



# **Criptografia Assimétrica**

**Segurança em redes de computadores**

# [ Secções Principais

1. Segurança em redes
2. Criptografia
3. Cifra assimétrica
4. Implementações
5. Aplicações
6. Conclusão
7. Bibliografia



- 1. Segurança em redes**
2. Criptografia
3. Cifra assimétrica
4. Implementações
5. Aplicações
6. Conclusão
7. Bibliografia

# [ Segurança em redes

---

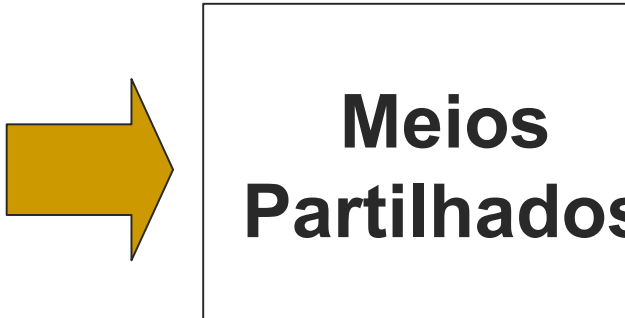
- Necessidade de segurança
  - Ambiente de guerra
  - Transacções comerciais e/ou financeiras
  - Privacidade

# [ Segurança em redes

## ■ Aplicações importantes:

- e-mail (transferência e armazenamento)
- Encaminhadores
- Instant messaging
- Transacções bancárias
- e-shopping
- Transacções financeiras
- Consulta/alteração de informação confidencial
- Outros...

# [ Segurança em redes

- Troca de informação sensível em sistemas distribuídos
  - Segurança em redes de computadores
    - Área local (LAN)
    - Internet
    - Wireless (IEEE 802.11)
- 
- Meios Partilhados**

# [ Segurança em redes

- Mecanismos desejáveis/necessários num ambiente seguro
  - *Confidencialidade*
  - *Integridade (conteúdo e origem)*
  - *Autenticação*
  - *Controlo de acesso*



1. Segurança em redes
2. **Criptografia**
3. Cifra assimétrica
4. Implementações
5. Aplicações
6. Conclusão
7. Bibliografia

# [ Criptografia

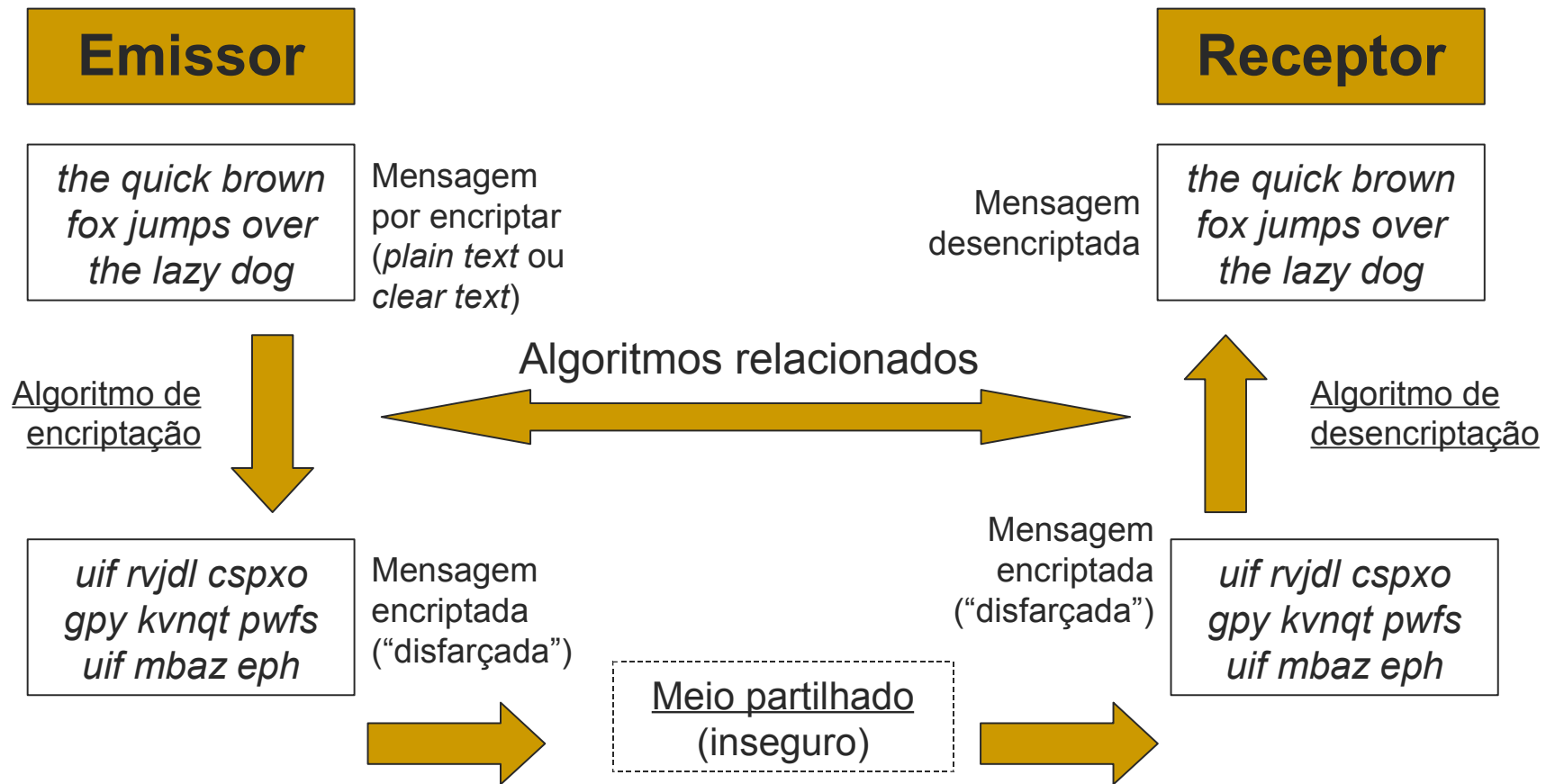
- Confidencialidade em ambiente partilhado
- Apenas as partes “autorizadas” entendem as mensagens

