Luan Machado Bernardt | GRR20190363
Lucas Soni Teixeira | GRR20190395

TRABALHO DE CRIPTOGRAFIA I

Neste trabalho foi implementado uma cifra de substituição, com os algoritmos de cifrar e decifrar. A cifra desenvolvida é baseada na Cifra de César, pois apenas substitui um caractere por outro no alfabeto de acordo com um valor de rotação.

CARACTERÍSTICAS:

- O alfabeto inclui todas as letras maiúsculas do alfabeto romano, os números de 0 a 9 e ainda alguns caracteres especiais ('.', ',', '!', '?', '"', '@', '#', '$');

- Existem quatro grupos ou sub-alfabetos nos quais os 44 caracteres se agrupam em 4 grupos de 11, assim um caractere pode eventualmente ser representado por qualquer um dos outros 10 presentes no grupo.

ALGORITMO:

Para criptografar um texto já formatado (sem espaços e todas as letras maiúsculas) se sucedem os seguintes passos:

- Salva-se a posição i do caractere na mensagem original e calcula-se i % 11 (tamanho dos subgrupos). O resultado deste cálculo será a rotação que esse caractere sofrerá. No entanto, há a chance dessa rotação ser 0 (caso i seja múltiplo de 11), nessa ocasião não haveria rotação, por isso atribui-se o valor 1 ou 10 (alterna-se entre um ou outro);

- Para efetivamente realizar a troca do caractere, deve-se levar em conta em qual subgrupo ele se encontra, pois se ele estiver no grupo A ou C as rotações ocorrem para a direita, enquanto no grupo B e D para a esquerda;

(A ou C) X -> (posição(X) + rotação) % 11;
(B ou D) Y <- (posição(Y) - rotação);

Para descriptografar (opção -d ou -D) o mesmo se sucede, no entanto, os conjuntos A e C trocam para a esquerda, enquanto B e D para a direita;