Técnicas de transposição

Denis Henrique dos Santos - 191024724
Mateus Rijo de Oliveira - 191025501
Miguel Cesar Corrêa - 191024686
Vinicius Machado Coutinho - 191025836

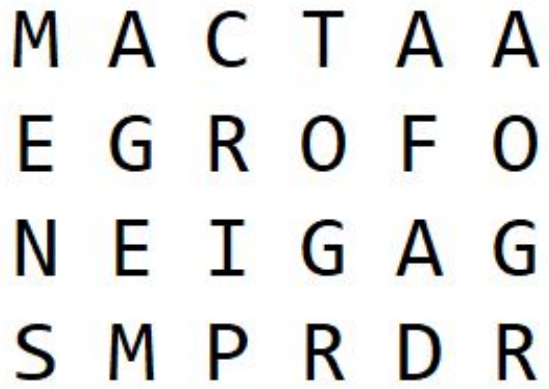
Cifras de transposição

- Técnicas de transposição são métodos de encriptação em que se faz uma permutação no texto plano, mudando a ordem dos caracteres.
- Isso pode ser realizado através da aplicação de uma função bijetora.
- Decifrar o texto criptografado é possível através da função inversa da função usada para cifrar.

Cifra das colunas básica

Trata-se de escrever o texto a ser cifrado por colunas, seguindo para a próxima coluna ao atingir um determinado número de linhas.

Pode-se adicionar caracteres extras no final para confundir quem tentar decifrar o texto ou para obter a mensagem com um número fixo de caracteres.



Cifra de Cítala

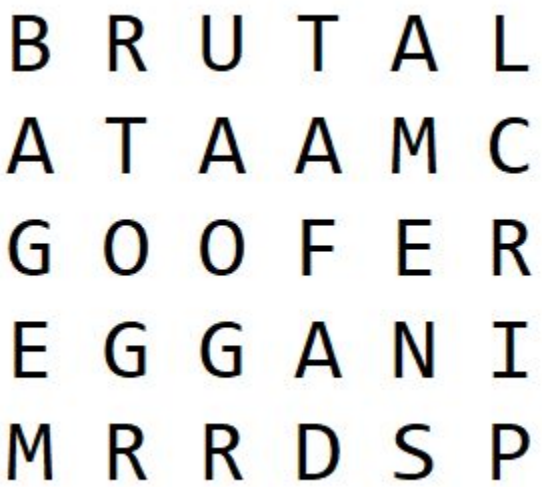
A cítala ou bastão de Licurgo foi um sistema de criptografia utilizado pelos líderes espartanos composto por duas varas de espessura semelhante e tiras de couro ou papiro.

Ela consistia em enrolar a tira em volta das varas e escrever a mensagem a ser cifrada, de modo que a ordem dos caracteres não seja a mesma ao desenrolar a tira.

Transposição de colunas

Consiste na aplicação da cifra das colunas utilizando uma chave determinando a ordem das colunas, podendo ser uma palavra cuja ordem alfabética determina a ordem das colunas.

Por exemplo, caso a chave seja “GATO” a ordem das colunas será 2143.



Transposição de colunas

```
string encryptMessage(string msg, string key) {
    map<int, int> keyMap;
    for (int i = 0; i < key.length(); i++) keyMap[key[i]] = i;
    int col = key.length();
    int row = msg.length() / col;
    if (msg.length() % col) row++;
    string cipher = "";
    for (map<int, int>::iterator itr = keyMap.begin(); itr != keyMap.end(); itr++) {
        for (int i = itr->second; i < msg.length(); i += col) {
            cipher += msg[i];
        }
    }
    return cipher;
}
```

Transposição de colunas

```
string decryptMessage(string msg, string key) {
    map<int, int> keyMap;
    for (int i = 0; i < key.length(); i++) keyMap[key[i]] = i;
    int col = key.length();
    int row = msg.length() / col;
    if (msg.length() % col) row++;
    string plainText = msg;
    int j = 0;
    for (map<int, int>::iterator itr = keyMap.begin(); itr != keyMap.end(); itr++) {
        for (int i = itr->second; i < msg.length(); i += col) {
            plainText[i] = msg[j];
            j++;
        }
    }
    return plainText;
}
```

Transposição de Myszkowski

Proposta por Émile Victor Théodore Myszkowski, a transposição de Myszkowski é uma variante da transposição de colunas.

O texto limpo é escrito em linhas sob uma palavra chave, assim como na transposição de colunas. A principal diferença é que letras repetidas recebem a mesma numeração, coisa que não acontece na transposição de colunas tradicional.

Colunas que possuem o mesmo número são lidas sequencialmente da esquerda para direita, seguindo a ordem crescente de numeração.

Transposição Myszkowski

B	A	T	A	T	A
2	1	3	1	3	1
M	E	N	S	A	G
E	M	C	R	I	P
T	O	G	R	A	F
A	D	A	O	G	R

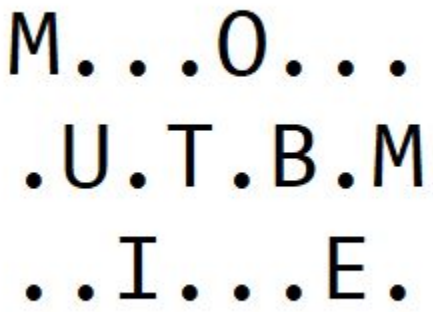
ESG MRP ORF DOR

META NA CI GA AG

Rail Fence

A técnica de Rail Fence consta em escrever a mensagem a ser cifrada diagonalmente para baixo, alternando a escrita para uma diagonal para cima ao atingir um certo número de linhas, formando um padrão em ziguezague, a mensagem então é lida horizontalmente.

