INSTITUTO FEDERAL
PIAUÍ

Criptografia

SEGURANÇA DA INFORMAÇÃO

Prof. Silvino Marques
silvinomarques@ifpi.edu.br

Introdução

Um elemento importante em muitos serviços e aplicações de segurança de computadores é a utilização de **algoritmos criptográficos**.

Ideia da Criptografia

- Utilizar símbolos ou códigos para substituir os caracteres da mensagem original por um padrão não inteligível;

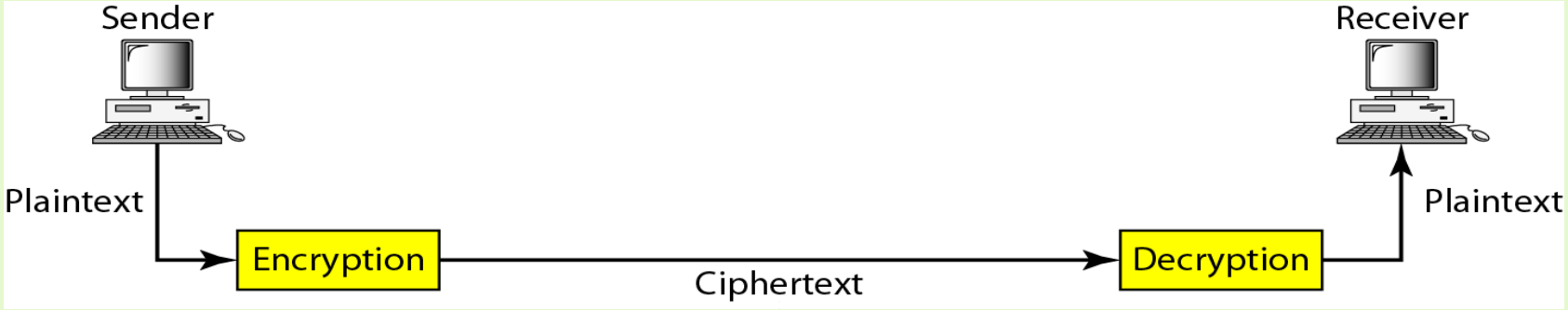
A criptografia é o **coração da segurança de redes**.

- Se precisarmos estabelecer **privacidade** em uma rede, é de suma importância pensarmos como iremos criptografar a informação no transmissor e decodificá-la no receptor;

Componentes

Criptografia

- A mensagem original é denominada **texto limpo** ou **texto em claro**;
- Após a transformação a mensagem passa a ser conhecida como **texto cifrado**, **texto criptografado** ou **criptograma**;
- Cifras
  - Algoritmos de cifragem e algoritmos de decifragem que utilizam **chaves** para transformar o texto limpo em texto cifrado;



Detalhamento

Cifras

- Substituição
  - Monoalfabética (Cifra de César): 1 –1
  - Polialfabética: 1 –N
- Transposição

Algoritmos de Criptografia

- Criptografia Clássica
  - Criptografia com Chave Simétrica
  - Criptografia com Chave Pública

Tipos Básicos de Cifras

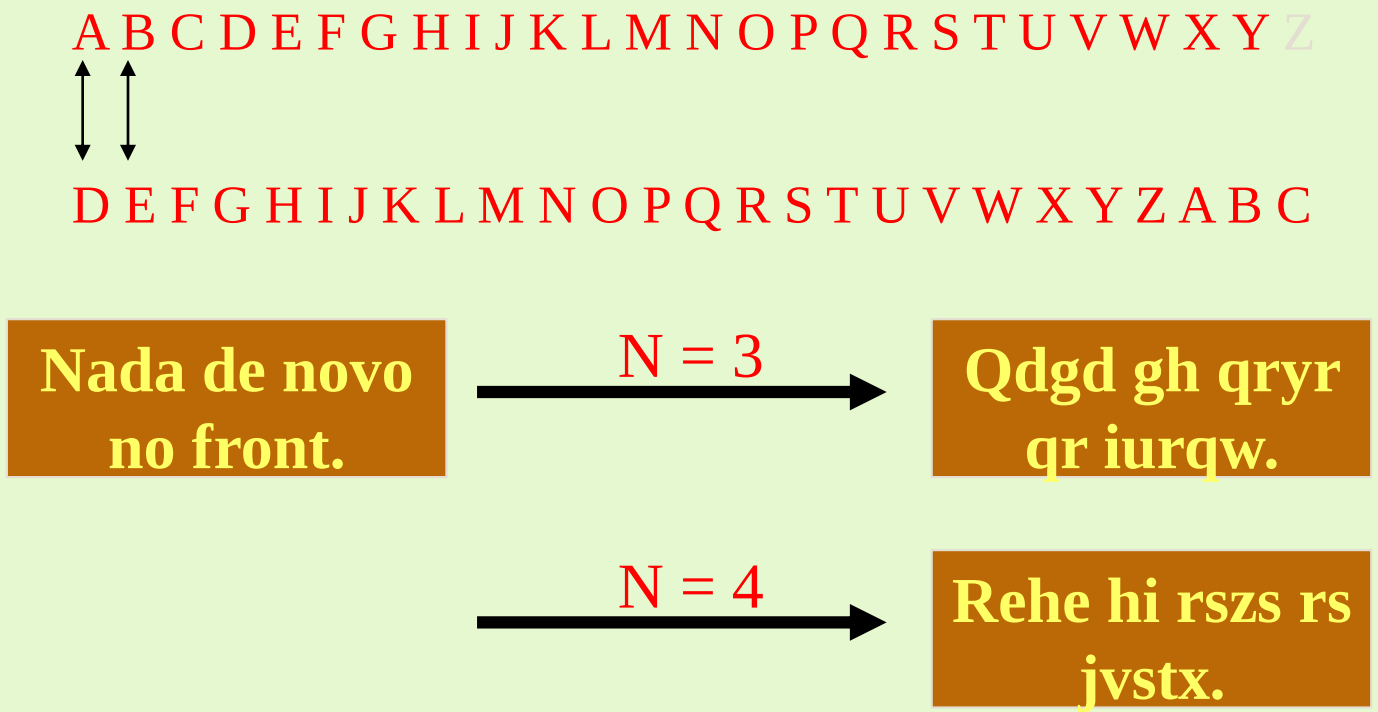
Cifras de Substituição

- Funcionamento
  - Esse tipo de cifra permuta cada símbolo do texto limpo por outro
- Classificação…
  - Substituição Monoalfabética
    - Um caractere no texto limpo sempre é substituído pelo mesmo caractere no texto cifrado não importando sua posição no texto limpo
    - Exemplo com chave = desloque 3

Plaintext: HELLO
Ciphertext: KHOOR

Substituição Monoalfabética

- Exemplo: **Cesar Cipher**
  - Chave: N = número de letras deslocadas



Ataques contra Cifras de Substituição

- Exemplo (texto encriptado):

```
iq ifcc vqqr fb rdq vfllcq na rdq
cfjwhwz hr bnnb hcc hwwhbsqvqbre hwq
vhlq
```

- Quão segura é a Cifra de Substituição?

