

Applied Cryptography

Open book assignment 2

Naman Chaudhary
PES200200209

Section: D

3. C/R Y/P T/O G/R A/P H/Y M/A T/H
02

C R Y P T O G R A P H Y M A T H
02 11 18 0F 13 0E 06 11 00 0F 07 18 0C 00 13 07

$$\text{State Matrix} = \begin{bmatrix} 02 & 13 & 00 & 0C \\ 11 & 0E & 0F & 00 \\ 18 & 06 & 07 & 13 \\ 0F & 11 & 18 & 07 \end{bmatrix}$$

Mix Column $[C_0]$:

$$C_0 = \begin{bmatrix} 02 \\ 11 \\ 18 \\ 0F \end{bmatrix} \Rightarrow \text{Mix Column} = \begin{bmatrix} 2 & 3 & 11 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \times \begin{bmatrix} 02 \\ 11 \\ 18 \\ 0F \end{bmatrix}$$

__/__/__

C R Y P T O G R A P H Y M A T H
41 52 59 50 54 4F 47 52 41 50 48 59 4D 41 54 48

$$= \begin{bmatrix} 43 & 54 & 41 & 4D \\ 52 & 4F & 50 & 41 \\ 59 & 47 & 48 & 54 \\ 50 & 52 & 59 & 48 \end{bmatrix}$$

Mix Column:

Shift Rows

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} 43 & 54 & 41 & 4D \\ 41 & 52 & 4F & 50 \\ 48 & 54 & 59 & 47 \\ 52 & 59 & 48 & 50 \end{bmatrix}$$

$$= \begin{bmatrix} 79 & 5C & 53 & 6E \\ 6C & 51 & 63 & 50 \\ 63 & 60 & 6A & 69 \\ 45 & 7B & 7C & 52 \end{bmatrix}$$

- _/_/_
1. Confusion: A cryptographic which is used to create faint cipher text. This technique is possible through substitution algorithm.

In confusion, vagueness is increased in resultant the relation between the cipher text and the key is masked by confusion:

Eg: Choc

Diffusion: To create cryptic plain text, Redundancy is increased in resultant. Only block ciphers use diffusion.

The relationship b/w the cipher text & the plain text is masked by diffusion

Eg: Shift Row/Shift Column.

2. AES: Advanced Encryption Standard, is a symmetric algorithm which uses a 128 bit plain text and secret key to produce a 128 bit block and a 16 BYTE CIPHERTEXT

DES: Data Encryption Standard, symmetric block cipher which uses 64 bit plaintext & 56 bit key to generate 64 BIT CIPHERTEXT

So, at the encrypted level

AES	has	-	16 BYTE CT
DES	has	-	64 BIT CT

AES → Byte level

DES → BIT level

4. S-Box gives five rows and 2 cols.

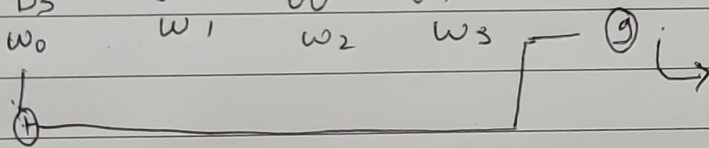
	0	1	2
0	63	7C	77
1	CA	82	C9
2	B7	FD	93
3	04	C7	23
4	09	83	2C
5	53	D1	00
	—	—	1

$$\therefore, A_i = (52)_{\text{HEX}}$$

$$B_i = S(A_i)_{\text{HEX}}$$

$$= S(52)_{\text{HEX}} = (00)_{\text{HEX}}$$

	B ₀	B ₁	B ₂	B ₃
5	13	AA	54	87
	AA	54	87	13
	AC	20	17	7D
	01	00	00	00
	w ₀	w ₁	w ₂	w ₃



AD 20 17 7D

$$\downarrow w_4$$

$$= AD \ 20 \ 17 \ 7D$$

$$\oplus \ 24 \ 75 \ A2 \ B3$$

$$w_4 = 89 \ 55 \ B5 \ CE$$

$$\oplus \ 34 \ 75 \ 56 \ 88$$

$$w_5 = BD \ 20 \ E3 \ 46$$

$$\oplus \ 31 \ E2 \ 12 \ 00$$

$$w_6 = 8C \ C2 \ F1 \ 46$$

$$\oplus \ 13 \ AA \ 54 \ 87$$

$$w_7 = 9F \ 68 \ A5 \ C1$$

6. Out of ECB & CBC, CBC mode should be chosen. ECB does not hide data pattern, unsuitable for long messages and is susceptible to replay attacks. In CBC, identical blocks do not have the same cipher and can be used to encrypt long messages.

7. ~~Cryptography~~
AES/DES in cipher feedback mode and output feedback mode can be used as stream ciphers. This is done because in CFB mode, it uses cipher block used in previous step as input of cipher in next step and a key stream is generated, thus the block cipher is used as stream cipher.

10.

Determine root of b^i in ecosystem of mod 8.

$$a = b^i \pmod{m}, m=8$$

$b =$	b^1	b^2	b^3	b^4	b^5	b^6	b^7
1	1	1	1	1	1	1	1
2	2	4	0	0	0	0	0
3	3	1	3	1	3	1	3
4	4	0	0	0	0	0	0
5	5	1	5	1	5	1	5
6	6	4	0	0	0	0	0
7	7	1	7	1	7	1	7

8 does not have any primitive root.