ElGamal Cryptosystem: A Study of Public-Key Encryption and Digital Signatures

Iman Ebrahimi, Oskar Emmerich

October 13, 2023

Abstract

This report presents an in-depth analysis of the ElGamal cryptosystem, a prominent public-key encryption algorithm developed by Taher ElGamal in 1985. This cryptographic system is widely employed for secure communication and digital signatures. The report delves into the theoretical underpinnings, key generation, encryption, and decryption processes, as well as the security aspects associated with the ElGamal cryptosystem.

Introduction

The ElGamal cryptosystem is a fundamental component of modern cryptography, offering both encryption and digital signature capabilities. This report aims to elucidate its mechanics and cryptographic principles.

Theoretical Background

Modular Exponentiation

The ElGamal cryptosystem leverages modular exponentiation, a mathematical operation vital to its encryption and decryption processes.

Discrete Logarithm Problem

Security in ElGamal hinges on the complexity of the discrete logarithm problem, which involves finding the exponent in modular arithmetic. The report explores the computational challenges associated with this problem.

Key Generation

Public Key Components

The key generation phase involves creating a public-private key pair. The public key consists of a prime number (p) and a primitive root modulo p (g). These

values are disclosed to all parties involved.

Private Key

The private key is composed of another prime number (x), which must remain confidential.

Encryption

In the ElGamal cryptosystem, the encryption process involves two main steps: selecting a random integer (k) and calculating the ciphertext components (C_1 and C_2).

Random Integer Selection

Before encrypting a message (M), the sender selects a random integer (k) from the set of integers modulo $p-1$, where p is a prime number and part of the recipient's public key. This random integer selection ensures that each encryption of the same message will produce different ciphertexts, enhancing security.

Encryption Process

Once the sender has chosen the random integer k, they proceed to calculate C_1 and C_2 as follows:

1. Calculate C_1: C_1 is the first component of the ciphertext and is computed as follows:

$$C_1 = g^k \mod p$$

Here, g is the primitive root modulo p, which is also part of the recipient's public key. p is a prime number, and k is the random integer selected by the sender.

2. Calculate C_2: C_2 is the second component of the ciphertext and is computed as follows:

$$C_2 = (M \cdot (y^k)) \mod p$$

In this equation: - M represents the plaintext message that the sender wishes to encrypt.

y is the recipient's public key, which is calculated as $y = g^x \mod p$, where x is the sender's private key. - k is the random integer selected by the sender. - p is the prime number that is part of the recipient's public key.

These two components, C_1 and C_2, together form the ciphertext, which can be sent securely to the recipient. When the recipient receives the ciphertext, they can use their private key to decrypt it and recover the original plaintext message (M).

This completes the encryption process in the ElGamal cryptosystem, which provides a secure way to send messages while keeping the recipient's private key confidential.

Decryption

The decryption phase requires the recipient to use their private key (x) to recover the original plaintext message (M). The following steps outline the mathematical operations involved in the decryption process.

1. Calculate S:

$$S = C_1^x \mod p$$

In this step: - C_1 is the first component of the ciphertext received from the sender. - x is the recipient's private key, which is a prime number.

2. Compute the modular multiplicative inverse of S:

$$S^{-1} = S^{-1} \mod p$$

Here, S^{-1} represents the modular multiplicative inverse of S modulo p. The modular multiplicative inverse is a crucial component of the decryption process, and it allows the recipient to recover the original random integer (k) used by the sender during encryption.

3. Calculate M:

$$M = (C_2 \cdot S^{-1}) \mod p$$

In this equation: - C_2 is the second component of the ciphertext received from the sender. - S^{-1} is the modular multiplicative inverse calculated in the previous step. - p is the prime number that is part of the recipient's private key.

After completing these steps, the recipient will have successfully decrypted the ciphertext and recovered the original plaintext message (M).

The decryption process in the ElGamal cryptosystem is reliant on the recipient's private key to perform the necessary mathematical operations to obtain the original message. This ensures that only the intended recipient, who possesses the private key, can decrypt and access the confidential information sent by the sender.

Proof that Decryption Works

The decryption process in the ElGamal cryptosystem allows for the recovery of the original plaintext message (M) because of the following congruence:

$$C_1^{-x} \cdot C_2 \equiv g^{-kx} \cdot (M \cdot (y^k)) \equiv g^{-kx} \cdot M \cdot (g^x)^k \equiv M \cdot (g^{-kx} \cdot g^{kx}) \equiv M \pmod{p}.$$

In this congruence:

- C_1 and C_2 are the components of the ciphertext received from the sender.
- x is the recipient's private key.
- k is the random integer used by the sender during encryption.
- g is the primitive root modulo p from the recipient's public key.

- M is the plaintext message to be recovered.
- y is the recipient's public key, computed as $y = g^x \mod p$.

The congruence shows that, when the recipient applies the decryption algorithm, the original plaintext message M can be successfully recovered, as demonstrated by the congruence equality ($\equiv M \pmod{p}$).

References

- Elementary Number Theory: David M. Burton.
- Handbook of Applied Cryptography, by A. Menezes, P. van Oorschot, and S. Vanstone, CRC Press, 1996.