# [ Criptografia

---

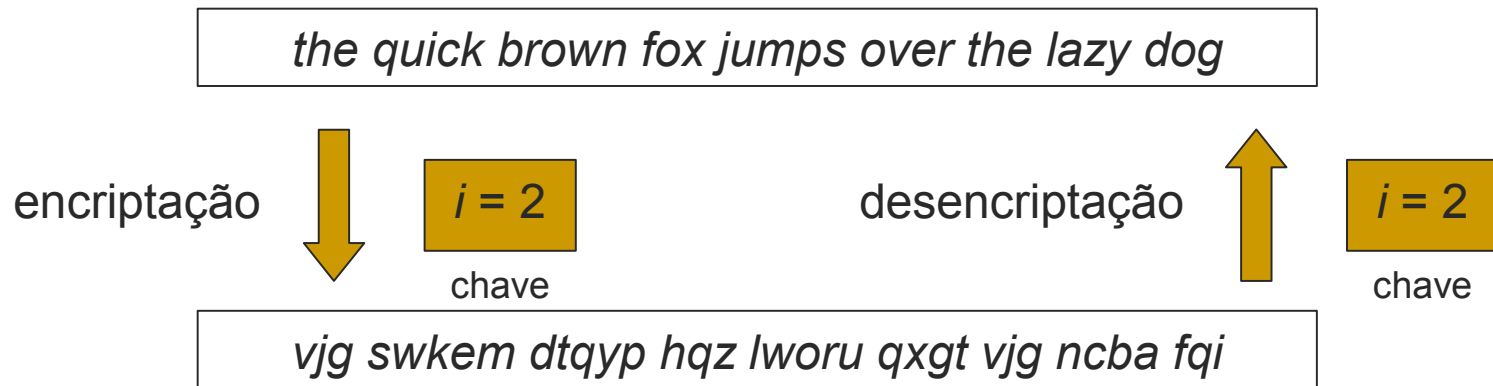
- Algoritmo de processamento de mensagens
- Encriptação no emissor
- Desencriptação no receptor

# Criptografia



# Criptografia

- Exemplo: cifra de Caesar
  - Cada letra da mensagem é substituída pela próxima  $i$ -ésima letra do alfabeto:



# [ Criptografia

---

- Tipos básicos:
  - Chave simétrica
  - Chave assimétrica



1. Segurança em redes
2. Criptografia
3. **Cifra assimétrica**
4. Implementações
5. Aplicações
6. Conclusão
7. Bibliografia

# Cifra assimétrica

- Tipo de algoritmo de criptografia
- A chave utilizada para encriptar difere da chave utilizada para descriptar

