Computer Security

Section (1)

AES

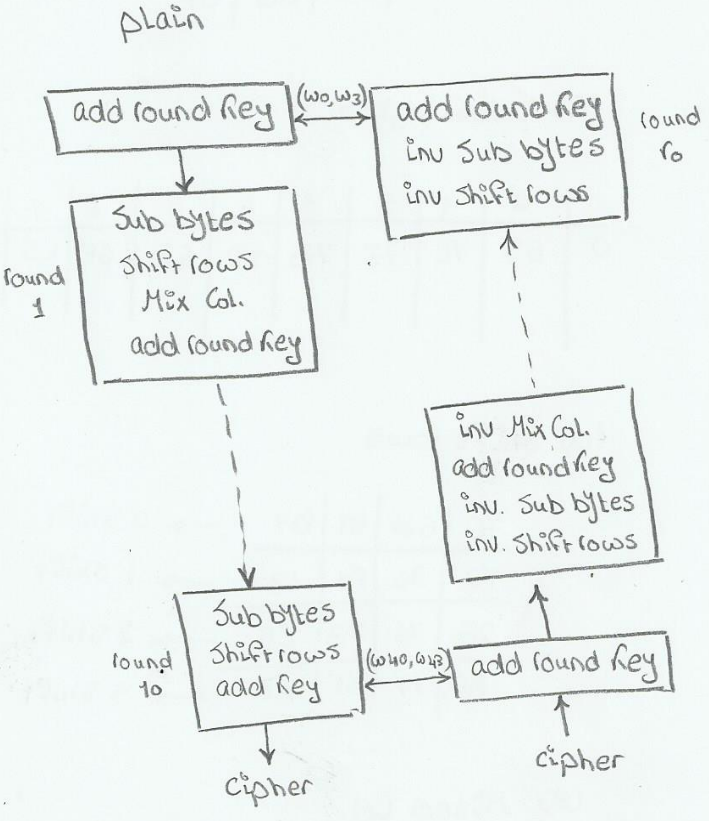
* key 128 bit

* block 128 bit = 16 byte = 4 words

plain

in0, in1, in2, in3, ---. in16
↓
byte0

State	in0	in4	in8	in12
	in1			
	in2			
	in3	in7	in11	in15
	word0	word1	word2	word3



Subs. byte

اشوف اول رقم hexa ⇐ لو مثلاً 1A
فبروح للمكان ف الجدول

horizontal → 1
vertical → A

و اشوف الـ value اللى موجودة
واحطها مكانهم

Shift left

بعمل circular shift left
كل row بيتعمله عدد shift مختلف.

$$\begin{matrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{matrix}$$

02 ⇒ 0000 0010 = x
03 ⇒ 0000 0011 = x+1

Mixed Col.

بيديني matrix اضربه ف الـ input
اللى عندى .. بس كله GF(2^8)

الـ inverse بتاعتها بيكون matrix

Sheet 4

3 plain text = {00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F}

Key = {01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01}

(a) State

00	04	08	0C
01	05	09	0D
02	06	0A	0E
03	07	0B	0F

(b) Add round key

⊕

01	01	01	01
01	01	01	01
01	01	01	01
01	01	01	01

=

01	05	09	0D
00	04	08	0C
03	07	0B	0F
02	06	0A	0E

(C) Subs. bytes

	0	1	2	3	4	5	6	7	8
0	63	7C	77	7B	F2	6B	6F	C5	30

⇒

7C	6B	01	D7
63	F2	30	FE
7B	C5	2B	76
77	6F	67	AB

(d) Shift rows

7C	6B	01	D7	→ 0 Shift
F2	30	FE	63	→ 1 Shift
2B	76	7B	C5	→ 2 Shift
AB	77	6F	67	→ 3 Shift

(e) Mixed Col.

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

*

7C	6B	01	D7
F2	30	FE	63
2B	76	7B	C5
AB	77	6F	67

=

75	87	0F	A2
55	E6	04	22
3E	2E	B8	8C
10	15	58	0A

$(7C * x) + (F2 * (x+1)) + (2B) + (AB)$

$7C * x \Rightarrow$ 1111 1000 ⇒ Shift left مرة واحدة

$F2 \Rightarrow$ 1111 0010

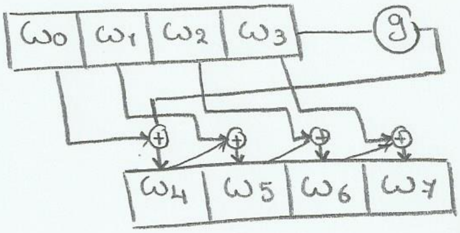
$F2 * x \Rightarrow$ 1110 0100

0001 1011

0000 1101 ⇒ F2(x+1)

```
1111  1000 → 7C*x
0000  1101 → F2*(x+1)
0010  1011 → 2B
1010  1011 → AB
---------------
0111 0101 → 75
```

Key generation



$w_4 = g \oplus w_0$

$w_5 = w_4 \oplus w_1$

$w_6 = w_5 \oplus w_2$

$w_7 = w_6 \oplus w_3$

(g) ⇒ Complex function :

1 1byte Circular Shift Left

b0 b1 b2 b3

b1 b2 b3 b0

2 Sub bytes

3 XOR with Round Const 01 / 00 / 00 / 00

الـ round Constant بيكون byte واحد .. فبحطه و بكمل الباقي 0s

2 $w_0 = w_1 = w_2 = w_3 = \{00\ 00\ 00\ 00\}$

∵ key = 0s

→ apply g on word 3 :

1- Shift left ⇒ 00 00 00 00

2- Sub. bytes ⇒ 63 63 63 63 $\oplus$

3- XOR with R.Const ⇒ $\boxed{01}$ 00 00 00

62 63 63 63

Round Const = 01

$w_4 = g(w_3) \oplus w_0$

$= (62\ 63\ 63\ 63) \oplus (00\ 00\ 00\ 00)$

$= (62\ 63\ 63\ 63)$

$w_4 = w_5 = w_6 = w_7$

6 Given word0 = (67 89 AB CD)

Apply Mix Col.

then inv. Mix Col.

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 02 & 03 & 01 \\ 03 & 01 & 01 & 02 \end{pmatrix} * \begin{pmatrix} 67 \\ 89 \\ AB \\ BC \end{pmatrix} = \begin{pmatrix} 28 \\ 45 \\ EF \\ 0A \end{pmatrix}$$

$$\begin{pmatrix} E & B & D & 9 \\ 9 & E & B & D \\ D & 9 & E & B \\ B & D & 9 & E \end{pmatrix} * \begin{pmatrix} 28 \\ 45 \\ EF \\ 0A \end{pmatrix}$$

$$(28 * E) \oplus (45 * B) \oplus (EF * D) \oplus (0A * 9)$$

$$x^3+x^2+x \qquad x^3+x+1 \qquad x^3+x^2+1 \qquad x^3+1$$

$$1010\ 1011 \oplus 1101\ 0001 \oplus 0100\ 0111 \oplus 0101\ 1010 = 67$$