Departamento de Ciência da Computação

Segurança Computacional

1º EXERCÍCIO
CIFRA DE VIGENÈRE

Trabalho apresentado à Universidade de Brasília, como pré-requisito para obtenção de nota parcial, referente à avaliação do semestre, na disciplina de Segurança Computacional, relativo ao primeiro semestre de 2023.

CIC0201
Professor: João José Costa Gondim.
Discente: Vinícius Giovani Moreira Nascimento – 170115437 (Turma 2)
Adriano Ulrich do Prado Wiedmann – 202014824 (Turma 1)

1. CIFRA DE VIGENÈRE

A cifra de Vigenère foi atribuída a Blaise de Viginère por volta de 1550. O método é baseado na cifra de César, representando uma cifração por substituição polialfabética, com a implementação do diferencial de rotações variáveis do alfabeto de acordo com a chave utilizada. Para realizar esta cifração, ampliamos uma chave escolhida (usualmente uma palavra do idioma) de acordo com o tamanho da mensagem a ser criptografada. Em seguida mapeamos os deslocamentos dos caracteres do *plaintext* através da tábula de Vigenère, conforme Fig. 1.

Apesar de ser um procedimento simples, esta cifra se mostrou extremamente eficaz, sobrevivendo por anos, devido ao deslocamento variável dos caracteres, quando mapeados aos caracteres do *ciphertext* podem levar a criptografia distintas para um mesmo caractere ou o mesmo símbolo criptográfico para caracteres distintos.

A cifra pode ser compreendida matematicamente ao transformarmos o alfabeto base em um vetor de 0 a 25, assim, somamos a cada letra a ser criptografada ao valor numérico da chave e realizamos a cifração de César naquele caractere com um deslocamento N, caso o número resultante seja maior que 25, realizamos a divisão por 25 e tomamos o resto, representando uma volta completa no alfabeto. Podemos representar essa equação como x mod n, e realizar a cifração de forma matem ática.Alguns procedimentos podem ser adotados para dificultar ainda mais a descoberta da chave, tais como a troca recorrente de chave, uso de chaves distintas e com caracteres menos repetitivos, divisão da cifra em palavras do mesmo tamanho ou a exclusão de caracteres mais frequentes do idioma no plaintext, como por exemplo a cifração de um texto em inglês sem os caracteres de letra ‘e’.

Figura 1 – Tábula ou Grade de Vigenère.

2. QUEBRANDO A CIFRA DE VIGENÈRE

Para descobrir a chave criptográfica a partir de um texto cifrado através da cifra de Viginère, realizamos procedimentos baseados em análise de frequência, metodologia desenvolvida por Friedrich Kasiski em por volta de 1850. Por se tratar de uma cifra por substituição, a cifra de Vigenère mantém as estatísticas de incidência de letras do alfabeto do idioma em que foi criptografada a mensagem em claro.

Na implementação do código, realizou-se o tratamento do dado de entrada (*ciphertext*), em seguida é realizado o cálculo de repetições de trigramas e suas respectivas distâncias no *chipertext*. Optamos inicialmente por aquele que possua o maior número de repetições.

Após a definição do trigrama, retiramos o Máximo Divisor Comum (MDC) dos valores encontrados, a fim de estimar o tamanho da chave. Como o método envolve a análise de frequência, há a possibilidade de encontrar erros no tamanho da chave ou na escolha do trigrama, sendo assim, o decifrador deverá considerar a possibilidade de refazer a decriptografia a partir de outras hipóteses.

Para a segunda etapa, quebramos o texto em n partes iguais do tamanho da chave e agrupamos em uma matriz. Separamos cada coluna da matriz em um vetor, pois estes valores foram criptografados com o mesmo caractere de chave, em seguida alocamos a distribuição de frequência das letras da coluna de acordo com a distribuição de frequência das letras do alfabeto da mensagem em claro, este procedimento é repetido para todas as colunas.

Por fim, realizamos a conferência da mensagem e com o valor do shift realizado em cada coluna do alfabeto conseguimos montar a chave utilizada ao realizar a associação com os números posicionais de cada letra no alfabeto.