UNIVERSIDADE
FEDERAL DO CEARÁ

Segurança - 2023.1 Prof. Marcos Dantas Ortiz - mdo@ufc.br

Aluno:_____

1) Cifre a mensagem a seguir usando cifra de César com K =7:

   "A Cesar o que e de Cesar. Todos os caminhos levam a Roma."

2) Decifre a mensagem abaixo sabendo que foi utilizada Cifra de César com k = 5

   "sfif jcnxyj ij yft inknhnq vzj sft xjof ajshnajq"

3) Resolva a cifra monoalfabética a seguir.

   LXIPBT JD TKSTRXRKXLBO AKD KRXQXUBE BYDWBT KE BQIBSDRO LXIPBWRD

   Chave: *b-s-l-j-d-i-g-h-x-m-z-q-e-w-o-y-a-p-t-r-k-v-n-c-f-u*

   Comente a fragilidade do criptográfico, apesar do espaço de chaves ser da ordem 26!

4) Resolva a cifra de Playfair a seguir:

   Texto cifrado: BZCNFQEHNKBNIGMRHI Chave: Criptografia

5) Cifre "001101111" e decifre usando cifra de bloco:

Cifragem: C(i) = Ks(M(i) XOR R(i))

Decifragem: M(i) = Ks(C(i)) XOR R(i)

R(1) = 001, R(2) = 111 e R(3) = 100

Tabela de mapeamento Ks

Entrada	Saída	Entrada	Saída
000	110	100	011
001	111	101	010
010	101	110	000
011	100	111	001

6) Comente o uso de números aleatórios na questão 5 (R1, R2 e R3). Por que é menos seguro usar apenas a tabela de mapeamento?

7) Repita o exercício da questão 5 utilizando a técnica de Encadeamento do Bloco de Cifra. Use R(1) como vetor de inicialização.

Bom Trabalho!