# Segurança da Informação

**Criptografia, protocolos seguros e suas aplicações**

# Criptografia – Serviços Oferecidos

| Serviços | Descrição |
|---|---|
| Disponibilidade | Garante que uma informação estará disponível para acesso no momento desejado. |
| Integridade | Garante que o conteúdo da mensagem não foi alterado. |
| Controle de acesso | Garante que o conteúdo da mensagem será acessado somente por pessoas autorizadas. |
| Autenticidade da origem | Garante a identidade de quem está enviando a mensagem. |
| Não-repudiação | Previne que alguém negue o envio e/ou recebimento de uma mensagem. |
| Privacidade (confidencialidade ou sigilo) | Impede que pessoas não autorizadas tenham acesso ao conteúdo da mensagem, garantindo que apenas a origem e o destino tenham conhecimento. |

# Criptografia – Serviços Oferecidos

**Exemplo de aplicação**: Compra pela Internet

- Informação que permite a transação - valor e descrição do produto adquirido - precisa estar disponível no dia e na hora que o cliente desejar efetuá-la (**disponibilidade**).
- O valor da transação não pode ser alterado (**integridade**).
- Somente o cliente que está comprando e o comerciante devem ter acesso à transação (**controle de acesso**).
- O cliente que está comprando deve ser quem diz ser (**autenticidade**).
- O cliente tem como provar o pagamento e o comerciante não tem como negar o recebimento (**não-repúdio**).
- O conhecimento do conteúdo da transação fica restrito aos envolvidos (**privacidade**).

# Fundamentos de Criptografia

- Componentes básicos para o ciframento de uma mensagem:
  - ***algoritmo***
  - ***chave***

**Princípio de Kerckhoff (1883)**: *Todos os algoritmos devem ser públicos; apenas as chaves são secretas*.

**Algoritmo secreto**: segurança pela obscuridade.

# Fundamentos de Criptografia

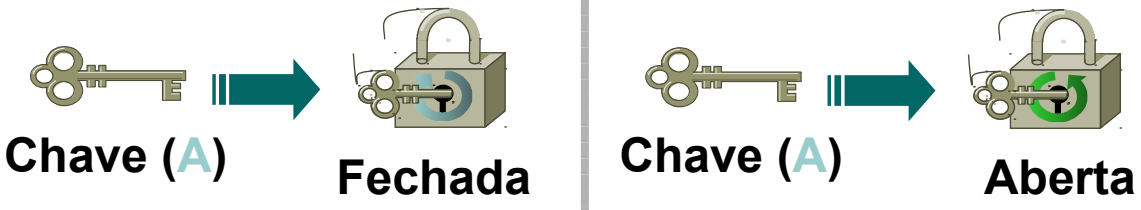
**Vantagens importantes para o uso de chaves**

- Permite a utilização do mesmo algoritmo criptográfico para a comunicação com diferentes receptores, trocando apenas a chave.
- Permite trocar facilmente a chave no caso de uma violação, mantendo o mesmo algoritmo.
- Número de chaves possíveis depende do tamanho (número de bits) da chave.
  - **Exemplo**: uma chave de 8 bits permite uma combinação de no máximo 256 chaves. Quanto maior o tamanho da chave, mais difícil quebrá-la.

