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 *plaintext* novamente inalterado, o texto cifrado e decifrado. É importante notar que o programa quando cifrar e decifrar, vai ignorar os espaços e caracteres especiais inseridos tanto no *plaintext* quanto na *key*.