Lista de exercícios: DES

1. Quando o DES foi desenvolvido?

2. Descreva passo a passo como o DES funciona.

3. O que é uma rede de Feistel? Escreva as equações relacionadas à encriptação e decriptação.

4. Escreva um pseudo-código para uma rede de Feistel com número de turnos e tamanho de bloco configuráveis.

5. Descreva um ataque eficiente contra o DES.

6. Descreva um ataque eficiente contra o DES usado duas vezes com duas chaves distintas em um mesmo bloco de dados.

7. Como adaptar o ataque Meet-in-the-middle contra 3DES?

8. Descreva a história de ataques contra o DES incluindo o papel da Electronic Frontier Foundation e da distributed.net.

9. É dito que existem quatro chaves fracas para o DES. Quais são elas?