Practical 3:

Note:
Assume domain of key Z26* in Multiplicative cipher. It is set of all integers x in Z26 such that x is relatively prime with 26.
-->Z26*={1,3,5,7,9,11,15,17,19,21,23,25}
-->Z26={0,1,2,3,....,25}

1. To implement Multiplicative Cipher.
   Encryption:
   Input: Plain Text and Key (from Z26*)
   Output: Cipher Text
   Hint: **C(i)=(P(i)*K) MOD 26, i=1,2...,L where L is the length of the plaintext.**

   Decryption:
   Input: Cipher Text and Key (from Z26*)
   Output: Plain Text
   Hint: **P(i)=(C(i)*(K^-1)) MOD 26, i=1,2...,L where L is the length of the ciphertext.**
   Here K^-1 is the Multiplicative Inverse of K.

   Crypt-analysis:
   Apply Brute-force attack.
   Input: Cipher Text and domain of Key i.e. Z26*
   Output: All possible Messages.

2. To implement Affine Cipher.
   Encryption:
   Input: Plain Text, Key K1(from Z26*) and Key K2 (from Z26)
   Output: Cipher Text
   Hint: **C(i)=(P(i)*K1+K2) MOD 26, i=1,2...,L where L is the length of the plaintext.**

   Decryption:
   Input: Cipher Text, Key K1(from Z26*) and Key K2 (from Z26)
   Output: Plain Text
   Hint: **P(i)=((C(i)-K2)*(K1^-1)) MOD 26, i=1,2...,L where L is the length of the ciphertext.**
   Here K1^-1 is the Multiplicative Inverse of K1.

   Crypt-analysis:
   Apply Brute-force attack.
   Input: Cipher Text, All possible pairs (K1,K2) i.e. key space
   Output: All Possible Messages.

Here, Keys are K1 and K2. K1 can be any of the 12 elements from Z26*. K2 can be any of the 26 elements. Therefore, the key space is **26*12=312.**

Hint for Cryptanalysis: Take nested for loops. Outer loop for values of K1 and Inner for values of K2. Try pair (K1,K2) and decrypt the message using equations specified. Print message for each iteration. There will be total 312 messages in the output.