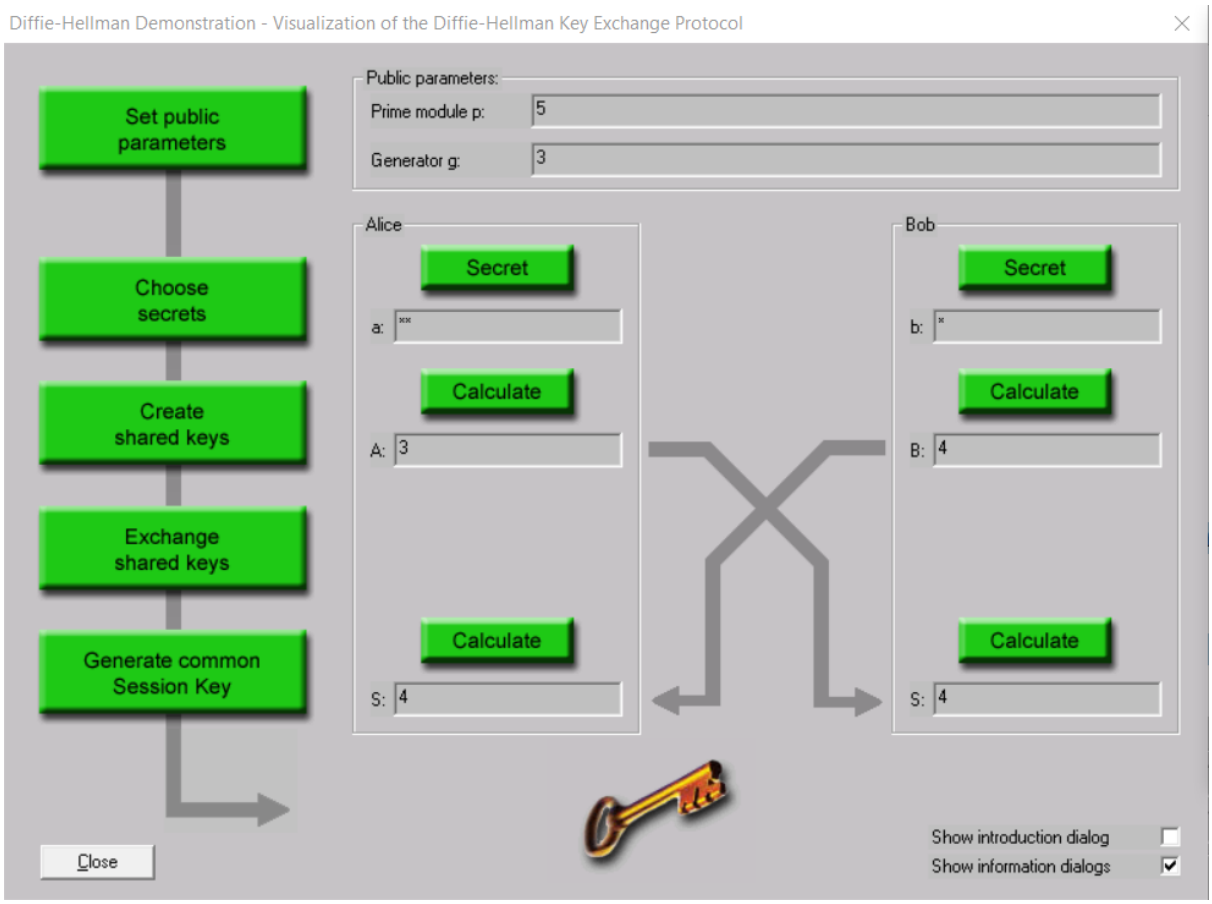
Name: Rehan Mumtaz
Roll No.: SE-19036

LAB TASK # 6

Q: Calculate the Symmetric Key using Diffie-Hellman Key Exchange method while considering the suitable values

Ans: I consider p = 5, g= 3, a =55, b = 2. Cryptool generates session key as "4"



EXERCISE

1. **Calculate the Symmetric Key using Diffie-Hellman Key Exchange method while considering the following values g=4, p=13 and a=10, b=8. Verify the Cryptool generated key with the manual calculations.**

Manual Calculation:

g=4, p=13
Let Alice's Secret number is a=10 and Bob's secre number is b=8.
We calculate the symmetric Key by Diffie-Hellman Key Exchange method as,

