Projeto 1
Cibersegurança

Vítor Carlos Fernandes, 190142332

***Abstract*—This work consists of implementing a Vigenère cypher in Java and then proceeding to retrieve the key utilized using a frequency analisys attack.**

***Index Terms*—Cybersecurity, Vigenère cypher, Cryptography, Frequency Analisys.**

I. Introdução

ESTE Projeto tem como objetivo a implementação de um algorítmo de criptografia usando a cifra de Vingènere

II. Fundamentação Téorica

Primeiramente, é importante definir alguns termos usados:

- Cifra de Vigènere: Uma cifra primeiramente descrita no século 16 por Giovan Battista Bellaso. Trata-se de um sistema de cifra de césar. Uitiliza substituição polialfebética.
- Ataque de Análise de Frequência: Trata-se de um ataque no qual procuramos analisar uma mensagem cifrada, observando a frequência em que cada letra é utilizada na linguagem da mensagem.
- Método de Kasiski: Trata-se de um método para encontrar o tamanho da chave através da identificação de sequências de caracter repetidos, então utilizando o MDC para achar possíveis tamanhos de chave
- String: String é uma estrutura de dados composta de uma sequência de caracteres.
- Shift: shift ou troca em Português trata-se de substituir uma letra por sua correspondente. Na cifra de césar por exemplo, vamos substituí-la por uma letra um número fixo de posições no alfabeto dependendo da chave.
- Tabela de frequência: Uma tabela com as frequências em que cada letra é utilizada em uma língua.

Nosso código apresenta as seguintes funcionalidades:
- Cifrar uma string utilizando uma chave e opcionalmente uma tabela de codificação.
- Decifrar uma string codificada com a cifra de Vingènere
- Extrair a chave através de um ataque de análise de frequência.
O processo de codificar uma frase usando a cifra de vingènere primeiro consiste em criar uma tabela de alfabeto usando várias cifras de césar, tal aplicação pode ser observada na função gettable. No próximo passo, ciframos a mensagem pegando cada carácter, calculando o shift em função da nossa tabela. O processo de decifração é parecido com o de cifração, a diferença é que vamos inverter coluna e fileira na nossa tabela, adquirindo assim, o carácter original.

O ataque de frequência é um pouco mais complicado, primeiro, devemos ter em mãos a tabela de frequência da linguagem da mensagem original, na qual iremos usar para categoriazar a frequência de cada carácter na mensagem cifrada. Depois, iremos usar o método de Kasiski para estimar possíveis tamanhos de chave, isso nos permitirá dividir a mensagem cifrada em blocos. Cada bloco corresponde a uma letra diferente na chave, podemos calcular o shift de cada bloco através de um ataque de substituição de uma letra usando a frequência em cada bloco, isso nos dará um array de shifts. Finalmente, podemos usar os shifts para determinar a chave usada para cifrar nossa mensagem.
Utilizando as seguintes ferramentas:
- Command Prompt. -Java Developer Kit

O processo experimental segue o seguinte roteiro: Após o desenvolvimento do algoritmo, devemos simplesmente testa-lo com diferentes entradas

III. Analise teorica

Apos executarmos os testes obtivemos os seguintes resultados: Para o nosso cifrador Entrada: Texto HELLO, chave ABC. Saída: HFNLP.

Para o nosso decifrador Entrada: Texto HFNLP, chave ABC. Saída: HELLO.

Para o nosso ataque no texto cifrado XYZXYZ com chave ABC ”Potential key lengths: [1, 2, 3]” Já que a chave tem tamanho 3, esse é um resultado satisfatório para o método utilizado.

IV. Conclusão

Ao final, verificamos a implementação bem sucedida da cifra de Vingènere, bem com a aplicação de um ataque de análise de frequência para estimar possíveis chaves utilizadas na cifração da menságem.

References

[1] J. K. Y. Lindell, *Introduction to Modern Cryptography*, 3rd ed. Boca Raton, Florida: CRC Press, 1994.

[1]