Sumeet Haldipur

2019130018

TE Comps

Batch A

Experiment 2: Diffie Hellman Algorithm

Github Link: https://github.com/sumeethaldipur/CSS_LAB/blob/main/Experiment2.py

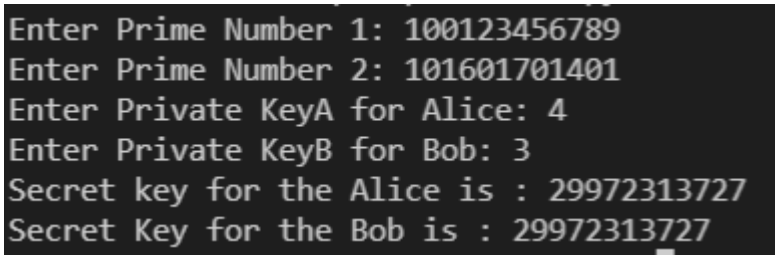
Aim:

To implement Diffie Hellman Algorithm in Python.

Code:

```
A = int(input('Enter Prime Number 1: '))
B = int(input('Enter Prime Number 2: '))

a = int(input('Enter Private KeyA for Alice: '))
m = int(pow(B,a,A))

b = int(input('Enter Private KeyB for Bob: '))
n = int(pow(B,b,A))

ka = int(pow(n,a,A))

kb = int(pow(m,b,A))

print('Secret key for the Alice is : %d'%(ka))
print('Secret Key for the Bob is : %d'%(kb))
```

Output:



Conclusion:

<u>Diffie Hellman Algorithm:</u>

The Diffie–Hellman (DH) Algorithm is a key-exchange protocol that enables two parties communicating over public channel to establish a mutual secret without it being transmitted over the Internet. DH enables the two to use a public key to encrypt and decrypt their conversation or data using symmetric cryptography. DH is generally explained by two sample parties, Alice and Bob, initiating a dialogue. Each has a piece of information they want to share, while preserving its secrecy. To do that they agree on a public piece of benign information that will be mixed with their privileged information as it travels over an insecure channel. Their secrets are mixed with the public information, or public key, and as the secrets are exchanged the information they want to share is commingled with the common secret. As they decipher the other's message, they can extract the public information and with knowledge of their own secret, deduce the new information that was carried along. While seemingly uncomplicated in this method's description, when long number strings are used for private and public keys, decryption by an outside party trying to eavesdrop is mathematically infeasible even with considerable resources. DH is one of the first practical implementations of public-key cryptography (PKC). It was published in 1976 by Whitfield Diffie and Martin Hellman. Other contributors who are credited with developing DH include Ralph Merkle and researchers within the United Kingdom's intelligence services (c. 1969).