

# **Criptoanálise – Vigenere (Teste de Kasiski)**

David Cainã Araújo Vieira<sup>1</sup>

<sup>1</sup>Escola Politécnica – Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS)  
– Porto Alegre – RS – Brasil

David.vieira@edu.pucrs.br

## **RESUMO**

O artigo descreve em linhas gerais o funcionamento da Cifra de Vigenère e os passos necessários para descriptografar um texto cifrado com esse método sem conhecimento prévio de nenhuma informação, salvo o idioma na qual o texto original foi cifrado.

## **ABSTRACT**

The article describes the operation of the Vigenère Cipher and the steps required to decrypt a ciphertext with this method without a prior knowledge of any information except the language in which the original text was ciphered.

## **1 Informações Gerais**

A cifra de Vigenère é um modelo de cifra clássica descrito em 1553 por Giovan Battista Bellaso em seu livro chamado “La cifra del. Sig. Giovan Battista Bellaso”. Curiosamente, a autoria e inclusive o nome desse método foi de forma equivocada designada a Blaise de Vigenère, criptógrafo francês que criou outro método mais robusto de criptografia, a “autochave” [1].

## **2 Cifra de Vigenère**

É importante esclarecer que este método de criptografia é ineficaz para fins de segurança nos dias atuais, devido ao poder computacional disponível. Todavia, representa mais um de vários feitos importantes na história da humanidade, sendo denominada de “cifra indecifrável”. Porém e já introduzindo o método utilizado para decifração, Friedrich Kasiski publicou um livro em 1863, que introduziu o “Teste de Kasiski”, que tornou a cifra de Vigenère insegura.

### **2.1 Funcionamento**

O funcionamento do método de Vigenère é muito similar a Cifra de Cesar, outro método de criptografia, onde cada letra do alfabeto é deslocada em três posições. A diferença entre os métodos se dá pela quantidade de cifras utilizadas em sequência. Em outras palavras, a cifra de Vigenère utiliza várias cifras de Cesar em sequências, com diferentes deslocamentos, que são determinados por uma chave.

Por exemplo, supondo que se quer criptografar o texto: DEZNOTRABALHO (“dez no trabalho”), e escolhendo a chave, e repetindo-a, até ter o comprimento do texto a cifrar, por exemplo, se a chave for “dez”. Logo, temos:

<b>TEXTO:</b>	DEZNOTRABALHO
<b>CHAVE:</b>	DEZDEZDEZDEZD
<b>TEXTO CIFRADO</b>	GIYQSSUEADPGR

Como pode-se ver na tabela acima, a primeira letra do texto, “D”, é cifrada utilizando “D”, que ocasionalmente, é a primeira letra da chave. O mesmo ocorrerá para todo o texto cifrado, utilizando a posição correspondente da chave para realizar a encriptação. Logicamente, a decifração é feita inversamente.

### 3 Decifrando

Para realizar a decifração, foi utilizado o método de Kasiski, cujo objetivo é deduzir o tamanho da chave e o índice de coincidências para deduzir qual a chave. Resumidamente, foram realizados três passos ao todo, sendo eles: a descoberta do tamanho da chave, descoberta da chave e a decifragem em si.

#### 3.1 Descoberta do Tamanho da Chave

Para descobrir o tamanho da chave, como dito anteriormente, foi utilizado o teste de Kasiski. Kasiski sugeriu que se pudessemos procurar fragmentos repetidos no texto cifrado e analisar a lista das distancias que as separam, é provável que o comprimento da chave divida muitas dessas distancias. Em outras palavras, se uma substring/set's (pedaço do texto cifrado) é criptografado utilizando a mesma chave, o texto cifrado contém uma substring repetida, e existe a probabilidade da distancia entre ambas ser um múltiplo do comprimento da chave [2].

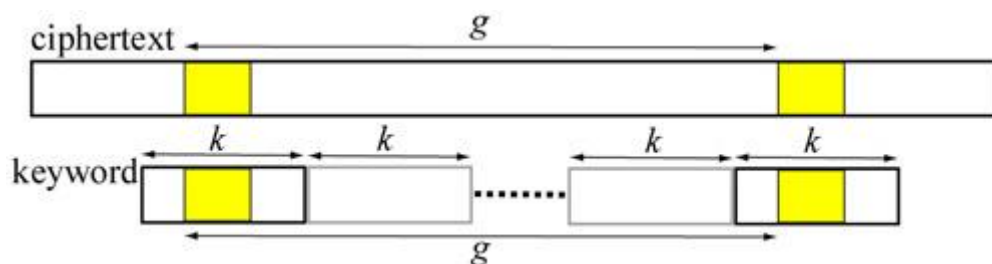


Figura 1: Exemplo teste de Kasiski

Por exemplo, como a figura acima mostra, a distância entre duas substring é mostrada em amarelo, no texto cifrado. Como a palavra chave possui um tamanho fixo, digamos que “K”, é repetida inúmeras vezes para preencher o comprimento do texto cifrado, a distância entre as repetições é um múltiplo do comprimento de “K”. Logo, é provável que G seja o comprimento da palavra chave.

