Segurança Computacional
Cifra de Vignère

Gabriel Teixeira da Silva - 17/0079538
Depa. Ciência da Computação - Universidade de Brasília (UnB)

1 Introdução

Este trabalho tem por objetivo dar suporte à quebra de uma Cifra de Vigenère, e também implementar a cifração e a decifração da mesma. Para a implementação da cifra de Vigenère foi criado um programa em python na versão 3.10.5, sua execução inicial está no arquivo `main.py`. Em relação à quebra da cifra, a frequência das letras do alfabeto da língua Portuguesa e da língua inglesa foram retirados da Wikipédia.

O programa se divide em:
- main.py
- cipher.py
- decipher.py
- attack.py
- freq.py
- keygenerator.py

O arquivo `main.py` é o principal do trabalho, ele e o responsável por chamar as funções de cifrar mensagem, decifrar, salvar resultado em arquivo de texto e atacar cifra sem chave. As funções de cifrar e decifrar usam a função de gerador de chave para fazer o keystream corretamente. A função de ataque chama a função de análise de frequências. O programa pode ser executado com:

```
python3 main.py
```

2 Implementação

Toda a lógica utilizada para a implementação do cifrador/decifrador estão em arquivos separados. A implementação do processo de cifrar ocorre após a criação da keystream, que é a repetição da key de tamanho igual à mensagem. O arquivo `cipher.py` tem uma função principal `cipher` que recebe uma mensagem, uma chave e realiza a cifração. Para cada letra na mensagem, é executada a soma da letra equivalente na string da chave, com módulo de 26 aplicado para que, por exemplo, a soma de "z" com o número "1" retorne a próxima posição possível, a letra "a".

Já a decifração funciona de forma muito similar à citada acima, mudando apenas a operação de soma para subtração entre o ascii da letra da mensagem e da *keystream*.

A parte mais complicada do trabalho, esta relacionada a função ataque. Para a decifração da chave, foi utilizada a análise de frequências das letras. Para isso, foi obtida a lista de

frequências padrão de cada letra na língua inglesa e portuguesa, e elas são usadas no programa para obter a diferença da frequência das letras na mensagem. Primeiro se analisa a repetição de vários grupos de 3 letras da cifra (espaços são desconsiderados tanto ao se escolher letras como para contar distâncias entre repetições) e se determina os números pelos quais aquela distância encontrada é divisível. A ocorrência que tiver a menor diferença representa uma letra da chave decifrada e este processo é feito em loop até encontrar toda a chave de acordo com seu tamanho obtido.

3 Conclusão

A implementação do trabalho trouxe alguns desafios, porem novos conhecimentos também. O trabalho e funcional e obedece os requisitos que foi pedido na especificação da implementação. Apesar que temos algumas limitações no tratamento de alguns caracteres que não são letras. Portanto, da mesma forma que trabalhar com a Cifra Vignère foi um grande desafio, também acabou proporcionando um enorme aprendizado.