Universidade de Brasília
Ciência da computação
Segurança Computacional

Trabalho de Implementação 1 - Cifra de Vigenére

Talles Marcelo de Mesquita Caldeira Mat:20/0060295

23 de setembro de 2023

1 Pré-requisitos

1. Versão do Python 3.x.x >=
2. Acesso ao prompt de comando(cmd)

2 Introdução

2.1 O que é a cifra de Vigenère

A cifra de Vigenère é um método de criptografia que usa uma série de cifras de César diferentes uma da outras com base nos caracteres da palavra-chave(key). Uma cifra de César é uma permutação simples que substitui cada letra do texto original(não cifrado) por outra letra de acordo com uma variação fixa do alfabeto. Por outro lado, na cifra de Vigenère, embora a palavra-chave seja fixa para uma única mensagem, ela é usada de forma cíclica ao longo do texto. Logo, embora a palavra-chave permaneça a mesma, cada letra do texto original pode ser cifrada usando um deslocamento diferente levando em consideração a posição na palavra-chave.

3 Desenvolvimento

3.1 Como o código encripta/decripta a mensagem?

Começamos com a definição de uma classe em Python chamada "VigenereCipher". Dentro dela, temos duas funções: "encrypt"e "decrypt". Na classe, recebemos a chave como parâmetro no construtor, que será usada para a cifragem da mensagem na função "encrypt". Em seguida, varremos toda a mensagem e verificamos se cada caractere é uma letra do alfabeto ou não. Se não for uma letra, simplesmente o concatenamos ao resultado.

Por outro lado, se for uma letra, fazemos o tratamento dos caracteres acentuados (diacríticos) usando o pacote Unicode. Após o tratamento, realizamos a validação se o caractere é maiúsculo ou minúsculo e calculamos o deslocamento da mensagem com base na chave. Em seguida, aplicamos a cifragem.

É importante notar que a descrição se refere a um processo de cifragem, e não a uma cifra de Vigenère completa. A cifra de Vigenère envolve a aplicação desses passos em uma sequência específica para criar um sistema de cifragem mais complexo.

Na função 'decrypt', seguimos um processo semelhante, mas ao contrário, para decifrar a mensagem usando a mesma chave. Assim, garantimos que a mensagem original seja recuperada corretamente.

3.2 Ataque de frequência

A classe Python chamada FrequencyAnalysisAttack, cujo objetivo é realizar análise de frequência em um texto cifrado com o propósito de quebrar cifras de Vigenère. Dentro dessa classe, são definidos métodos e funcionalidades essenciais para esse processo.

No construtor da classe, dois parâmetros são recebidos: o texto cifrado que se deseja analisar e a frequência de letras do idioma a ser considerado na análise. Essa frequência de letras, denotada por language_freq, é crucial para comparar as frequências das letras no texto cifrado com as frequências esperadas no idioma escolhido.

O código implementa métodos essenciais para a cifragem e decifragem de mensagens usando a cifra de Vigenère, bem como para a comparação das frequências das letras. O método vigenere é responsável por cifrar o texto com uma chave fornecida, levando em consideração se o caractere é uma letra do alfabeto, aplicando deslocamentos com base na chave e mantendo caracteres não alfabéticos inalterados.

A função compare_frequency desempenha um papel fundamental ao comparar as frequências das letras no texto cifrado com as frequências esperadas no idioma. Essa comparação auxilia na identificação da chave de cifragem mais provável.

O núcleo da análise de frequência está no método solve_vigenere. Ele tenta encontrar chaves de cifragem possíveis testando diversas combinações de chaves com diferentes comprimentos, selecionando aquela que melhor se ajusta às frequências das letras no texto cifrado.

Além disso, o código inclui subclasses especializadas para análise em português (FrequencyAnalysisAttackPT) e inglês (FrequencyAnalysisAttackENG). Cada uma dessas subclasses utiliza as frequências de letras específicas do idioma correspondente.

4 Conclusão

A demais, o código apresentado demonstra uma implementação para a quebra de cifras de Vigenère por meio da análise de frequência. Ele oferece funcionalidades cruciais para a cifragem, decifragem e comparação de frequências das letras, auxiliando na busca pela chave de cifragem correta.

No entanto, é importante destacar que o código não aborda de forma adequada a manipulação de caracteres acentuados ou diacríticos, o que pode resultar em dificuldades na decifração de mensagens que contenham tais caracteres. Essa limitação é um ponto importante a ser considerado ao usar essa ferramenta, especialmente em idiomas que fazem uso frequente de acentos. Logo, a forma a contornar tal problema foi retirar todos os acentos, mas de forma alguma impede da pessoa compreender a mensagem decifrada.