Logo o texto plano “MUITOBEM”, com um número de linhas de 3, se torna o texto cifrado “MOUTBMIE”, de acordo com a seguinte grelha:



Rail Fence

```
string encryptRailFence(string text, int key)
{
    char rail[key][(text.length())];
    for (int i=0; i < key; i++)
        for (int j = 0; j < text.length(); j++)
            rail[i][j] = '\n';
    bool dir_down = false;
    int row = 0, col = 0;
    for (int i=0; i < text.length(); i++)
    {
        if (row == 0 || row == key-1)
            dir_down = !dir_down;
        rail[row][col++] = text[i];
        dir_down?row++ : row--;
    }
    string result;
    for (int i=0; i < key; i++)
        for (int j=0; j < text.length(); j++)
            if (rail[i][j]!='\n')
                result.push_back(rail[i][j]);
    return result;
}
```

Rail Fence

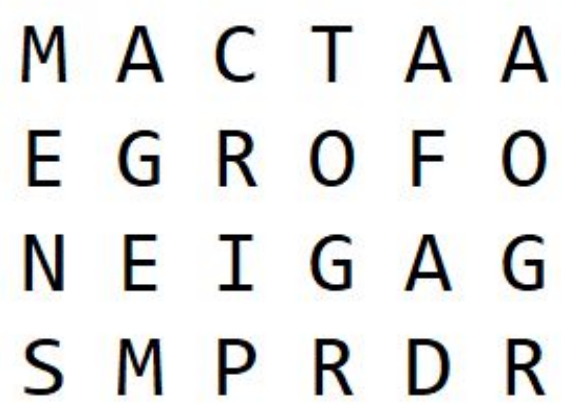
```
string decryptRailFence(string cipher, int key)
{
    char rail[key][cipher.length()];
    for (int i=0; i < key; i++)
        for (int j=0; j < cipher.length(); j++)
            rail[i][j] = '\n';
    bool dir_down;
    int row = 0, col = 0;
    for (int i=0; i < cipher.length(); i++)
    {
        if (row == 0)
            dir_down = true;
        if (row == key-1)
            dir_down = false;
        rail[row][col++] = '*';
        dir_down?row++ : row--;
    }
```

```
    int index = 0;
    for (int i=0; i<key; i++)
        for (int j=0; j<cipher.length(); j++)
            if (rail[i][j] == '*' && index<cipher.length())
                rail[i][j] = cipher[index++];
    string result;
    row = 0, col = 0;
    for (int i=0; i< cipher.length(); i++)
    {
        if (row == 0)
            dir_down = true;
        if (row == key-1)
            dir_down = false;
        if (rail[row][col] != '*')
            result.push_back(rail[row][col++]);
        dir_down?row++: row--;
    }
    return result;
}
```

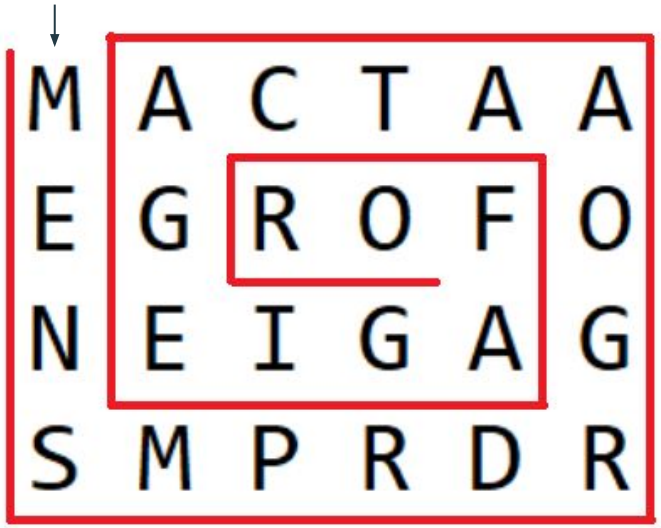
Cifra em Rota

A cifra em rota é um método onde a mensagem é escrita em uma matriz, de dimensões definidas pela chave secreta, e depois, lido em uma rota também definida pela chave.

Uma variação da cifra de rota é a cifra de rota da União, utilizada na guerra civil americana por soldados da União. A diferença para a cifra de rota comum, é que na cifra da União, palavras inteiras eram transpostas.



Cifra em Rota



Seguindo em uma rota em espiral, iniciando no canto superior esquerdo, a mensagem:

MENSAGEM CRIPTOGRAFADA

Se torna:

MENSMP RDRGOA ATCAGE IGAFOR

Sabendo as dimensões da matriz e a rota definida, o receptor pode remontar a mensagem criptografada no *grid* e ler a mensagem original.

Cifra em Rota

- A cifra de rota é mais segura que a cifra *rail fence*, pois, além do tamanho do grid ser definido pela chave, a rota também é. Como existem muitos caminhos que podem ser seguidos, existem muitas chaves secretas disponíveis.
- Por outro lado, nem todas as rotas garantem uma boa proteção. Alguns caminhos podem deixar fragmentos do texto original ou seções invertidas, facilitando a criptoanálise.

Detecção e Criptoanálise

- Como a criptografia de transposição não altera a frequência de símbolos individuais, transposições simples podem ser detectadas facilmente por criptoanalistas com uma contagem de frequência.

- O criptoanalista pode usar anagramas, movendo seções do texto procurando palavras na língua da mensagem. Depois de encontrar esses anagramas, pode-se inferir informações do padrão de transposição, facilitando a quebra do código.