Fundamentos de Segurança Informática (FSI)

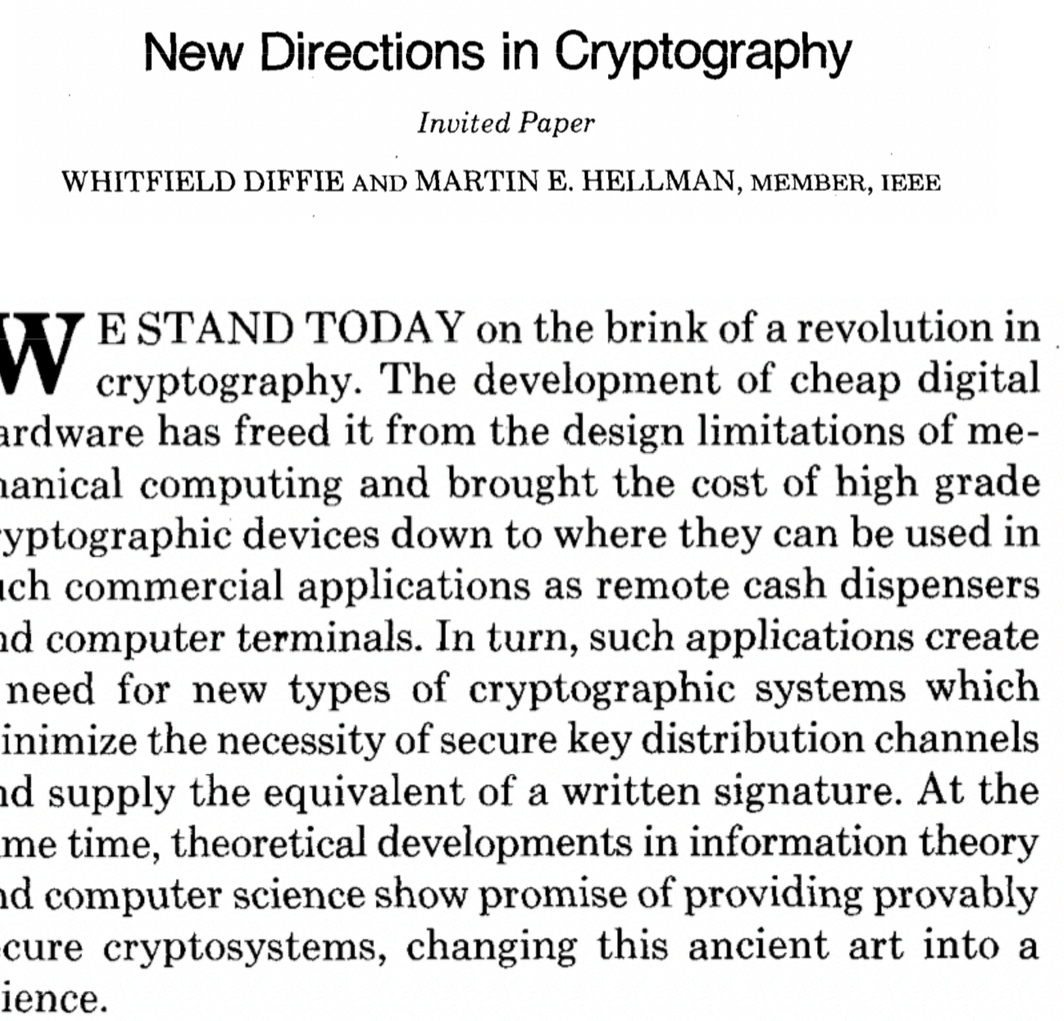
2021/2022 - LEIC

Manuel Barbosa
mbb@fc.up.pt

Aula 16
Criptografia: Parte 3

Criptografia de Chave Pública

- Revolução nos anos 70
  - antes: apenas criptografia simétrica
  - chaves pré-partilhadas
  - Entre 1975 e 1978 surgem:
    - cifras de chave pública
    - assinaturas digitais
    - acordos de chave



