UNIVERSIDADE DE BRASÍLIA
DEPARTAMENTO DE CIÊNCIA DA COMPUTAÇÃO

CIC0201 - Segurança Computacional - 2023.2 - Turma 01

Trabalho de Implementação 1

Cifra de Vigenère

Rafael Rodrigues Gama D. de Aragão - 190134780

1. Introdução

Este trabalho explora a cifra de Vigenère, tendo duas partes: o cifrado/decifrador e o ataque de recuperação de senha por análise de frequência. A cifra de Vigenrère é uma cifra de substituição polialfabética em que cada símbolo é deslocado baseado em uma chave criptográfica, diferentemente de uma cifra monoalfabética, onde cada símbolo é deslocado por um valor fixo. Durante muito tempo, essa cifra foi sinônimo de confiança e chegou a ser classificada como inquebrável. Porém, em 1854, Charles Babbage provou que era possível quebrar a cifra. Ao analisar repetições no texto consegue-se achar o tamanho da chave e então, utilizando análise de frequência, descobrir a chave em si.

2. Fundamentação teórica

Numa cifra de César, cada letra do alfabeto é deslocada da sua posição um número fixo de lugares; por exemplo, se tiver um deslocamento de 3, "A" torna-se "D", "B" fica "E", etc. A cifra de Vigenère consiste no uso de várias cifras de César em sequência, com diferentes valores de deslocamento ditados por uma palavra-chave".

Para cifrar, é usada uma tabela de alfabetos que consiste no alfabeto escrito 26 vezes em diferentes linhas, cada um deslocado ciclicamente do anterior por uma posição. Uma palavra é escolhida como "palavra-chave" e é repetida até ter o comprimento do texto a ser cifrado. Cada letra desta palavra vai indicar a linha a ser utilizada para cifrar ou decifrar uma letra da mensagem.

Por exemplo, supondo que se quer criptografar o texto “THINKABOUT” usando a chave “VINTAGE”. Primeiramente, repetindo a palavra-chave até o tamanho do texto tem-se que a chave resultante é “VINTAGEVINTA”. A primeira letra do texto, T, é cifrada usando o alfabeto na linha V, que é a primeira letra da chave. Basta olhar para a letra na linha V e coluna T na grelha de Vigenère, e que é um O, repetindo isso para cada letra obtém-se o texto cifrado que é “OPVGKGFJCGBT”. A desencriptação é feita utilizando o processo inverso.

Do ponto de vista matemático, a cifra pode ser descrita pela equação

$$C_i = P_i + K_i \pmod{26}$$

em que C_i é a letra criptografada, P_i é a letra a ser criptografada, K_i é a letra da chave, mod é o resto da divisão e a-z são representados como números inteiros de 0 a 25. De forma semelhante, a desencriptação pode ser descrita como

$$P_i = C_i - K_i \pmod{26}.$$

O ponto fraco da cifra é que a chave é repetida diversas vezes, resultando em pedaços iguais no texto criptográfico. Essa repetição é mais provável que ocorra quando a mesma sequência de letras do texto simples é criptografada com a mesma parte da chave.

Para quebrar a cifra, primeiramente busca-se pedaços do texto que são repetidos várias vezes. Em seguida, calcula-se a distância entre os pedaços repetidos e os divisores de cada distância. O divisor que aparece mais vezes é provavelmente o tamanho da chave.

Sabendo o tamanho da chave, pode-se então dividir o texto em n subtextos, em que n é o tamanho da chave, cada texto tendo sido criptografado pela mesma letra. Desse modo, o problema se torna igual ao da quebra da cifra de César e pode ser descriptografado por análise de frequência.

Cada letra do alfabeto tem uma frequência usual em que aparece nos textos de cada língua. Pode-se calcular a frequência em que cada letra aparece do subtexto criptografado e comparar com a frequência no idioma. De forma prática, isso pode ser feito utilizando a soma dos quadrados da diferença. Calcula-se esse valor para cada um dos 26 deslocamentos possíveis, o deslocamento que obtiver o menor resultado é provavelmente o deslocamento utilizado para aquele subtexto. Realizando esse procedimento para cada um dos subtextos, descobre-se a chave criptográfica utilizada.

3. Metodologia

Para implementação da cifra foi utilizada a linguagem de programação Python. O código está disponível em https://github.com/rafael2903/Vigenere-cipher. O arquivo vigenere.py contém

a implementação das funções de encriptação, desencriptação e quebra da cifra. O arquivo tests.py contém alguns testes unitários que testam essas funções. Para executar os testes é necessário rodar o comando `python -m unittest -v tests.py`. Também foi adicionado ao programa uma interface de linha de comando, sendo possível executar todas as funções pelo terminal passando um arquivo de entrada. A seguir são mostrados alguns exemplos de utilização dessa interface.

Encriptação

```
python vigenere.py -e -i plain_text.txt -o cipher_text.txt -k "key"
```

Desencriptação

```
python vigenere.py -d -i cipher_text.txt -o plain_text.txt -k "key"
```

Quebra da cifra

```
python vigenere.py -b -i cipher_text.txt -o plain_text.txt -l PORTUGUES
```

Mais exemplos de uso estão disponíveis no GitHub citado.

4. Conclusão

Em conclusão, a implementação da cifra de Vigenère e suas funcionalidades de criptografia, descriptografia e quebra por análise de frequência ilustram a aplicação prática dos princípios criptográficos. Este trabalho não apenas aprofundou nosso entendimento da criptografia clássica, mas também fortaleceu nossas habilidades de programação e resolução de problemas, enriquecendo nosso conhecimento em segurança da informação e contribuindo significativamente para nossa formação acadêmica nessa área.

5. Referências

- Criptoanálise da cifra de Vigenère - frwiki.wiki. Disponível em: <https://pt.frwiki.wiki/wiki/Cryptanalyse_du_chiffre_de_Vigen%C3%A8re>. Acesso em: 1 out. 2023.
- Como uma cifra do século XVII se torna uma criptografia intransponível? Disponível em: <https://www.kaspersky.com.br/blog/vigenere-cipher-history/5688/>. Acesso em: 1 out. 2023.
- WIKIPEDIA CONTRIBUTORS. Vigenère cipher. Disponível em: <https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher>.
- Vigenere CIpher. YouTube, 6 jul. 2015. Disponível em: <https://www.youtube.com/watch?v=SkJcmCaHqS0>
- Cryptography - Breaking the Vigenere Cipher. Disponível em: <https://www.youtube.com/watch?v=P4z3jAOzT9I>.