Experiment No. 6

6.1 Aim:

To study and demonstrate **Forensic Tools of the Trade: Encrypting and Decrypting Files** using simple text files to understand how encryption ensures confidentiality and decryption restores original data.

Example Scenario:
You are working as a student intern in a digital forensics training lab. Your instructor has given you a set of plain text files containing short confidential messages. To protect these messages, you must apply a simple encryption technique using Notepad. Later, you decrypt the same file to verify whether the original message can be recovered successfully.

This activity helps in understanding how encryption secures information and how decryption restores it for forensic analysis.

Tasks:

1. Open a text file in Notepad and write a sample secret message.
2. Apply a simple encryption method.
3. Save the encrypted text in a new file.
4. Open the encrypted file and perform decryption to get back the original message.
5. Document the encryption and decryption steps with screenshots or notes.

6.2 Lab Outcome:

- Learned how to encrypt and decrypt files using simple forensic tools.
- Understood how encryption ensures confidentiality and integrity of digital evidence.

6.3 Learning Objectives:

- To understand how encryption protects files from unauthorized access.
- To learn the process of encrypting and decrypting files using forensic tools.

- To demonstrate the importance of secure key management in digital forensics.

6.4 Requirement:

Hardware:

- Desktop or Laptop system (for investigation)
- USB flash drive (for testing)

Software Tools:

- File encryption/decryption tool
- Text editor (Notepad for creating sample evidence file)
- Internet connection

6.5 Related Theory:

- **Encryption:** Conversion of readable data (plaintext) into unreadable form (ciphertext) using an algorithm and key.
- **Decryption:** Conversion of ciphertext back into plaintext using the correct key.

In Digital Forensics:

- Encryption secures evidence files so that only authorized investigators can access them.
- This ensures **confidentiality, integrity, and proper chain of custody** of digital evidence.

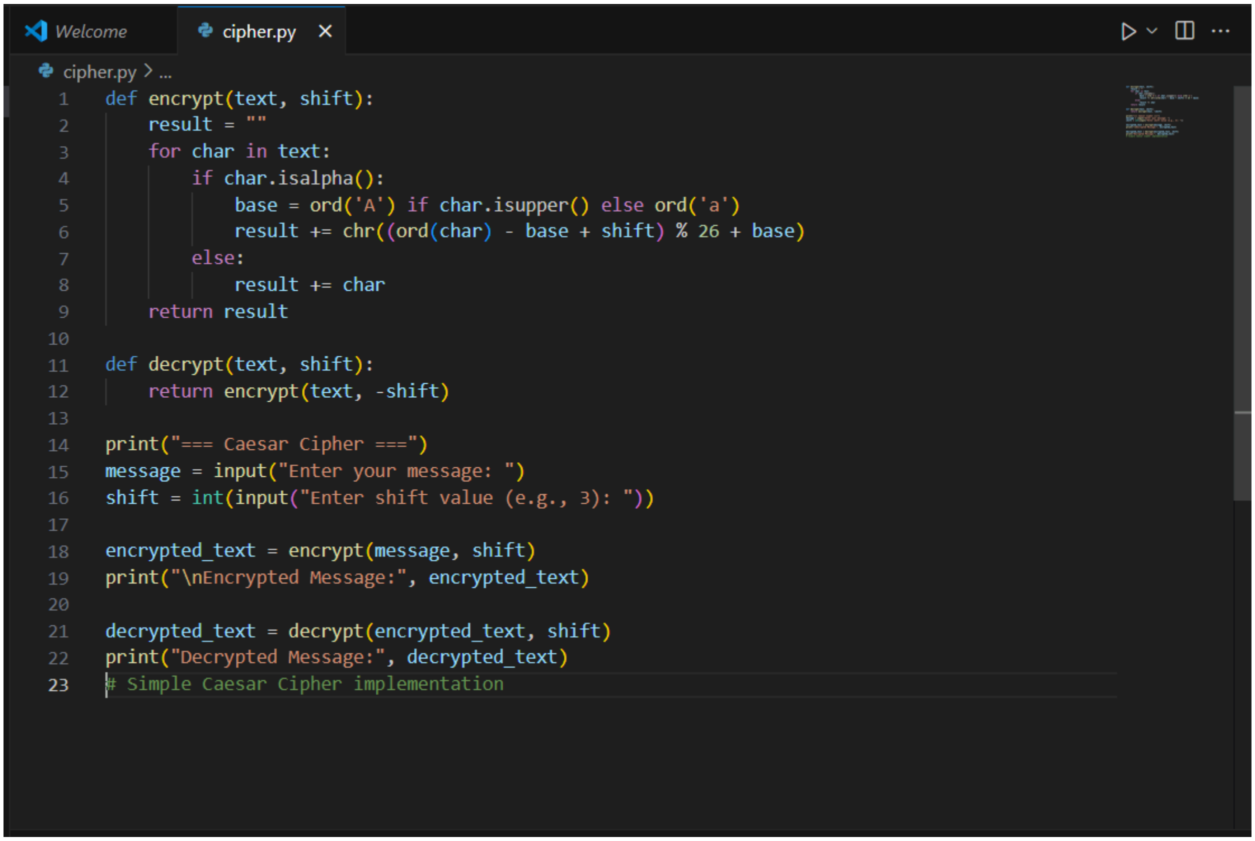
Types of Encryption:

- **Symmetric Encryption:** Same key is used for encryption and decryption (e.g., AES).
- **Asymmetric Encryption:** Public key for encryption and private key for decryption (e.g., RSA).

Key Management:

- Secure storage and handling of keys is critical.
- Losing the key = losing access to the data.

6.6 Output:



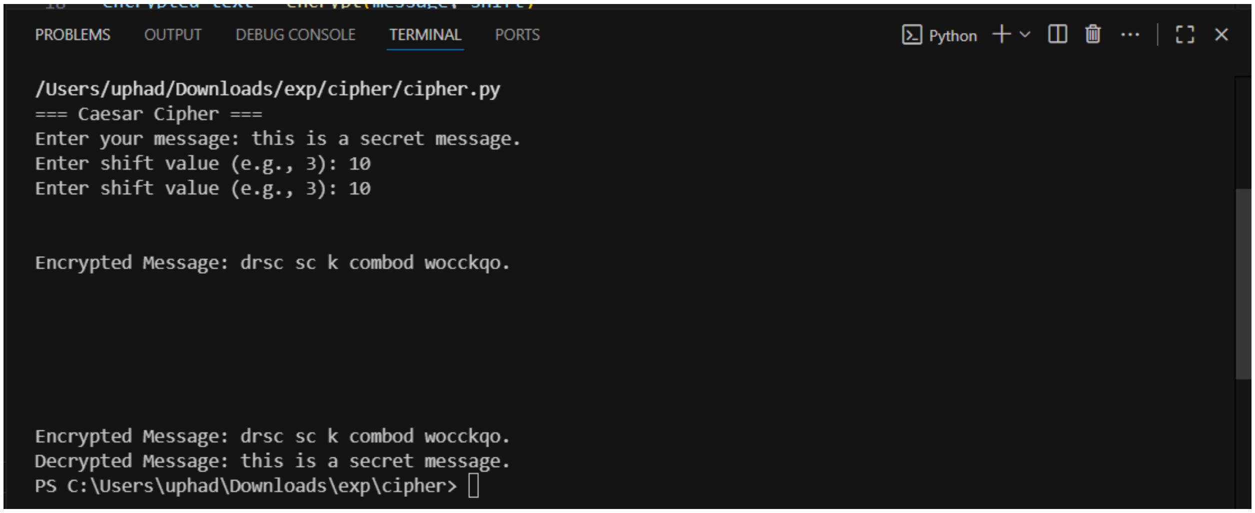
```python
def encrypt(text, shift):
    result = ""
    for char in text:
        if char.isalpha():
            base = ord('A') if char.isupper() else ord('a')
            result += chr((ord(char) - base + shift) % 26 + base)
        else:
            result += char
    return result

def decrypt(text, shift):
    return encrypt(text, -shift)

print("=== Caesar Cipher ===")
message = input("Enter your message: ")
shift = int(input("Enter shift value (e.g., 3): "))

encrypted_text = encrypt(message, shift)
print("\nEncrypted Message:", encrypted_text)

decrypted_text = decrypt(encrypted_text, shift)
print("Decrypted Message:", decrypted_text)
# Simple Caesar Cipher implementation
```



```
/Users/uphad/Downloads/exp/cipher/cipher.py
=== Caesar Cipher ===
Enter your message: this is a secret message.
Enter shift value (e.g., 3): 10
Enter shift value (e.g., 3): 10


Encrypted Message: drsc sc k combod wocckqo.





Encrypted Message: drsc sc k combod wocckqo.
Decrypted Message: this is a secret message.
PS C:\Users\uphad\Downloads\exp\cipher> 
```

6.7 Conclusion:

The experiment demonstrated how simple encryption and decryption can protect sensitive data.

- Encryption secured the confidential message from unauthorized access.
- Decryption successfully restored the original message, proving the process reliable.
- In digital forensics, proper use of encryption ensures **confidentiality, integrity, and trustworthiness of digital evidence**.