Practical 3 Cryptography

*1. Hashing :-

-> Hashing ensures data integrity by generating a fixed-size string (hash) for any input. Tools like md5sum, sha256sum, or openssl are commonly used.

Generate an MD5 hash.

```
echo "Hello, Parul Students" | md5sum
9508049ecefe74d74400cf41bb0c1333 -
```

Generate a SHA-256 hash

```
echo "Hello, Parul Students" | sha256sum
11bfde1655e72a6956ce936911c5c807f610e44200f27386
9ba0444ba686177 -
```

Step-3 See the plain text file and encrypted file:

plain text file:

```
$cat plaintext.file
this is my secret file.
this is my secret.
```

encrypted file:

```
$cat encrypted.txt
Salted__ ♦N@..<b{`♦v♦#♦ P0♦ )N♦♦
```

Step-4 Decrypt a file using OpenSSL

```
$ openssl enc -d -aes-256-cbc -in encrypted.txt
  -out decrypted.txt.

enter AES-256-CBC decryption password:
12345
```

Step-5 See the encrypted file and decrypted file:

encrypted file:

```
$ cat encrypted.txt
Salted__ ♦N@..<b{`♦v♦#♦ P0♦ )N♦♦
```

decrypted file:

```
cat decrypted.txt
this is my secret file.
this is my secret.
```

Step-3 See the plain text file and encrypted file:

plain text file:

```
$cat plaintext.file
this is my secret file.
this is my secret.
```

encrypted file:

```
$cat encrypted.txt
Salted__ ♦N@..<b{`♦v♦#♦ P0♦ )N♦♦
```

Step-4 Decrypt a file using OpenSSL

```
$openssl enc -d -aes-256-cbc -in encrypted.txt
 -out decrypted.txt.

enter AES-256-CBC decryption password:
12345
```

Step-5 See the encrypted file and decrypted file:

encrypted file:

```
$ cat encrypted.txt
Salted__ ♦N@..<b{`♦v♦#♦ P0♦ )N♦♦
```

decrypted file:

```
cat decrypted.txt
this is my secret file.
this is my secret.
```