

5. Criptografia

- Criptografia tem origem do grego *kryptos* (oculto) e *graphein* (escrita).
- A criptografia é o estudo de técnicas para a comunicação e armazenamento seguro de dados.
- Basicamente, existem dois tipos de chaves que são usadas nesse processo de criptografia: **simétricas** e **assimétricas**.

5. Criptografia - *tipos*

- ***Criptografia simétrica***

- Utiliza uma ***única chave*** para encriptar e decriptar a mensagem.

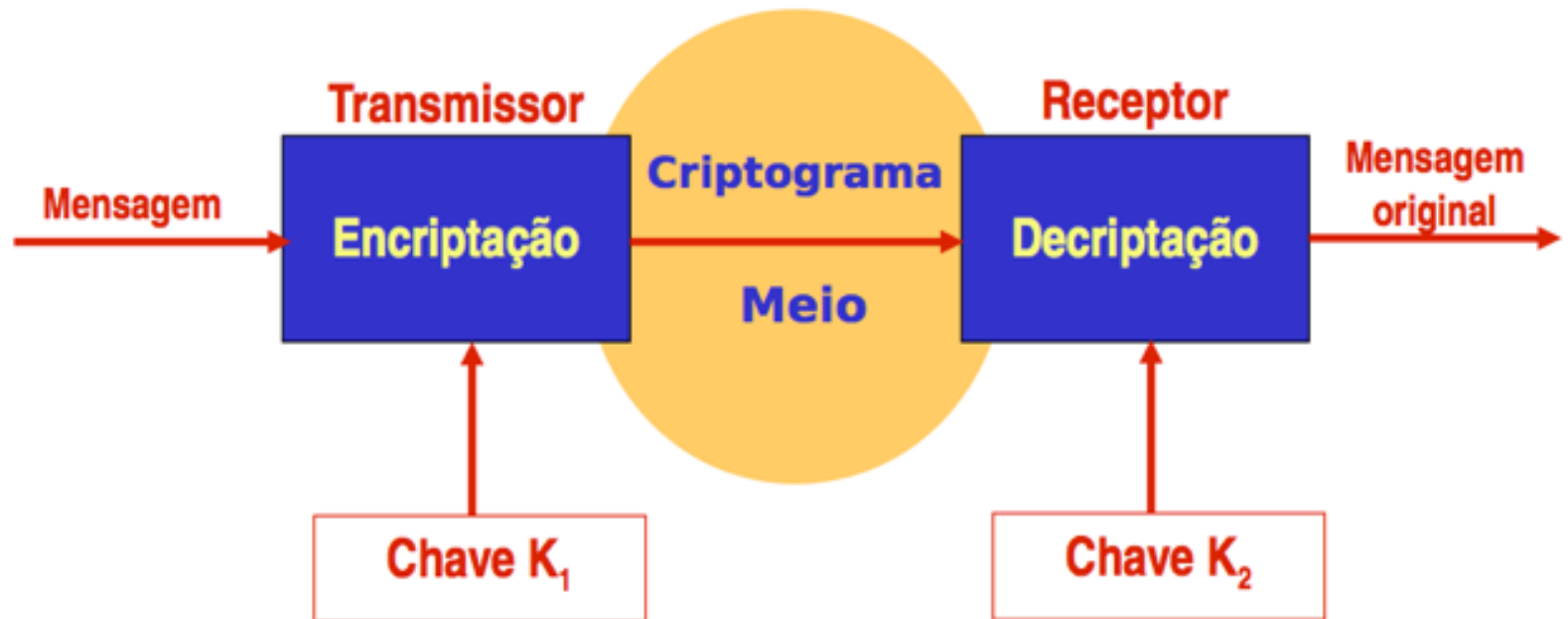
- ***Criptografia Assimétrica***

- Cada entidade possui uma chave pública e uma chave privada.
- Uma chave é privada e apenas o proprietário tem acesso, a outra é pública e é compartilhada com qualquer um que queira encriptar a mensagem.

