Cifra Deslocamento Simples

A cifra de Júlio César (100ac-44ac) é um cifra simples cuja chave secreta é definida pelo deslocamento que se estabelece nas letras do alfabeto (ao que se sabe esse deslocamento era de três posições).

$$e = \begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s \\ d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v \\ t & u & v & w & x & y & z & & & & & & & & & & & & \\ w & x & y & z & a & b & c & & & & & & & & & & & & \end{pmatrix}$$

Mais genericamente temos

Definição (Cifra Deslocamento)

Seja $\mathcal{M} = \mathcal{C} = \mathbb{Z}_{26}^*$, $\mathcal{K} = \mathbb{Z}$. Para $0 \leq K \leq 25$, define-se:

$$e_K(x) = (x + K) \mod 26$$

e

$$d_K(y) = (y - K) \mod 26$$

para todo o $x, y \in \mathbb{Z}_{26}$

Exercício Prático 1

Implemente a Cifra de Deslocamento Simples.

$$E_K(x) = (x + K) \mod |\mathcal{A}|$$

- Alfabeto Português incompleto $\mathcal{A} = \{\text{a-z}\}$.
- Cifração carácter a carácter.
- Interface Entrada/Saída: ficheiros e linha de comando.
- Implementação (cifrar/decifrar) em C (ou C++).

Cifra de Deslocamento Linear

Definição (Cifra de Deslocamento Linear)

Seja $\mathcal{M} = \mathcal{C} = \mathbb{Z}_{26}^*$, e seja:

$$\mathcal{K} = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \ : \ \mathrm{mdc}(a, 26) = 1\}.$$

Para $K = (a, b) \in \mathcal{K}$, define-se:

$$e_k(x) = (ax + b) \mod 26$$

e

$$d_k(y) = a^{-1}(y - b) \mod 26$$

para todo o $x, y \in \mathbb{Z}_{26}$

Cifras de Substituição

As cifras anteriores são casos particulares de *cifras de substituição*. Cifras de substituição substituem símbolos (ou grupos de símbolos) por outros símbolos (ou grupos de símbolos).

Definição (Cifra de Substituição Simples)

Seja $\mathcal{A}$ um alfabeto com q símbolos e $\mathcal{M}$ o conjunto das sequências de caracteres de $\mathcal{A}$ de comprimento t. Seja $\mathcal{K}$ o conjunto de todas as permutações num conjunto $\mathcal{A}$. Define-se para cada $e \in \mathcal{K}$ uma função de encriptação como sendo:

$$E_e(m) = (E_e(m_1)E_e(m_2)\ldots E_e(m_t)) = (c_1c_2\ldots c_t) = c$$

onde $m = (m_1m_2\ldots m_t) \in \mathcal{M}$. Isto é para cada símbolo num t-tuplo, substitui-se esse símbolo por um outro símbolo de $\mathcal{A}$ de acordo com uma dada permutação e. Para decifrar $c = (c_1c_2\ldots c_t)$ calcula-se a permutação inversa $d = e^{-1}$, tendo-se então a função de desencriptação:

$$D_d(c) = (D_d(c_1)D_d(c_2)\ldots D_d(c_t)) = (m_1m_2\ldots m_t) = m$$

E_e é designada uma cifra de substituição simples, ou cifra de substituição mono-alfabética

Cifra de Substituição Poli-alfabética

Definição (Cifra de Substituição Poli-alfabética)

Uma cifra de substituição poli-alfabética com comprimento de bloco t dado o alfabeto $\mathcal{A}$ é uma cifra que possuí as seguintes propriedades:

1. *o espaço das chaves $\mathcal{K}$ consiste em todos os conjuntos ordenados de t permutações $(p_1, p_2, \ldots, p_t)$ aonde cada uma das permutações p_i é definida no conjunto $\mathcal{A}$;*
2. *a encriptação da mensagem $m = (m_1 m_2 \ldots m_t)$ com a chave $e = (p_1, p_2, \ldots, p_t)$ é dada por $E_e(m) = (E_{p_1}(m_1) E_{p_2}(m_2) \ldots E_{p_t}(m_t))$;*
3. *a chave de decifração associada com $e = (p_1, p_2, \ldots, p_t)$ é $d = (p_1^{-1}, p_2^{-1}, \ldots, p_t^{-1})$.*

Cifra de Vigenère

Cifra de Vigenère

Seja $\mathcal{A} = \{a, b, c, \ldots, x, z\}$ e $t = 3$. A chave é "dhk" que corresponde a $e = (p_1, p_2, p_3)$ sendo que para cada uma das componentes da chave se aplica uma encriptação por deslocamento simples, isto é, p_1 transforma as letras em $\mathcal{A}$ numa outra letra de $\mathcal{A}$ três posições à sua direita, p_2 numa sete posições à sua direita, e p_3 dez posições à sua direita. Se a mensagem a cifrar for a seguinte:

$$m = \text{est aci fra nao ese gur axx}$$

então

$$c = E_e(m) = \text{hbf djt ial qha hbp jdd dfi}$$

Blaise de Vigenère (Saint-Pourçain, 1523–1596) foi um diplomata e criptógrafo francês.

Criptoanálise

Definição (Criptoanálise)

Criptoanálise *é o estudo dos procedimentos necessários para tentar comprometer as técnicas criptográficas, e mais genericamente, os serviços de segurança da informação.*

- Stinson, Douglas, *Cryptography: Theory and Practice*, CRC, 2006.
- Pedro Quaresma, Augusto Pinho, Análise de Frequências da Língua Portuguesa, Livro de Actas InterTIC 2007, 3 a 5 de Dezembro de 2007, Porto, Portugal, pags 267-272, IASK, 2007.

Criptoanálise - Objectivos do Adversário

Cifra (parcialmente) Quebrada O objectivo principal de um adversário que queira atacar uma cifra é o de recuperar, de forma sistemática, texto claro a partir de texto cifrado. Se este objectivo for atingido diz-se, que a cifra foi parcialmente quebrada.

Cifra (formalmente) Quebrada Um objectivo mais ambicioso é o de obter a chave privada de uma dada entidade, nesse caso a cifra é completamente, e formalmente, quebrada.