|  |  |
| --- | --- |
| Subject: Cryptography & System Security Lab | Course ID: CSL-602 |
| Semester: VI | Course: AI & DS |
| Laboratory: 302 | Name of teacher: Prof. Gitanjali Korgaonkar |
| Name of Student: Ayush Gupta | Roll No: VU2S2324001 |

**EXPERIMENT NO. 2**

**Aim:**

Implementation of Diffie Hellman Key exchange algorithm

**Theory:**

The Diffie-Hellman Key Exchange is a cryptographic protocol that allows two parties to securely generate a shared secret over an insecure communication channel. This shared secret can be used for encrypted communication. Proposed by Whitfield Diffie and Martin Hellman in 1976, this algorithm was one of the first practical methods for establishing a secure key exchange in public-key cryptography.

**Working Principle**

The Diffie-Hellman algorithm is based on the mathematical concept of modular exponentiation and the difficulty of computing discrete logarithms. The core idea is that two parties can agree on a common secret without directly transmitting it, making it difficult for an eavesdropper to intercept the key.

**Steps of Diffie-Hellman Key Exchange**

1. **Public Parameters**:
   * Both parties agree on two publicly known numbers:
     + A large prime number P.
     + A generator (primitive root) G of P.
2. **Private Key Selection**:
   * Each party selects a private key:
     + Alice chooses a random private key a.
     + Bob chooses a random private key b.
3. **Public Key Generation**:
   * Alice computes her public key: A = Ga mod P.
   * Bob computes his public key: B = Gb mod P.
4. **Exchange of Public Keys**:
   * Alice and Bob exchange their public keys A and B over the insecure channel.
5. **Shared Secret Computation**:
   * Alice computes: S = Ba mod P.
   * Bob computes: S = Ab mod P.
   * Since (Gb mod P)a = (Ga mod P)b, both computations result in the same shared secret S.

**Security Considerations:**

The security of the Diffie-Hellman algorithm relies on the difficulty of computing discrete logarithms. Given P, G, and Ga mod P, it is computationally infeasible to determine a without solving the discrete logarithm problem, making it resistant to brute-force attacks.

**Applications:**

* **Secure Key Exchange**: Used in SSL/TLS protocols to establish encrypted communication.
* **VPNs (Virtual Private Networks)**: Used for secure data transmission.
* **End-to-End Encryption**: Applied in messaging services like WhatsApp and Signal.

**Limitations:**

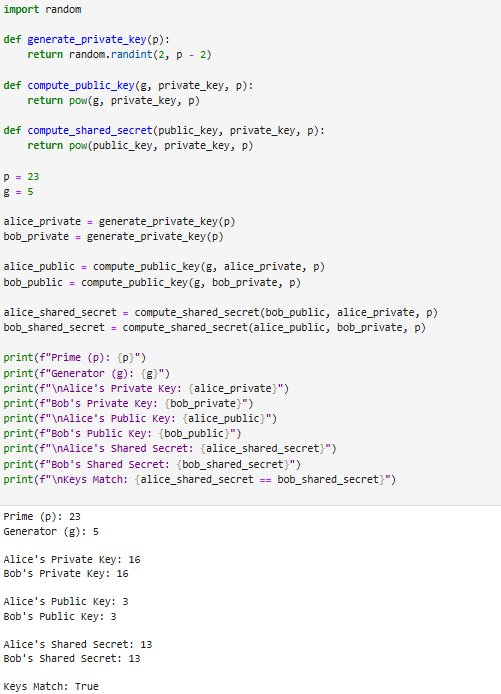
* **Man-in-the-Middle Attacks (MITM)**: If the public keys are intercepted and replaced, an attacker can establish separate shared secrets with each party. This can be mitigated using authentication mechanisms like digital signatures.
* **No Authentication**: Diffie-Hellman alone does not verify the identities of the communicating parties.

**Conclusion:**

The Diffie-Hellman Key Exchange algorithm is a fundamental cryptographic protocol that enables secure communication. Despite its limitations, it remains widely used and forms the basis of many modern encryption techniques. To enhance its security, it is often combined with authentication mechanisms to prevent MITM attacks.



**Program and Output:**

****