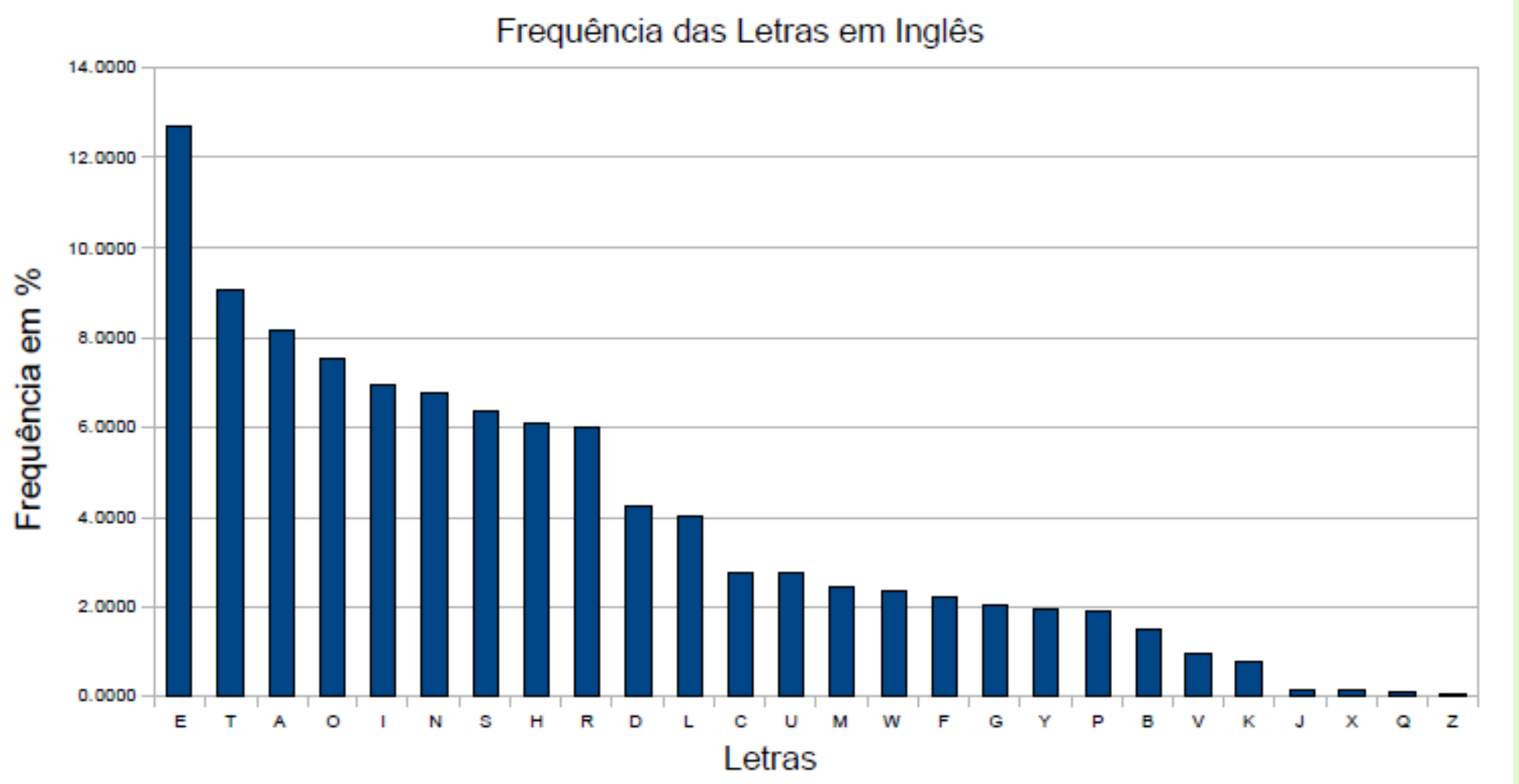
Ataques contra Cifras de Substituição

- **Ataque: Busca exaustiva da chave (Ataque de Força Bruta)**
  - Simplesmente tente todas as tabelas de substituição possíveis até que um texto em claro inteligível apareça (note que cada tabela de substituição é uma chave)
- Quantas tabelas de substituição (= chaves) existem?
  - $26 \times 25 \times \ldots \times 3 \times 2 \times 1 = 26! \approx 2^{88}$
- Pergunta: Podemos concluir que a cifra de substituição é segura, já que o ataque de força bruta não é viável?
- Resposta: Não! Nós temos que estar protegidos contra **todos** os ataques possíveis.

Ataques contra Cifras de Substituição

- **Ataque: Análise de frequência das letras (Ataque analítico)**
- As letras na língua inglesa tem frequências de uso muito diferentes
  - Além disso: o texto encriptado preserva a frequência das letras do texto em claro.
  - Por exemplo, "**e**" é a letra mais comum em inglês; quase 13% de todas as letras em um texto típico em inglês são "**e**"s. A letra seguinte mais comum é o "**t**" com aproximadamente 9%.

Ataques contra Cifras de Substituição



Ataques contra Cifras de Substituição

- **Quebrando a Cifra de Substituição com a Análise de Frequência das Letras**
- Vamos voltar ao exemplo e identificar a letra mais frequente:

```
iq ifcc vqqr fb rdq vfllcq na rdq cfjwhwz hr bnnb hcc hwwhbsqvqbre hwq
vhlq
```

- Trocamos a letra q por E e obtemos:

```
iE ifcc vEEr fb rdE vfllcE na rdE cfjwhwz hr bnnb hcc hwwhbsEvEbre hwE
vhlE
```

- Por um processo de tentativa e erro, baseado na frequência das letras restantes do texto encriptado, nós obtemos o texto em claro:

```
WE WILL MEET IN THE MIDDLE OF THE LIBRARY AT NOON ALL ARRANGEMENTS ARE
MADE
```

Tipos Básicos de Cifras

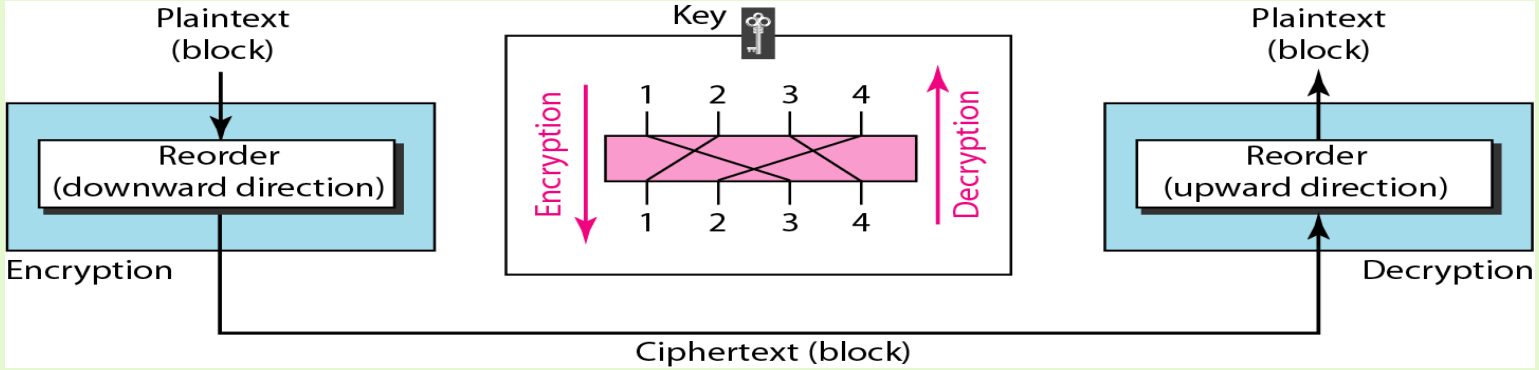
- Substituição Polialfabética
  - Cada ocorrência de um caractere pode ter um substituto diferente;
  - A correspondência entre um caractere do texto limpo e um do texto cifrado é de um para muitos;
  - Exemplos:
    - Tome a posição do caractere, a ser substituído, no texto limpo, divida o número por 10 e use o valor do resto da divisão como valor de deslocamento
    - Exemplo de Texto Claro e Cifrado

Plaintext: HELLO
Ciphertext: ABNZF

Tipos Básicos de Cifras

Cifras de Transposição…

- Os caracteres permanecem na forma original do texto limpo mas mudam de posição através de permutações para criar o texto cifrado;
- O texto é organizado em uma matriz bidimensional e as colunas são permutadas de acordo com o valor da chave;

