Cyber Security Internship – Task 6 Report

Title: Introduction to Cryptography

Objective: The objective of this task is to understand cryptography fundamentals including encryption, hashing, digital signatures, and real-world usage.

Tools Used:
Primary Tool: OpenSSL
Alternative Tool: CyberChef

Theory:
Cryptography is the practice of securing information by converting it into unreadable format. Encryption protects data confidentiality, hashing ensures integrity, and digital signatures provide authentication and non-repudiation.

Symmetric Encryption: Uses a single secret key for encryption and decryption. Example: AES. It is fast and suitable for large data.

Asymmetric Encryption: Uses public and private key pairs. Example: RSA. It is used for secure key exchange and authentication.

Hashing: Hashing converts data into a fixed-length value. It is irreversible and used for data integrity verification.

Digital Signature: Digital signatures ensure authenticity and integrity of data using hashing and asymmetric encryption.

Real-World Applications: HTTPS, VPNs, Email Security, Disk Encryption, and Secure Authentication.

Conclusion: This task helped in gaining strong foundational knowledge of cryptography and its real-world importance in cybersecurity.