In [2]:

```
'''
Practical No. : 06
Program Code with output
Title : Implement the different Hellman Key Exchange mechanism using HTML and
parties (Alice) and the JavaScript application as other party (bob).

'''

def isPrime(x):
    j = 2
    limit = x ** 0.5

    while (j <= limit):
        if (x % j == 0):
            return False
        j += 1

    return True


def find_primimtive_root(q):
    # 1 is never a primitive root of any number

    a = 2
    res = []

    while (True):
        flag = 0
        res.clear()

        for i in range(1, q):
            r = a ** i % q
            if (r < 1 or r > q - 1 or r in res):
                break
            res.append(r)
        else:
            print(a)
            return a

        a += 1


def accept_private_key(q):
    while (True):
        print(f'Enter a number less than q = {q} : ')
        private_key = int(input())
        if (private_key < q):
            break
    return private_key

def generate_symmetric_key(public_key,private_key,q):
    return (public_key**private_key)%q

def main():
    while (True):
        q = int(input("Enter a prime number q : "))
```

```
        if (isPrime(q)):
            break

    a = find_primimtive_root(q)

    print("Private key of user 'a' : ")
    Xa = accept_private_key(q)

    Ya = pow(a,Xa,q)

    print("Private key of user 'b' : ")
    Xb = accept_private_key(q)

    Yb = pow(a,Xb,q)

    Key_Generated_For_Sender_a = pow(Yb,Xa,q)
    Key_Generated_For_Receiver_b = pow(Ya,Xb,q)

    print(f"Private key of user 'a' = {Xa}")
    print(f"Public key of user 'a' = {Ya}")

    print(f"\nPrivate key of user 'b' = {Xb}")
    print(f"Public key of user 'b' = {Yb}")

    print(f"\nKey Generated For Sender 'a' = {Key_Generated_For_Sender_a}")
    print(f"Key Generated For Receiver 'b' = {Key_Generated_For_Receiver_b}")

main()
```

```
Enter a prime number q : 17
3
Private key of user 'a' :
Enter a number less than q = 17 :
15
Private key of user 'b' :
Enter a number less than q = 17 :
13
Private key of user 'a' = 15
Public key of user 'a' = 6

Private key of user 'b' = 13
Public key of user 'b' = 12

Key Generated For Sender 'a' = 10
Key Generated For Receiver 'b' = 10
```