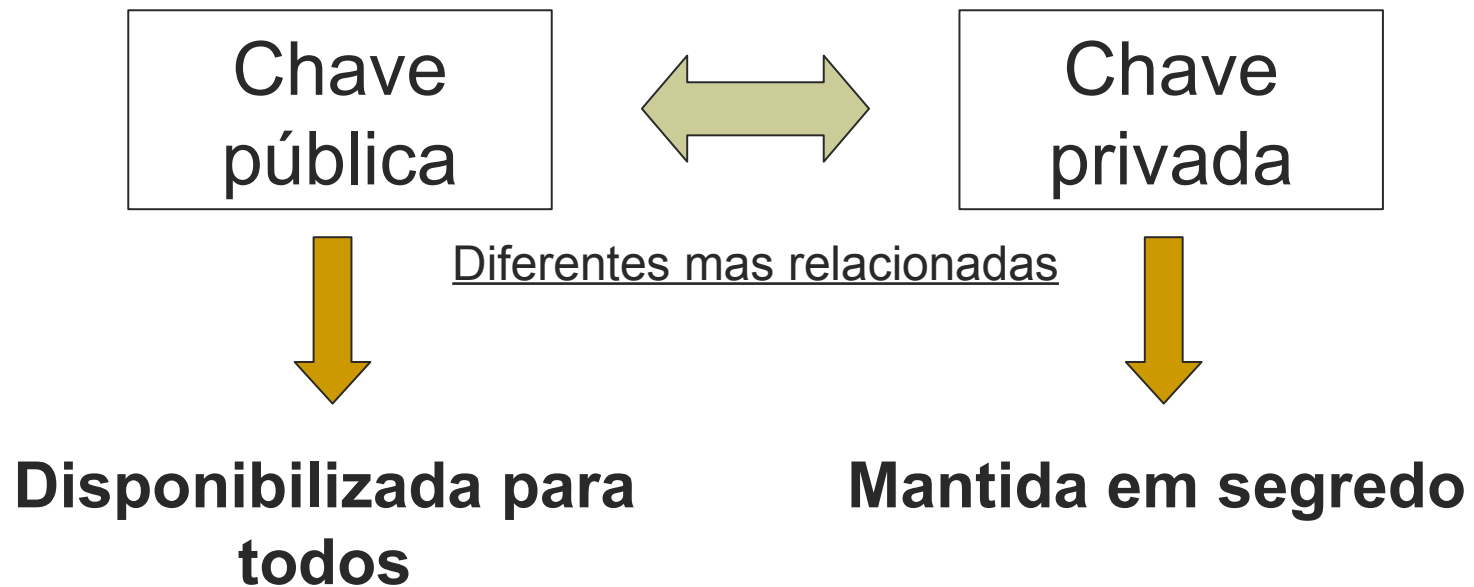
**Não precisa de chave secreta  
partilhada**

# [ Cifra assimétrica

- Baseada no algoritmo *Diffie-Hellman key exchange*
- Propriedades para além da confidencialidade
  - **Autenticação**
  - **Integridade**

