Lista de exercícios 5
Modos de operação
Segurança da Informação

1. Porque são necessários modos de operação para cifras de blocos?

2. Explique porque existem diferentes modos de operação de cifras de blocos? Quais são as principais funcionalidades que os diferenciam?

3. Defina matematicamente cada um dos seguintes modos de operação: ECB,CFB,OFB,CTR e CBC.

4. Prove que o modo ECB é inseguro.

5. Compare o funcionamento dos modos CBC e CTR.

6. O que é o Galoi Counter Mode?