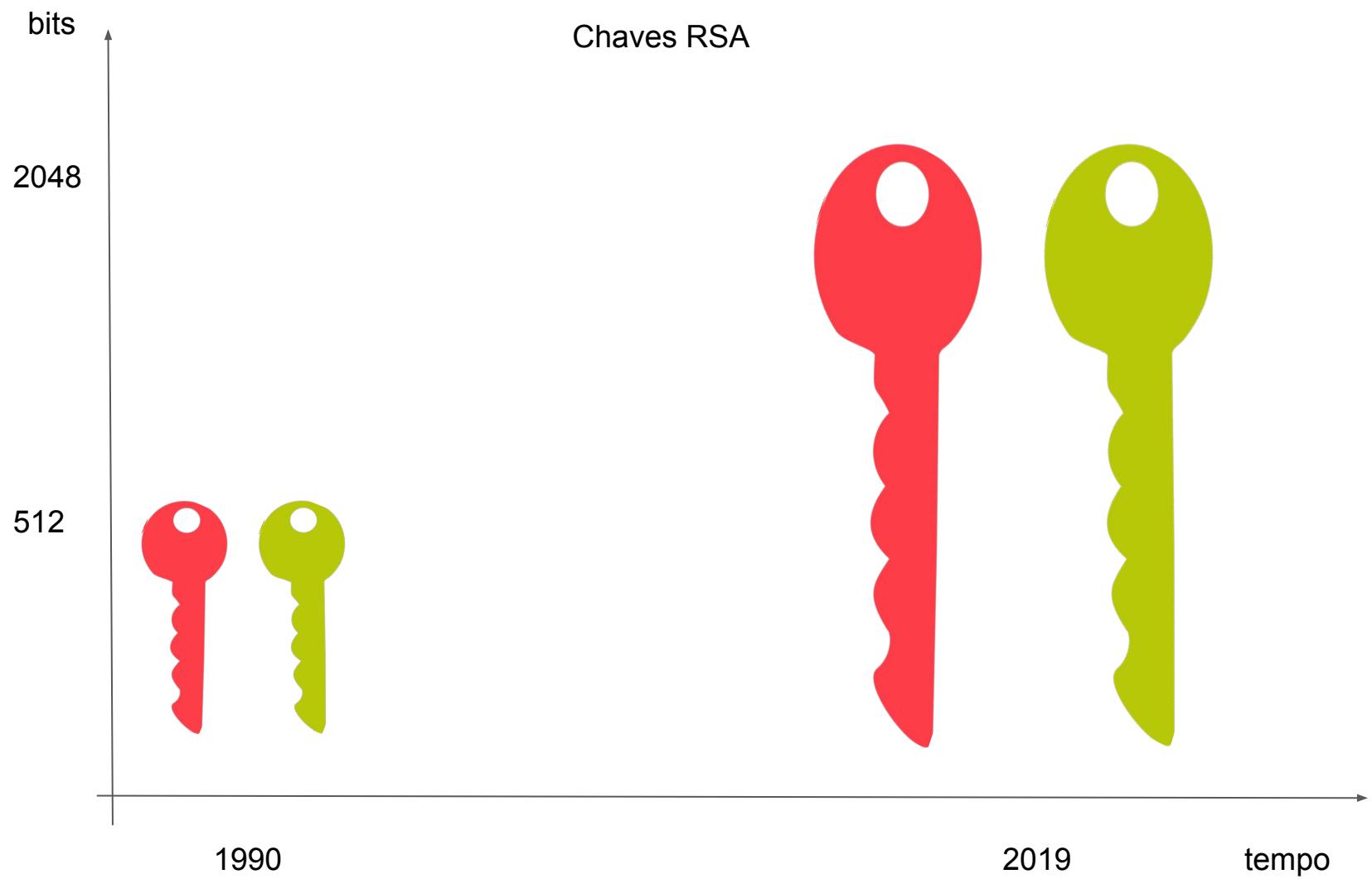


Algoritmo de cifragem assimétrica

- Rivest–Shamir–Adleman (RSA)
- Elliptic Curves Digital Signature Algorithm (ECDSA)

Problema dos esquemas de criptografia assimétrica

Chaves precisam ser trocadas com o tempo

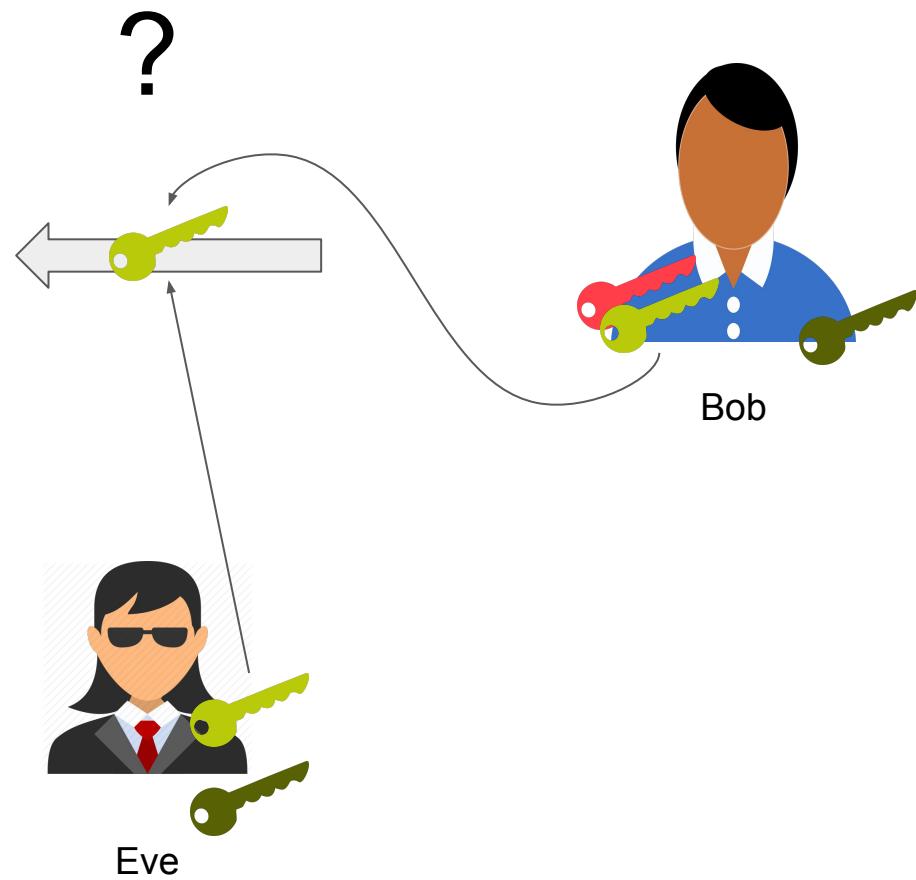


Certificado Digital (Como autenticar chaves)

Esta chave pública é mesmo de Bob?



