

# 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.

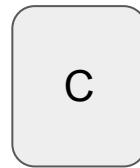
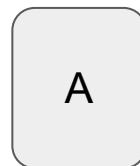
*Criptografia*: registrar algo de forma oculta...

... 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**

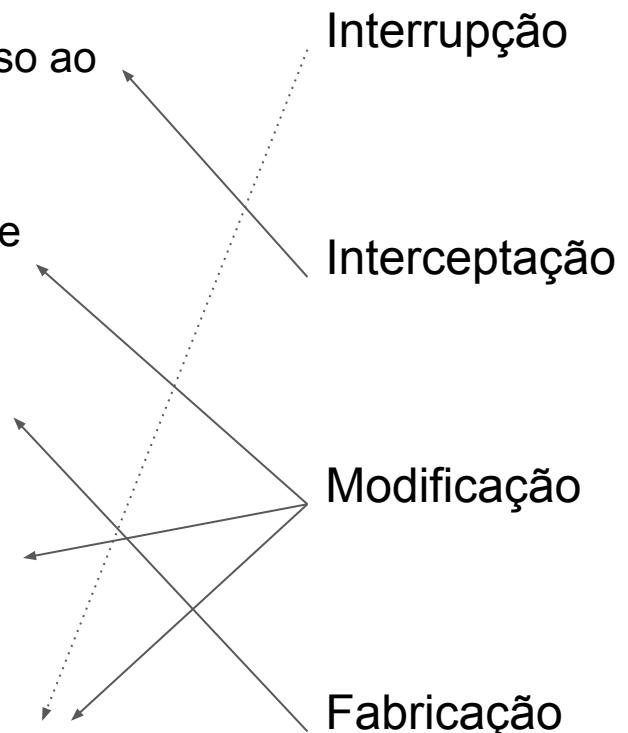
- Quem recebe a mensagem consegue identificar o remetente

- **Não recusa ou não repúdio**

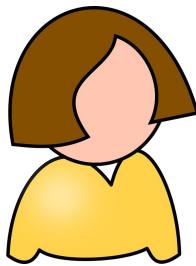
- Quem envia a mensagem não pode negar que a enviou

- **Irretroatividade – tempestividade**

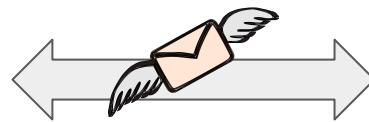
- Garantias sobre a existência de uma mensagem em determinada data



# Nossos personagens....

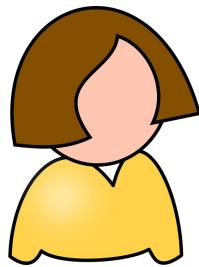


Alice



Bob

# Nossos personagens....



Alice



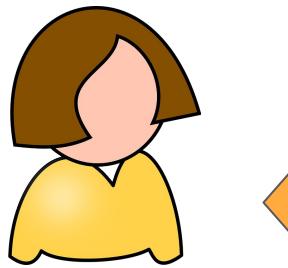
Bob



Eve

*Ameaça:  
Interceptação*

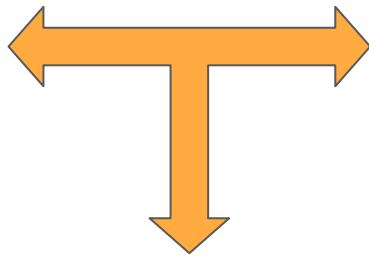
# Nossos personagens....



Alice



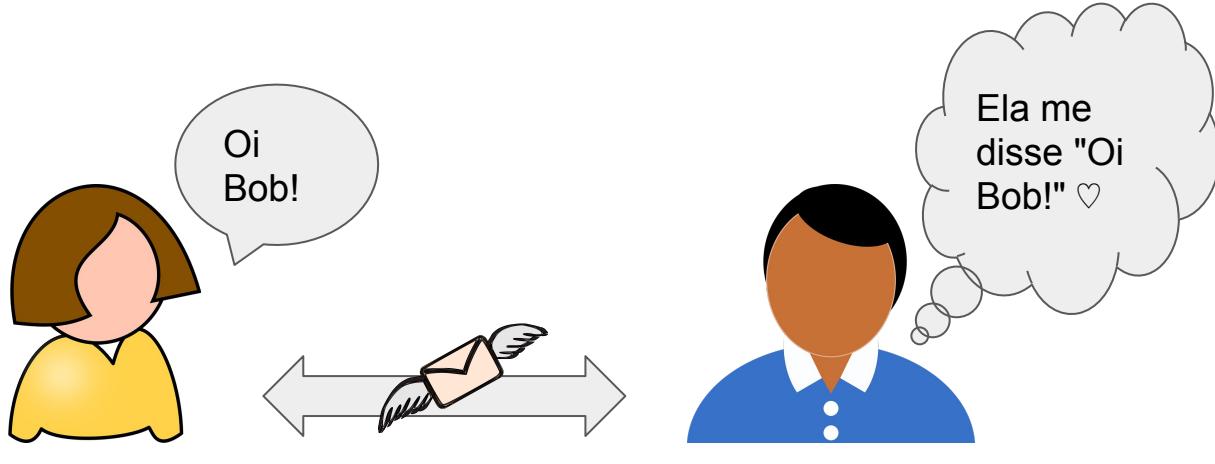
Bob



Mallory

Ameaças:  
*Interceptação*  
*Interrupção*  
*Modificação*  
*Fabricação*

# Sigilo

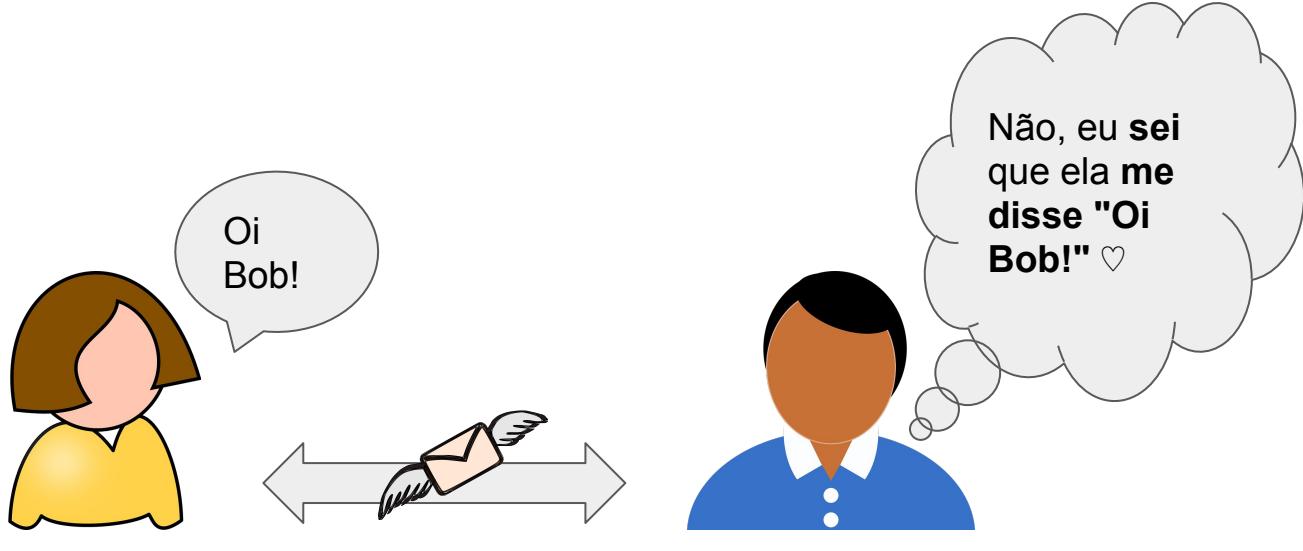


Alice

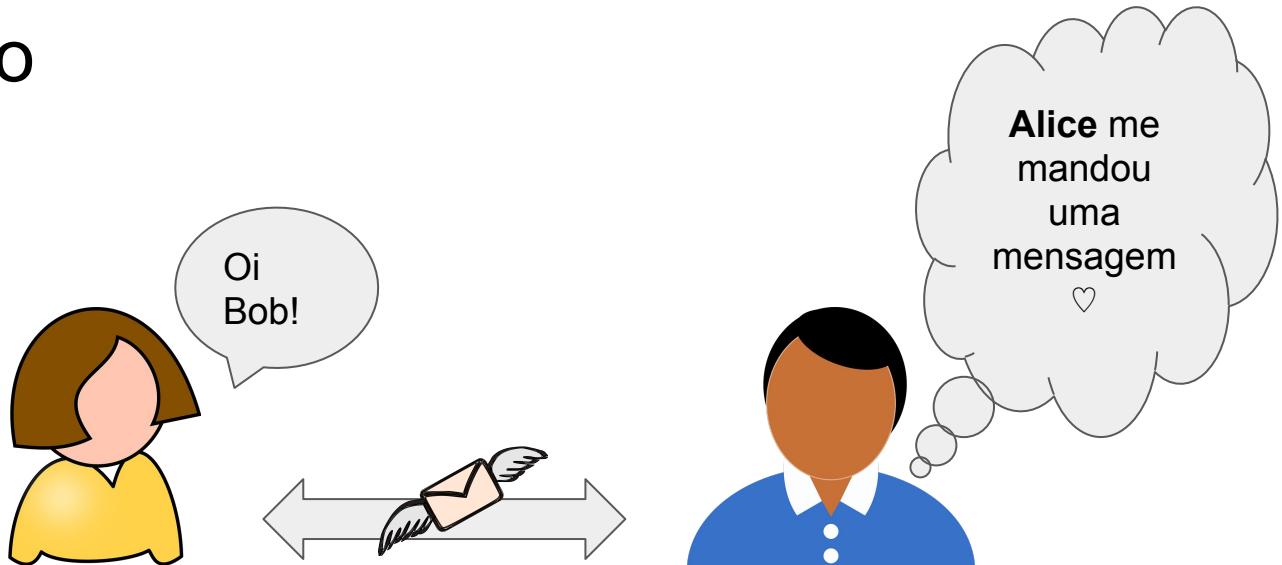


Eve

# Integridade



# Autenticação



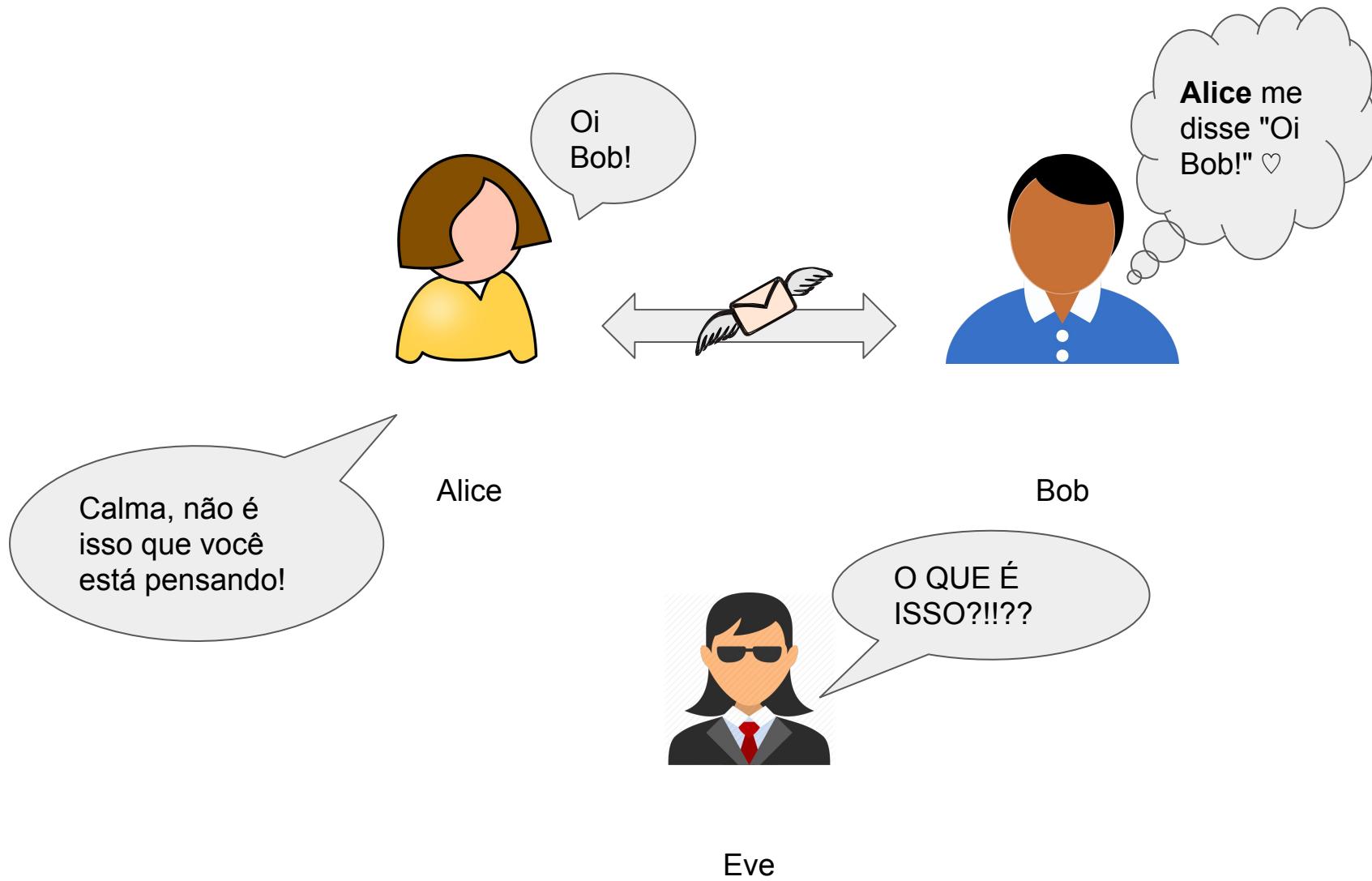
Alice

Bob

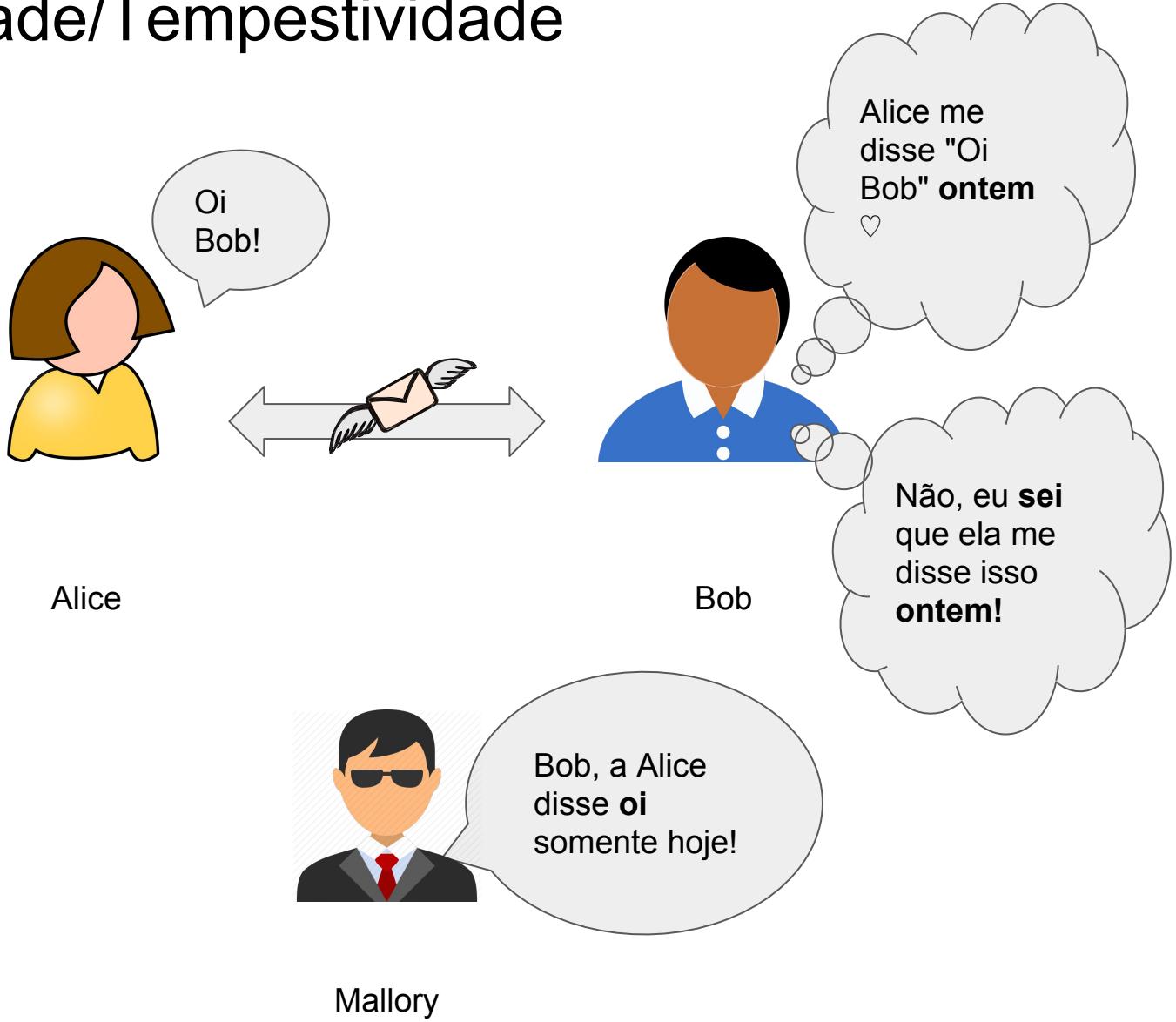


Mallory

# 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 - segunda parte do curso
- Transporte: Transmitir dados usando a chave secreta com garantia de integridade e confidencialidade - primeira parte do curso

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

# Como é um algoritmo criptográfico de cifragem?

Cifragem → Transporte seguro

$$c(m) = m+5$$

$$m(c) = c-5$$

Função matemática (cifragem) e sua inversa (decifragem)

# Como é um algoritmo criptográfico de cifragem?

As cifras normalmente operam dentro de um domínio finito de valores, por exemplo através da operação módulo:

$$c(m) = (m+5) \pmod{26}$$

$$m(c) = (c-5) \pmod{26}$$

# MÓDULO



- 1) O que é módulo?
- 2) Um exemplo de operação modular do dia-a-dia?



