Problem 1 109550096 杜峯.

A. generate 0 : 0.4
generate 1 : 0.6.

At first we have a function - generator(), with output are "0" for probabilty 0.4 or "1" for probability 0.6.
For each time we call generator() for twice time.
The expected output has four types: "00". "01". "10". "11".
The probability of these four types are:

$$\begin{cases} 00 : (0.4)^2 = 0.16 \\ 01 : 0.4 \cdot 0.6 = 0.24 \\ 10 : 0.6 \cdot 0.4 = 0.24 \\ 11 : 0.6 \cdot 0.6 = 0.36 \end{cases}$$

Then, we define "01" as "0" and "10" as "1".
With other two types, we ignore them.
In other words, if the output is "00" or "11", we did nothing to them, but call the function - generator() for twice again until the output is either "01" or "10".
At before, we have defined "01" as "0" and "10" as "1".
And now, both "0" and "1" have the probability 0.24.
Because we only consider these two types with the same probability, we can say the probability of them appearing in sequence is the same for 0.5. #

B. If we want to generate a valid output bit, the input bits must be "01" or "10", and the total probability is $0.24 + 0.24 = 0.48$.
For any 2 bits, the probability that we can transform the input bits into a valid output bit is 0.48.
So, we calculate $2/0.48 = 4.1\bar{6}$.
$\Rightarrow$ the expected number : $4.1\bar{6}$ #

Problem 2. BBS, n=238589771, seed 7477, generate 1,000,000 bits.

A. In my program, there are total 488686 numbers of "1", and 511314 numbers of "0".

The ratios of "1" is 0.488686,

"0" is 0.511314.

Both of them are around 50%. #

B. In my program,

$$\text{the number} \Rightarrow \begin{cases} 00: 263119 \\ 01: 248195 \\ 10: 248195 \\ 11: 240490 \end{cases}$$

$$\text{the ratio} \Rightarrow \begin{cases} 00: 0.263119 \\ 01: 0.248195 \\ 10: 0.248195 \\ 11: 24049 \end{cases}$$

All of them are around 25%. #

Problem 3.

A. $n = 143 = 11 \times 13$.

Bob's public key : 13 , $C = 60$

$\phi(n) = 10 \times 12 = 120$

$d = e^{-1} \bmod \phi(n) = 13^{-1} \bmod 120 = 37$

Bob's private key : 37 #

$\Rightarrow C^{37} \bmod 143$, $C = 60 \Rightarrow 60^{37} \bmod 143$

$$
\begin{aligned}
60^{37} \bmod 143 &= (3600)^{18} \cdot 60 \bmod 143 \\
&= (25)^{18} \cdot 60 \bmod 143 \\
&= (625)^{9} \cdot 60 \bmod 143 \\
&= (53)^{9} \cdot 60 \bmod 143 \\
&= (2809)^{4} \cdot 53 \cdot 60 \bmod 143 \\
&= (92)^{4} \cdot 53 \cdot 60 \bmod 143 \\
&= (8464)^{2} \cdot 53 \cdot 60 \bmod 143 \\
&= (27)^{2} \cdot 53 \cdot 60 \bmod 143 \\
&= 47 \text{ \#.}
\end{aligned}
$$

