Diffie-Helman Algorithm

1.The Diffie-Hellman algorithm was developed by Whitfield Diffie and Martin Hellman in 1976.

2.This algorithm was devices not to encrypt the data but to generate same private cryptographic key at both ends so that there is no need to transfer this key from one communication end to another.

3.It is used to exchange secret key between two users.

4.use asymmetric encryption (public or private key concept) to exchange the secret key between users.

5. The most challenging part in this type of encryption is the transfer of the encryption key from sender to receiver without anyone intercepting this key in between.

6. This transfer or rather generation on same cryptographic keys at both sides secretively was made possible by the Diffie-Hellman algorithm.

Defination:- Diffie – Hellman algorithm is an algorithm that allows two parties to get the shared secret key using the communication channel, which is not protected from the interception but is protected from modification.

Algo:-

C

A----------→B

1. The first step in public-key cryptography A and B want exchange an encryption key over an insecure communication link where Eve is listening in.
2. To do this they need to use a prime number.
3. The Diffie-Hellman algorithm uses a simple concept in mathematics where a prime number can be used to generate a list of numbers in a seemingly random sequence.
4. This seemingly random sequence is what make the algorithm secure.

Steps:-

1. A and B agree on a prime number q.
2. Select α such that it must be primitive root of q and $\alpha < q$

Suppose 'a' is a primitive root of q if

a mod q

a^2 mod q

a^3 mod q……a^{q-1} mod q

Example:- q=7

3^1 mod 7=3

3^2 mod 7=2

3^3 mod 7=6

3^4 mod 7=4

3^5 mod 7=5

3^6 mod 8=1

It gives result={1,2,3,…….q-1}

That value should not be repeated and should have all values in the output set from 1 to q-1.

Example:-

5^1 mod 7=5

5^2 mod 7=4

5^3 mod 7=6
5^4 mod 7=2
5^5 mod 7=3
5^6 mod 7=1
So 5 is the primitive root of 7.

Example:-

Let q=7(prime)

$\alpha < q$

α =5

We can take any of two primitive root 3 or 5.

α and q are global public element (known to every one)

1. **Key generation of person A:-**

X-private key
Y-public key

Assume X_A(private key) and X_A <q

(X_A-private key of A)

Calculate $Y_A = \alpha^{XA} \bmod q$

(Y_A=public key of A)

Assume private key $X_A=3$ $X_A < q$ $(3<7)$

$Y_A = \alpha^{XA} \bmod q$

$Y_A = 5^3 \bmod 7$

$Y_A=6$

2. **Key generation of person B:-**

Assume X_B(private key) and $X_B < q$

(X_B--private key of B)

Calculate $Y_B = \alpha^{XB} \bmod q$

(Y_B=public key of B)

Assume private key $X_B=4$ $X_B < q$ $(4<7)$

$Y_B = \alpha^{XB} \bmod q$

$Y_B = 5^4 \bmod 7$

$Y_B=2$

Summery:-

Person A		**Person B**
Private key	global element	Private key
$X_A=3$	$q=7, \alpha=5$	$X_B=4$
	Public key	
	$Y_A=6$	
	$Y_B=2$	

Now calculate the secret key :-

To calculate the secret key ,both the sender and receiver will use public key

$K_A=(Y_B)^{XA} \bmod q$ $KB=(Y_A)^{XB} \bmod q$

Note:- Here Y_B and Y_A is public key and it is known to all.

$$\mathbf{K_1=K_2}$$

$K_A=(Y_B)^{XB} \bmod q$

$K_A = 2^3 \bmod 7$

$K_A = 8 \bmod 7$

$K_A = 1$

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

$K_B = 6^4 \bmod 7$

$K_B = 1$

So $K_1 = K_2$

Thus the key are exchanged**.**

Uses of Diffie Hellman Algorithm:-

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

2.**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 Protocol is a good example that is based on this technique.

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

Advantages:

1.The sender and receiver have no prior knowledge of each other.

2.Communication can take place through an insecure channel.

3.Sharing of secret key is safe.

Disadvantage:

1. A problem with asymmetric encryption, however, is that it is slower than symmetric encryption. It requires far more processing power to both encrypt and decrypt the content of the message.
2. The algorithm can not be sued for any asymmetric key exchange.
3. Similarly, it can not be used for signing digital signatures.
4. Since it doesn’t authenticate any party in the transmission, the Diffie Hellman key exchange is susceptible to a man-in-the-middle attack.