Cryptographic Techniques - Python Programs

# 4. Caesar Cipher

def caesar\_cipher(text, shift):  
 result = ""  
 for char in text:  
 if char.isalpha():  
 base = ord('A') if char.isupper() else ord('a')  
 result += chr((ord(char) - base + shift) % 26 + base)  
 else:  
 result += char  
 return result  
  
message = "HelloWorld"  
shift = 3  
encrypted = caesar\_cipher(message, shift)  
decrypted = caesar\_cipher(encrypted, -shift)  
  
print("Encrypted:", encrypted)  
print("Decrypted:", decrypted)

# 5. Vernam Cipher

def vernam\_cipher(message, key):  
 encrypted = ''.join([chr(ord(m) ^ ord(k)) for m, k in zip(message, key)])  
 return encrypted  
  
message = "HELLO"  
key = "XMCKL" # Must be the same length as message  
  
encrypted = vernam\_cipher(message, key)  
decrypted = vernam\_cipher(encrypted, key)  
  
print("Encrypted:", encrypted)  
print("Decrypted:", decrypted)

# 6. Hash Code using SHA256

import hashlib  
  
message = "SecureMessage"  
hash\_object = hashlib.sha256(message.encode())  
hash\_code = hash\_object.hexdigest()  
  
print("SHA256 Hash:", hash\_code)

# 7. Rail Fence Technique

def rail\_fence\_encrypt(text):  
 rail1 = text[::2]  
 rail2 = text[1::2]  
 return rail1 + rail2  
  
def rail\_fence\_decrypt(cipher):  
 half = (len(cipher) + 1) // 2  
 rail1 = cipher[:half]  
 rail2 = cipher[half:]  
 result = ""  
 for i in range(half):  
 result += rail1[i]  
 if i < len(rail2):  
 result += rail2[i]  
 return result  
  
message = "HELLOWORLD"  
encrypted = rail\_fence\_encrypt(message)  
decrypted = rail\_fence\_decrypt(encrypted)  
  
print("Encrypted:", encrypted)  
print("Decrypted:", decrypted)

# 8. Simple Columnar Transposition

def columnar\_encrypt(message, key):  
 key\_order = sorted(list(key))  
 columns = ['' for \_ in range(len(key))]  
  
 for i, char in enumerate(message):  
 col = i % len(key)  
 columns[col] += char  
  
 encrypted = ''  
 for k in key\_order:  
 index = key.index(k)  
 encrypted += columns[index]  
  
 return encrypted  
  
message = "HELLOCRYPTO"  
key = "4312567"  
encrypted = columnar\_encrypt(message, key)  
print("Encrypted:", encrypted)