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

Atividade Cap. 03
Para 17/10/2023

Nome Completo:José Elias de Lima

Nome Completo:
Questões retiradas do livro-texto da disciplina.

1. Responda os questionamentos a seguir:

(a) Por que é importante estudar a cifra de Feistel?
R: Porque muitos algoritmos são baseados nessa cifra.

(b) Qual é a diferença entre uma cifra de bloco e uma cifra de fluxo?
R: A diferença é, a de fluxo cifra bit ou byte por vez, enquanto que a cifra de bloco um conjunto de bit é cifrado ao mesmo tempo, normalmente entre 64 a 128 bits.

(c) Por que não é prático usar uma cifra de substituição reversível qualquer do tipo mostrado na Tabela 3.1?
R: Se a cifra for um bloco pequeno, ela acaba sendo como uma cifra clássica, sensível à análise estatística do texto claro.

(d) O que é uma cifra de produto?
R: É o uso de duas ou mais cifras ao mesmo tempo, resultado em uma cifra mais mais forte.

(e) Qual é a diferença entre difusão e confusão?
R: Na difusão a estrutura estatística do texto claro e dissipada em estatística de longa duração de texto cifrado, já a confusão tem o relacionamento do texto claro com a chave de encriptação mais complexo possível.

(f) Que parâmetros e escolhas de projeto determinam o algoritmo real de uma cifra de Feistel?
R: São os seguintes parâmetros, tamanho do bloco, quanto maiores mais segurança, tamanho da chave, também quanto maior mais segura, número de rodadas, quanto maior o número de rodadas mais segurança, algoritmo de geração de subchave, maior complexidade nesse algoritmo mais difícil será fazer a análise, função F, como anteriormente maior complexidade mais difícil será a análise, rápida encriptação e decriptação, o algoritmo tem que fazer isso de forma rápida e por último facilidade na análise, um algoritmo facil de análise fica mais fácil de explicar e descobrir falhas.

(g) Explique o efeito avalanche.
R: É quando uma pequena alteração no texto claro ou na chave, produz uma mudança significativa no texto cifrado.

2. Qual(is) dos recursos abaixo estão presentes no projeto da rede de Feistel? Explique.
(a) Tamanho do bloco e da chave;
(b) Função da rodada;
(c) Gerador de sub-chaves;
(d) Todas as alternativas.
R: Todas as alternativas, como explicado na questão 2 letra f. o tamanho do bloco e da chave importam, a função da rodada quanto mais melhor, e um gerador de sub-chave complexo.

3. Qual é o tamanho do texto claro no Data Encryption Standard (DES)? Explique.
(a) 57;
(b) 48;
(c) 32;
(d) 64.
R: 64 bits, o algoritmo transforma uma entrada de 64 bits, faz uma série de etapas e depois tem uma saída de 64 bits.

4. A cifra de Feistel do algoritmo de encriptação utilizada no Data Encryption Standard (DES) utiliza quantos S-boxes? Explique.
(a) 8;
R: 8 caixas, elas são usadas em cada iteração.

(b) 7;
(c) 6;
(d) 5.

5. O Data Encryption Standard possui uma chave de 56 bits, o que torna possível um espaço de 2^56 chaves possíveis. Essa sentença trata de ataque de. . . Explique.
(a) Tempo;
R: Tempo, ataque de temporização explora o fato de que um algoritmo de encriptação ou decriptação em geral exige quantidades ligeiramente diferentes de tempo para diversas entradas
(b) Matemático;
(c) Força-Bruta;
(d) DoS.

6. Demonstre, através de um exemplo, como realizar a cifragem de 16 bits (dois caracteres), em 2 rounds, em seguida, decifre o texto cifrado. Explique o processo passo a passo. Forneça um código Python/Sagemath com sua solução.
R: Código no github

7. Considere uma cifra de Feistel composta de 16 rodadas com tamanho de bloco de 128 bits e tamanho de chave de 128 bits. Suponha que, para determinado k, o algoritmo de escalonamento de chave defina valores as oito primeiras chaves de rodada, k1, k2, . . . , k8, e depois estabeleça

k9 = k8, k10 = k7, k11 = k6, . . . , k16 = k1

Admita que você tenha um texto cifrado S. Explique como, com acesso a um oráculo de encriptação, você pode decriptar c e determinar m usando apenas uma única consulta a ele. Isso mostra que tal cifra é vulnerável a um ataque de texto claro escolhido. (Um oráculo de encriptação pode ser imaginado como um dispositivo que, dado um texto claro, retorna o texto cifrado correspondente. Os detalhes internos do dispositivo não são conhecidos, e você não pode abri-lo. Você só consegue obter informações do oráculo fazendo consultas a ele e observando suas respostas.)

R: **Passo 1: Escolha de Texto Claro**

Escolha um texto claro PPP tal que ele tenha uma estrutura simples, por exemplo, todos os bits zerados:

Passo 2: Encriptação com o Oráculo

Utilize o oráculo de encriptação para obter o texto cifrado correspondente ao texto claro PPP:

C=E(P)C = E(P)C=E(P)

Suponha que o texto cifrado resultante seja CCC.

Passo 3: Usar a Estrutura da Chave para Decriptação

A estrutura da chave de rodada fornece uma pista importante. As chaves das rodadas k9k_9k9 a k16k_{16}k16 são as mesmas que as chaves das rodadas k8k_8k8 a k1k_1k1, mas em ordem inversa. Isso significa que podemos explorar a simetria no processo de encriptação e decriptação.

Descrição do Processo de Decriptação:

Para decriptar CCC e obter PPP, faça o seguinte:

1. **Dividir o Texto Cifrado**: Divida CCC em duas metades, L16L_{16}L16 e R16R_{16}R16:

C=(L16,R16)C = (L_{16}, R_{16})C=(L16,R16)

2. **Simetria da Cifra de Feistel**: Utilizando a simetria e a repetição das chaves de rodada, note que as últimas 8 rodadas de encriptação são as primeiras 8 rodadas de decriptação.

3. **Inverso da Encriptação**: Aplique as mesmas 8 rodadas de encriptação de CCC novamente. Devido à estrutura da cifra, isso irá reverter o processo e efetivamente decriptar o texto cifrado.
4. **Resultado**: Após aplicar as 8 rodadas, obteremos o texto claro PPP.