Nama : Fazar Rizwanul Ikhlas

NPM : 20123065

Kelas : C.2.23

Kriptografi Pertemuan 2

A. Aktivitas Praktikum

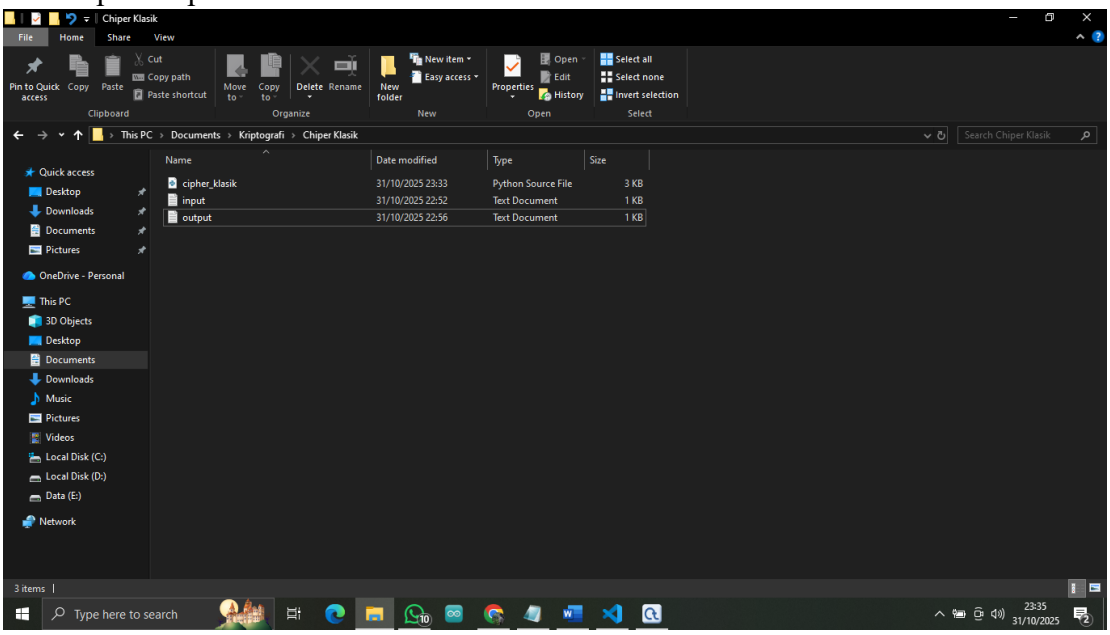
1. Implementasikan dua cipher klasik menggunakan Python.

```python
# ====================================================
# Praktikum Kriptografi 02 - Implementasi Cipher Klasik
# Implementasi Caesar dan Vigenère Cipher dengan File I/O
# ====================================================

# --- Caesar Cipher ---
def caesar_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 caesar_decrypt(cipher, shift):
    return caesar_encrypt(cipher, -shift)


# --- Vigenère Cipher ---
def vigenere_encrypt(plain, key):
    key = key.upper()
    result = ''
    for i, char in enumerate(plain.upper()):
        if char.isalpha():
            shift = ord(key[i % len(key)]) - 65
            result += chr((ord(char) - 65 + shift) % 26 + 65)
        else:
            result += char
    return result

def vigenere_decrypt(cipher, key):
    key = key.upper()
    result = ''
    for i, char in enumerate(cipher.upper()):
        if char.isalpha():
            shift = ord(key[i % len(key)]) - 65
            result += chr((ord(char) - 65 - shift) % 26 + 65)
        else:
            result += char
    return result

print("=== Praktikum Kriptografi 02 ===")
print("Implementasi Caesar & Vigenère Cipher\n")

# Membaca teks dari file input.txt
try:
    with open('input.txt', 'r') as f:
        text = f.read().strip()
except FileNotFoundError:
    print("⚠ File 'input.txt' tidak ditemukan. Buat file input.txt terlebih dahulu.")
    exit()

print(f"Teks Asli   : {text}")

# Parameter
shift = 3               # nilai geser untuk Caesar
key = "LEMON"           # kunci untuk Vigenere

# Proses Caesar Cipher
caesar_cipher = caesar_encrypt(text, shift)
caesar_plain = caesar_decrypt(caesar_cipher, shift)

# Proses Vigenere Cipher
vigenere_cipher = vigenere_encrypt(text, key)
vigenere_plain = vigenere_decrypt(vigenere_cipher, key)

print("\n=== Hasil Caesar Cipher ===")
print(f"Ciphertext : {caesar_cipher}")
print(f"Dekripsi   : {caesar_plain}")

print("\n=== Hasil Vigenère Cipher ===")
print(f"Kunci      : {key}")
print(f"Ciphertext  : {vigenere_cipher}")
print(f"Dekripsi    : {vigenere_plain}")

with open('output.txt', 'w') as f:
    f.write("=== Caesar Cipher ===\n")
    f.write(f"Ciphertext: {caesar_cipher}\n")
    f.write(f"Dekripsi: {caesar_plain}\n\n")
    f.write("=== Vigenère Cipher ===\n")
    f.write(f"Kunci: {key}\n")
    f.write(f"Ciphertext: {vigenere_cipher}\n")
    f.write(f"Dekripsi: {vigenere_plain}\n")

print("\n✅ Hasil enkripsi dan dekripsi telah disimpan ke 'output.txt'")