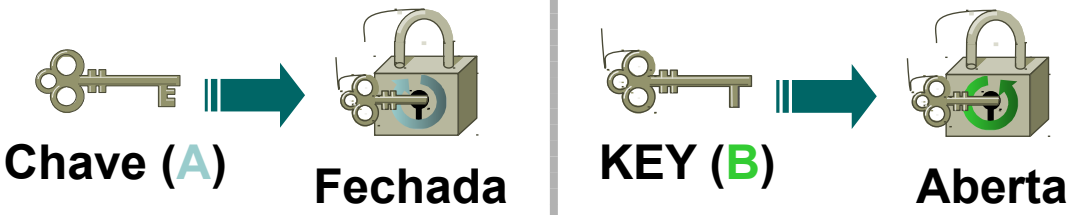
# Criptografia - Tipos

**Tipos básicos de Criptografia**
**(em relação ao uso de chaves)**

- **Criptografia Simétrica (chave secreta)**




- **Criptografia Assimétrica (chave pública)**



# Criptografia Simétrica

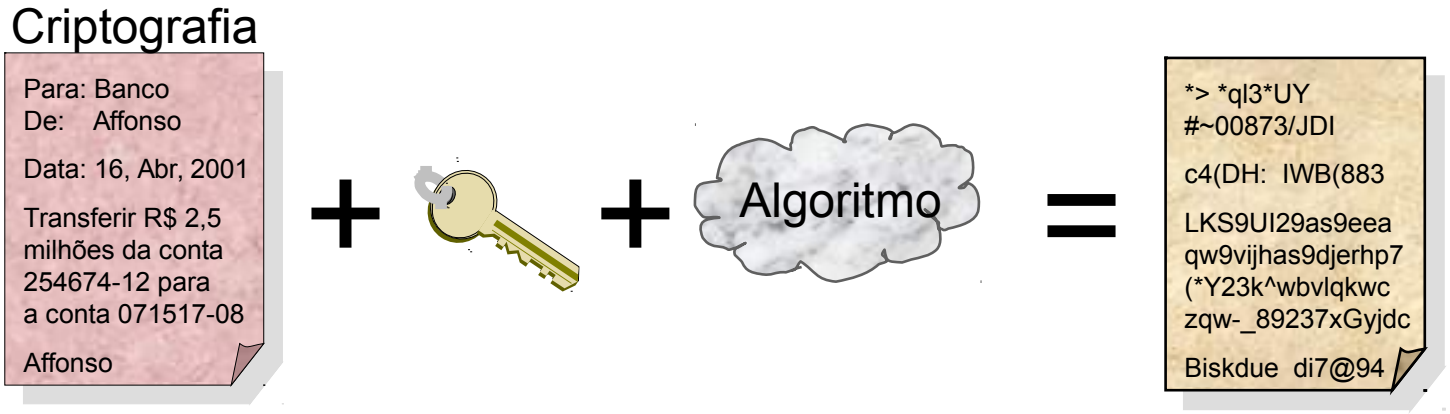
**Texto claro**  **Mensagem cifrada**

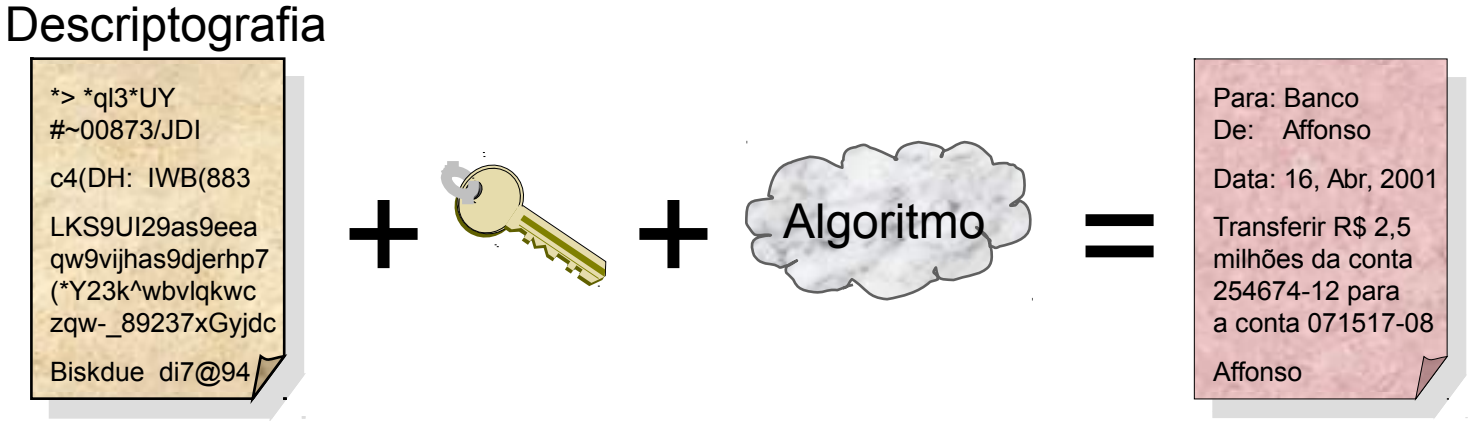
- Utiliza uma mesma chave tanto para cifrar como para decifrar (ou pelo menos a chave de decifração pode ser obtida trivialmente a partir da chave de cifração)

