Cryptography hw8

0716074 蔡育宏

#1

(a) $Y_B = \alpha^{X_B} \bmod 8 = 5^{X_B} \bmod 23 = 10 \Rightarrow X_B = 3$ ※

(b) $Y_A = \alpha^{X_A} \bmod 8 = 8 \Rightarrow K = \alpha^{X_A X_B} \bmod 8 = 8^{X_B} \bmod 23 = 8^3 \bmod 23 = 6$ #

(c) $\mathbb{Z}_{23}^* = \{1,2,3,4,5,6,7,8,9,10,11,12,13,111,22\}$

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
$5^i \bmod 23$	5	2	10	4	20	8	17	16	11	9	22	18	21	13	19	3	15	6	7	12	14	1	5

$\{5^i \bmod 23 \mid i \in \mathbb{Z}, 1 \le i < 23\} = \mathbb{Z}_{23}^*$ ∴ 5 is primitive root of 23 #

#2 $C_1 = \alpha^k \bmod 8 = 5^3 \bmod 157 = 125$ $(k' = (Y_B)^k \bmod 8 = (10)^3 \bmod 157 = 58)$

$C_2 = MK' \bmod 8 = 9 \cdot 58 \bmod 157 = 51$

∴ cipher = (125, 51) #

#3 $7x^{10} + 1 \equiv 0 \pmod{23}$ $5^{22} \equiv 1 \pmod{23}$

∴

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
$7x^{10}+1$	1	8	16	11	20	18	6	0	22	12	21	15	15	21	12	22	0	6	18	20	11	16	8

$x^{10} \equiv 13 \bmod 23 \equiv 5^{14} \pmod{23}$

$\equiv 5^{14}(5^{22})^3 \equiv 5^{14}(5^{22})^8 \pmod{23}$

Double check

$\Rightarrow x \equiv 5^8 \equiv 16 \pmod{23}$ or $x \equiv 5^{19} \equiv 7 \pmod{23}$ #

#4

(a) $7G = 4G + 2G + G$

$= (5,4) + (10,4) + (3,2) = (6,8)$ ※

$\begin{cases} G = (3,2) \\ 2G = (10,4) \\ 4G = (5,4) \end{cases}$ $6G = (7,7)$ $7G = (6,8)$

*Addition $P(x_1,y_1) + Q(x_2,y_2)$

① if $P = Q$, $\lambda = \frac{3x_1^2 + a}{2y_1}$, $x_3 = \lambda^2 - x_1 - x_2$

$y_3 = \lambda(x_1 - x_3) - y_1$

② if $P \neq Q$, $\lambda = \frac{y_1 - y_2}{x_1 - x_2}$, $x_3 = \lambda^2 - x_1 - x_2$

$y_3 = \lambda(x_1 - x_3) - y_1$

* multiplication (n)

↳ addition for n times

(b) $C_m = \{kG, P_m + k \cdot P_B\}$

$k = 5$, $P_m = (10,7)$

$\begin{cases} H = (6,8) \\ 2H = (3,9) \\ 4H = (10,7) \\ 5H = (4,8) \end{cases}$

$(10,7) + \underbrace{5 \times (6,8)}_{(4,8)} = (1,8)$

∴ $C_m = \{(4,8), (1,8)\}$ ※

(c) $C_m = \{C_1, C_2\}$

⇒ B recieve C_m, which is encrypted from P_m

from A using P_A ⇒ $P_m = C_2 - n_A \cdot C_1 = P_m + k(n_A \cdot G) - n_A(kG) = P_m$ ※