Kartik Padave

A022

70362019039

Experiment 5

Aim

To implement Diffie Hellman.

Theory

Diffie–Hellman key exchange is a method of securely exchanging cryptographic keys over a public channel and was one of the first public-key protocols as conceived by Ralph Merkle and named after Whitfield Diffie and Martin Hellman. DH is one of the earliest practical examples of public key exchange implemented within the field of cryptography. Published in 1976 by Diffie and Hellman, this is the earliest publicly known work that proposed the idea of a private key and a corresponding public key.

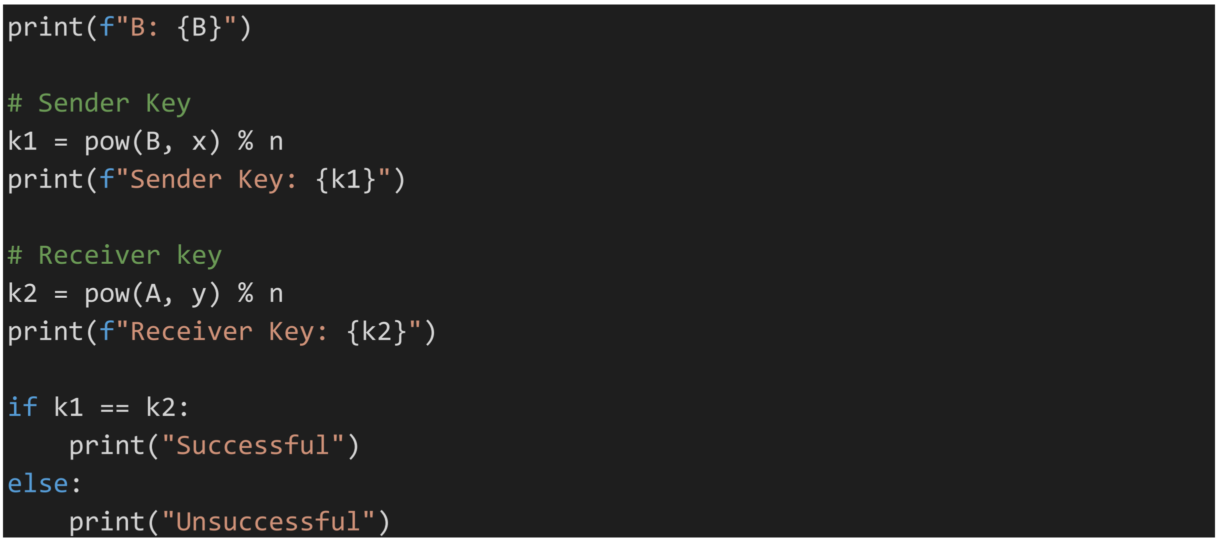
Traditionally, secure encrypted communication between two parties required that they first exchange keys by some secure physical means, such as paper key lists transported by a trusted courier. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure channel. This key can then be used to encrypt subsequent communications using a symmetric-key cipher.

Code

```python
n = int(input("Enter prime number (n): "))
g = int(input("Enter prime number (g): "))

# Sender A
x = int(input("Enter +ve number (x): "))
A = pow(g, x) % n
print(f"A: {A}")

# Receiver B
y = int(input("Enter +ve number (y): "))
B = pow(g, y) % n
```



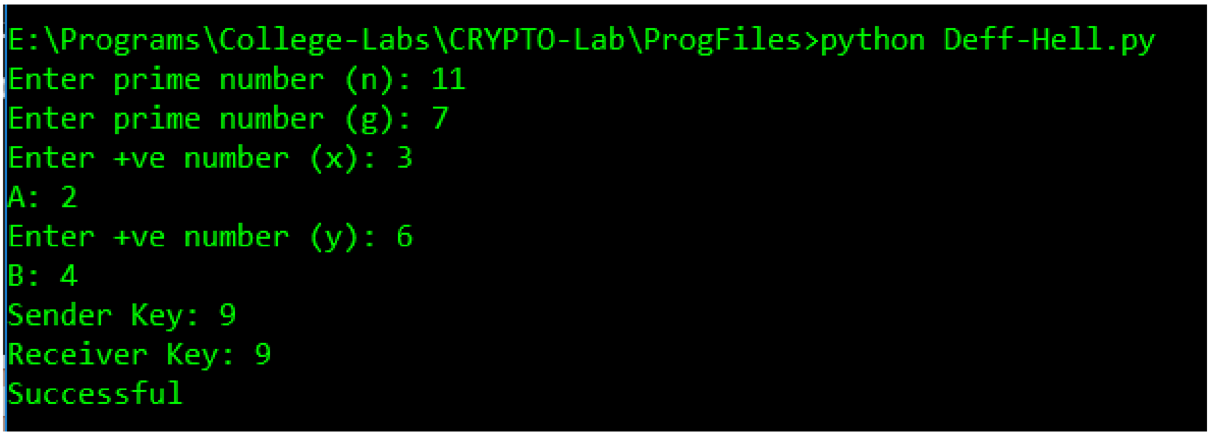
```python
print(f"B: {B}")

# Sender Key
k1 = pow(B, x) % n
print(f"Sender Key: {k1}")

# Receiver key
k2 = pow(A, y) % n
print(f"Receiver Key: {k2}")

if k1 == k2:
    print("Successful")
else:
    print("Unsuccessful")
```

Output



```
E:\Programs\College-Labs\CRYPTO-Lab\ProgFiles>python Deff-Hell.py
Enter prime number (n): 11
Enter prime number (g): 7
Enter +ve number (x): 3
A: 2
Enter +ve number (y): 6
B: 4
Sender Key: 9
Receiver Key: 9
Successful
```

Conclusion

Hence, we were able to implement DES.