

Assignment B3

Execution Date: 19/05/2021

Submission Date: 21/05/2021

Title: Diffie - Hellman Key exchange

Problem Statement:

To implement Diffie - Hellman Key exchange

Objective:

- Understand basic concepts of Diffie Hellman key exchange
- Logical implementation of algorithm.

Outcome:

Students will be understand and implement Diffie - Hellman Key exchange.

Software Requirements:

- Jupyter Notebook
- Python 3.8.5
- 64 bit operating system.

Hardware Requirements:

- Computer with 64 bit processor

Theory:

The Diffie Hellman algorithm was widely known as key exchange algorithm or key agreement algorithm developed by Whitfield Diffie and Martin Hellman.

Diffie Hellman algorithm is used to generate some (symmetric) private cryptographic key at the sender as well as receiver end so that there is no need to transfer this key from sender to receiver.

Remember, This algorithm is used only for key agreement not for decryption or encryption of messages.

If sender and receiver want to communicate with each other, they agree on the same key generated by algorithm later on they can use this key for encryption or decryption.

Algorithm:

- 1) Sender and receiver gets public numbers g & α .
- 2) Both select private keys 'a' and 'b'.
- 3) Following values are computed.

$$x = \alpha^a \text{ mod } g$$

$$y = \alpha^b \text{ mod } g$$

- 4) Both users exchange x and y .
- 5) Following computations are performed to calculate Symmetric Key.

$$K_a = y^a \bmod q$$

$$K_b = x^b \bmod q$$

$$K_a = K_b$$

Example:

1) Let $q = 23$ and $\alpha = 9$

2) let $a = 4$ and $b = 3$

3) $x = 9^4 \bmod 23 = 6$

$$y = 9^3 \bmod 23 = 16$$

4) Exchange x and y

5) $K_a = y^a \bmod q$
 $= 16^4 \bmod 23 = 9$

$$K_b = x^b \bmod q$$
$$= 6^3 \bmod 23 = 9$$

\therefore Secret Key is 9.

Test Cases:

Description	Expected O/P	Actual O/P
1) Test algorithm with random numbers	Both secret keys are equal	Successful
2) Test algorithm with above example.	Both secret keys: 9	Successful

Conclusion:

Therefore, we have successfully implemented Diffie hellman key exchange algorithm.