|  |  |
| --- | --- |
| Semester | T.E. Semester VI – Computer Engineering |
| Subject | Cryptography and cyber security |
| Subject Professor In-charge | Prof. Amit Nerurkar |
| Assisting Teachers | Prof. Amit Nerurkar |
| Laboratory | M312B |

|  |  |
| --- | --- |
| Student Name | Deep Salunkhe |
| Roll Number | 21102A0014 |
| TE Division | A |

**Title:** Design and Implementation of Diffie Hellman Key Establishment



**Explanation:**

1. **Setup**: Both parties agree on two public parameters:
   * A large prime number *p*.
   * A primitive root *g* modulo *p*, which is an integer less than *p*.
2. **Private Key Generation**: Both Alice and Bob independently choose secret integers:
   * Alice selects a secret integer and keeps it private.
   * Bob selects a secret integer and keeps it private.
3. **Public Key Computation**: Both parties compute their public keys:
   * Alice calculates her public key by raising the base *g* to the power of her secret integer modulo *p*.
   * Bob calculates his public key by raising the base *g* to the power of his secret integer modulo *p*.
4. **Key Exchange**: Alice and Bob exchange their public keys over the insecure channel.
5. **Shared Secret Calculation**: Once both parties receive each other's public keys:
   * Alice computes the shared secret key by raising Bob's public key to the power of her secret integer modulo *p*.
   * Bob computes the shared secret key by raising Alice's public key to the power of his secret integer modulo *p*.
6. **Result**: Both Alice and Bob now possess the same shared secret key, which they can use for encryption and decryption purposes.

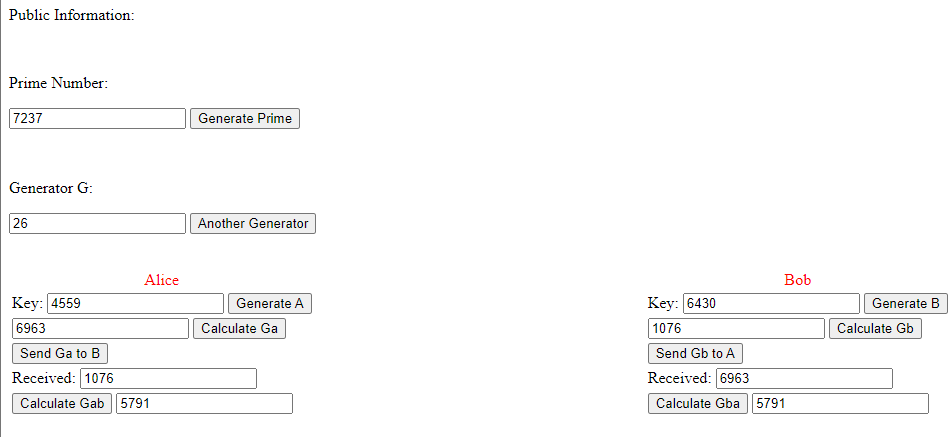
The security of the Diffie-Hellman key exchange relies on the computational difficulty of solving the discrete logarithm problem, making it practically infeasible for an eavesdropper to determine the shared secret key even if they intercept the exchanged public keys.



**Result:**

A screenshot of a computer

Description automatically generated





**Conclusion:**

In conclusion, the Diffie-Hellman key establishment protocol provides a secure method for two parties to establish a shared secret key over an insecure communication channel. By leveraging mathematical principles, specifically the difficulty of solving the discrete logarithm problem, Diffie-Hellman ensures that even if adversaries intercept the exchanged public keys, they cannot feasibly determine the shared secret key without knowledge of the private keys. This shared secret key can then be utilized for encryption, enabling secure communication between the parties. Overall, Diffie-Hellman plays a fundamental role in modern cryptography, serving as a cornerstone for secure communication protocols and encryption systems.