Shared Key of Alice:
A=g^a mod p
A=4^10 mod 13 = 1048576 mod 13
A=9

Name: Rehan Mumtaz
Roll No.: SE-19036

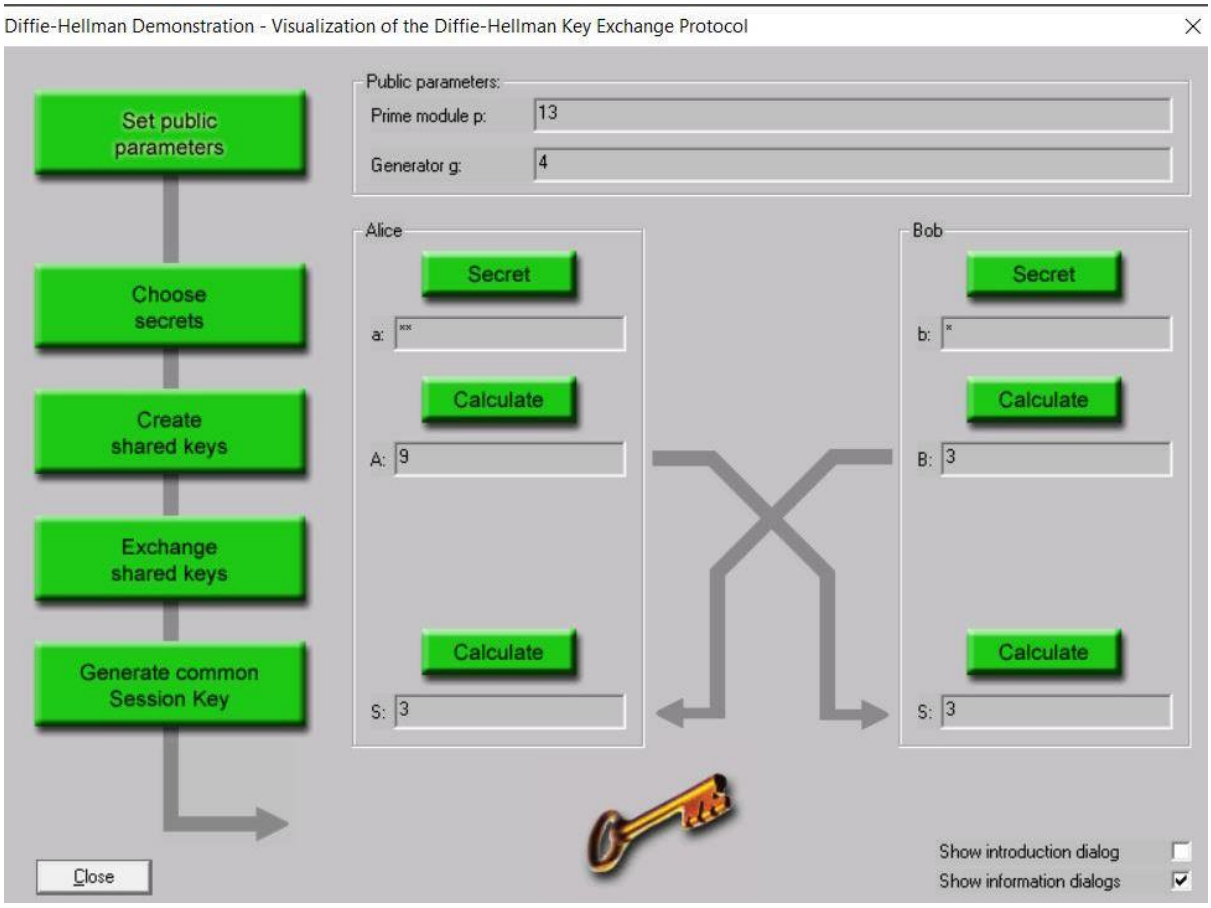
Shared Key of Bob:
B=g^b mod p
B=4^8 mod 13 = 65536 mod 13
B=3

Session Key of Alice
Alice= B^a mod p
Alice = 3 ^10 mod 13 = 59049 mod 13
Alice = 3

Session Key of Bob
Bob= A^b mod p
Bob= 9 ^10 mod 13 = 43046721 mod 13
Bob= 3

They encrypt their message with symmetric key “3”

Cryptool Output:



Hence verified by cryptool.

Name: Rehan Mumtaz
Roll No.: SE-19036

2. How Man in the Middle Attach is possible in Diffie-Hellman Key Exchange method.

Ans. In a man-in-the-middle (MITM) attack, an attacker intercepts and modifies the communication between two parties without either party being aware. In the context of the Diffie-Hellman key exchange, an MITM attack is possible if the attacker can intercept and modify the messages being exchanged between the two parties.

Here's an example of how an MITM attack could work in a Diffie-Hellman key exchange:

1. Alice and Bob want to establish a secure communication channel and agree to use the Diffie-Hellman key exchange to do so.
2. The attacker, Eve, intercepts the initial message that Alice sends to Bob containing Alice's public key.
3. Eve sends her own public key to Bob instead of forwarding Alice's message.
4. Bob generates a secret key and sends it to Eve, thinking that she is Alice.
5. Eve sends the secret key to Alice, pretending to be Bob.
6. Alice and Bob both generate the same secret key, thinking that they are communicating with each other directly. However, the secret key that they generate is based on Eve's public key, not each other's.
7. Eve now has the secret key that Alice and Bob are using to communicate, and can decrypt and read any messages that are sent over the secure channel.

To prevent an MITM attack in a Diffie-Hellman key exchange, it is important to verify the authenticity of the public keys being used. This can be done through the use of certificates or other authentication methods.