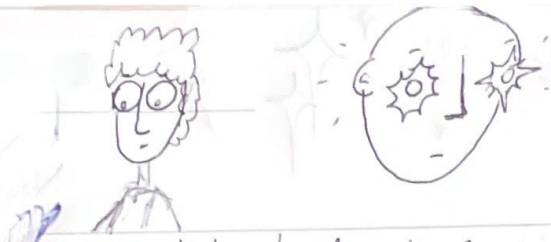

IDEA - International Data Encryption Algorithm
↳ Usa três operações: → XOR
→ Adição Módulo 2^{16}
→ Multiplicação módulo $2^{16}+1$

Lista 05.

1) Usando o S-DES, codifique a mensagem M = 0111.1001 utilizando a chave K = 10010.11101 manualmente.

1º. Geração das subchaves K_1 e K_2

K = 1 0 0 1 0 . 1 1 1 0 1
(1 2 3 4 5 6 7 8 9 10)

P10 = 0 0 0 1 1 1 0 1 0

P10 = {3, 5, 2, 7, 4, 10, 1, 9, 8, 6}

P8 = {6, 3, 7, 4, 8, 5, 10, 9}

Deslocamento Circular à Esquerda de cada Metade

L_{S_1} = 0 0 1 1 0 . 1 0 1 0 1 (1 2 3 4 5 6 7 8 9 10) ⇒ Passa por P8 e gera K_1

P8 ⇒ 1 1 0 1 1 0 1 0 → K_1 = 1 1 0 1 1 0 1 0

↳ Deslocamento Circular à Esquerda de Duas posições

L_{S_2} = 1 1 0 0 0 . 1 0 1 1 0 (1 2 3 4 5 6 7 8 9 10) ⇒ Passa por P8 e gera K_2

P8 ⇒ 1 0 0 0 1 0 0 1 ⇒ K_2 = 1 0 0 0 1 0 0 1

Encrypt ⇒ M ⇒ P ⇒ 0 1 1 1 1 0 0 1 (1 2 3 4 5 6 7 8)

↳ IP = 1 0 1 0 ; 1 1 1 0 (1 2 3 4 | 1 2 3 4)

L_0 R_0

IP = {2, 6, 3, 1, 4, 8, 5, 7}

IP^{-1} = {4, 1, 3, 5, 7, 2, 8, 6}

E/P = {4, 1, 2, 3, 2, 3, 4, 1}

P4 = {2, 4, 3, 1}

E/P(R_0) = 0 1 1 1 1 1 0 1

⊕ K_1 = 1 1 0 1 1 0 1 0

E/P(R_0) ⊕ K_1 = 1 0 1 0 ; 0 1 1 1

S_0 S_1

S_0 = 1 0 1 0

S_0 = [1 0] [0 1] = 10
(L_2 C_1)

S_1 = 0 1 1 1

S_1 = [0 1] [1 1] = 11
(L_1 C_3)

S_0S_1 = 1 0 1 1

P4(S_0S_1) = 0 1 1 1

Tabelas de Substituição:

S_0 =

	0	1	2	3
0	1	0	3	2
1	3	2	1	0
2	0	2	1	3
3	3	1	3	2

S_1 =

	0	1	2	3
0	0	1	2	3
1	2	0	1	3
2	3	0	1	0
3	2	1	0	3

$F_K = P4 \oplus L_0 \Rightarrow 0111 \oplus 1010 = 1101 = F_K = R_1$

$E/P(R_1) = 11101011$

$\oplus K_2 = 10001001$

01101010

$S_0 \quad S_1$

$S_0 = [00][11] = 10 \quad S_1 = [00][01] = 01 \Rightarrow S_0S_1 = 1001$

$P4(S_0S_1) = 0101$

$F_K = P4 \oplus L_1^{R_0} \Rightarrow 0101 \oplus 1110 = 1011$

CONCATENA

$F_K \cdot L_1^{R_1} \,|\, F_K R_1 = 10111101 \Rightarrow$ Passa no IP^{-1} = Mensagem Criptografada

$\Rightarrow IP^{-1} = 11110011$ Encrypt

2) Código

3) Utilize o DES para cifrar a mensagem M: BABBA23456789FDC(h) com a K: A012345DABC34567(h). Mostrar a saída após o 1º Round.