Alice



Certificado Digital



- Documento eletrônico *assinado*
- Contém dados do titular do certificado e **sua chave pública**
- Geralmente emitido por uma terceira parte confiável que chamamos de *Autoridade Certificadora*
- Exemplo de dados:
 - Nome do servidor (hostname)
 - Nome completo e CPF (pessoa física)
 - Email
- Cria um vínculo de um *par de chaves* com uma *entidade*

Exemplo de certificado digital

Conceitos de criptografia - Go Moodle UFSC - Apoio aos Cursos Presenciais Martín

Secure https://moodle.ufsc.br

Connection is secure Your information (for example, passwords or credit card numbers) is private when it is sent to this site. [Learn more](#)

Flash Allow

Certificate (Valid)

Cookies (11 in use)

Site settings

Perguntas frequentes Veja respostas para as dúvidas frequentes

Tutoriais Aprenda mais sobre o Moodle e como nele realizar algumas tarefas

Supporte a usuários Saiba onde obter ajuda

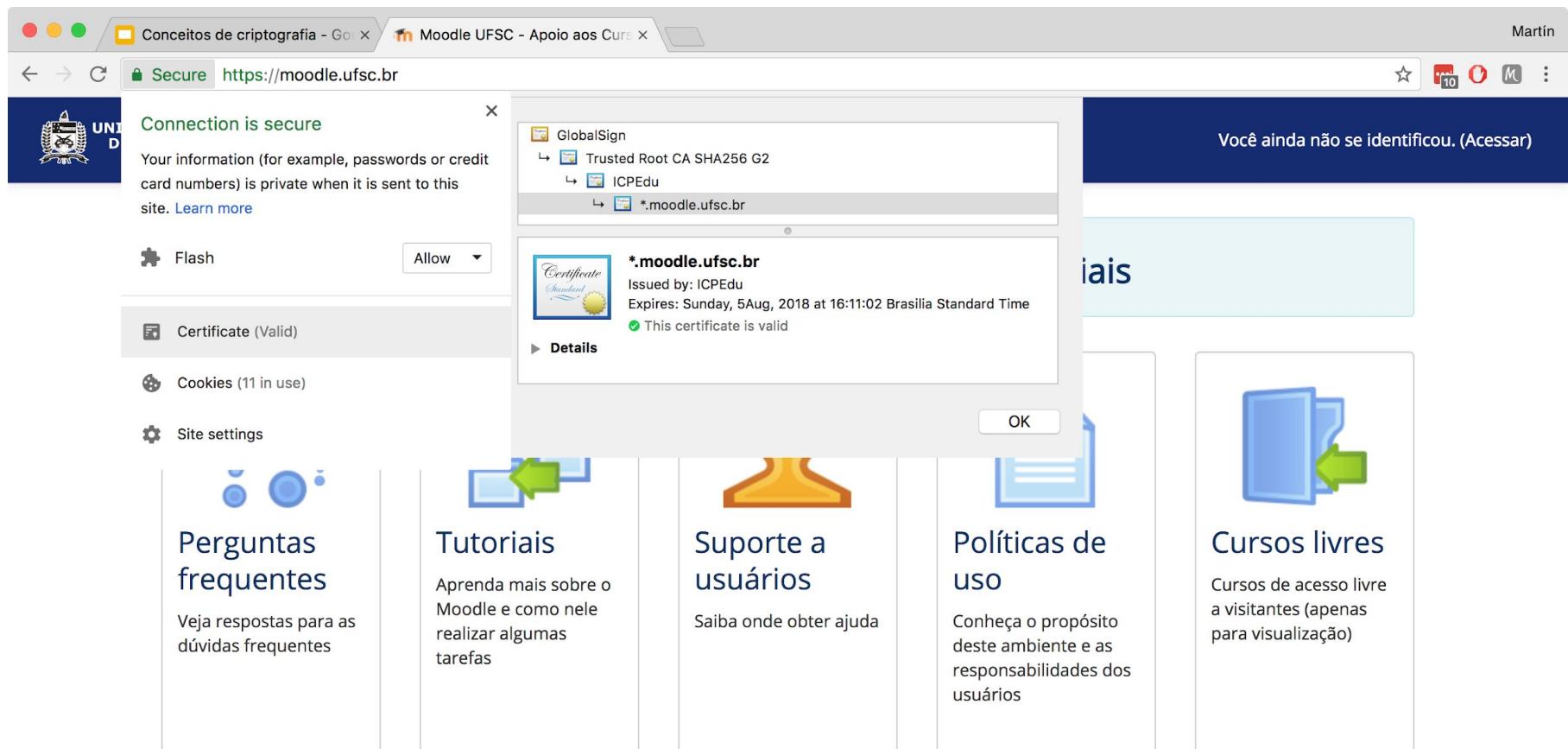
Políticas de uso Conheça o propósito deste ambiente e as responsabilidades dos usuários

Cursos livres Cursos de acesso livre a visitantes (apenas para visualização)

*.moodle.ufsc.br Issued by: ICPEdu Expires: Sunday, 5Aug, 2018 at 16:11:02 Brasilia Standard Time This certificate is valid

OK

Você ainda não se identificou. (Acessar)