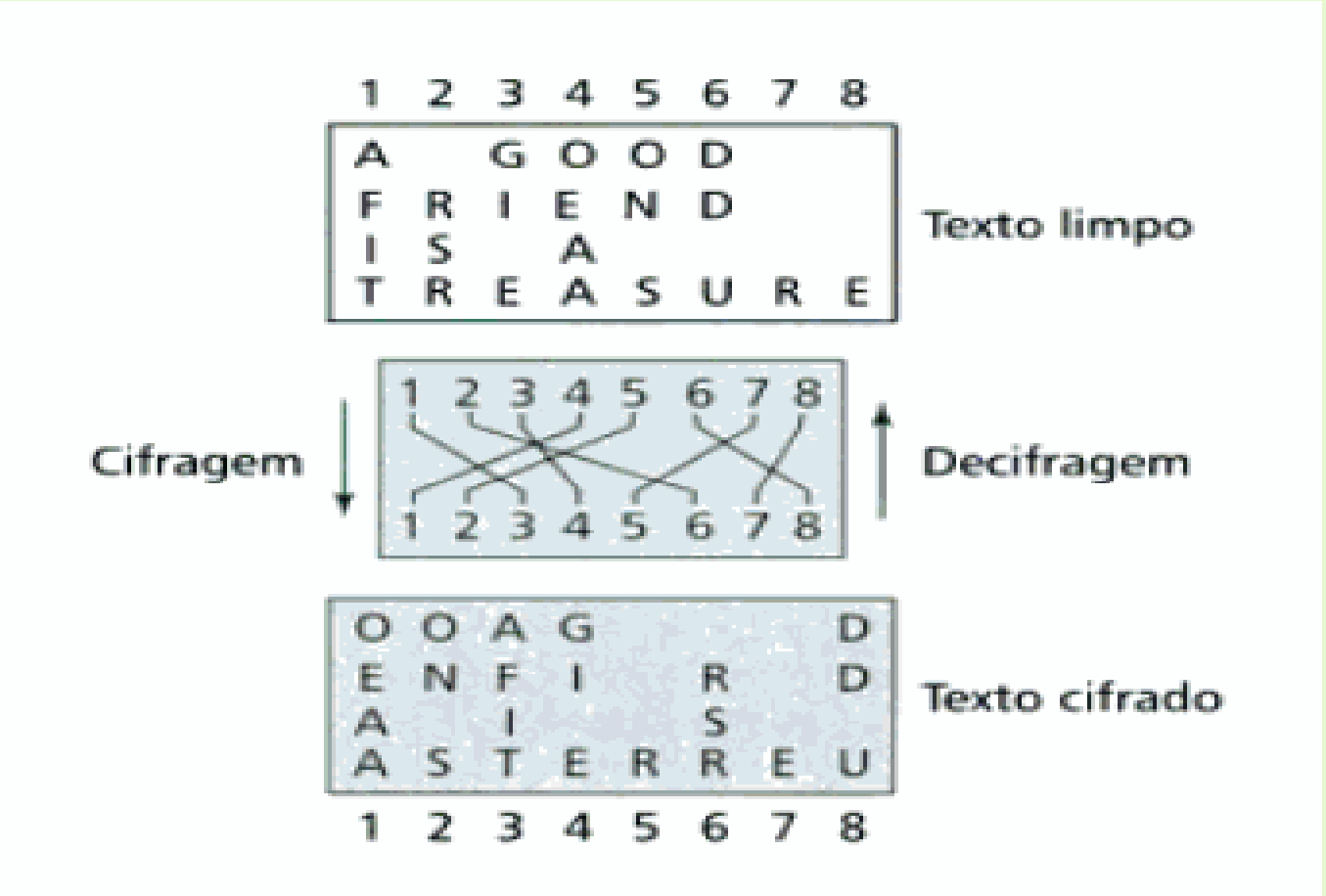


Tipos Básicos de Cifras

Cifras de Transposição

- A chave define quais colunas devem ser permutadas;
- Como podemos ver, a criptografia por transposição não é muito segura;
- A frequência dos caracteres é preservada;
- Esse método é combinado com outros métodos para produzir esquemas de cifras seguros;
- O texto limpo pode ser determinado por força bruta;

Cifras de Transposição



Criptografia com Chave Simétrica

Detalhamento

- A mesma chave é usada para cifrar e decifra a mensagem;
- A chave é compartilhada;

- O algoritmo de decifragem é recíproco do algoritmo de cifragem;
  - ✓ Se o algoritmo de cifragem usa uma combinação de operações de adição e multiplicação o de decifragem usa uma combinação de operações de subtração e divisão

Criptografia com Chave Simétrica

Os algoritmo de chave simétrica são eficientes e as chaves são usualmente menores que as chaves dos algoritmos de chave pública;

- É usada frequentemente na cifragem e decifragem de mensagens longas;

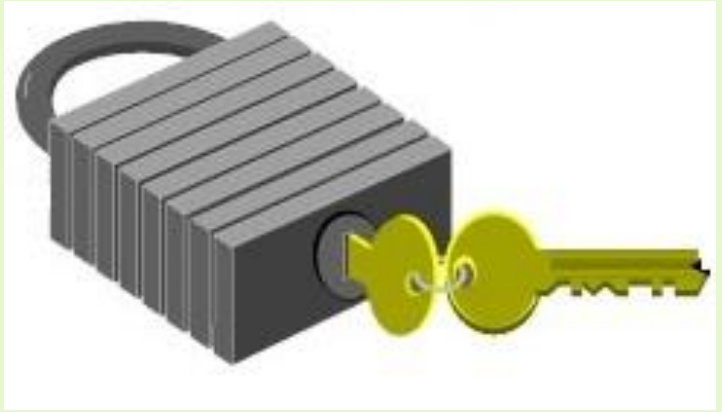
Desvantagens

- A cada usuário participante deve estar associada uma única chave;
- A distribuição segura de chaves é um problema difícil de resolver.

Algoritmos Simétricos

Algoritmos:

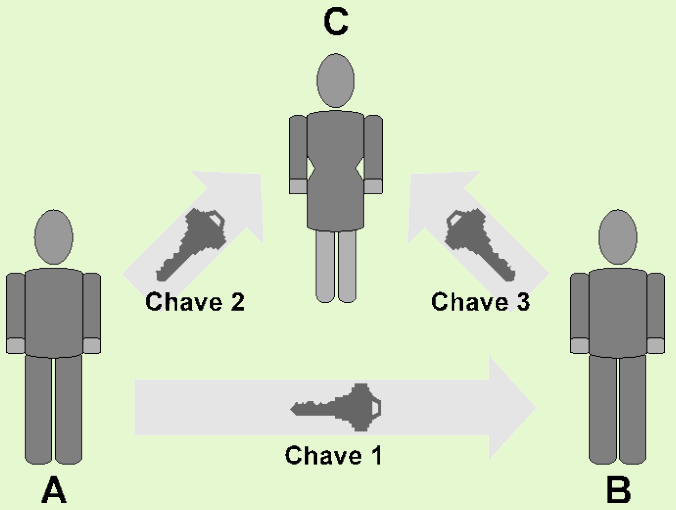
- DES;
- 3DES ou DES-EDE;
- IDEA;
- Blowfish;
- Cast-128;
- RC6;
- AES: atual padrão americano;



Criptografia com Chave Pública

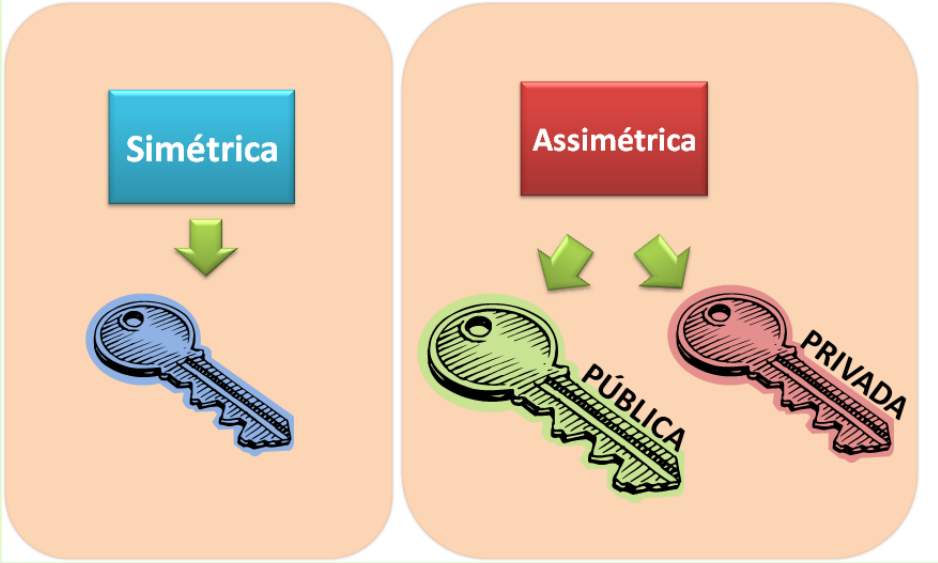
Detalhamento

- O problema de **distribuição de chaves** sempre foi o elo mais fraco da maioria dos sistemas de criptografia, pois todos os usuários devem ter a mesma chave usada para ambos os processos;

