3. Criptografia

Histórico, Técnicas e Aplicações

3. Criptografia

3.1. Apresentação

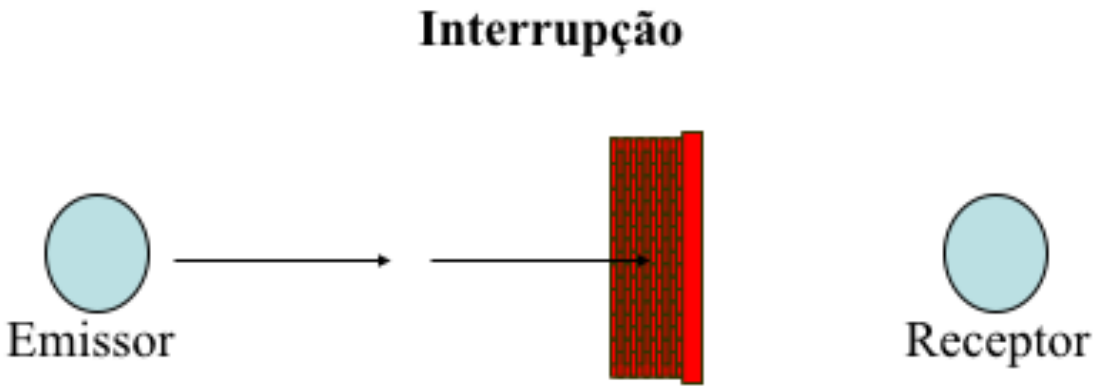
Por que estudar criptografia

- Ferramenta fundamental para atingir objetivos (prover serviços) de segurança
  - Importante para compreender soluções reais de segurança
- Modelos de funcionamento e de ataques simples e bem-caracterizados
  - Bom ponto de partida para entender arquiteturas de segurança
  - Sempre ter em mente que o mundo real é mais complexo do que os diagramas simplificados que veremos a seguir – lembre dos diversos ataques até agora estudados

Modelo de comunicação "segura"

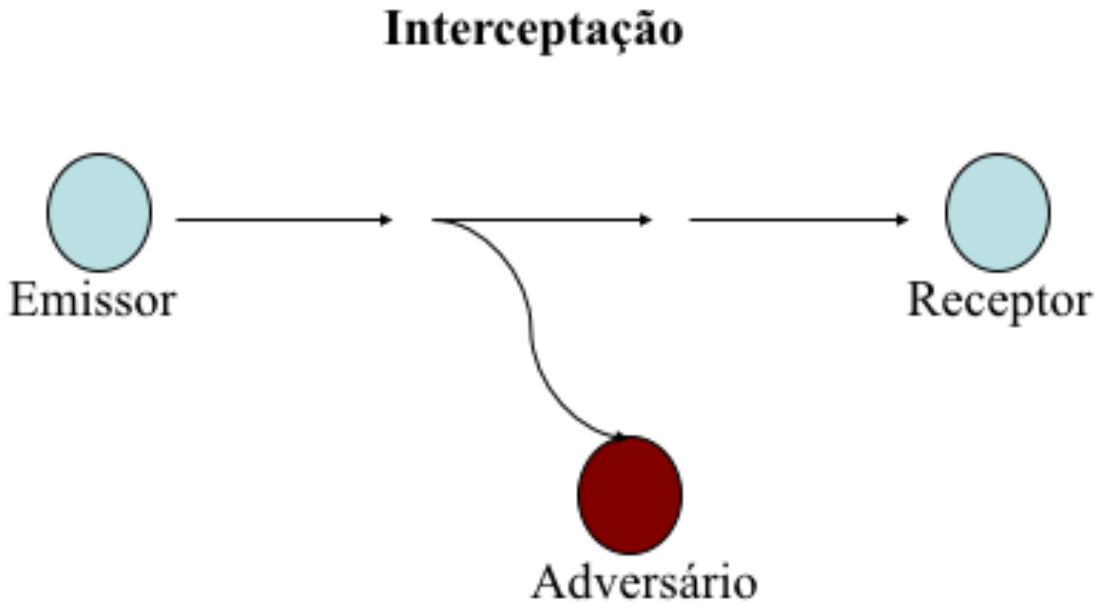
Fluxo normal da informação

Ataques à segurança: disponibilidade



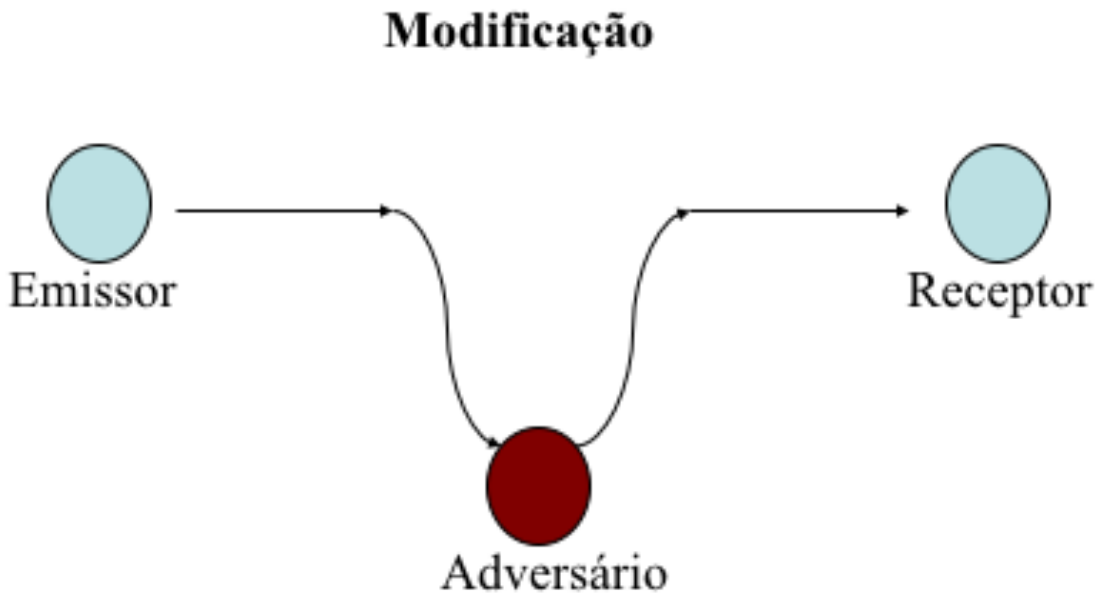
É um ataque à disponibilidade da informação

