Q3 Vigenere Cipher is a method of encrypting alphabetic text. It uses a simple form of polyalphabetic substitution. A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. The encryption of the original text is done using this using Vigenere square or table. At different points in the encryption process, the cipher uses a different alphabet from one of the rows. The alphabet used at each point depends on a repeating keyword

→ Input: GEEKSFORGEEKS

Keyword: AYUSH

Output: ciphertext: GCYCZFMLYLEIM ∴ for generating key, the given keyword is repeated in a circular manner until it matches the length of plain text.

Encryption :- $E_i = (P_i + K_i) \% 26$

Decryption :- $D_i = (E_i - K_i + 26) \% 26$

Q4 Encryption for vigenere cipher:-

```
string = "GEEKSFORGEEKS"
keyword= "SHARAN"

def generateKey (string , key) :
    key = list (key)
    if len (string) == len (key) :
      return (key)
   else :
      for i in range (len (string) - len (key)):
         key. append ( key [i % len (key)])
   return(" ". join (key))
def encrypt_ cipherText (string , key):
   ciphertext= []
   for i in range (len (string)):
      x = ((ord (string [i]) + ord ( key (i])) % 26 + ord ('A')
   return (" ". join (ciphertext))

key = generateKey (string , ~~key~~ keyword)
print ("Original Message :- ", string)
print (" Keyword :- ", keyord)
ciphertext = encrypt_Ciphertext (string, key)
print ("cipher text :- ", ciphertext )
```

Output:

```
Original Message :- GEEKSFORGEEKS
Keyword :- SHARAN
Ciphertext :- YLEBSSGYAVEXK
```

* Public key of Alice : $5^{\text{private key of Alice}} \% 17$

i.e. $5^4 \% 17$

$= 13$

Public key of Bob : $5^{\text{private key of Bob}}$

$= 5^6 \bmod 17$

$= 2$

Secret key obtained by Alice : $2^{\text{private key of Alice}} \bmod 7$

$= 2^4 \bmod 7$

$= 16$

" " by Bob : $13^{\text{private key of Bob}} \bmod 7$

$= 13^6 \bmod 17$

$= 16$

∴ Both have same values for secret key (option (A))