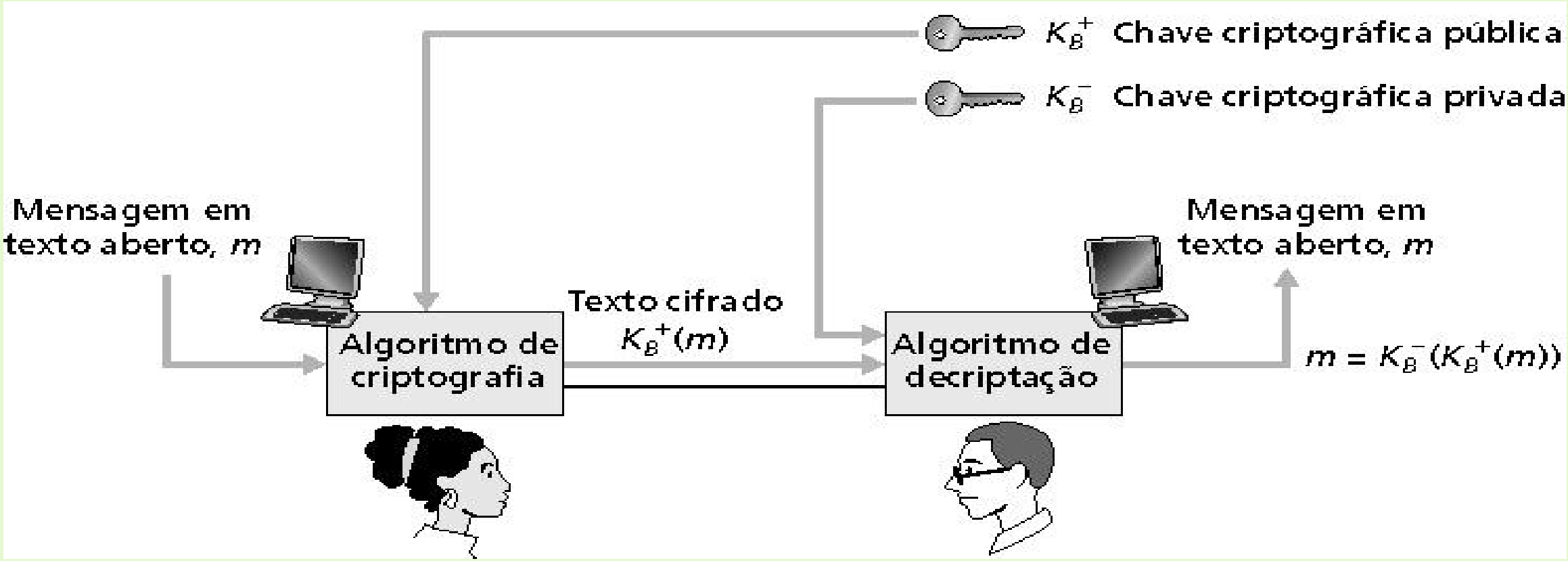


Criptografia com Chave Pública

- Na criptografia com chave pública, há duas chaves: uma **privada** e uma **pública**;
- A chave privada é mantida pelo proprietário B e a chave pública é distribuída publicamente sem qualquer restrição.



Visão da Criptografia de Chave Pública



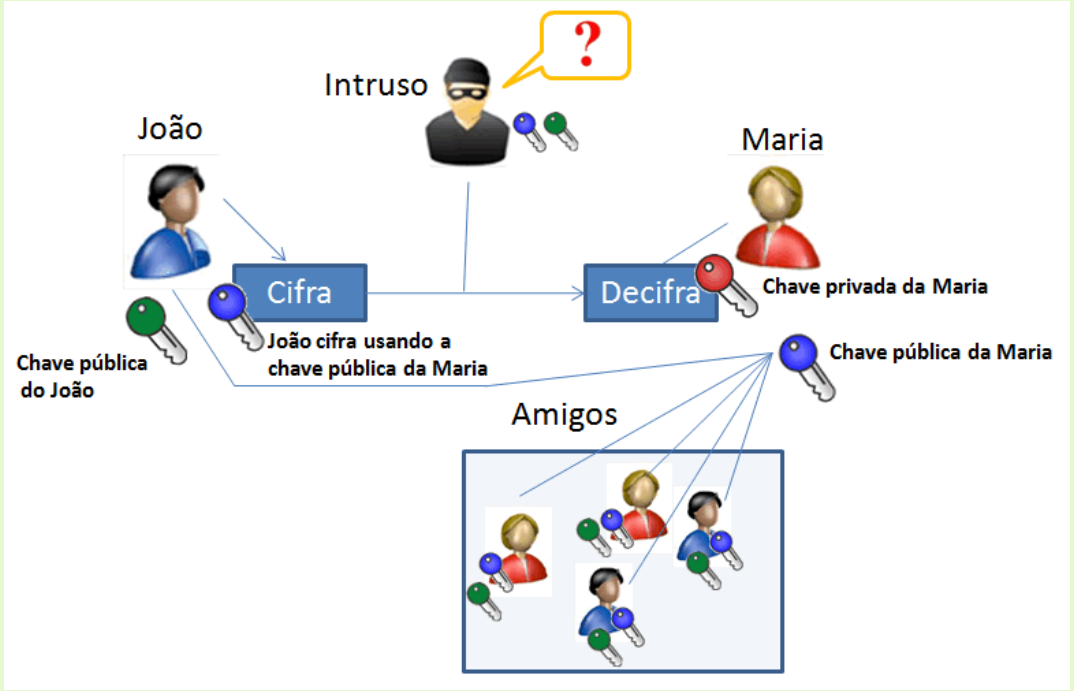
Algoritmos de Chave Pública

Considerações

- A chave pública utilizada para a cifragem deve ser diferente da chave privada utilizada para a decifragem
- Vantagens
  - Remove a necessidade de uma chave simétrica compartilhada entre duas entidades (pessoas ou processos);
  - Quando usamos a criptografia assimétrica, cada entidade cria um par de chaves e a chave pública pode ser utilizada para se comunicar com qualquer outra parte;
  - A quantidade de chaves necessárias é reduzida tremendamente;

Algoritmos de Chave Pública

- Desvantagens
  - Algoritmos complexos;
  - O Tamanho das chaves é relativamente extenso;
  - A associação entre uma entidade e sua chave pública deve ser certificada através de uma entidade certificadora.



Algoritmos Assimétricos

Algoritmos:

- RSA (Rivest, Shamir e Adleman);
- ElGamal
- Diffie-Hellman

Assinatura Digital

Introdução

A segurança está relacionada a vários aspectos, entre eles: ***privacidade***, ***autenticação***, ***integridade*** e ***não-repúdio;***

Já foi demonstrado através da criptografia como alcançar a privacidade (confidencialidade), mas para discutirmos as outras três características precisamos analisar a ***Assinatura Digital***.

Introdução

A ideia é similar a assinatura em um documento de identificação;

- Quando transmitimos um documento eletronicamente, devemos assiná-lo;

Temos duas escolhas para isso:

- Assinar todo o documento ;
- Assinar uma visão resumida ou sintetizada do documento (***digest message***).

