Cyber Security Internship Report

Cyber Security Internship – Task 6

Introduction to Cryptography – Experiment Report

Submitted by: Hetal Antala

Date : 23 / 01 / 2026

1. Introduction

Cryptography is the foundation of modern cybersecurity. It is used to protect sensitive data, ensure secure communication, and maintain data integrity. This task focuses on understanding cryptographic concepts such as encryption, hashing, and digital signatures through practical experiments using OpenSSL.

2. What is Encryption?

Encryption is the process of converting readable data (plaintext) into an unreadable format (ciphertext) to prevent unauthorized access. Only authorized users with the correct key can decrypt the data..

3. Symmetric vs Asymmetric Encryption

3.1 Symmetric Encryption

- Uses the same key for encryption and decryption
- Faster and efficient
- Example: AES

3.2 Asymmetric Encryption

- Uses a public key and a private key
- More secure for key exchange
- Example: RSA

---

4. Symmetric Encryption Using AES

In this experiment, AES-256 encryption was performed using OpenSSL.

Steps Performed

- A plaintext file was created
- The file was encrypted using AES-256
- The encrypted file was decrypted using the same password

Observation

The decrypted file matched the original plaintext, proving successful encryption and decryption.

---

5. Asymmetric Encryption Using RSA

- RSA encryption was demonstrated by generating cryptographic keys.

Steps Performed

- Generated a 2048-bit private key
- Generated a public key from the private key

Observation

- The public key can be shared, while the private key must be kept secret to ensure security.

---

6. Hashing and Integrity Verification

Hashing was performed using the SHA-256 algorithm.

Steps Performed

- Generated a hash of a plaintext file
- Re-generated the hash to verify integrity

Observation

The hash value remained unchanged, confirming that the file was not modified.

7. Digital Signature

Digital signatures were used to ensure authenticity and integrity.

Steps Performed

- Signed a file using the private key
- Verified the signature using the public key

Observation

Successful verification confirmed the authenticity of the file.

---

8. Real-World Applications of Cryptography

- **HTTPS:** Secure web communication
- **VPN:** Encrypted network tunnels
- **Digital Certificates:** Identity verification
- **Blockchain:** Hashing and digital signatures

---

9. Importance of Cryptography

- Protects sensitive data
- Ensures privacy
- Prevents data tampering
- Builds trust in digital systems

10. Conclusion

This task provided hands-on experience with cryptographic techniques using OpenSSL. Understanding encryption, hashing, and digital signatures is essential for securing data and communication in real-world cybersecurity environments.