Universidade Federal do Agreste de Pernambuco
Av. Bom Pastor s/n - Boa Vista
55292-270 Garanhuns/PE
☎ +55 (87) 3764-5500
m 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: Antonio Carlos de Oliveira Bezerra

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.

   R=

   Confidencialidade: Baixo impacto, pois as informações são públicas e não são sensíveis.

   Disponibilidade: Moderado impacto, pois a interrupção do servidor web pode afetar o acesso às informações públicas.

   Integridade: Baixo impacto, pois as informações públicas geralmente não são alteradas com frequência.

   (b) uma organização de aplicação da lei gerindo informações de investigação extremamente sensíveis.

   R=

   Confidencialidade: Alto impacto, pois a perda de confidencialidade dessas informações pode comprometer investigações.

   Disponibilidade: Moderado impacto, pois a falta de acesso temporário pode atrasar investigações, mas não comprometer gravemente.

   Integridade: Alto impacto, pois qualquer modificação não autorizada nas informações pode comprometer a validade das evidências.

   (c) uma organização financeira gerindo informações administrativas rotineiras (sem informações relacionadas à privacidade).

   R=

   Confidencialidade: Baixo impacto, pois as informações são rotineiras e não relacionadas à privacidade.

   Disponibilidade: Baixo impacto, pois a interrupção temporária pode ser gerenciada sem consequências graves.

Integridade: Baixo impacto, pois a modificação não autorizada dessas informações geralmente não teria grandes repercussões.

(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.

R=

Confidencialidade: Moderado a alto impacto, dependendo da sensibilidade dos dados na fase de pré-solicitação.

Disponibilidade: Moderado impacto, pois a interrupção temporária pode afetar o processo de aquisição.

Integridade: Moderado a alto impacto, dependendo da criticidade da integridade dos dados durante o processo de aquisição

(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 adminis- trativas. avalie o impacto de haver dois conjuntos de dados separadamente e o sistema de informação único.

R=

Confidencialidade: Moderado a alto impacto, dependendo da sensibilidade dos dados do SCada.

Disponibilidade: Alto impacto, pois a interrupção no controle de distribuição de energia pode ter consequências graves.

Integridade: Alto impacto, pois qualquer manipulação não autorizada dos dados do SCada pode comprometer a segurança da distribuição de energia

2. Responda, explique com exemplos, as questões abaixo:

(a) Quais são os elementos essenciais de uma cifra simétrica? Explique-as.

R=

Chave Secreta Compartilhada: Uma cifra simétrica utiliza a mesma chave para cifrar e decifrar a mensagem. Essa chave precisa ser mantida em segredo entre as partes autorizadas.

Algoritmo de Cifragem/Decifragem: Um conjunto de regras matemáticas ou procedimentos lógicos que determinam como a cifragem e a decifragem ocorrem.

(b) Quais são as duas funções básicas usadas nos algoritmos de encriptação? Explique-as.

R=

Substituição: Substituir elementos da mensagem por outros de acordo com um algoritmo ou tabela predefinida. Exemplo: cifra de César.

Transposição: Rearranjar a ordem dos elementos na mensagem. Exemplo: cifra de Hill.

(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.

R=

Se ambas as partes utilizam uma cifra simétrica, apenas uma chave é necessária para ambas cifrarem e decifrarem as mensagens. Esta chave deve ser compartilhada de forma segura entre as partes envolvidas.

(d) Quais são as duas técnicas gerais para atacar uma cifra? Explique-as.

R=

Ataque de Força Bruta: Tentativa sistemática de todas as chaves possíveis até encontrar a chave correta.

Criptoanálise: Análise das características do algoritmo e/ou da chave para encontrar fraquezas que possam ser exploradas para quebrar a cifra de forma mais eficiente do que um ataque de força bruta.

(e) Defina resumidamente a cifra de César; a cifra de Hill; a cifra de Feistel (por que é impor- tante estudá-la?); e, a diferença entre DES, Rijndael e AES.