**A mesma chave utilizada para "fechar o cadeado" é utilizada para "abrir o cadeado".**

# Criptografia Simétrica

**Criptografia Simétrica** - Requer uma chave compartilhada



# Criptografia Simétrica

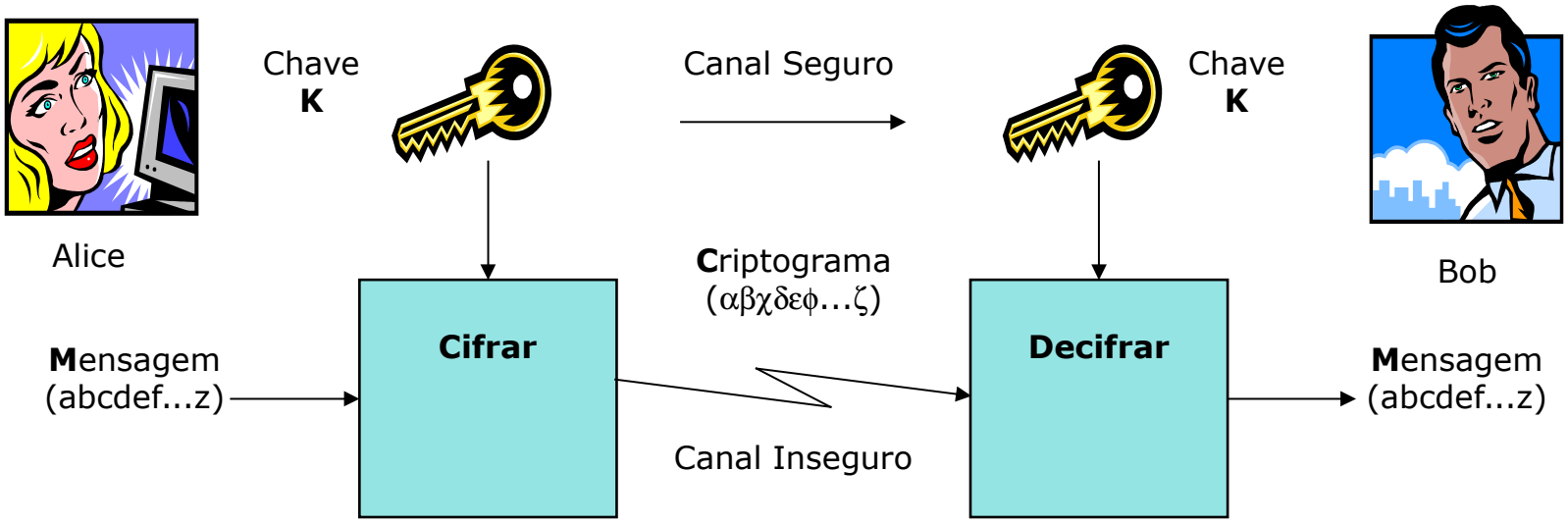
- **Algoritmos simétricos** - exigem que a chave seja mantida secreta, do conhecimento exclusivo dos dois interlocutores.

- É requerido um ***canal seguro*** que permita a um usuário transmitir a chave ao seu interlocutor.

Se uma pessoa quer se comunicar com outra com segurança, ela deve passar primeiramente a chave utilizada para cifrar a mensagem. Este processo é chamado **distribuição de chaves**.

# Criptografia Simétrica

Uso de algoritmo criptográfico **simétrico** (chave secreta)



