**Course – Cryptography and System Security (CSS)**

|  |  |
| --- | --- |
| **UID** | 2021300038 |
| **Name** | Atharva Gite |
| **Class and Batch** | BE Computer Engineering - Batch VIII |
| **Date** | 19/09/2024 |
| **Lab #** | 4 |
| **Aim** | Implement Diffie-Hellman algorithm |
| **Problem Definition** | The experiment uses key exchange algorithm namely *Diffie-Hellman* and symmetric cryptosystem to provide two security services. In the first part, the experiment covers key distribution problem using *Diffie-Hellman key exchange algorithm*. This allows sharing secret key between sender and receiver without using any third party entity. In the second part, symmetric cryptosystem covers sending large message from the sender to the receiver using the secret key shared in the first step. |
| **Theory** | The Diffie-Hellman algorithm allows for the establishment of a shared secret that can be used for secure communications by enabling users to exchange data over a public network. In its elliptic curve variant, this process involves using elliptic curves to generate points, ultimately deriving a secret key from specified parameters. The algorithm relies on four key components: a large prime number ppp, a generator ggg (a primitive root modulo ppp), and two private values aaa and bbb chosen by the users, often referred to as Alice and Bob.  Both ppp and ggg are publicly available numbers, which means they can be shared openly without compromising security. Alice and Bob each select their private keys aaa and bbb, which should be kept secret and generated randomly to ensure security. They then compute their public keys: Alice calculates her public key A=gamod  pA = g^a \mod pA=gamodp, and Bob computes his public key B=gbmod  pB = g^b \mod pB=gbmodp. After exchanging these public keys, both parties can generate the shared secret key: Alice computes S=Bamod  pS = B^a \mod pS=Bamodp, and Bob computes S=Abmod  pS = A^b \mod pS=Abmodp. Due to the mathematical properties of modular arithmetic, both calculations result in the same shared secret SSS.  This shared secret can then be used for encryption, enabling Alice and Bob to communicate securely by encrypting their messages with a symmetric encryption algorithm. The strength of the Diffie-Hellman algorithm lies in its reliance on the discrete logarithm problem, which is computationally challenging to solve, thereby providing a secure means of key exchange. Additionally, the elliptic curve variant enhances security and efficiency, allowing for shorter key lengths while maintaining a high level of security, making it particularly suitable for resource-constrained environments. |
| **Output** |  |