DTU/2K16/MC/13

Q4) A generalization of the caesar cipher, known as the Affine Cipher generates the ciphertext letter C for any plaintext P using the formula $C = E([x,b], p) = (xp+b) \bmod 26$. A basic requirement of any encryption is that it be one-to-one. That is if $p \neq q$, then $E(K,p) \neq E(K,q)$. Otherwise decryption is impossible, because more than one plaintext character maps to the same ciphertext.

The affine caesar cipher is not one-to-one for all values of x. For example, for $x=2$ and $b=3$, then $E([x,b], 0) = E([x,b], 13) = 3$. In such a case determine which values of x are not allowed so that the given cipher is one-to-one.

Ans 4) We define the Affine cipher which encrypts/produces the ciphertext character C for plaintext character P as.

$$C = E([a,b], P) = (ap+b) \bmod 26$$

and the decryption algorithm as

$$P = D([a,b], C) = (C-b)\, a^{-1} \bmod 26$$

Now, both operation, substraction by 'b' and 'a^{-1}' congruent to $\equiv \bmod 26$ need to be invertible operations.

The shift operator is congruent for all elements in the set $\mathbb{Z}_{26}$.

So, $b \in \{0,1,2,3,4,5,6 \ldots 21,22,23,24,25\}$

Now, we the (a^{-1}) inverse operation under $\mathbb{Z}_{26}$ which isn't defined ~~for~~ for every element in $\mathbb{Z}_{26}$. We will use the multiplicative set $\mathbb{Z}_{26}^{*}$ for that.

$$a \in \mathbb{Z}_{26}^{*} = \{1,3,5,7,9,11,15,17,19,21,23,25\}$$

Every element in this set has an inverse also present in $\mathbb{Z}_{26}^{*}$ such that $(a * a^{-1}) \bmod 26 = 1$ where a^{-1} is called the multiplicative inverse.

A few examples are

$(1 * 1) \bmod 26 = 1$
$(3 * 9) \bmod 26 = 1$
$(5 * 21) \bmod 26 = 1$
$(7 * 15) \bmod 26 = 1$ etc.

$(9 * 3) \bmod 26 = 1$
$(11 * 19) \bmod 26 = 1$
$(17 * 23) \bmod 26 = 1$
$(25 * 25) \bmod 26 = 1$

So, $\boxed{x = a \in \mathbb{Z}_{26}^{*}}$

Q5) DTU/2K16/MC/13

Using the playfair matrix: Encrypt the message "Must See You over Cadogan West Coming at Once"

M	F	H	I/J	K
U	N	O	P	Q
Z	V	W	X	Y
E	L	A	R	G
D	S	T	B	C