UNIVERSIDADE DE BRASÍLIA DEPARTAMENTO DE CIÊNCIA DA COMPUTAÇÃO

CIC0201 - Segurança Computacional – 2021/1 Trabalho de Implementação 1 - Cifra de Vigenere

> Caio Massucato -Caroline Ferreira - 16/0067766

1. INTRODUÇÃO

Cifra de Vigenere é um método de criptografia que consiste em uma série de cifras de César diferentes, tendo como base as letras de uma *keyword*.

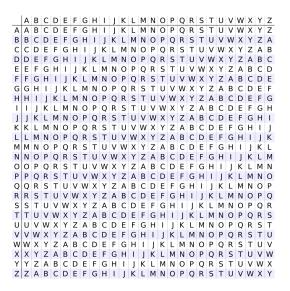


Figura 1. Quadrado de Vigenère, com as combinações de alfabetos

Essa cifra se baseia em várias cifras de César que são utilizadas sequencialmente, com diferentes valores de deslocamento e obtidos a partir de uma *keyword*. A cifragem é realizada por meio de uma tabela de alfabetos, também chamada de "quadrado de Vigenère" (figura 1), que baseia-se no alfabeto escrito 26 vezes em linhas diferentes, cada um deslocado de forma cíclica para a esquerda comparado com o alfabeto anterior, de modo a combinar às 26 possíveis cifras de César. Ao longo desse processo de criptografia, a cifra usa um alfabeto diferente de uma das linhas, e o alfabeto a ser utilizado em cada ponto depende da *keyword*, que é repetida caso a mensagem a ser cifrada seja maior do que ela.

2. OBJETIVOS

Este trabalho tem como objetivo explorar a cifra de Vigenere, consistindo em duas partes:

- Cifrador/decifrador: o cifrador recebe uma senha e uma mensagem que será cifrada pela cifra de Vigenere, resultando em um criptograma, enquanto o decifrador receberá uma senha e um criptograma que será decifrado pela cifra de Vigenere, recuperando uma mensagem.
- Ataque de recuperação de senha por análise de frequência: duas mensagens cifradas (uma em português e outra em inglês) serão providas com senhas distintas. Cada uma dessas mensagens deverá ser utilizada na recuperação da senha responsável pela geração do keystream utilizado na cifração e então, serão decifradas.

3. IMPLEMENTAÇÃO

4. CONCLUSÃO