Universidade de Brasília – UnB

Departamento de CIC

Segurança Computacional

Alunos: Alexandre Victor Curcino Vasconcelos Cruvinel e Lucas Gonçalves Morais.

Matrículas: 19/0023546 e 19/0033240.

Relatório do Trabalho 1

Na função de Cifração de Vigenère a gente recebeu a mensagem a ser cifrada e a senha, dada essa informação, procuramos a posição de cada caractere do texto no alfabeto e também fomos procurando a posição de cada caractere da senha no alfabeto, além disso se a mensagem for maior que a senha precisamos resetar, pois dessa forma não teria a keystream e geraria um problema no código. Outrossim, agora vem o mais importante da cifração, essa foi a geração de cada linha da tabela cíclica conforme a criação de Vigenère, fizemos isso utilizando o complementar de dois arrays e com esse fomos achando cada caracter da cifra correspondente ao texto a ser cifrado de acordo com o número da posição, juntando as letras formando o resultado dessa cifra.

Já na função de Decifração de Vigenère recebemos a mensagem cifrada e a senha, a ideia é parecida com a cifração, porém agora estamos tratando de fazer o inverso que a cifração faz. Dessa maneira, pegamos o índice da senha no alfabeto, geramos a tabela cíclica de acordo com a senha , pesquisamos o índice de cada caracter da mensagem cifrada no alfabeto parcial(linhas da tabela cíclica de Vigenère). Por fim, achamos cada caractere do texto decifrado no alfabeto e juntamos as letras formando o resultado dessa decifração.

E por último, mas não menos importante, o ataque de recuperação da senha por análise de frequência, o qual criamos funções para pontuar as frequências em português e inglês. Por fim, não conseguimos implementar.

Limitações: A senha só pode ser letras, portanto sem pontos, vírgulas e etc.