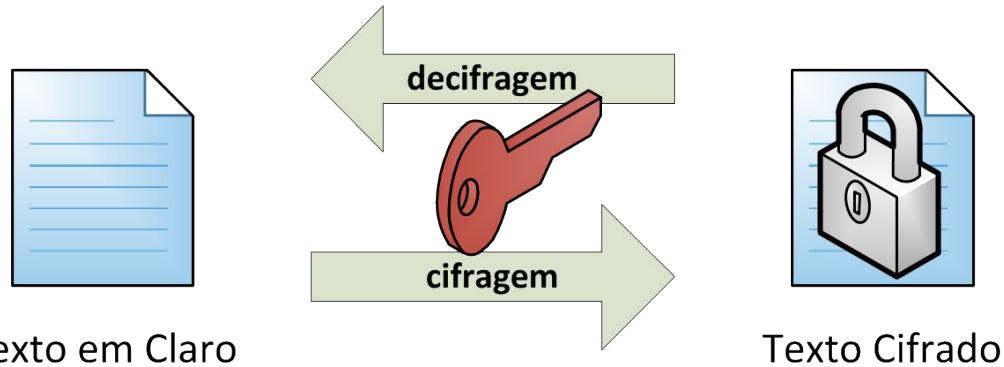
# Como é um algoritmo criptográfico de cifragem?

Toda cifra tem uma ou mais *chaves*, que são a **única** parte secreta:

$$c(m,k) = (m+k) \pmod{26}$$

$$m(c,k) = (c-k) \pmod{26}$$

# Cifragem

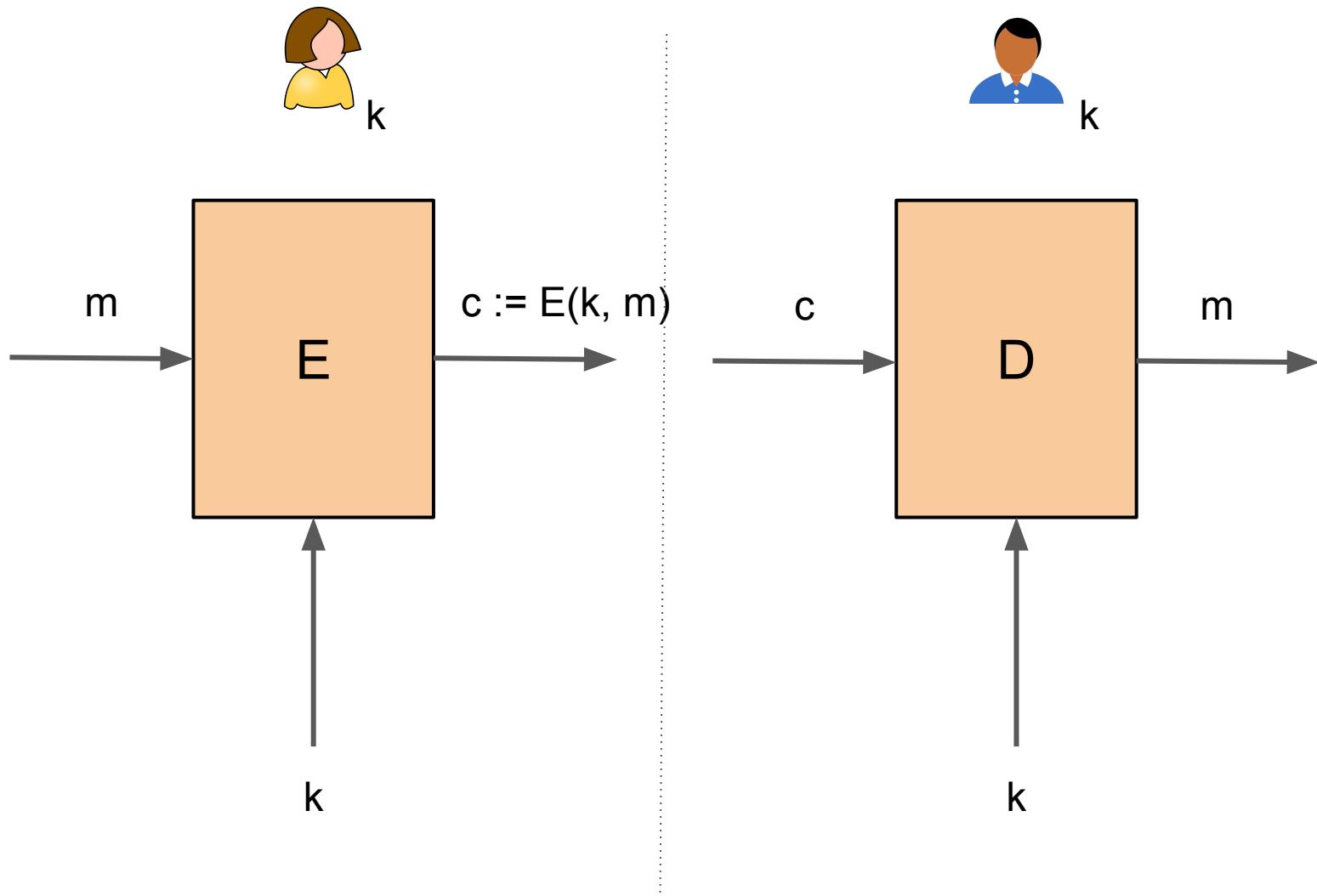


E, D, m, k

Algoritmo (E, D) **publicamente** conhecidos

Chave k é a **única** parte secreta

# Cifragem: notação



# Princípios básicos de criptografia

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



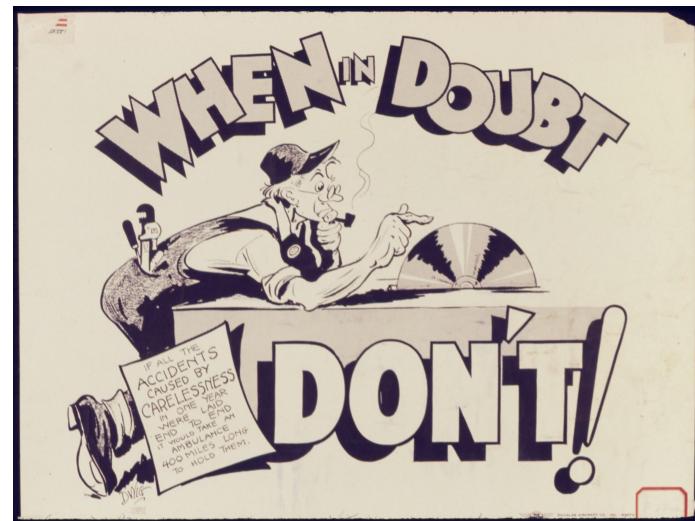
# A lição mais importante...

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!

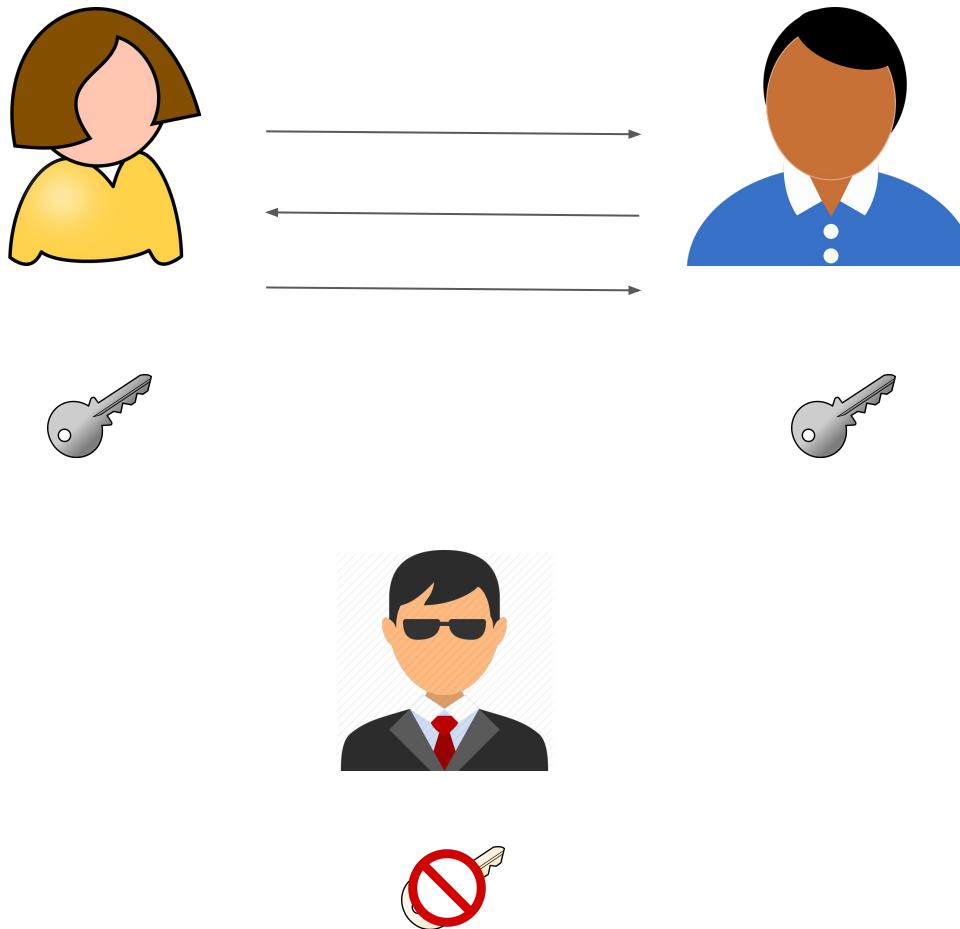
A única coisa secreta é chamada de *chave*!



# Aplicações de criptografia

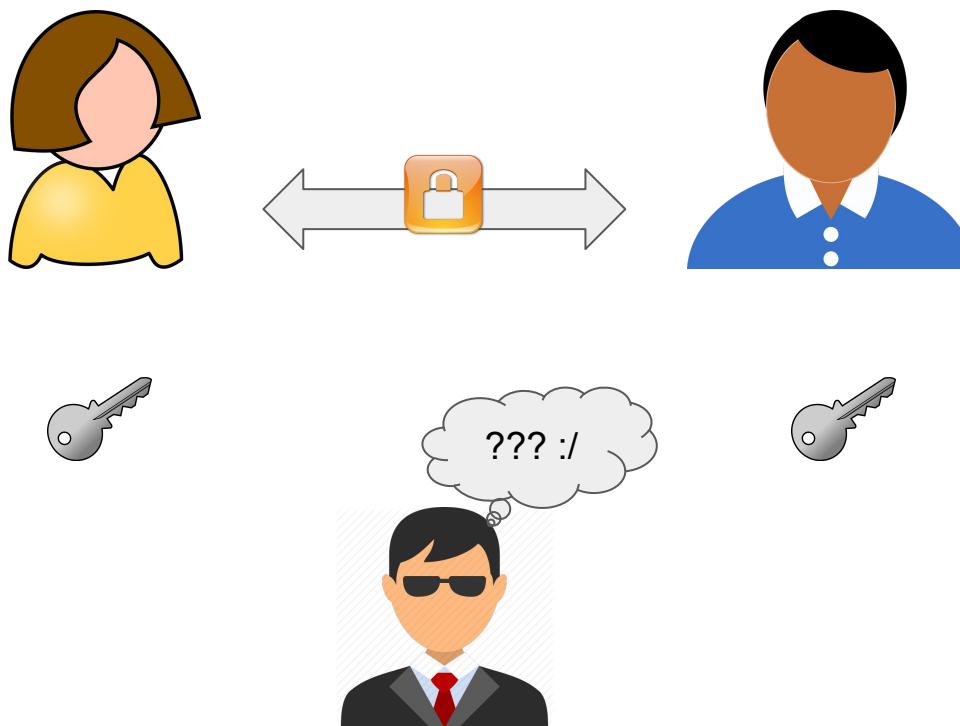
# Core: Comunicação Segura

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.

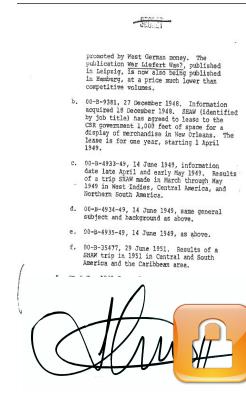
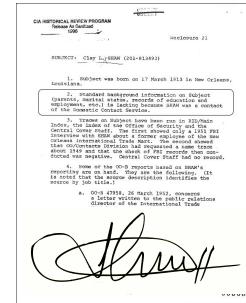
A handwritten signature in black ink, appearing identical across four instances.

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.

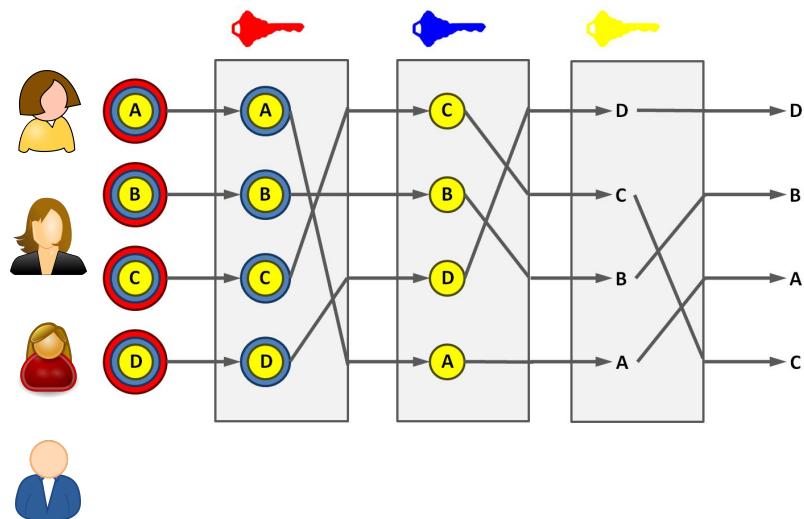
d. 00-9-933-49, 14 June 1948, same general subject and background as above.