R=

Cifra de César: Substituição simples onde cada letra na mensagem é deslocada por um número fixo de posições no alfabeto.

Cifra de Hill: Substituição poligráfica onde blocos de letras são transformados linearmente através de uma matriz chave.

Cifra de Feistel: Um tipo de estrutura de cifragem simétrica em que a mensagem é dividida em blocos e cada bloco passa por várias rondas de transformações.

Diferença entre DES, Rijndael e AES:

DES (Data Encryption Standard): Um antigo padrão de cifragem simétrica, com uma chave de 56 bits.

Rijndael: Um algoritmo de cifragem simétrica que suporta chaves de diferentes tamanhos (128, 192, ou 256 bits).

AES (Advanced Encryption Standard): O AES é baseado no Rijndael, mas foi escolhido como o padrão de cifragem simétrica pelo Instituto Nacional de Padrões e Tecnologia dos EUA (NIST). O AES suporta chaves de 128, 192 e 256 bits

3. Quando o barco de patrulha norte-americano PT-109, sob o comando do tenente John f. Ken- nedy, 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.

R=

R	**O**	**Y**	**A**	**L**
N	**E**	**W**	**Z**	**D**
V	**B**	**C**	**F**	**G**
H	**I/J**	**K**	**M**	**P**
Q	**S**	**T**	**U**	**X**

Aplicando uma substituição considerando a matriz temos: Linha x Coluna

KX JE YU RE BE ZW EH EW RY TU HE YF

PT BO AT ON EO WE NI NE LO ST IN AC

SK RE HE GO YF IW TX XT TU OL KS YC AJ PO

TI ON IN BL AC KE TT ST RA IT TW OM IL

BO TE IZ ON TX BY BN TG ON EY CU ZW RG

ES SW ME RE SU CO VE XC RE WO FT WE LV

DS ON SX BO UY WR HE BA AH YU SE DQ

EX RE QU ES TA NY IN FO RM AT IO NX

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

```
import numpy


#Esta função cria uma matriz 3x3
#a partir da chave fornecida, onde os elementos da matriz
#são os valores numéricos equivalentes às letras da chave.
def create_matrix_from(key):
    m=[[0] * 3 for i in range(3)]
    for i in range(3):
        for j in range(3):
            m[i][j] = ord(key[3*i+j]) % 65
    return m



# C = P*K mod 26
def encrypt(P, K):
    C=[0,0,0]
    C[0] = (K[0][0]*P[0] + K[1][0]*P[1] + K[2][0]*P[2]) % 26
    C[1] = (K[0][1]*P[0] + K[1][1]*P[1] + K[2][1]*P[2]) % 26
    C[2] = (K[0][2]*P[0] + K[1][2]*P[1] + K[2][2]*P[2]) % 26
    return C


#Esta função divide a mensagem em blocos de três letras e, em seguida,
criptografa cada bloco
def Hill(message, K):
    cipher_text = []
    #Transformando a mensagem em 3 caracteres por vez
```

```
    for i in range(0,len(message), 3):
        P=[0, 0, 0]
        #Atribua o valor inteiro correspondente a cada letra
        for j in range(3):
            P[j] = ord(message[i+j]) % 65
        #Criptografar três letras
        C = encrypt(P,K)
        #Adicione as 3 letras criptografadas ao texto cifrado final
        for j in range(3):
            cipher_text.append(chr(C[j] + 65))
        #Repita até que todos os conjuntos de três letras sejam
processados.

    #retornar uma string
    return "".join(cipher_text)

#Esta função calcula a matriz inversa de K em módulo 26 usando a inversa
multiplicativa modular.
def MatrixInverse(K):
    det = int(numpy.linalg.det(K))
    det_multiplicative_inverse = pow(det, -1, 26)
    K_inv = [[0] * 3 for i in range(3)]
    for i in range(3):
        for j in range(3):
            Dji = K
            Dji = numpy.delete(Dji, (j), axis=0)
            Dji = numpy.delete(Dji, (i), axis=1)
            det = Dji[0][0]*Dji[1][1] - Dji[0][1]*Dji[1][0]
            K_inv[i][j] = (det_multiplicative_inverse * pow(-1,i+j) *
```

```
det) % 26
    return K_inv



if __name__ == "__main__":

    message = "MYSECRETMESSAGE"
    key = "RRFVSVCCT"
    #Crie a matriz K que será usada como chave
    K = create_matrix_from(key)
    print(K)
    # C = P * K mod 26
    cipher_text = Hill(message, K)
    print ('Cipher text: ', cipher_text)



    # Decrypt
    # P = C * K^-1 mod 26
    K_inv = MatrixInverse(K)
    plain_text = Hill(cipher_text, K_inv)
    print ('Plain text: ', plain_text)


# K x K^-1 verificando se a matriz é igual à matriz identidade
    M = (numpy.dot(K,K_inv))
    for i in range(3):
        for j in range(3):
            M[i][j] = M[i][j] % 26
    print(M)
```