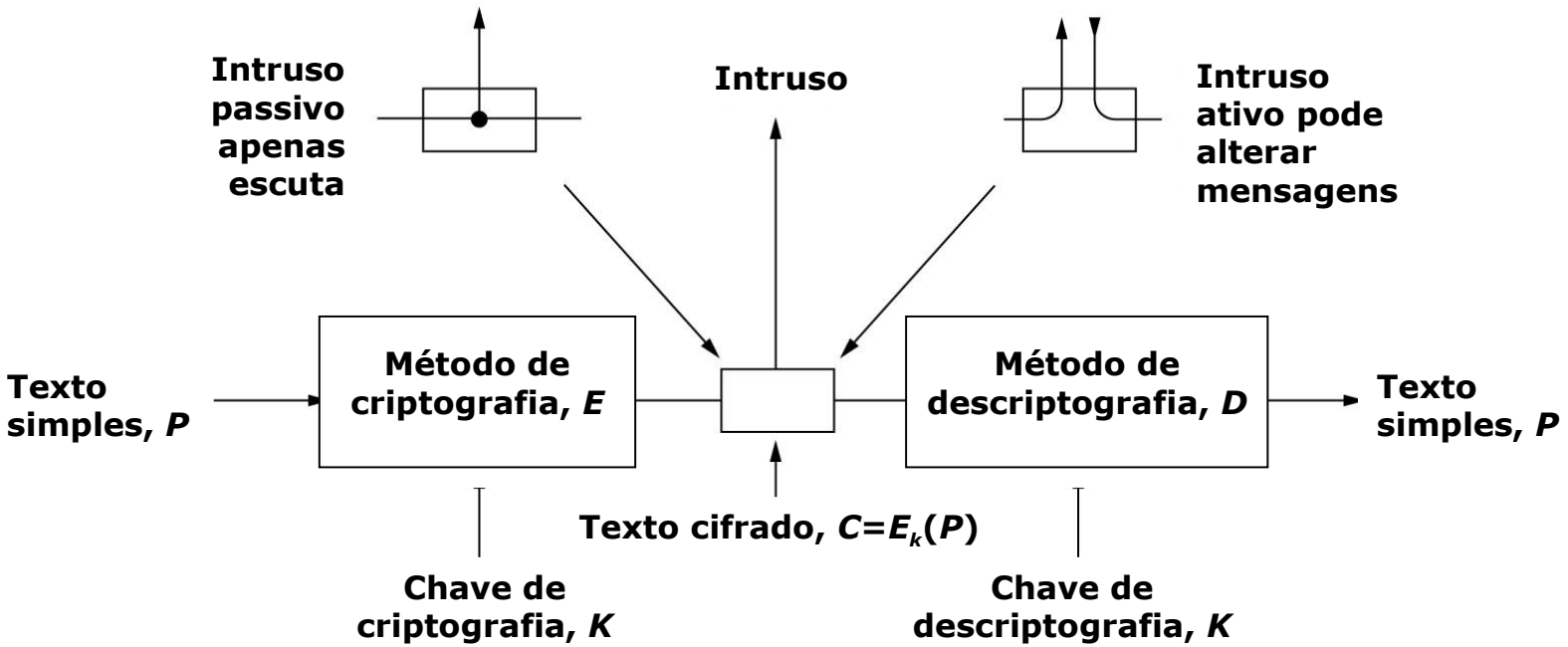

Alice e Bob precisam **acordar** uma chave secreta que irá proteger as mensagens trocadas entre eles.

# Criptografia Simétrica

- *Alice* **cifra** uma mensagem - utiliza um algoritmo de ciframento e uma chave secreta para transformar uma mensagem clara em um texto cifrado.
- *Bob* **decifra** uma mensagem - utiliza o algoritmo de deciframento correspondente e a mesma chave para transformar o texto cifrado em uma mensagem em claro.
- *Eva* - não possui a chave secreta, mesmo conhecendo o algoritmo, não consegue decifrar a mensagem.
- **A segurança do sistema reside não mais no algoritmo e sim na chave empregada**. É ela que agora, no lugar do algoritmo, deverá ser mantida em segredo por *Alice* e *Bob*.

# Criptografia Simétrica

**Modelo de criptografia (para uma cifra de chave simétrica)**




$$D_k(E_k(P)) = P$$

# Criptografia Simétrica

## Tipos de cifras utizadas

- **Cifras de corrente**: quando se cria uma chave aleatória com o mesmo tamanho do texto a ser cifrado, e combina-se a chave com a mensagem a ser enviada.

- **Cifras de Bloco**: aceita um grupo de bits ou bloco de dados, podendo ser utilizados em cadeia. geralmente usados para grandes quantidades de dados.

# Criptografia Simétrica

**Exemplos de algoritmos que utilizam chaves secretas:**

- **DES**
- **Triple DES**
- **IDEA**
- **RC2**

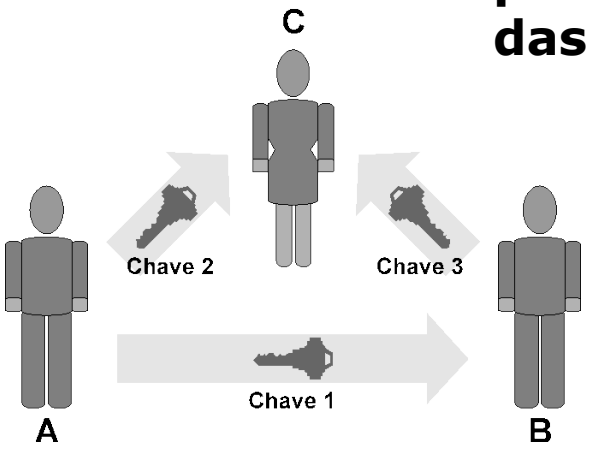
# Criptografia Simétrica

- **Vantagem**
  - Rapidez na criptografia e descriptografia da informação.

