CYBER SECURITY INTERNSHIP – TASK 6

Introduction to Cryptography

Name: Anshu
Domain: Cyber Security

1. Introduction
Cryptography is the practice of securing information by converting readable data into an unreadable format.
It ensures confidentiality, integrity, authentication, and non-repudiation.

2. Symmetric vs Asymmetric Encryption

Symmetric Encryption:
Uses a single key for encryption and decryption.
Example: AES (Advanced Encryption Standard).
It is fast and suitable for encrypting large files.

Asymmetric Encryption:
Uses two keys – Public key and Private key.
Example: RSA.
It is mainly used for secure key exchange and digital signatures.

3. AES Encryption Experiment

A text file named "secret.txt" was created and encrypted using AES-256-CBC via OpenSSL.
Command used:
openssl enc -aes-256-cbc -salt -in secret.txt -out secret.enc

The file was decrypted using:
openssl enc -aes-256-cbc -d -in secret.enc -out decrypted.txt

This demonstrated symmetric encryption and decryption.

4. RSA Key Generation

Private key generated using:
openssl genrsa -out private.pem 2048

Public key extracted using:
openssl rsa -in private.pem -pubout -out public.pem

This demonstrated asymmetric encryption fundamentals.

5. Digital Signature

A file was digitally signed using:
openssl dgst -sha256 -sign private.pem -out signature.bin secret.txt

Signature verification performed using:
openssl dgst -sha256 -verify public.pem -signature signature.bin secret.txt

Digital signatures ensure authenticity and integrity.

6. Hashing and Integrity

SHA-256 hash generated using:
openssl dgst -sha256 secret.txt

If the file changes, the hash value changes, proving integrity verification.

7. Comparison of Algorithms

AES – Symmetric, fast, used for file encryption.
RSA – Asymmetric, used for secure communication.
SHA-256 – Hash function, used for integrity.

8. Real-World Applications

HTTPS uses RSA for key exchange and AES for encryption.
VPNs use encryption to secure communication channels.
Digital certificates use asymmetric cryptography.

9. Conclusion

This experiment provided practical understanding of encryption, hashing, digital signatures, and cryptographic fundamentals.