Professor: Antonio Augusto Rocha
Disciplina: Segurança da Informação
Período: 2013/2
Aluno:_____

Instituto de computação

Lista de Exercícios 2

Obs.: As soluções da lista de exercícios devem ser individuais e podem ser digitadas ou redigidas. A entrega deve ser feita no final da aula do dia previsto na página do curso. Não serão aceitas entregas por e-mail ou fora do prazo.

1. Por que é importante estudar a Cifra de Feistel?

2. Qual a diferença entre uma Cifra de Bloco e uma Cifra de Fluxo?

3. Por que não é prático usar uma Cifra de Substituição Reversível qualquer do tipo mostrado na tabela abaixo?

Plaintext	Ciphertext
0000	1110
0001	0100
0010	1101
0011	0001
0100	0010
0101	1111
0110	1011
0111	1000
1000	0011
1001	1010
1010	0110
1011	1100
1100	0101
1101	1001
1110	0000
1111	0111

Ciphertext	Plaintext
0000	1110
0001	0011
0010	0100
0011	1000
0100	0001
0101	1100
0110	1010
0111	1111
1000	0111
1001	1101
1010	1001
1011	0110
1100	1011
1101	0010
1110	0000
1111	0101

4. O que é uma Cifra de Produto?

5. Qual é a diferença entre Difusão e Confusão?

6. Que parâmetros e escolhas de projeto determinam o algoritmo real de uma Cifra de Feistel?

7. Explique o Efeito Avalanche.

8. Cite os 5 modos de operação e dê detalhes sobre as execuções de cada um deles.

9. Diferencie os três tipos de operação do DES (simples, DES duplo, DES Triplo com duas chaves e DES Triplo com três chaves).