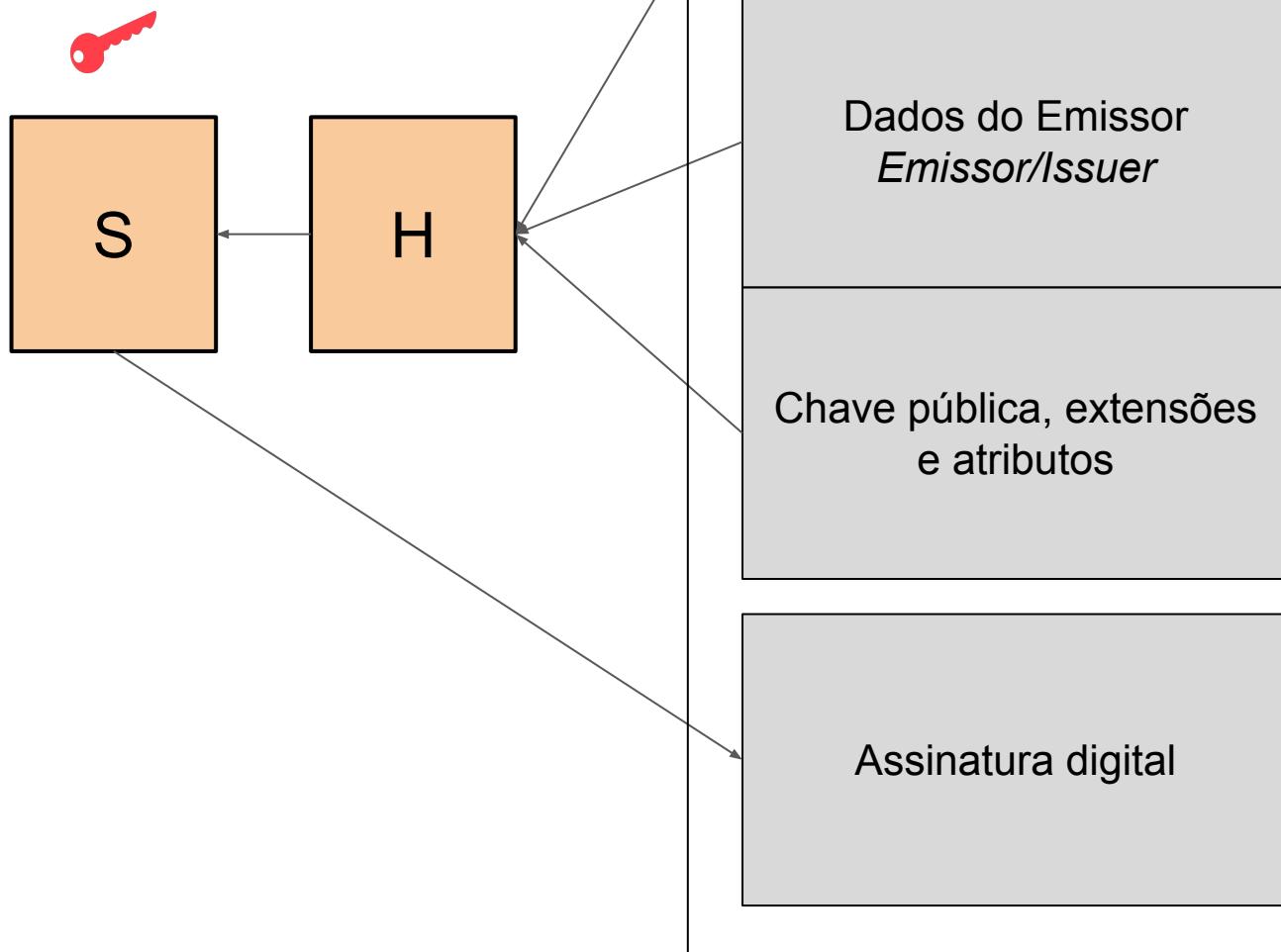


:: Este é o Moodle UFSC - Apoio aos Cursos Presenciais. Consulte a [lista de implantações de Moodle da UFSC](#) para ver outras opções.

Você ainda não se identificou. (Acessar)



Estrutura de um certificado



Ok, mas...

E como eu vou confiar na chave da *terceira parte* confiável?

Como fica a escalabilidade disso?

E se eu perder o controle da minha chave privada?

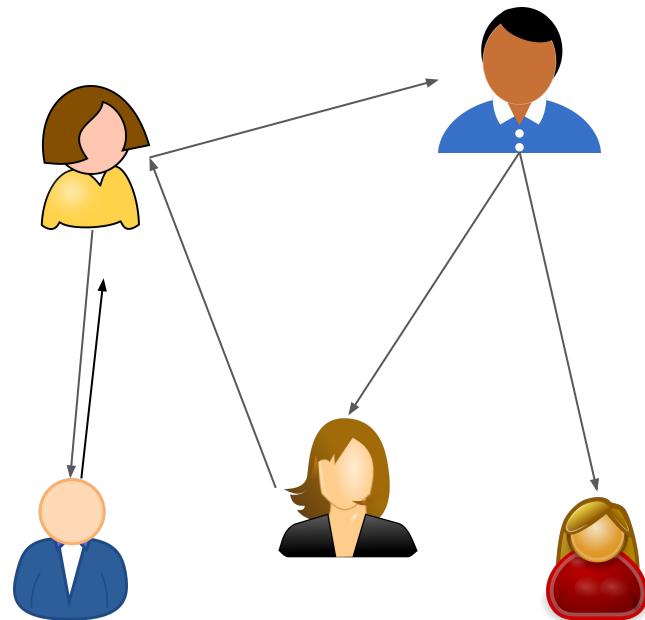
ICP

(como garantir não repúdio)

ICP - Infraestrutura de Chaves Publicas

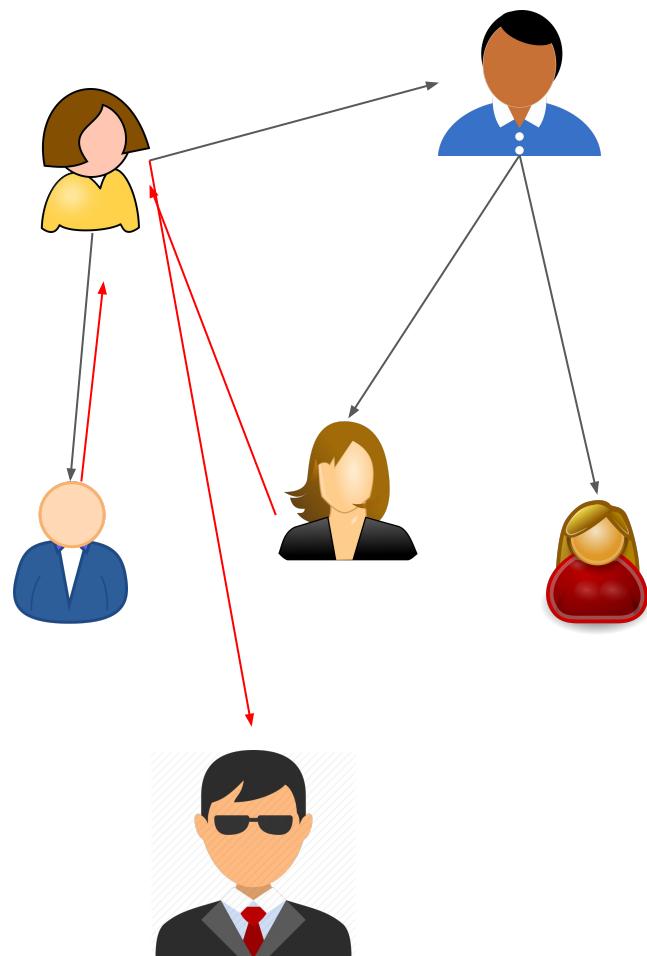
- *PKI* - Public Key Infrastructure
- Conjunto de políticas, procedimentos, papéis e sistemas para gestão de chaves públicas
- Emissão, revogação, publicação de certificados

Web of Trust - PGP (1991)



- Cada seta representa uma assinatura de confiança/verificação de identidade
- Pode-se inferir confiança para os demais nós
- Pode-se cancelar estas assinaturas ao publicar uma "assinatura de revogação"