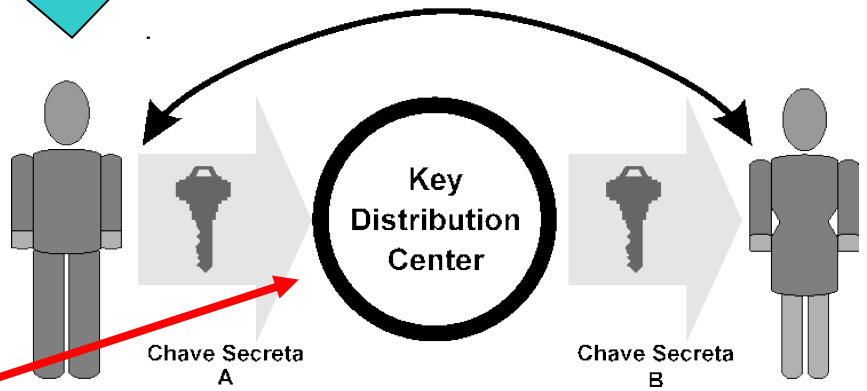
- **Desvantagens**
  - A chave deve ser trocada entre as partes e armazenada de forma segura, o que nem sempre é fácil de garantir;
  - A criptografia simétrica não garante a identidade de quem enviou ou recebeu a mensagem (autenticidade e não-repudiação).
  - Cada par necessita de uma chave para se comunicar de forma segura. Em geral, se *n* pessoas querem se comunicar usando chave secreta, serão necessárias $\frac{(n)(n-1)}{2}$ chaves - problema para o gerenciamento de chaves.