New Directions in Cryptography

Invited Paper

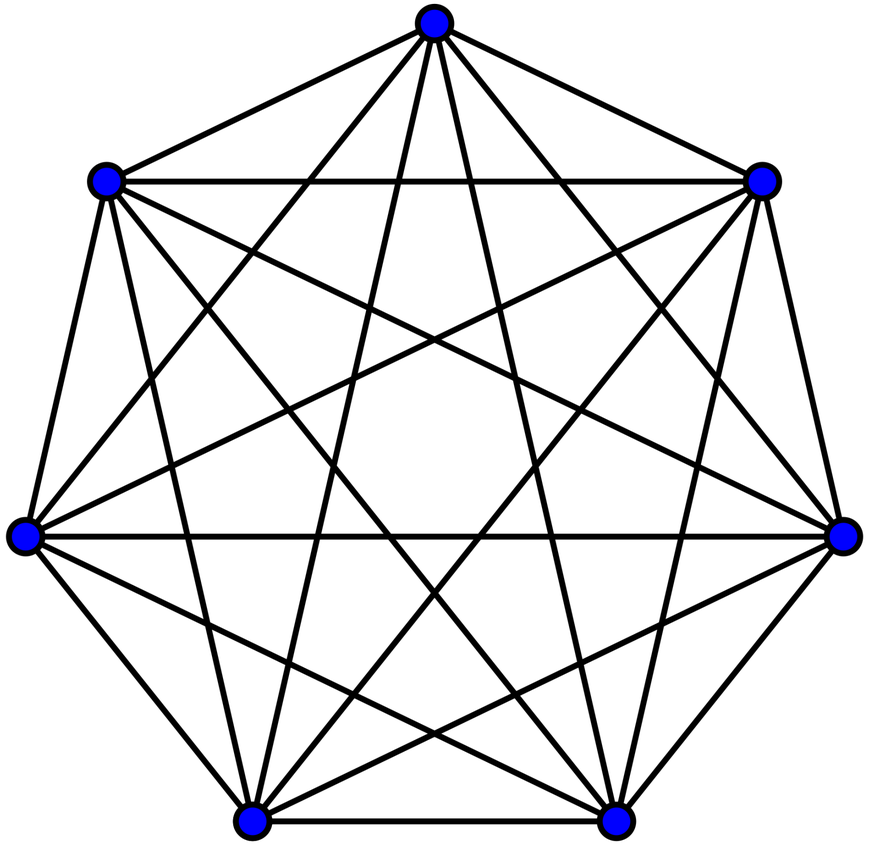
WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

WE STAND TODAY on the brink of a revolution in cryptography. The development of cheap digital hardware has freed it from the design limitations of mechanical computing and brought the cost of high grade cryptographic devices down to where they can be used in such commercial applications as remote cash dispensers and computer terminals. In turn, such applications create a need for new types of cryptographic systems which minimize the necessity of secure key distribution channels and supply the equivalent of a written signature. At the same time, theoretical developments in information theory and computer science show promise of providing provably secure cryptosystems, changing this ancient art into a science.

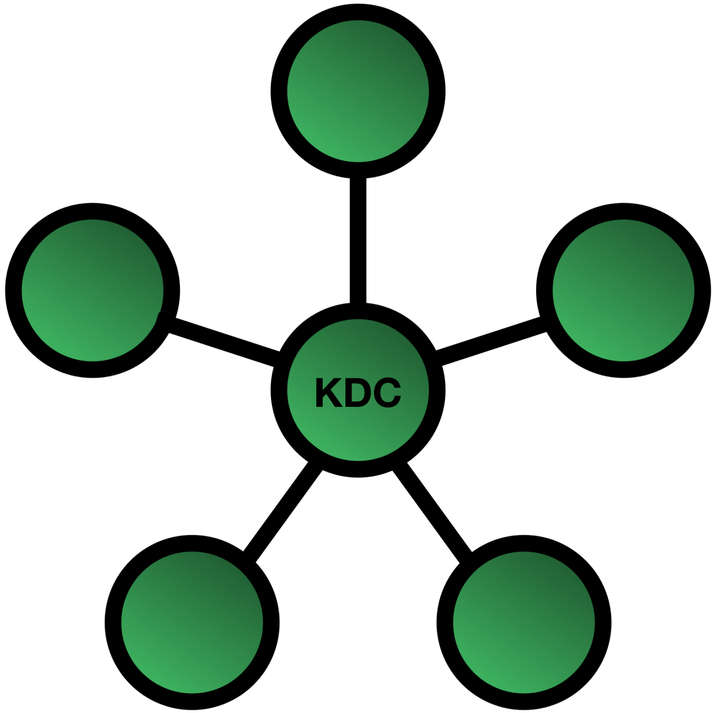
https://ee.stanford.edu/~hellman/publications/24.pdf

Gestão de Chaves

- Com criptografia simétrica:
  - N agentes
    - solução ad-hoc => N(N-1)/2 chaves
  - Pré-distribuição de chaves
    - distribuição manual?
    - como adicionar um novo agente?