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

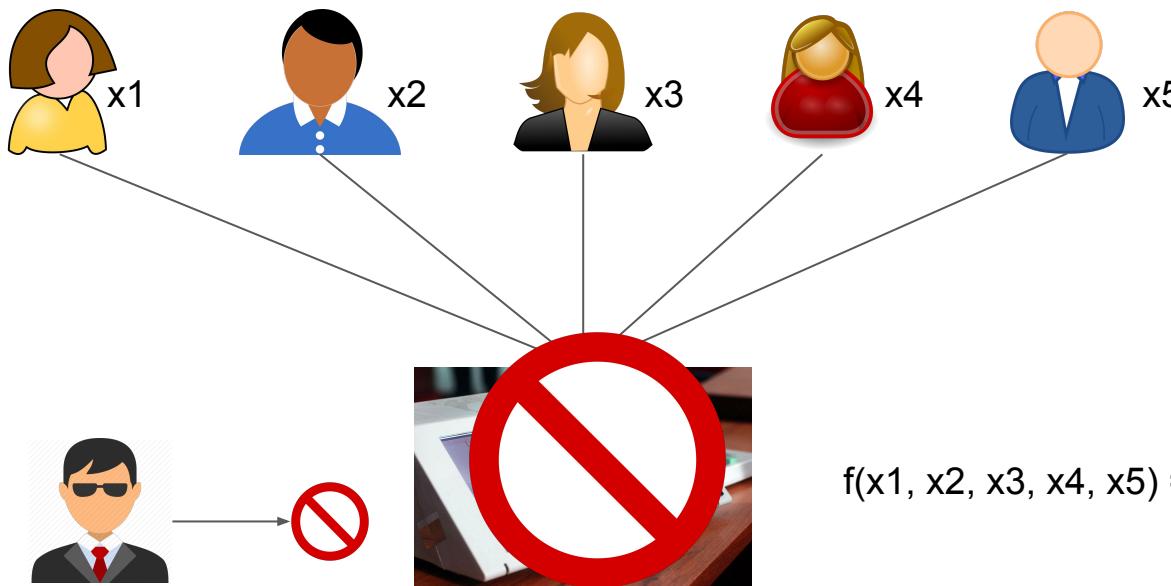
Problema: Como contar o total de votos em cada opção, sem que:

- 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

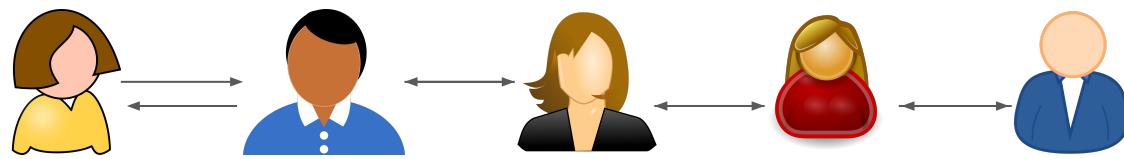


# Computação multiparty segura

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.

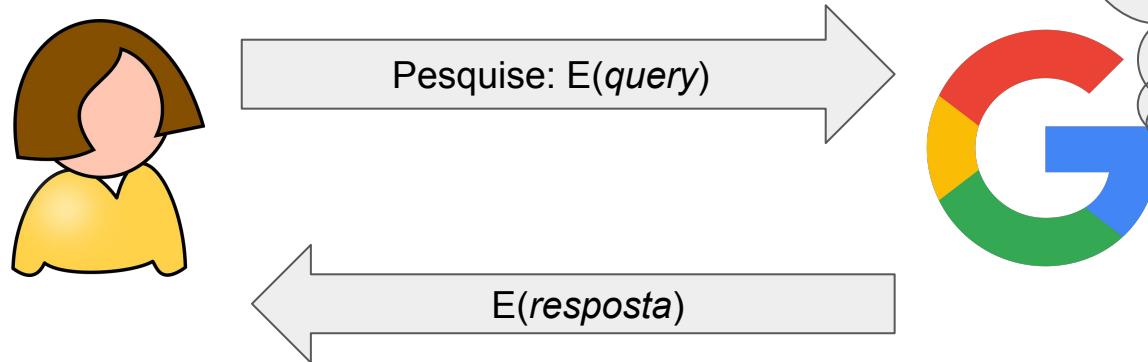
# Eleições



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

# “Mágicas criptográficas”

Computação em nuvem sem revelar o conteúdo

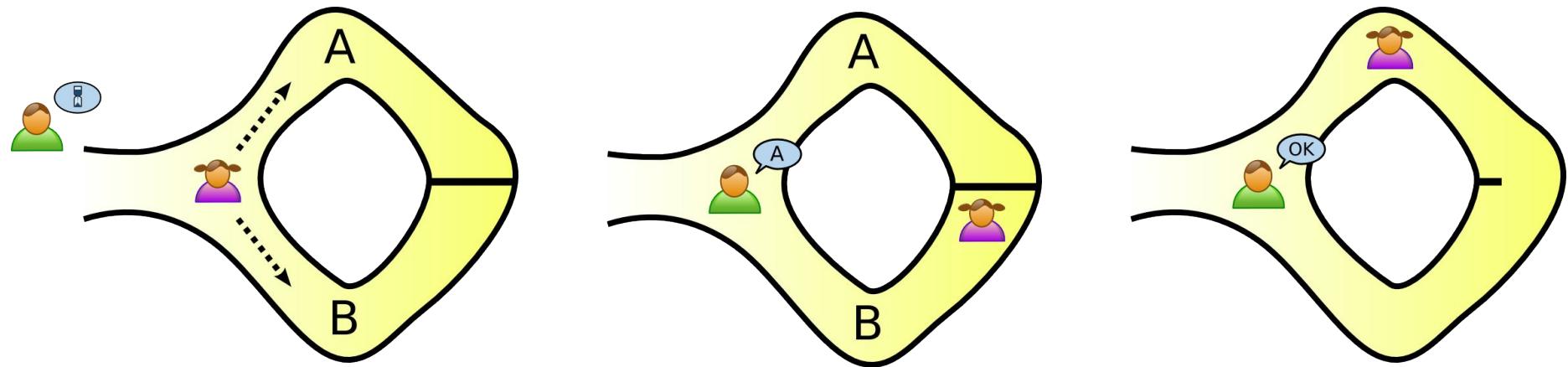


Possível? SIM!

Mas ainda apenas para aplicações extremamente mais simples!

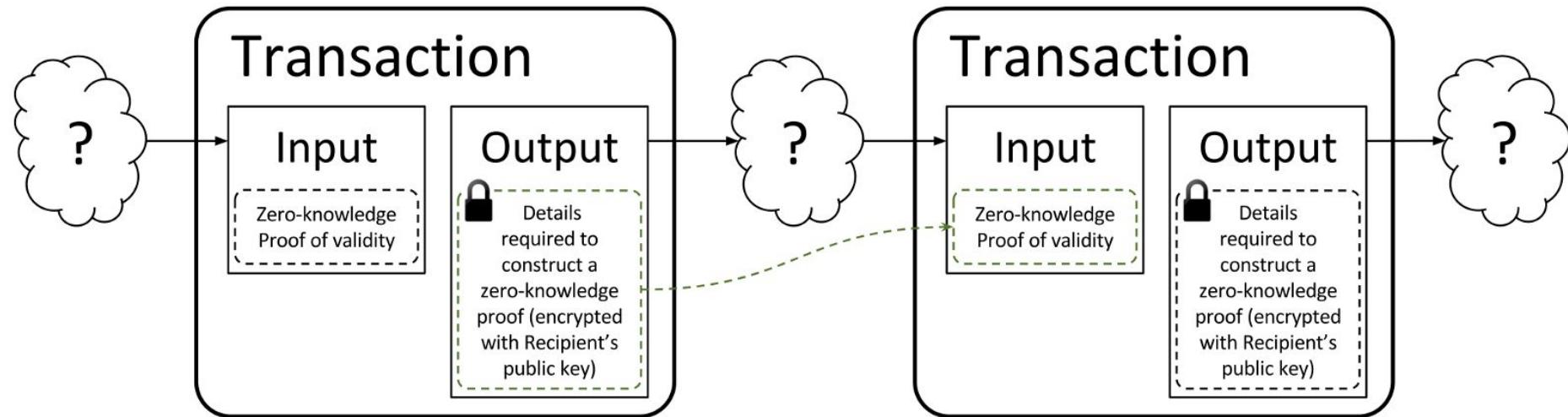
# Zero knowledge

Provar a alguém que você tem a solução de um problema, sem revelar a solução



# Zero knowledge

- Aplicado em contextos onde privacidade é desejável
- Exemplos de criptomoedas:
  - A transação é válida? Ex. o pagador de fato tem as moedas que ele está gastando?
  - Esconder pagador/receptor

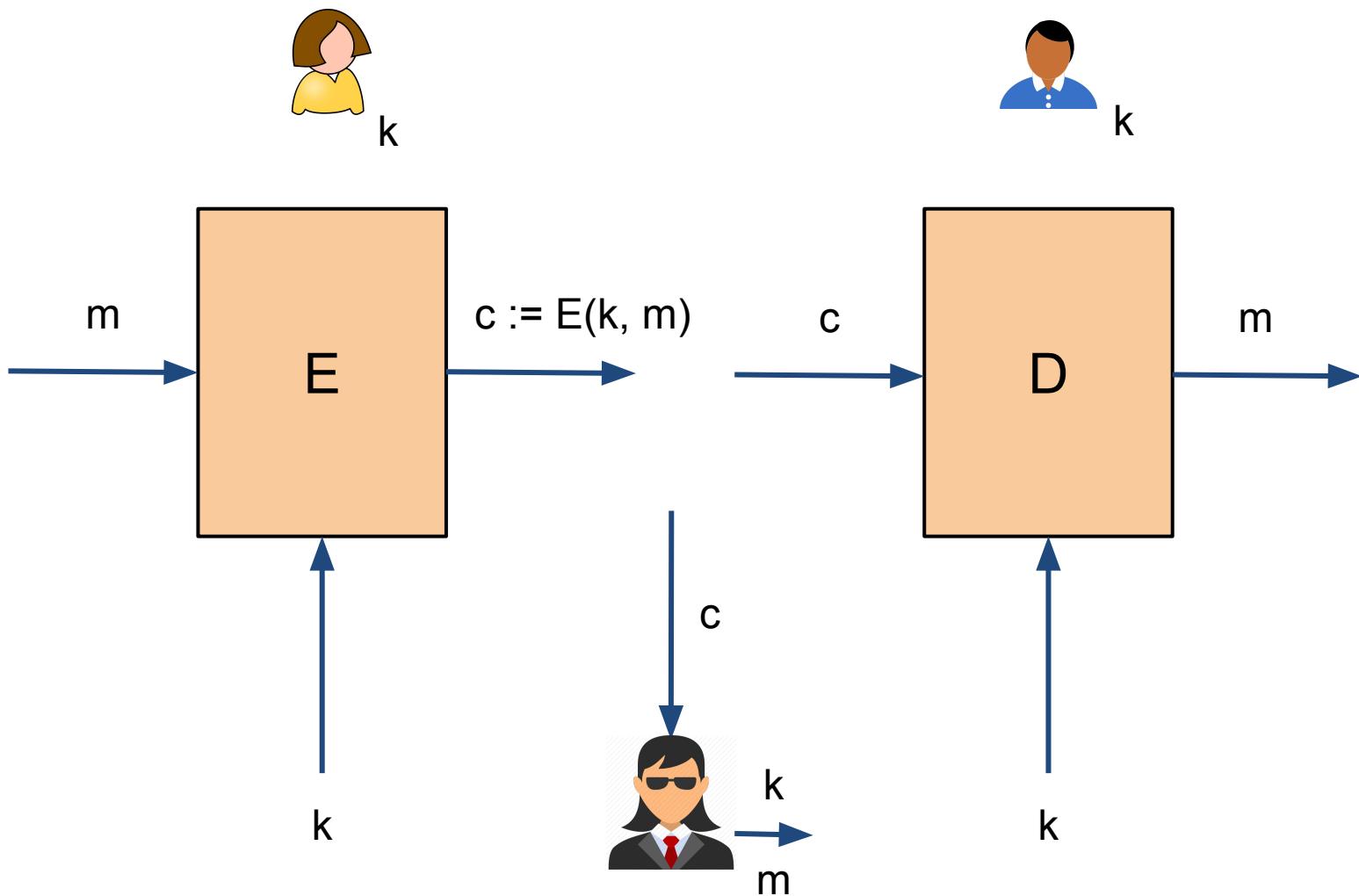


# Criptoanálise

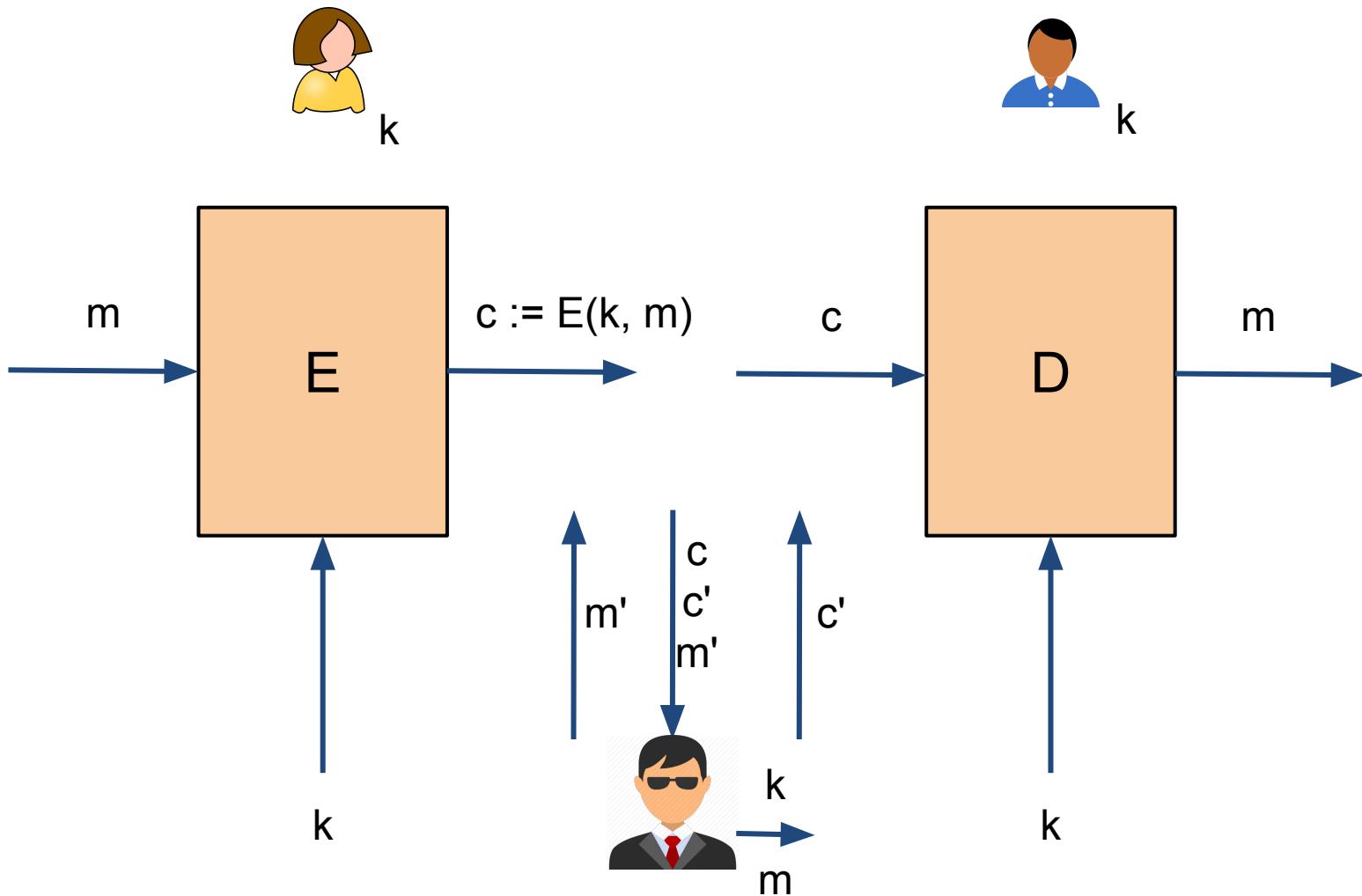
# Criptografia x Criptoanálise

- Criptografia
  - Operações no texto claro para texto cifrado
  - Trabalha com
    - Geração de chaves
    - A forma como o texto claro é processado
- Criptoanálise
  - Ataque na natureza do algoritmo
  - Trabalha com
    - Características do texto (claro e cifrado)
    - Força bruta