Assinando um documento

A **cifragem com chave pública** pode ser utilizada para assinar um documento;

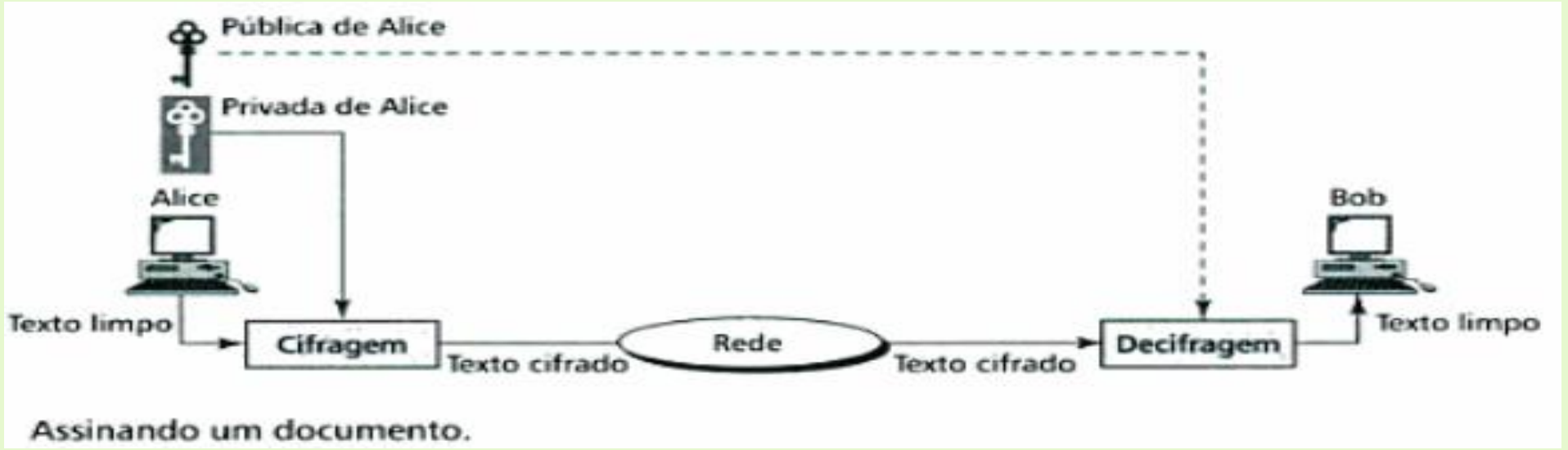
Nesse caso, os papeis das chaves pública e privada são diferentes;

A **chave privada é usada para cifrar (assinar)** o documento e **a chave pública é usada para decifrar (verificar a assinatura)** o documento.

Assinatura Digital

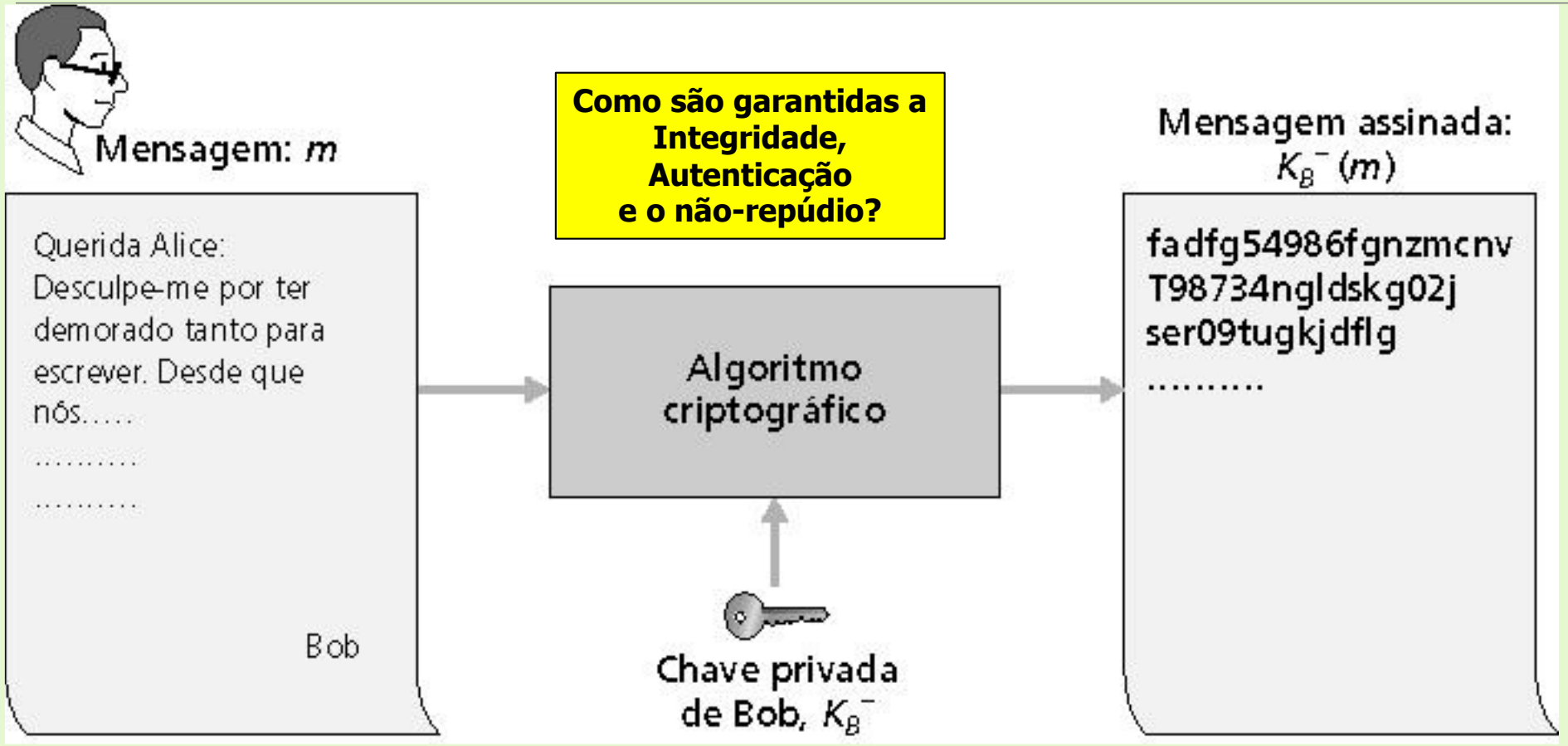
Processo

- Alice assina ***m***, criptografando-a com sua chave privada K^-_A, criando a mensagem "assinada", $K^{-A}(m)$;
- O receptor verifica que ***m*** foi assinada por Alice usando a chave pública de Alice K^+_A para $K^-_A(m)$, então verifica que $K^+_A(K^-_A(m))=m$;



Assinando um documento.

Assinatura Digital



Assinatura Digital

A assinatura digital pode agregar **integridade**, **autenticação** e o **não-repúdio**;

- A integridade é preservada por que se alguém a interceptar e modificá-la a mensagem ficará inteligível para ela;
- A autenticação pode ser garantida pois o intruso não possui a chave privada da pessoa por quem ele quer se passar;
- O não-repúdio pode ser evitado pois a cifragem/decifragem da mensagem salva com as chaves pública e privada do transmissor gera uma duplicata da mensagem salva;

Assinando a Síntese de um Documento

Sumário de Mensagem (Message Digest)

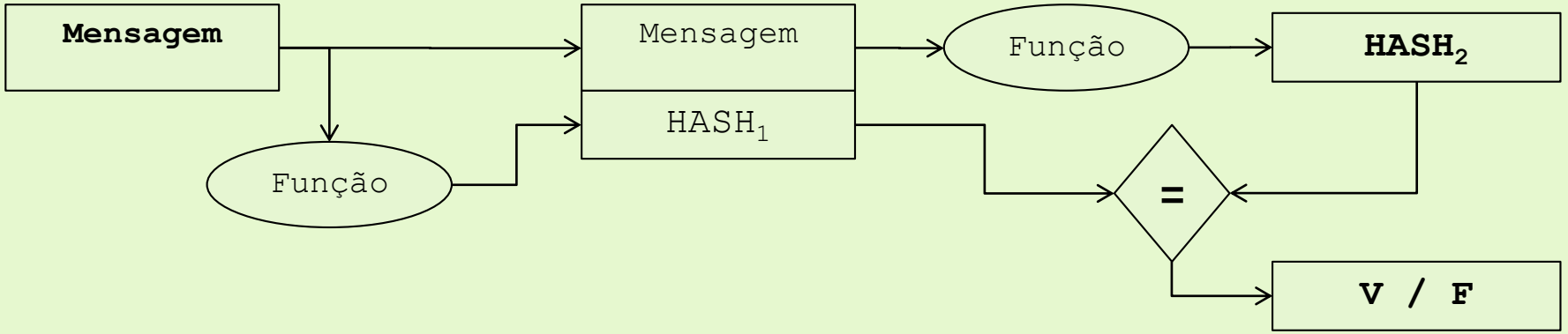
- Como já sabemos, a criptografia de chave pública é bastante eficiente com mensagens pequenas, então assinar um documento inteiro pode tornar o processo pouco eficiente;
- A solução é permitir que uma versão resumida do documento seja assinada em vez de assinar o documento inteiro;
- O dono da chave privada cria uma versão resumida do documento e o assina, então o receptor verifica a assinatura na versão sintetizada.
  - Autenticação e sigilo, os quais nem sempre são necessários simultaneamente;

