CS553 Cryptography

BitBees

Question 3

Question 3

Part A

An affine cryptosystem is given by the following encryption function, where a, b are chosen from Z_{26}

$$enc_{a,b} : Z_{26} \rightarrow Z_{26}$$

$$x \rightarrow ax + b \,\epsilon\, Z_{26}$$

Given, $a = 3$ and $b = 5$
To find $enc_{3,5}(cryptography)$:

$$enc_{3,5}(cryptography) = \textbf{"lezykvxefyaz"}$$

The corresponding decryption function is as follows:

$$dec_{3,5}(y) = 9(y - 5) \mod 26$$

Applying the above decryption formula, we get:

$$dec_{3,5}("xrhlafuuk") = "\textbf{geschafft}"$$

Part B

For the Affine cipher, the formulae for encryption and decryption are defined as follows:

$$\implies enc_{a,b}(x) = (a.x + b) \mod m$$

$$\implies dec_{a,b}(y) = a^{-1} \times (y - b) \mod m$$

We observe that in order for the cipher to satisfy the central requirement of cryptography that plain text must be computable from the key and cipher text, a must be invertible in Z_m. Inverse for an element in Z_m exists if and only if $gcd(element, m) = 1$
Consider the case where $(a, b) = (2, 3)$.
There does not exist an inverse for 2 in Z_{26}. Hence, $enc_{2,3}(x)$ violates the central rule of cryptography.

Part C

Since $b = 0$, our encryption and decryption rules respectively become:

$$enc_{a,0}(x) = a.x$$
$$dec_{a,0}(x) = a^{-1}.x$$

Now, considering "a" to be the plaintext being encoded. "a" maps to an x of 0. Hence the encryption rule defined above always returns 0 irrespective of value of a(from the tuple, $(a, 0)$). This 0 maps back to a ciphertext of "a".

Before proving a similar condition for "n", let us consider the following:
In order for a(from (a, b) to be invertible, we can be sure that a is not even (i.e. $a \mod 2 = 1 \ \forall a \epsilon Z_m$). Since, if a is even, then $gcd(a, 26)$ is never 1 as the least possible greatest common divisor will become 2. Hence, a must be an odd number.
Now, coming to the plaintext "n", it maps to $x = 13$. Odd multiples of 13 always return 13 for multiplication that is closed in Z_{26}. This 13 maps back to the ciphertext "n".
Hence, all affine codes with $b = 0$ map the letter a to a and the letter n to n.