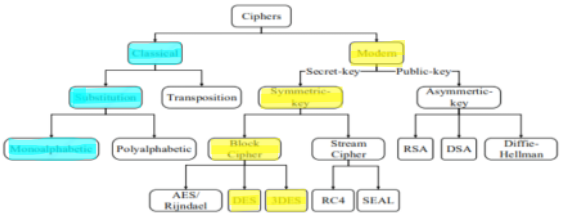
Introdução à Criptografia (Criptoanálise)

segunda-feira, 17 de agosto de 2020 21:47

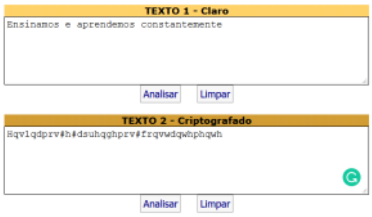
Classificação das Técnicas de Criptografia



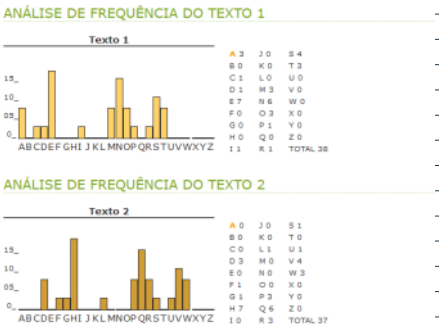
Fonte: SINGH, 2013, p.34..

Criptografia: "**São técnicas de descaracterização da informação através de algoritmos matemáticos**" *by Fábio Cabrini*

Cifra de César: Simétrica e de Substituição Monoalfabética



Quebra da Cifra de César por análise de frequência pode ter sido realizada por trabalhos de Alquindi no século IX.



http://numaboa.com.br/criptografia/criptoanalise/309-Ferramenta-de-frequencia

1983

- Alfabeto Samaritano
- ASCII tem 255 caracteres

Material de Apoio: CRIPTOGRAFIA: DES, AES, RSA e Blowfish - Qual a Diferença?

Criptografia Cifra de César

Deslocamento (**substituição**) mono alfabética

Relacionamento 1:1 exemplo: A (+3) = D

BANANA - (+3)

EDQDQD

Ensinamos e aprendemos constantemente

Hqvlqdprv#h#dsuhqghprv#frqvwdqwhphqwh

Apresenta a distribuição de frequência da língua portuguesa...

a, e, i, o, u

e -> h = 3

OTP (One Time Pad)

https://www.khanacademy.org/computing/computer-science/cryptography/crypt/v/caesar-cipher

https://jrinconada.medium.com/cracking-caesar-cipher-8fe79226aabd

https://www.khanacademy.org/computing/computer-science/cryptography/crypt/v/one-time-pad

Pílula - Q18

terça-feira, 18 de abril de 2023 09:39

QUESTÃO 18

O algoritmo de criptografia *Data Encryption Standard* (DES) cifra blocos de 64 bits utilizando chaves simétricas de 56 bits. Atualmente o DES não é mais considerado uma cifra segura devido ao pequeno número de bits utilizado para a chave. Para resolver o tamanho da chave, foi proposto o DES Triplo (3DES), que utiliza três execuções do DES e chaves de até 168 bits. A chave k para o 3DES é dividida em três partes (k_a, k_b, k_c) e cada uma destas partes é utilizada na execução de uma instância do DES.

STALLINGS, W. **Criptografia e Segurança de Redes**: Princípios e práticas. 4ª ed. São Paulo: Pearson Prentice Hall, 2008 (adaptado).

O algoritmo DES define uma função $C(m, k_1)$ que cifra uma mensagem m com uma chave k_1 e uma função (Dc, k_1) que decifra uma mensagem C cifrada com a chave k_1. Para que o 3DES seja capaz de decifrar mensagens cifradas com o DES, sua implementação deve ser

A) $D(C(D(m, k_a), k_b), k_c)$, sendo $k_a \neq k_b \neq k_c$ partes da chave usada no 3DES e k_a a chave usada no DES.

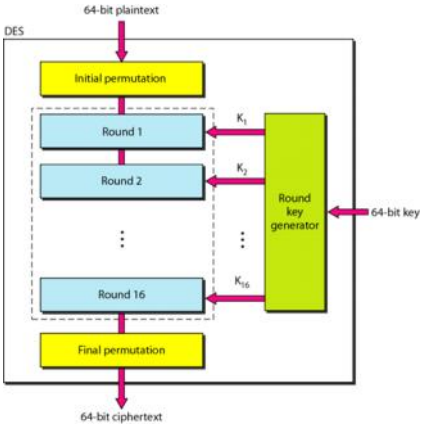
B) $D(D(D(m, k_a), k_b), k_c)$, sendo $k_a \neq k_b \neq k_c$, partes da chave do 3DES e k_a a chave usada no DES.

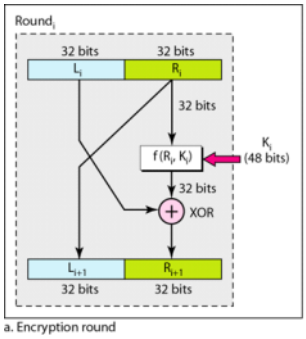
C) $D(D(D(m, k_a), k_b), k_c)$, sendo $k_a = k_b = k_c$, partes da chave do 3DES e k_a a chave usada no DES.

D) $D(C(D(m, k_a), k_b), k_c)$, sendo $k_a = k_b = k_c$ partes da chave usada no 3DES e k_a a chave usada no DES.

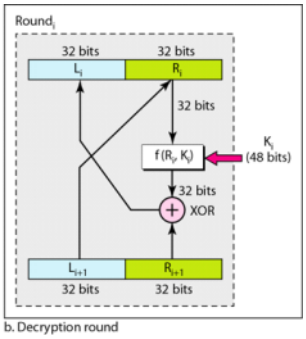
E) $D(D(C(m, k_a), k_b), k_c)$, sendo $k_a = k_b = k_c$ partes da chave usada no 3DES e k_a a chave usada no DES.

Legenda:
D Decriptografia
C Criptografia
M (Mensagem e/ou Bloco)
K_x Chave de Criptografia



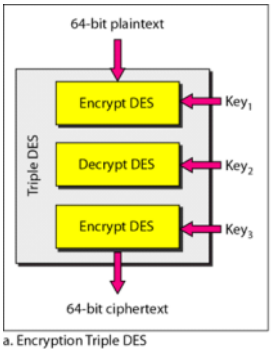


a. Encryption round

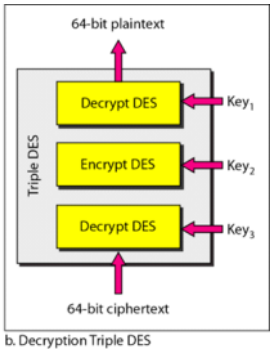


b. Decryption round

3DES



a. Encryption Triple DES



b. Decryption Triple DES

- ✓ No DES a chave utilizada na criptografia é a mesma utilizada na decriptografia.
- ✓ No 3DES é fortemente recomendado o uso de 3 (chaves distintas).