Encryption Systems Report

Pavan Sekhar Naidu Routhu

Roll Number: 22B1028

Mentor: Siddharth Varma

June 2024

Contents

1 Introduction

In This report we are exploring mainly three encryption systems RSA,Paillier,elgamel

2 RSA

RSA (Rivest–Shamir–Adleman) is an asymmetric cryptographic algorithm widely used for secure communication. It involves the use of a public key for encryption and a private key for decryption. The security of RSA relies on the difficulty of factoring large prime numbers.

2.1 Key Generation

1. **Choose Primes**: Select two large prime numbers, p and q.
2. **Compute** n: Compute $n = p \times q$, where n is the modulus.
3. **Compute** $\phi(n)$: Calculate Euler's totient function $\phi(n) = (p-1)(q-1)$.
4. **Choose** e: Select an integer e such that $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$. e is the public exponent.
5. **Compute** d: Find d, the modular multiplicative inverse of e modulo $\phi(n)$, i.e., $d \equiv e^{-1} \pmod{\phi(n)}$. d is the private exponent.

2.2 Encryption

To encrypt a message M:

$$C \equiv M^e \pmod{n}$$

where C is the ciphertext.

2.3 Decryption

To decrypt the ciphertext C:

$$M \equiv C^d \pmod{n}$$

where M is the original message.

2.4 How it Works

$$C \equiv M^e \pmod{n}$$
$$c^d \equiv M^{ed} \pmod{n}$$
$$ed \equiv 1 \pmod{\phi(n)}$$
$$ed = 1 + k\phi(n)$$
$$c^d \equiv MM^{k\phi(n)} \pmod{n}$$
$$n = pq$$

m is relatively prime to both p and q as these prime numbers are very large prime numbers// from fermats little theorem

$$m^{p-1} \equiv 1 \pmod{p}$$

$$M^{\phi(n)} \equiv 1 \pmod{p} \quad \text{and} \quad M^{\phi(n)} \equiv 1 \pmod{q}$$

so

$$C \equiv m \pmod{p}$$

$$C \equiv m \pmod{q}$$

From chinese remainder theorem

$$C \equiv m \pmod{pq}$$

$$C \equiv m \pmod{n}$$

3 Paillier's Cryptosystem

The Paillier cryptosystem is a probabilistic asymmetric encryption scheme with homomorphic properties, proposed by Pascal Paillier in 1999. It consists of the following key components:

3.1 Key Generation

- Choose two large prime numbers, p and q.
- Compute $n = p \times q$.
- $\phi(n) = (p-1)(q-1)$
- **Public Key**: g where $g = n + 1$.
- **Private Key**: Derive μ such that $\mu = \phi(n)^{-1} \pmod{n}$, where $\phi(n)^{-1}$ is the modular inverse of $\phi(n)$ modulo n.

3.2 Encryption

To encrypt a message m:

$$c = g^m \cdot r^n \mod n^2$$

where r is a random integer in $\mathbb{Z}_n^*$.

3.3 Decryption

To decrypt the ciphertext c:

$$m = L(c^{\phi(n)} \mod n^2) \cdot \mu \mod n$$

where $L(x) = \frac{x-1}{n}$ and μ is the private key.

3.4 How it works

$$c^{\phi(n)} \mod n^2$$

$$c = g^m \cdot r^n \mod n^2$$

$$\phi(n^2) = \phi(pq^2) = pq(p-1)(q-1) = n\phi(n)$$

$$r^{n\phi(n)} \equiv 1 \mod n^2$$

$$c^{\phi(n)} \mod n^2 \equiv g^{m\phi(n)} \mod n^2$$

$$(n+1)^{m\phi(n)} = 1 + m\phi(n)n + ...n^2 + ... = (1 + m\phi(n)n) mod n^2$$

$$c^{\phi(n)} \mod n^2 \equiv (1 + m\phi(n)n) \mod n^2$$

$$d \equiv c^{\phi(n)} \mod n^2$$

$$d = 1 + m\phi(n)n - kn^2$$

$$\frac{d-1}{n} = m\phi(n) - kn$$

$$\frac{d-1}{n} = m\phi(n) \mod n$$

multiplying with e which is modular inverse of $\phi(n)$ modulo n.

$$\frac{d-1}{n} \times e = m \mod n$$

4 ElGamal Cryptosystem

The ElGamal cryptosystem is an asymmetric encryption algorithm named after its inventor Taher ElGamal. It consists of the following key components:

4.1 Key Generation

- **Prime Selection**: Choose a large prime number p.
- **Primitive Root**: Find a primitive root α modulo p.
- **Private Key**: Select a random integer a, where $1 \leq a \leq p-1$.
- **Public Key**: Compute $e = \alpha^a \mod p$.

4.2 Encryption

To encrypt a message m:

- Choose a random integer k, where $1 \leq k \leq p-2$.
- Compute $c_1 = \alpha^k \mod p$.
- Compute $c_2 = m \cdot e^k \mod p$.

The ciphertext is (c_1, c_2).

4.3 Decryption

To decrypt the ciphertext (c_1, c_2):

- Compute $m = (c_1)^{p-1-a} \cdot c_2 \mod p$

4.4 How it works

$$m = (c_1)^{p-1-a} \cdot c_2 \mod p$$
$$c_1^{p-1-a} \cdot c_2 \mod p = (\alpha^k)^{p-1-a} m \cdot e^k \mod p$$
$$c_1^{p-1-a} \cdot c_2 \mod p = (\alpha^{p-1})^k (\alpha^{-a})^k m \cdot (\alpha^a)^k \mod p$$
$$c_1^{p-1-a} \cdot c_2 \mod p = m \mod p$$