Q-3) Alphabet size is 30 so $30 \times 30 = 900$ possible bigrams

key space size : $E(x) = (ax + b) \bmod m$

Alpha values (a) : the value can be any number that is coprime with 900 which is $2^2 \times 3^2 \times 5^2$. So a can not be any multiple of 2, 3 or 5

For beta (b) values there are 900 possible values

key space size $= \phi(900) \times 900$

$$\phi(n) = n \prod_{i=1}^{n} (1 - 1/p_i)$$

$$\phi(900) = 900(1-1/2)(1-1/3)(1-1/5) = 900 \cdot (1/2)(2/3)(4/5)$$

$$= 240$$

$$240 \times 900 = \underline{216\,000}$$

Q-4)

- If some bigram appears multiple times in the plaintext, it will always be encrypted to the same ciphertext bigram assuming the key remains the same
- if an attacker has access to a portion of plaintext and it is corresponding ciphertext, they could potentially reverse-engineer the key.
- The key space of this cipher as I calculated relatively small. This small key space makes it susceptible to brute force attack.

Q->6

- We can denote the Alphabet size by N ($N=29$) And the letters would be $A=0$, $B=1$ --- $Z=25$.
- The numerical value of α is a, random shift value k and ciphertext letter β is b:

$$b = (a+k) \bmod N$$

- the probability of occuring ciphertext β:

$$P_\beta = \sum_{\alpha=0}^{N-1} \sum_{k=0}^{N-1} P_\alpha P_k$$

- since k values are selected uniformly randomly

$$P_k = \frac{1}{N} \quad \text{for all } k \text{ in } \{0,1 \dots N-1\}$$

$$\sum_{k=0}^{N-1} P_k = 1 \rightarrow P_\beta = \sum_{\alpha=0}^{N-1} P_\alpha \cdot 1 = \sum_{\alpha=0}^{N-1} P_\alpha = 1$$

- Since there are N possible values for β and also the total prob sum 1 the prob of any given ciphertext letter β must be $\frac{1}{N} = \frac{1}{29}$