Assinando a Síntese de um Documento

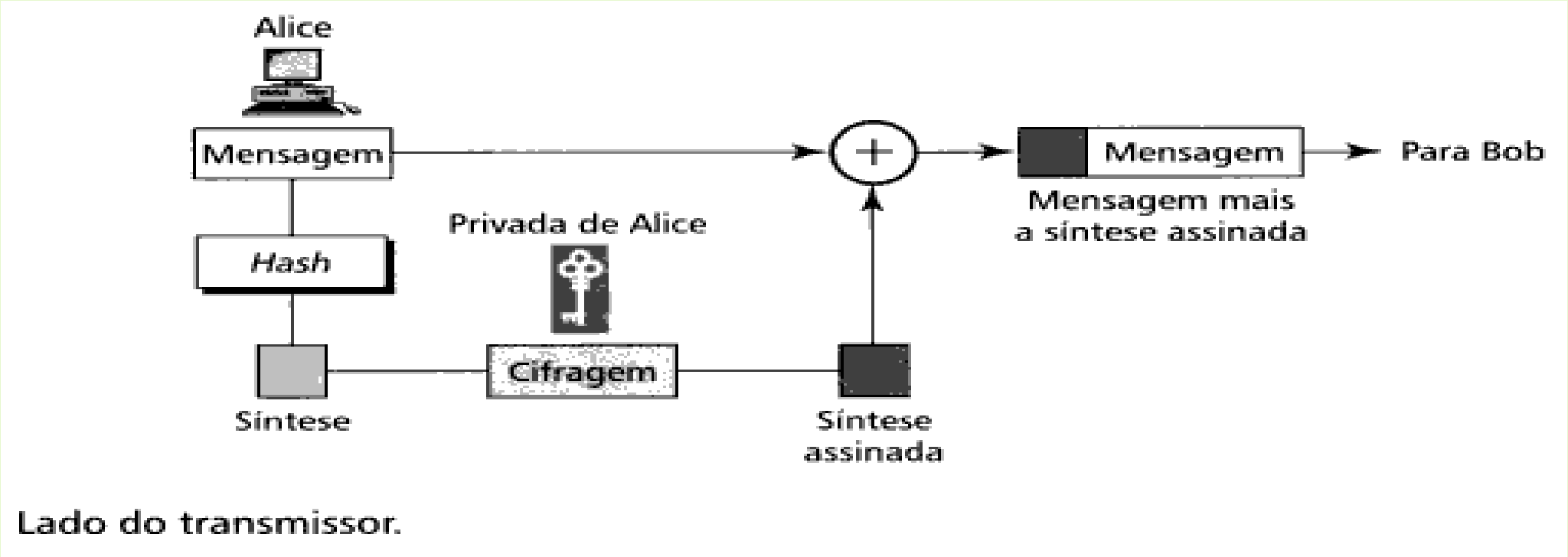
Para criar uma síntese da mensagem usamos uma ***função de hash***;

- A finalidade da função de hash é criar uma síntese da mensagem de tamanho fixo a partir da mensagem original de tamanho variável;
- A versão sintetizada só pode ser criada a partir da versão original da mensagem e a probabilidade de que duas mensagens gerem o mesmo sumário é praticamente nula ;
- As duas funções de hash mais conhecidas são MD5 e SHA-2;

Cálculo e verificação de um *hash*

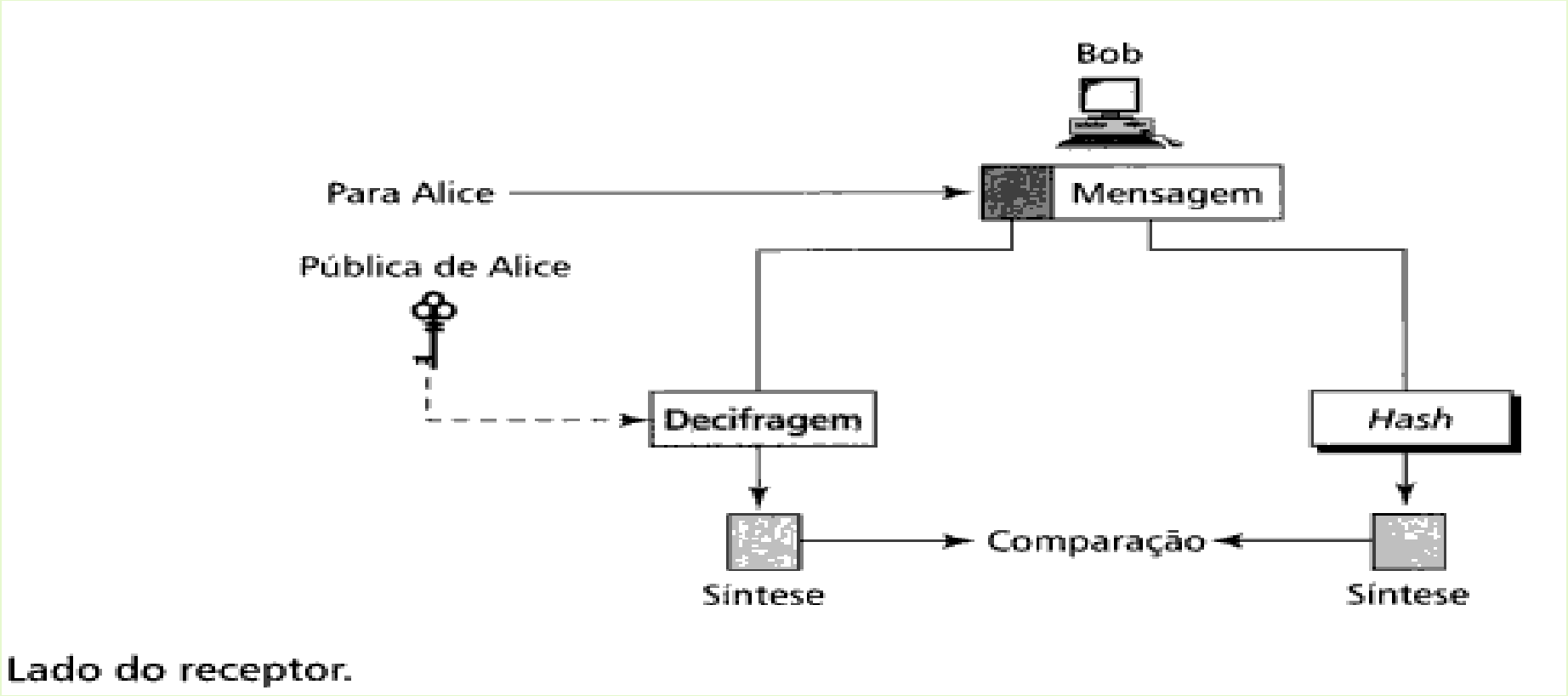


Funcionamento



Lado do transmissor.

Funcionamento



Lado do receptor.

Gerenciamento de Chaves Públicas

Faremos uma breve abordagem sobre o problema de garantir a autenticidades de chaves públicas ;

Considerações sobre a Criptografia de Chave Pública:

- Torna possível a comunicação segura para entidades que não compartilham uma chave comum;
- Possibilita a assinatura de mensagens sem a presença de uma terceira parte confiável.