# Cifra assimétrica

- Cada utilizador tem um par de chaves

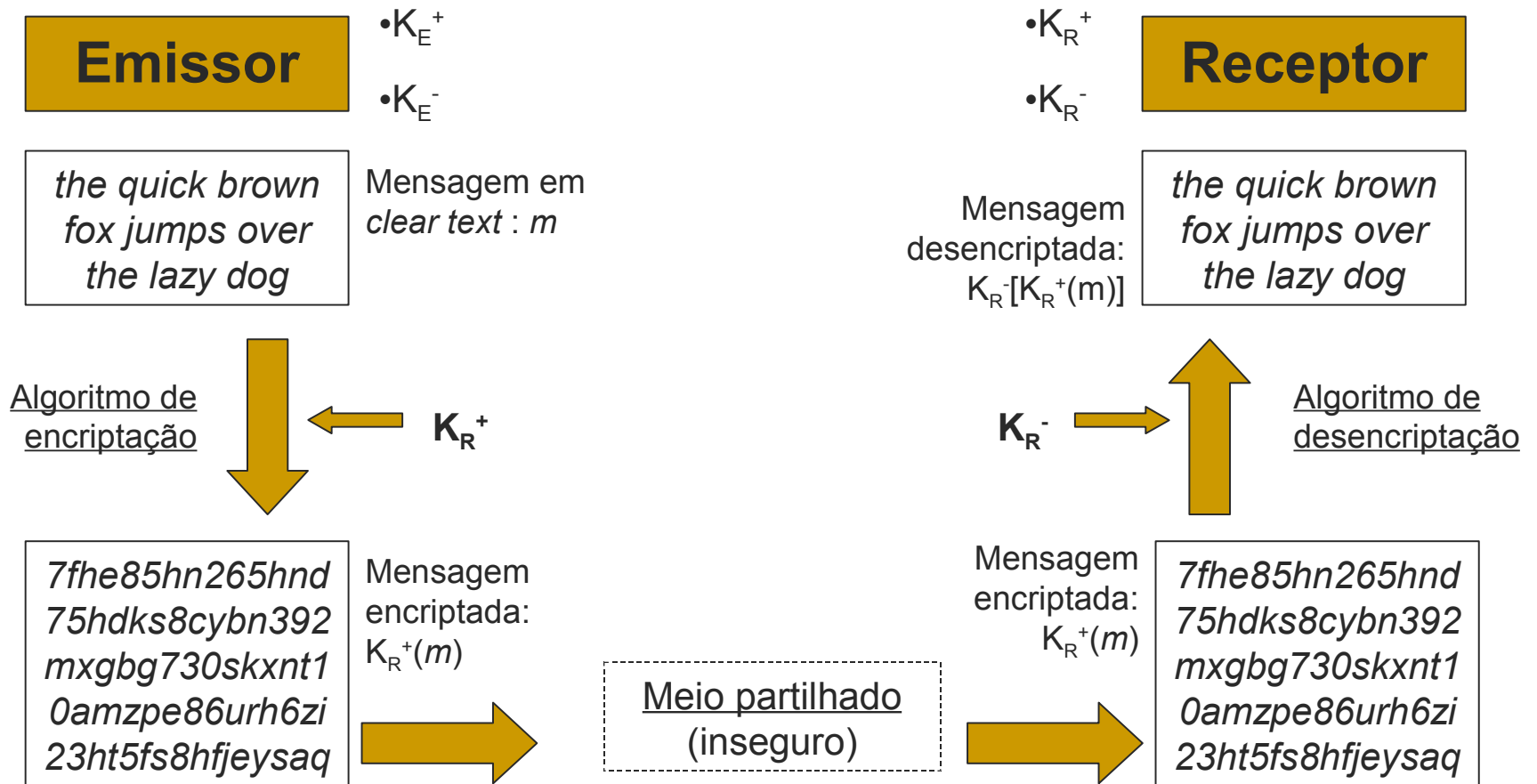


# Cifra assimétrica

## ■ Nomenclatura:

- $K^+$  - chave pública
- $K^-$  - chave privada
- $K(m)$  – encriptação da mensagem  $m$  com a chave  $K$
- $K_A$  – chave do utilizador “A”

# Cifra assimétrica



# Cifra assimétrica

- Propriedade fundamental:

$$K_Z^- [K_Z^+ (m)] = m$$

- Consequências:
  - Necessário conhecer a chave pública do receptor
  - As chaves privadas não podem ser comprometidas

# Cifra assimétrica

- Confidencialidade:
  - O algoritmo e as chaves têm que garantir a impossibilidade computacional de calcular  $K^-$  a partir de  $K^+$ .

