ITSE306
Cryptpgraphic and Computer System security

Course Report about:

Public Key Cryptography
and
The Knapsack Cryptosystem

Pro. Omar Abosadaa

Report of Student:
Sanad AlArousi 2181801442
Group 3 Green

Table of Contents

1. Introduction

Cryptography is fundamental to securing digital communication in today's interconnected world. Among its various types, public key cryptography stands out due to its innovative use of asymmetric keys for encryption and decryption. This report delves into public key cryptography, exploring its core concepts, popular algorithms, and a notable yet historically significant cryptosystem, the knapsack cryptosystem.

2. Public Key Cryptography

Overview

Public key cryptography, also known as asymmetric cryptography, utilizes two keys: a public key for encryption and a private key for decryption. Unlike symmetric cryptography, where the same key is used for both processes, this method enhances security by separating the keys.

Key Concepts

- **Public Key:** Known to everyone and used to encrypt data.
- **Private Key:** Kept secret and used to decrypt data encrypted with the corresponding public key.
- **Encryption:** Converting plaintext into ciphertext using a public key.
- **Decryption:** Converting ciphertext back into plaintext using a private key.
- **Digital Signatures:** Verifying the authenticity and integrity of a message. The sender encrypts a hash of the message with their private key, creating a signature that the recipient can verify using the sender's public key.

Popular Public Key Cryptosystems

RSA (Rivest-Shamir-Adleman)

RSA is based on the difficulty of factoring large composite numbers. It involves:

- **Key Generation:** Selecting two large prime numbers and computing their product.
- **Encryption:** Using the public key to transform plaintext into ciphertext.
- **Decryption:** Using the private key to revert ciphertext back to plaintext.

Elliptic Curve Cryptography (ECC)

ECC uses the algebraic structure of elliptic curves over finite fields, providing equivalent security to RSA but with smaller key sizes, making it more efficient.

3. The Knapsack Cryptosystem

Historical Context

The knapsack cryptosystem, one of the earliest public key cryptosystems, is based on the subset sum problem, an NP-complete problem. Although initially promising, it was later found to be vulnerable to certain attacks.

Key Generation

- **Superincreasing Sequence:** Choose a sequence S=(s1,s2,...,sn)S = (s_1, s_2, ..., s_n)S=(s1,s2,...,sn) where each element is greater than the sum of all previous elements.
- **Modulus and Multiplier:** Select a large integer NNN and a multiplier MMM such that gcd(M,N)=1\gcd(M, N) = 1gcd(M,N)=1.
- **Public Key Sequence:** Compute P=(p1,p2,...,pn)P = (p_1, p_2, ..., p_n)P=(p1,p2,...,pn) where pi=si×Mmod Np_i = s_i \times M \mod Npi =si×MmodN.

Encryption Process

- **Binary Vector:** Convert the plaintext message into a binary vector b=(b1,b2,...,bn)b = (b_1, b_2, ..., b_n)b=(b1,b2,...,bn).
- **Ciphertext:** Compute the ciphertext C=∑i=1nbi×piC = \sum_{i=1}^{n} b_i \times p_iC=∑i=1nbi×pi.

Decryption Process

- **Modular Inversion:** Compute C′=C×M−1mod NC' = C \times M^{-1} \mod NC′=C×M−1modN, where M−1M^{-1}M−1 is the modular inverse of Mmod NM \mod NMmodN.
- **Subset Sum:** Use the superincreasing sequence SSS to solve the subset sum problem for C′C'C′ and retrieve the original binary vector bbb.

4. Security Analysis

Strengths and Weaknesses

Initially, the knapsack cryptosystem appeared secure due to the complexity of the subset sum problem. However, weaknesses emerged, particularly with the advent of polynomial-time attacks. In contrast, modern cryptosystems like RSA and ECC offer robust security through well-understood mathematical foundations.

Known Attacks

- **Shamir's Attack:** Adi Shamir demonstrated a polynomial-time attack on the knapsack cryptosystem, significantly undermining its security.
- **Other Attacks:** Further research uncovered additional vulnerabilities, making it less viable compared to RSA and ECC.

5. Applications

Secure Communication

Public key cryptography ensures the confidentiality and integrity of data transmitted over networks, crucial for secure online transactions and communications.

Digital Signatures

Digital signatures provide a mechanism to verify the authenticity of digital messages and documents, preventing forgery and tampering.

Key Exchange

Secure key exchange mechanisms, like Diffie-Hellman, facilitate the secure exchange of cryptographic keys over an insecure channel, forming the basis for many secure communication protocols.

6. Conclusion

Public key cryptography revolutionized the field of cryptography, enabling secure communication and digital signatures. While the knapsack cryptosystem played a pivotal historical role, modern cryptosystems like RSA

and ECC dominate due to their superior security. Continuous advancements in cryptographic research remain crucial for protecting information in our digital age.

7. References

- 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.
- Koblitz, N. (1987). Elliptic curve cryptosystems. Mathematics of Computation, 48(177), 203-209.
- Shamir, A. (1982). A polynomial-time algorithm for breaking the basic Merkle-Hellman cryptosystem. IEEE Transactions on Information Theory, 29(2), 245-247.
- Stallings, W. (2017). Cryptography and Network Security: Principles and Practice. Pearson.