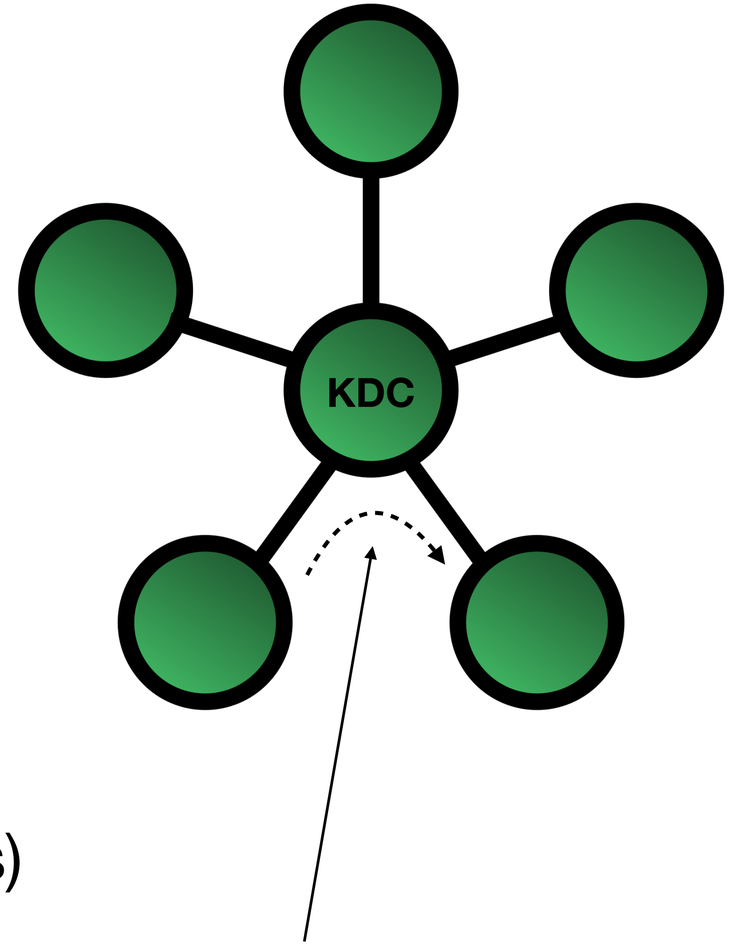
Gestão de Chaves: Sistemas Fechados



- Com criptografia simétrica:
  - N agentes (contexto bem definido)
    - solução centralizada => N chaves
  - Key Distribution Center
    - armazena 1 chave de longa duração partilhada com cada agente
    - como adicionar um novo agente?
    - como comunica o agente A com o agente B?

Gestão de Chaves: Sistemas Fechados

- Com criptografia simétrica:
  - N agentes (contexto bem definido)
    - solução centralizada => N chaves
  - Key Distribution Center
    - utilizado de forma generalizada (e.g., Kerberos)
    - sempre on-line => ponto central de falha



Chaves de longa duração:
- canais seguros entre cada agente e o KDC
- permitem estabelecer chaves de curta duração entre pares de agentes