```

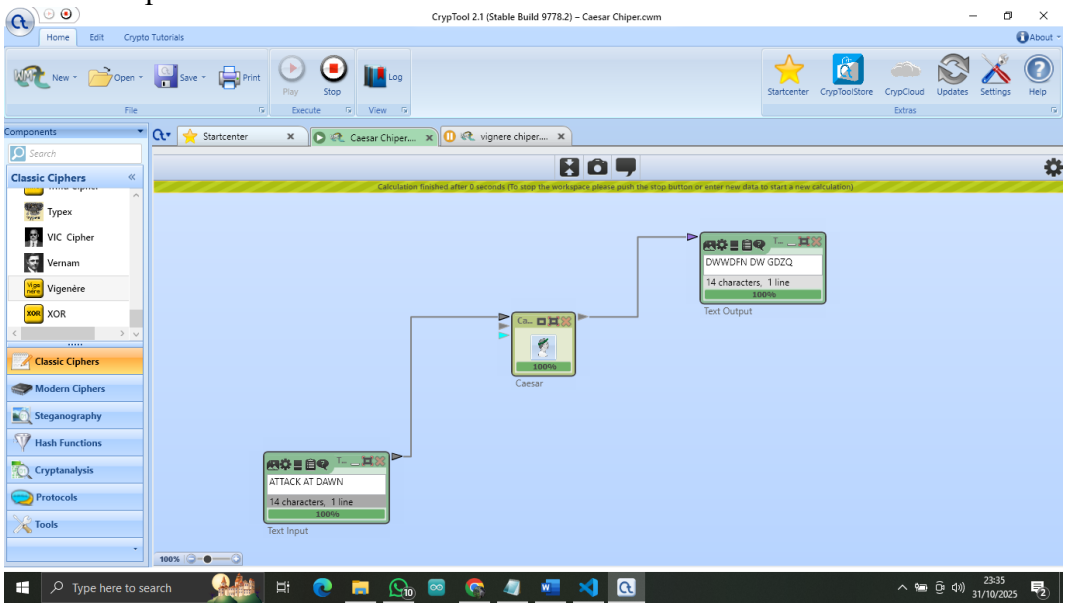
Hasil :

```
(base) C:\Users\LENOVO\Documents\Kriptografi\Chiper Klasik>python cipher_klasik.py
=== Praktikum Kriptografi 02 ===
Implementasi Caesar & Vigenère Cipher

Teks Asli   : ATTACK AT DAWN

=== Hasil Caesar Cipher ===
Ciphertext : DWWDFN DW GDZQ
Dekripsi   : ATTACK AT DAWN

=== Hasil Vigenère Cipher ===
Kunci       : LEMON
Ciphertext  : LXFOPV MH OEIB
Dekripsi    : ATTACK AT DAWN

✅ Hasil enkripsi dan dekripsi telah disimpan ke 'output.txt'

(base) C:\Users\LENOVO\Documents\Kriptografi\Chiper Klasik>
```