5. Responda, resumidamente, as questões a seguir:

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

   R=

   Cifra de Bloco: Opera em blocos fixos de dados, cifrando-os independentemente. Exemplo: DES, AES.

   Cifra de Fluxo: Ópera em bits ou pequenas unidades, cifrando de forma contínua. Exemplo: RC4.

   (b) O que é uma cifra de produto?

   R=

   É 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.

   (c) Qual é a diferença entre difusão e confusão? Explique.

   R=

   Na difusão, a estrutura estatística do texto claro é dissipada em estatísticas de longa duração do texto cifrado. A confusão 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.

   (d) Quais parâmetros e escolhas de projeto determinam o algoritmo real de uma cifra de Feistel?

   R=

   O tamanho de bloco, o tamanho de chave e o número de rodadas.

   (e) Explique o efeito avalanche.

   R=

   É uma pequena mudança no texto claro ou na chave produza uma alteração significativa no texto cifrado.

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

   R=

   $a \cdot b \equiv 1 \pmod{n}$

   a=1

   $1 \cdot 1 = 1 \pmod{5}$

   Inverso multiplicativo de 1 é 1.

a=2

$2 \cdot 3 = 1 \pmod 5$

Inverso multiplicativo de 2 é 3.

a=3

$3 \cdot 2 = 1 \pmod 5$

Inverso multiplicativo de 3 é 2.

a=4

$4 \cdot 4 = 1 \pmod 5$

Inverso multiplicativo de 4 é 4.

7. Para a aritmética de polinômios com coeficientes em Z_{10}, realize os seguintes cálculos: 1.

   1. $(7x + 2) - \left(x^2 + 5\right)$

      R= $7x + 2 - x^2 - 5 \Rightarrow -x^2 + 7x - 3$ **em** $\boldsymbol{Z_{10}}$

   2. $\left(6x^2 + x + 3\right)\left(5x^2 + 2\right)$

      R= $30x^4 + 12x^3 + 18x^2 + 5x^3 + 2x + 3 \Rightarrow 30x^4 + 17x^3 + 18x^2 + 2x + 3$

      $\Rightarrow 7x^3 + 8x^2 + 2x + 3$ **em** $\boldsymbol{Z_{10}}$

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?

   R=

Rodada 0 (Round 0):

Após a adição da chave da rodada (Add round key): 1100 1000 0101 0000

Rodada 1 (Round 1):

Após a substituição de nibbles (Substitute nibbles): 1100 0110 0001 1001

Após o deslocamento de linhas (Shift rows): 1100 1001 0001 0110

Após a mistura de colunas (Mix columns): 1110 1100 1010 0010

Após a adição da chave da rodada (Add round key): 1110 1100 1010 0010

Rodada 2 (Round 2):

Após a substituição de nibbles: 1111 0000 1000 0101

Após o deslocamento de linhas: 0111 0001 0110 1001

Após a adição da chave da rodada: 0000 0111 0011 1000

Portanto, o texto cifrado após duas rodadas é 0000 0111 0011 1000, que corresponde ao que os designers do S-AES obtiveram.

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.