# Modelo de Criptoanálise



# Modelo de Criptoanálise



# Criptoanálise

Tipo de Ataque	Acessível ao Criptoanalista
Texto Cifrado	Algoritmo, texto cifrado
Texto Claro Conhecido	Algoritmo, texto cifrado Pares texto claro-texto cifrado
Texto Claro Escolhido	Algoritmo, texto cifrado Pares texto claro-texto cifrado Texto claro escolhido pelo criptoanalista
Texto Cifrado Escolhido	Algoritmo, texto cifrado Pares texto claro-texto cifrado Texto cifrado escolhido pelo criptoanalista
Texto Escolhido	Algoritmo, texto cifrado Pares texto claro-texto cifrado Texto claro escolhido pelo criptoanalista, texto cifrado escolhido pelo criptoanalista

# Incondicionalmente Seguro

X

# Computacionalmente Seguro

- Incondicional
  - Texto cifrado não contém informação suficiente para determinar o texto claro
- Computacional
  - Custo de quebrar excede o valor da mensagem
  - O tempo requerido é maior que a vida útil da mensagem

## Estimativa de quebra de chave por força bruta

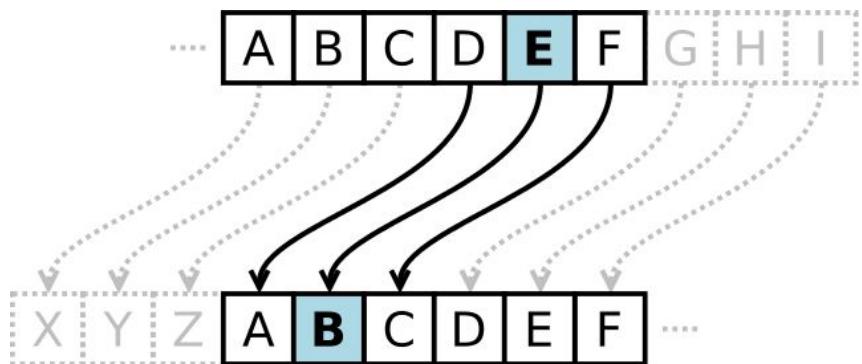
Key Size (bits)	Number of Alternative Keys	Time required at 1 decryption/μs	Time required at 10 <sup>6</sup> decryptions/μs
32	$2^{32} = 4.3 \times 10^9$	$2^{31} \mu\text{s} = 35.8 \text{ minutes}$	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	$2^{55} \mu\text{s} = 1142 \text{ years}$	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	$2^{127} \mu\text{s} = 5.4 \times 10^{24} \text{ years}$	$5.4 \times 10^{18} \text{ years}$
168	$2^{168} = 3.7 \times 10^{50}$	$2^{167} \mu\text{s} = 5.9 \times 10^{36} \text{ years}$	$5.9 \times 10^{30} \text{ years}$
26 characters (permutation)	$26! = 4 \times 10^{26}$	$2 \times 10^{26} \mu\text{s} = 6.4 \times 10^{12} \text{ years}$	$6.4 \times 10^6 \text{ years}$

Ataques tentam reduzir o tempo necessário para ataque de força bruta

"Quebrado" → Mais rápido que força bruta

Um pouco de história

# Cifrador de Cesar



Não é bem um cifrador, pois  
não tem chave:  
 $c := m+3 \bmod 26$

Diz-se que era utilizado pelo  
Imperador Julio Cesar

# Cifrador de César melhorado

a	e
b	f
c	g
...	...
z	d

$k = 4$ ,  
 $c :=$

Como já vimos, podemos transformar em uma cifra adicionando a chave k

$$c := m+k \bmod 26$$

# CIFRADOR DE CÉSAR



- 1) Qual o "espaço de chaves" (quantidades de chaves possíveis) do Cifrador de César "melhorado" para 26 letras?
- 2) Quantas tentativas, em média, são necessárias para decifrar a chave (força bruta)

# Cifra de substituição

a	h
b	w
c	o
...	...
z	e

$c := E(k, "bacz") = "whoe"$

$D(k, c) = "bacz"$

# CIFRADOR DE SUBSTITUIÇÃO



- 1) Qual o "espaço de chaves" ( $|K|$ ) de um cifrador de substituição com 26 letras?
  - a)  $|K| = 26$
  - b)  $|K| = 26!$
  - c)  $|K| = 2^{26}$
  - d)  $|K| = 26^2$

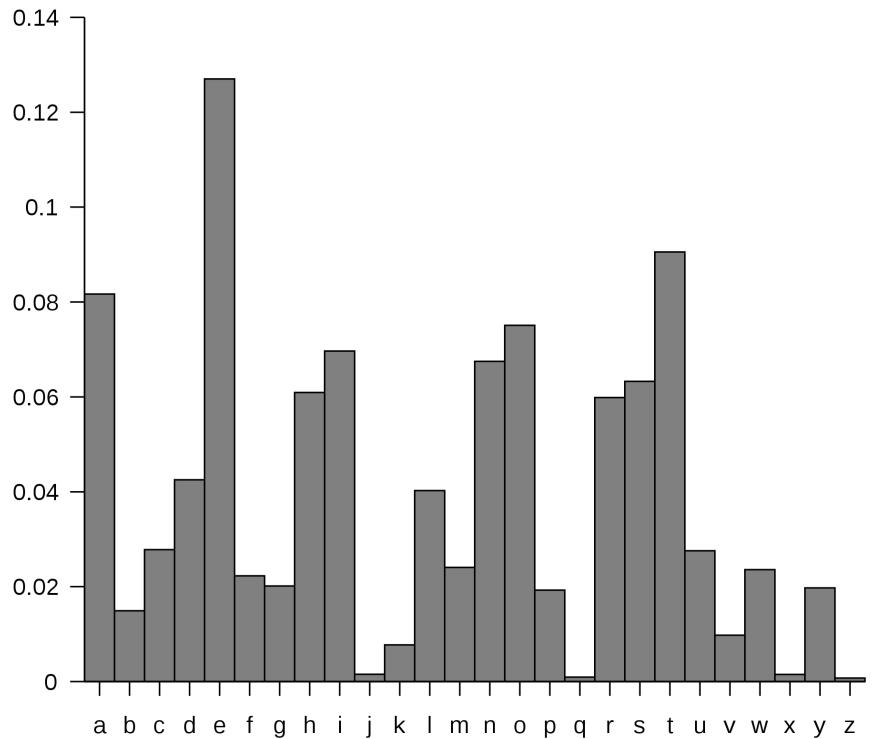
# CRIPTOANÁLISE DE CIFRA DE SUBSTITUIÇÃO



- 1) Qual a letra mais comum em textos em português?
- 2) Qual a letra mais comum em textos em inglês?

# Frequênciа de letras

- As linguagens apresentam padrões, com relativa precisão, de frequênciа de letras nos textos
- Mais do que isso, também são já conhecidos padrões de frequênciа de dígrafos, trígrafos, letras iniciais de palavras, etc.



# Criptoanálise por frequência (inglês)

- Letras mais frequentes: e, t, a, o, n, r, i, s, h, d
  - Dígrafos mais frequentes: th, he, an, re, er, in, on, at, nd
  - Letras repetidas mais frequentes: ll, ee, ss, oo, tt, ff, rr, nn, pp, cc
- 
1. Avalie a frequência de repetições do texto cifrado
  2. Substitua a com maior ocorrência (cerca de 12,7%) por "e"
  3. Substitua a segunda com maior ocorrência (cerca de 9,1%) por "t", terceira (8,1%) por "a"
  4. Verifique se as ocorrências de dígrafos são coerentes com as substituições anteriores, e faça as substituições de dígrafos ("t"->"th", "e"->"he, "re", "er")
  5. Aproveite as novas informações identificando substituições
  6. Busque palavras óbvias e identifique novas substituições

# Substituição Monoalfabética

- Exemplo que vimos é o de substituição "monoalfabética"
- Um alfabeto → outro alfabeto
- Fácil de identificar frequências de letras e utilizar para quebrar

# Enigma

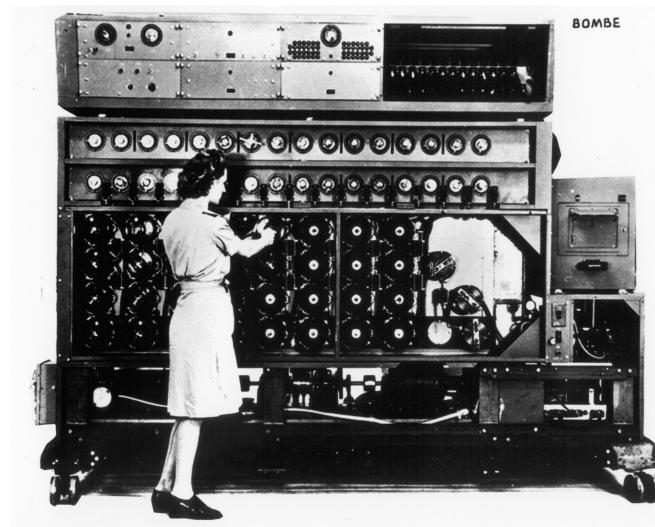
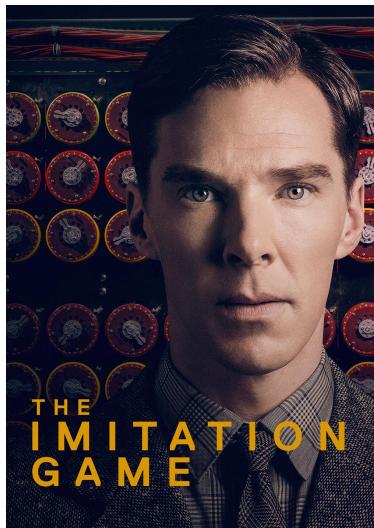


# Enigma

- Conjunto de cilindros independentes
- Cada cilindro um cifrador mono-alfabético
- Chave:
  - Ordem dos Rotores, posição inicial, posição do alfabeto, ligação do teclado, retroalimentação
  - $2^{36}$  chaves aproximadamente

<http://enigmaco.de/enigma/enigma.html>

# Enigma - como foi quebrado



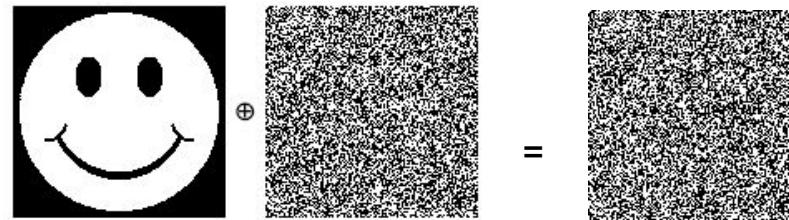
## One-Time Pad (1822)

- Chave do tamanho da mensagem
- Incondicionalmente seguro

ciphertext: ANKYODKYUREPFJBYOJDSPREYIUNOFDOIUFPLUYTS  
key: pxlmvmsydoфuyrvzwc tnlebnecvgdupahfzzlmnyih  
plaintext: mr mustard with the candlestick in the hall

ciphertext: ANKYODKYUREPFJBYOJDSPREYIUNOFDOIUFPLUYTS  
key: mfugpmiydgaxgoufhkllmhsqdqogtewbqfggyovuhwt  
plaintext: miss scarlet with the knife in the library

One-time-pad é perfeito. E two-time-pad?



=



Só pode ser usado UMA vez!!!

# Era digital...

- Governo (americano) começou a comprar produtos de criptografia e para isso definiu padrões
- DES (1974) - Data Encryption Standard
  - $|K| = 2^{56}$
  - Trabalhava com cifragem de blocos de 64 bits ao invés de letras
  - Quebrado por brute-force (tamanho de chave)

# NIST, FIPS

- *National Institute of Standards and Technology*

- "INMETRO"
- Agência não regulatória
- Organiza escolha de competições para novos padrões de algoritmos



- *Federal Information Processing Standards*

- Padrões de segurança para processamento de dados
- Agências de governo (não militar)
- Prestadores de serviço para governo



# NIST é confiável?

- Padrão NIST 800-90 (2007) com algoritmo proposto pela NSA (Dual\_EC\_DRBG) para geração de números aleatórios
- Já eram conhecidos problemas pequenos no algoritmo
- Foi encontrada uma "falha" que parecia proposital - *backdoor*?
  - Constantes do código de origem não explicada (propostos pela NSA)
  - Foi demonstrado que elas têm relação com um segundo conjunto de números - "chave mestra"
  - Apenas 32 bytes de saída do gerador são suficientes para prever próxima saída
  - Questão: Alguém conhece a "chave mestra"?
  - 2013: NYT: Memorando vazado por Snowden comprova teoria de *backdoor*

Lição: 1) Confie na comunidade, e naquilo que é mais usado e testado.  
2) Não confie naquilo que já se sabe que tem pequenas falhas.

# Outras referências...

- *European Telecommunications Standards Institute*
  - União Européia
  - Referência na área de Assinatura Digital avançada
- *Bundesamt für Sicherheit in der Informationstechnik*
  - Avalia e recomenda algoritmos e tamanhos de chaves criptográficas
- *Instituto de Tecnologia da Informação*
  - Operação da AC Raiz brasileira (Casa Civil)
- *Comitê Gestor ICP-Brasil*
  - Órgão colegiado responsável pela normatização de assinatura digital no Brasil (governo+sociedade civil)



# 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

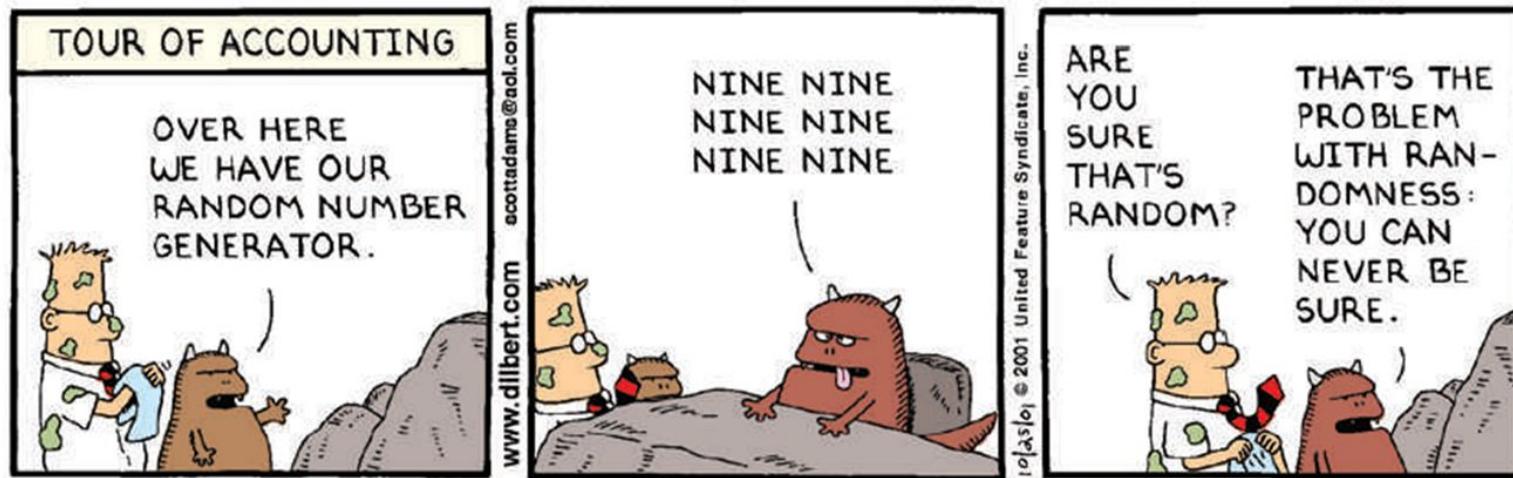
# Casos famosos...

