Assignment B3

Title: Implementation of Diffie – Hellman key exchange

Problem Statement:

Implement Diffie – Hellman key exchange algorithm.

Objective:

❖ To understand how Diffie- Hellman key exchange algorithm works.

Outcome

Students will be able to:

Understand and implement Diffie – Hellman key exchange algorithon.

Software and Hardware Requirements:

Core 2 Duo /13/15/i7 64-bit processor OS- Linux 64 bit os

Editor / Eclipse -gedit/

Software – C++ / JAVA / Python

Theory:

Diffie Hellman (DH) key exchange algorithm is a method for securely exchanging cryptogmphic keys over a public

communication channel. keys are not actually exchanged - they are jointly derived. It is named after their inventors Whitfield Diffie and Martin Hellman.

Working of Diffie-Hellman Algorithmn

1. In Public key encryption schemes are secure only if authenticity of the public key is assured.

2. Dithe - Hellman key exchange is a simple public key algorithm.

3. The protocol enables 2 users to establish a secret key using a public key scheme based on discrete algorithms.

4. The protocol is secure only if the authenticity of the 2 participants can be established.

5. There are 2 publicly known numbers: A prime number q and an integer X that is a primitive root of q.

6. k= (YA)^xb mod q → same as calculated by 8

7. Global Public Elements

   a) q: prime number

   b) X: x < q and it is a primitive root of q

8. User A Key Generation

   a) Select Private key Xa XA < q

   b) Calculation of Public key YA YA = Xa mod q

9. User B Key Generation

   a) Select Private key XB XB < q

   b) Calculation of Public key YB Yb = Xb mod q

10. Calculation of Secret Key by A

   a) k= (Yb)^xa mod q

11. Calculation of Secret Key by B

   a) k = (YA)Xb mod q

12. The result is that two sides have exchanged a secret value.

Discrete Logarithms

Discrete logarithms are logarithms defined with regard to multiplicative cyclic groups. IF G is a multiplicative cyclic group and g is a generator of G, then we know every element h in G can be written as g for some x. The discrete logarithm to the base at h in the group is defined to be x.

The discrete logarithm problem is defined as: given a group G, a generator to the base group and an element of Gn, to find the discrete logariton of h in the group G. Discrete logarithm problem is not always hard. The hardness of finding discrete bogarithms depends on the groups. For example, a popular choice of groups for discrete logarithm based crypto-systems is ^{3}p where p is a prime number, if p-1 is a product of small primes, then the Pohling- Hellman algorithon he discrete logarithm problem in this can solve s group very efficiently. That's why we always want p to be a safe prime when using "p" as the basis of discrete logarithm based crypto-systems. A safe prime is a prime number which equals 2q + 1 where q is a large prime number. This guarantees that p-1 = 2q has a large prime factor so that the Pohlig – Hellman algorithm cannot solve the discrete logarithm problem easily.

Even p is a safe prime, here is a sub-exponential algorithm which is called the index calculus. That means p must be very large Cusually at least 1024-bit to make the crypto-systems safe the algorithm's security lies on the fact that it is easy

to carulate exponential modula a prime, last difficult to calculate discrete logarithm.

Uses of Diffie - Hellman Algorithmn

Aside from using the algorithm for generating public keys, there are some other places where DH Algorithon can be used:

❖ Encryption

Diffie Hellman key exchange algorithm can be used to do encryption one of the first schemes to do it was ElGamal encryption. One modern example of it is called Integrated Encryption Scheme which provides security against chosen plain text and chosen clipboard attacks.

❖ Password Authenticated Agreement

When two parties share a password, a password-authenticated key agreement can be used to prevent the Man in the middle attack. This key agreement can be in the form of Diffie-Hellman. Secure Remote Password Protocal is a good example that is based on this technique.

❖ Forward Secrecy

Forward secrecy based protocols can generate new key pairs for each new session, and they can automatically discard them at the end when the session is finished too. In these forward Secrecy protocols more often than not, the Diffie Hellman key exchange is used.

Advantages of the Diffic Hellman Algorithms

❖ The sender and receiver don't need any prior knowledge of each other.

❖ Once the keys are exchanged the communication of through an insecure channel.

❖ The sharing of the secret key is safe

Disadvantages of the Diffie Hellman Algorithon

❖ The algorithm cannot be used for any asymmetric key exchange.

❖ Similarly, it cannot 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:

Successfully implemented the Diffie. Hellman bey exchange algorithm.

User A		User B
Generate a Random		Generate a Random.
$X_A < q$		$X_B < q$
Calculate	Y_A Y_B	Calculate
$Y_A = \alpha^{X_A} \bmod q$		$Y_B = \alpha \bmod q$
Calculate		Calculate
$K = (Y_B)^{X_A} \bmod q$		$K = (Y_B)^{X_A} \bmod q$