**Week 7**

**1. Write a program to implement a Hash function.**

def simple\_hash(text):

h = 0

for char in text:

h = (h + ord(char)) % 256

return h

print("Hash:", simple\_hash("CyberSecurity"))

**2. Write a program to implement BlowFish algorithm.**

from Crypto.Cipher import Blowfish

from Crypto.Random import get\_random\_bytes

from Crypto.Util.Padding import pad, unpad

key = get\_random\_bytes(16)

cipher = Blowfish.new(key, Blowfish.MODE\_ECB)

data = b"SecretMsg123"

ciphertext = cipher.encrypt(pad(data, Blowfish.block\_size))

print("Encrypted:", ciphertext)

decipher = Blowfish.new(key, Blowfish.MODE\_ECB)

decrypted = unpad(decipher.decrypt(ciphertext), Blowfish.block\_size)

print("Decrypted:", decrypted)

**3. Write a program to implement TwoFish algorithm.**

from Crypto.Cipher import Twofish

key = b'ThisIsA16ByteKey'

cipher = Twofish.new(key, Twofish.MODE\_ECB)

plaintext = b"CyberSec1234567"

ciphertext = cipher.encrypt(plaintext)

print("Encrypted:", ciphertext)

decrypted = cipher.decrypt(ciphertext)

print("Decrypted:", decrypted)

**4. Implement the Diffie-Hellman Key Exchange scheme.**

# Publicly shared prime and base

p = 23

g = 5

# Alice

a = 6

A = (g \*\* a) % p

# Bob

b = 15

B = (g \*\* b) % p

# Shared secret

secret\_A = (B \*\* a) % p

secret\_B = (A \*\* b) % p

print("Shared Secret (Alice):", secret\_A)

print("Shared Secret (Bob):", secret\_B)

**5. Calculate the message digest of a text using the SHA-1 algorithm.**

import hashlib

text = "CyberSecurity"

hash\_obj = hashlib.sha1(text.encode())

print("SHA-1 Digest:", hash\_obj.hexdigest())