Ataques à segurança: confidencialidade



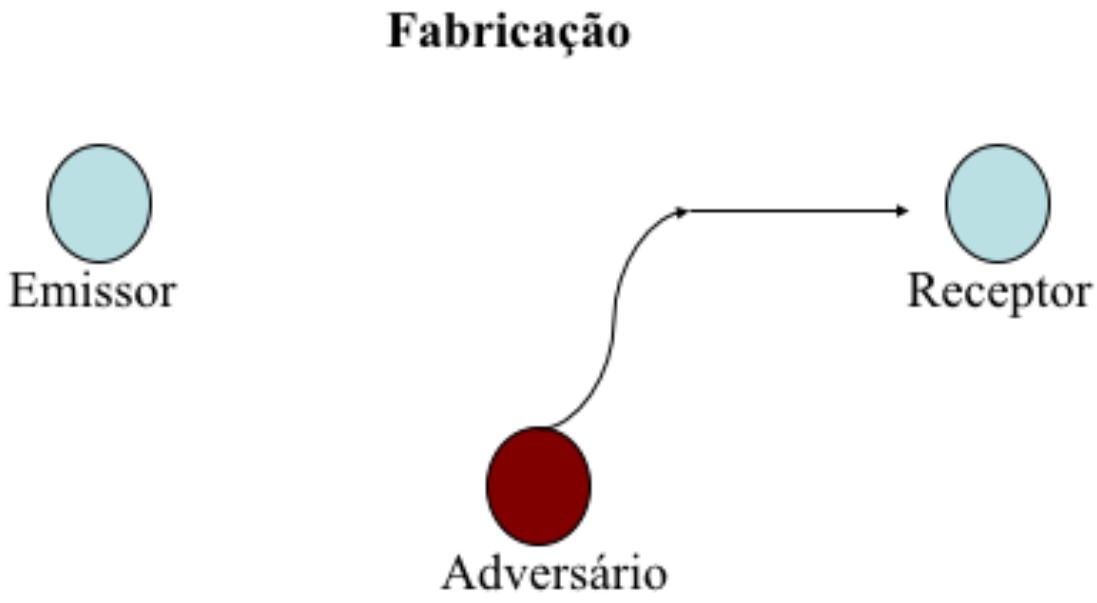
É um ataque à confidencialidade da informação

Ataques à segurança: integridade



É um ataque à integridade da informação

Ataques à segurança: autenticidade



É um ataque à autenticidade da informação

O que é criptografia?

- Uma ferramenta matemática para atingir objetivos de segurança da informação
  - De fato, é elemento fundamental, presente na maioria das soluções de segurança
  - Frequentemente não será a única ferramenta
  - Outras ferramentas:
    - Assinatura (clássica X digital)
    - Lacres
    - Lei (exemplo da violação de correspondência)
    - Políticas de segurança
    - Controle do acesso físico

Criptografia

- **escrita** (-grafia) **secreta** (cripto-)
- Terminologia
  - Texto plano ou mensagem plana – mensagem original
  - Texto cifrado ou mensagem cifrada – mensagem codificada
  - Transformação criptográfica – função que leva textos planos a cifrados (trans. de encriptação) ou textos cifrados a planos (transf. de decriptação)
  - Chave - informação que determina uma transformação criptográfica a ser utilizada

