

I love Sookmyung 16 Byte Plaintext
 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

key: 1713523171352317 16 Byte Key

$$\begin{array}{r} 16 \\ \times 8 \\ \hline 128 \end{array} \quad 16\text{Byte} = 128 \text{ bits}$$

① Add Round Key

8	4	2	1
₍₂₎			

A:10	D:13
B:11	E:14
C:12	F:15

같으면 0 다르면 1

I		l	o	v	e		S	o	o	k	m	y	u	n	g
49	20	6C	6F	76	65	20	53	6F	6F	6B	6D	79	75	6E	67

XOR

31	37	31	33	35	32	33	31	37	31	33	35	32	33	31	37
1	7	1	3	5	2	3	1	7	1	3	5	2	3	1	7

11

78	17	5D	5C	43	57	13	62	58	5E	58	58	4B	46	5F	50
x	ETB	J	W	C	W	DC3	b	X	^	X	X	K	F	-	P

② Substitute Bytes

BC	F0	4C	4A	1A	5B	7D	AA	6A	58	6A	6A	B3	5A	CF	53
		L	J	SUB	C	3		j	X	j	j		Z		S

③ Shift Rows

BC	FO	4C	4A
1A	5B	7D	AA
6A	58	6A	6A
B3	5A	CF	53

 \Rightarrow

BC	FO	4C	4A
5B	7D	AA	1A
6A	6A	6A	58
53	B3	5A	CF

BC	FO	4C	4A	5B	7D	AA	1A	6A	6A	6A	58	53	B3	5A	CF
	L	J	C	Y		SUB	j	j	j	X	S		Z		

④ Mix Column

$$x^8 + x^4 + x^3 + x + 1 \quad \begin{matrix} 7 & 6 & 5 & 4 \\ \begin{array}{|c|c|c|c|} \hline 8 & 4 & 2 & 1 \\ \hline 3 & 2 & 1 & 0 \\ \hline \end{array} & (2) \end{matrix}$$

A:10 D:13
B:11 E:14
C:12 F:15

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} BC & FO & 4C & 4A \\ 5B & 7D & AA & 1A \\ 6A & 6A & 6A & 58 \\ 53 & B3 & 5A & CF \end{pmatrix} = \begin{pmatrix} u_0 & u_1 & u_2 & u_3 \\ u_4 & u_5 & u_6 & u_7 \\ u_8 & u_9 & u_{10} & u_{11} \\ u_{12} & u_{13} & u_{14} & u_{15} \end{pmatrix}$$

$$\begin{aligned}
 u_0 &= x((x^7 + x^5 + x^4 + x^3 + x^2) + (x+1)(x^6 + x^4 + x^3 + x + 1)) \\
 &\quad + (x^6 + x^5 + x^3 + x) + (x^6 + x^4 + x + 1) \\
 &= x^8 + x^6 + x^5 + x^4 + x^3 + x^6 + x^4 + x^3 + x + x^7 + x^5 + x^4 + x^2 + x \\
 &\quad + x^5 + x^4 + x^3 + x \\
 &= x^8 + x^7 + x^5 + x^3 + x^2 \\
 &= x^9 + x^5 + x^4 + x^2 + x + 1 \rightarrow B7
 \end{aligned}$$

$$\begin{aligned}
 u_1 &\Rightarrow 1(7+6+5+4) + (1+0)(6+5+4+3+2+0) + (6+5+3+1) \\
 &\quad + (1+5+4+1+0) \\
 &= 8+5+6+5+4+3+2+0 + 7+6+5+4+3+1 + 3+4+0 \\
 &= 8+7+5+4+3+2+1 \\
 &= 7+5+2+0 \rightarrow A5
 \end{aligned}$$

$$x^8 + x^4 + x^3 + x + 1$$

7	6	5	4
8	4	2	1
3	2	1	0

A:10 D:13

B:11 E:14

C:12 F:15

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} BC & FO & 4C & 4A \\ 5B & 7D & AA & 1A \\ 6A & 6A & 6A & 58 \\ 53 & B3 & 5A & CF \end{pmatrix} = \begin{pmatrix} u_0 & u_1 & u_2 & u_3 \\ u_4 & u_5 & u_6 & u_7 \\ u_8 & u_9 & u_{10} & u_{11} \\ u_{12} & u_{13} & u_{14} & u_{15} \end{pmatrix}$$

$$\begin{aligned} u_2 &\Rightarrow 1(6+3+2) + (1+0)(7+5+3+1) + (6+5+3+1) + (6+4+3+1) \\ &= 17+3+7+5+3+1+8+6+4+2+5 \\ &= 8+6+4+2+1 = 6+3+2+0 \rightarrow 4D \end{aligned}$$

