__/__/____

ISP ICA Assignment

Q1 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?

Soln Given

$q = 17$ $\quad a = 5$

Private key:

Alice = 4 (A)

Bob = 6 (B)

(i) Value of public key calculation

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

$= 5^4 \bmod 17$

$= 13$

Public key of Bob:-

$= 5^B \bmod 17$

$= 5^6 \bmod 17$

$= 2$

(ii) Secret key calculation

$= 2^A \bmod 17$

$= 2^4 \bmod 17$

$= 16$

Secret key of Bob

$13^B \bmod 17$

$13^6 \bmod 17$

$= 16$

Value of common secret key = 16.

Q2 Write encryption and decryption code for Vingenere cipher.

Soln

Encryption

```
String = "_ _ _ _"
keyword = "_ _ _ _"
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 = generatekey(string, keyword)

print("original message", string)
print("keyword:", keyword)
cipher_text = encrypt_cipherText(string, key)
print(cipher_text)
```

__/__/____

decryption

```
def decrypt(cipher_text, key):
    orig_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))

key = generate_key(string, keyword)
cipher_text = encrypt_cipherText(string, key)
print("Ciphertext:", cipher_text)
print("Original text:", decrypt(cipher_text, key))
```