# Criptografia Simétrica

**Proposta de solução para o problema da distribuição das chaves secretas**




**Forma tradicional**




**Forma moderna: Uso de um Centro de Distribuição de Chaves (KDC)**

**Possíveis problemas?**

# Criptografia Assimétrica

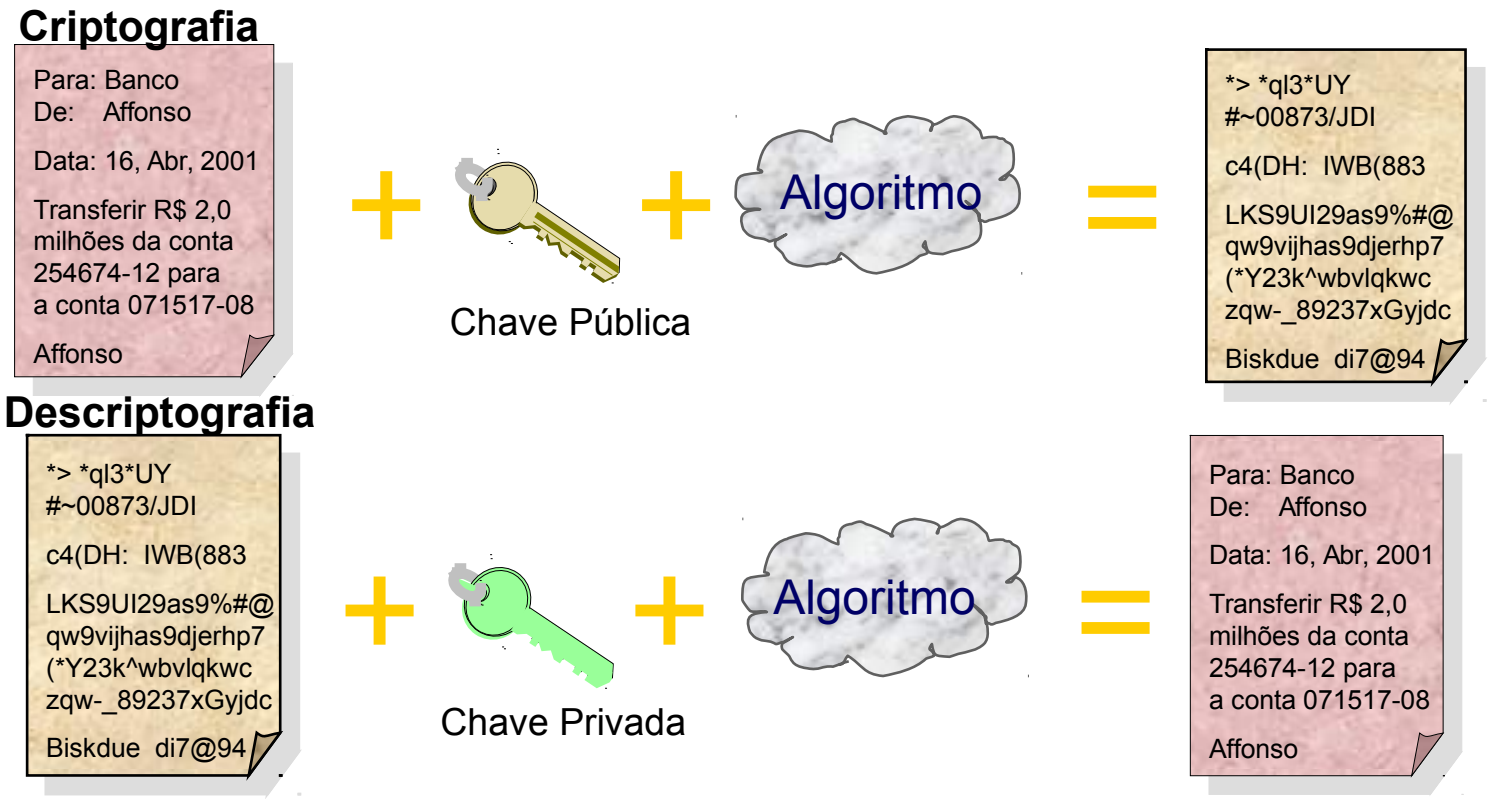
**Texto claro**  **Mensagem cifrada**

- As chaves são sempre geradas aos pares: uma para cifrar e a sua correspondente para decifrar.
- A chave pública é divulgada, a chave privada é proprietária (normalmente não abandona o ambiente onde foi gerada).

**Uma chave é utilizada para "fechar o cadeado" e outra chave, diferente, mas relacionada à primeira, é utilizada para "abrir o cadeado"**

# Criptografia Assimétrica

**Criptografia Assimétrica** - Não possui segredos compartilhados




As duas chaves são relacionadas através de um processo matemático, usando funções unidirecionais para a codificação da informação.

# Criptografia Assimétrica

- **Algoritmos assimétricos** - permitem que **a chave de cifração possa ser tornada pública**, disponibilizando-a em um "canal público" (Ex.: repositório de acesso público) - **chave-pública**.

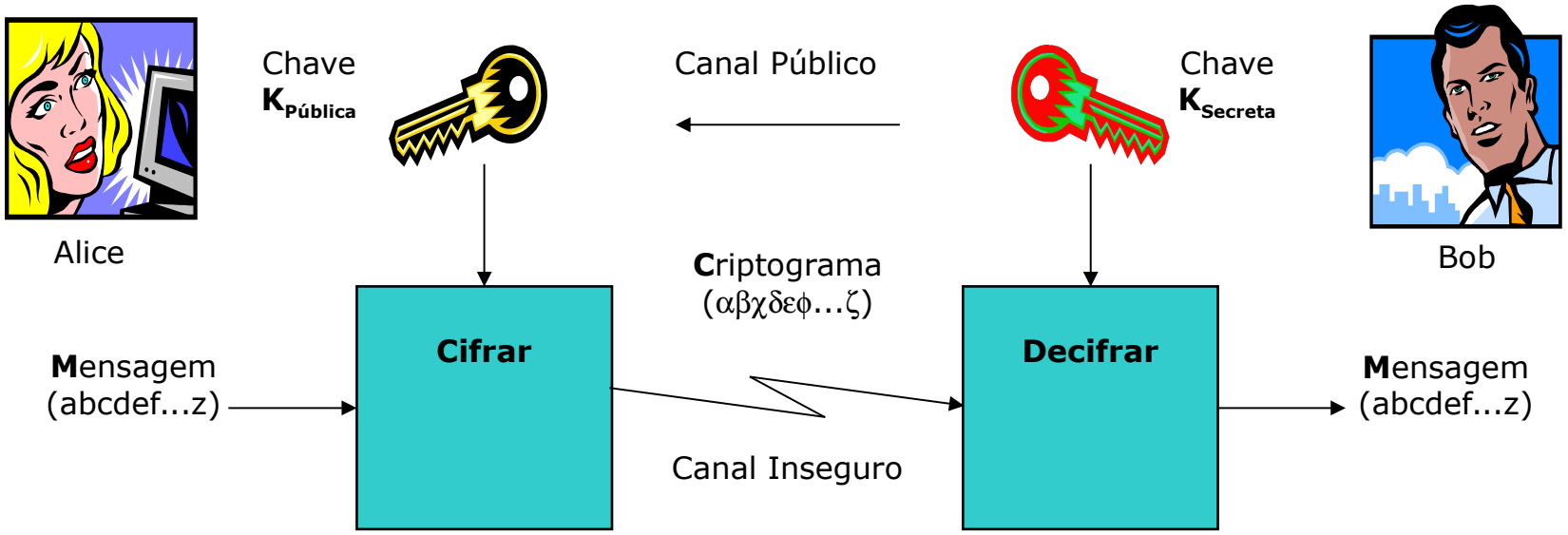
- Qualquer um pode cifrar mensagens com uma dada chave-pública.