Chaves de sessão

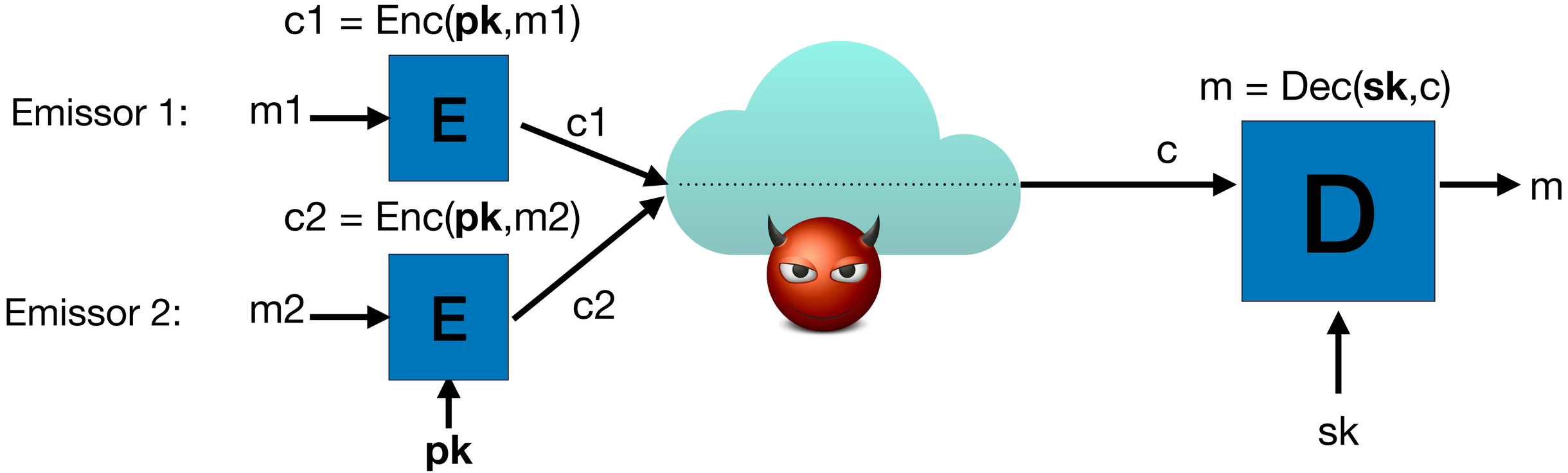
- Os sistemas modernos distinguem
  - chaves de longa duração <> chaves de sessão
  - chaves de sessão: efémeras, danos limitados se comprometidas
  - chaves de longa duração:
    - requisitos fortes de segurança no armazenamento
    - exemplo: Hardware Security Module, *smartcard*, etc.

Limitações com a criptografia simétrica

- quando é possível viver sem criptografia de chave pública
  - excelente! usamos criptografia simétrica => economia de mecanismos
- problema #1: chaves simétricas de longa duração pré-partilhadas
  - em sistemas abertos assíncronos => cifras de chave pública
  - em sistemas abertos síncronos => acordos de chave + assinaturas digitais
- problema #2: não repúdio (como implementar com criptografia simétrica?)
  - em sistemas abertos => assinaturas digitais

Cifras de chave pública

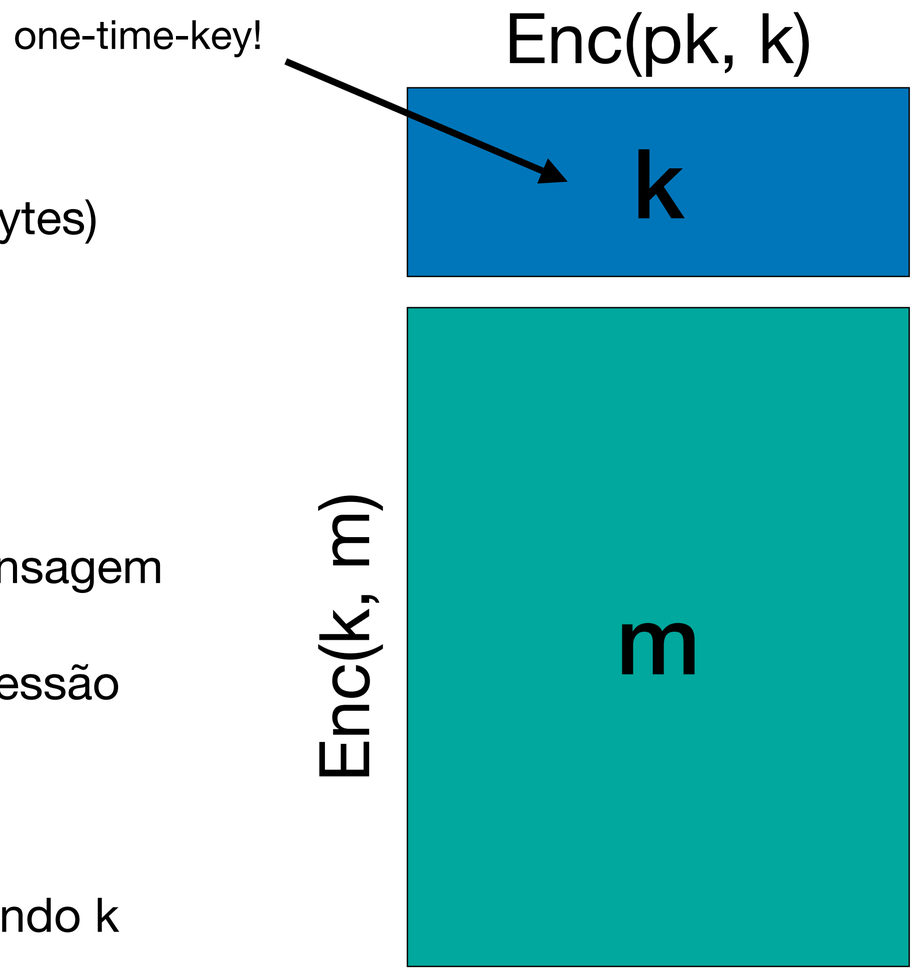
- Ferramenta para gerir chaves simétricas