Gerenciamento de Chaves Públicas

Considerações sobre a Criptografia de Chave Pública

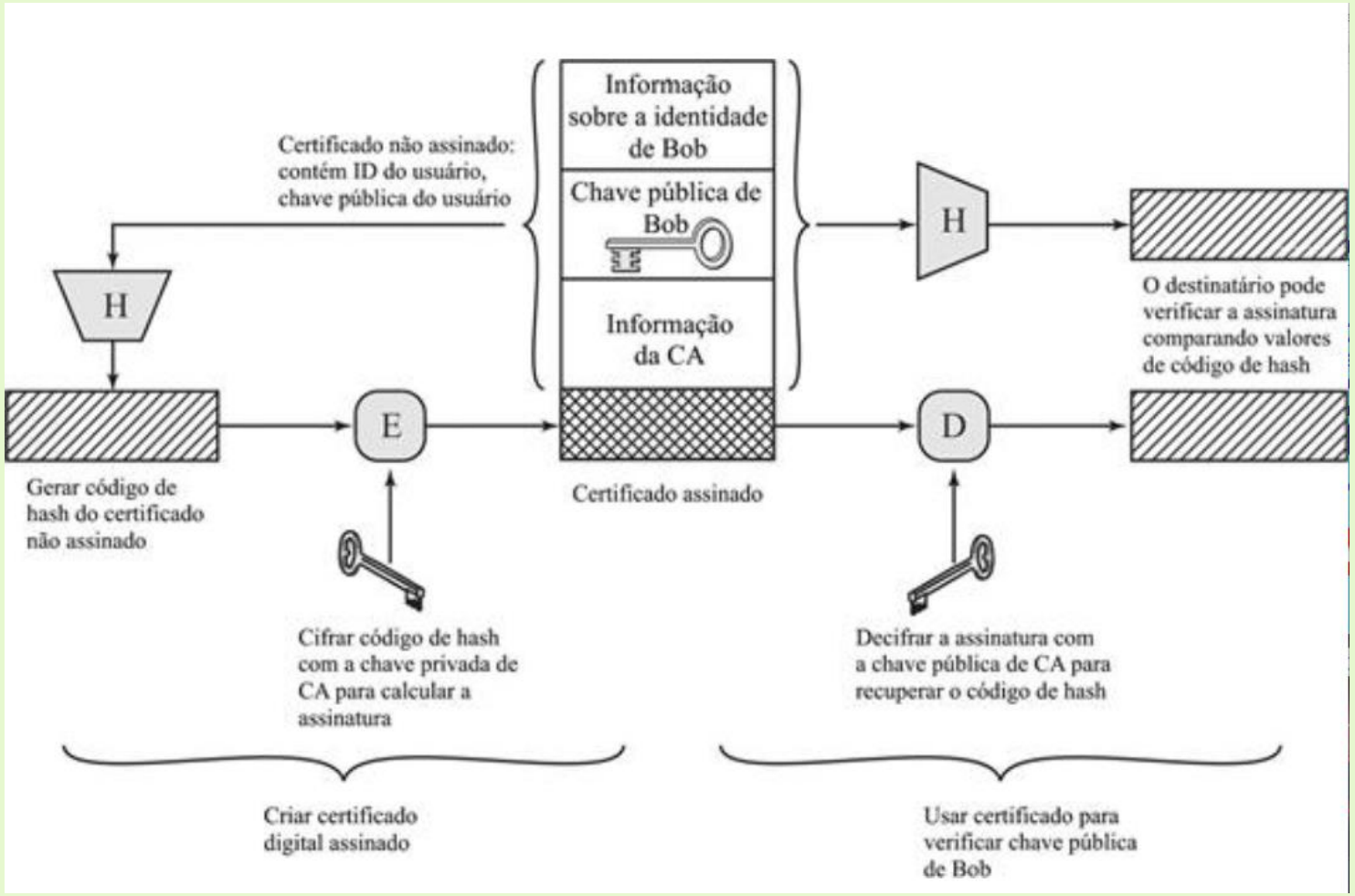
- Ideia
  - Usuários poderiam se comunicar e solicitar as chaves públicas um do outro;
- Qual é o problema com essa ideia?
  - E se, um terceiro elemento interceptar o pedido de troca de chaves e assumir a identidade do outro?
  - Resultado: mensagens serão criptografadas com a chave pública do destino errado;

Gerenciamento de Chaves Públicas

Solução

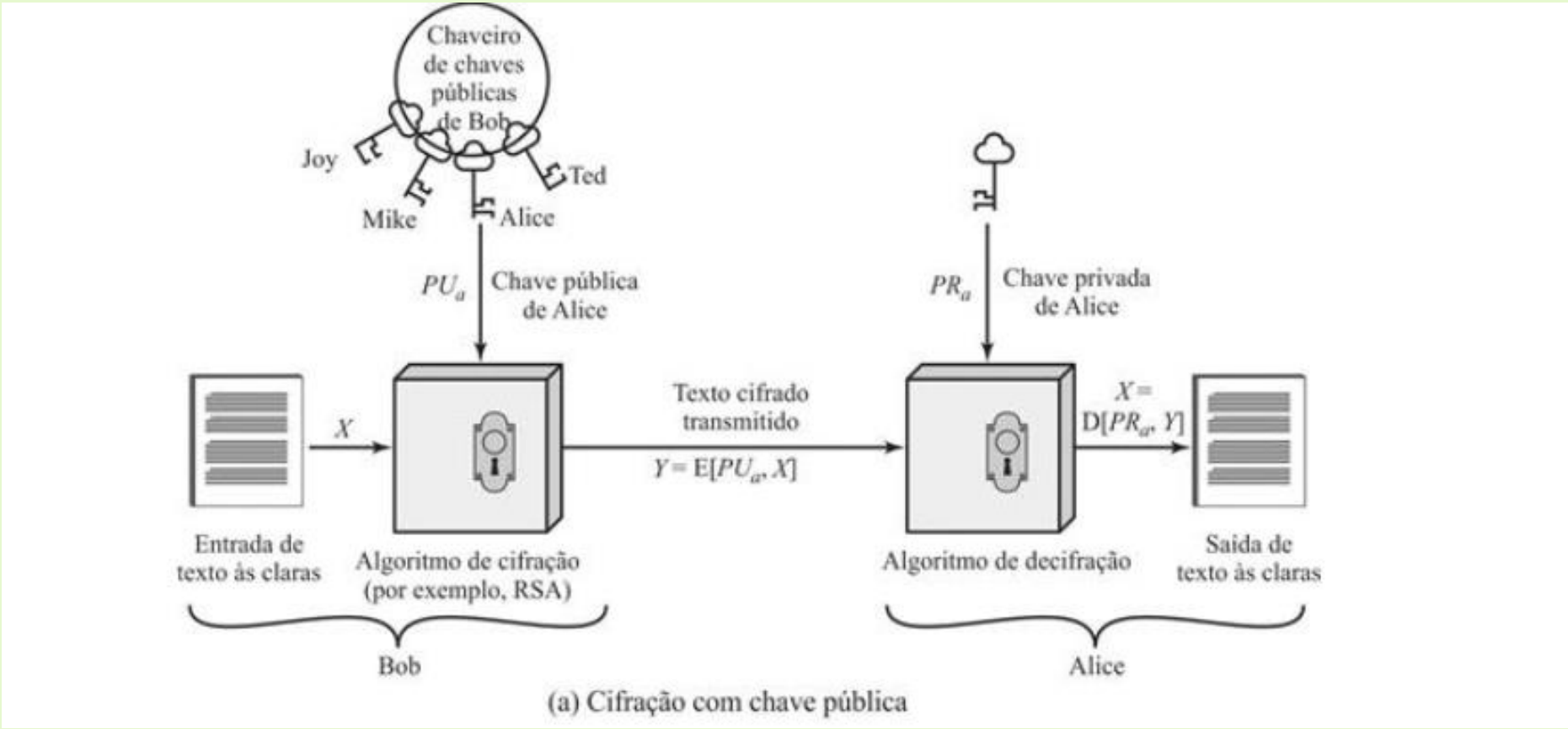
- Centro de Distribuição de Chaves (KDC)
  - **Representa um gargalo por estar sempre on-line;**
- Certificador de Chaves Públicas, CA (Certification Authority)
  - **Vincula uma chave pública a uma entidade através da assinatura digital de um certificado emitido para essa entidade.**

Certificação Digital



Resumindo..