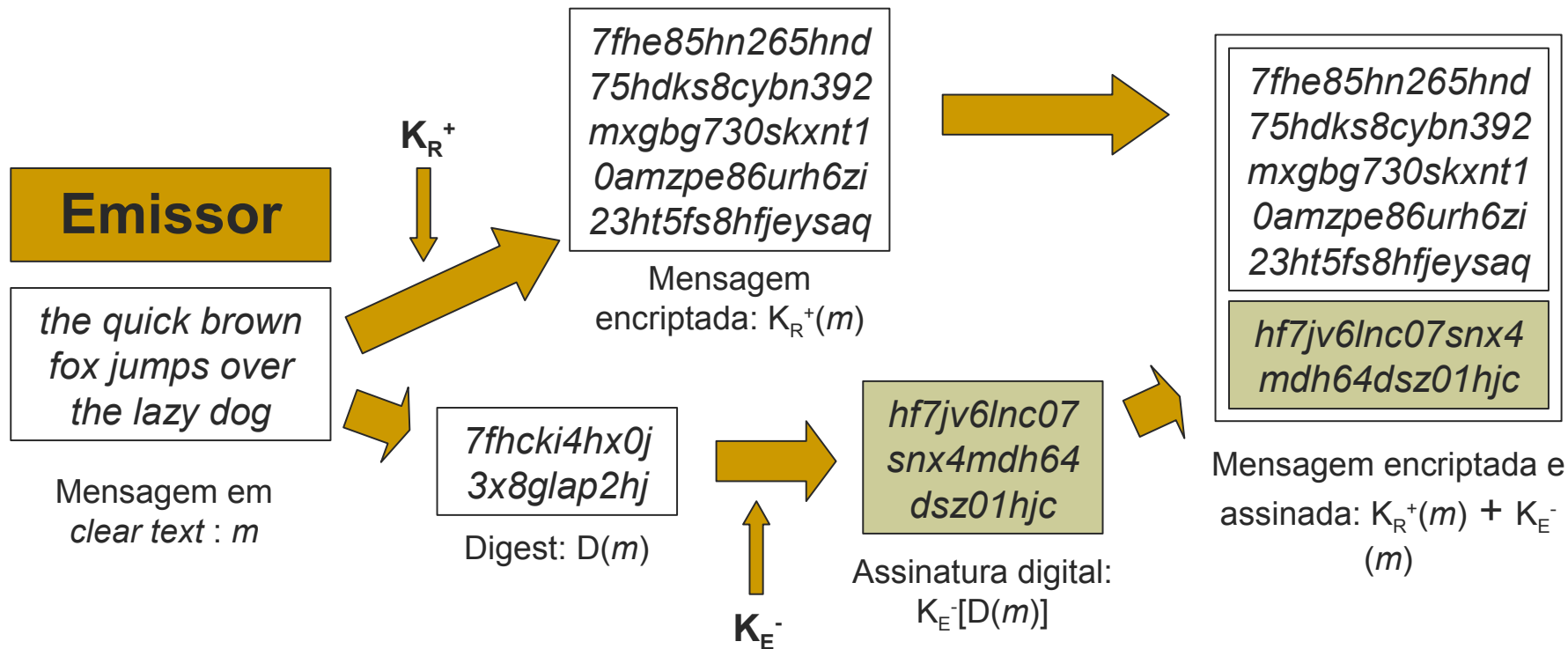
# [ Cifra assimétrica

---

- Integridade:
  - Qualquer utilizador pode encriptar uma mensagem e enviá-la ao receptor. Como saber se o emissor é quem diz ser?