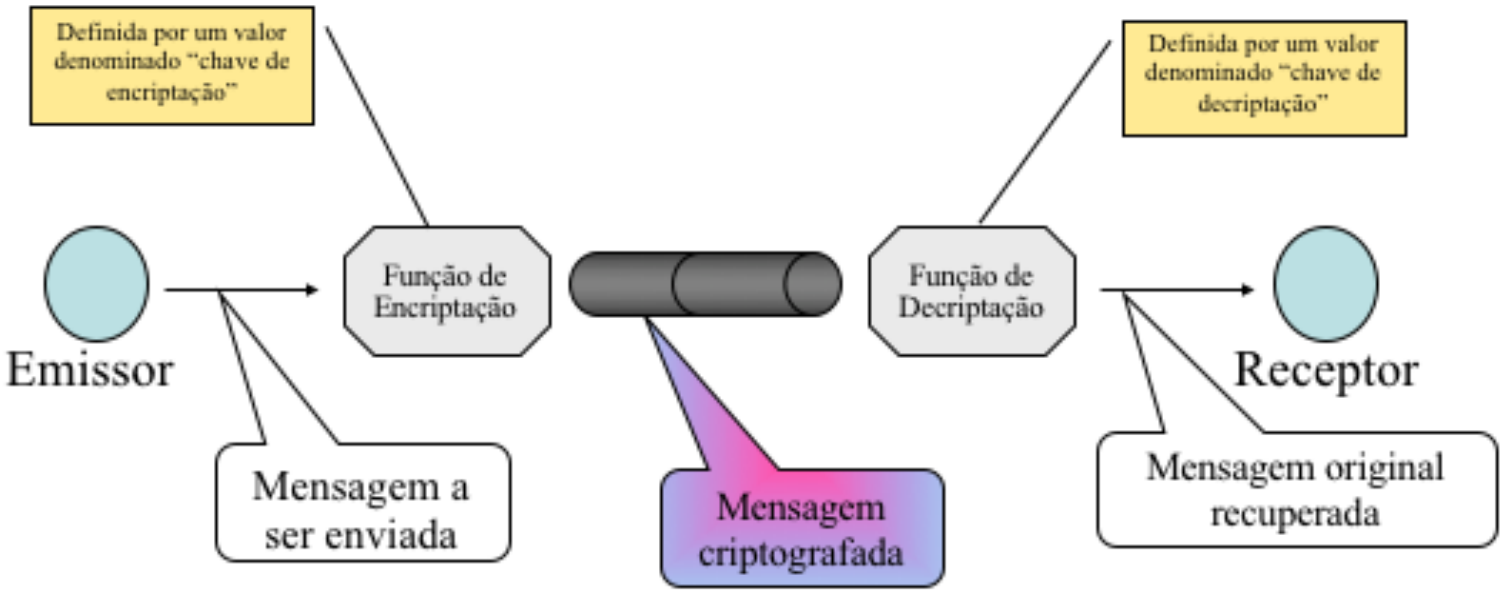
Criptografia

- Terminologia
  - Criptografar (encriptar) – converter texto plano em cifrado
  - Cifra – conjunto de transformações criptográficas indexadas por chaves
  - Descriptografar (decriptar) – converter texto cifrado em plano

Criptografia

- Terminologia
  - criptografia – estudo dos princípios e métodos de encriptação
  - criptanálise – estudo dos princípios e métodos para descriptografar sem o conhecimento da chave
  - criptologia – campo de estudo da criptografia e criptanálise
  - código – algoritmo que transforma uma mensagem compreensível em uma incompreensível a partir de um livro de códigos (ex.: códigos militares)

Funcionamento básico de um esquema de encriptação



Kerchhoff desiderata (1883)

- Requisitos para um esquema de encriptação
  - O esquema deve ser inquebrável, se não na teoria, na prática
  - Divulgação dos detalhes do esquema não deve causar problemas (redução de segurança)
  - Chave deve ser memorizável sem auxílio de anotações e facilmente (freqüentemente) modificada
  - Criptograma deve ser transmissível por telégrafo
  - Aparato de encriptação deve ser transportável e operável por uma única pessoa
  - O esquema deve ser facilmente utilizável, não necessitando-se de conhecimento prévio ou elevado poder mental

3. Criptografia

3.2. Visão do Livro =)

Funções unidirecionais e hash criptográfico

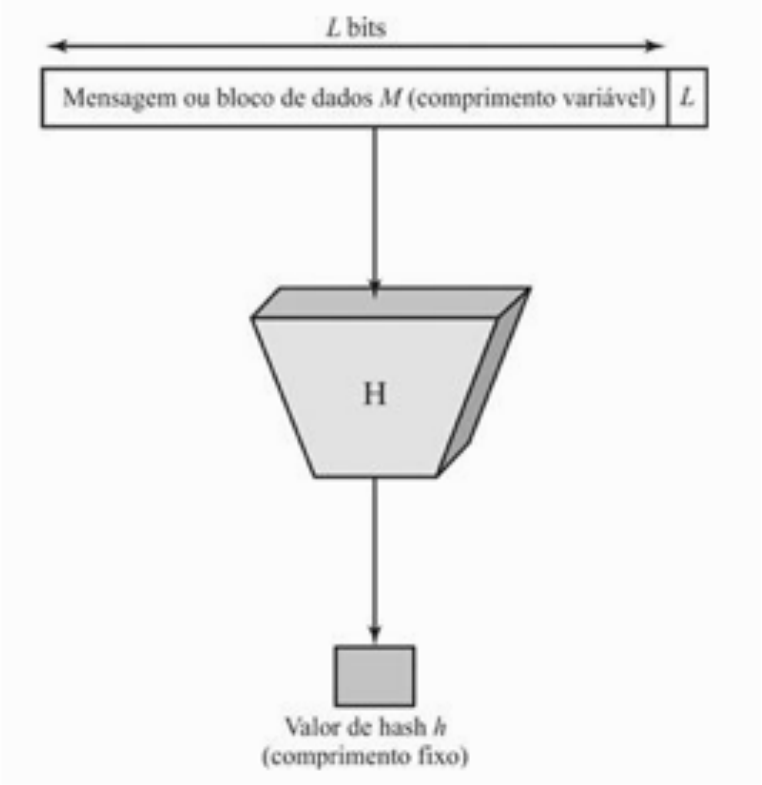
- Função unidirecional: fácil computar, difícil inverter
  - "A" ferramenta fundamental da criptografia
  - Exemplo: $f(x)=3x \bmod 17$
- Hash criptográfico: recebe como entrada uma mensagem e gera um pequeno "resumo"
  - É uma função unidirecional: inviável encontrar mensagem a partir de um resumo
  - Resistência a colisões: inviável encontrar duas mensagens com o mesmo resumo
  - Não confundir com tabela de dispersão e hash não-criptográfico

