Cifras simétricas monoalfabéticas

Playfair e Cifra de Hill

Playfair

- A cifra de encriptação de múltiplas letras mais conhecida é a **Playfair**, que trata os digramas no texto claro como unidades isoladas e as traduz para digramas de texto cifrado;
- O algoritmo **Playfair** é baseado no uso de uma matriz 5 × 5 de letras construídas usando uma palavra-chave;
- Nesse caso, a palavra-chave é *monarchy*. A matriz é construída com o preenchimento das letras da palavra-chave (menos duplicatas) da esquerda para a direita e de cima para baixo, e depois do restante da matriz com as outras letras na ordem alfabética. As letras I e J contam como uma só;

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

Regras do **playfair**

1. Letras de texto claro repetidas que estão no mesmo par são separadas por uma de preenchimento, como **x**, de modo que *balloon* seria tratado como *ba lx lo on*;

2. Duas letras de texto claro que estejam na mesma linha da matriz são substituídas pela letra à direita, com o primeiro elemento da linha vindo após o último, de forma rotativa. Por exemplo, **ar** é encriptado como **RM**;

3. Duas letras de texto claro que estejam na mesma coluna são substituídas pela letra abaixo, com o elemento de cima da coluna vindo após o último, de forma rotativa. Por exemplo, **mu** e encriptado como **CM**.

4. Caso contrário, cada letra de texto claro em um par é substituída por aquela que esteja em sua própria linha e na coluna ocupada pela outra letra de texto claro. Assim, **hs** torna-se **BP**, e **ea** torna-se **IM** (ou **JM**, a critério do cifrador).

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

Playfair: outras características

- A cifra Playfair representa um grande avanço em relação as cifras monoalfabéticas simples;
- Primeiramente, enquanto existem apenas 26 letras, existem 26 × 26 = 676 digramas, de modo que a identificação de digramas individuais é mais difícil;
- Além do mais, as frequências relativas das letras individuais exibem um intervalo muito maior do que o dos digramas, tornando a análise de frequência muito mais difícil;
- Por esses motivos, a cifra Playfair foi, por muito tempo, considerada indecifrável;

Playfair: outras características

- Ela foi usada como sistema de campo padrão pelo Exército britânico na Primeira Guerra Mundial, e ainda gozava de um uso considerável pelo Exército dos Estados Unidos e outras forças aliadas durante a Segunda Guerra Mundial;
- Apesar desse nível de confiança em sua segurança, a cifra Playfair é relativamente fácil de ser quebrada, pois ainda deixa intacta grande parte da estrutura da linguagem de texto claro: algumas centenas de letras de texto cifrado geralmente são suficientes para quebrá-la.

Cifra de Hill

- Desenvolvida pelo matemático Lester Hill em 1929;
- Esse algoritmo de encriptação utiliza *m* letras de texto claro sucessivas e as substitui por *m* letras de texto cifrado;
- A substituição é determinada por *m* equações lineares, em que cada caractere recebe um valor numérico (a = 0, b = 1, ..., z = 25);
- Para *m* = 3, o sistema pode ser descrito da seguinte forma:

$$(c_1\ c_2\ c_3) = (p_1\ p_2\ p_3)\begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \bmod 26$$

- Isso pode ser expresso em termos de vetores de linhas e matrizes:

$$c_1 = (k_{11}p_1 + k_{21}p_2 + k_{31}p_3) \bmod 26$$
$$c_2 = (k_{12}p_1 + k_{22}p_2 + k_{32}p_3) \bmod 26$$
$$c_3 = (k_{13}p_1 + k_{23}p_2 + k_{33}p_3) \bmod 26$$

Cifra de Hill

- Também pode ser escrito como **C = PK** mod 26, onde **C** e **P** são vetores de coluna de tamanho 3, representando o texto claro e o texto cifrado, e **K** e uma matriz 3 × 3, indicando a chave de encriptação – as operações são realizadas com mod 26;
- Exemplo: para o texto "*paymoremoney*" e chave de encriptação **K** (ao lado);
- As três primeiras letras do texto claro são representadas pelo vetor (15 0 24);
- Então, (15 0 24)**K** = (303 303 531) mod 26 = (17 17 11) = RRL;
- Continuando dessa forma, o texto cifrado para o texto claro inteiro é RRLMWBKASPDH.

$$\mathbf{K} = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

Cifra de Hill

- A decriptação exige o uso do inverso da matriz **K**. Podemos calcular det **K** = 23 e, portanto, $(\det \mathbf{K})^{-1} \bmod 26 = 17$. Nesse caso, o inverso é:

$$\mathbf{K}^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$$

- Ou seja:

$$\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} = \begin{pmatrix} 443 & 442 & 442 \\ 858 & 495 & 780 \\ 494 & 52 & 365 \end{pmatrix} \bmod 26 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

- Se a matriz K^{-1} for aplicada ao texto cifrado, então o texto claro é recuperado.