SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING(IoT and Cybersecurity Including BCT)

COURSE NAME : Fundamentals Of Cryptography

II YEAR / III SEMESTER

Unit III-

Topic : Elagamal Algorithm

The El Gamal Algorithm provides an alternative to the RSA for public key encryption.

1) Security of the RSA depends on the (presumed) difficulty of factoring large integers.
2) 2) Security of the El Gamal algorithm depends on the (presumed) difficulty of computing discrete logs in a large prime modulus.

Idea of El Gamal cryptosystem:

Suppose Alice wants to communicate with Bob.

1.Bob generates public and private keys:

1. Bob chooses a very large number **q** and a cyclic group $\mathbf{F}_q$.
2. From the cyclic group $\mathbf{F}_q$, he choose any element **g** and an element **a** such that gcd(a, q) = 1.
3. Then he computes $h = g^a$.
4. Bob publishes **F**, $\mathbf{h = g^a}$, **q**, and **g** as his public key and retains **a** as private key.

2.Alice encrypts data using Bob's public key :

1. Alice selects an element **k** from cyclic group **F** such that gcd(k, q) = 1.
2. Then she computes $p = g^k$ and $s = h^k = g^{ak}$.
3. She multiples s with M.
4. Then she sends $(p, M*s) = (g^k, M*s)$.

3.Bob decrypts the message :

1. Bob calculates $s' = p^a = g^{ak}$.
2. He divides M*s by s' to obtain M as $s = s'$.

Advantages:

•**Security:** ElGamal is based on the discrete logarithm problem, which is considered to be a hard problem to solve. This makes it secure against attacks from hackers.

•**Key distribution:** The encryption and decryption keys are different, making it easier to distribute keys securely. This allows for secure communication between multiple parties.

•**Digital signatures:** ElGamal can also be used for digital signatures, which allows for secure authentication of messages.

Disadvantages:

•**Slow processing:** ElGamal is slower compared to other encryption algorithms, especially when used with long keys. This can make it impractical for certain applications that require fast processing speeds.

•**Key size:** ElGamal requires larger key sizes to achieve the same level of security as other algorithms. This can make it more difficult to use in some applications.

•**Vulnerability to certain attacks:** ElGamal is vulnerable to attacks based on the discrete logarithm problem, such as the index calculus algorithm. This can reduce the security of the algorithm in certain situations.