ISP Assignment

Q.1 Given

$n = 17$

$a = 5$

Private key of Alice $= 4$

Private key of Bob $= 6$

Step I

Public key of Alice

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

$= 5^{4} \bmod 17$

$= 13$

Public key of Bob

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

$= 5^{6} \bmod 17$

$= 2$

Step II

Secret key obtained by Alice

$= 2^{\text{Private key of Alice}} \bmod 17$

$= 2^{4} \bmod 17$

$= 16$

Secret key obtained by Bob

$= 13^{\text{Private key of Bob}} \bmod 17$

$= 13^{6} \bmod 17$

$= 16$

Both Parties obtain same value of secret key

secret key $= 16$

option (1) is correct

```
Q.2 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):
        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: SHARAN
ciphertext: YLEBSSGYGVEKK
```