

Cifra Fieira

Uma cifra fieira podem ser caracterizadas como sendo uma cifra por bloco em que o comprimento do bloco é 1 e em que função de transformação pode mudar a cada bloco.

- é possível mudar a função de transformação a cada símbolo.
- não sofrem do efeito de propagação de erros.

As cifras por fieiras podem também ser importantes sempre que o dispositivo de transmissão não tenha a capacidade de armazenamento necessária para processar um bloco de informação.

65 / 246

Cifra Fieira

Definição (Chave Fieira)

Seja \mathcal{K} o espaço das chaves de uma função de encriptação. Uma sequência de símbolos $e_1 e_2 e_3 \dots e_i \in \mathcal{K}$, 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.

66 / 246

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 $e \in \mathcal{K}$. Seja $m_1 m_2 m_3 \dots$ um texto claro e seja $e_1 e_2 e_3 \dots$ uma chave fieira de \mathcal{K} .

Uma cifra fieira transforma um texto em claro e produz um texto cifrado $c_1 c_2 c_3 \dots$ 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.

67 / 246

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 $m_1 m_2 \dots m_t$ é transformada através de uma chave fieira $k_1 k_2 \dots k_t$ de igual comprimento de forma a produzir a sequência cifrada $c_1 c_2 \dots c_t$ 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 singular no tempo** ("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 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.

68 / 246