5044

PAGE No.
DATE / /

ISP Assignment

Q) given:

$n = 17$

$a = 5$

Private key of Alice = 4

Private key of Bob = 6.

Public key of Alice

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

$= 5^4 \bmod 17$

$= 13$

Public key of Bob

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

$= 5^6 \bmod 17$

$= 2.$

Secret key obtained by Alice

$= 2^{\text{Priv key of alice}} \bmod 17$

$= 2^4 \bmod 17$

$= 16.$

Secret key obtained by Bob

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

$= 136 \bmod 17$

$= 16.$

So both of them obtain the same value of secret key

∴ The value of the secret key obtained = 16

PAGE No.
DATE / /

a) Encryption & Decryption code for Vigenere cipher.

encryption :- To generate key

```
def encrypt_ciphertext (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)).
```

for encryption :

```
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)).
```

for decryption :

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