Exemplo de função unidirecional

- Seja $X=\{1,\ldots,16\}$ e $f(x)$ o resto da divisão de 3^x por 17
  - Dado $x \in X$, é relativamente fácil obter $f(x)$
  - Entretanto, não é tão fácil obter, por exemplo, o valor de x tal que $f(x)=7$.
    - Provavelmente teremos que tentar todas as 16 possibilidades

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$f(x)$	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

Funcionamento do hash criptográfico

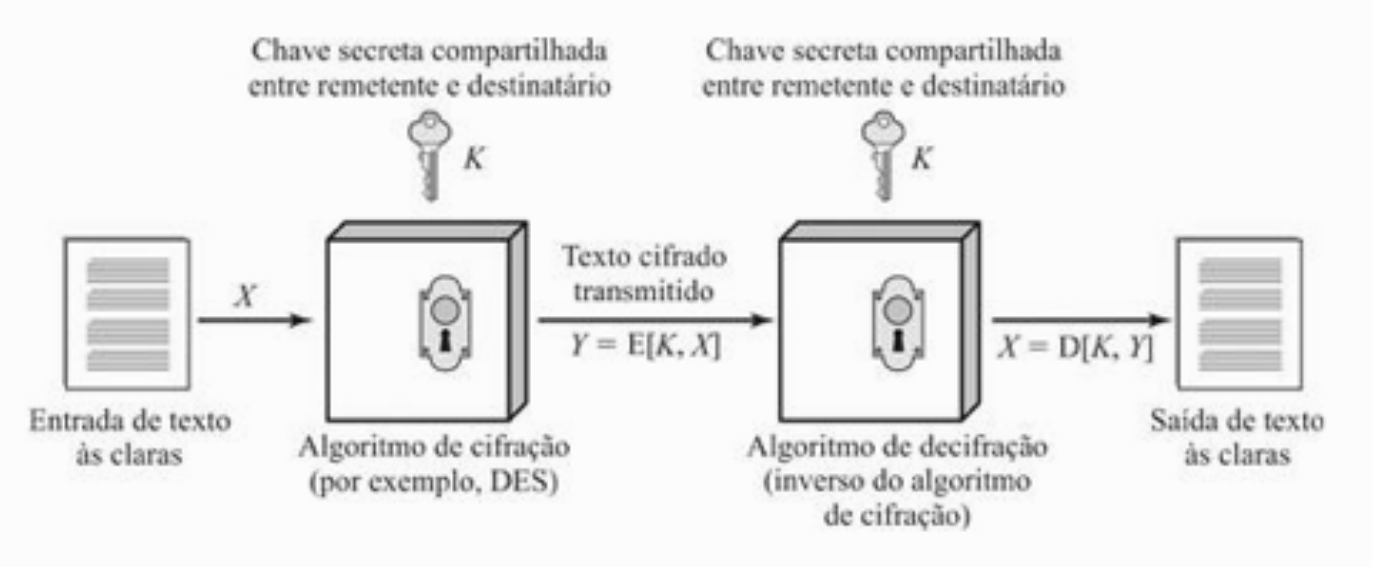


Segurança da função hash

- Resistência a identificação de pré-imagem
  - Para qualquer código dado h, é inviável em termos computacionais achar x tal que H(x) = h.
- Resistência fraca a colisão
  - Para qualquer mensagem dada x, é inviável em termos computacionais achar $y \neq x$ tal que H(y) = H(x).
- Resistência forte a colisão
  - É inviável, em termos computacionais, achar qualquer par (x, y) tal que H(x) = H(y).

Cifração Simétrica

- Texto em claro / às claras
- Algoritmo de cifração
- Chave secreta
- Texto cifrado
- Algoritmo de decifração



Algoritmo de cifração de bloco

- Cifra mensagem processando-a em "blocos" de tamanho fixo.
- Algoritmos mais importantes
  - Data Encryption Standard (FIPS PUB 46)
  - Triple DES (ANSI X9.17 e FIPS PUB 46-3)
  - Advanced Encryption Standard (FIPS PUB 197)
- Modos de operação – como trabalhar com blocos em mensagens longas
  - Exemplo mais simples: ECB

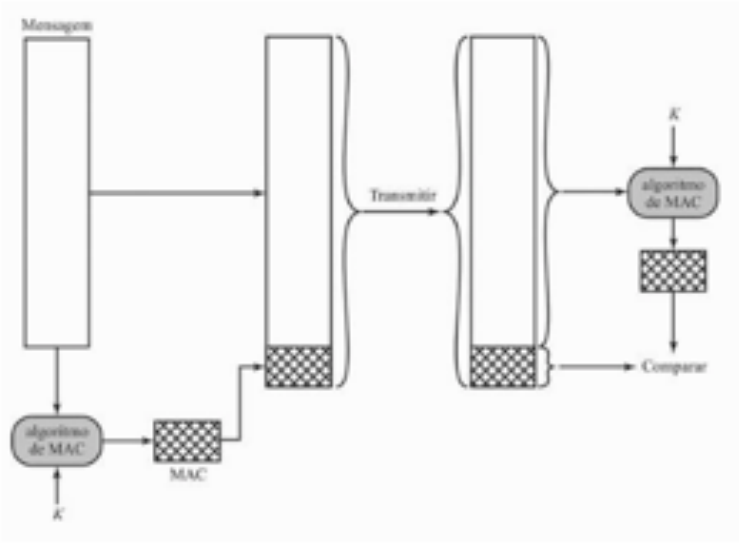
Cifra de fluxo

- Processa mensagem bit-a-bit (ou byte-a-byte)
- Estreitamente relacionada a geradores de números aleatórios
  - Exemplo de abordagem: XOR entre os bits da mensagem e os bits de um PRNG

