## Assignment No 6

**Title**:

Write a java program to implement Diffie Hellman Key Exchange Algorithm.

**Theory**:

Whitefield Diffie and Martin Hellman develop Diffie Hellman key exchange Algorithms in 1976 to overcome the problem of key agreement and exchange. It enables the two parties who want to communicate with each other to agree on a symmetric key, a key that can be used for encrypting and decryption; note that Diffie Hellman key exchange algorithm can be used for only key exchange, not for encryption and decryption process. The algorithm is based on mathematical principles.

### Diffie Hellman Key Exchange Algorithm for Key Generation

The algorithm is based on Elliptic Curve Cryptography, a method of doing public-key cryptography based on the algebra structure of elliptic curves over finite fields. The DH also uses the trapdoor function, just like many other ways to do public-key cryptography. The simple idea of understanding to the DH Algorithm is the following.

1. The first party picks two prime numbers, g and p and tells them to the second party.
2. The second party then picks a secret number (let's call it a), and then it computes $g^a$ mod p and sends the result back to the first party; let's call the result A. Keep in mind that the secret number is not sent to anyone, only the result is.
3. Then the first party does the same; it selects a secret number b and calculates the result B similar to the step 2. Then, this result is sent to the second party.
4. The second party takes the received number B and calculates $B^a$ mod p
5. The first party takes the received number A and calculates $A^b$ mod p

This is where it gets interesting; the answer in step 5 is the same as the answer in step 4. This means both parties will get the same answer no matter the order of exponentiation.

$(g^a \ mod \ p)^b \ mod \ p = g^{ab} \ mod \ p$
$(g^b \ mod \ p)^a \ mod \ p = g^{ba} \ mod \ p$

The number we came within steps 4 and 5 will be taken as the shared secret key. This key can be used to do any encryption of data that will be transmitted, such as blowfish, AES, etc.

### Diffie Hellman Algorithm

1. key $=(Y_A)^{XB} \text{mod } q$ -> this is the same as calculated by B

2. Global Public Elements

- q: q is a prime number

- a: $a < q$ and $\alpha$ is the primitive root of q

3. Key generation for user A

- Select a Private key $X_A$ Here, $X_A < q$

Now, Calculation of Public key $Y_A$ $Y_A = a^{XA} \bmod q$

4. Key generation for user B

- Select a Private key $X_B$ Here, $X_B < q$
- Now, Calculation of Public key $Y_B$ $Y_B = a^{Xb} \bmod q$

5. Calculation of Secret Key by A

- key $=(Y_B)^{XA} \bmod q$

6. Calculation of Secret Key by B

- key $=(Y_A)^{XB} \bmod q$

Example

1. Alice and Bob both use public numbers P = 23, G = 5

2. Alice selected private key a = 4, and Bob selected b = 3 as the private key

3. Both Alice and bob now calculate the value of x and y as follows:

- Alice: $x = (5^4 \bmod 23) = 4$
- Bob: $y = (5^3 \bmod 23) = 10$

4. Now, both Alice and Bob exchange public numbers with each other.

5. Alice and Bob now calculate the symmetric keys

- Alice: $k_a = y^a \bmod p = 10^4 \bmod 23 = 18$
- Bob: $k_b = x^b \bmod p = 4^3 \bmod 23 = 18$

6. 18 is the shared secret key.

**Advantages of the Diffie Hellman Algorithm**

- The sender and receiver don't need any prior knowledge of each other.
- Once the keys are exchanged, the communication of data can be done through an insecure channel.

- The sharing of the secret key is safe.

**Disadvantages of the Diffie Hellman Algorithm**

- The algorithm can not be sued for any asymmetric key exchange.
- Similarly, it can not be used for signing digital signatures.
- Since it doesn't authenticate any party in the transmission, the Diffie Hellman key exchange is susceptible to a man-in-the-middle attack.

**Conclusion**

The Diffie Hellman key Exchange has proved to be a useful key exchange system due to its advantages. While it is really tough for someone snooping the network to decrypt the data and get the keys, it is still possible if the numbers generated are not entirely random. Also, the key exchange system makes it possible to do a man in the middle attack; to avoid it, both parties should be very careful at the beginning of the exchange.