1. (a) Addition Table for $GF(7)$

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

(b) Multiplication Table for $GF(7)$

$\times$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

(c) Additive Inverses of $GF(7)$

$$-0 = 0$$
$$-1 = 6$$
$$-2 = 5$$
$$-3 = 4$$
$$-4 = 3$$
$$-5 = 2$$
$$-6 = 1$$

(d) Multiplicative Inverses of $GF(7)$

$-0 = \text{DNE}$
$-1 = 1$
$-2 = 4$
$-3 = 5$
$-4 = 2$
$-5 = 3$
$-6 = 6$

2. (a) Addition Table for $GF(2^2)$

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$+$	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

(b) Multiplicative Table for $GF(2^2)$

$\times$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	x^2	x^2+x
$x+1$	0	$x+1$	x^2+x	x^2+2x+1

$\times$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

$\times$	00	01	10	11
00	00	00	00	00
01	00	01	10	11
10	00	10	11	01
11	00	11	01	10

(c) Additive Inverses of $GF(2^2)$

$$\begin{aligned} -0 &= 0 \\ -1 &= 1 \\ -x &= x \\ -(x+1) &= x+1 \end{aligned}$$

(d) Multiplicative Inverses of $GF(2^2)$

$$\begin{aligned} -0 &= \text{DNE} \\ -1 &= 1 \\ -x &= \text{DNE} \\ -(x+1) &= x \end{aligned}$$

3. (a) 00000000 00000000 00000000 00000000
   (b) 63636363 63636363 63636363 63636363
   (c) 63636363 63636363 63636363 63636363
   (d) 63

4. (a) k_1 = e8e9e9e9 17161616 e8e9e9e9 17161616
   (b) k_2 = adaeae19 bab8b80f 525151e6 454747f0

(3) (a) result of initial key addition using k_0

all f key XOR w/ all f input $\Rightarrow$ all 0

(b) all bytes after key addition are 00

let $x=0$, $y=0$, using AES S-Box Table

gives Byte Substitution Layer of 63....63

(c) since Byte Substitution Layer is all 63,

the ShiftRows transformation is all 63.

(d) $C_0 = 02 \times B_0 + 03 \times B_5 + 01 \times B_{10} + 01 \times B_{15}$

$= 02 \times 63 + 03 \times 63 + 01 \times 63 + 01 \times 63$

$= 10 \times 01100011 + 11 \times 01100011 + 01 \times 01100011 + 01 \times 01100011$

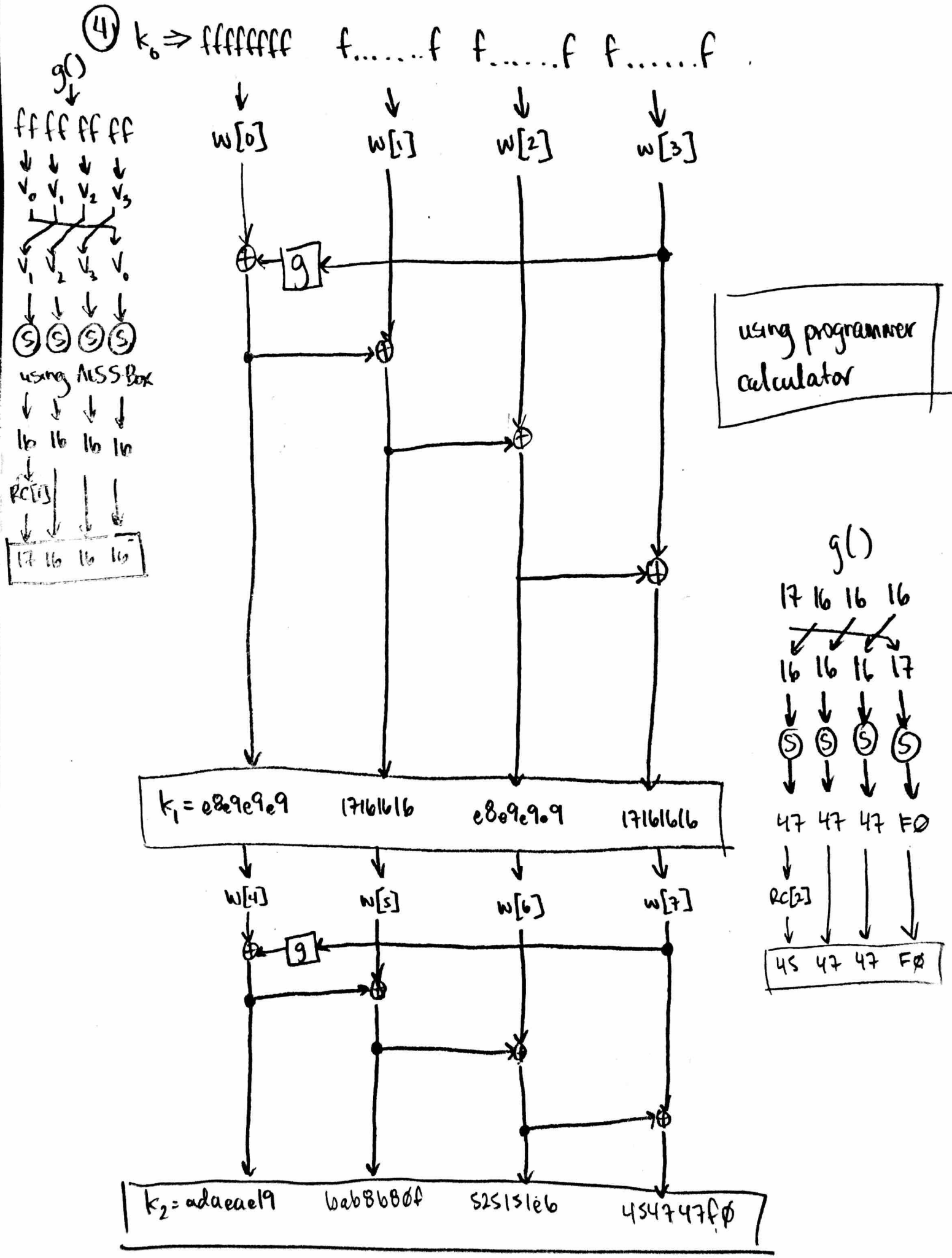
$= x(x^6+x^5+x+1) + (x+1)(x^6+x^5+x+1) + (x^6+x^5+x+1) + (x^6+x^5+x+1)$

$= x^7+x^6+x^2+x + x^7+x^6+x^2+x + x^6+x^5+x+1$

$= x^6+x^5+x+1$

$= 01100011$

$C_0 = 63$


④
$k_0 \Rightarrow$ ffffffff f.....f f.....f f.....f
g()
ff ff ff ff
v_0 v_1 v_2 v_3
v_1 v_2 v_3 v_0
S S S S
using AES S-Box
16 16 16 16
RC[i]
17 16 16 16
w[0] w[1] w[2] w[3]
g
using programmer calculator
k_1 = e8e9e9e9 17161616 e8e9e9e9 17161616
w[4] w[5] w[6] w[7]
g
k_2 = adaeae19 bab86808 52515le6 45474 7f0
g()
17 16 16 16
16 16 16 17
S S S S
47 47 47 F0
RC[2]
45 47 47 F0