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

1ª Verificação de Aprendizagem
Para 28/11/2023.

Nome Completo: _____

Questões retiradas do livro-texto da disciplina.

1. Para cada um dos seguintes recursos, determine um nível de impacto baixo, moderado ou alto à perda de confidencialidade, disponibilidade e integridade, respectivamente. Justifique suas respostas.
   (a) uma organização gerenciando informações públicas em seu servidor web.
   (b) uma organização de aplicação da lei gerindo informações de investigação extremamente sensíveis.
   (c) uma organização financeira gerindo informações administrativas rotineiras (sem informações relacionadas à privacidade).
   (d) um sistema de informação utilizado para grandes aquisições em uma organização voltada a contratações que contém dados sensíveis da fase de pré-solicitação e dados administrativos rotineiros. avalie o impacto de haver dois conjuntos de dados separadamente e o sistema de informação único.
   (e) uma indústria de energia contém um sistema SCada (controle supervisório e aquisição de dados, do acrônimo em inglês para *supervisory control and data acquisition*) controlando a distribuição da energia elétrica para uma grande instalação militar. o sistema SCada contém tanto sensores de dados em tempo real quanto informações das rotinas administrativas. avalie o impacto de haver dois conjuntos de dados separadamente e o sistema de informação único.

2. Responda, explique com exemplos, as questões abaixo:
   (a) Quais são os elementos essenciais de uma cifra simétrica? Explique-as.
   (b) Quais são as duas funções básicas usadas nos algoritmos de encriptação? Explique-as.
   (c) Quantas chaves são necessárias para duas pessoas se comunicarem por meio de uma cifra? Explique-as, demonstrando, você pode se utilizar de gráficos ou desenhos.
   (d) Quais são as duas técnicas gerais para atacar uma cifra? Explique-as.
   (e) Defina resumidamente a cifra de César; a cifra de Hill; a cifra de Feistel (por que é importante estudá-la?); e, a diferença entre DES, Rijndael e AES.

3. Quando o barco de patrulha norte-americano PT-109, sob o comando do tenente John f. Kennedy, foi afundado por um destróier japonês, uma mensagem foi recebida na estação sem fio australiana em código playfair:

   ```
   KXJEY UREBE ZWEHE WRYTU HEYFS
   KREHE GOYFI WTTTU OLKSY CAJPO
   BOTEI ZONTX BYBNT GONEY CUZWR
   GDSON SXBOU YWRHE BAAHY USEDQ
   ```

   a chave usada foi `royal new zealand navy`. decripte a mensagem. traduza TT para tt.

4. Crie uma aplicação que possa encriptar e decriptar usando uma cifra de Hill 2×2.

5. Responda, resumidamente, as questões a seguir:
   (a) Qual é a diferença entre uma cifra de bloco e uma cifra de fluxo?
   (b) O que é uma cifra de produto?
   (c) Qual é a diferença entre difusão e confusão? Explique.
   (d) Quais parâmetros e escolhas de projeto determinam o algoritmo real de uma cifra de Feistel?
   (e) Explique o efeito avalanche.

6. Encontre o inverso multiplicativo de cada elemento diferente de zero em Z_5

7. Para a aritmética de polinômios com coeficientes em Z_{10}, realize os seguintes cálculos:
   1. $(7x + 2) - (x^2 + 5)$
   2. $(6x^2 + x + 3) \times (5x^2 + 2)$

8. Use a chave `1010 0111 0011 1011` para encriptar o texto claro `"ok"`conforme expresso em ASCII, ou seja, `0110 1111 0110 1011`. Os projetistas do S-AES obtiveram o texto cifrado `0000 0111 0011 1000`. E você?

9. Compare AES com DES. Para cada um dos seguintes elementos do DES, indique o elemento comparável no AES ou explique por que ele não é necessário no AES.
   (a) XOR do material da subchave com a entrada da função f.
   (b) XOR da saída da função f com a metade esquerda do bloco.
   (c) função f.
   (d) permutação P.
   (e) troca de metades do bloco.

10. Calcule a saída da transformação **MixColumns** para a seguinte sequência de bytes de entrada `"67 89 AB CD"`. Aplique a transformação **InvMixColumns** ao resultado obtido para verificar seus cálculos. Altere o primeiro byte da entrada de `"67"`para `"77"`, realize a transformação **MixColumns** novamente para a nova entrada e determine quantos bits mudaram na saída.

    Nota: você pode realizar todos os cálculos à mão ou escrever um programa que dê suporte a eles. Se escolher escrever um programa, ele deverá ser feito inteiramente por você; nesta tarefa, não use bibliotecas ou código fonte de domínio público (você pode se guiar pelos exemplos Sage disponibilizados).

11. (2 pontos-extra) Crie um software que possa encriptar e decriptar usando S-AES. Dados de teste: um texto claro binário de `0110 1111 0110 1011` encriptado com uma chave binária de `1010 0111 0011 1011` deverá dar o texto cifrado binário `0000 0111 0011 1000`. A decriptação deverá funcionar da mesma forma.

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