CIFRA DE VIGENÈRE - SEGURANÇA COMPUTACIONAL

Rafael Hamú, 202006448
Susannah Gurgel, 222029172

[1]Dep. Ciência da Computação – Universidade de Brasília (UnB)
CIC0201 - SEGURANÇA COMPUTACIONAL

rafahamu@gmail.com, susannahgurgel@gmail.com

Resumo. *O relatório fala sobre a implementação da Cifra de Vigenere na liguagem python. Sua codificação e decodificação, ataques utilizando tamanho da senha e análises de frequências de palavras.*

1. Introdução

A cifra de vigenere é um método de criptografia que se baseia nas séries de diferentes cifras de César baseadas em letras de uma senha. Foi criada no ano de 1553 por Giovan Battista(Wikipedia 2023). Nela, os deslocamentos se baseiam nas posições das letras das chaves que foram usadas para codificar.

2. Implementação

Nessa sessão, será apresentada como a implementação dos diferentes requisitos do trabalho práticos foram feitas.

2.1. Codificação

De forma geral, o algoritmo de codificação de uma palavra pra cifra de vigenere funciona seguindo os passos: conseguir pegar a posição do alfabeto de cada carácter do texto e de cada letra da chave, somar os 2 e dividir pelo módulo de 26.

```
for i in range(len(texto)):
    if texto[i] != ' ':
        posicao_letra_palavra = int(alfabeto.index(texto[i]))
        posicao_letra_chave = int(alfabeto.index(keyFinal[i]))
        mensagem_criptografada += str(alfabeto[(posicao_letra_palavra+posicao_letra_chave) %26])
    else:
```

Na criptografia do programa, é preciso inserir uma chave (KEY) e uma mensagem para que seja criptografada

```
Digite a chave: key
Digite a mensagem para ser criptografada: abacate
kfymero
```

Figure 1. TESTE DA CRIPTOGRAFIA

2.2. Decodificação

Seguindo os passos do codificador, o decodificador funciona basicamente da mesma forma. Ao invés de somar os posições das letras da palavra original com as letras

da chave e dividir pelo módulo de 26, elas vão ser subtraídas. Para que assim, ache a palavra que foi codificada.

```
posicao_letra_palavra = int(alfabeto.index(texto[i]))
posicao_letra_chave = int(alfabeto.index(keyFinal[i]))
mensagem_criptografada += str(alfabeto[(posicao_letra_palavra-posicao_letra_chave) %26])
```

Na descriptografia do programa, é preciso inserir uma chave (KEY) e uma mensagem para que seja descriptografada.

```
Digite a chave: key
Digite a cifra para ser descriptografada: kfymero
abacate
PS C:\Users\rafah\Documents\seguranca>
```

Figure 2. TESTE DA DESCRIPTOGRAFIA

2.3. Ataque

O ataque da segunda parte do projeto não foi implementada de forma prática. Para quebrar a cifra de Vigenère, o primeiro passo é descobrir o tamanho da chave. O método de Kasiski é uma das ferramentas utilizadas para identificar padrões de repetição no texto cifrado, indicando o provável comprimento da chave. Em seguida, usa-se a análise de frequência das letras, essa frequência varia de idioma para idioma. Observando os padrões de ocorrência de letras em cada idioma, é possível deduzir a chave e, consequentemente, descriptografar o texto cifrado.

3. Conclusão

A Cifra de Vigenère é uma técnica clássica de criptografia que, apesar de sua antiguidade, continua a demonstrar sua robustez mesmo nos tempos modernos. Durante a implementação da cifra, ficou evidente que ela é acessível e de fácil entendimento, especialmente no que diz respeito à codificação e decodificação usando uma chave conhecida. No entanto, essa aparente simplicidade na aplicação não se mantém na hora do ataque, onde, ainda hoje, se mostra uma técnica robusta, se corretamente aplicada. O grupo teve pleno entendimento de como a cifra funcionava de forma usual, mas apresentou dificuldades em realizar a quebra da mesma de forma prática.

4. Referências

Cifra de Vigenere - Wikipedia.
Cryptanalysis of Vigenere cipher - Proof of Concept.
Vigenere cipher - Geeks for Geeks.