Autenticação de mensagem e funções hash

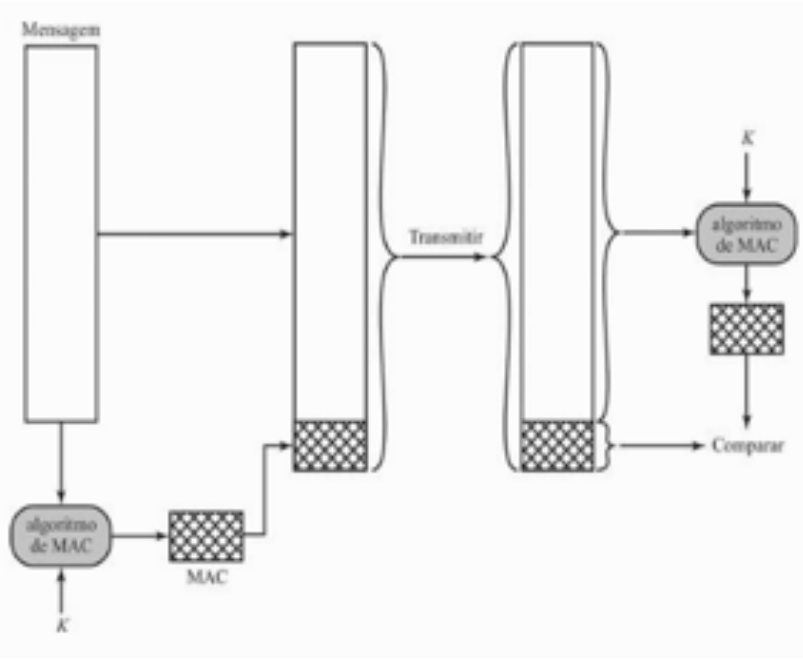
› Autenticação com cifra simétrica
  – Mensagens válidas devem compor um código

› Autenticação sem cifra simétrica
  – Mensagem segue junto com código de autenticação

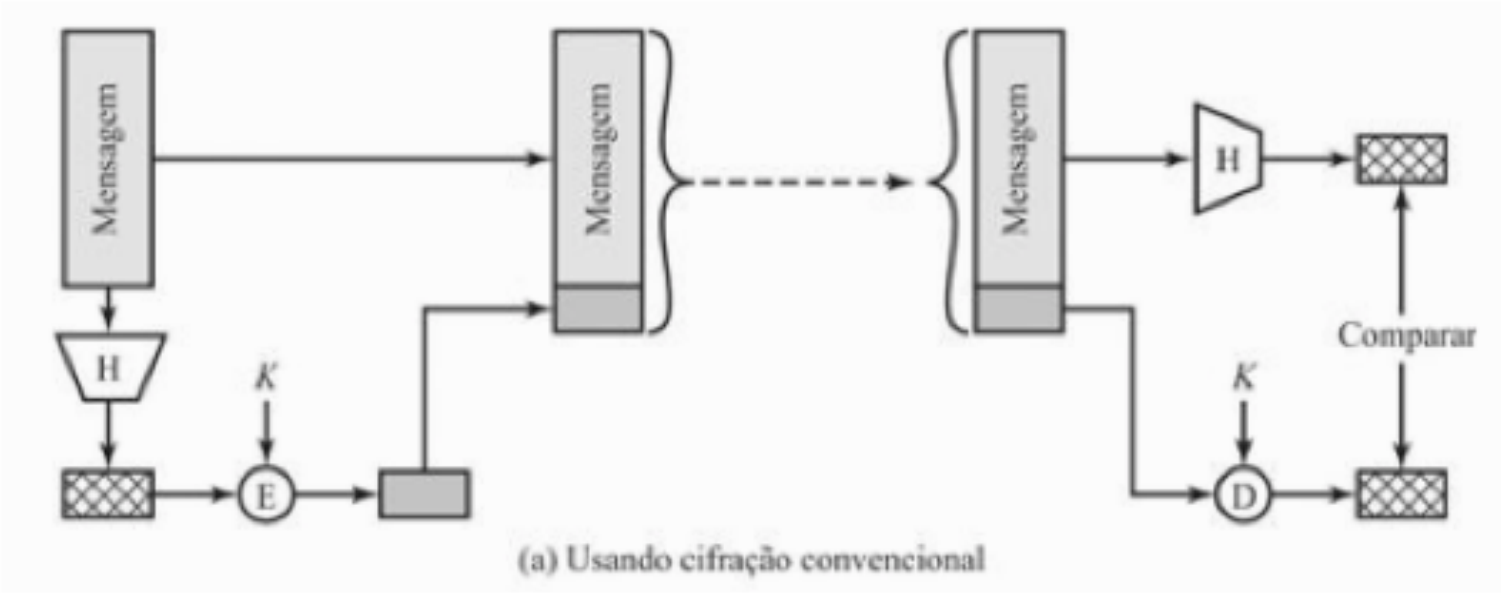


Message authentication code (MAC)

