Diffie-Hellman Key Exchange – Example:

The Diffie-Hellman Key Exchange is a method for securely exchanging cryptographic keys over a public channel. It enables two parties to establish a shared secret key, which can then be used for secure communication via symmetric encryption, even if an eavesdropper is listening to the exchange. Below is a detailed explanation with an example.

Steps of Diffie-Hellman Key Exchange:

1. Choose Public Parameters:
- **Both parties agree on two public parameters:**
  - **A prime number (p).**
  - **A primitive root (generator) (g) modulo (p). This generator (g) is such that its powers modulo (p) generate all numbers from 1 to (p-1).**

These values (p) and (g) can be made public.

Example of Public Parameters:
- **Let (p = 23) (a prime number).**
- **Let (g = 5) (a primitive root modulo 23).**

2. Private Keys:
- **Each party chooses their private key, which is a secret number that is never shared publicly.**
  - **Let's call Alice's private key (a).**
  - **Let's call Bob's private key (b).**

Example of Private Keys:
- **Alice chooses her private key (a = 6).**
- **Bob chooses his private key (b = 15).**

3. Calculate Public Keys:
- **Using the public parameters (p) and (g), both parties calculate their public keys and share them with each other. The public key is computed as:**
  - **Alice's public key: (A = g^a mod p)**
  - **Bob's public key: (B = g^b mod p)**

Example of Public Key Calculation:

- **Alice calculates her public key:**
  [A = 5^6 mod 23 = 15625 mod 23 = 8]
- **Bob calculates his public key:**
  [B = 5^{15} mod 23 = 30517578125 mod 23 = 19]

- **Now Alice and Bob exchange their public keys:**
  - **Alice sends (A = 8) to Bob.**
  - **Bob sends (B = 19) to Alice.**

4. Calculate Shared Secret:

- **Both Alice and Bob now use each other's public key to compute the shared secret. The shared secret is computed as:**
  - **Alice computes: (S = B^a mod p)**
  - **Bob computes: (S = A^b mod p)**

Even though they use different formulas, they end up with the same result due to the properties of modular arithmetic.

Example of Shared Secret Calculation:

- **Alice computes the shared secret using Bob's public key (B = 19):**
  [S = 19^6 mod 23 = 47045881 mod 23 = 2]
- **Bob computes the shared secret using Alice's public key (A = 8):**
  [S = 8^{15} mod 23 = 35184372088832 mod 23 = 2]

Thus, both Alice and Bob now share the same secret (S = 2), which can be used as the symmetric key for encryption.

Why Diffie-Hellman is Secure:

The security of the Diffie-Hellman key exchange relies on the difficulty of solving the discrete logarithm problem. Given (g^a mod p) and (p), it is computationally infeasible to determine (a) (the private key) unless one uses brute force, especially if (p) is a large prime (e.g., 2048 bits). This makes it very hard for an eavesdropper to compute the shared secret, even if they know (g), (p), and both public keys.

Summary:

- **Public information: (p = 23), (g = 5), (A = 8), (B = 19).**
- **Alice's private key: (a = 6), Bob's private key: (b = 15).**
- **Shared secret: (S = 2).**