HW3 #Writing problem.

1.

(A.) $P_0 = 0.4 = 0.5 - p$

$P_1 = 0.6 = 0.5 + p.$

Examine the bit stream as a sequence of non-overlapping pair.

Discard all 00 and 11 pairs. Replace each 01 pair with 0 and each 10 pair with 1.

(B) $P_{01} = 0.4 \times 0.6 = 0.24 = P_{10}.$

$E = 2X \times 0.24 = 0.12X$ #.

2.

(A). yes.

(B) yes.

3.

(A.) $d = e^{-1} \bmod \phi(n)$

$n = 11 \times 13$. $\phi(n) = 10 \times 12 = 120$

$d = 13^{-1} \bmod 120 = 37$

$M = C^d \bmod n = 60^{37} \bmod 143 = 101$ ✱

$37 \rightarrow 100101$

$0 = R = 1$ $X = 60$

$1 = R = 60$. $X = 3600 \bmod 143 = 25$

2: $X = 625 \bmod 143 = 53$

3: $R = 3180 \bmod 143 = 34$. $X = 2809 \bmod 143 = 92$

4: $X = 8464 \bmod 143 = 27$

5: $X = 729 \bmod 143 = 14$

6: $R = 476 \bmod 143 = 47$.

4. $Y_A = 6^{15} \bmod 143 = 71$ ※

15 → 1111

0: R=1. X=6

1: R=6. X=36

2: R=216 mod 131=85. X=1296 mod 131=117

3: R=9945 mod 131=120. X=13689 mod 131=65

4: R=7800 mod 131=71

$Y_B = 6^{27} \bmod 131 = 104$ ※

27 → 11011

0: R=1 X=6

1: R=6. X=36

2: R=216 mod 131=85. X=1296 mod 131=117

3: X=13689 mod 131=65

4: R=5525 mod 131=23. X=4225 mod 131=33

5: R=759 mod 131=104

shared secret key $= 71^{27} \bmod 131 = 104^{13} \bmod 131 = 71$ ※

15 → 1111

0: R=1. X=104

1: R=104. X=10816 mod 131=74

2: R=7696 mod 131=98. X=5476 mod 131=105.

3: R=10290 mod 131=72. X=11025 mod 131=21

4: R=1512 mod 131=71

5.

(A) $3^4 \bmod 131 = 81 \bmod 131 = 81$

$C_1 = 6^4 \bmod 131 = 1296 \bmod 131 = 117$

$C_2 = 81 \times 9 \bmod 131 = 729 \bmod 131 = 74$

Ciphertext C=(117. 74).

(B) $\begin{cases} 65 = k^{-1} M_1 \bmod 130 \\ 64 = k^{-1} M_2 \bmod 130. \end{cases}$

$\Rightarrow 65 \cdot k^{-1} M_2 \equiv 64 \cdot k^{-1} M_1 \pmod{130}.$

$\Rightarrow 65 M_2 \equiv 64 M_1 \pmod{130}$ ※

6.

(A)

x	$(x^3+3x+1) \bmod 7$	y
0	1	1.6
1	5	X
2	1	1.6
3	2	3.4
4	0	0
5	1	1.6
6	4	2.5

All points = (0.1). (0.6). (2.1). (2.6). (3.3). (3.4). (4.0). (5.1)

(5.6). (6.2). (6.5) ※

(B) $\lambda = \frac{3xp^2+a}{2yp} = \frac{3 \cdot 3^2+3}{2 \cdot 3} = 5$

$P_B = n_B \times G$

$= 4x(3,3)$

$= 2x(2x(3,3))$

$= 2x(5^2-3-3,\ 5(3-5)-3)$

$= 2x(5.1)$

$= (4^2-5-5,\ 4(5-6)-1) \Rightarrow \lambda = 4.$

$= (6.2)$ ※

(c) $Cm = \{kG,\ Pm + kP_B\}$

$= \{3(3,3),\ (2,1) + 3(6,2)\}$

$= \{2(3,3) + (3,3),\ (2,1) + [2(6,2) + (6,2)]\}$

$= \{(5,1) + (3,3),\ (2,1) + [(6,5) + (6,2)]\}$

$= \{(0,1),\ (2,1)\}$ ※

(d) $Cm = \{(5,1),\ (2,6)\}$

$k(3,3) = (5,1) \Rightarrow k = 2$

$Pm + 2(6,2) = (2,6)$

$Pm + (6,5) = (2,6)$

$Pm = (2,6) - (6,5)$

$= (2,6) + (6,2)$

$= ((-1)^2 - 2 - 6,\ (-1) \cdot 2 - 6)$

$= (0,6)$ ※