Computer Security week 4

Khaula Molapo

1.

In today’s digital age, sensitive information such as financial records, medical data, and personal communications must remain secure. Imagine an online banking platform where customers frequently transfer funds, view statements, and pay bills. Without cryptography, attackers could intercept usernames, passwords, and account balances during transmission. To prevent this, the bank applies cryptographic techniques such as encryption and digital signatures. Data is encrypted before leaving the user’s device, ensuring only the intended server can decrypt it. Similarly, the server signs its responses to prove authenticity and avoid tampering. If a hacker attempted a man-in-the-middle attack, they would face unreadable ciphertext. This process ensures confidentiality, integrity, and authentication in every transaction. For example, when a customer sends payment instructions, encryption prevents outsiders from reading the details, while signing ensures the bank can verify the sender’s identity. Cryptography transforms vulnerable online transactions into secure, trusted exchanges between user and institution.

2.

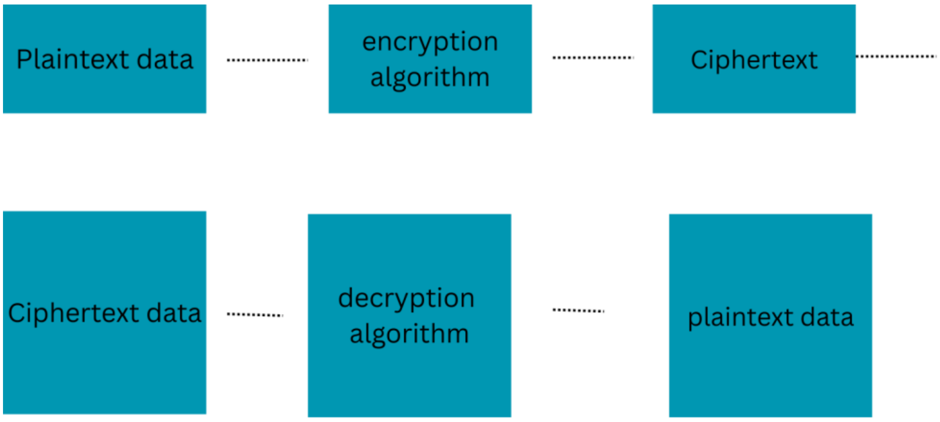
RSA is one of the most widely used public-key cryptography algorithms. It relies on the mathematical difficulty of factoring large prime numbers. In RSA, two keys are generated: a public key for encryption and a private key for decryption. This separation allows secure communication, as anyone can encrypt data using the public key, but only the private key holder can decrypt it. RSA also supports digital signatures, where the private key is used to sign a message, and the public key is used to verify authenticity. Its role is vital in securing online transactions, SSL/TLS certificates, and encrypted communications.

3.

I experimented with encrypting a text file using OpenSSL. First, I generated a symmetric key and applied AES encryption on the file. The result was ciphertext that could not be understood without the key. I then tested decryption, which restored the original file. This exercise showed me how encryption adds a protective layer against unauthorized access. Even if someone intercepted the file, they would not be able to read its contents without the correct key. The process highlighted how command-line tools like OpenSSL can make real-world cryptography both practical and accessible for securing data efficiently.

4.

The encryption workflow diagram created in Canva illustrates the key steps of securing a message. First, the sender takes plaintext data and applies an encryption algorithm with a public key, producing ciphertext. This ciphertext is transmitted across the network. On the receiver's side, the ciphertext is decrypted using the private key, restoring the original plaintext. The diagram also includes optional steps like digital signing to ensure authenticity. By showing arrows for data flow and labeling each stage, the diagram makes it easy to understand how cryptography protects data confidentiality and integrity during communication, ensuring safe exchanges in digital systems.


Plaintext data
encryption algorithm
Ciphertext
Ciphertext data
decryption algorithm
plaintext data