- Recebe como entrada uma mensagem M e uma chave secreta K_{AB} e gera como saída um pequeno bloco de dados $MAC_M=F(K_{AB},M)$, o cód. aut. mensagem
- Trasmissor envia M e MAC_M
- Receptor recalcula $F(K_{AB},M)$ e compara com MAC_M recebido
- Funciona porque só se pode gerar MAC_M conhecendo-se a chave secreta K_{AB}

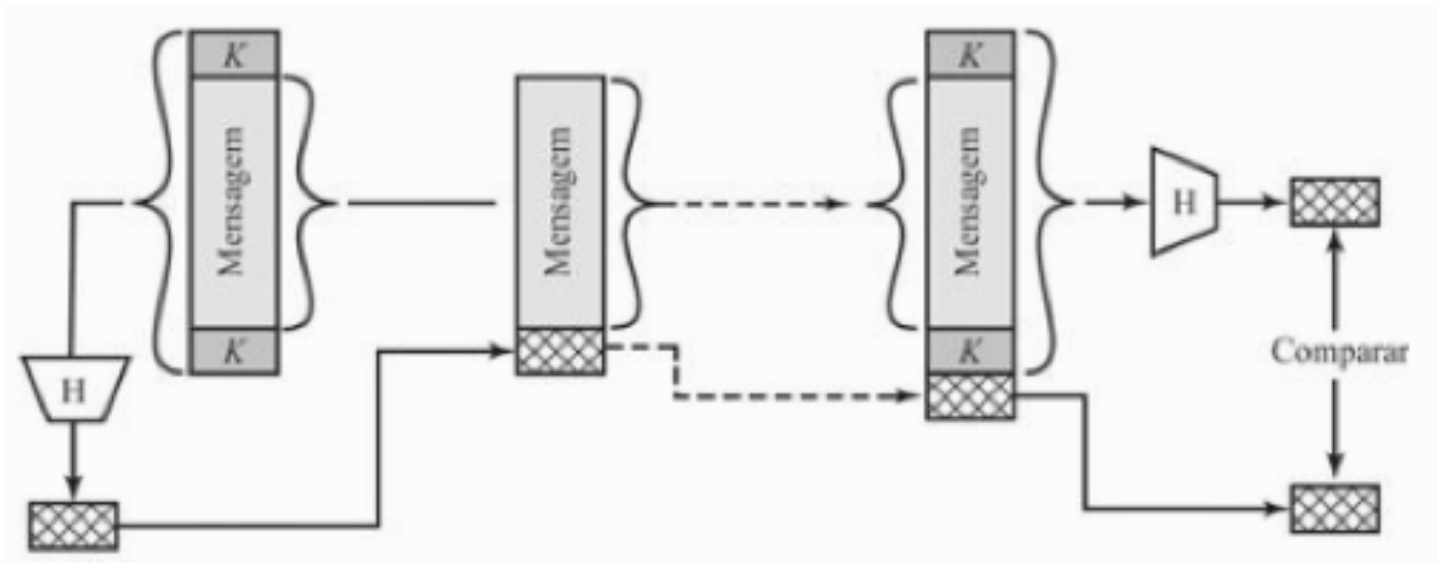


Autenticação com cifra simétrica

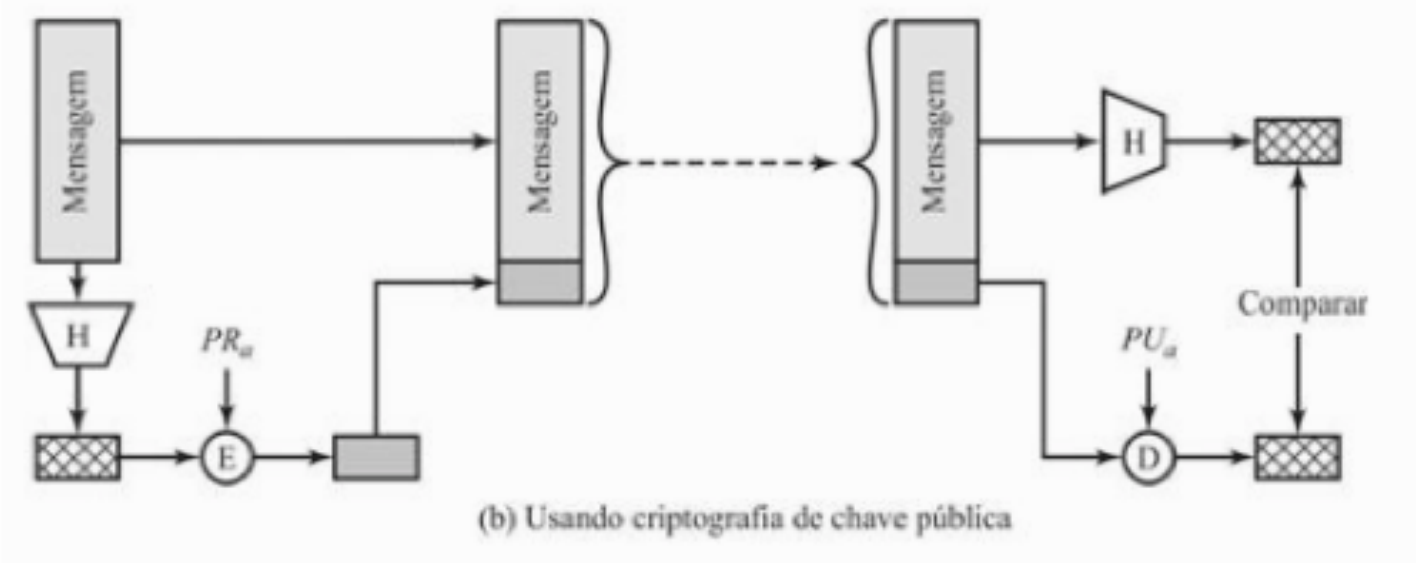


(a) Usando cifração convencional

Autenticação com hash/MAC



Autenticação com chave pública