M = 1011.1010.1011.1011.1010.0010.0011.0100.0101.0110.0111.1000.1001.1111.1101.1100

K = 1010.0000.0001.0010.0011.0100.0101.1101.1010.1011.1100.0011.0100.0101.0110.0111

IP(M) = 0100.0111.0100.0011.0011.1111.0110.0011 | 1110.1000.0010.0000.1110.0110.1101.1011

L0 | R0

$E/P(R_0) = 11101010.0000.0010.0000.1110.1001.1001.1011.0110.1101.1011$

Gerar Subchave K1

↳ PC-1 (K)

↳ Dividir em C_0 e D_0 (28 bits cada) → Rotação à esquerda de 1 bit (1 round)

↳ PC-2 sobre $C_1|D_1 = K_1$ (48 bits)

PC-1(K) = 1111.0000.1010.1010.1010.1111.0000.00 ⇒ C0
1111.0000.1100.0000.0011.0011.0000.00 ⇒ D0

Rotação à Esquerda de C0 e D0 (1 bit pois 1º Round)

C0 = 1110.0001.0101.0101.0101.1111.0000.001

D0 = 1110.0001.1000.0000.0110.0110.0000.01

↳ PC-2 (C0||D0) = 0001.1011.0000.0010.1110.1111.1111.1100.0111.0000.0111.0010.1100.1101.0001.1010.0010.1101 = K1

↳ E/P(R0) ⊕ K1 = 1111.0001.0000.0000.1110.0001.0110.0101.1100.0110.1010.1001

↳ Dividir em 8 blocos de 6 bits → Aplicar cada bloco às 8-S-Boxes.

B1 B2 B3 B4 B5 B6 B7 B8

S-B1 ⇒ 111100 ⇒ [10][1110] = L2 e C14 = 5 → 0101

S-B2 ⇒ 010000 ⇒ [00][1000] = L0 e C8 = 9 → 1001

S-B3 ⇒ 000011 ⇒ [01][0001] = L1 e C1 = 7 → 0111

S-B4 ⇒ 100001 ⇒ [11][0000] = L3 e C0 = 3 → 0011

S-B5 ⇒ 011001 ⇒ [01][1100] = L1 e C12 = 3 → 0011

S-B6 ⇒ 011100 ⇒ [00][1110] = L0 e C14 = 5 → 0101

S-B7 ⇒ 011010 ⇒ [00][1101] = L0 e C13 = 10 → 1010

S-B8 ⇒ 101001 ⇒ [11][0100] = L3 e C4 = 4 → 0100

S-Box = 0101.1001.0111.0011.0011.0101.1010.0100

↳ Aplicar P(S-Box) = 1010.1101.1101.1001.0011.1010.0101.0011

R1 = L0 ⊕ f(R0,K1) → função de feistel → P(S-BOX

L0 = 0101.1001.0111.0011.0011.0101.1010.0100

f(R0,K1) = 1010.1101.1101.1001.0011.1010.0101.0011

R1 = 1111.0100.1010.1010.0000.1111.1111.0111

e L1 = R0

Final do 1º Round

AES - Advanced Encryption Standard → PADRÃO ATUAL
↳ Slide & Tídio no classroom

04. Utilize o IDEA para cifrar a mensagem M: BA12345DABC34567(h) com a K: BA12345DABC34567A012345DABC34567(h). Mostrar a saída após 1 round

X_1 BA12 47634
X_2 345D 13405
X_3 ABC3 43971
X_4 4567 17767
K: " "
Z_1 BA12 47634
Z_2 345D 13405
Z_3 ABC3 43971
Z_4 4567 17767
Z_5 A012 40978
Z_6 345D 13405

$X_1 \cdot Z_1 \bmod (2^{16}+1)$
$2^{16}+1 = 65537$
$47634 \cdot 47634 = 2265036356$
$2265036356 \bmod 65537 = X_1$
$X_1 = 52562$

$X_2 + Z_2 \bmod 2^{16}$
$13405 + 13405 = 26810$
$X_2 = 26810$

$X_3 + Z_3 \bmod 2^{16}$
$43971 + 43971 = 87942$
$X_3 = 87942 \bmod 2^{16} = 22406$

