MELHORIAS IMPLEMENTADAS

Uma melhoria da Cifra Cesar foi a criação da "Cifra monoalfabética", nela consiste uma chave diferente para cada letra da mensagem que será criptografada (existem 26 chaves, cada uma indica uma letra do alfabeto diferente para ser o A) , ou seja, cada letra tem uma ordem do alfabeto diferente. Essa técnica deixa a cifra de Cesar muito mais complicada de ser decodificada por terceiros.

Texto Original	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Texto Cifrado	UMGSCWXZFPBNTKHEYOVRDIAJLQ

Na imagem acima é possivel perceber que, mesmo o texto original sendo o alfabeto na ordem certa, o texto cifrado não tem nenhuma padrão perceptivel. Cada letra tem uma chave diferente.

Também tem a versão mais simplificada da Cifra monoalfabética apresentada acima, ela tem o mesmo intuito, criar diferentes tipos de chaves para não deixar a Cifra de Cesar original tão previsivel (Na original, o A sempre é equivalente ao D). Porém, nessa cifra simplificada é utilizada apenas 1 chave para a mensagem toda, ou seja, enquanto a cifra monoalfabética original usa 1 chave diferente para cada letra, essa mais simplificada usa apenas 1 chave para a mensagem inteira. No nosso trabalho, foi utilizado essa técnica mais simplificada da cifra de Cesár monoalfabética.

http://clubedosgeeks.com.br/sem-categoria/cifra-de-cesar-criptografia-monoalfabetica

https://www.gta.ufrj.br/grad/10_1/aes/index_files/Page1294.htm

http://wiki.stoa.usp.br/images/c/cf/Stallings-cap2e3.pdf