Review of Public Key Cryptography

Chibuogwu Victor Chukwuemeka
200551029

Department of Mathematics
Faculty of Science
Lagos State University

September 2024

Project Overview

A project submitted to the Department of Mathematics, Faculty of Science, Lagos State University, in partial fulfilment of the requirement for the award of Bachelor of Science Degree (B.Sc HONS.) in Mathematics.

Certification

I certify that this project work with the title *REVIEW OF PUBLIC KEY CRYPTOGRAPHY* submitted by CHIBUOGWU, VICTOR CHUKWUEMEKA with matriculation number **200551029** was carried out under my supervision in the Department of Mathematics, Faculty of Science, Lagos State University, Ojo, Lagos.

....

Dr. AbdulKareem A.O.
Supervisor

Abstract

This work presents the use case of Public Key encryption, discussing in detail the models and methods for encryption and decryption. It also illustrates the algorithms of each method, providing examples to solve unconstrained problems.

INTRODUCTION

Public Key Cryptography (PKC), introduced by Whitfield Diffie and Martin Hellman in 1976, revolutionized secure communication by addressing the challenge of key distribution. Unlike traditional symmetric key cryptography, PKC uses a pair of mathematically related keys: a public key for encryption and a private key for decryption. This dual-key system has enabled the development of secure communication protocols and digital signatures, among other applications.

Background of the Study

Since its inception, PKC has undergone significant development. Major algorithms like RSA (Rivest-Shamir-Adleman), DSA (Digital Signature Algorithm), and ECC (Elliptic Curve Cryptography) have been introduced to address various cryptographic challenges. These algorithms are characterized by their computational efficiency, security against attacks, and suitability for different applications. The security of PKC relies on the difficulty of mathematical problems such as factoring large integers or solving discrete logarithm problems in finite fields.

Statement of Problem

Despite its advantages, PKC faces several challenges:

- **Key Management:** Generating, distributing, and storing keys securely.
- **Computational Efficiency:** Ensuring encryption and decryption operations are fast and scalable.
- **Vulnerabilities:** Addressing vulnerabilities such as side-channel attacks, quantum computing threats, and implementation errors.

The primary aim of this study is to provide a comprehensive examination of public key cryptography from a mathematical perspective. The specific objectives include:

- **Historical Development:** Tracing the historical development and evolution of public key cryptography.
- **Mathematical Principles:** Explaining the mathematical principles underlying key generation, encryption, and decryption.
- **Real-World Applications:** Evaluating the effectiveness of public key cryptographic systems in various real-world applications.
- **Security Analysis:** Identifying and analyzing major security threats and vulnerabilities associated with public key cryptography.
- **Future Directions:** Suggesting potential improvements and future research directions.

Significance of the Study

This study advances our understanding of the mathematical foundations of public key cryptography, provides insights into real-world applications and challenges, and guides policymakers in understanding and regulating cryptographic technologies.

Scope of the Study

The study comprehensively examines public key cryptography, including its theoretical foundations, development from inception to current technologies, real-world applications in secure communication, digital signatures, blockchain, and challenges such as key management and performance optimization. Future directions include post-quantum cryptography. Symmetric key cryptography is covered only for context or comparison.

Definition of Terms

- **Public Key Cryptography (PKC):** A cryptographic system that uses two keys—a public key for encryption and a private key for decryption.
- **RSA (Rivest-Shamir-Adleman):** A widely used PKC algorithm based on the difficulty of factoring large integers.
- **Digital Signature:** A mathematical scheme for verifying the authenticity and integrity of digital messages or documents.
- **Elliptic Curve Cryptography (ECC):** A PKC algorithm based on the properties of elliptic curves over finite fields.
- **Key Exchange:** The process of securely exchanging cryptographic keys between parties.

LITERATURE REVIEW

Mathematical Principles of Public Key Cryptography Public Key Cryptography is built upon several fundamental mathematical principles:

- **Number Theory:** PKC algorithms rely on prime factorization and discrete logarithms.
- **Modular Arithmetic:** Modular arithmetic is used in PKC algorithms to perform operations within finite sets of integers.
- **Group Theory:** Group theory concepts like cyclic groups define cryptographic primitives.
- **Complexity Theory:** The security of PKC relies on computationally hard problems such as factoring large integers or solving discrete logarithm problems.

Key Generation

In RSA, each user generates a pair of keys: a public key and a private key. The public key consists of two components: the modulus n and the public exponent e. The private key consists of n and the private exponent d. The security of RSA is based on the difficulty of factoring the modulus n into its prime factors.

Encryption and Decryption

- To encrypt a message m, the sender uses the recipient's public key (n, e) to compute $c = m^e \mod n$.
- To decrypt the ciphertext c, the recipient uses their private key (n, d) to compute $m = c^d \mod n$.