$X_4 + Z_4 \bmod (2^{16}+1)$
$17767 + 17767 = 315677089$

$x_4 = 315677089 \bmod (2^{16}+1) = 38291$

$P = x_1 \oplus x_3$

$Q = x_2 \oplus x_4$

$P = 40356$

$Q = 13227$

$P' = (P \cdot 25) \bmod (2^{16}+1)$

$Q' = (Q + P') \bmod 2^{16}$

$Q'' = (Q \cdot 25) \bmod (2^{16}+1)$

$P'' = (P' + Q'') \bmod 2^{16}$

$P' = P \cdot 25 \bmod 65537$

$P' = 22028$

$Q' = Q + P' \bmod 65536$

$Q' = 35257$

$Q'' = Q' \cdot 26 \bmod (2^{16}-1)$

$Q'' = 8843$

$P'' = P' + Q'' \bmod 2^{16}$

$P'' = 30871$

$X1 = X1 \oplus Q'' = 44165$

$X2 = X2 \oplus P'' = 5853$

$X3 = X3 \oplus Q'' = 31253$

$X4 = X4 \oplus P'' = 9228$

X1	44165	AC65
X2	5853	16DD
X3	31253	7ACD
X4	9228	240C

↳ AC6516DD7ACD240C

↳ 1° Round

05) Utilize o AES para cifrar a mensagem M: ~~EE23456789ABCDEFABD12345D~~ ~~ABC34567(H)~~ ERRADO! Ver slide com a K = CCD123456789FDC1F1234567894BCDEF(H).
Mostre a saída após o 1° round.

State 0 = $\begin{bmatrix} EE & 89 & AB & 67 \\ 23 & AB & 01 & 89 \\ 45 & CD & 23 & FD \\ 67 & GF & 45 & C1 \end{bmatrix}$

Matriz K0 = $\begin{bmatrix} CC & 67 & F1 & 89 \\ D1 & 89 & 23 & AB \\ 23 & FD & 45 & CD \\ 45 & C1 & 67 & EE \end{bmatrix}$

XOR - coluna por coluna:

$\begin{bmatrix} 22 & EE & 5A & EE \\ F2 & 22 & 28 & 22 \\ 66 & 30 & 66 & 30 \\ 22 & 26 & 22 & 26 \end{bmatrix}$

Aplica S-Box -> Vou resumir essa parte pois tenho muito amor a vida

22 -> Linha [2] Coluna [2] -> S-Box [2][2] = 93
F2 -> Linha [F] coluna [2] -> S-Box [F][2] = 07
EE -> 9A
5A -> D0
EE -> 9A
22 -> 93
22 -> 93
22 -> 93
66 -> A1
30 -> F5
66 -> A1

30 → F5
22 → 93
2E → DB
22 → 93
2E → 0B

↳ $\begin{bmatrix} 93 & 9A & DD & 9A \\ 07 & 93 & 93 & 93 \\ A1 & F5 & A1 & F5 \\ 93 & 0B & 93 & 0B \end{bmatrix}$

→ Shift Rows

Linha 0 → Sem shift ⇒ $\begin{bmatrix} 93 & 9A & DD & 9A \end{bmatrix}$
Linha 1 → Shift 1p ⇒ $\begin{bmatrix} 93 & 93 & 9A & 07 \end{bmatrix}$
Linha 2 → Shift 2p ⇒ $\begin{bmatrix} A1 & F5 & A1 & F5 \end{bmatrix}$
Linha 3 → Shift 3p ⇒ $\begin{bmatrix} 0B & 93 & 0B & 93 \end{bmatrix}$

→ Mix Columns → aplicar com GF(2^8) e Matriz AES:

L0 ⇒ $(2 \cdot 93) \oplus (3 \cdot 93) \oplus (1 \cdot A1) \oplus (1 \cdot 0B) = 0x39$
L1 ⇒ $(1 \cdot 93) \oplus (2 \cdot 93) \oplus (3 \cdot A1) \oplus (1 \cdot 0B) = 0x5D$
L2 ⇒ $(1 \cdot 93) \oplus (1 \cdot 93) \oplus (2 \cdot A1) \oplus (3 \cdot 0B) = 0x44$
L4 ⇒ $(3 \cdot 93) \oplus (1 \cdot 93) \oplus (1 \cdot A1) \oplus (2 \cdot 0B) = 0x8A$