- Somente o destinatário, detentor da correspondente chave de decifração (**chave-privada**, ou **secreta**), poderá decifrar a mensagem.

A chave-privada não precisa e nem deve ser dada a conhecer a ninguém, devendo ser guardada em segredo pelo seu detentor apenas, que deve também ter sido o responsável pela geração do seu *par de chaves*, enquanto a chave-pública pode ser publicada livremente.

# Criptografia Assimétrica

Uso de algoritmo criptográfico **assimétrico** (chave pública).




Para que Alice envie uma mensagem confidencial a Bob, ela deve encriptar essa mensagem com a chave pública de Bob que, de posse de sua chave privada, consegue descriptá-la. Como, em tese, ninguém tem acesso à chave privada de Bob, ninguém pode descriptar a mensagem.

# Criptografia Assimétrica

- **Descrição do funcionamento do sistema**
  (forma simplificada)
  - *Bob* e todos os que desejam comunicar-se de modo seguro geram uma chave de ciframento e sua correspondente chave de deciframento.
  - Bob mantém secreta a chave de deciframento; esta é chamada de sua *chave privada*.
  - Bob torna pública a chave de ciframento: esta é chamada de sua *chave pública*.
  - Qualquer pessoa pode obter uma cópia da chave pública. *Bob* encoraja isto, enviando-a para seus amigos ou publicando-a em boletins. *Eva* não tem nenhuma dificuldade em obtê-la.

# Criptografia Assimétrica

- **Descrição do funcionamento do sistema**
  (forma simplificada)
  - *Alice* deseja enviar uma mensagem a *Bob*: precisa primeiro encontrar a chave pública dele. Feito isto, ela cifra sua mensagem utilizando a chave pública de *Bob*, despachando-a em seguida.
  - *Bob* recebe a mensagem, a decifra facilmente com sua chave privada.
  - *Eva*, que interceptou a mensagem em trânsito, não conhece a chave privada de *Bob*, embora conheça sua chave pública. Mas este conhecimento não a ajuda a decifrar a mensagem.
  - Mesmo *Alice*, que foi quem cifrou a mensagem com a chave pública de *Bob*, não pode decifrá-la agora.

# Criptografia Assimétrica

- **Algoritmo deve atender 3 requisitos básicos:**

1. ***D*(*E*(*P*)) = *P***.
2. É extremamente difícil deduzir ***D*** a partir de ***E***.
3. ***E*** não pode ser decifrado por um ataque de **texto simples escolhido**.

**Três principais variações para a Criptoanálise**:

- **Texto cifrado** – determinado volume de texto cifrado e nenhum texto simples.
- **Texto simples conhecido** – há uma correspondência entre o texto cifrado e o texto simples.
- **Texto simples escolhido** – criptoanalista tem a possibilidade de codificar trechos do texto simples escolhidos por ele mesmo.

# Criptografia Assimétrica

**Exemplos de algoritmos que utilizam chaves públicas:**

- **RSA**
- **ElGamal**
- **Diffie-Hellman**
- **Curvas Elípticas**

# Criptografia Simétrica *x* Assimétrica

**Número de chaves necessárias/número de participantes**

| Nº de participantes | Criptografia Simétrica $n(n-1)/2$ | Criptografia Assimétrica $2n$ |
|---|---|---|
| 2 | 1 | 4 |
| 4 | 6 | 8 |
| 8 | 28 | 16 |
| 16 | 120 | 32 |

# Criptografia Simétrica *x* Assimétrica

| Simétrica | Assimétrica |
|---|---|
| **Funcionamento**<br>○ Utiliza um algoritmo e uma chave para cifrar e decifrar<br><br>**Requisito de Segurança**<br>○ A chave tem que ser mantida em segredo<br>○ Tem que ser impossível decifrar a mensagem<br>○ Algoritmo mais alguma parte do texto cifrado devem ser insuficientes para obter a chave | **Funcionamento**<br>○ Utiliza um algoritmo e um par de chaves para cifrar e decifrar<br><br>**Requisito de Segurança**<br>○ Uma chave é pública e a outra tem que ser mantida em segredo<br>○ Algoritmo com alguma parte do texto cifrado com uma das chaves não devem ser suficientes para obter a outra chave |

# Criptografia Simétrica *x* Assimétrica

**Problemas**

- **Criptografia Simétrica**
  - Como distribuir e armazenar as chaves secretas de forma segura?
  - Quantas chaves são necessárias para uma comunicação segura entre *n* pessoas?
- **Criptografia Assimétrica**
  - Como garantir que o detentor da chave pública é realmente quem diz ser?
  - Necessidade de ter uma infra-estrutura para armazenar as chaves públicas.

