

LAB 6

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.

$g=4$, $p=13$

Let Alice's Secret number is $a=10$ and Bob's secret number is $b=8$.

We calculate the symmetric Key by Diffie-Hellman Key Exchange method as,

Shared Key of Alice:

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

$$A = 4^{10} \bmod 13 = 1048576 \bmod 13$$

$$A = 9$$

Shared Key of Bob:

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

$$B = 4^8 \bmod 13 = 65536 \bmod 13$$

$$B = 3$$

Session Key of Alice

$$\text{Alice} = B^a \bmod p$$

$$\text{Alice} = 3^{10} \bmod 13 = 59049 \bmod 13$$

$$\text{Alice} = 3$$

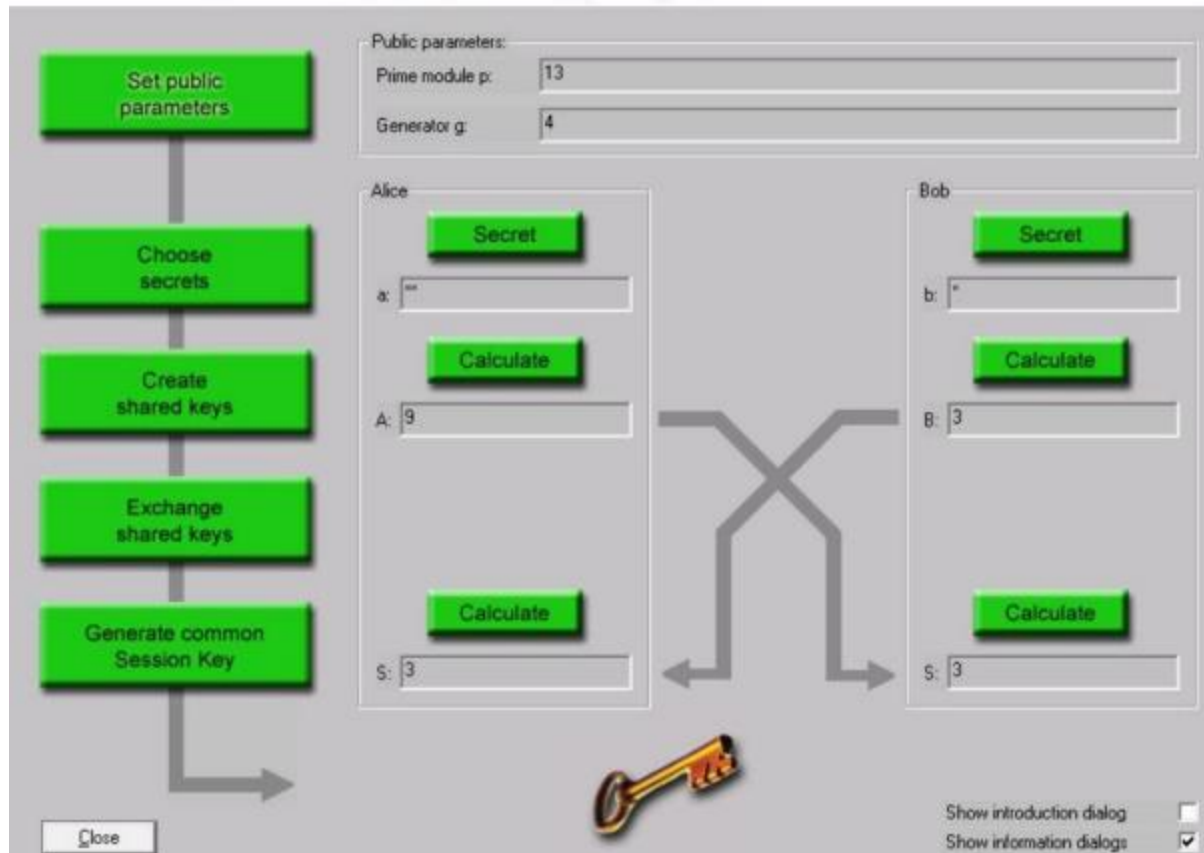
Session Key of Bob

$$\text{Bob} = A^b \bmod p$$

$$\text{Bob} = 9^{10} \bmod 13 = 43046721 \bmod 13$$

$$\text{Bob} = 3$$

They encrypt their message with symmetric key "3"



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

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.

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

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

The screenshot shows the Cryptool Diffie-Hellman Key Exchange interface. On the left, a vertical flowchart with green buttons outlines the process: "Set public parameters", "Choose secrets", "Create shared keys", "Exchange shared keys", and "Generate common Session Key". Below the flowchart is a "Close" button. The main area is divided into sections for "Public parameters:", "Alice", and "Bob".

Public parameters:

- Prime module p : 5
- Generator g : 3

Alice's side:

- Secret: (button)
- a : (input field)
- Calculate: (button)
- A : 3 (output field)
- Calculate: (button)
- S : 4 (output field)

Bob's side:

- Secret: (button)
- b : (input field)
- Calculate: (button)
- B : 4 (output field)
- Calculate: (button)
- S : 4 (output field)

Arrows indicate the exchange of public keys A and B between Alice and Bob. A large 'X' is drawn over the exchange arrows, and a key icon is shown at the bottom center, representing the shared session key $S = 4$. At the bottom right, there are checkboxes for "Show introduction dialog" (unchecked) and "Show information dialogs" (checked).