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

Given:-

$n = 17$

$a = 5$

Private key of Alice $= 4$

Private key of Bob $= 6$

Public key of Alice $= 5^4 \% 17$
$= 13$

Secret key obtained by Alice $= 2^4 \% 17$
$= 16$

Public key of Bob $= 5^6 \% 17$
$= 2$

Secret key obtained by Bob $= 13^6 \% 17$
$= 16$

Finally, both the parties obtain the same value of secret key.
The value of common secret key $= 16$.
Option (a)

Write encryption code for Vignère Cipher..

```
string = "GEEKSFORGEEKS"
keyword = [redacted] "RUSHIL"

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):
    cipher_text = []
    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 = generate Key (string, keyword)
print("Original Message", string)
print("Keyword:", keyword)
cipher_text = encrypt_cipherText (string, key)
print ("Ciphertext: ", cipher_text)
```

Output:-

```
    Original Message   GEEKSFORGEEKS
    Keyword:           RUSHIL
    Ciphertext:        XYWRAQFLYLMVJ
```

Write decryption code for Vignere Cipher

```
ciphertext = "XYWRAQFLYMVJ"
keyword = "RUSHIL"
def generatekey(ciphertext, 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 decrypt_original text (ciphertext, key):
    origtext = []
    for i in range(len(ciphertext)):
        x = ((ord(ciphertext[i] - ord( key [i]]) % 26) + ord("A")
        origtext.append (chr(x))
    return(" ".join(origtext)

key = generatekey(ciphertext, keyword)
print("Cipher text", ciphertext)
print("Keyword ", keyword)

string = decrypt_original text (ciphertext, key)
print("Original text; ", string)
```

OUTPUT:

```
Ciphertext: XYWRAQFLYMVJ
keyword : RUSHIL
Original text: GEEKSFORGEEKS
```