Coluna 0: $\begin{bmatrix} 39 \\ 5D \\ 44 \\ 8A \end{bmatrix}$

$L1 = (1 \cdot 93) \oplus (2 \cdot 93) \oplus (3 \cdot 93) \oplus (1 \cdot 0B) = 0x5D$
$L2 = (1 \cdot 93) \oplus (1 \cdot 93) \oplus (2 \cdot A1) \oplus (3 \cdot 0B) = 0x44$
$L3 = (3 \cdot 93) \oplus (1 \cdot 93) \oplus (1 \cdot A1) \oplus (2 \cdot 0B) = 0x8A$

Nova Coluna 0 = $\begin{bmatrix} 39 \\ 5D \\ 44 \\ 8A \end{bmatrix}$

__/__/__

5) - NOVA COLUNA 1: $(2 \cdot 27) \oplus (3 \cdot CF) \oplus (1 \cdot 84) \oplus (1 \cdot A5) = 0x45$

$C1 = (1 \cdot 27) \oplus (2 \cdot CF) \oplus (3 \cdot 84) \oplus (1 \cdot A5) = 0x48$

$C2 = (1 \cdot 27) \oplus (1 \cdot CF) \oplus (2 \cdot 84) \oplus (3 \cdot A5) = 0x47$

$C3 = (3 \cdot 27) \oplus (1 \cdot CF) \oplus (1 \cdot 84) \oplus (2 \cdot A5) = 0x43$

NOVA COLUNA 1: $\begin{bmatrix} 45 \\ 48 \\ 47 \\ 43 \end{bmatrix}$

↳ Não aguento mais, então pulei os resultados das próximas colunas.

$\begin{bmatrix} 45 & 65 & B7 & 1B \\ 48 & 7C & 2C & A9 \\ F1 & 18 & 4C & 62 \\ F4 & 5F & 34 & E7 \end{bmatrix}$

↳ 45657B71B487C2CA9F1184C62F45F34E7

↳ final do 1º Round

6_ a) No AES, o XOR ocorre no início e a cada rodada com a subchave gerada

b) No AES não há divisão em metade, a função equivalente seria a operação XOR do resultado da etapa Mix Columns como State

c) A função f do DES combina expansão, S-Boxes e permutação. No AES, isso é feito pelas etapas: SubBytes (S-boxes), ShiftRows, MixColumns e AddRoundKey

e) Não trata de metade de blocos no AES, pois AES opera sobre uma matriz de 4x4 bytes (State) inteira, sem dividir em metades.

07.) Entrada: $\begin{bmatrix} 77 \\ 98 \\ BA \\ CD \end{bmatrix}$ Matriz AES - No SLIDE

↳ MixColumns:

$R0 = (02 \cdot 77) \oplus (03 \cdot 98) \oplus BA \oplus CD = E7$

$R1 = 77 \oplus (02 \cdot 98) \oplus (03 \cdot BA) \oplus CD = 96$

$R2 = 77 \oplus 98 \oplus (02 \cdot BA) \oplus (03 \cdot CD) = F4$

$R3 = (03 \cdot 77) \oplus 98 \oplus BA \oplus (02 \cdot CD) = F2$

- Primeiro byte de 77 para 78: $\begin{bmatrix} 78 \\ 98 \\ BA \\ CD \end{bmatrix}$

↳ MixColumns: E1 94 F6 F5

E7 96 F4 F2

⊕ E1 94 F6 F5

Nº de bits diferentes:

2 + 1 + 1 + 3 = 7

08) $B8_{(H)} = 1011\,1000 \Rightarrow x^7 + x^6 + x^5 + x^4 + x^3$

$74_{(H)} = 0111\,0100 \Rightarrow x^6 + x^5 + x^4 + x^2$

B8 · F4 = Pela tabela

= B8 · F4

= D3

09) (A) - A criptografia de chave simétrica pode manter os dados seguros, mas, se for necessário compartilhar informações confidenciais com outras pessoas, também se deve compartilhar a chave utilizada para criptografar os dados.