Universidade Federal do
Agreste de Pernambuco
Av. Bom Pastor s/n - Boa Vista
55292-270 Garanhuns/PE
☎ +55 (87) 3764-5500
http://www.ufape.edu.br

Bacharelado em Ciência da Computação
CCMP3079 Segurança de Redes de Computadores
Prof. Sérgio Mendonça

Atividade Cap. 06 - Operação de Cifra de Bloco
Para 11/12/2023

Nome Completo: _____

Questões retiradas do livro-texto da disciplina.
Conforme conversamos em sala de aula, as atividades devem ser realizadas para apresentação e discussão em sala, sempre nas aulas das quintas-feiras, atribuindo ao estudante uma nota de 0 ou 1 por cada atividade realizada e apresentada.

1. O que é encriptação tripla?
2. O que é ataque *meet-in-the-middle*?
3. Quantas chaves são usadas na encriptação tripla?
4. Por que a parte do meio do 3DES é decriptação, em vez de encriptação?
5. Por que alguns modos de operação de cifra de bloco só utilizam a encriptação, enquanto outros empregam encriptação e decriptação?
6. Você deseja construir um dispositivo de hardware para realizar encriptação de bloco no modo cipher block chaining (CBC) usando um algoritmo mais forte do que DES. 3DES é um bom candidato. A Figura 1 mostra duas possibilidades, ambas acompanhando a definição do CBC. Qual das duas você escolheria:
   (a) Por segurança?
   (b) Por desempenho?
7. Crie um software que possa encriptar e decriptar no modo cipher block chaining usando uma das seguintes cifras: módulo affine 256, módulo Hill 256, S-DES, DES.
   Teste os dados para S-DES usando um vetor de inicialização binário de `1010 1010`. Um texto claro binário de `0000 0001 0010 0011` encriptado com uma chave binária de `01111 11101` deverá dar um texto claro binário de `1111 0100 0000 1011`. A decriptação deverá funcionar de modo correspondente.

Livro-texto da disciplina:
STALLINGS, William. Criptografia e segurança de redes. Princípios e práticas, Ed. 6. 2014.

Figura 1: Uso de triple DES no modo CBC.