

## **Day 90**

### **Topic: Cryptography**

**Objective:** To understand encryption, hashing, and PKI (Public Key Infrastructure).

#### **Theoretical Concepts:**

We distinguished between Symmetric Encryption (AES, DES) and Asymmetric Encryption (RSA, ECC). We discussed Hashing (MD5, SHA-256) and its use in integrity verification. We also covered Digital Signatures.

#### **Practical Work:**

We used **OpenSSL** to generate RSA private/public key pairs. We encrypted a text file with the public key and decrypted it with the private key. We also used hashing tools to generate checksums of files and verified them to detect tampering.

**Tools Used:** OpenSSL, Hashing Tools.

**Outcome:** Practical knowledge of how to secure data at rest and in transit.