5. Criptografia – *chave simétrica*

- é o tipo de chave mais simples e a **mesma** utilizada tanto pelo emissor quanto por quem recebe a informação;
- a mesma chave é usada para codificação e decodificação dos dados;
- vários algoritmos de criptografia foram desenvolvidos a partir de chaves simétricas. Dentre os mais comuns estão o **DES**, o **IDEA** e o **RC**.

5. Criptografia - *modelo*



Em Algoritmos Simétricos $K_1 = K_2$ (K)

5. Criptografia – *chave simétrica*

DES (Data Encryption Standard)

- Criado pela IBM, em 1977, o DES usa chaves de 56 bits, permitindo até 72 quatrilhões de combinações.



IDEA (International Data Encryption Algorithm)

- é um algoritmo que usa chaves de 128 bits e tem estrutura semelhante ao DES.

5. Criptografia – *chave simétrica*

RC (Ron's Code ou Rivest Cipher)

- ***é muito usado em e-mails*** e usa chaves de 8 a 1024 bits. Há várias versões: RC2, RC4, RC5 e RC6. Cada uma delas difere da outra por trabalhar com chaves de maior complexidade.

5. Criptografia – *chave simétrica*

AES (Advanced Encryption Standard)

- considerado um dos algoritmos mais seguros da atualidade;
- baseado em 128 bits, mas suas chaves também podem ser aplicadas em 192 e 256 bits. Por isso, é extremamente difícil quebrar sua criptografia em ataques convencionais.

ps.: o governo dos Estados Unidos e várias organizações de segurança utilizam esse modelo

5. Criptografia – *chave simétrica*

Blowfish

- criado como um substituto ao DES;
- separa as informações em blocos de 64 bits e criptografa cada um deles de maneira individual;
- é mais ***comum em plataformas online de compra e venda de produtos***;
- tem como destaque a rapidez na encriptação de informações;
- é considerado por especialistas um dos poucos modelos que não pode ter o código quebrado.


5. Criptografia – *chave simétrica*

Twofish

- variante do Blowfish;
- mesmos princípios;
- o grande diferencial é que ele é formado por blocos de 128 bits e chaves de até 256 bits;
- há ainda uma terceira variação chamada Threefish, que usa blocos de 256, 512 e 1024 bits, com chaves no mesmo formato.

5. Criptografia – *chave simétrica*

SAFER

- baseado na criptografia de blocos de 64 bits;
 - ganhou versões mais atualizadas, mas que ainda não chegam a ser tão seguras quanto outras formas de criptografia.
- 

5. Criptografia – *chave simétrica*

IDEA

- essa forma de criptografia opera em blocos de 64 bits e usa chaves de 128 bits;
- principal característica é confundir os atacantes ao misturar as informações codificadas, impedindo que elas sejam realinhadas da maneira correta.

5. Criptografia – *chave assimétrica*

- também conhecida como “**chave pública**”, a chave assimétrica trabalha com dois modelos principais: um privado e outro público;
- no método privado, como o próprio nome sugere, a chave é secreta;
- no modelo público uma pessoa deve criar uma chave de codificação e enviá-la a quem for lhe mandar informações;
- entre os algoritmos que mais utilizam chaves assimétricas estão o ***RSA*** e o ***ElGamal***.


5. Criptografia – *chave assimétrica*

RSA (Rivest, Shamir and Adleman)

- é um dos algoritmos de chave assimétrica mais usados;
- nele, números primos são utilizados da seguinte forma: dois números primos são multiplicados para se obter um terceiro valor; a chave privada são os números multiplicados e a chave pública é o valor obtido.

5. Criptografia – *chave assimétrica*

ElGamal

- esse algoritmo usa um problema matemático conhecido por “logaritmo discreto” para se tornar seguro;
 - seu uso é mais frequente em assinaturas digitais.
- 

5. Criptografia – *redes sem fio*

- WEP
- WPA/WPA2.



REFERÊNCIAS

