In a Diffie-Hellman Key Exchange, Alice and Bob have chosen prime value q = 17 and prime root = 5. If Alice's secret key is 4 and Bob's secret key is 6. what is the secret key they exchanged ?.

$n = 17$

$a = 5$

Private Key of Alice = 4

Private Key of Bob = 6

$5^{\text{Private key of Alice}} \bmod 17 =$ public key of Alice

$5^{4} \bmod 17$

$= 13$

$5^{\text{Private key of Bob}} \bmod 17 =$ Public of Key of Bob

$= 5^{6} \bmod 17$

$= 2$

Secret key obtained by alice

$= 2^{\text{Private key of Alice}} \bmod 7$

$= 2^{4} \bmod 17$

$= 16$

Secret key obtained by Bob

$= 13^{\text{Private key of Bob}} \bmod 7$

$= 13^{6} \bmod 17$

$= 16$

The value of common secret key is 16.

Vigenère (±) Encryption

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

def generateKey(string, key):
      key = list(key)
      if(len(string) == len(key)):
       ~~retur~~ 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):
      cipher_text = []
   for ~~for~~ i in range(len(string)):
      x = ((ord(string[i])+ord(key[i]))%26)+ord('A')
       cipher_text.append(chr(x))
   return(". join(cipher_text))

 key = generateKey(string, keyword)
 print(string, keyword)

 cipher_text = encrypt_cipherText(string, key)
 print(cipher_text)
```

PAGE No.
DATE / /

Vigenere Decryption

```
def originalText(cipher_text, key):
        orig_text = []
        for i in range ( len(cipher_text)):
                x = (ord(cipher_text[i]) - ord(key[i]) +26 )%26
                x+ = ord ('A')
                orig_text. append (chr (x))
        return
        ~~return~~ ("" . join(orig_text))

if __name__ = = "__main__":
    string = "GEEKSFORGEEKS"
    keyword = "AYUSH"
    key = generateKey (string, keyword)
    cipher_text = cipherText (string, key)
    print ("Ciphertext: ", cipher_text)
    print ("Original / Decrypted Text:",
              originalText (cipher_text, key))
```