Cifra de Vigenère

Devido à vulnerabilidade das cifras de substituição simples, foi necessário a criação de uma cifra que conseguisse se proteger disso. A **Cifra de Vigenère** veio com esse propóstio e é basicamente uma extensão da fórmula da Cifra de César. Ela gera uma distribuição praticamente uniforme em uma análise de frequência e foi considerada **inquebrável** por 3 séculos.

> Ela tem esse nome em homenagem a Blaise de Vigenère

Essa Cifra consiste basicamente em pegar uma **palavra-chave** e aplicar a cifra de César várias vezes, de acordo com os caracteres da palavra-chave.

Por exemplo, se nós queremos encriptar a mensagem `the cake is a lie` usando a palavra-chave `portal`, primeiro cada caractere da palavra-chave terá um número de rotações equivalente (de acordo com sua posição no alfabeto):

letra	P	O	R	T	A	L
rotações	16	15	18	20	1	12

Assim, para cada letra da mensagem será rotacionada de acordo com a sequência de rotações acima:

```
mensagem:          T H E  C A K E  I S  A  L I E
chave:             P O R  T A L P  O R  T  A L P
mensagem cifrada:  I V V  V A V T  W J  T  L T T
```

Essa cifra, diferentemente das cifras de substituição simples, é uma **Cifra de Substituição Polialfabética**.

Detectando

Um texto encriptado por essa cifra pode ser detectado através de uma **análise de frequência**.

A Cifra de Vigenère costuma gerar textos com uma distribuição de frequência das letras próximo ao uniforme. Se um texto cifrado que não é esperado esse tipo de distribuição obter esse resultado, provavelmente é Cifra de Vigenère, ou alguma outra Cifra Polialfabética.

Solucinando

Mesmo gerando uma distribuição uniforme em análises de frequência, essa cifra tem uma vulnerabilidade: a palavra-chave é usada várias vezes em um texto grande.

Dessa forma, se a chave tiver tamanho 5, por exemplo, e ajustarmos o texto em linhas de comprimento 5, cada coluna terá a mesma rotação. Assim, podemos chutar tamanhos da palavra-chave e usar a mesma análise de cifra de substituição simples para cada coluna.

Uma ferramenta online muito útill para quebrar a Cifra de Vigenère é o site dcode.

Referências

GeeksforGeeks

Exercícios

OverTheWire: Krypton4

OverTheWire: Krypton5

picoCTF-2018: blaise's cipher

Revision #5
Created Sat, Oct 6, 2018 6:49 PM by Andrew
Updated Mon, Jan 28, 2019 10:14 PM by Andrew