Question Number 4

An affine cryptosystem is given by the following encryption function, where a, b are chosen from $\mathbb{Z}_{26}$.

$$enc_{a,b} : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$$
$$x \to \text{ax} + \text{b} \epsilon \mathbb{Z}_{26}$$

- Encrypt the plaintext cryptography using the affine code $enc_{3,5}$. What is the decryption function corresponding to $enc_{3,5}$? Decrypt the ciphertext XRHLAFUUK.
- A central requirement of cryptography is that the plaintext must be computable from the key and the ciphertext. Explain why $enc_{2,3}$ violates this rule. Show that the function enca,b satisfies the rule if and only if $gcd(a, 26) = 1$.
- In the following we consider only functions enca,b with $gcd(a, 26) = 1$. Show that all affine codes with $b = 0$ map the letter a to a and the letter n to n.

Solution.