   R=

   No DES, executamos XOR na subchave com a entrada da função ao longo de cada uma das 16 rodadas. Com o AES, seguimos o mesmo procedimento, realizando uma operação XOR entre a subchave e a entrada em cada uma das 10 rodadas antes de passar para a próxima

   (b) XOR da saída da função f com a metade esquerda do bloco.

   R=

   No DES, a permutação de expansão de 32 bits para 48 bits é seguida por uma operação XOR no lado esquerdo do bloco. Porém, como AES não é criptografia baseado na cifra de Feistel, a operação XOR não é realizada para o meio bloco esquerdo no AES. Com o AES, cada bit é tratado como um bloco separado.

   (c) função f.

   R=

   A função f corresponde à expansão, mistura, substituição e permutação do DES. AES não é uma cifra fixa, portanto a função é diferente.

   (d) permutação P.

   R=

   Enquanto o DES usa permutações inicial e final como parte integrante do processo, o AES emprega outras operações que não incluem uma permutação P específica, mas tem o shiftrows que trata de permutação entre bytes.

   (e) troca de metades do bloco.

   R=

   No DES, os blocos esquerdo e direito são trocados após cada rodada. O AES evita essa troca tratando todo o bloco de texto simples como uma única unidade e executando operações em todo o bloco de uma só vez.

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).

    R=

    Na operação mixcolumns, cada byte de uma coluna é gerado como um novo valor adicionando todos os quatro bytes dessa coluna, portanto para operação de colunas mistas teremos:

    Input = 67 89 AB CD

$$\text{Output} = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} 67 \\ 89 \\ AB \\ CD \end{bmatrix} = \begin{bmatrix} 67\cdot 2+89\cdot 3+AB+CD \\ 67+89\cdot 2+AB\cdot 3+CD \\ 67+89+AB\cdot 2+CD\cdot 3 \\ 67\cdot 3+89+AB+CD\cdot 2 \end{bmatrix} = \begin{bmatrix} CE+80+AB+CD \\ 67+09+E6+CD \\ 67+89+4D+4C \\ A9+89+AB+81 \end{bmatrix} = \begin{bmatrix} 28 \\ 45 \\ EF \\ 0A \end{bmatrix}$$

    Aplicando a transformação InvMixColumns ao resultado obtido:

$$\text{Input} = \begin{bmatrix} E & B & D & 9 \\ 9 & E & B & D \\ D & 9 & E & B \\ B & D & 9 & E \end{bmatrix} \begin{bmatrix} 28 \\ 45 \\ EF \\ 0A \end{bmatrix} = \begin{bmatrix} 28\cdot E+45\cdot B+EF\cdot D+0A\cdot 9 \\ 28\cdot 9+45\cdot E+EF\cdot B+0A\cdot D \\ 28\cdot D+45\cdot 9+EF\cdot E+0A\cdot B \\ 28\cdot B+45\cdot D+EF\cdot 9+0A\cdot E \end{bmatrix} = \begin{bmatrix} AB+D1+47+5A \\ 73+9B+13+72 \\ D3+5B+6D+4E \\ 23+54+D6+6C \end{bmatrix} = \begin{bmatrix} 67 \\ 89 \\ AB \\ CD \end{bmatrix}$$

    agora mudando o primeiro bit na entrada, teremos:

    Input = 77 89 AB CD

$$\text{Output} = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} 77 \\ 89 \\ AB \\ CD \end{bmatrix} = \begin{bmatrix} 77\cdot 2+89\cdot 3+AB+CD \\ 77+89\cdot 2+AB\cdot 3+CD \\ 77+89+AB\cdot 2+CD\cdot 3 \\ 77\cdot 3+89+AB+CD\cdot 2 \end{bmatrix} = \begin{bmatrix} EE+80+AB+CD \\ 77+89+E6+CD \\ 77+89+4D+4C \\ C7+89+AB+81 \end{bmatrix} = \begin{bmatrix} 08 \\ 55 \\ FF \\ 3A \end{bmatrix}$$

    O número de bits alterados na saída é 5.

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.