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.



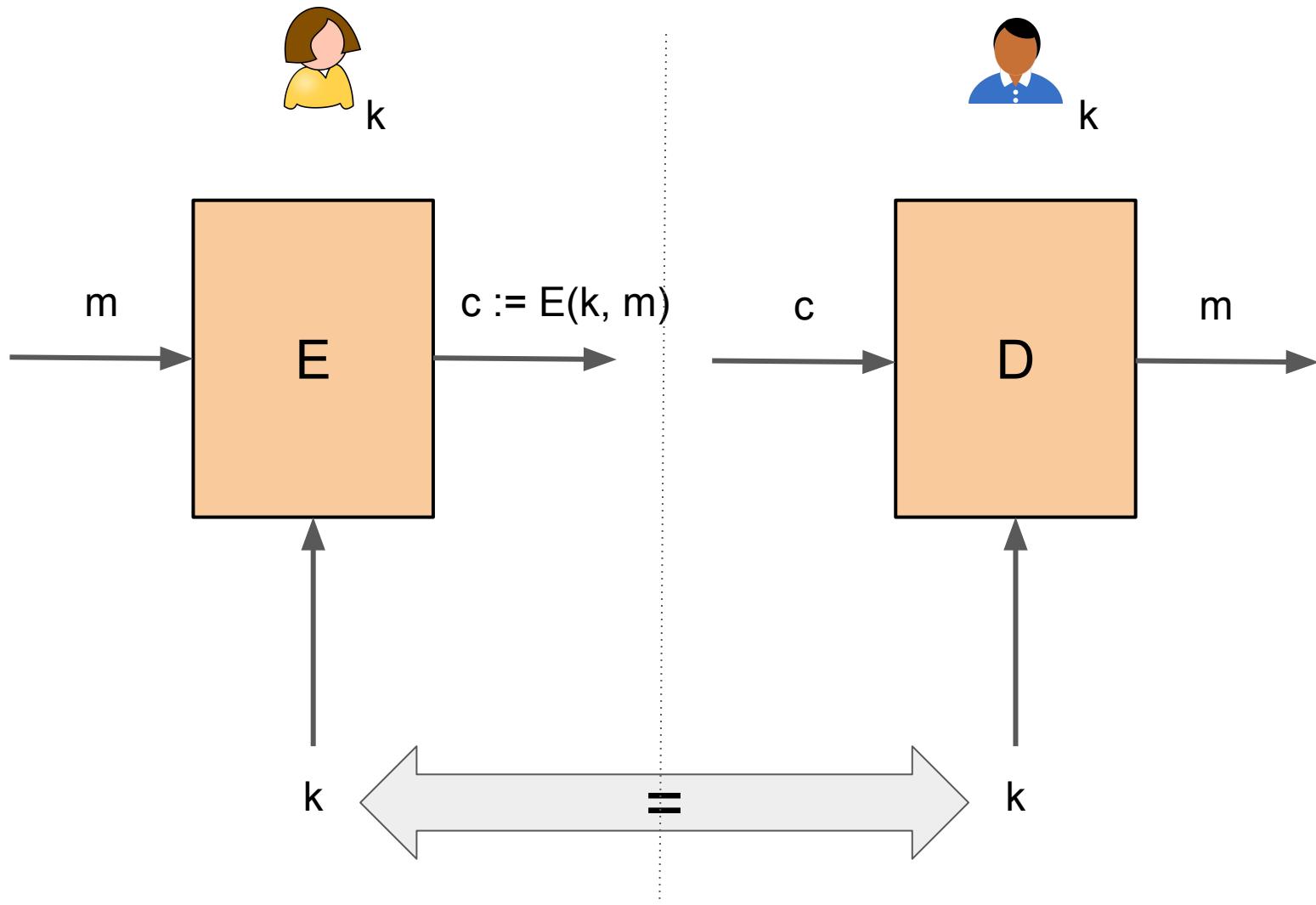
Um horário, além de ser um péssimo *seed*, é informação pública e impressa em relatório da urna!

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

# Cifradores simétricos

# 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

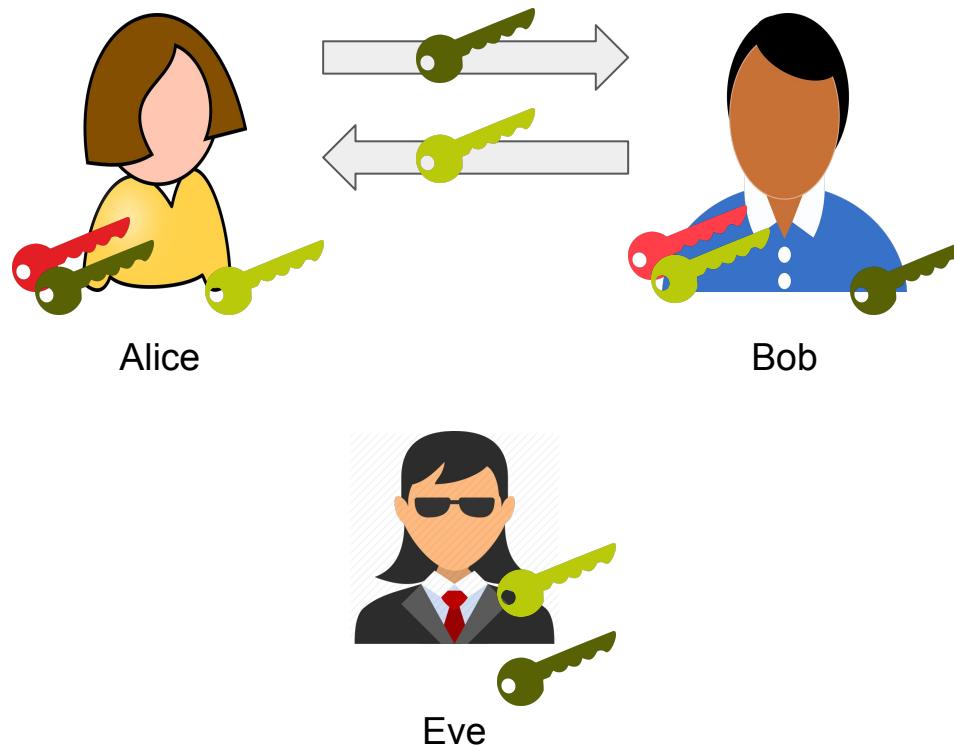
# Como distribuir a chave simétrica?

- Canal seguro?
  - Exemplo: entregar em mãos
- Porque não usar o canal seguro pra mensagem?
  - A chave pode ser utilizada várias vezes
- Qual o problema?
  - Caro e muitas vezes impraticável!
- Seria bom poder distribuir a chave *em claro...*

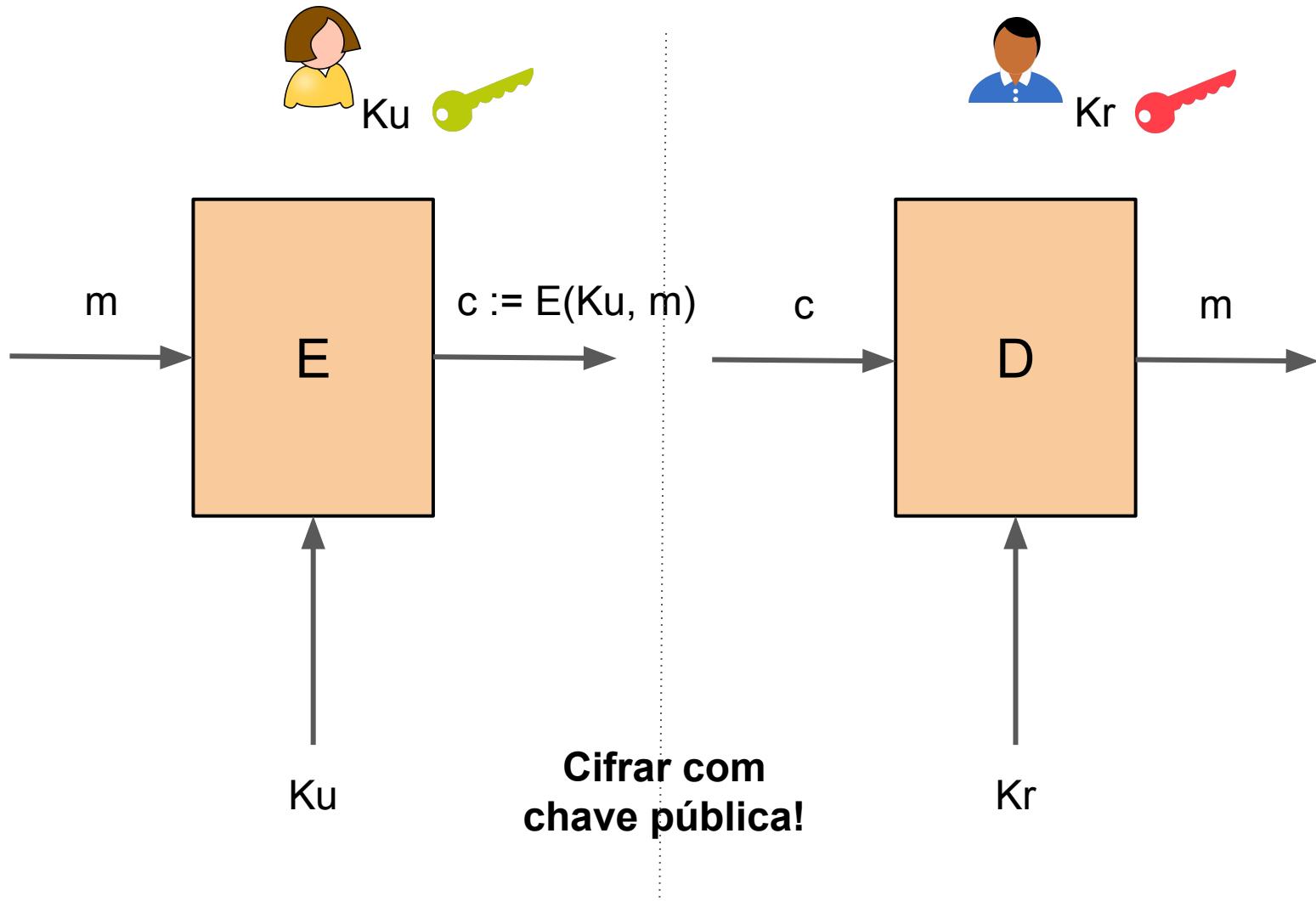


# Seria bom... e é!

- Criptografia **assimétrica**: Chave privada ( $K_p$ ) x Chave pública ( $K_u$ )
- Chave privada "desfaz" aquilo que foi feito com chave pública
- Chave pública não permite recuperar chave privada



# Cifragem assimétrica



# Algoritmo de cifragem assimétrica

- RSA
- Elliptic curves

# PORQUE AINDA SE USA SIMÉTRICA?



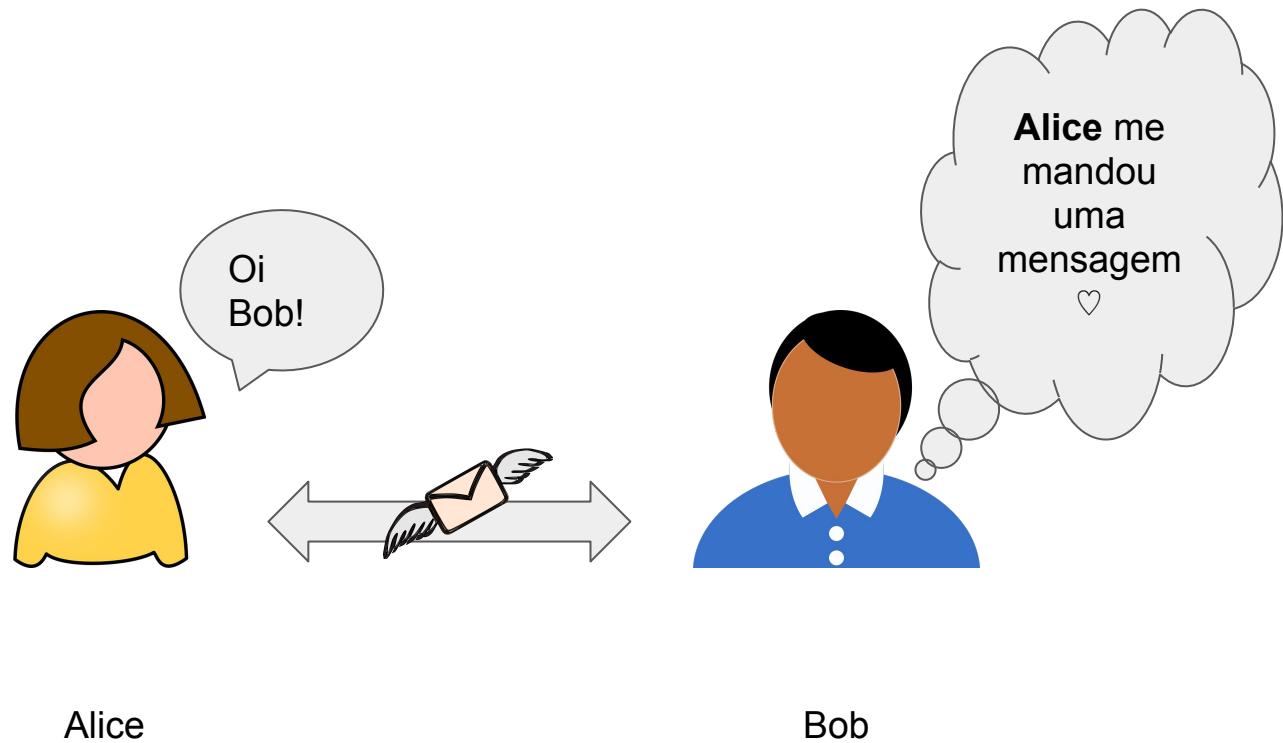
- 1) Se a criptografia assimétrica resolve o problema, porque se usa a simétrica?

