Smc 3, ff 1-2

Smc 3) i) $O \sim 14$ $K \sim 10$

$G \sim 6$ $E \sim 4$

$$P = a'C + b' \pmod{26}$$

$$14 \equiv 6a' + b' \pmod{26}$$

$$10 \equiv 4a' + b' \pmod{26}$$

$$4 \equiv 2a' \pmod{26}$$

$$a' = 15$$

$$10 \equiv 4(15) + b' \pmod{26}$$

$$b' \equiv (10 - 4(15)) \pmod{26} = 2$$

$$(a', b') = (15, 2)$$

ii) $a' = 15$ $b' = 2$

CT	$P = a'C + b' \pmod{26}$	PT
N	$15(13) + 2 \pmod{26} = 15$	P
G	$15(6) + 2 \pmod{26} = 14$	O
I	$15(8) + 2 \pmod{26} = 18$	S
P	$15(15) + 2 \pmod{26} = 19$	T
N	15	P
G	14	O
Z	$15(25) + 2 \pmod{26} = 13$	N
O	$15(14) + 2 \pmod{26} = 4$	E
Y	$15(24) + 2 \pmod{26} = 24$	Y
G	14	O

W	$15(22)+2 \pmod{26} = 20$	U
B	$15(1)+2 \pmod{26} = 17$	R
D	$15(3)+2 \pmod{26} = 21$	V
Q	$15(16)+2 \pmod{26} = 8$	I
I	18	S
Q	8	I
P	19	T
G	$15(6)+2 \pmod{26} = 14$	O
E	$15(4)+2 \pmod{26} = 10$	K

iii) $C \equiv aP + b \pmod{26}$

$6 \equiv 14a + b \pmod{26}$

$4 \equiv 10a + b \pmod{26}$

$2 \equiv 4a \pmod{26} \Rightarrow 1 \equiv 2a \pmod{13}$ $\qquad 2^{-1} = 7$

$a = 7$ $\qquad \underline{13} = \underline{2} \cdot 6 + \underline{1}$

$4 \equiv 10 \cdot 7 + b \pmod{26}$ $\qquad 1 = \underline{13} - 6 \cdot \underset{\downarrow 7}{\underline{2}}$

$b \equiv 4 - 70 \pmod{26} = 12$

$(a, b) = (7, 12)$

PT	$C \equiv aP + b \pmod{26}$	CT
C	$7(2)+12 \pmod{26} = 0$	A
O	$7(14)+12 \pmod{26} = 6$	G
M	$7(12)+12 \pmod{26} = 18$	S
E	$7(4)+12 \pmod{26} = 14$	O
S	$7(18)+12 \pmod{26} = 8$	I

O	6	G
O	6	G
N	$7(13)+12 \pmod{26} = 25$	Z
O	6	G
K	$7(10)+12 \pmod{26} = 4$	E

CT: AGSOIGGZGE

FF-1) i)

$i =$	1	2	3	4	5	6	7	8	9	10	11	12
$2^i =$	2	4	8	3	6	12	11	9	5	10	7	1

ii)

$i =$	1	2	3	4	5	6	7	8	9	10	11	12
$b = 2^i =$	2	4	8	3	6	12	11	9	5	10	7	1
$r =$	12	6	4	3	12	2	12	3	4	6	12	1

$(b)^r \pmod{13} = 1 \quad (2^2)^6 \quad (2^3)^4 \quad (2^5)$

$\underline{13} = 6 \cdot 2 + \underline{1} \qquad 1 = 13 - 6 \cdot 2 \qquad r = 1$

iii) $(2^i)^r \pmod{13} = 1$

$(i \cdot r) \pmod{13} = 12$

iv) $3 \cdot 12 \pmod{13} = 10$

$\log_2(3) = 4$

$\log_2(12) = 1$

$\log_2(3 \cdot 12) = 6$

$9 \cdot 10 \pmod{13} = 12$

$\log_2(9) = 4$

$\log_2(10) = 6$

$\log_2(9 \cdot 10) = 1$

$11 \cdot 5 \pmod{13} = 3$

$\log_2(11) = 12$

$\log_2(5) = 12$

$\log_2(11 \cdot 5) = 4$

$$\log_2(a \cdot b) = \log_2(a \cdot b \pmod{13})$$

FF-2) i)

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
3^i	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

$g = 3$

ii) Smallest i of 3 that gives me 2 is 14.
Power r=1 of 2 gives 1. $(2^{12})^1 \pmod{13} = 1$