Cifra de Vigenère

Rafael Campos Nunes
19/0098295

Contents

1 A Cifra de Vigenère

A cifra de Vigenère é caracterizada como uma cifra de fluxo simétrica pois atua em cada caractere (*byte*) que passa pelo algoritmo, transformando texto em criptograma que, por fim, é retornado. Ele é considerado simétrico pois utiliza a mesma chave para as etapas de cifragem e decifragem.

Uma característica importante da cifra é que ela é polialfabética, o que reduz ataques relacionados à frequência de caracteres do criptograma e, embora isso seja possível, a análise do criptograma através da frequência de palavras é um pouco mais complicada pois envolve mecanismos que não são conhecidos *a priori*, tal como o tamanho da chave utilizada para cifrar o texto.

1.1 Cifração

A cifra do algoritmo é um processo similar ao utilizado na cifra de Caesar, com a diferença de utilizar um polialfabeto para transformar o texto puro em criptograma.

O processo de cifragem de uma mensagem M com uma chave K de tamanho n é denotado pela equação abaixo para um alfabeto definido na tabela ASCII.

$$C_i = M_i + K_i \mod len(K) \tag{1}$$

A soma definida na equação 2 é uma soma aritmética da posição da letra M_i na tabela ASCII com a letra pertencente a chave $K_i \mod len(K)$ também na tabela ASCII. O resultado é um criptograma C com tamanho idêntico à mensagem M.

1.2 Decifração

O processo de decifragem é análogo ao de cifragem, com a diferença na operação que, ao invés de somar é realizado a operação de subtração sobre a mensagem, como denota a equação abaixo

$$M_i = C_i - K_i \mod len(K) \tag{2}$$

2 Utilização da ferramenta

A ferramenta pode ser utilizada de acordo com as opções definidas em –help.

```
$ ./vigenere.exe --help
```

3 Limitações da ferramenta

Apesar do programa ter a função de realizar a criptoanálise sobre um texto, é importante ressaltar que essa configuração só funcionará para chaves de até 100 caracteres. Esse número não é por acaso, foi limitado dessa maneira para facilitar a análise de grandes corpos de texto em que se supõe que o número de coincidências do criptograma com ele mesmo em diferentes posições não terá uma distância maior do que 100 caracteres.