Universidade Federal do
Agreste de Pernambuco
Av. Bom Pastor s/n - Boa Vista
55292-270 Garanhuns/PE
T +55 (87) 3764-5500
m 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: Luan Valentino Sampaio Marques

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?

Solução: A encriptação tripla, também conhecida como 3DES (Triple DES), é um método de criptografia que aplica o algoritmo DES (Data Encryption Standard) três vezes a cada bloco de dados. O objetivo é aumentar a segurança em relação ao DES simples. No 3DES, o processo envolve três etapas de criptografia: a primeira etapa encripta o dado com a primeira chave, a segunda etapa decripta o dado com a segunda chave, e a terceira etapa encripta o dado novamente com a terceira chave.

2. O que é ataque *meet-in-the-middle*?

Solução: O ataque meet-in-the-middle é um tipo de ataque criptográfico que reduz a complexidade da quebra de criptografias que usam múltiplas camadas de encriptação, como o 3DES. Neste ataque, o invasor encripta o texto claro até o ponto intermediário usando uma chave e decripta o texto cifrado até o mesmo ponto intermediário usando uma segunda chave. O invasor então compara os resultados intermediários para encontrar uma correspondência, permitindo que ele descubra as chaves utilizadas.

3. Quantas chaves são usadas na encriptação tripla?

Solução: Na encriptação tripla (3DES), podem ser usadas uma, duas ou três chaves distintas. O esquema mais comum utiliza três chaves diferentes (3K3DES), o que aumenta significativamente a segurança. No entanto, existem variantes que utilizam apenas duas chaves (2K3DES) ou uma chave repetida três vezes (1K3DES), cada uma oferecendo diferentes níveis de segurança.

4. Por que a parte do meio do 3DES é decriptação, em vez de encriptação?

Solução: A parte do meio do 3DES é uma decriptação para garantir compatibilidade retroativa com o DES simples. Quando a mesma chave é usada para todas as três etapas, o 3DES equivale a

uma simples encriptação DES, tornando-o compatível com sistemas legados que usam DES. Além disso, esse processo de encriptação-decriptação-encriptação (EDE) aumenta a segurança do esquema sem sacrificar a compatibilidade.

5. Por que alguns modos de operação de cifra de bloco só utilizam a encriptação, enquanto outros empregam encriptação e decriptação?

Solução: Alguns modos de operação de cifra de bloco, como o modo de cifra de bloco ECB (Electronic Codebook) e o CBC (Cipher Block Chaining), utilizam apenas a encriptação durante o processo de cifragem porque os dados são tratados em blocos independentes ou com dependência do bloco anterior, sem necessidade de decriptação no processo. Outros modos, como o CFB (Cipher Feedback) e o OFB (Output Feedback), podem usar tanto encriptação quanto decriptação para garantir que o processo funcione corretamente, especialmente em cenários de streaming de dados onde os blocos de saída são alimentados de volta no processo de cifragem.

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?

Solução: Opção (b) CBC com três loops é a melhor escolha para segurança.

Justificativa:

- A opção (b) aplica três operações criptográficas distintas (encriptação, decriptação e encriptação novamente) com três chaves diferentes (K1, K2 e K3). Isso adiciona camadas de complexidade e resistência contra ataques, como o ataque meet-in-the-middle, porque a presença de três operações distintas e chaves diferentes torna muito mais difícil para um atacante quebrar o esquema.

- Cada estágio do processo criptográfico no CBC com três loops utiliza chaves diferentes, o que contribui significativamente para a segurança geral do sistema.

(b) Por desempenho?

Solução: Opção (a) CBC com um loop é a melhor escolha para desempenho.

Justificativa:

- A opção (a) é mais eficiente porque utiliza uma única etapa de criptografia (EDE) com um ciclo de retroalimentação, o que significa que apenas um ciclo é necessário para processar cada bloco de dados. Como o algoritmo EDE encapsula três operações de criptografia em uma, ele reduz o número de operações separadas necessárias, resultando em maior velocidade e menor latência no processamento dos dados.

- O fato de que o CBC com um loop precisa realizar menos operações de criptografia por bloco torna-o mais rápido, economizando recursos computacionais e tempo.

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.

Solução: