UNIVERSIDADE
FEDERAL DO CEARÁ

Segurança - 2022.1

Prof. Marcos Dantas Ortiz - mdo@ufc.br

Aluno:_____

1) Explique porque algoritmos de criptografia que geram repetição de padrões não são indicados para uso não-acadêmico.

2) Motive o uso da Confusão e da Difusão para evitar os problemas da questão 1. Como esses requisitos são implementados no DES?

3) Diferencie cifra de fluxo da cifra de bloco. Cite uma cifra de cada tipo.

4) 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

5) Comente o uso de números aleatórios na questão 4 (R1, R2 e R3). Por que é menos seguro usar apenas a tabela de mapeamento?

6) Repita o exercício da questão 4 utilizando a técnica de Encadeamento do Bloco de Cifra. Use R(1) como vetor de inicialização.

7) Explique porque o algoritmo *One Time Pad* é considerado uma cifra perfeita (inquebrável).
   a) Faça o ataque força bruta do texto cifrado: 1001
   b) Qual chave gerou esse texto cifrado?