2) Prime no: $p = 17$.
Primitive root, $q = 5$.
Private key of Alice, $a = 4$
Private key of Bob, $b = 6$.

Public key of Alice $x = q^a \bmod p$
$\rightarrow 5^4 \bmod 17$
$\rightarrow x = 13$

Public key of Bob: $y = q^b \bmod p$
$y = 5^6 \bmod 17$
$y = 2$

Secret key of Alice: $k_a = y^a \bmod p$.
$\rightarrow 2^4 \bmod 17$
$\rightarrow k_a = 16$

Secret key of Bob: $k_b = x^b \bmod p$.
$\rightarrow 13^6 \bmod 17$
$\rightarrow k_b = 16$

Secret key = 16

ENCRYPTION FOR VIGENERE CIPHER:

String = "GEEKS FOR GEEKS"
Keyword = "SIDHARTH"

```
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 = []
    for i in range (len(string)):
        x = ((ord(string[i]) + ord (Key[i])) %.26) + ord('A')
        cipher.append (chr(x))
    return ("".join(cipher))

Key = generateKey (string, keyword).
print ("Original text:", string)
print ("Key word:", Keyword)
cipher_text = encrypt_ciphertext (string, Key)
print ("Ciphertext:" cipher_text).
```

OUTPUT:

Original ~~message~~ text: GEEKS FOR GEEKS
Keyword: SIDHARTH
Cipher text: YMHRS WHY YMHRS.

Decryption For Vignere Cipher

```
ciphertext = "YMNRS WHYYMHRS"
keyword = "SIDHARTH"
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_originaltext (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 ("Ciphertext:", ciphertext)
print ("keyword:", keyword)
string = decrypt_originaltext (ciphertext, key)
print ("Original text:", string).
```

Output:

Ciphertext: YMNRS WHYYMHRS

Keyword: SIDHARTH.

Original text: GEEKS FOR GEEKS.