# Porque usar cifragem simétrica então?

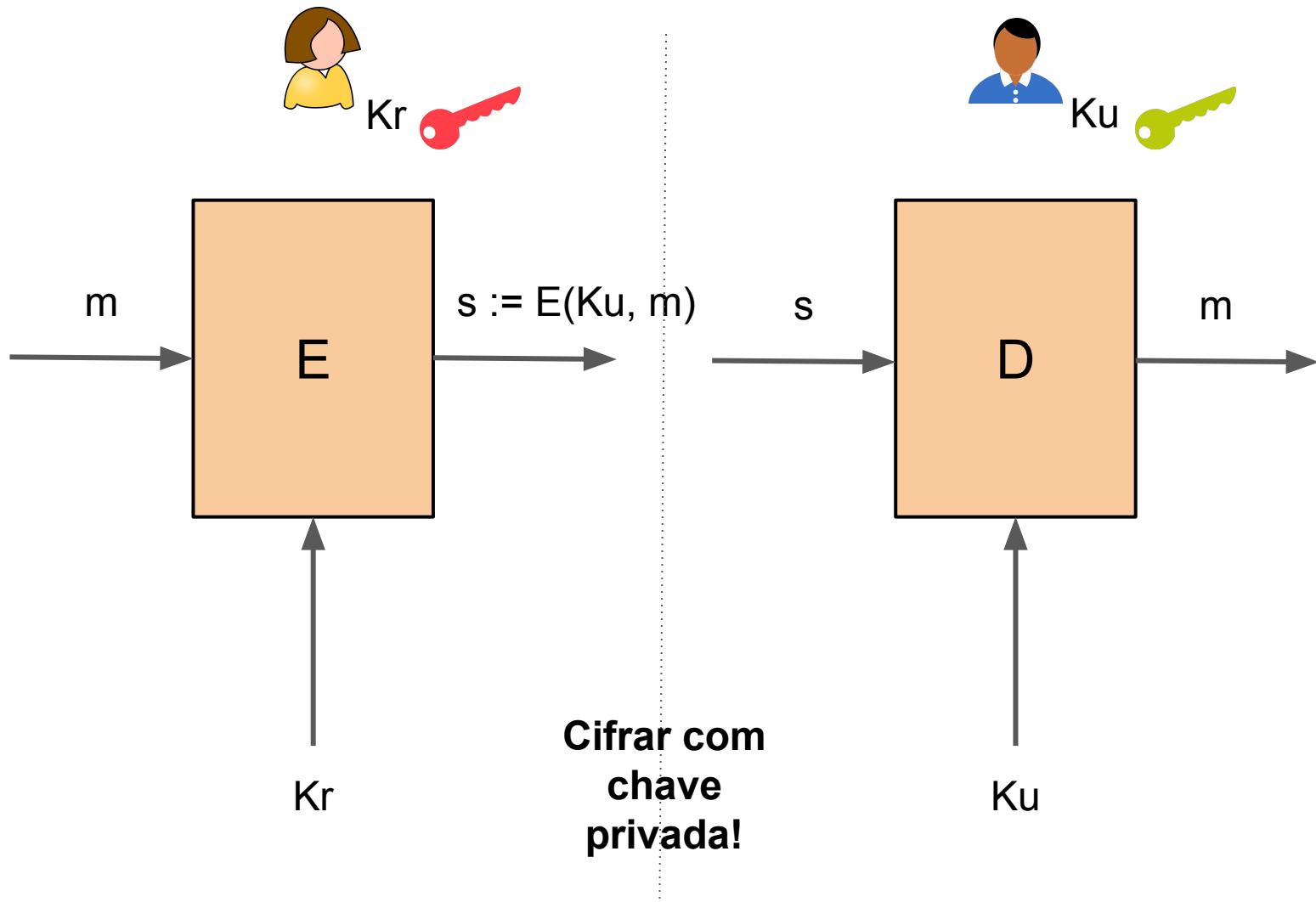
- Criptografia assimétrica é geralmente mais lenta
- Criptografia assimétrica exige chaves maiores
- Criptografia assimétrica tem maior complexidade matemática/computacional e custo de memória

Tipicamente, usa-se criptografia assimétrica para o *acordo de chave simétrica*.

# Autenticidade e não repúdio



# Assinatura utilizando cifragem assimétrica



# Hash (Resumo Criptográfico)

# O que é um *hash* - resumo criptográfico

- Função de caminho único
- Tamanho de um hash -  $|H(\cdot)|$  - é fixo
- Produz uma *impressão digital* de uma mensagem

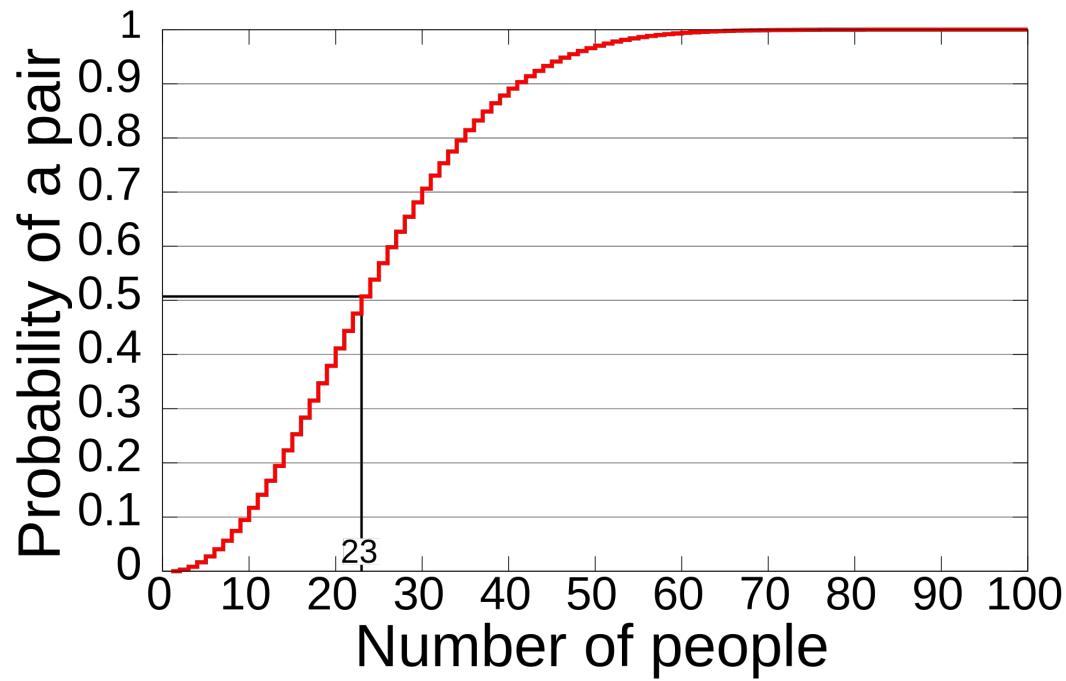
# O que é um *hash* - resumo criptográfico

- Requisitos:
  - Fácil de computar para qualquer  $m$
  - É impossível achar  $m$  tendo  $H(\cdot)$  → não inversível
  - Efeito avalanche / aleatoriedade
  - Resistência a colisão/ataques de pré-imagem

# Ataque de colisão

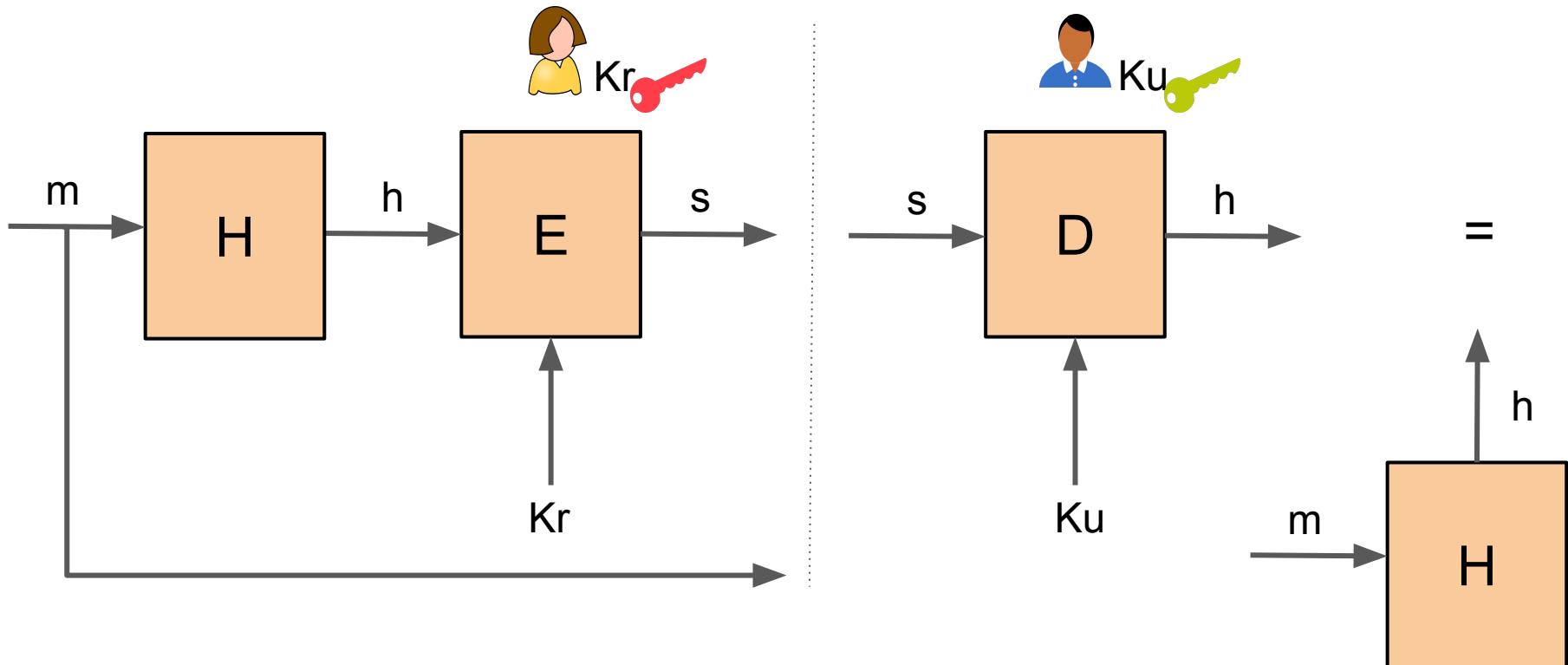
- $|m|$  variável,  $|H(\cdot)|$  fixo  $\rightarrow$  se  $|m| > |H(\cdot)|$ , então há colisão!
- Deve ser difícil encontrar  $x$  e  $y$  quaisquer tal que  $H(x) = H(y)$
- Resistência a colisão não significa que não existem colisões
- *Paradoxo do aniversário*: necessário calcular  $2^{n/2}$  mensagens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

# "Paradoxo" do aniversário



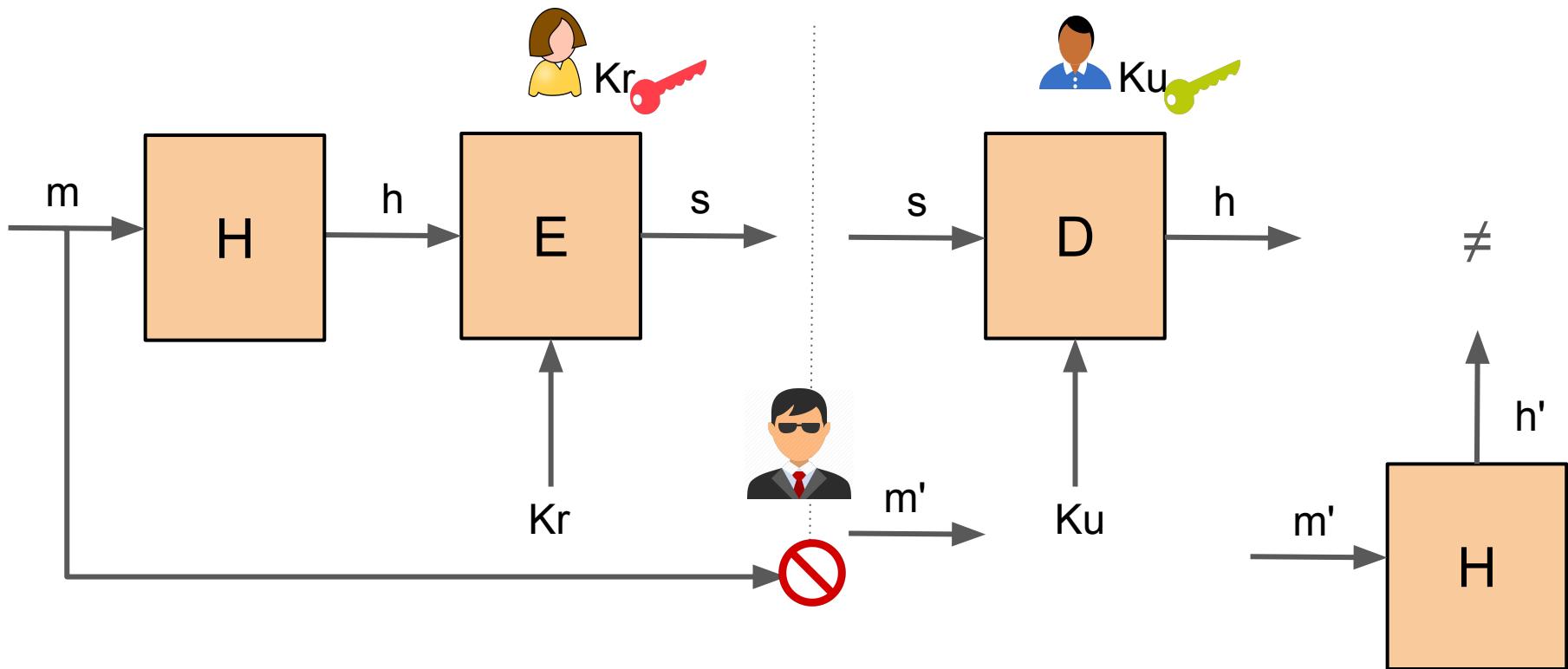
# Hash e assinatura digital

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



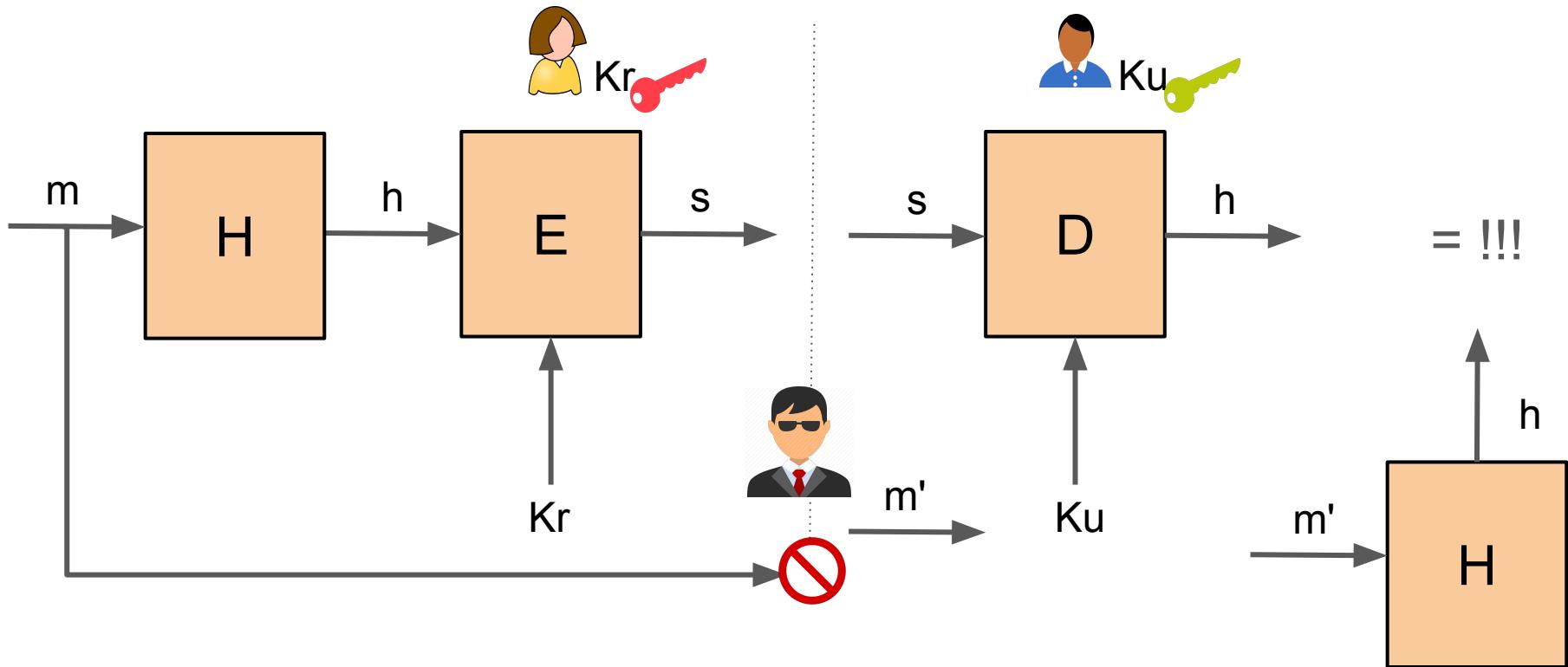
# Assinatura Digital e 2<sup>a</sup> pré imagem

