SNS COLLEGE OF TECHNOLOGY

Coimbatore-35
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 ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

19ITB302-Cryptography and Network Security

UNIT-2 NUMBER THEORY AND PUBLIC KEY CRYPTOSYSTEMS

RSA Algorithm

2. Encryption

To encrypt a message M, it is first converted to numerical representation using ASCII and other encoding schemes. Now, use the public key (n, e) to encrypt the message and get the cipher text using the formula:

C = Me mod n, where C is the Cipher text and e and n are parts of public key.

RSA Algorithm

3. Decryption

To decrypt the cipher text C, use the private key (n, d) and get the original data using the formula:

M = Cd mod n, where M is the message and d and n are parts of private key.

Idea behind RSA Algorithm

The idea of RSA is based on the fact that it is difficult to factorize a large integer. The Public Key is (n, e), where n and e are publicly known, while the Private Key is (n, d). Since only the receiver knows the value of d, only they can decrypt the message. But is it possible to find the value of d using n and e?

We know that (d * e) ≡ 1 mod Φ(n), so if we can calculate the value of Φ(n), we can find the value of d. But Φ(n) = (p – 1) * (q – 1). So, we need the value of p and q. Now, one might think that it's quite easy to find the value of p and q as n = p * q and n is already publicly known but RSA Algorithm takes the value of p and q to be very large which in turn makes the value of n extremely large and factorizing such a large value is computationally impossible.

Diffie-Hellman algorithm:

The Diffie-Hellman algorithm is being used to establish a shared secret that can be used for secret communications while exchanging data over a public network using the elliptic curve to generate points and get the secret key using the parameters.

For the sake of simplicity and practical implementation of the algorithm, we will consider only 4 variables, one prime P and G (a primitive root of P) and two private values a and b.

P and G are both publicly available numbers. Users (say Alice and Bob) pick private values a and b and they generate a key and exchange it publicly. The opposite person receives the key and that generates a secret key, after which they have the same secret key to encrypt.

Diffie-Hellman algorithm:

Step-by-Step explanation is as follows:

Alice	Bob
Public Keys available = P, G	Public Keys available = P, G
Private Key Selected = a	Private Key Selected = b
Key generated = $x=G^a \bmod P$	Key generated = $y=G^b \bmod P$

Diffie-Hellman algorithm

Exchange of generated keys takes place	
Key received = y	key received = x
Generated Secret Key = $k_a = y_a \bmod P$	Generated Secret Key = $k_b = x_b \bmod P$
Algebraically, it can be shown that $k_a = k_b$	

ElGamal Encryption Algorithm

Elgamal Cryptographic Algorithm

The ElGamal cryptographic algorithm is an asymmetric key encryption scheme based on the Diffie-Hellman key exchange. It was invented by Taher ElGamal in 1985. The algorithm is widely used for secure data transmission and has digital signatures and encryption applications. Here's an overview of its components and how it works:

Components of the ElGamal Algorithm

Key Generation:

Public Parameters: Select a large prime number p and a generator g of the multiplicative group Z*p.

Private Key: Select a private key x such that $1 \leq x \leq p-2$.

Public Key: Compute $h=g^x \bmod p$. The public key is (p,g,h) and the private key is x.

ElGamal Encryption Algorithm

- ncryption:
- To encrypt a message M:
- Choose a random integer k such that $1 \leq k \leq p-2$.
- Compute C1 = $g^k \bmod p$.
- Compute C2 = $M \cdot h^k \bmod p$.
- The ciphertext is (c1,c2).

ElGamal Encryption Algorithm

Decryption:

To decrypt the ciphertext (c1,c2) using the private key x:

Compute the shared secret s= Cx1 mod p.

Compute s−1 mod p (the modular inverse of s).

Compute the original message M = C2·s−1 mod p.

ElGamal Encryption Algorithm

Idea of ElGamal Cryptosystem

Suppose Alice wants to communicate with Bob.

- ✓ **Bob generates public and private keys:**
- ✓ **Bob chooses a very large number q and a cyclic group Fq.**
- ✓ **From the cyclic group Fq, he choose any element g and**
- ✓ **an element a such that gcd(a, q) = 1.**
- ✓ **Then he computes h = ga.**
- ✓ **Bob publishes F, h = ga, q, and g as his public key and retains an as a private key.**
- ✓ **Alice encrypts data using Bob's public key :**
- ✓ **Alice selects an element k from cyclic group F**
- ✓ **such that gcd(k, q) = 1.**
- ✓ **Then she computes p = gk and s = hk = gak.**
- ✓ **She multiples s with M.**
- ✓ **Then she sends (p, M*s) = (gk, M*s).**