B. $C = 60$, $n = 143$, Bob's PU $= 13$, Alice's key : 7 , $d = 103$.

$7 \times 103 - 1 = k\phi(n) \Rightarrow k\phi(n) = 720$

$d' = 13^{-1} \bmod 720 = 157$

$\because d' \equiv d \bmod \phi(n)$

$\therefore C^{d'} \bmod n = C^{d} \bmod n$

$$
\begin{aligned}
\Rightarrow 60^{157} \bmod 143 &= (3600)^{78} \cdot 60 \bmod 143 \\
&= (25)^{78} \cdot 60 \bmod 143 \\
&= (625)^{39} \cdot 60 \bmod 143 \\
&= (53)^{39} \cdot 60 \bmod 143 \\
&= (2809)^{19} \cdot 53 \cdot 60 \bmod 143 \\
&= (92)^{19} \cdot 53 \cdot 60 \bmod 143 \quad , \ 53 \cdot 60 \bmod 143 = 34 \\
&= (8464)^{9} \cdot 92 \cdot 34 \bmod 143 \quad , \ 92 \cdot 34 \bmod 143 = 125 \\
&= (27)^{9} \cdot 125 \bmod 143 \\
&= (729)^{4} \cdot 125 \cdot 27 \bmod 143 \quad , \ 125 \cdot 27 \bmod 143 = 86 \\
&= (14)^{4} \cdot 86 \bmod 143 \\
&= (196)^{2} \cdot 86 \bmod 143 \\
&= (53)^{2} \cdot 86 \bmod 143
\end{aligned}
$$

$= 2809 \cdot 86 \bmod 143$, $2809 \bmod 143 = 92$

$= 92 \cdot 86 \bmod 143 = 47$

Without factoring $n = 143$, we still can use another way to decrypt C, as long as they both use the same n. $\square$

Problem 4. Diffie-Hellman key exchange technique

prime $q = 131$, $\alpha = 6$

Alice : $X_A = 15$ $\Rightarrow$ Y_A?

Bob : $X_B = 27$ $\quad$ Y_B?

$$
\begin{aligned}
Y_A = 6^{15} \bmod 131 &= (216)^5 \bmod 131 \\
&= (85)^5 \bmod 131 \\
&= (7225)^2 \cdot 85 \bmod 131 \\
&= (20)^2 \cdot 85 \bmod 131 = 71
\end{aligned}
$$

$$
\begin{aligned}
Y_B = 6^{27} \bmod 131 &= (216)^9 \bmod 131 \\
&= (85)^9 \bmod 131 \\
&= (7225)^4 \cdot 85 \bmod 131 \\
&= (20)^4 \cdot 85 \bmod 131 \\
&= (400)^2 \cdot 85 \bmod 131 \\
&= (7)^2 \cdot 85 \bmod 131 = 104
\end{aligned}
$$

$$
\begin{aligned}
\text{Key} = Y_A^{X_B} \bmod q &= 71^{27} \bmod 131 \\
&= (5041)^{13} \cdot 71 \bmod 131 \\
&= (63)^{13} \cdot 71 \bmod 131 \\
&= (3969)^6 \cdot 63 \cdot 71 \bmod 131, \quad 63 \cdot 71 \bmod 131 = 19 \\
&= (39)^6 \cdot 19 \bmod 131 \\
&= (1521)^3 \cdot 19 \bmod 131 \\
&= (80)^3 \cdot 19 \bmod 131 \\
&= (6400) \cdot 80 \cdot 19 \bmod 131, \quad 80 \cdot 19 \bmod 131 = 79 \\
&= 112 \cdot 79 \bmod 131 = 71
\end{aligned}
$$

$Y_A = 71$, $Y_B = 104$, Shared secret key $= 71$ #

Problem 5 $q = 131,\ \alpha = 6,\ Y_B = 3$

A. $M = 9,\ k = 4$

$K = (Y_B)^k \bmod q = 3^4 \bmod 131 = 81 \bmod 131 = 81$

$C_1 = \alpha^k \bmod q = 6^4 \bmod 131 = 117$

$C_2 = KM \bmod q = 81 \cdot 9 \bmod 131 = 74$

The ciphertext : $C(117, 74)$ #

B. $k = 4$ M_1, M_2 encrypt $\Rightarrow (12, 65), (12, 64)$

In the two encryption, they have the same K and C_1.

Then, we have : $65 = M_1 K \bmod 131$

$64 = M_2 K \bmod 131$

Suppose, there exist two number $a, b, (a, b) \in R$.

Then, rewrite as :

$M_1 k = 131 \cdot a + 65$ ... I

$M_2 k = 131 \cdot b + 65$ ... II.