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



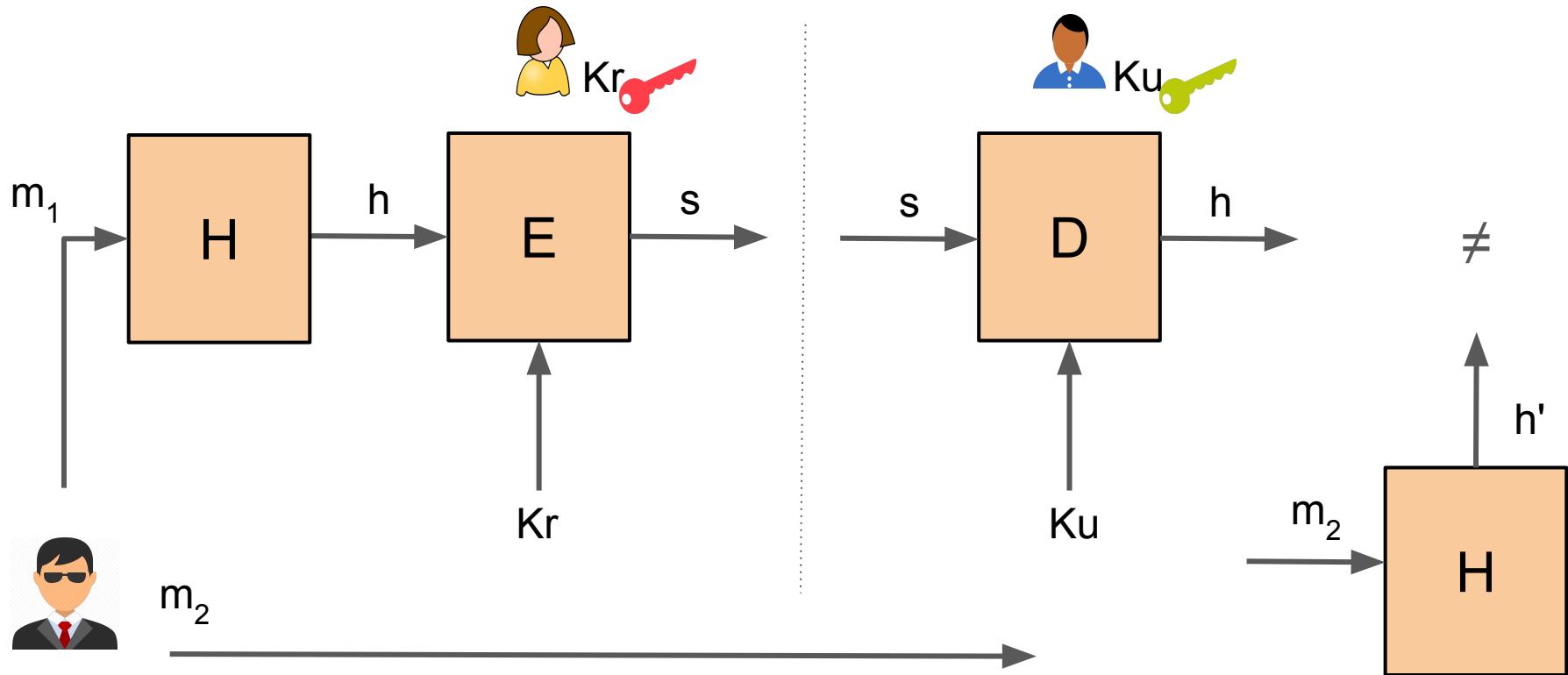
# Assinatura Digital e 2<sup>a</sup> pré imagem

- Se Mallory conseguisse, poderia substituir o documento assinado!



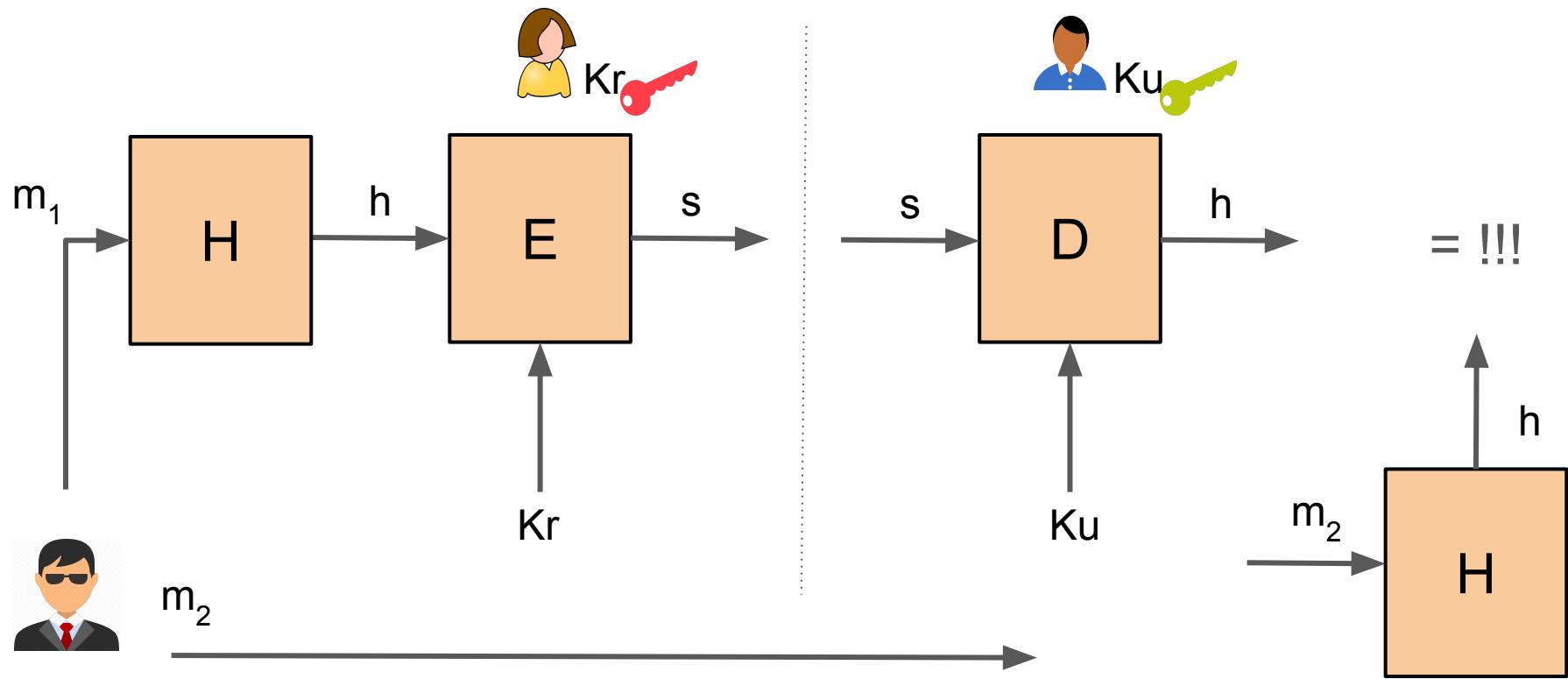
# Assinatura Digital e colisão

- Mallory não consegue gerar  $m_1$  e  $m_2$ ,  $m_1 \neq m_2$  que tenha mesma assinatura (*hash*)



# Assinatura Digital e colisão

- Se conseguisse, poderia convencer Alice a assinar uma versão do documento e entregar a Bob a outra versão



# Na prática...



MD5 (foto1.jpg) = 253dd04e87492e4fc3471de5e776bc3d  
MD5 (foto2.jpg) = 253dd04e87492e4fc3471de5e776bc3d

# Ataques ao MD5

- Colisão pode ser encontrada em segundos em computador comum ( $2^{24}$ )
- Ataque de "prefixo escolhido" em horas ( $2^{39}$ )
- Continua sendo muito utilizado, apesar disso!
  - <https://blog.silentsignal.eu/2015/06/10/poisonous-md5-wolves-among-the-sheep/>
- Flame
  - Microsoft tinha um certificado confiável com permissão de *code signing* que utilizava MD5
  - Foi criada uma versão modificada do mesmo para assinar componentes do Vírus

# Algoritmos

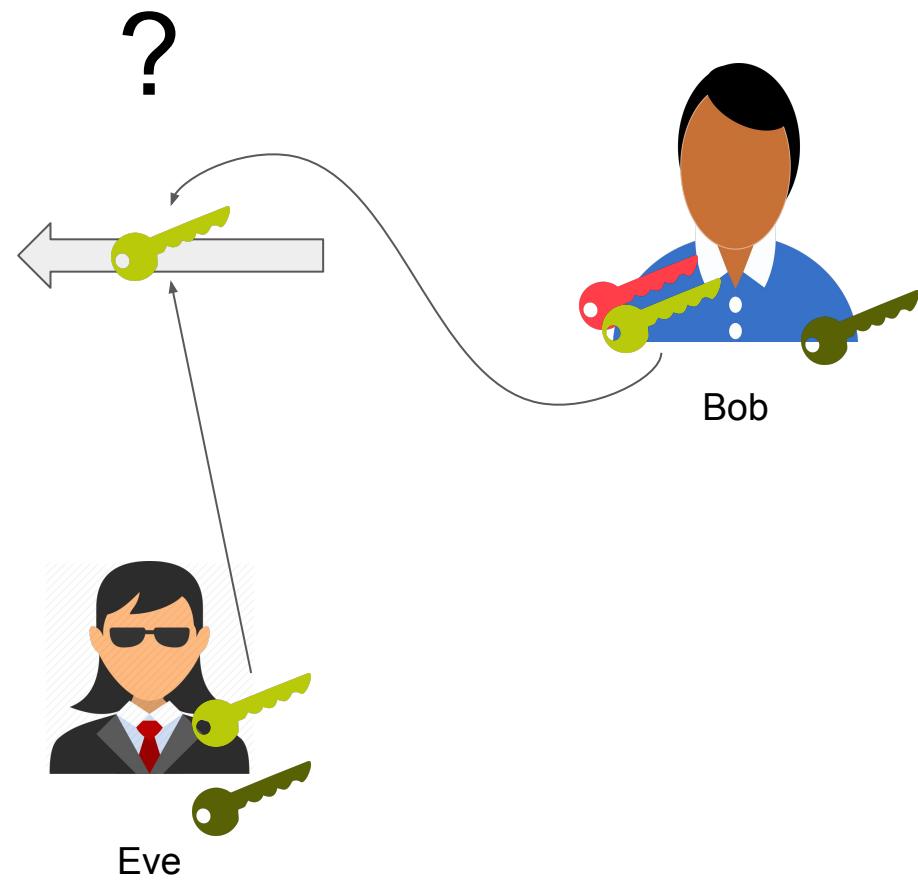
- MD5 - Quebrado, não use!
- SHA1 - Pare de usar!
  - Deadline do NIST foi em 2010
  - Ataques teóricos conhecidos
  - Ataque prático iminente
- SHA2 - OK!
  - Família de *hashes*: SHA-256 e SHA512
- SHA3 - Migrar para...
  - Escolhido por competição pública
- Whirlpool
  - Desenvolvido por Barreto (USP) e Vincent Rijmen (criador do AES)
  - Padrão ISO

# Certificado Digital

# 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

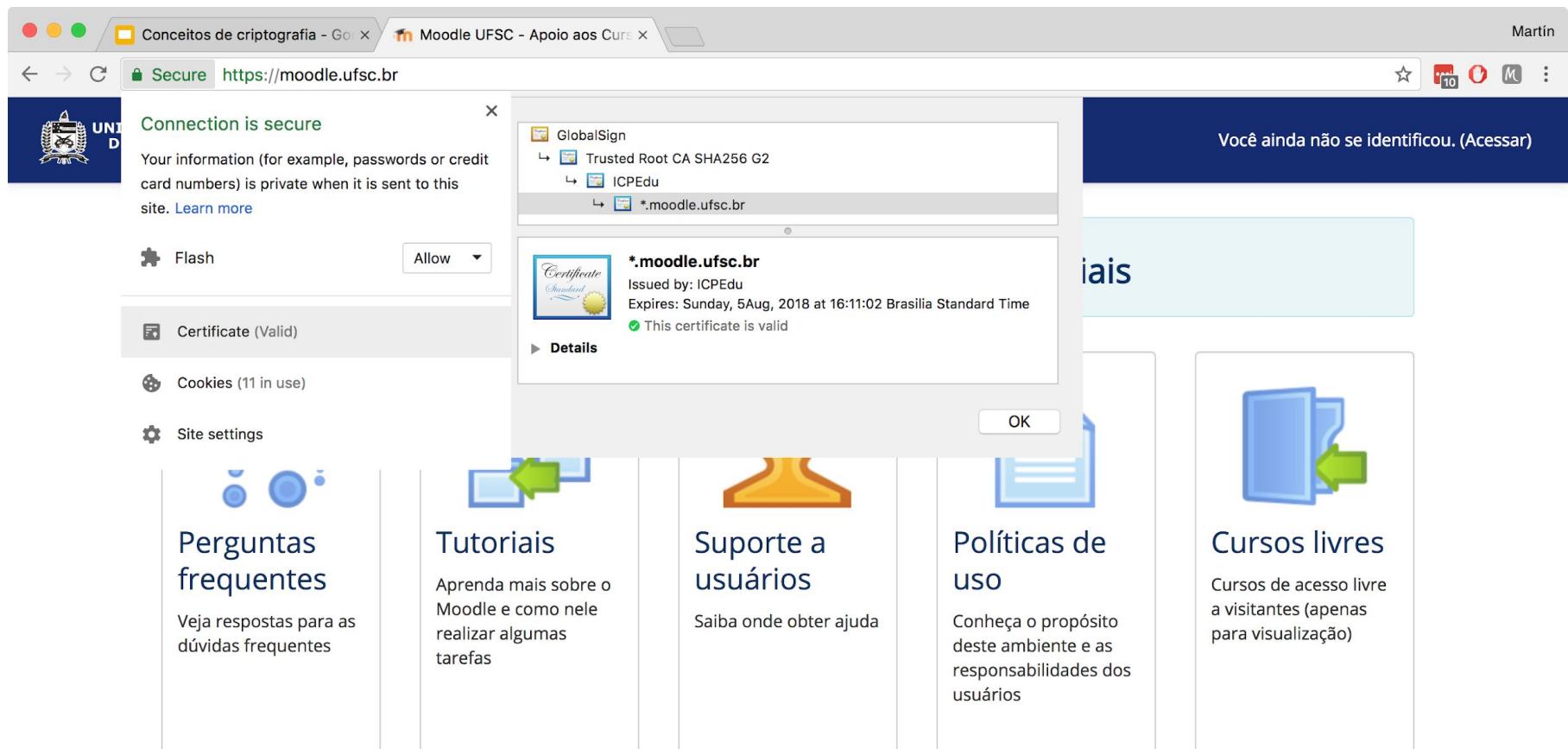
Políticas de uso Conheça o propósito deste ambiente e as responsabilidades dos usuários

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)

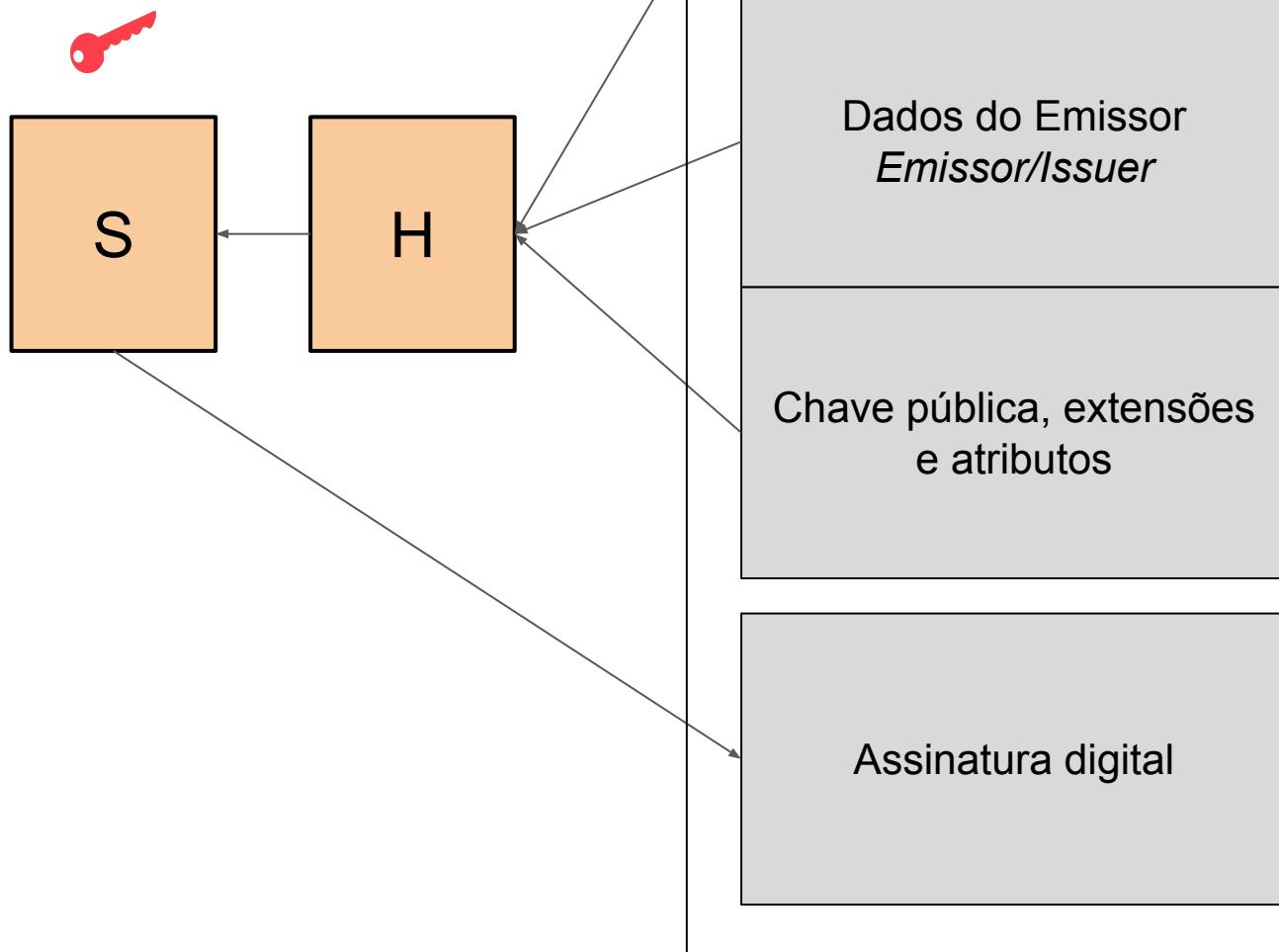


:: Este é o Moodle UFSC - Apoio aos Cursos Presenciais. Consulte a [lista de implantações de Moodle da UFSC](#) para ver outras opções.

