1.

A. set a random number generator rd, if 0 is generated, then output it, if 1 is generated and rd % 3 == 1 or 2, output it, if rd % 3 == 0, discard the bit 1 #

B. $\frac{0.4+0.6\times\frac{2}{3}}{0.4+0.6} = \frac{4}{5} = \frac{1}{1.25} \Rightarrow 1.25$ #

2. A. Yes, there are 499695 zeroes and 500305 ones both of them are around 50% #

B. Yes, there are

248614	00s	both of them are around 25%
251080	01s	
251081	10s	
249224	11s	

#

3. A. ed mod $\phi(n) = 1 \Rightarrow 13d \bmod (10\times12) = 1 \Rightarrow$ private key = 37

120		1	0
13		0	1
3	9	1	-9
1	4	-4	37

$60^{37} \bmod 143 \Rightarrow$ group 11 and group 13

$c' = 60 \bmod 11 = 5$ $\quad c'' = 60 \bmod 13 = 8$

$d' = 37 \bmod 10 = 7$ $\quad d'' = 37 \bmod 12 = 1$

$m' = 5^7 \bmod 11 = 3$ $\quad m'' = 8$

$M = [3\times13\times(13^{-1} \bmod 11) + 8\times11\times(11^{-1} \bmod 13)] \bmod 143$

$= 47 \Rightarrow$ plaintext $= 47$ #

B. By def. of Alice's key : $M^7 \bmod 143 = C$, $C^{103} \bmod 143 = M$

$\Rightarrow (M^7)^{103} \bmod 143 = M^{721} \bmod 143 = M$

$\Rightarrow M^{720} \bmod 143 = 1$

and we have to solve $M^{13} \bmod 143 = 60$

$M^{720} \equiv (M^{13})^{55} \cdot M^5 \equiv 60^{55} \cdot M^5 \equiv 122 M^5 \equiv 1$

$\Rightarrow M^5 \equiv 122^{-1} \bmod 143 = 34$

$\Rightarrow M^{10} \bmod 143 = 12$

$\Rightarrow M^{13} \equiv M^{10} \cdot M^3 \equiv 12M^3 \equiv 60$

$\Rightarrow M^3 \bmod 143 = 5$

$\Rightarrow M^5 \equiv M^3 \cdot M^2 \equiv 5M^2 \equiv 34$

$\Rightarrow M^2 \equiv (5^{-1} \times 34) \bmod 143 = 64$

$\Rightarrow M^3 \equiv M^2 \cdot M \equiv 64M \bmod 143 = 5$

$\Rightarrow M = (64^{-1} \times 5) \bmod 143 \equiv 38 \times 5 \equiv 47$ #

4. $Y_A = \alpha^{X_A} \bmod q = 6^{15} \bmod 131 = 71$

$Y_B = \alpha^{X_B} \bmod q = 6^{27} \bmod 131 = 104$

shared secret : $\begin{cases} Y_B^{X_A} \bmod q = 104^{15} \bmod 131 = 71 \\ Y_A^{X_B} \bmod q = 71^{27} \bmod 131 = 71 \end{cases}$ #

5.

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

$C_2 = Y^k \cdot M \bmod q = (3^4 \cdot 9) \bmod 131 = 74$

$(117, 74)$ #

B. $C_2 = (3^k \cdot M_1) \bmod 131 = 65$

$C_2' = (3^k \cdot M_2) \bmod 131 = 64$

$\Rightarrow 3^k (M_1 - M_2) \bmod 131 = 1$

$\Rightarrow 3^{-k} \bmod 131 = M_1 - M_2$ #

6.

A. $(0,1), (0,6), (3,3), (3,4), (4,0), (6,2), (6,5)$ #

B. $P_B = n_B G = (5,5)$ #

C. $C_m = \{P_B = kG, P_m + kP_A\} = ((2,2), (3,2))$ #

D. $(2,6) - 4(5,1) = (3,2)$ #