**CRIPTOGRAFIA**

**HISTÓRIA**

- Surgiu da necessidade de enviar mensagens com segurança

- como por exemplo o envio de mensagens entre aliados de guerra.

- Ao longo da história, a necessidade de manter informações em segredo possibilitou a criação de diferentes métodos de criptografia

- Cifra de César, é considerado um dos métodos mais antigos que se conhece.

¬ uma das mais simples e conhecidas técnicas de criptografia

¬ cifra de substituição, no qual cada letra do alfabeto é substituida por outra que se apresenta abaixo dela um número fixo de vezes

¬ Homenagem à Júlio César que o usou para se comunicar com os seus generais

¬ é frequentemente incorporado como parte de esquemas mais complexos

¬ assim como as cifras de substituição monoalfabéticas, a cifra de César é facilmente decifrada e na prática não oferece nenhuma segurança de comunicação

- Cifra de Vigenère

- Cifra de Hill

- Decodificar x Decifrar

decodificar, o receptor já conhece o código e aplica o algoritmo para retirar o código da mensagem recebida

decifrar, é necessário descobrir qual o algoritmo que foi utilizado na codificações para retirar a cifra da mensagem.

- Para codificar as informações, são utilizadas diversas técnicas. As mais conhecidas envolvem o conceito de chaves, conhecidas como chaves criptográficas

- O uso de chaves facilita, pois não é necessário criar um método criptográfico para cada receptor, e sim deixar apenas um método com diversas chaves, uma para cada receptor

- Há dois tipos de chaves criptográficas: chaves simétricas e assimétricas.

\* Chave simétrica – tipo de chave mais simples, em que o emissor e o receptor usam a mesma chave, ou seja, uma única chave é usada na codificação e decodificação da informação.

-> DES (Data Encryption Standard)

-> IDEA (International Data Encryption Algorithm)

-> RC (Ron’s Code ou Rivest Cipher)

-> Outros: AES (Advanced Encryption Standard) baseado no DES, 3DES, Twofish…

-> Sua utilização não é adequada em situações em que a informação é muito valiosa. É necessário usar uma grande quantidade de chaves, caso muitas pessoas estejam envolvidas. Além disso, tanto o emissor quanto o receptor precisam conhecer a mesma chave, a transmissão desta pode não ser tão segura.

\* Chave assimétrica

-> também conhecida como chave pública, ela trabalha com duas chaves: uma denominada pública e outra privada

->RSA (Rivest, Shamir and Adleman)

->Diffle-Hellman

-> EIGamal

->DSA (Digital Signature Algorithm)

->Schnorr

**RSA**

* Algoritmo de encriptação de dados
* Chave assimétrica
* Talvez um dos mais seguros algoritmos atuais de encriptação

Bibliografia:

- http://cimm.ucr.ac.cr/ocs/index.php/xiii\_ciaem/xiii\_ciaem/paper/viewFile/1817/630

- <http://www.infowester.com/criptografia.php>

- <http://pt.scribd.com/doc/35442992/Criptografia-Classica-e-Moderna>