1. **Select Security Level :**

|  |  |
| --- | --- |
| **Security Level** | **Key Length(Bit)** |
| Level 1 | 512 |
| Level 2 | 1024 |
| Level 3 | 2048 |
| Level 4 | 4096 |

1. **Key Generation**

* Choose four large prime numbers p, q, r and s randomly and independently of each other. All primes should be of equivalent length.
* By using the database provided the values of n, m , phi, λ is decided
* .They are computed as
  + Compute n = p x q, m= r x s, phi = (p-1) x (q-1) and λ=(r-1) x (s-1).
  + Choose an integer *e*, 1 < e <phi, such that gcd (e,phi) = 1.
  + Compute the secret exponent *d*, 1 < d <phi, such that e x d mod phi=1.
  + Select an integer g=m+1.
  + Compute the modular multiplicative inverse: µ = µ-1 mod m.

1. **Index Exchange :**

* We now exchange Nid ,Mid, Eid ,Did, gid, λid (using Deffi-Hellmen)

1. **Encryption**
2. Retrieve the public key (n, m, g, e) from the database.
3. Encrypt the data by using the functions of BigInteger library.

That is c=g mesg^emod nx rm mod m2

1. **Decryption**
2. Retrieve the public key (d,µ, λ) from the database.
3. Decrypt the data by using the functions of bigInteger library.

That is m== (((cλ mod m2 – 1)/ m) xµmod m)dmod n.