$$\begin{aligned} u_3 &\Rightarrow 1(6+3+1) + (1+0)(4+3+1) + (6+4+3) + (7+6+3+2+1+0) \\ &= 4+3+1+5+4+2+1+0 = 5+3+2+0 \rightarrow 2D \end{aligned}$$

$$\begin{aligned} u_4 &\Rightarrow (1+5+4+3+2) + 1(6+4+3+1+0) + (1+0)(6+5+3+1) + (6+4+1+0) \\ &= 3+6+5+3+1+7+6+4+2+6+4+0 \\ &= 7+6+5+2+1+0 \rightarrow E7 \end{aligned}$$

$$\begin{aligned} u_5 &\Rightarrow (1+6+5+4) + 1(6+5+4+3+2+0) + (1+0)(6+5+3+1) + (7+5+4+1+0) \\ &= 3+6+5+3+1+7+6+4+2+7+5+4+0 \\ &= 2+1+0 \rightarrow 07 \end{aligned}$$

$$\begin{aligned} u_6 &\Rightarrow (6+3+2) + 1(7+5+3+1) + (1+0)(6+5+3+1) + (6+4+3+1) \\ &= 8+6+5+3+1+7+6+4+2+6+1 \\ &= 8+7+6+5+4+3+2 \\ &= 7+6+5+2+1+0 \rightarrow E7 \end{aligned}$$

$$\begin{aligned} u_7 &\Rightarrow (6+3+1) + 1(4+3+1) + (1+0)(6+4+3) + (7+6+3+2+1+0) \\ &= 5+4+6+4+3+7+5+4+7+0 \\ &= 6+4+3+0 \rightarrow 59 \end{aligned}$$

