MES Wadia College of Engineering Pune-01

Department of Computer Engineering

Name of Student:	**Class: TE Comp**
Semester/Year: 6th	**Roll No:**
Date of Performance:	**Date of Submission:**
Examined By: Prof(Dr.)S.K.Wagh	**Experiment No: Part 2-IS-05**

PART 2- LPII-ELII-IS-ASSIGNMENT NO: 05

AIM:
To Implement the Diffie-Hellman Key Exchange mechanism using HTML and JavaScript. (Consider the end user as one of the parties (Alice) and the JavaScript application as other party (bob))

OBJECTIVES:

1. Understand Secure Key Exchange Concepts

- Grasp the principles of secure key exchange and the problem it solves in cryptographic communications, emphasizing the ability to securely share a secret key between two parties without prior secure communication channels.

2. Learn the Diffie-Hellman Protocol

- Understand the steps involved in the Diffie-Hellman Key Exchange mechanism, including the generation of public and private values, the exchange of public values, and the computation of the shared secret.

3. Implement Algorithm Steps

APPRATUS:

- Operating System recommended: 64-bit Open source Linux or its derivative.
- HTML and JavaScript.

THEORY:

Diffie–Hellman key exchange is a mathematical method of securely exchanging cryptographic keys over a public channel and was one of the first public-key protocols as conceived by Ralph Merkle and named after Whitfield Diffie and Martin Hellman. DH is one of the earliest practical examples of public key exchange implemented within the field of cryptography. Published in 1976 by Diffie and Hellman, this is the earliest publicly known work that proposed the idea of a private key and a corresponding public key.

Traditionally, secure encrypted communication between two parties required that they first exchange keys by some secure physical means, such as paper key lists transported by a trusted courier. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure channel. This key can then be used to encrypt subsequent communications using a symmetric-key cipher.

Diffie–Hellman is used to secure a variety of Internet services. However, research published in October 2015 suggests that the parameters in use for many DH Internet applications at that time are not strong enough to prevent compromise by very well-funded attackers, such as the security services of some countries.

The scheme was published by Whitfield Diffie and Martin Hellman in 1976, but in 1997 it was revealed that James H. Ellis, Clifford Cocks, and Malcolm J. Williamson of GCHQ, the British signals intelligence agency, had previously shown in 1969 how public-key cryptography could be achieved.

Method of Operation in Diffie-Hellman Key Exchange

Diffie-Hellman key exchange algorithm is based on the principles of modular exponentiation and discrete logarithms to allow two parties to securely establish a shared secret key over an insecure communication channel. Here is an operational overview of the process in context to Alice and Bob :

1. Parameters Setup

Alice and Bob must agree upon two number:

- A large prime number p,
- A generator g of p, which is the primitive root of p

These two number are shared and are not kept secret.

2. Key Generation

- Alice and Bob randomly chose a private key, say xa and xb, where xa is the private key of Alice and xb is the private key of Bob.
- These private keys are kept secret and not being shared.

3. Public Key Exchange

- Both Alice and Bob perform a calculation to generate their corresponding public keys.

ya = g rest to a (mod p)

yb = g rest to b (mod p),

where ya is the public key of Alice and yb is the public key of Bob

- The public key are then shared with each other, ya is shared with Bob and yb is shared with Alice.

4. Shared Secret Key Calculation

- Alice then calculates the shared secret using the yb received from Bob and her private key as:

k = (yb rest to xa (mod p)

- Bob also calculates the shared secret using the ya received from Alice and his private key xb as:

k = (ya rest to xb (mod p)

5. Resulting Secret

Alice and Bob will end upon the same shared secret key, which can be used for encryption and decryption of information using symmetric key algorithms.

CONCLUSION:

We have successfully studied Diffie-Hellman key exchange algorithm.

QUESTIONS:

1. Address Security Considerations for DHKE algorithm.

2. Discuss the importance of choosing large and secure values for *p* and *g* to prevent vulnerabilities to attacks such as discrete logarithm problems for DHKE algorithm.