- E, D: algoritmos (encrypt, decrypt) => **públicos e standard!!!**
- pk: chave pública para cifrar; sk => chave secreta para decifrar

Cifras de chave pública

- Muito mais ineficientes do que cifras simétricas
  - chaves assimétricas: milhares de bits (vs 128 bits)
  - apenas viável cifrar mensagens muito pequenas (dezenas de bytes)
  - payload: chave simétrica
- Paradigma híbrido (e.g., email S/MIME):
  - emissor gera chave de sessão simétrica e usa-a para cifrar mensagem
  - emissor conhece chave pública do recetor pk: cifra chave de sessão
  - receptor obtém dois criptogramas:
    - recupera 1) chave de sessão k usando sk 2) mensagem usando k



Cifras de chave pública

- Como construir cifras de chave pública?
  - Muitas opções hoje em dia
  - Construção conceptualmente simples:
    - começar por um objeto matemático
    - “permutação unidirecional com alçapão”
    - ou: one-way trapdoor permutation

One-way trapdoor permutation

KeyGen: produzir pk, sk

Eval: $y = F(pk,x)$

Invert: $x = F^{-1}(sk,y)$

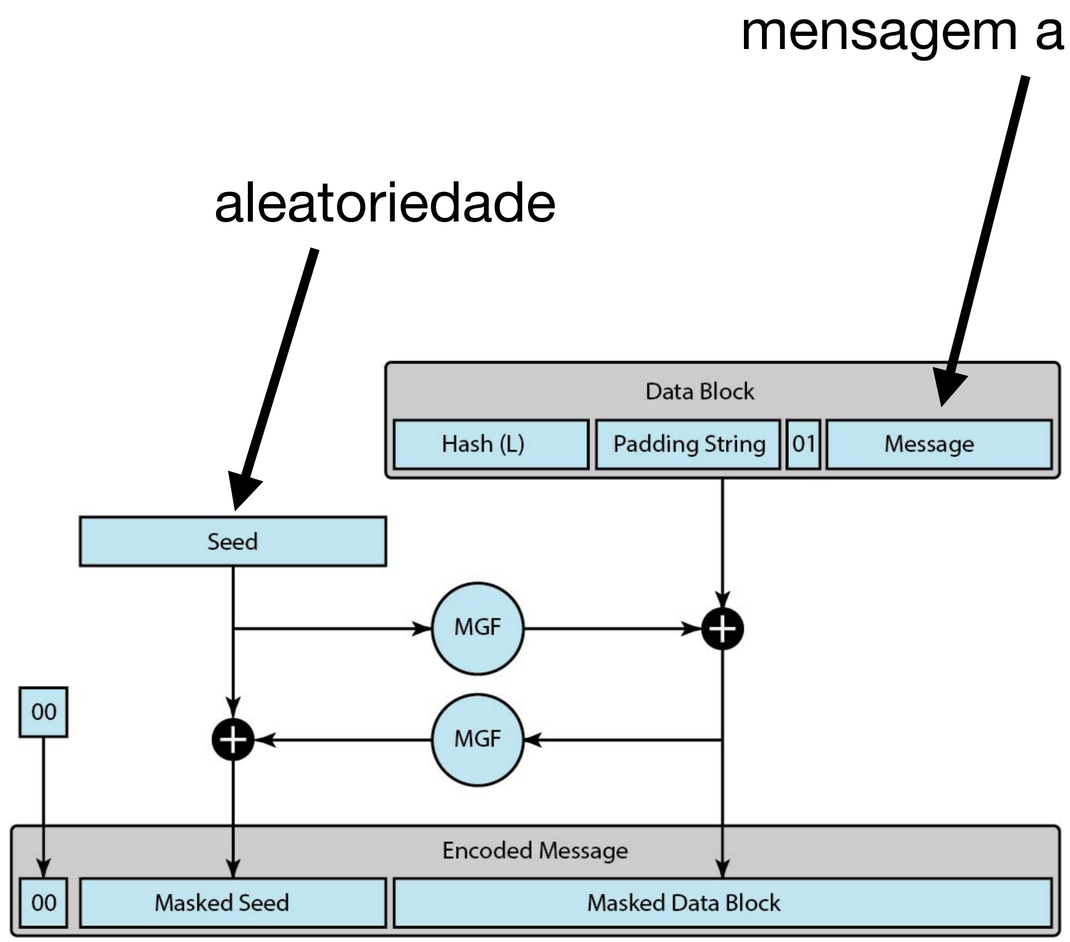
Permutação:
- conhecendo sk
- dado F(pk,x)
- é possível recuperar x