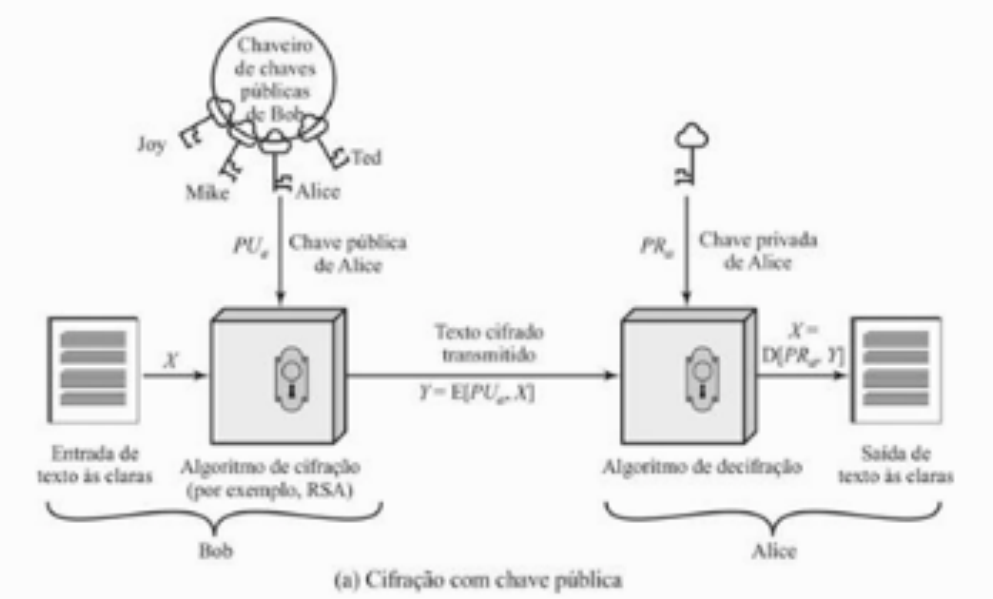
(b) Usando criptografia de chave pública

Criptografia de chave pública

› Acordo de chaves: Diffie e Hellman, 1976

› Cifra de chave pública: Rivest Shamir e Adleman, 1977

› Supostamente conhecido pelo GCHQ em 1973



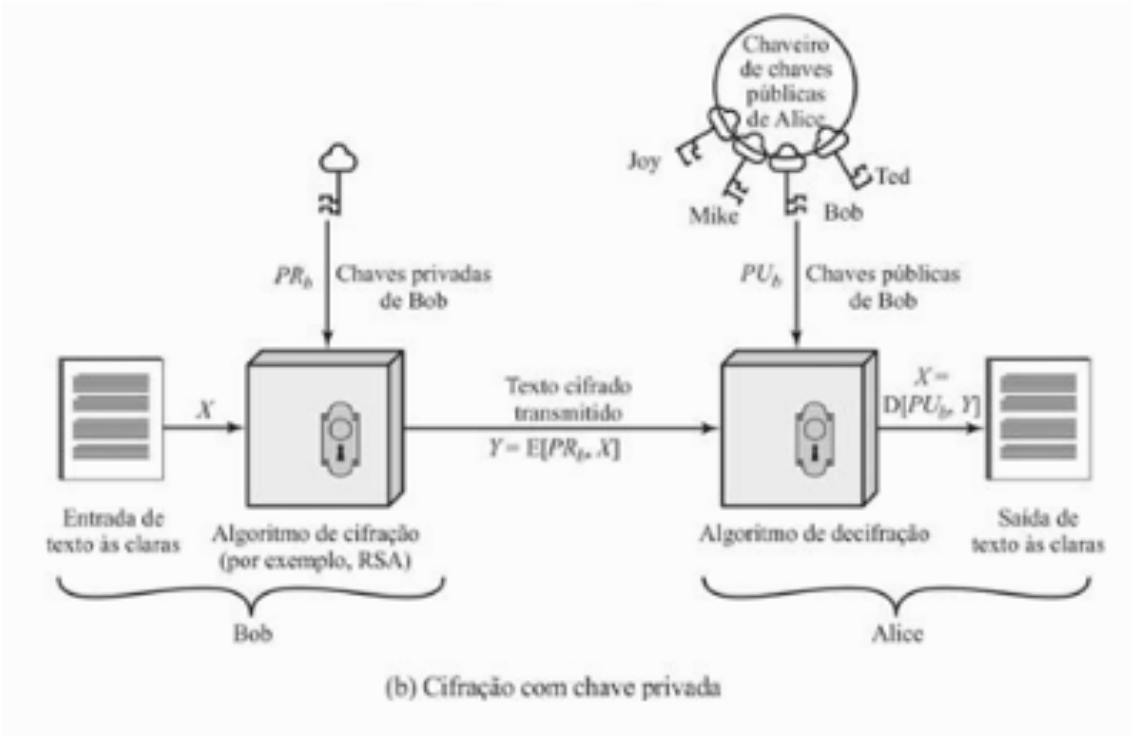
(a) Cifração com chave pública

Função unidirecional com alçapão =)

- Trapdoor one-way function
  - Fácil de computar, difícil de inverter, mas fica fácil de inverter se você conhece um ”segredo” (o trapdoor).
- O trapdoor faz o papel de ”chave privada”
- Exemplo do RSA...