Web of Trust - PGP - Riscos

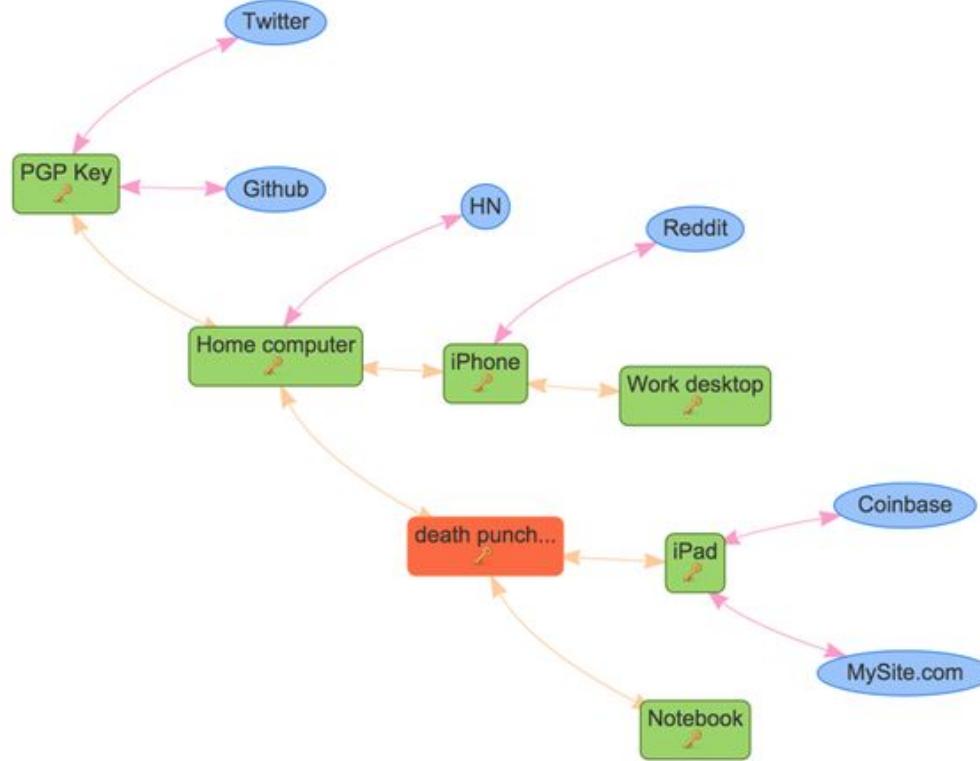


HOW TO USE PGP TO VERIFY
THAT AN EMAIL IS AUTHENTIC:

LOOK FOR THIS
TEXT AT THE TOP?



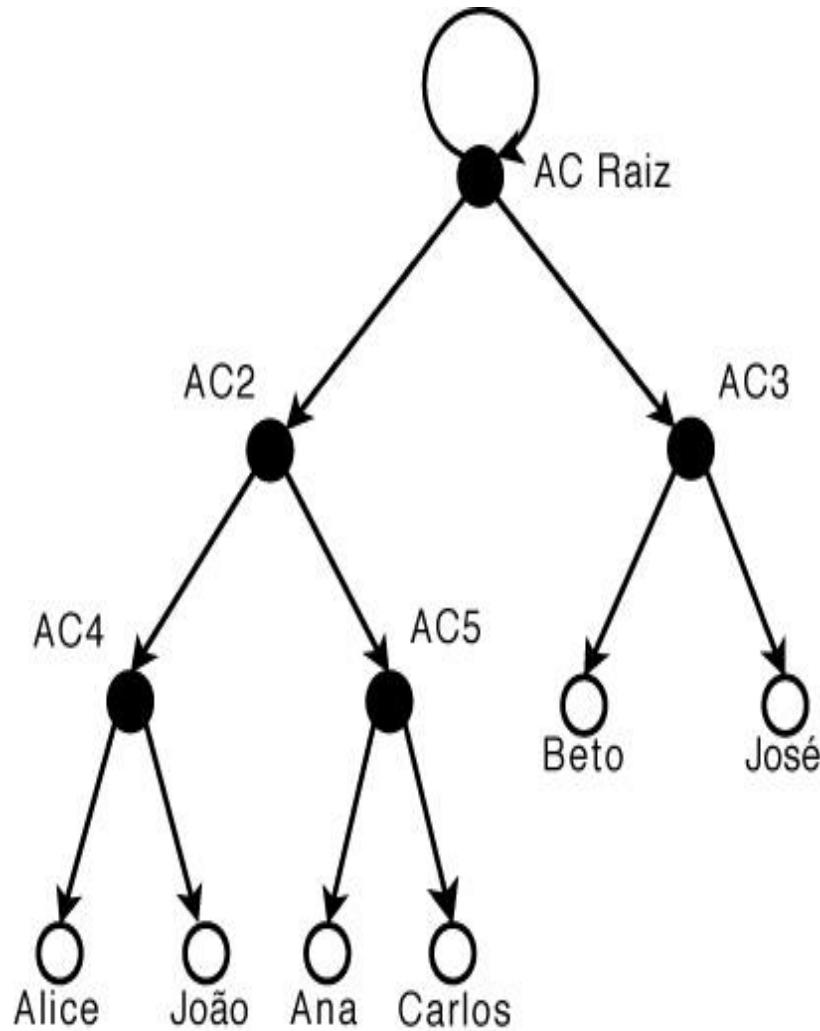
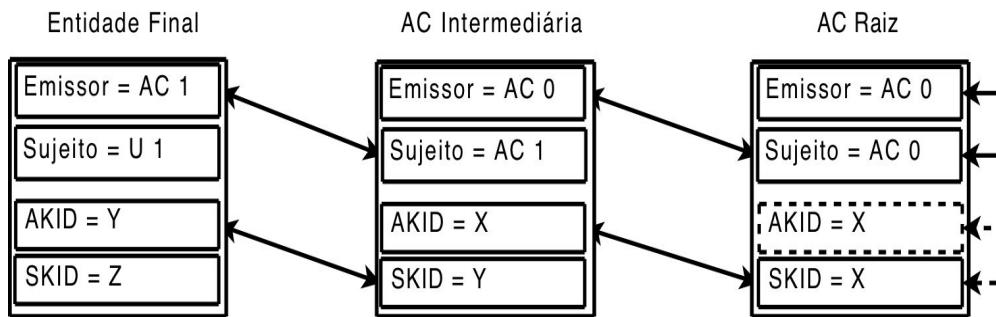
KeyBase



<https://keybase.io>

ICP X.509

- Cadeia de Autoridades Certificadoras
- Estrutura hierárquica
- ACs intermediárias para
 - Escalabilidade
 - Políticas de emissão



Validação de caminho de certificação

- Validação/Verificação do Caminho de Certificação
 - Para cada certificado do caminho encontrado, verificar:
 - Assinatura Digital
 - Validade
 - Situação (revogado ou não)
 - Extensão *BasicConstraints*
 - Extensões Críticas

LCR

Lista de certificados que não são mais válidos

Certificados mantidos na lista até sua expiração

OCSP

Resposta de um servidor sobre o status de um certificado específico

Não é possível saber o status de um certificado expirado!!!

ICP-Brasil

Regulamentação



**Presidência da República
Casa Civil
Subchefia para Assuntos Jurídicos**

MEDIDA PROVISÓRIA Nº 2.200-2, DE 24 DE AGOSTO DE 2001.

Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências.