One-way:
- se x for aleatório
- F(pk,x) é difícil de inverter
- mesmo conhecendo pk

OAEP Encryption

- Como construir cifras de chave pública?
  - Muitas opções hoje em dia
  - Construção conceptualmente simples:
    - começar por um objeto matemático
    - “permutação unidirecional com alçapão”
    - ou: one-way trapdoor permutation
    - codificar x de maneira “inteligente”

valor x a colocar em F(pk,x)

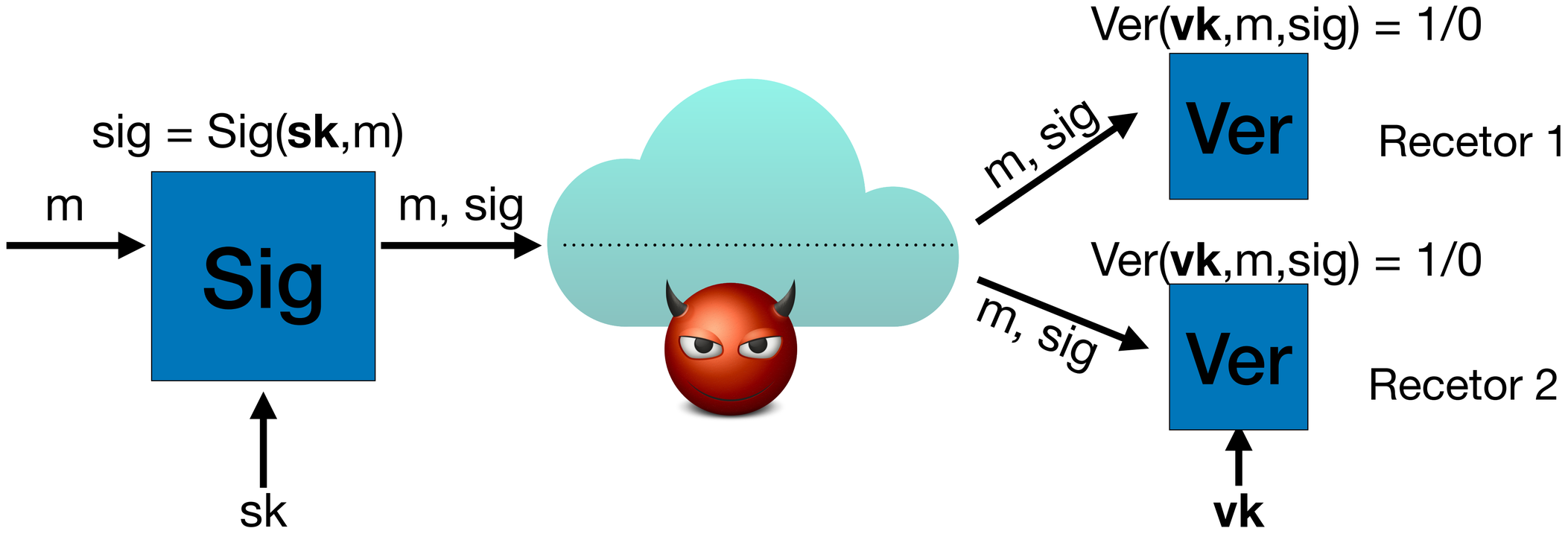


Exemplo de *trapdoor permutation*

- Função RSA (Rivest, Shamir, Adleman 1977)
  - escolher dois primos grandes p, q (hoje > 2048 bits cada)
  - calcular: `n = p*q` `v = (p-1)*(q-1)`
  - escolher expoente público `e`, e.g., `e = 0x10001`
  - calcular `d` tal que: `(d*e) mod v = 1, em que (mod = %)`
