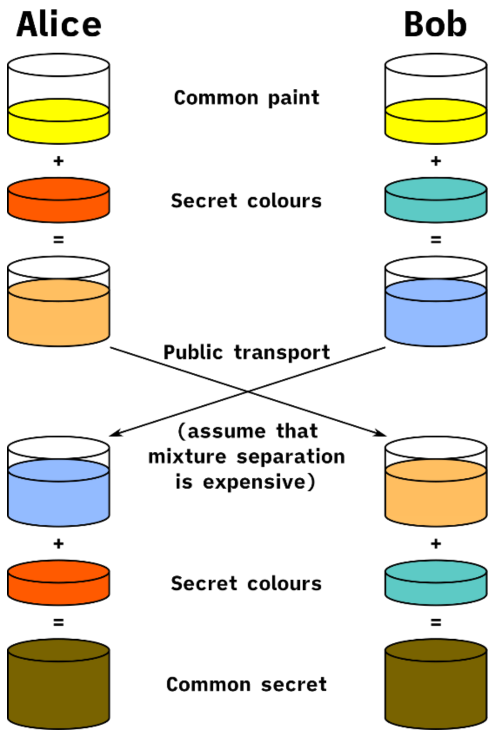
COP 5615 – Distributed Operating System Principles
Assignment/Weekly Report – 8
10/26 – 10/30
Suprith Reddy Gurudu, UFID: 9961-2134

Diffie-Hellman Key Exchange Algorithm Implementation

Reference: https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange

The Diffie-Hellman key exchange was one of the most significant key exchange algorithms in public-key cryptography. It allows two parties, who have not known before, to securely establish a key which they can use to secure their communications on a channel. The below figure briefly explains the step by step flow of the algorithm.



$$A = g^{a} \bmod p$$

$$B = g^{b} \bmod p$$

Both Alice and Bob have arrived at the same values because under mod p,

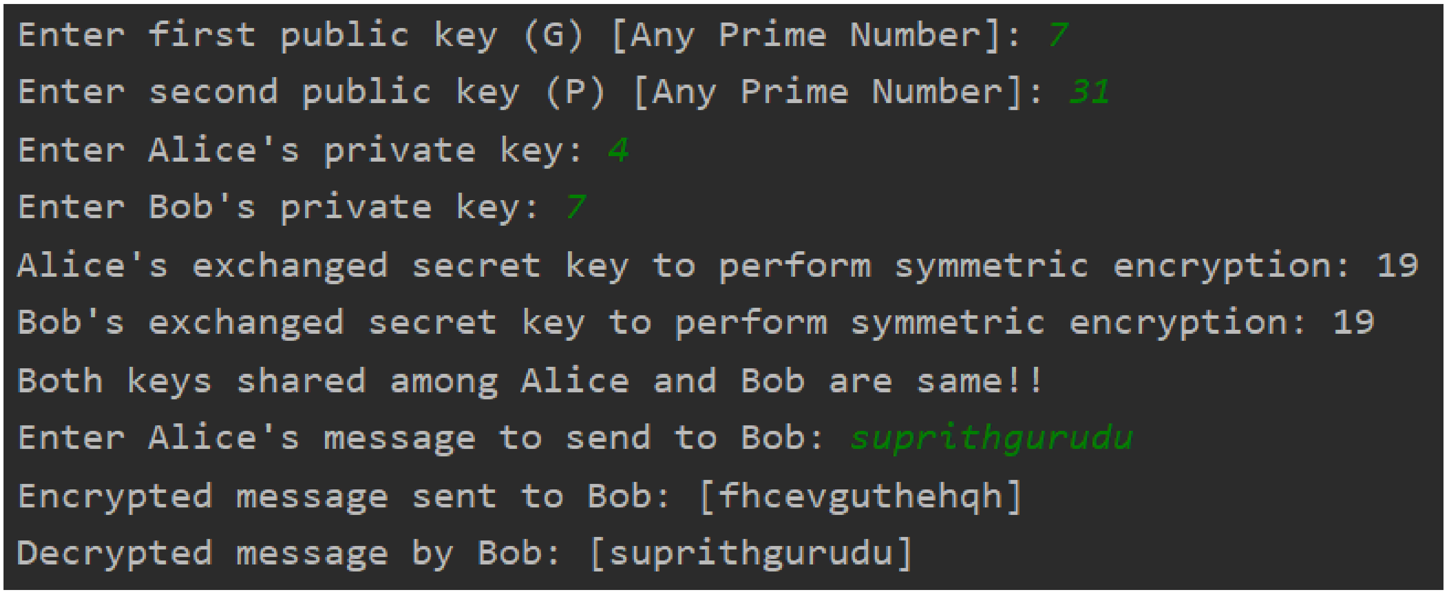
$$A^{b} \bmod p = g^{ab} \bmod p = g^{ba} \bmod p = B^{a} \bmod p$$