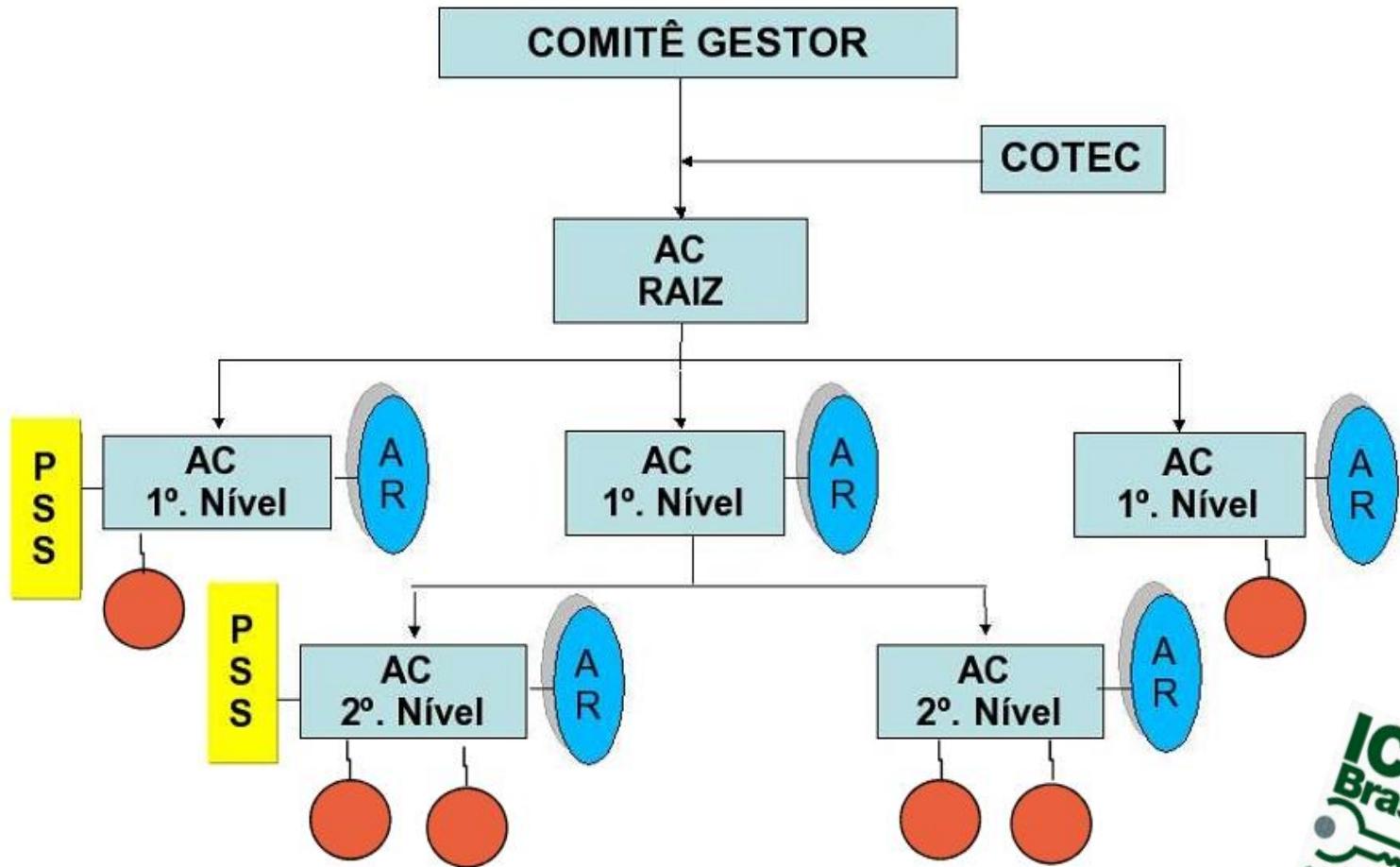
O PRESIDENTE DA REPÚBLICA, no uso da atribuição que lhe confere o art. 62 da Constituição, adota a seguinte Medida Provisória, com força de lei:

Art. 1º Fica instituída a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.

Validade Jurídica

*Art 10(...) As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil **presumem-se verdadeiros em relação aos signatários**, na forma do art. 131 da Lei no 3.071, de 10 de janeiro de 1916 - Código Civil.*

Estrutura



Autoridade de Registro



Identificador

SSP
Secretaria de Segurança Pública

RG

mundo real

AC
Autoridade Certificadora

Certificado Digital

mundo virtual



Autoridade de Registro

Autoridade de Carimbo de Tempo (como garantir tempestividade)