Botando em pratica, obteve-se:

▶ {Integer@623} 1 -> {Integer@624} 8683	▶ {Integer@638} 8 -> {Integer@639} 1077
▶ {Integer@625} 2 -> {Integer@626} 4375	▶ {Integer@640} 9 -> {Integer@641} 861
▶ {Integer@627} 3 -> {Integer@628} 2797	▶ {Integer@642} 10 -> {Integer@643} 801
▶ {Integer@629} 4 -> {Integer@630} 2152	▶ {Integer@644} 11 -> {Integer@645} 870
▶ {Integer@631} 5 -> {Integer@632} 1641	▶ {Integer@646} 12 -> {Integer@647} 636
▶ {Integer@633} 8197 -> {Integer@623} 1	▶ {Integer@648} 8204 -> {Integer@629} 4
▶ {Integer@634} 6 -> {Integer@635} 1335	▶ {Integer@649} 13 -> {Integer@650} 671
▶ {Integer@636} 7 -> {Integer@637} 7080	▶ {Integer@651} 14 -> {Integer@652} 3614

Figura 2: Lista de substrings e suas respectivas ocorrências.

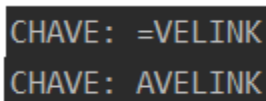
Entre os mais de três mil resultados obtidos, podemos observar as distancias (a esquerda) e o número de ocorrências (a direita), através da amostra acima. Simplificando o processo, pode-se ver que as distancias de “1” e “7” se sobressaem em número de ocorrências,

se comparado as outras. Descartando a hipótese de a chave ser de tamanho um, pelo fato se tratar da cifra de Vigenère, assumiu-se que o tamanho da chave é 7.

### 3.2 Descobrindo a Chave

Para o descobrimento da chave, foi utilizado um método não ideal, visto que não trouxe resultados exatos, mas sim um resultado aproximado ao resultado ideal. Ainda, sendo necessário “analisar” as chaves obtidas, foi possível “otimizar” a solução em questão.

Dando continuidade, o texto cifrado foi novamente dividido, só que dessa vez em partes de tamanho igual a da chave. Como próximo passo, foi calculado a frequência das letras no texto para cada uma das sete partes. Como resultado obtido:



```
CHAVE: =VELINK
CHAVE: AVELINK
```

Figura 3: Resultado para descoberta da chave.

Como pode-se ver, a primeira chave encontrada “foge” do alfabeto, o que possibilitou uma pequena otimização na solução. Limitando o intervalo de conversão e abrangendo somente os 26 caracteres do alfabeto, ficou claro que a chave do trabalho é “Avelino”, apesar de não ter acertado o ultimo caractere.

### 3.3 Descobrindo a Chave

Por fim, conhecendo a chave, para decifrar o texto foi somente necessário efetuar o deslocamento das letras de acordo com a posição no texto e a posição da chave. Como resultado, obteve-se o seguinte texto:

*“QUEMHAGINCOENXAANNOSXIVESSEECORAGEQDEPUBLMCARUMLMVROCOMSO  
DESUMRERMAINISERIAJYLGADOVMSIONARMOOUAPAMXONADOUUENOVIEOUNO  
QUIRIAVROWESPLENHORES DUQREGIMERPOLITIGOQUEPRSMETTIALUMANIDEDE  
UMANSVAERATSDARADIENTE...”*

## 4 Conclusão

O principal ponto que se pode tirar do desenvolvimento do trabalho, foi que: apesar de todo acesso a informação, poder computacional, sabendo-se como as cifras funcionam e como decifra-las, ainda assim não foi possível encontrar a chave “correta”. O que remeteu a reflexam sobre o quão difícil era decifrar tais questões e o quão determinado os criadores e decifradores estavam.

## 5 Referencias

- [1] [https://pt.wikipedia.org/wiki/Cifra\\_de\\_Vigen%C3%A8re%E2%80%8B](https://pt.wikipedia.org/wiki/Cifra_de_Vigen%C3%A8re%E2%80%8B)
- [2] <https://www.dcode.fr/vigenere-cipher>