Cifra Fieira

Definição (Chave Fieira)

Seja $\mathcal{K}$ o espaço das chaves de uma função de encriptação. uma sequência de símbolos $e_1e_2e_3\ldots e_i \in \mathcal{K}$, é designada por chave fieira.

Definição (Geradores de Chaves Fieira)

A chave fieira pode ser gerada: aleatoriamente; a partir de um valor inicial (semente); a partir de um valor inicial e do texto a cifrar. A este tipo de algoritmo designa-se por gerador de chaves fieira.

Cifra Fieira

Definição (Cifra Fieira)

Seja $\mathcal{A}$ um alfabeto de q símbolos e seja E_e uma cifra de substituição simples com um bloco de comprimento 1, e aonde $e \in \mathcal{K}$. Seja $m_1m_2m_3\ldots$ um texto claro e seja $e_1e_2e_3\ldots$ uma chave fieira de $\mathcal{K}$.

Uma cifra fieira transforma um texto claro e produz um texto cifrado $c_1c_2c_3\ldots$ aonde $c_i = E_{e_i}(m_i)$.

Se d_i denota o inverso de e_i, então $D_{d_i}(c_i) = m_i$ decifra o texto previamente cifrado.

As cifras de fieira aplicam funções de transformação muito simples de acordo com a chave fieira em uso.

Cifra de Vernam

Definição (Cifra de Vernam)

A cifra de Vernam *é uma cifra fieira definida no alfabeto $\mathcal{A} = \{0, 1\}$. Uma mensagem binária $m_1m_2\ldots m_t$ é transformada através de uma chave fieira $k_1k_2\ldots k_t$ de igual comprimento de forma a produzir a sequência cifrada $c_1c_2\ldots c_t$ onde:*

$$c_i = m_i \oplus k_i, \quad 1 \leq i \leq t.$$

Se a chave fieira é gerada aleatoriamente e não é nunca re-usada, a cifra de Vernam é designada por cifra de uso único *("one-time system" ou "one-time pad").*

- Se a chave é re-usada é possível criptoanalisar o sistema.
- Se a chave não é re-usada, pode-se demonstrar (matematicamente) que o sistema não é quebrável.

Há registos de que, até há pouco tempo, o sistema de comunicação entre Moscovo e Washington era feito através de um sistema deste tipo. O transporte da chave era feito através de meios (físicos) seguros.

Byteisses

Para a implementação da cifra FEAL é necessário recorrer a um conjunto de manipulações em "bytes".

- rotações de Nbits - `ROTN`.
- "Mascarar" um dado conjunto de "bits".
- Separar uma sequência de "bits" em partes.
- Juntar várias partes numa só sequência de "bits".
- Ou exclusivo (XOR) entre "bytes".