Assinaturas digitais

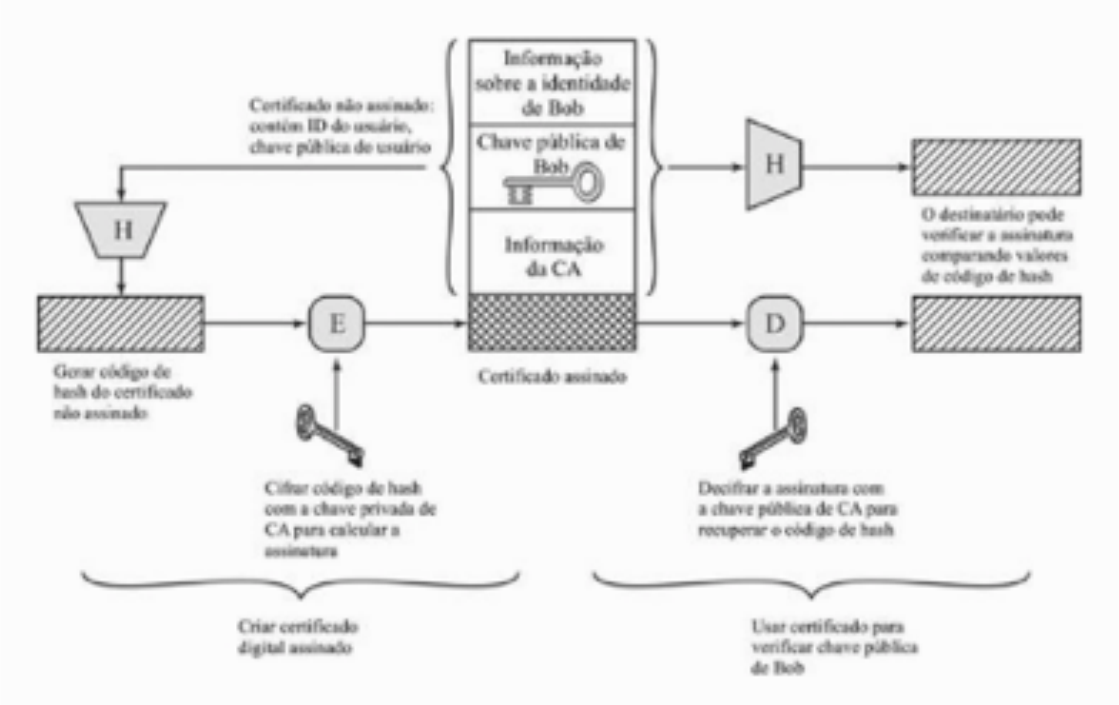
› Uso da chave privada para atestar a origem



(b) Cifração com chave privada

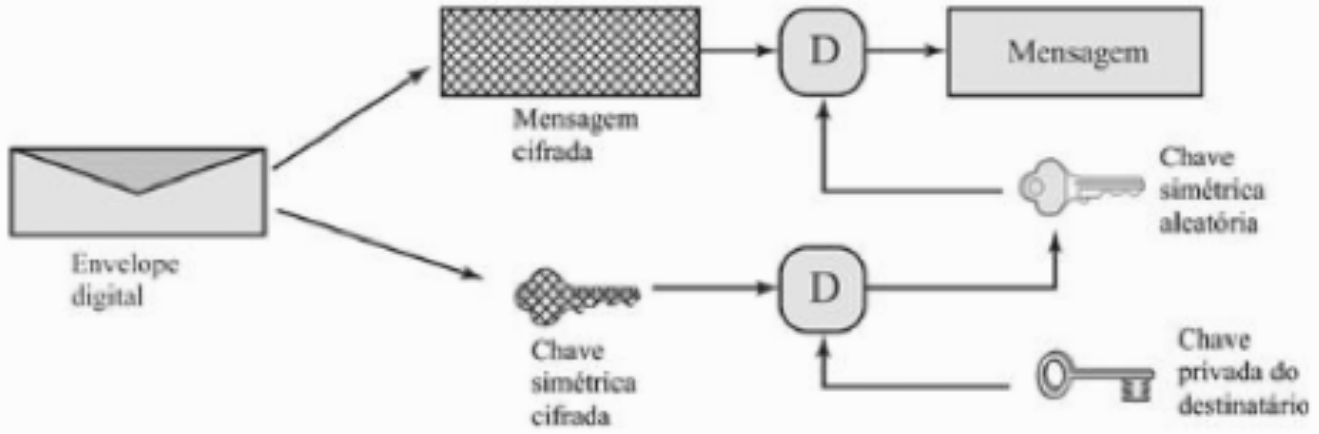
Certificados de chave pública

› Associação entre "identidade" e "chave pública" realizada por terceiras partes confiáveis



Envelope digital

› Mensagem é cifrada simetricamente e a chave é cifrada com a chave pública do destinatário



(b) Abertura de um envelope digital

Números aleatórios e pseudo-aleatórios

- Aplicações
  - Criação de chaves criptográficas
  - Uso em cifras de stream (fluxo de bist)
  - Criação de nounces/IV em protocolos e modos de operação
  - Desafios em protocolos challenge-response
  - Aplicações em protocolos diversos (desde sorteio até...)
- Aleatoriedade verdadeira e pseudo-aleatoriedade