$$U_8 \Rightarrow (1+5+4+3+2) + (6+4+3+1+0) + 1(6+5+3+1) + (1+0)(6+4+1+0)$$

$$= 5+4+1+0+6+4+1+0+7+5+2+1$$

$$= 17+6+2+1 \rightarrow C6$$

$$U_{12} \Rightarrow (0+1)(1+5+4+3+2) + (6+4+3+1+0) + (6+5+3+1) + 1(6+4+1+0)$$

$$= 8+6+5+4+3+1+5+4+3+2+4+1+0+1+2$$

$$= 8+6+4+1+0 = 6+3 \rightarrow 48$$

$$U_9 \Rightarrow (1+6+5+4) + (6+5+4+3+2+0) + 1(6+5+3+1) + (1+0)(1+5+4+1+0)$$

$$= 6+4+3+0+7+5+4+1+0+8+6+5+2+1$$

$$= 8+7+3+2 = 7+4+2+1+0 \rightarrow 97$$

$$U_{13} \Rightarrow (0+1)(1+6+5+4) + (6+5+4+3+2+0) + (6+5+3+1) + 1(7+5+4+1+0)$$

$$= 6+5+4+0+1+6+5+1+6+5+4$$

$$= 6+5+0 \rightarrow 61$$

$$U_{10} \Rightarrow 6+3+2+7+5+3+1+7+6+4+2+6+3+1+7+5+4+2$$

$$= 1+6+4+3+2 \rightarrow DC$$

$$U_{14} \Rightarrow 6+3+2+7+4+3+1+7+5+3+1+6+5+3+1+7+5+4+2$$

$$= 7+5 \rightarrow AO$$

$$U_{11} \Rightarrow 6+3+1+4+3+1+7+5+4+7+6+3+2+1+0+8+7+4+3+2+1$$

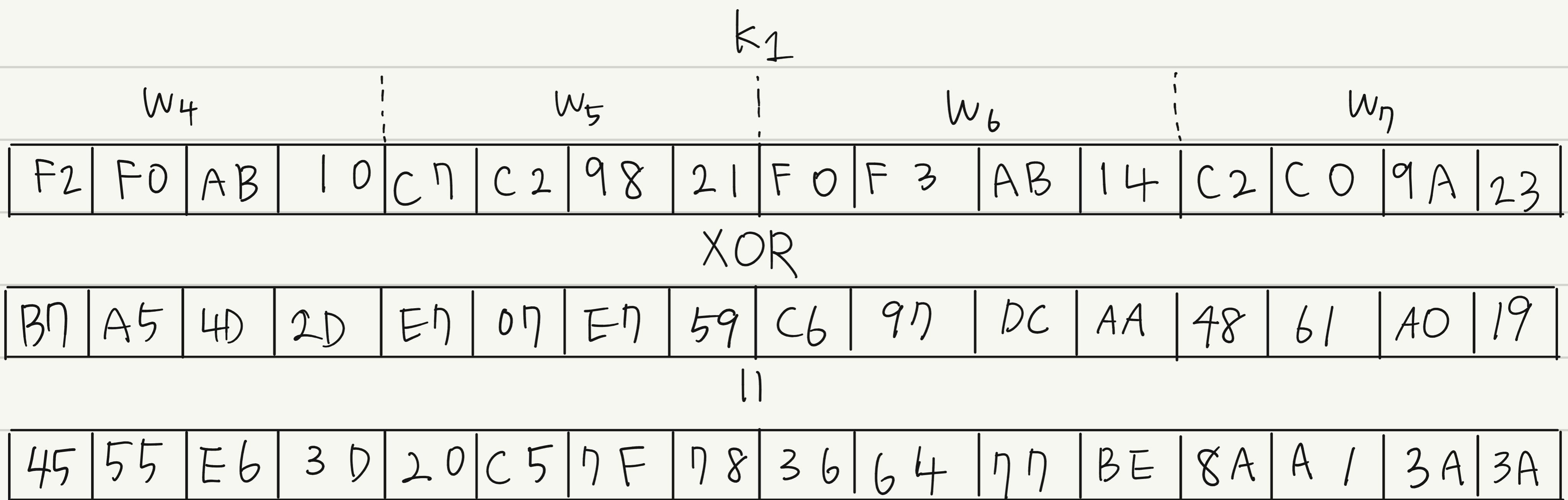
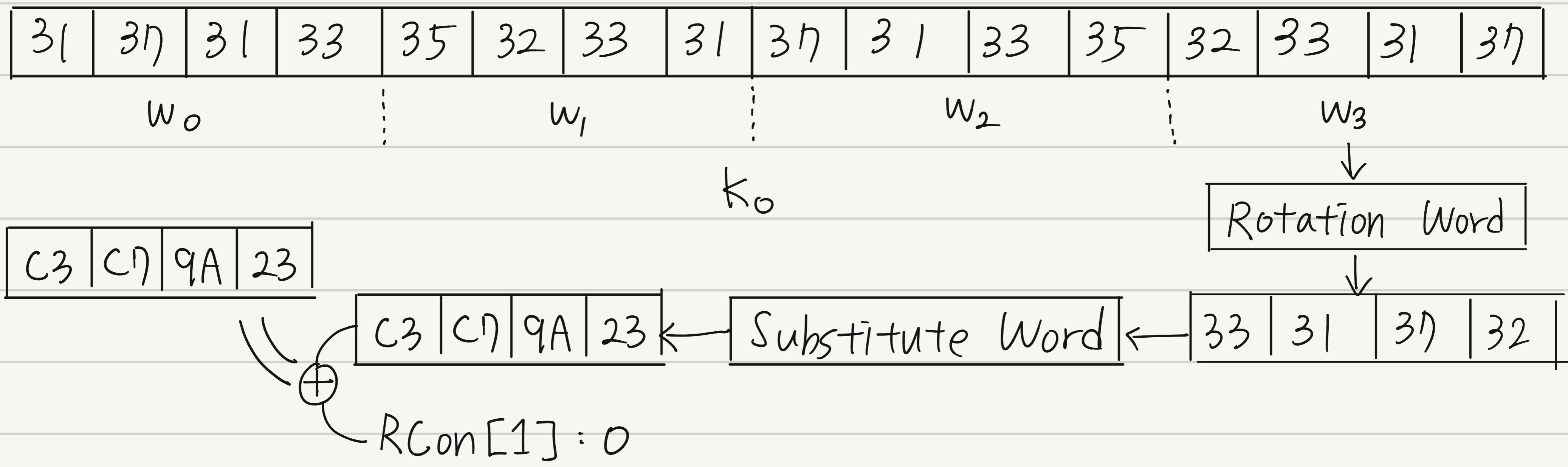
$$= 8+7+5+4+0 = 7+5+3+1 \rightarrow AA$$

$$U_{15} \Rightarrow 6+3+1+7+4+2+4+3+1+6+4+3+8+7+4+3+2+1$$

$$= 8+1 = 4+3+0 \rightarrow 19$$

B7	A5	4D	2D	E7	07	E7	59	C6	97	DC	AA	48	61	AO	19
----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----

⑤ KEY Expansion And Add Round Key.



$\begin{bmatrix} 8 & 4 & 2 & 1 \end{bmatrix}$

A:10 C:12 E:14

B:11 D:13 F:15