**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. 03**  **Para 30/10/2023** |
| --- |

**Nome Completo:**

* Izabel Yale Neves Nascimento
* Jonas Ferreira Leal Junior

**Questões retiradas do livro-texto da disciplina.**

**1. Responda os questionamentos a seguir:**

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

Porque muitos algoritmos de encriptação de blocos simétricos atuais são baseados na estrutura da cifra de Feistel.

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

Uma cifra de fluxo encripta os dados em fluxo, ou seja, um bit ou byte por vez. Já a cifra de bloco encripta um bloco do texto claro por vez, o bloco é tratado como o todo e é cifrado com o mesmo tamanho de caracteres.

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

Não é prático por conta do tamanho da chave que para garantir segurança deve ser bem grande. Para uma cifra de bloco segura de n bits sua chave deve ser (n\*2^n). Então quanto maior o bloco maior deve ser a chave em proporção exponencial.

**(d) O que é uma cifra de produto?**

É a execução de duas ou mais cifras simples uma seguida da outra, assim o resultado do produto, ou seja, do texto cifrado, é mais forte.

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

Na difusão cada dígito do texto claro faz muita diferença no texto cifrado, então caso haja modificação em um caractere apenas do texto claro, o texto cifrado muda consideravelmente.

Já a confusão procura deixar o mais complexo possível o valor da chave de encriptação e o texto cifrado, assim dificultando a descoberta da chave.

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

* Tamanho do bloco;
* Tamanho da chave;
* Número de rodadas;
* Algoritmo de geração da subchave;
* Função F;

**(g) Explique o efeito avalanche.**

É uma propriedade que uma pequena mudança no texto claro ou na chave produz uma alteração significativa no texto cifrado. Esse efeito é uma característica do DES. 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.**

Como listado acima, o algoritmo de Feistel pede as três alternativas da questão para completar suas rodadas de encriptação.

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

(a) 57;

(b) 48;

(c) 32;

**(d) 64.**

Cada vez que o DES é processado sua entrada, o texto claro, tem como tamanho fixo 64 bits, um dos passos da encriptação é dividir esse texto em duas partes de 32 bits cada e trocá-las. Além disso, esse tamanho contribui para a segurança do algoritmo.

**4. A cifra de Feistel do algoritmo de encriptação utilizada no Data Encryption Standard (DES) utiliza quantos S-boxes? Explique.**

**(a) 8;**

Utiliza de 8 S-boxes e cada uma tem responsabilidade pelo processo de substituição dos bits utilizando da confusão e difusão.

(b) 7;

(c) 6;

(d) 5.

**5. O Data Encryption Standard possui uma chave de 56 bits, o que torna possível um espaço de 256 chaves possíveis. Essa sentença trata-se de ataque de. . . Explique.**

(a) Tempo;

(b) Matemático;

**(c) Força-Bruta;**

O ataque de força bruta torna-se praticamente impossível já que a possibilidade de quantidade de chaves utilizadas (2^56) é aproximadamente 7,2 x 10^16.

(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.**

**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*, . . . , k*16 = *k*1**

**Admita que você tenha um texto cifrado *S*. Explique como, com acesso a um oráculo de en criptação, 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 en criptação 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.)**

**Livro-texto da disciplina:**

**STALLINGS, William. Criptografia e segurança de redes. Princípios e práticas, Ed. 6. 2014.**