A validade de uma assinatura digital

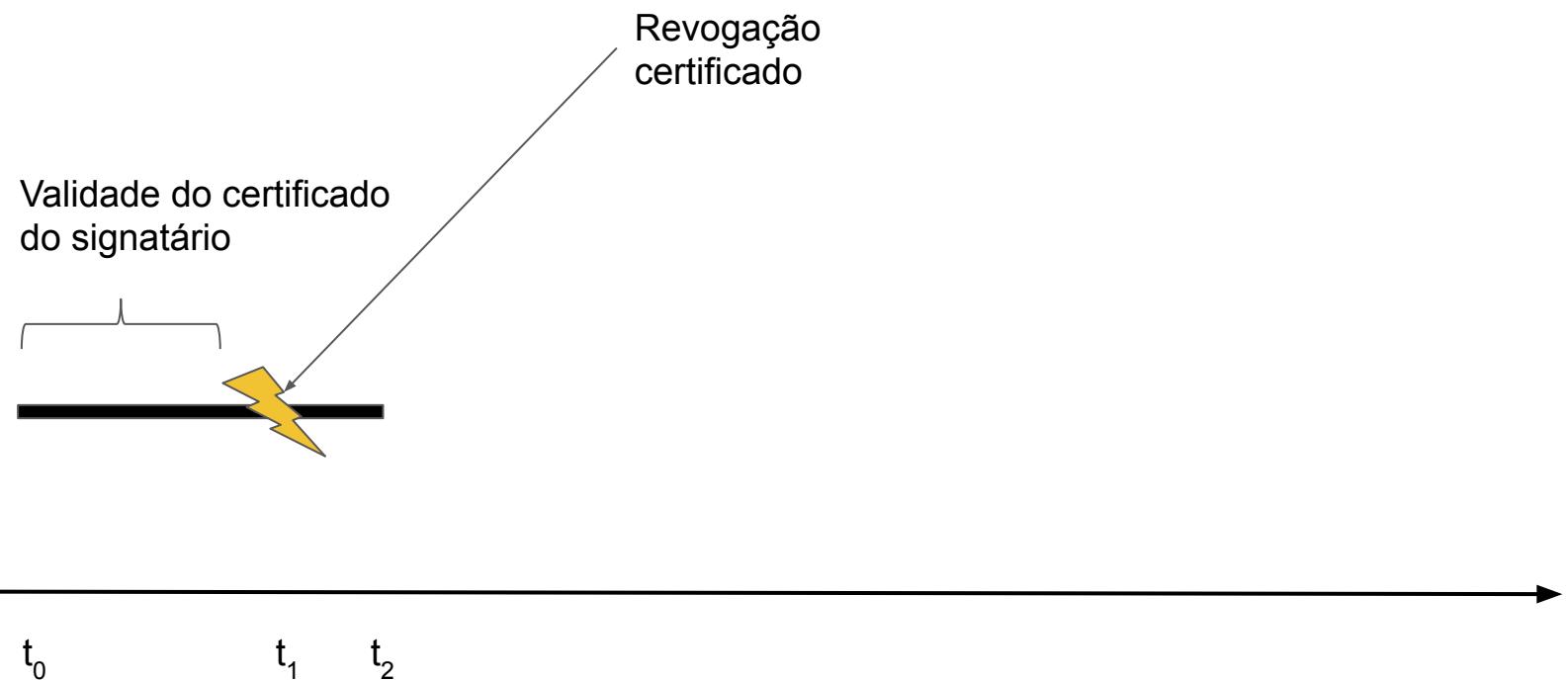
Validade do certificado
do signatário



t_0

t_1

A validade de uma assinatura digital



A validade de uma assinatura digital

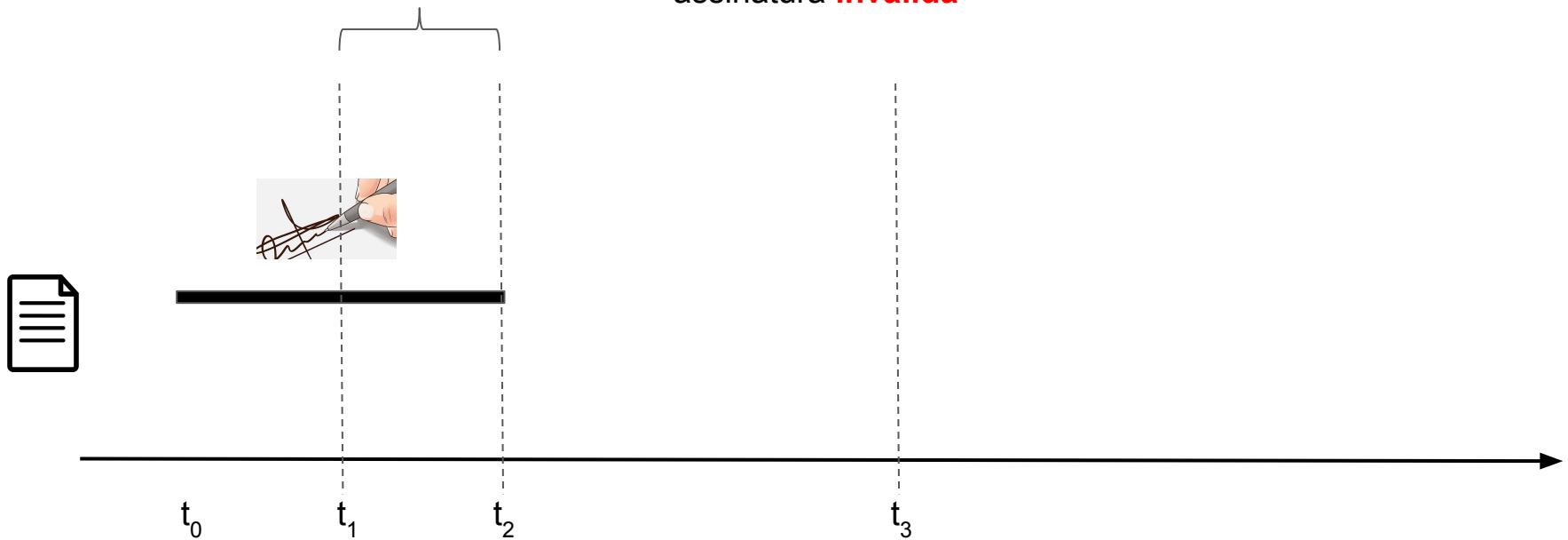
Validade da assinatura



A validade de uma assinatura digital

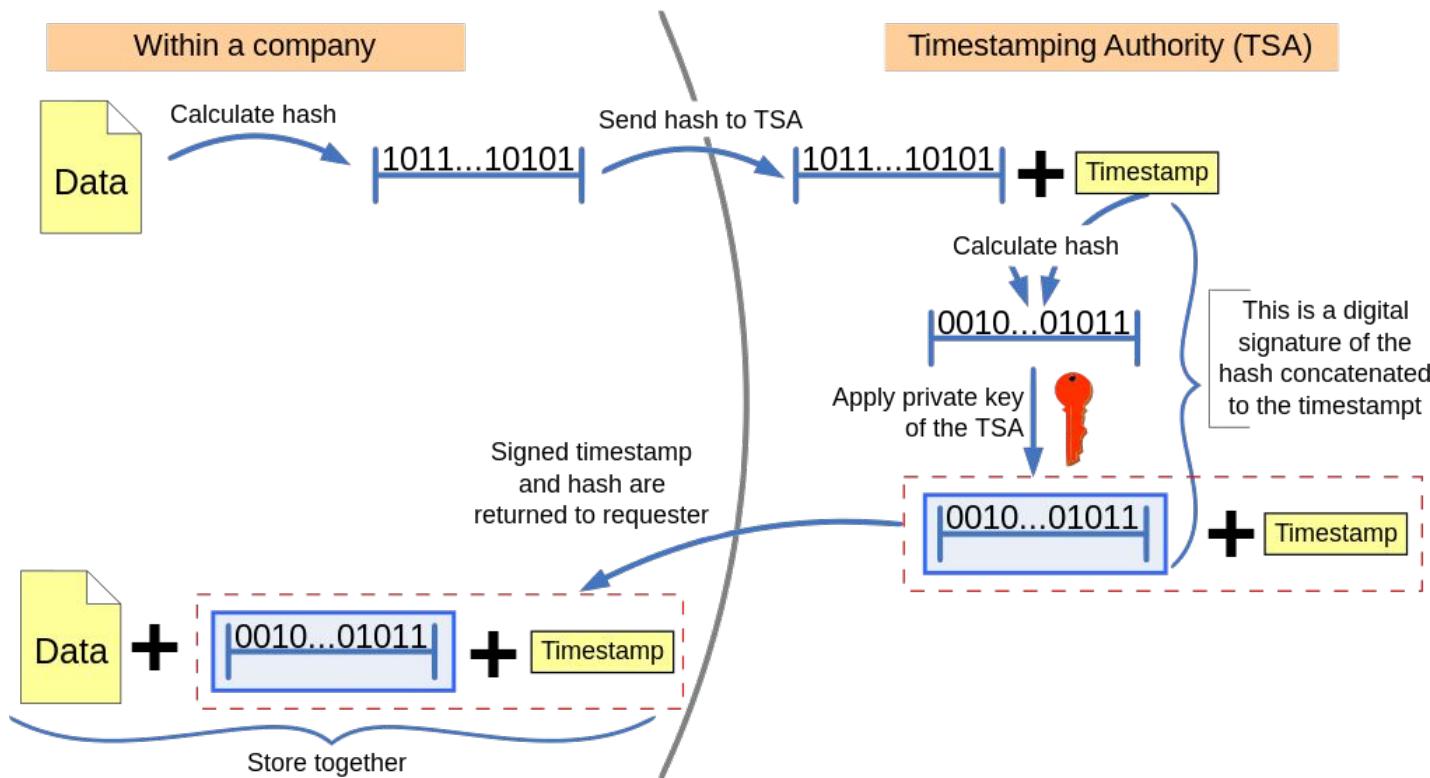
Validade da assinatura

Verificação da assinatura:
assinatura **inválida**



Autoridade de carimbo do tempo (ACT)

