Cifra de Vigenère

A cifra de Vigenère é um método de criptografia que foi inventado no século XVI por Blaise de Vigenère, um criptógrafo francês. Ela é uma cifra de substituição polialfabética, o que a torna mais segura do que as cifras de substituição simples.

Por ser polialfabética, ela usa várias tabelas de substituição em vez de apenas uma. Cada letra da chave é usada para cifrar uma letra correspondente na mensagem, e a chave é repetida ao longo da mensagem conforme necessário.

A segurança da cifra de Vigenère depende fortemente da chave utilizada. A chave é uma sequência de caracteres alfabéticos (geralmente uma palavra ou frase), e cada caractere da chave é usado para cifrar o caractere correspondente da mensagem.

Para cifrar uma mensagem usando a cifra de Vigenère, cada letra da mensagem é combinada com a letra correspondente da chave usando uma operação de soma modular. A operação de soma modular ajuda a manter a cifra segura e a torna resistente à análise estatística. Apesar de ser possível fazer uma ataque a essa cifra usando o método de Kasiski.

Para decifrar a mensagem, o destinatário precisa da chave correta. A chave é usada para reverter o processo de cifragem, subtraindo a letra da chave da letra cifrada usando a mesma operação de soma modular.

A cifra de Vigenère era considerada segura em sua época, mas, eventualmente, foi quebrada com o desenvolvimento de técnicas de criptoanálise mais avançadas. Hoje em dia, é considerada uma cifra relativamente fraca e não é usada para criptografia de alta segurança.

Programa

O programa é bem simples. Possui uma classe “Vig” e 3 métodos. Um método “Vig” que recebe a key, um método “encryption” que recebe o *plaintext* e um método “decryption” que recebe o criptograma.

O programa recebe de entrada um *plaintext* e uma *key* e retorna o texto cifrado. Depois recebe um texto cifrado e a *key* correspondente e decifra o texto.

A entrada pode ter caracteres especiais, mas serão ignorados na saída.

Exemplo de Cifração:

Entrada: Hoje é um belo dia, mas com certeza irá chover.

Key: parental

Saída: WOAIHFBPAOUMNFADRODGRKTPOAZVPAOGTR

Exemplo de Decifração:

Entrada: WOAIHFBPAOUMNFADRODGRKTPOAZVPAOGTR

Key: parental

Saída: HOJEUMBELODIAMASCOMCERTEZAIRCHOVER

Também é preciso ficar atento ao fato que, os textos de entrada não podem possuir quebras de linha pois isso vai gerar inconsistências na execução.

Ataque a Cifra de Vigenère

O ataque a cifra foi feito usando analise de frequência. No primeiro desafio, eu fiz uma suposição que o criptograma estaria em inglês pois existia um apóstrofo em meio ao texto. A análise de frequência das letras mostrou que as letras “e”, “i” e “t” eram as que mais repetiam respectivamente. Com o quadro de Frequências relativas das letras na língua inglesa pode-se deduzir que essas letras sejam respectivamente “e”, “t” e “a”.

Também fiz uma análise por grupo de letras, que resultou em “ty” e “ie” aparecendo com mais frequência. O grupo de letras “tye” apareceu com menos frequência, mas pareceu se assemelhar com o “the” da língua inglesa. Partindo

desse ponto as primeiras letras da *key* que combinam com essas letras é “ar”. A partir disso foi possível supor o início da primeira palavra do *plaintext* como “Regul”. E supondo que esse início estava realmente certo, o resto do criptograma foi sendo decifrado, chegando na *key* “arara” decifrando o criptograma.

O segundo desafio foi um pouco mais difícil, pois o texto era maior. Apesar disso já era possível saber que o segundo desafio se tratava do texto em português. A análise de frequência das letras mostrou que as letras “t” e “e” eram as que mais repetiam (143x) respectivamente. Com o quadro de Frequências relativas das letras na língua inglesa pode-se deduzir que essas letras sejam respectivamente “a” e “e”. Também fiz uma análise por grupo de letras, que resultou em “ex” e “tg” aparecendo com mais frequência (17x). Na primeira tentativa, utilizei a dupla de letras “tp”, ao invés de “ex” ou “tg”, que se repetia com uma certa frequência (10x), pois ela se encontrava no início do criptograma. Assim o “t” do criptograma, poderia ser o “a” do *plaintext* oque era referente ao “t” na *key*. A partir desse ponto não consegui avançar mais.