Example Encrypting $M = 123$:

$$C = 123^{17} \mod 3233 = 855$$

Decrypting $C = 855$:

$$M = 855^{2753} \mod 3233 = 123$$

ECC uses elliptic curves defined by the equation $y^2 = x^3 + ax + b$ over finite fields. It offers equivalent security to RSA but with smaller key sizes, making it suitable for constrained environments such as mobile devices and IoT.

Key Generation

- Select an elliptic curve E defined over a finite field F_p.
- Choose a base point G on the curve E with a large prime order n.
- Select a random integer d as the private key such that $1 < d < n - 1$.
- Compute the public key $Q = dG$, where G is the base point.

Encryption and Decryption

- **Encryption:** To encrypt a message M (represented as a point on the curve), the sender computes the ciphertext pair (C_1, C_2), where $C_1 = kG$ and $C_2 = M + kQ$.
- **Decryption:** The recipient recovers the message M by computing $M = C_2 - dC_1$ using their private key d.

Pairing-Based Cryptography

Definition Pairing is a bilinear map defined over elliptic curve subgroups. Let G_1, G_2, and G_T be groups of the same prime order q. A bilinear map $e : G_1 \times G_2 \to G_T$ satisfies the following properties:

- **Bilinearity:** For all $(S, T) \in G_1 \times G_2$ and for all $a, b \in \mathbb{Z}$, we have $e(aS, bT) = e(S, T)^{ab}$.
- **Non-degeneracy:** $e(S, T) = 1$ for all $T \in G_2$ if and only if $S = 1$.
- **Computability:** For all $(S, T) \in G_1 \times G_2$, $e(S, T)$ is efficiently computable.

Consequences of Pairings Pairings have important consequences on the hardness of certain variants of the Diffie-Hellman problem. For instance, symmetric pairings lead to a strict separation between the intractability of the computational Diffie-Hellman problem and the hardness of the corresponding decision problem.

Method of Study

RSA Cryptosystem The RSA cryptosystem is based on the difficulty of factoring large prime numbers. The steps for key generation, encryption, and decryption are described as follows:

- Choose two distinct prime numbers p and q.
- Compute $N = pq$ and the totient $\phi(N) = (p-1)(q-1)$.
- Choose an integer e such that $1 < e < \phi(N)$ and e is coprime with $\phi(N)$.
- Compute d as the modular multiplicative inverse of e mod $\phi(N)$.

The public key is (e, N), and the private key is (d, N).

Elliptic Curve Cryptography ECC is based on the algebraic structure of elliptic curves over finite fields. The security of ECC relies on the difficulty of the elliptic curve discrete logarithm problem.

The RSA algorithm relies on the difficulty of factoring large composite numbers. The key steps are outlined below.

Key Generation

Given two large prime numbers p and q, we compute:

$$N = p \times q$$

where N is the modulus. Next, calculate Euler's totient function:

$$\phi(N) = (p - 1) \times (q - 1)$$

Choose an integer e such that:

$$1 < e < \phi(N) \quad \text{and} \quad \gcd(e, \phi(N)) = 1$$

The public key is (N, e). To generate the private key, compute d as the modular inverse of e modulo $\phi(N)$:

$$d \times e \equiv 1 \mod \phi(N)$$

The private key is (N, d).

Decryption

Given a plaintext message M, the ciphertext C is computed using the public key (N, e):

$$C = M^e \mod N$$

To decrypt the ciphertext C, the recipient uses their private key (N, d) to recover the original message M:

$$M = C^d \mod N$$

Example

Let $p = 61$ and $q = 53$. First, compute:

$$N = 61 \times 53 = 3233$$

Next, calculate:

$$\phi(N) = (61 - 1) \times (53 - 1) = 3120$$

Choose $e = 17$, which is coprime to $\phi(N)$. Now, compute d, the modular inverse of $17 \mod 3120$, which gives $d = 2753$.
For encryption, given $M = 123$, calculate:

$$C = 123^{17} \mod 3233 = 855$$

To decrypt, calculate:

$$M = 855^{2753} \mod 3233 = 123$$

Thus, the encryption and decryption process works as expected.

Elliptic Curve Definition

ECC is based on the algebraic structure of elliptic curves over finite fields. The security of ECC relies on the difficulty of solving the elliptic curve discrete logarithm problem (ECDLP).
An elliptic curve E over a finite field F_p is defined by the equation:

$$y^2 = x^3 + ax + b \mod p$$

where $4a^3 + 27b^2 \neq 0 \mod p$, ensuring the curve has no singularities.