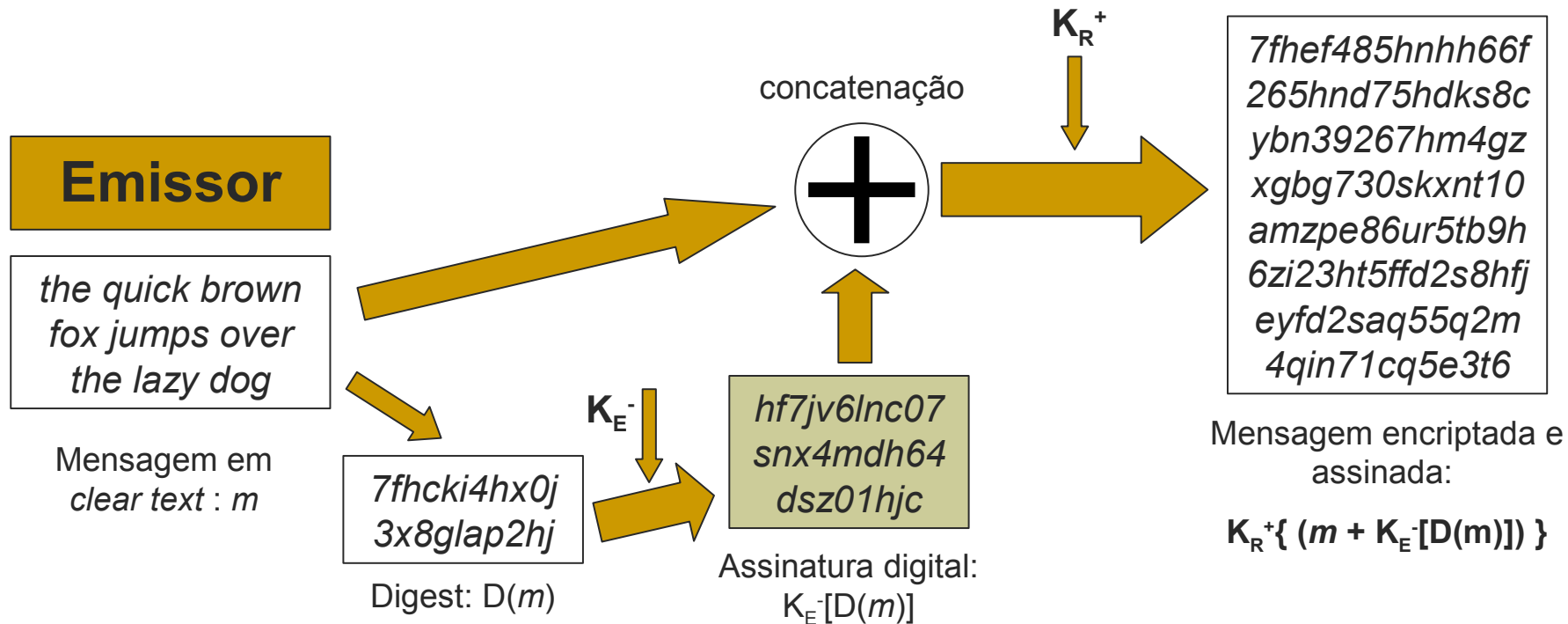
# Cifra assimétrica

## ■ Digital Signature: emissão



# Cifra assimétrica

## ■ Digital Signature: emissão

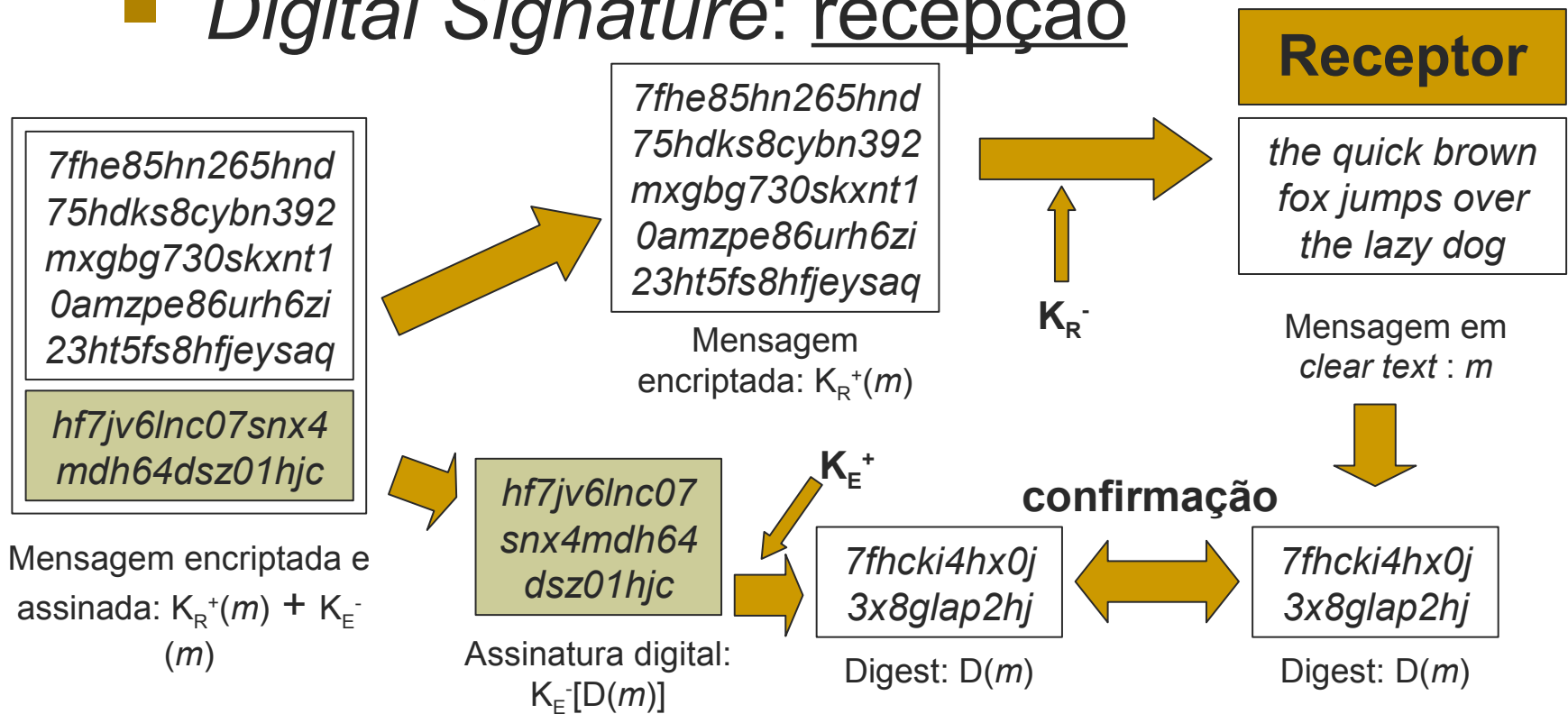


# Cifra assimétrica

- *Digest*  $D(m)$ :
  - Computacionalmente impossível: encontrar  $m_1$  e  $m_2$  tal que  $D(m_1)=D(m_2)$
  - Impossível calcular  $m$  a partir de  $D(m)$ 
    - Função hash: não unívoca
