📄 Task 6: Introduction to Cryptography

By : NROUPSINH GOHIL

Deliverable: Cryptography Experiment Report

🔐 Objective

To understand basic cryptography concepts including encryption, hashing, digital signatures, and their real-world usage using OpenSSL.

🧩 Concepts Learned

1. Symmetric Encryption

- Uses **one secret key** for both encryption and decryption.
- Fast and efficient for large data.
- Example algorithm: **AES**

2. Asymmetric Encryption

- Uses **two keys**: public key and private key.
- Public key encrypts data, private key decrypts it.
- Example algorithm: **RSA**

🛠️ Practical Experiments Performed

🔒 AES File Encryption

- A text file was encrypted using **AES-256** with OpenSSL.
- The same password was used to decrypt the file successfully.
- This demonstrated **symmetric encryption**.

🔑 RSA Key Generation

- Generated a **2048-bit RSA private key**.
- Extracted the corresponding **public key**.
- Demonstrated **asymmetric encryption** and key separation.

✍️ Digital Signature (Concept)

- Message is hashed first.
- Hash is encrypted using sender's **private key** to create a digital signature.
- Receiver verifies it using sender's **public key**.

- Ensures **authentication and integrity**.

🔍 **Hashing & Integrity Check**

- Generated **SHA-256 hash** of a file.
- After modifying the file, hash value changed.
- Proved that hashing detects data tampering.

🌐 **Real-World Applications**

- **HTTPS** uses RSA for key exchange and AES for data encryption.
- **VPNs** use encryption to protect data over public networks.
- Hashing ensures file and message integrity.
- Digital signatures verify software and sender authenticity.

🎯 **Outcome**

This task provided a strong foundation in cryptography fundamentals, including encryption methods, hashing, digital signatures, and their real-world security applications.

📁 **Files Used**

- secret.txt
- secret.enc
- decrypted.txt
- private_key.pem
- public_key.pem