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?

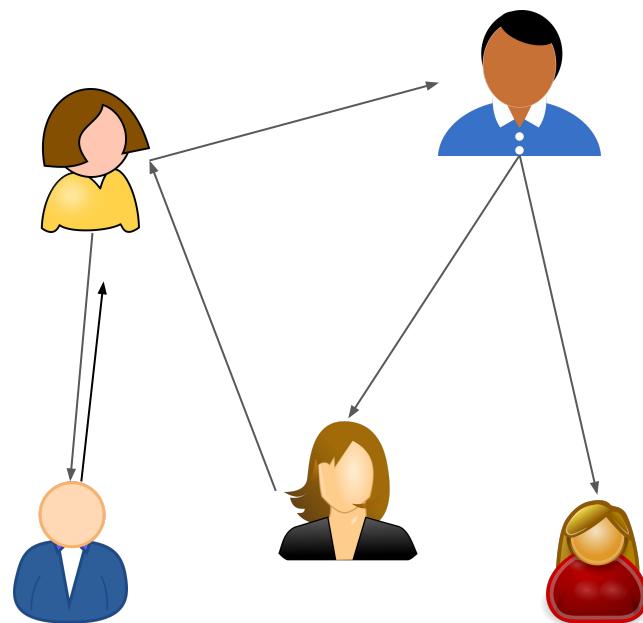
E se eu perder o controle da minha chave privada?

**ICP**

# ICP - Infraestrutura de Chaves Publicas

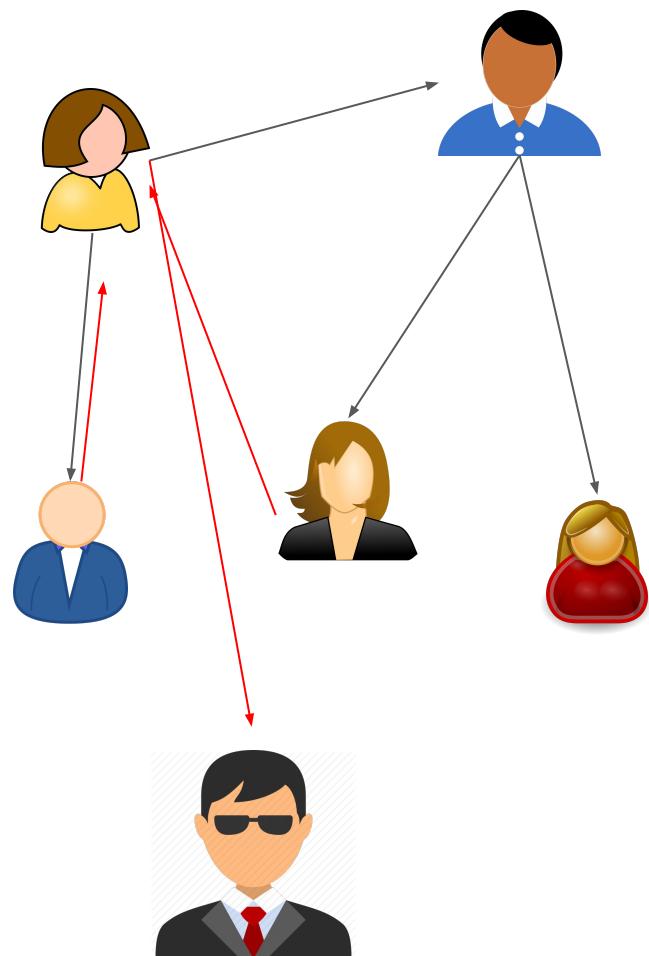
- *PKI* - Public Key Infrastructure
- Conjunto de políticas, procedimentos, papéis e sistemas para gestão de chaves públicas
- Emissão, revogação, publicação de certificados

# 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

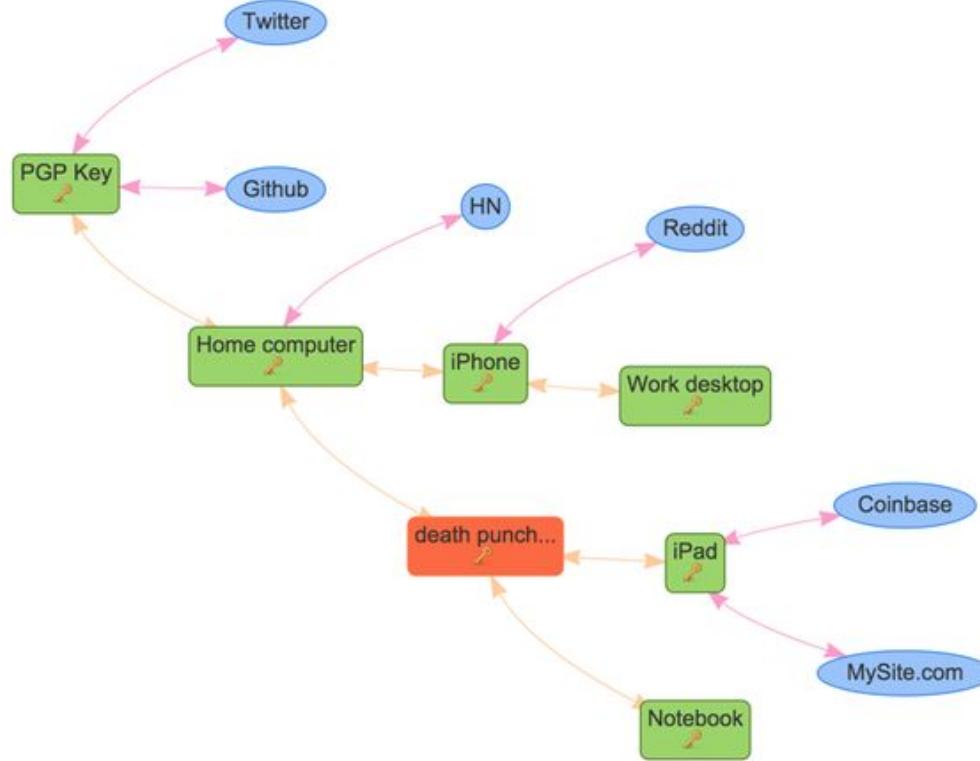


HOW TO USE PGP TO VERIFY  
THAT AN EMAIL IS AUTHENTIC:

LOOK FOR THIS  
TEXT AT THE TOP?



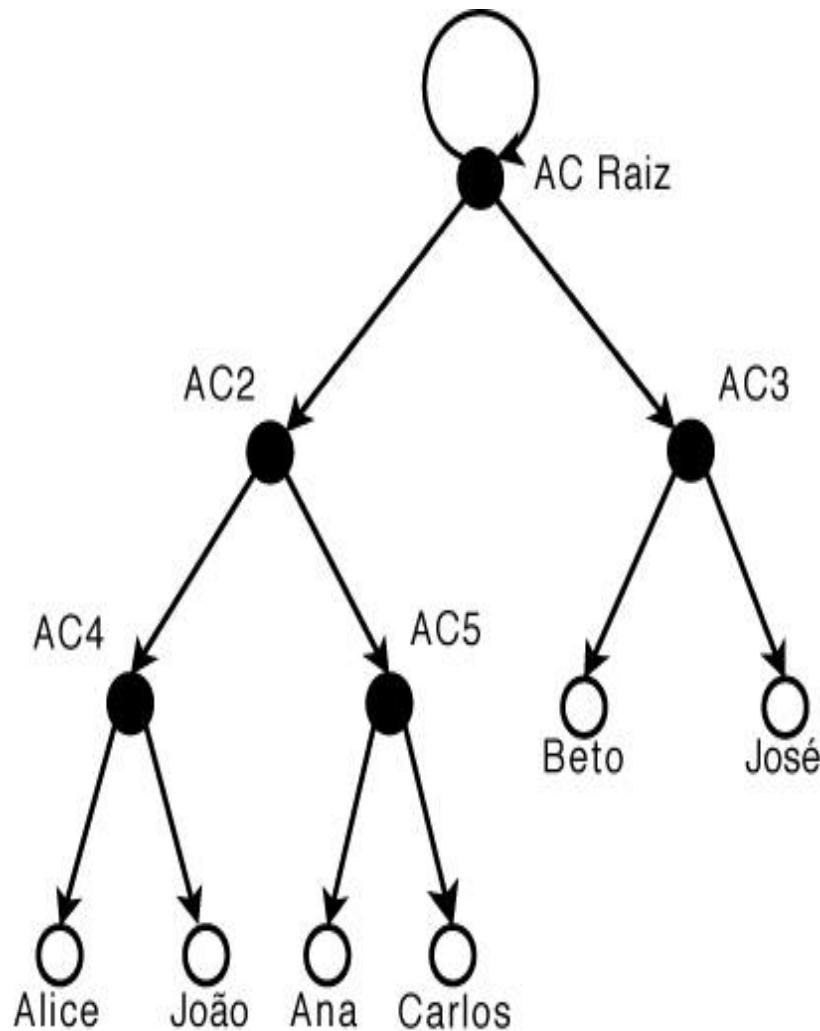
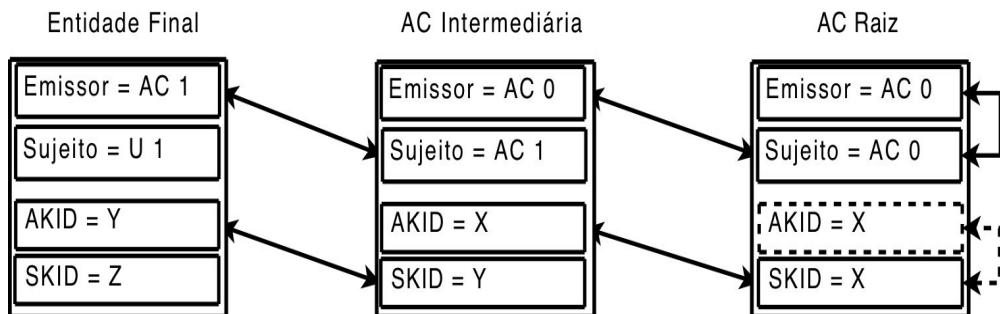
# KeyBase



<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.

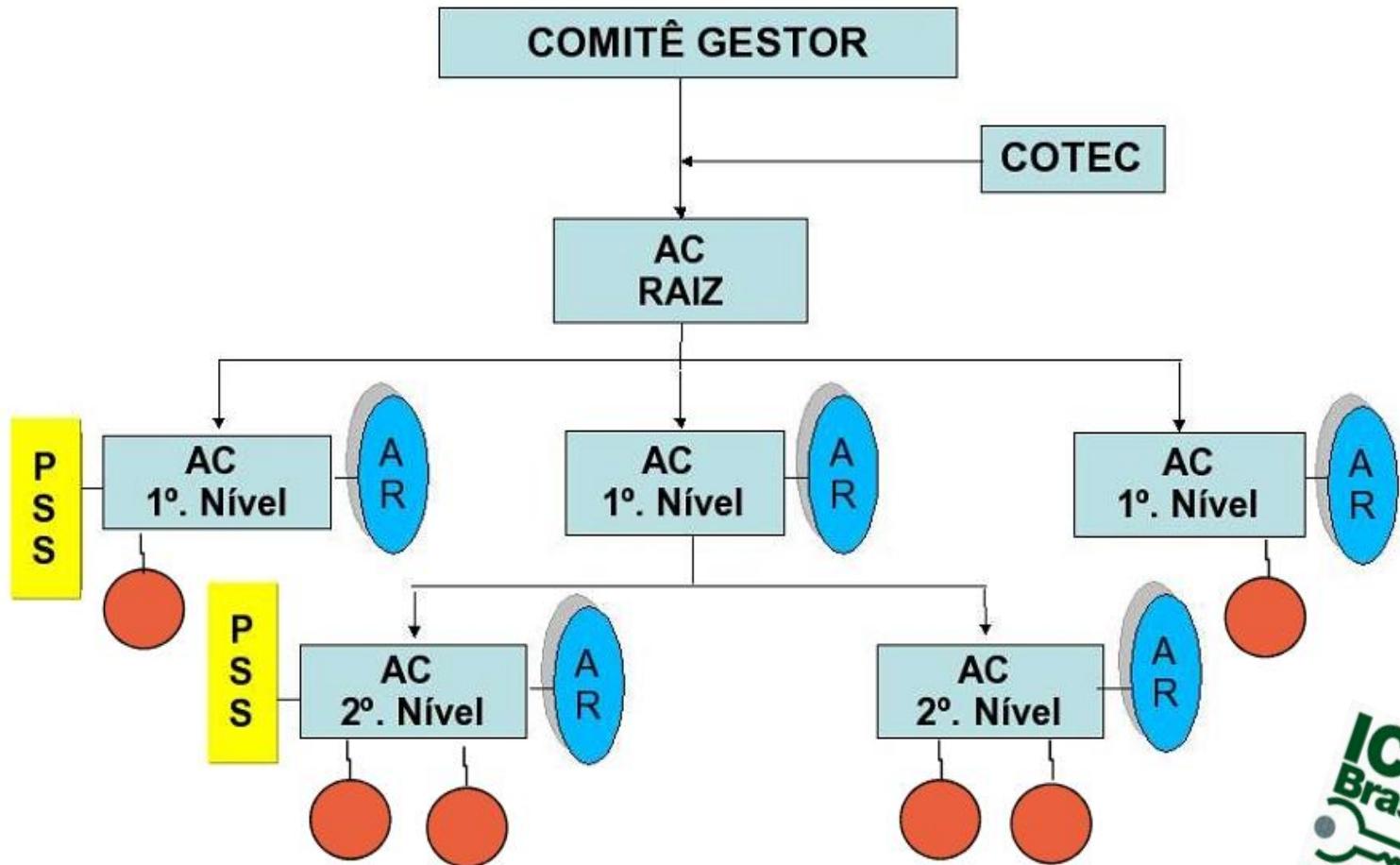
**O PRESIDENTE DA REPÚBLICA**, no uso da atribuição que lhe confere o art. 62 da Constituição, adota a seguinte Medida Provisória, com força de lei:

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



mundo real



mundo virtual



Autoridade de Registro