  - Cálculo muito rápido

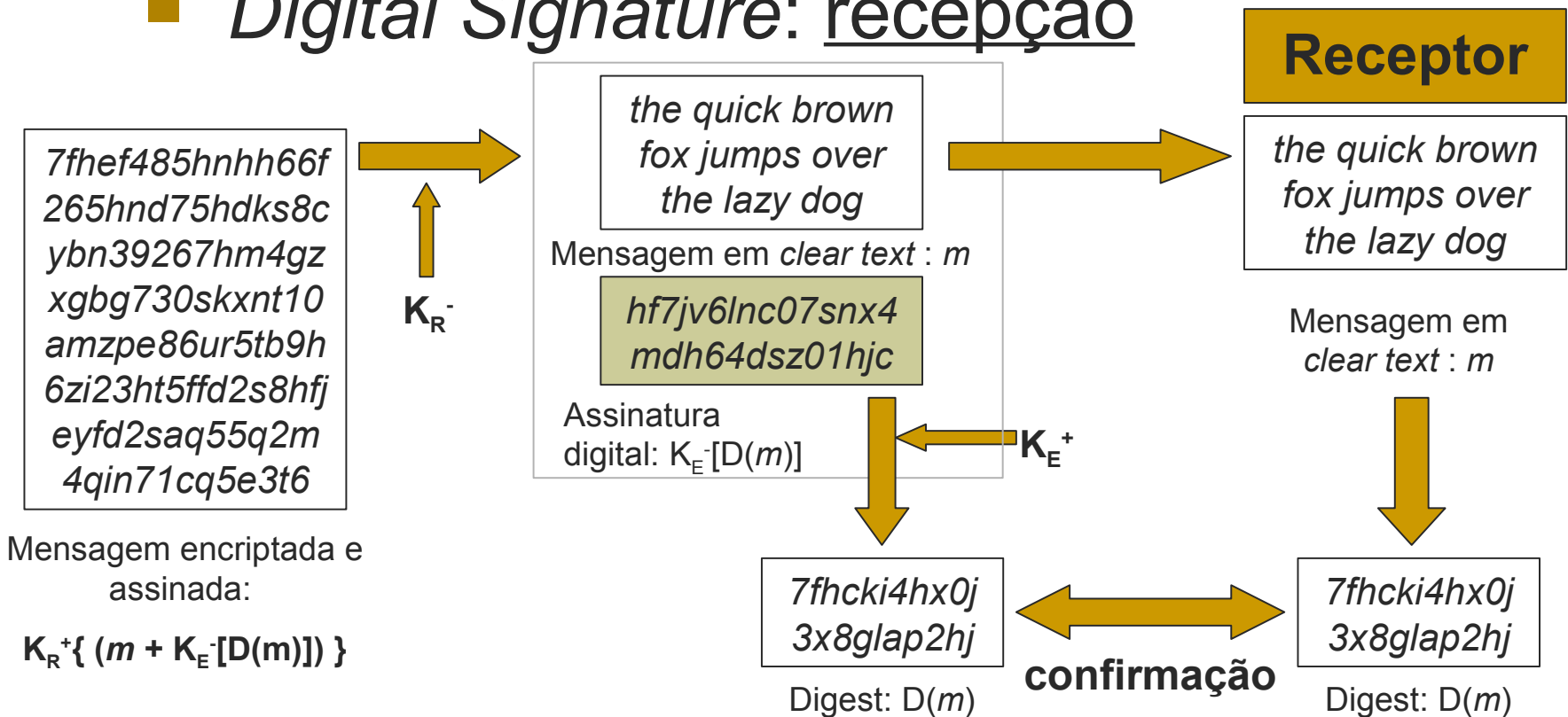
# Cifra assimétrica

## Digital Signature: recepção



# Cifra assimétrica

## Digital Signature: recepção



# Cifra assimétrica

- Algoritmo D conhecido por ambos os intervenientes
- $D(m)$  é cifrado com a chave privada do emissor.
- Se a mensagem for genuína, no receptor:
  - $D(m)$  calculado iguala  $D(m)$  recebido