  - chave pública: `(e, n)` chave secreta: `(d, n)`
  - $F(pk,x) := x^e \bmod n$ $F^{-1}(sk,y) := y^d \bmod n$

Assinaturas Digitais

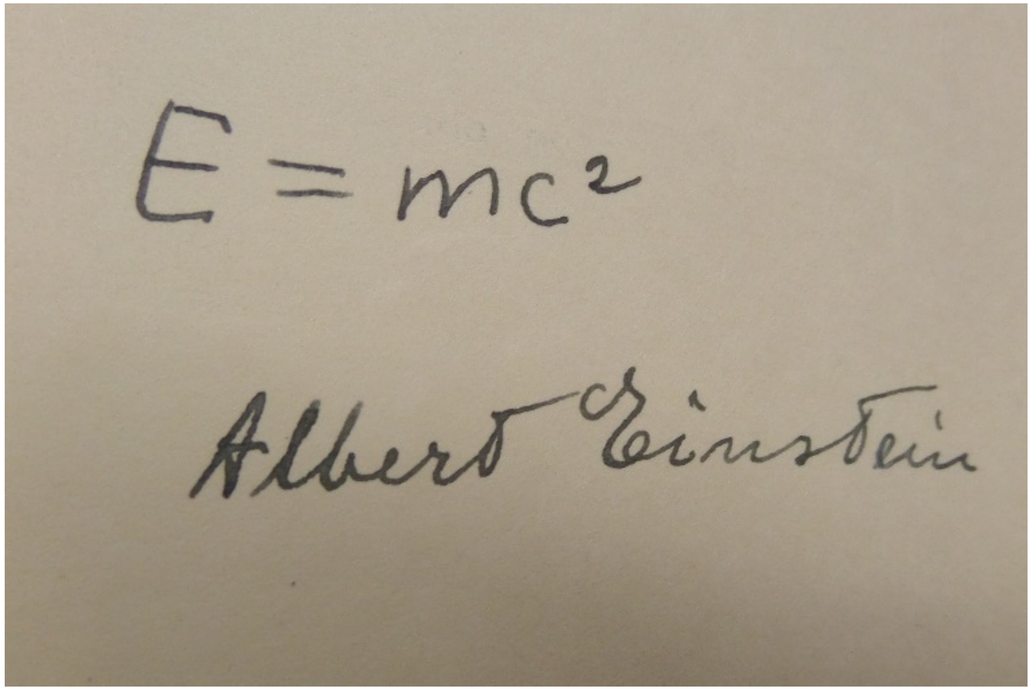
- Equivalente eletrónico às assinaturas manuscritas



- Sig, Ver: algoritmos (sign,verify) => **públicos e standard!!!**
- sk: chave de assinatura; vk => chave (pública) de verificação

Assinaturas Manuscritas

- Que propriedades lhes atribuímos?
  - Não: falsificável, reutilizável, repudiável
  - Garantia de autoria do documento/acordo com o conteúdo
  - Documento não alterado depois da assinatura
  - etc.
- Quantas destas propriedades são mesmo *impossíveis* de quebrar?
  - sob que pressupostos utilizamos esta “tecnologia” na sociedade?