Confidencialidade



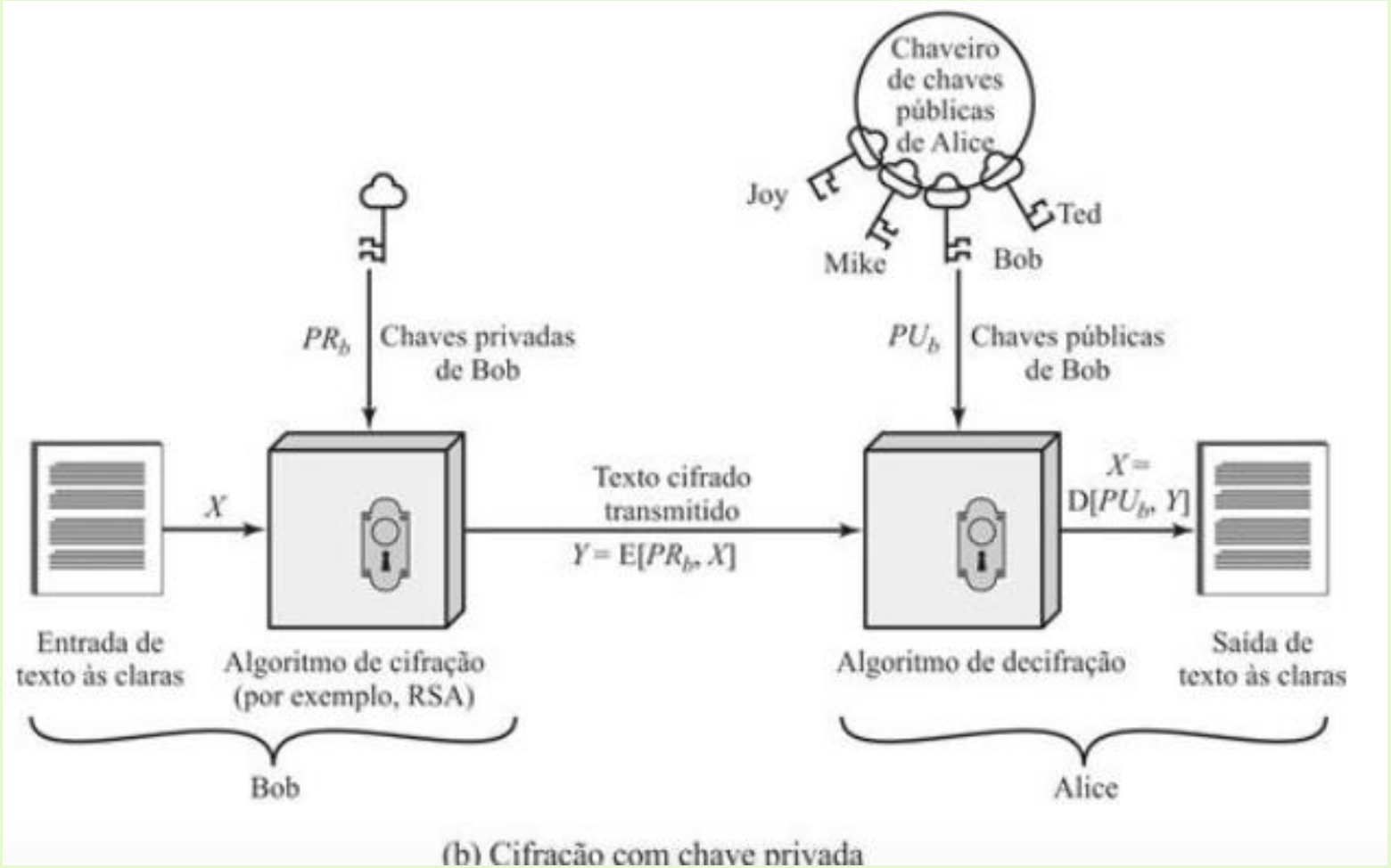
(a) Cifração com chave pública

Resumindo..

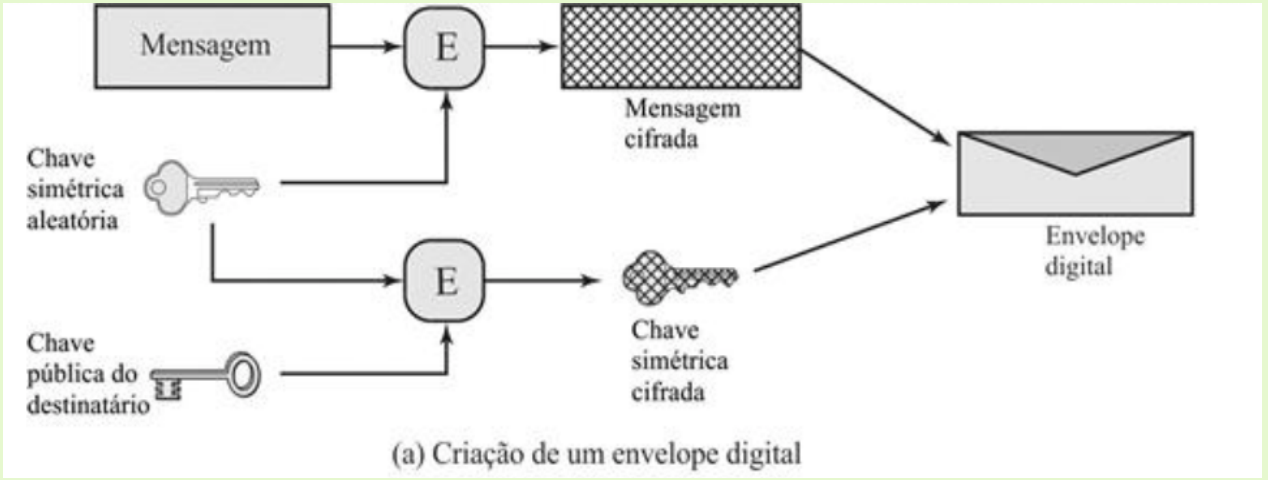
Irretratabilidade

Integridade

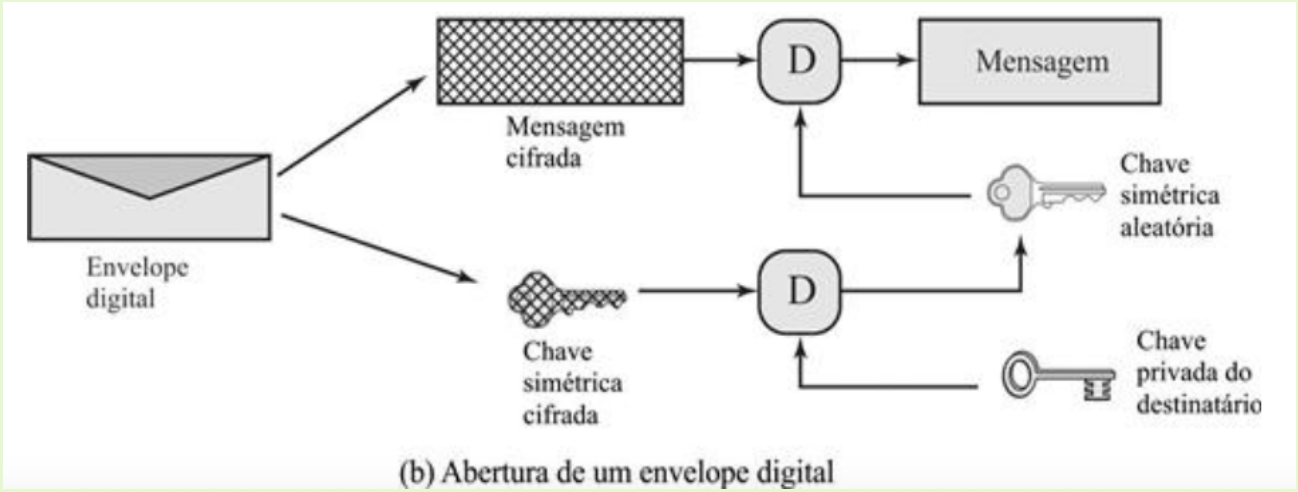
Autenticidade



Envelopes digitais



(a) Criação de um envelope digital



(b) Abertura de um envelope digital

Referências Bibliográficas

Forouzan, Behrouz A. **Comunicação de Dados e Redes de Computadores**. 3ª Ed. – Porto Alegre: Bookman, 2006.