From I, we write it as $-65 = 131a - M_1 k$, which equal to

$-M_1 K = -65 \bmod 131 = 66$

Similarly to II, we can have

$-M_2 K = -64 \bmod 131 = 67$

So, we can have the relation :

$$\frac{-M_1 K}{-M_2 k} = \frac{66}{67} = \frac{M_1}{M_2} \Rightarrow \quad M_1 : M_2 = 66 : 67 \ \#.$$

Problem 6. $y^2=x^3+3x+1$ over Z_7, $G=(3,3)$, Bob's private key: $n_B=4$. $\to a=3, b=1$

A. For $x=0$ $y=1,6$

$x=2$ $y=1,6$

$x=3$ $y=3,4$

$x=4$ $y=0$

$x=5$ $y=1,6$

$x=6$ $y=2,5$

$\Rightarrow (0,1)(0,6)(2,1)(2,6)(3,3)(3,4)$

$(4,0)(5,1)(5,6)(6,2)(6,5)$ #

B. $P_B=n_B\cdot G=4\cdot(3,3)=2[2(3,3)]$

$$\alpha'=\frac{3x^2+a}{2y}=\frac{3\times3^2+3}{2\times3}=\frac{27+3}{2\times3}=\frac{30}{6}=5$$

$\Rightarrow x'=(5)^2-2\times3=25-6=19$ over $Z_7=5$

$y'=5\times(3-5)-3=5\cdot(-2)-3=-13$ over $Z_7=1$

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

$2(5,1)=4(3,3)$

$$\alpha''=\frac{3x^2+a}{2y}=\frac{3\times5^2+3}{2\times1}=\frac{75+3}{2}=\frac{78}{2}=39$$

$\Rightarrow x''=(39)^2-2\times5=1521-10=1511$ over $Z_7=6$

$y''=39\times(5-6)-1=-39-1=-40$ over $Z_7=2$

$\Rightarrow 2(5,1)=4(3,3)=(6,2)$

$P_B=(6,2)$ #

C. $P_m=(2,1)$, $k=3$, $C_m=?$

$C_m=(P_A=kG,\ P_m+kP_B)$

$P_A=kG=3\cdot(3,3)=2(3,3)+(3,3)$

From "B", we have already calculated $2(3,3)=(5,1)$.

What we need to do is calculating $(5,1)+(3,3)$

$\Delta=(3-1)/(3-5)=2/-2=-1$

$x' = \lambda^2 - x_1 - x_2 = (-1)^2 - 5 - 3 = 1 - 5 - 3 = -7$ over $Z_7 = 0$
$y' = -y_1 + \lambda(x_1 - x_3) = -1 + (-1)(5-0) = -1 - 5 = -6$ over $Z_7 = 1$

$\Rightarrow P_A = kG = 3(3,3) = (0,1)$

$P_m + kP_B = (2\ 1) + 3(6.2)$
$2(6,2)$
$\lambda = \frac{3\times 6^2 + 3}{2\times 2} = \frac{111}{4}$ over $Z_7 = 5$
$x' = (5^2) - 2\times 6 = 25 - 12 = 13$ over $Z_7 = 6$
$y' = 5\cdot(6-6) - 2 = -2$ over $Z_7 = 5$
$(6,5) + (6,2)$
$\because (6,5)$ and $(6,-2)$ are the same over Z_7
$\therefore (6,5) + (6,2) = 0$

$\Rightarrow P_m + kP_B = (2,1) + 0 = (2,1)$

$\Rightarrow C_m = ((0,1),(2,1))$

D. Decrypt $((5,1),(2,6))$ with private key $n_B = 4$
$P_m + kP_B - n_B P_A \Rightarrow (2,6) - 4(5,1) = P_m$.
Calculate, $4(5,1) = 2(2(5,1))$
From "B", we have already calculated $2(5,1) = (6,2)$.
And from "c" we have already calculated
$2(6,2) = (6,5)$
Then, we need to calculate $(2,6) - (6,5) = (2,6) + (6,-5)$
$= (2,6) + (6,2)$

$(2,6) + (6,2)$
$\lambda = -4/4 = -1$
$x = (-1)^2 - 2 - 6 = 1 - 8 = -7$ over $Z_7 = 0$
$y = -6 + (-1)\cdot(2) = -8$ over $Z_7 = 6$

$\Rightarrow$ the plaintext $= (0,6)$ #