# ELEVATE LABS (CYBER SECURITY INTERNSHIP)

# Task 6: Introduction to Cryptography

## 1. Symmetric vs Asymmetric Encryption

Symmetric encryption uses the same key for both encryption and decryption. It is fast and efficient but key sharing is difficult.

Asymmetric encryption uses two keys: a public key for encryption and a private key for decryption. It is more secure for key exchange but slower.

## 2. Encrypting Files Using AES

AES (Advanced Encryption Standard) is a symmetric encryption algorithm.

It is commonly used to encrypt files and data because it is fast and secure.

The same secret key is required to encrypt and decrypt the file.

## 3. Generating RSA Keys

RSA is an asymmetric encryption algorithm.

It uses a pair of keys called public key and private key.

RSA keys are generated using cryptographic tools and are used for secure communication and key exchange..

## 4. Digital Signatures

A digital signature is used to verify the authenticity and integrity of data.

It is created using the sender’s private key and verified using the public key.

Digital signatures ensure that the data is not modified and comes from a trusted source.

## 5. Hashing Files and Verifying Integrity

Hashing converts file data into a fixed-length value.

When a file is hashed before and after transmission, matching hash values confirm integrity.

Hashing is used to detect unauthorized changes.

## 6. Comparison of Encryption Algorithms

Symmetric algorithms like AES are fast and suitable for large data.

Asymmetric algorithms like RSA are slower but useful for secure key exchange.

Each algorithm is used based on security and performance requirements.

## 7. Real-World Usage of Encryption

Encryption is widely used in technologies such as HTTPS and VPNs.

HTTPS secures web communication, while VPNs protect network traffic.

Encryption ensures confidentiality and secure data transfer.

## 8. Documentation of Findings

The study shows that encryption is essential for data security.

Different encryption methods serve different purposes.

Proper use of encryption ensures confidentiality, integrity, and authenticity of data.