$$(g^{a} \bmod p)^{b} \bmod p = (g^{b} \bmod p)^{a} \bmod p$$

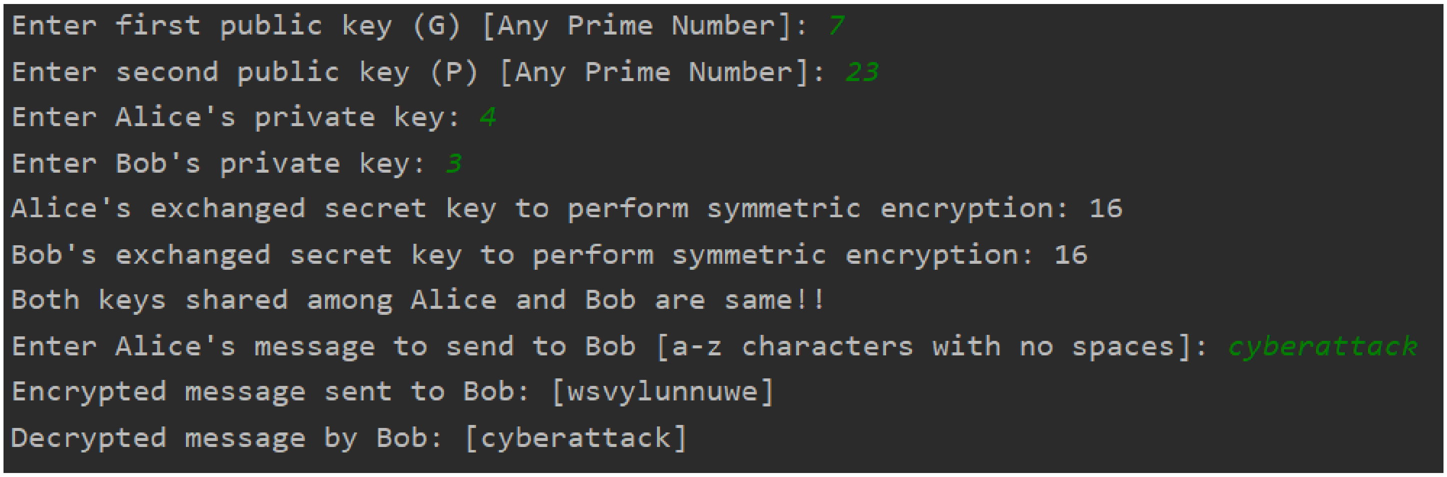
In the implementation, I have considered only 4 variables one prime P and G (a primitive root of P) and two private keys as a (represents Alice) and b (represents Bob). P and G are both publicly available keys. Two parties, for instance Alice and Bob, chooses private keys a and b and they generate a key and exchange it publicly. The other party receives the key and generates a secret using the received key. Finally, the key generated by both parties at last step will be same and can be used to encrypt the further messages in the communication.

Results from the Implementation:

```
>scalac DiffieHellman.scala
>scala DiffieHellman.scala
```



```
Enter first public key (G) [Any Prime Number]: 7
Enter second public key (P) [Any Prime Number]: 31
Enter Alice's private key: 4
Enter Bob's private key: 7
Alice's exchanged secret key to perform symmetric encryption: 19
Bob's exchanged secret key to perform symmetric encryption: 19
Both keys shared among Alice and Bob are same!!
Enter Alice's message to send to Bob: suprithgurudu
Encrypted message sent to Bob: [fhcevguthehqh]
Decrypted message by Bob: [suprithgurudu]
```



```
Enter first public key (G) [Any Prime Number]: 7
Enter second public key (P) [Any Prime Number]: 23
Enter Alice's private key: 4
Enter Bob's private key: 3
Alice's exchanged secret key to perform symmetric encryption: 16
Bob's exchanged secret key to perform symmetric encryption: 16
Both keys shared among Alice and Bob are same!!
Enter Alice's message to send to Bob [a-z characters with no spaces]: cyberattack
Encrypted message sent to Bob: [wsvylunnuwe]
Decrypted message by Bob: [cyberattack]
```