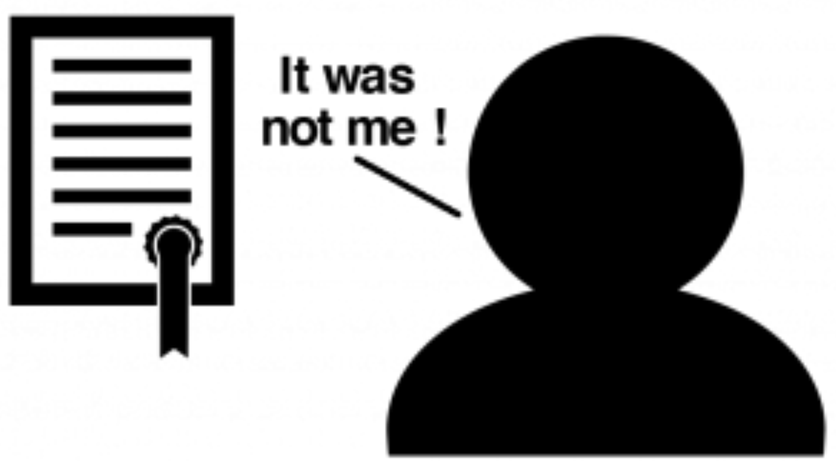


Assinaturas Digitais

- Garantem criptograficamente as mesmas propriedades
  - Não: falsificável, reutilizável, repudiável
  - Garantia de autoria do documento/acordo com o conteúdo
  - Documento não alterado depois da assinatura
- As garantias dependem também de pressupostos:
  - chave de assinatura não comprometida
  - algoritmo de assinatura criptograficamente seguro
  - **chave pública autêntica => infra-estrutura de chaves públicas (aula futura)**

Assinaturas Digitais

- As assinaturas digitais garantem autenticidade e integridade
  - tal como os Message Authentication Codes simétricos
- Mas:
  - não necessitam de chave secreta pré-partilhada
  - garantem a propriedade adicional de não-repúdio
- Não repúdio:
  - signatário não pode negar que gerou assinatura
  - MAC não garante não repúdio: porquê?



Assinaturas Digitais

- Como construir assinaturas digitais?
- Duas soluções dominam:
  - Assinaturas com base em RSA
    - historicamente as mais populares, ineficientes, legacy
    - predominantes ainda em aplicações de assinatura eletrónica
  - Assinaturas com base em curvas elípticas (ECDSA)
    - mais eficientes, chaves públicas mais pequenas
    - predominantes em autenticação: protocolos de handshake (TLS, Whatsapp)

Assinaturas Digitais

- Como construir assinaturas digitais?
- Exemplo, assinatura com base em RSA:
  - `(vk, sk) = (pk, sk)` da função RSA
  - `Sig(m,sk) := F`$^{-1}$`(sk,H(m)) => sig`
  - `Ver(m,sig,vk) :=` OK sse `F(vk,sig) = H(m)`
- Porque é seguro? Estudar criptografia

Envelopes Digitais

- Como combinar cifras assimétricas e assinaturas digitais?
  - no mundo simétrico vimos que era benéfico autenticar o criptograma
  - para garantir não repúdio:
    - assinar documento original e só depois cifrar
    - nas cifras de chave pública quem cifra não consegue decifrar
    - pode alegar que assinou um criptograma cujo conteúdo desconhecia
  - assinatura sobre criptograma permite re-assinar criptograma (problema?)

https://theworld.com/~dtd/sign_encrypt/sign_encrypt7.html
https://crypto.stackexchange.com/questions/5458/should-we-sign-then-encrypt-or-encrypt-then-sign

O que vimos até agora

- Criptografia simétrica
  - canais seguros e eficientes
  - exigem chaves secretas iguais de ambos os lados
  - chaves secretas confidenciais e autenticas

O que vimos até agora

- Criptografia de chave pública
  - autenticação e não-repúdio com assinaturas digitais
  - confidencialidade com cifras de chave pública
    - usadas para transportar chaves simétricas
  - não exigem chaves partilhadas e confidenciais
  - ainda exigem chaves públicas autênticas (aula sobre PKI)

Exercício

- Como usar:
  - cifras de chave pública
  - assinaturas digitais
  - AEAD
- Para construir um canal seguro sem chaves pré-partilhadas?
  - ou: como desenhar o protocolo TLS de raiz. :-)