# Cifra assimétrica

- Chave pública sujeita ao ataque “man in the middle”
  - Resolve-se com chaves públicas certificadas
    - Entidade externa certifica autenticidade de chaves públicas através da inserção da sua assinatura digital
  - Resolve-se também com servidores de distribuição de chaves
    - Utilização de chave simétrica previamente acordada com cada utilizador para trocar chaves públicas

# Cifra assimétrica

- Ineficiente face a encriptação simétrica
  - 100 vezes mais lento do que DES por software
  - 1000 - 10000 vezes mais lento que DES por hardware
- Solução de compromisso
  - Utilização de cifra assimétrica para acordar chave simétrica



1. Segurança em redes
2. Criptografia
3. Cifra assimétrica
- 4. Implementações**
5. Aplicações
6. Conclusão
7. Bibliografia

# Implementações

## ■ RSA

1. Escolhem-se  $p$  e  $q$  aleatórios e primos
2.  $p, q$  maiores:
  - Mais difícil de decifrar
  - Processo mais lento
3. Calcula-se  $n = p \times q$
4. Calcula-se  $z = (p-1) \times (q-1)$
5. Escolhe-se  $e < n$  sem factores comuns com  $z$  ( $e$  e  $z$  dizem-se primos relativos)
6. Encontra-se  $d$  tal que  $(e \times d - 1)$  seja divisível por  $z$

# Implementações

- $K^+ = (n, e)$
- $K^- = (n, d)$
- A mensagem é codificada em ASCII e encriptada byte a byte
- $K^+(m) = c = m^e \text{ mod } n$
- $K^-[K^+(m)] = m = c^d \text{ mod } n$
- $K^-[K^+(m)] = K^+[K^-(m)]$

# Implementações

- Segurança do algoritmo RSA:
  - Não existem algoritmos eficientes na factorização de números
    - Não se sabe sequer se existem algoritmos rápidos de factorização
  - $n = p \times q$
  - $z = (p-1) \times (q-1)$
  - $e$  e  $z$  primos entre si
  - $exd-1$  divisível por  $z$



1. Segurança em redes
2. Criptografia
3. Cifra assimétrica
4. Implementações
5. **Aplicações**
6. Conclusão
7. Bibliografia

# Aplicações

- **SSL – *secure sockets layer***
  1. Servidor envia a sua chave pública ( $K_S^+$ )
  2. Cliente cifra a chave simétrica com  $K_S^+$  e envia para o servidor
  3. Cliente e servidor cifram a comunicação com a chave simétrica acordada

# [ Aplicações

---

- SSL

- Imaps

- https

- Pops

- Secure smtp

- ssh – *secure shell*

- Utiliza um método semelhante ao SSL

# [ Aplicações

- gpg - *Gnu Privacy Guard*
  - Encriptação e assinatura de e-mail
  - Utilização de chave pública (possivelmente certificada) e chave simétrica
  - E-mails tipicamente curtos: tempo de processamento desprezável



1. Segurança em redes
2. Criptografia
3. Cifra assimétrica
4. Implementações
5. Aplicações
- 6. Conclusão**
7. Bibliografia

# [ Conclusão

---

- Vantagens:
  - Encriptação “forte”
  - Permite resolver o problema da confidencialidade e da integridade

# [ Conclusão

- Desvantagens
  - Sujeita a ataques do tipo “man in the middle”
    - Distribuição de chaves públicas sujeita a cuidados especiais
  - Lenta face a encriptação simétrica

# [ Conclusão

---

- Utilização:
  - Compromisso: utilizada em conjunto com encriptação simétrica



1. Segurança em redes
2. Criptografia
3. Cifra assimétrica
4. Implementações
5. Aplicações
6. Conclusão
7. **Bibliografia**

# [ Bibliografia

---

- James F. Kurose, Keith W. Ross, *Computer Networking*, Addison-Wesley, 2003
- <http://www.rsasecurity.com/rsalabs/faq/>