Key Generation

- Select a finite field F_p and an elliptic curve E defined over F_p.
- Choose a base point G on the curve E with large prime order n.
- Select a random integer d (the private key) such that $1 < d < n - 1$.
- Compute the public key $Q = d \times G$, where G is the base point on the curve.

Encryption

To encrypt a message M (represented as a point on the curve), the sender chooses a random integer k and computes the ciphertext pair (C_1, C_2):

$$C_1 = k \times G$$

$$C_2 = M + k \times Q$$

Decryption

To decrypt the ciphertext (C_1, C_2), the recipient uses their private key d to recover the original message:

$$M = C_2 - d \times C_1$$

Example

Consider the elliptic curve $y^2 = x^3 + x + 1$ over F_{89}, and let the base point be $G = (2, 22)$. Suppose the private key is $d = 10$. The public key is:

Pairing-Based Cryptography

Pairing-based cryptography relies on bilinear maps, enabling applications like identity-based encryption.

Mathematical Definition of Pairing

Let G_1 and G_2 be cyclic groups of prime order q, and let G_T be a multiplicative group of the same order. A pairing is a bilinear map:

$$e : G_1 \times G_2 \to G_T$$

satisfying the following properties:

- **Bilinearity:** For all $P \in G_1$, $Q \in G_2$, and $a, b \in \mathbb{Z}_q$:

$$e(aP, bQ) = e(P, Q)^{ab}$$

- **Non-degeneracy:** $e(P, Q) = 1$ if and only if $P = 1$ or $Q = 1$.
- **Computability:** The pairing $e(P, Q)$ can be computed efficiently.

Example of Pairing

Let $P \in G_1$ and $Q \in G_2$. The pairing $e(P, Q)$ can be computed using Miller's algorithm or the Tate pairing, depending on the elliptic curve used.

RSA Encryption and Decryption

The following code demonstrates how to encrypt and decrypt a message using RSA keys:

```python
from Crypto.Cipher import PKCS1_OAEP
from Crypto.PublicKey import RSA
from Crypto.Random import get_random_bytes

# RSA Encryption
def rsa_encrypt(message, public_key_path='public_key.pem'):
    with open(public_key_path, 'rb') as pub_file:
        public_key = RSA.import_key(pub_file.read())
    cipher_rsa = PKCS1_OAEP.new(public_key)
    encrypted_message = cipher_rsa.encrypt(message.encode('utf-8'))
    return encrypted_message

# RSA Decryption
def rsa_decrypt(encrypted_message, private_key_path='private_key.pem'):
    with open(private_key_path, 'rb') as priv_file
```

ECC Key Generation

ECC provides security with smaller key sizes. Here's the Python code for ECC key generation:

```python
from ecdsa import SigningKey, SECP256k1

# Generate ECC key pair
def generate_ecc_keys():
    private_key = SigningKey.generate(curve=SECP256k1)
    public_key = private_key.get_verifying_key()

    with open('ecc_private_key.pem', 'wb') as priv_file:
        priv_file.write(private_key.to_pem())

    with open('ecc_public_key.pem', 'wb') as pub_file:
        pub_file.write(public_key.to_pem())

    print("ECC Keys Generated and Saved.")
```

Summary

This project explores the applications of cryptographic techniques, specifically RSA and Elliptic Curve Cryptography (ECC), in secure communication. The project examines the theoretical foundations of RSA and ECC and investigates their real-world applications, highlighting RSA's role in securing web traffic through SSL/TLS, authenticating sender identities via digital signatures (PGP), and validating software updates. Additionally, the project discusses ECC's efficiency benefits in mobile devices, IoT devices, smart cards, and cryptocurrency (Bitcoin, blockchain). The project demonstrates the significance of cryptographic techniques in ensuring secure communication and provides insights into their practical applications. Overall, the project showcases the importance of RSA and ECC in maintaining secure communication in various industries and technologies.

Conclusion

This study has provided an in-depth exploration of RSA, Elliptic Curve Cryptography (ECC), and Pairing-Based Cryptography. Each method was explored mathematically with examples provided to illustrate their applications in cryptography. These methods play critical roles in ensuring the security and privacy of digital communications, and understanding their mathematical foundations is essential for implementing secure cryptographic systems., making it applicable to a broader class of problems.

References

Diffie 1976 Diffie, W., & Hellman, M. (1976). *New Directions in Cryptography*. IEEE Transactions on Information Theory, 22(6), 644-654.

Kannan 1969 Kannan, R. (1969). *Some Results on Fixed Points*. Bulletin of the Calcutta Mathematical Society, 61(1), 71-76.

Rivest 1978 Rivest, R. L., Shamir, A., & Adleman, L. (1978). *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*. Communications of the ACM, 21(2), 120-126.