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. 03
Para 30/10/2023

Nome completo: Thiago Cavalcanti Silva

Questões retiradas do livro-texto da disciplina.

1. Responda os questionamentos a seguir:

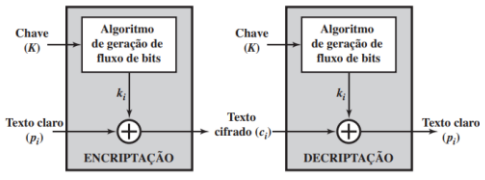
(a) Por que é importante estudar a cifra de Feistel?

Ela oferece um modelo que foi usado como base para várias outras cifras simétricas, ou seja, além de sua importância histórica, auxilia no entendimento de alguns conceitos e etapas utilizados por outras cifras.

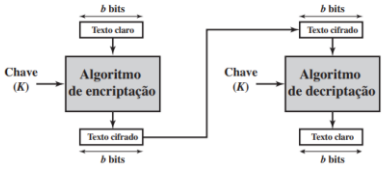
(b) Qual é a diferença entre uma cifra de bloco e uma cifra de fluxo?

Cifra de fluxo é aquela que encripta um fluxo de dados digital um bit ou um byte por vez.

Já a de bloco, é aquela em que um bloco de texto claro é tratado como um todo e usado para produzir um de texto cifrado com o mesmo tamanho.



(a) Cifra de fluxo usando gerador algorítmico de fluxo de bits



(b) Cifra de bloco

(c) Por que não é prático usar uma cifra de substituição reversível qualquer do tipo mostrado na Tabela 3.1?

Se ela for usada em um tamanho de bloco pequeno, como n = 4, então o sistema é equivalente a uma cifra de substituição clássica. Esses sistemas, como já vimos, são vulneráveis a uma análise estatística do texto claro.

Já para um grande tamanho de bloco, ela não é prática, de um ponto de vista de implementação e de desempenho.

(d) O que é uma cifra de produto?

A execução de duas ou mais cifras simples em sequência, de tal forma que o resultado ou produto final seja criptograficamente mais forte do que qualquer uma das cifras componentes.

(e) Qual é a diferença entre difusão e confusão?

A confusão é quando a estrutura estatística do texto claro é dissipada em estatísticas de longa duração do texto cifrado. Ou seja, ela busca tornar o relacionamento estatístico entre o texto claro e o texto cifrado o mais complexo possível, a fim de frustrar tentativas de deduzir a chave. Isso é obtido fazendo-se que cada dígito do texto claro afete o valor de muitos do texto cifrado.

Enquanto a difusão procura estabelecer o relacionamento entre as estatísticas do texto cifrado e o valor da chave de encriptação o mais complexo possível, novamente para frustrar tentativas de descobrir a chave. Assim, mesmo que o atacante possa ter alguma ideia das estatísticas do texto cifrado, o modo pelo qual a chave foi usada para produzir esse texto cifrado é tão complexo que torna difícil deduzir a chave.

(f) Que parâmetros e escolhas de projeto determinam o algoritmo real de uma cifra de Feistel?

Tamanho de bloco, tamanho da chave, número de rodadas, algoritmo de geração de subchave e função F.

(g) Explique o efeito avalanche.

Quando uma pequena mudança no texto claro ou na chave produza uma alteração significativa no texto cifrado. Em particular, uma mudança em um bit do texto claro ou um bit da chave deverá produzir uma modificação em muitos bits do 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.

Letra D. Todos os recursos acima fazem parte da cifra de Feistel e influenciam na segurança do algoritmo.

3. Qual é o tamanho do texto claro no Data Encryption Standard (DES)? Explique.

(a) 57;

(b) 48;

(c) 32;

(d) 64.

Letra D. O DEA (Data encryption Algorithm), algoritmo utilizado pelo DES, encripta os dados em blocos 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;

(b) 7;

(c) 6;

(d) 5.

Letra A. O DES possui oito tabelas de substituição, chamadas de S-boxes, utilizadas a cada iteração.

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;

(b) Matemático;

(c) Força-Bruta;

(d) DoS.

Letra C. O ataque por força-bruta envolve tentar todas as combinações possíveis de chaves até encontrar a chave correta que descriptografa os dados com sucesso. Um ataque de força-bruta envolveria testar cada uma dessas chaves, o que seria demorado, mas possível.

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.

Considerando uma encriptação simples, que aplica apenas um XOR no texto. A chave 1 será %, a chave 2 será U e a palavra será OK.

Temos que:

O = 79 = 01001111

K = 75 = 01001011

Chave 1 = % = 37 = 00100101

Chave 2 = U = 85 = 01010101

Primeira rodada da encriptação:

O = 01001111	K = 01001011
Chave 1 = 00100101	Chave 1 = 00100101
XOR = 01101010 = 106 = j	XOR = 01101110 = 110 = n

Segunda rodada da encriptação:

j = 01101010	n = 01101110
Chave 2 = 01010101	Chave 2 = 01010101
XOR = 00111111 = 63 = ?	XOR = 00111011 = 59 = ;

Para decriptar, basta fazer o processo inverso.

Primeira rodada da decriptação:

? = 00111111	; = 00111011
Chave 2 = 01010101	Chave 2 = 01010101
XOR = 01101010 = 106 = j	XOR = 01101110 = 110 = n

Segunda rodada da decriptação:

j = 01101010	n = 01101110
Chave 1 = 00100101	Chave 1 = 00100101
XOR = 01001111 = 79 = O	XOR = 01001011 = 75 = K

A parte prática está disponível no Notebook do SageMath, no arquivo “Exercícios do capítulo 3.ipynb”.

https://cocalc.com/projects/715090fc-6c4e-4dae-a5a7-272936e472a9/files/Exerc%C3%ADcios%20do%20cap%C3%ADtulo%203.ipynb#id=fd3dc8

https://github.com/ThiagoCavalcantiSilva/seguranca-de-redes

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, k_1, k_2, . . . , k_8, e depois estabeleça

$$k_9 = k_8, k_{10} = k_7, k_{11} = k_6, \ldots, k_{16} = k_1$$

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.)

Temos que explorar a vulnerabilidade consequente da derivação de subchaves, visto que elas são espelhadas, tornando a decriptação o inverso da encriptação. Nesse caso, ao passar S para o oráculo, será devolvido S' que é o texto cifrado de S (que já é cifrado).

Portanto, basta pedir ao oráculo que criptografe m', que é o c, ou seja, cifrar o texto cifrado. Dessa forma, o oráculo retornará m, ou seja, a descriptografia de c.

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