Trusted timestamping



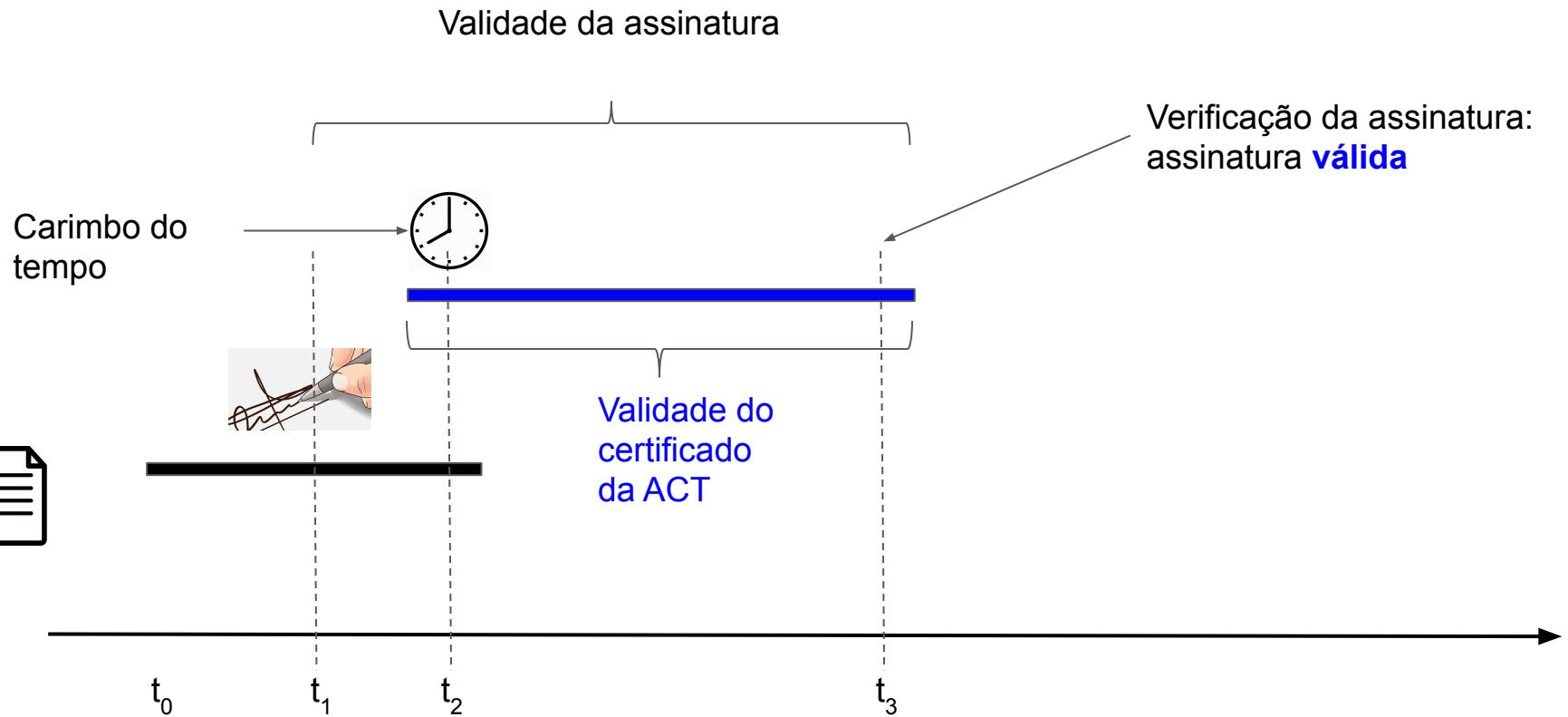
Autoridade de carimbo do tempo (ACT)

Assume-se que uma ACT provê a data e hora **corrente**.

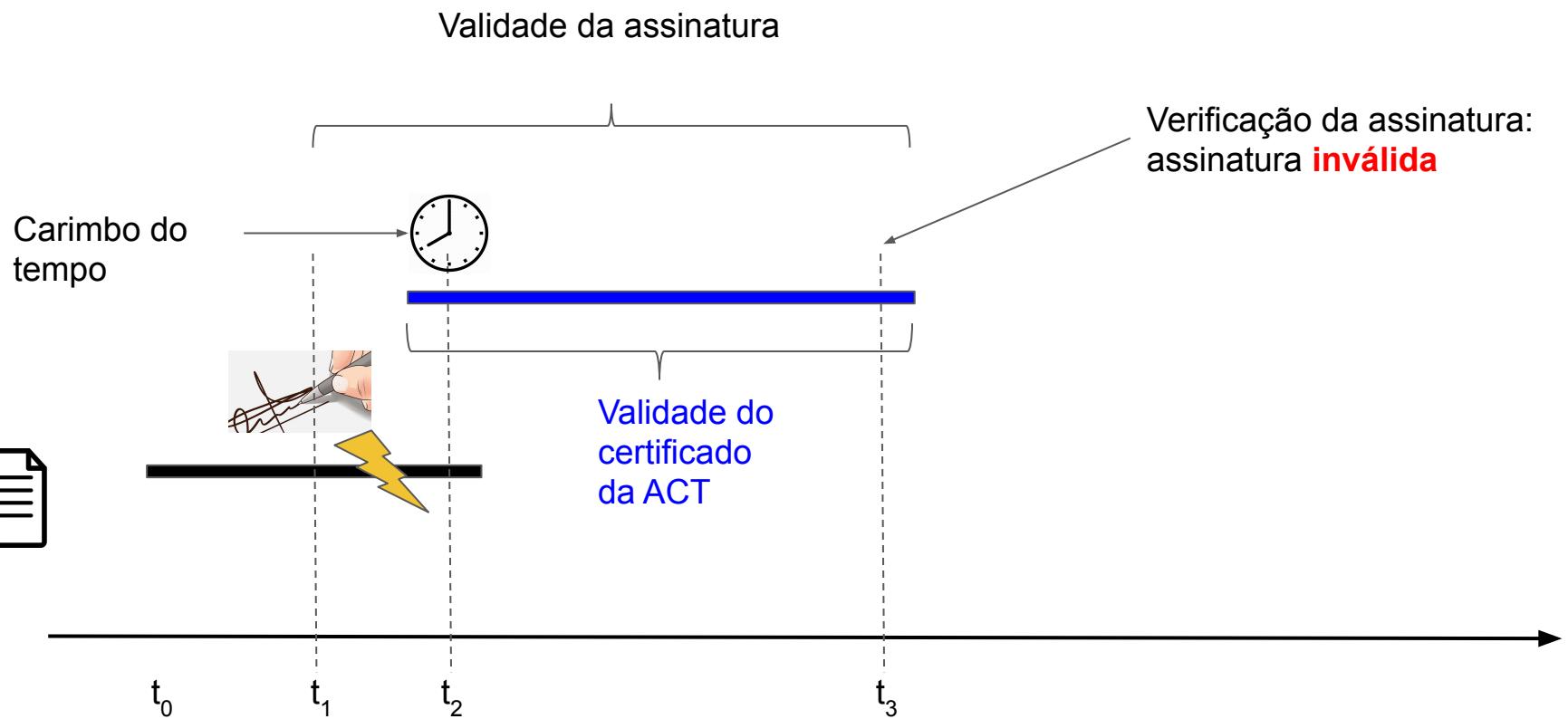
Ou seja, espera-se que a ACT **nunca** forneça uma data e hora:

- Passada
- Futura

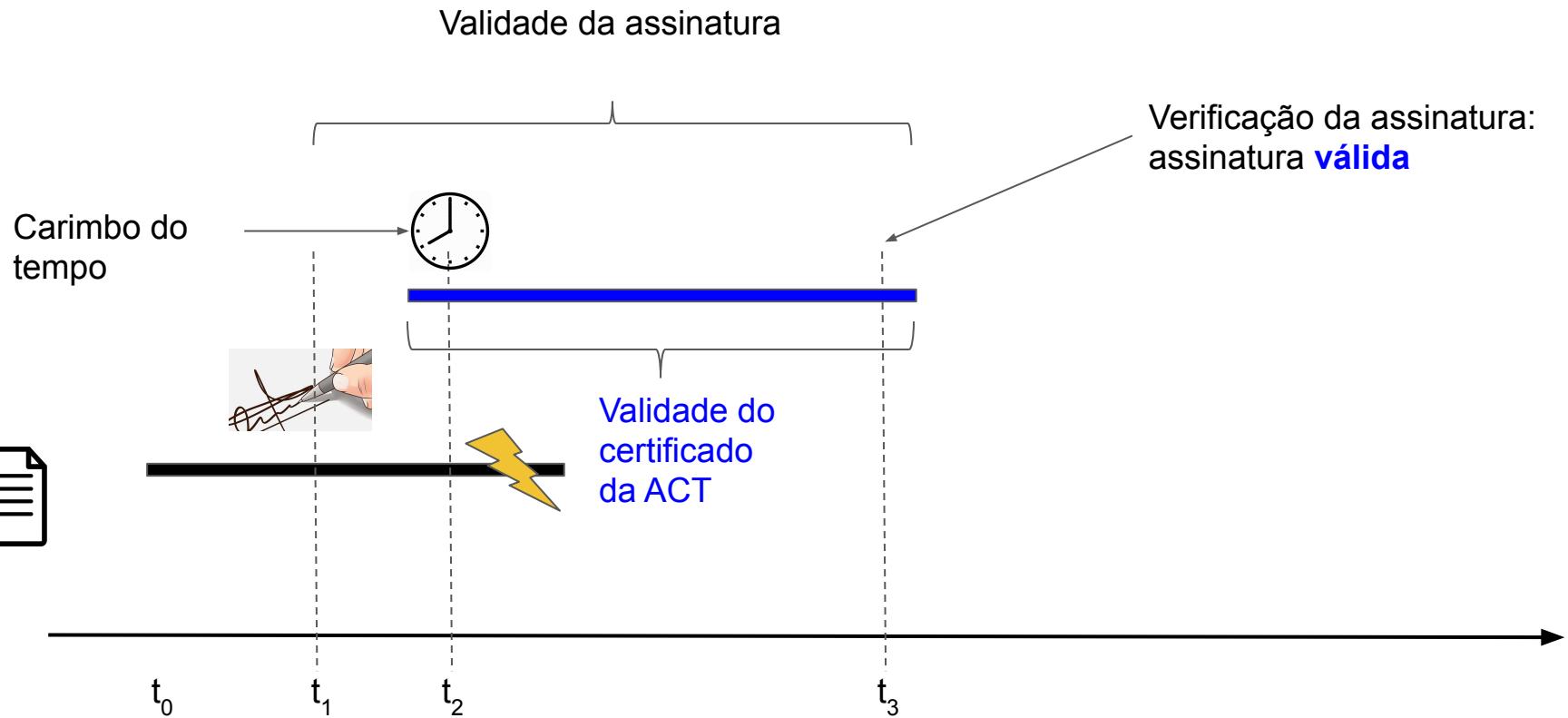
A validade de uma assinatura digital



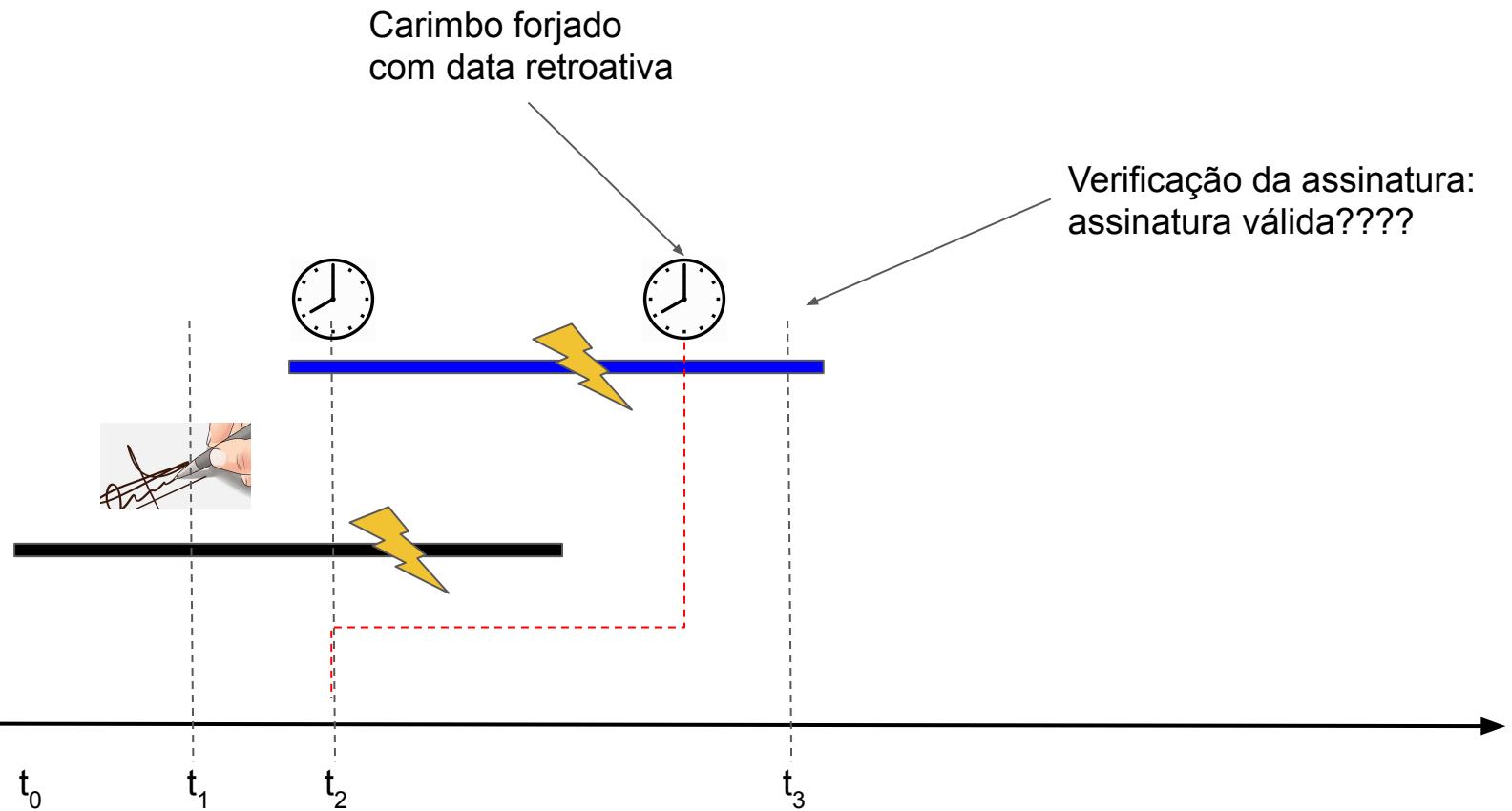
A validade de uma assinatura digital



A validade de uma assinatura digital



A validade de uma assinatura digital



A validade de uma assinatura digital

Verificação da assinatura:
assinatura **válida**

