Diffie Hellman key exchange :

The Diffie Hellman key exchange is a method for securely exchanging cryptographic keys over an insecure channel. It is a fundamental building block of many secure communication protocols. The Diffie Hellman key exchange works by allowing two parties to agree on a shared secret key over an insecure channel. without any other party being able to intercept the key to learn anything about it.

Process :

Alice	Bob
• Public key available = (P, G)	• Public key available = (P, G)
• Private key selected = a	• Private key selected = b
• key generated : $x = G^a \bmod P$	• key generated : $y = G^b \bmod P$
Exchange of Generated key takes place	
• key received = y	• key received = x
• Generated secret key : $K_a = y^a \bmod P$	• Generated secret key $K_b = x^b \bmod P$

* Algebraically it can be shown that $K_a = K_b$

Example:

- Alice and Bob get public key $P = 23$ and $G = 9$
- Alice selected a private key $a = 4$ and
  Bob selected a private key $b = 3$
- Alice and Bob generate their key.

  Alice's key : $x = G^a \bmod P = 9^4 \bmod 23 = 6$

  Bob's key : $y = G^b \bmod P = 9^3 \bmod 23 = 16$
- Alice and Bob exchange their generated keys.
- Alice receives ~~Public~~ key $y = 16$ and
  Bob receives ~~public~~ key $x = 6$
- Alice and Bob computes the secreat key.

  Alice : $K_a = y^a \bmod P = 16^4 \bmod 23 = 9$

  Bob : $K_b = x^b \bmod P = 6^3 \bmod 23 = 9$
- Thus, 9 is the shared secreat.

Problem 1:

In a Diffie-Hellman key exchange, Alice and Bob have chosen prime value $P = 17$ and primitive root $G = 5$. If Alice's secret key is 4 and Bob's secret key is 6, what should be their common secret key?

Given, $P = 17$, $G = 5$, $a = 4$ and $b = 6$

Alice and Bob generates a key for exchange,

Alice's key: $G^a \bmod P = 5^4 \bmod 17 = 13$

Bob's key: $G^b \bmod P = 5^6 \bmod 17 = 2$

Alice and Bob exchange their keys. Thus, Alice receives $y = 2$ and Bob receives $x = 13$

Both Alice and Bob calculate their secret key.

Alice's secret key: $K_a = y^a \bmod P = 2^4 \bmod 17 = 16$

Bob's secret key: $K_b = x^b \bmod P = 13^6 \bmod 17 = 16$

Thus, the common secret key for both Alice and Bob is 16.

Vulnerabilities of Diffie-Hellman key exchange:

The Diffie-Hellman key exchange is a widely used and trusted technique for securely exchanging cryptographic key. However like all cryptographic system it is not completely immune to attacks and vulnerabilities.

1) Man in the middle attack:

If an attacker is able to intercept and

modify the messages exchanged between Alice and Bob during the key exchange, they may be able to impersonate Alice or Bob and establish secure channel with the other party.

This can be prevented by using certificate-based authentication and/or by verifying the authenticity of the message.

ii) Small group attack:

If the prime number p used in the key exchange has a small subgroup, an attacker may be able to use this to their advantage to recover the shared secret key.

To prevent this, it is important to use a large prime number with no known small subgroups.

iii) Exponent attack:

If the secret exponents (a and b) used in the key exchange are not chosen randomly, an attacker may be able to use this to their advantage to recover the shared secret key.

To prevent this it is important to use a strong random number generator to generate the secret exponents.

Application of Diffie Hellman Key exchange:

The Diffie Hellman Key exchange is widely used and trusted technique for securely exchanging cryptographic keys over an insecure channel.

i) **Secure Communication protocol:**

The Diffie-Hellman key exchange is used in many secure communication protocols such as SSL/TLS and SSH to establish a secure channel between two parties.

ii) **Virtual private network:**

The Diffie-Hellman key exchange is often used in VPNs to establish a secure connection between a client and a server.

iii) **Secure file transfer protocol:**

The Diffie-Hellman Key exchange is used in many secure file transfer protocols, such as SFTP and FTPS to establish a secure channel for transferring files between two parties.

iv) **Other applications:**

The Diffie Hellman key exchange is also used in many other applications where secure connection is required such as email, secure web browsing, secure voice over IP (VoIP) etc.