Task 6: Introduction to Cryptography

Introduction

Cryptography is the science of securing information by converting it into an unreadable format to prevent unauthorized access. It ensures confidentiality, integrity, authentication, and non-repudiation of data.

Objectives

- Understand symmetric and asymmetric encryption
- Encrypt files using AES
- Generate RSA keys
- Verify data integrity using hashing
- Understand digital signatures

Tools Used

Primary Tool: OpenSSL
Alternative Tool: CyberChef

Symmetric Encryption (AES)

AES uses a single shared key for encryption and decryption. It is fast and secure.
Command used:

```
openssl enc -aes-256-cbc -salt -in secret.txt -out secret.enc
```

Asymmetric Encryption (RSA)

RSA uses public and private keys for secure communication.
Commands used:

```
openssl genrsa -out private.pem 2048
openssl rsa -in private.pem -pubout -out public.pem
```

Hashing and Integrity

SHA-256 hashing ensures file integrity.

```
openssl dgst -sha256 secret.txt
```

Digital Signatures

Digital signatures ensure authenticity and integrity.

```
openssl dgst -sha256 -sign private.pem -out signature.bin secret.txt
```

Real World Usage

- HTTPS
- VPN
- Digital Certificates
- Secure Password Storage

Conclusion

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