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: _____

Questões retiradas do livro-texto da disciplina.

1. Responda os questionamentos a seguir:
   (a) Por que é importante estudar a cifra de Feistel?
   (b) Qual é a diferença entre uma cifra de bloco e uma cifra de fluxo?
   (c) Por que não é prático usar uma cifra de substituição reversível qualquer do tipo mostrado na Tabela 3.1?
   (d) O que é uma cifra de produto?
   (e) Qual é a diferença entre difusão e confusão?
   (f) Que parâmetros e escolhas de projeto determinam o algoritmo real de uma cifra de Feistel?
   (g) Explique o efeito avalanche.
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.
3. Qual é o tamanho do texto claro no Data Encryption Standard (DES)? Explique.
   (a) 57;
   (b) 48;
   (c) 32;
   (d) 64.
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.

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.

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, $k_1, k_2, \ldots, k_8$, 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.)

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