# Criptografia Simétrica *x* Assimétrica

**Assinatura Digital**

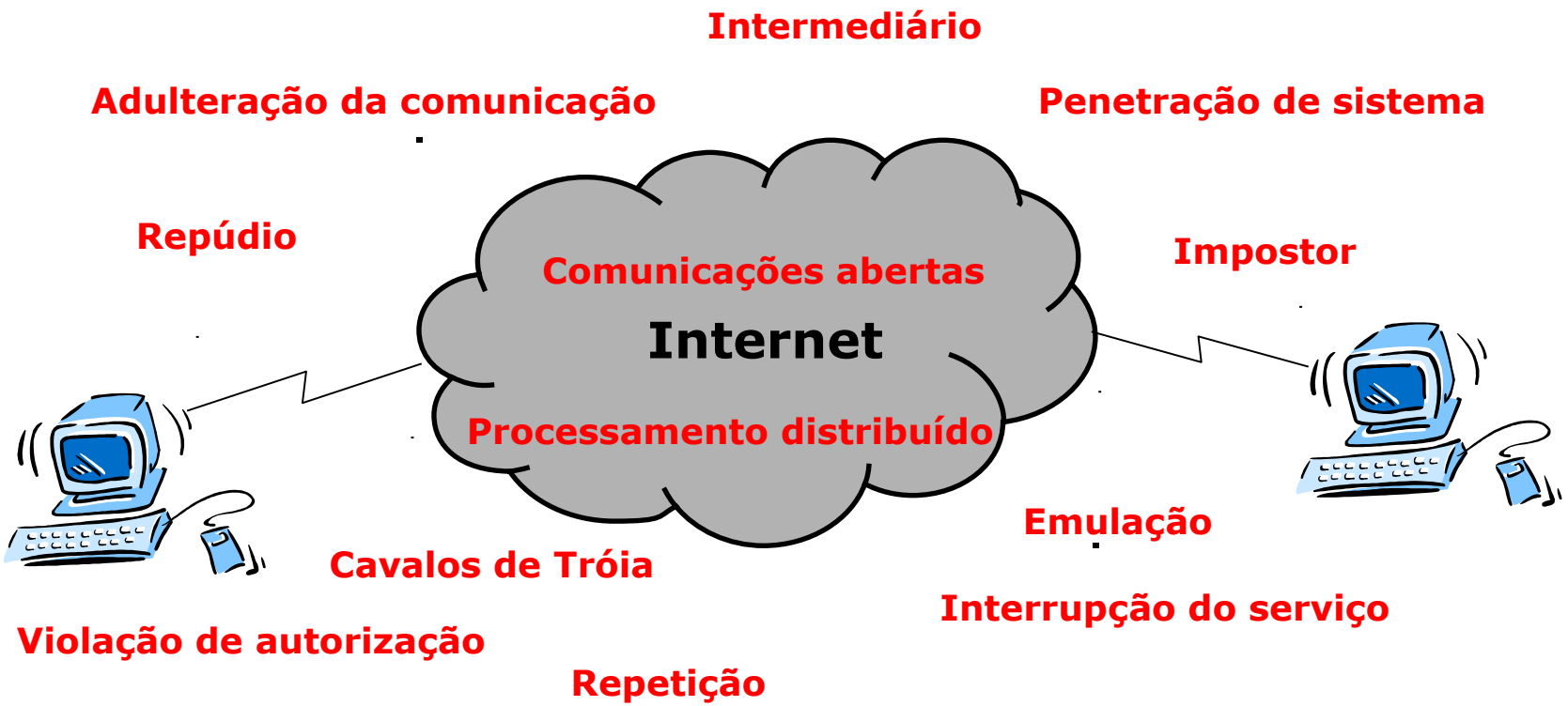
Qual a melhor técnica?

Como garantir a autenticidade de quem envia a mensagem?

Como garantir a integridade do conteúdo?

**Certificado Digital**

# Ameaças do Ambiente Eletrônico



# Comunicação Segura