Cyber Security Internship – Task 6

Introduction to Cryptography

1. Introduction

Cryptography is the practice of securing data using encryption, hashing, and digital signatures to ensure confidentiality, integrity, and authenticity.

2. Symmetric Encryption

Symmetric encryption uses the same key for encryption and decryption. AES is a commonly used symmetric algorithm.

Example: AES-256 encryption using OpenSSL.

3. Asymmetric Encryption

Asymmetric encryption uses a public key and a private key. RSA is a widely used asymmetric algorithm.

Public key encrypts data, and private key decrypts it.

4. Hashing

Hashing converts data into a fixed-length value. Hashes are used to verify file integrity.

SHA-256 produces a unique hash for a file.

5. Digital Signature

A digital signature ensures authenticity and integrity. It confirms that data has not been modified and verifies the sender.

6. Comparison of Encryption Algorithms

Feature	Symmetric	Asymmetric
Keys	Single key	Public & Private
Speed	Fast	Slower
Usage	File encryption	Key exchange

7. Real-World Usage

- HTTPS
- VPNs
- Secure file storage
- Email security

8. Conclusion

This task provided hands-on experience with cryptography fundamentals using OpenSSL.