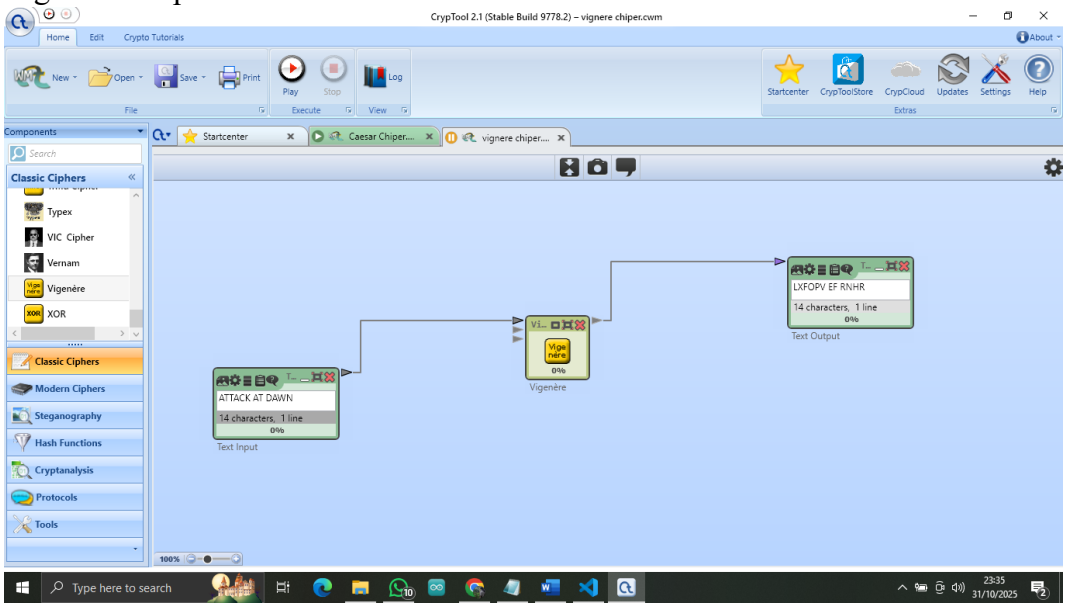
2. Buat input/output file teks



3. Bandingkan hasilnya dengan CrypTool atau CyberChef.
   - Caesar Chiper



   - Vigenère Chiper



B. Tugas Mini

1. Buat Program Sederhana yang:
   - Menerapkan Caesar & Vigenère Cipher.
   - Mampu enkripsi dan dekripsi otomatis.
   - Menyimpan hasil ke file .txt.

a. Alat dan Bahan

1) Perangkat lunak:
   - Python 3.12
   - Code Editor (VS Code)
2) Perangkat keras:
   - Laptop/PC dengan OS Windows
3) File:
   - cipher_tugasmini.py
   - input.txt
   - output.txt (Otomatis ada setelah Program dijalankan)

b. Langkah Kerja/Prosedur

1) Membuat file input.txt berisi beberapa plaintext berbeda.
2) Menulis program Python untuk:
   - Implementasi Caesar & Vigenère Cipher
   - Enkripsi dan dekripsi otomatis
   - Penyimpanan hasil ke output.txt
3) Menjalanan program di terminal dengan perintah:
   python cipher_tugasmini.py
4) Memeriksa hasil pada file output.txt

c. Hasil dan Pembahasan

1) Program sederhana menggunakan Python

```python
# ====================================================
# Tugas Mini - Kriptografi 02
# Implementasi Caesar & Vigenère Cipher (Enkripsi & Dekripsi Otomatis)
# ====================================================

# --- Caesar Cipher ---
def caesar_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 caesar_decrypt(cipher, shift):
    return caesar_encrypt(cipher, -shift)


# --- Vigenère Cipher ---
def vigenere_encrypt(plain, key):
    key = key.upper()
    result = ''
    for i, char in enumerate(plain.upper()):
        if char.isalpha():
            shift = ord(key[i % len(key)]) - 65
            result += chr((ord(char) - 65 + shift) % 26 + 65)
        else:
            result += char
    return result

def vigenere_decrypt(cipher, key):
    key = key.upper()
    result = ''
    for i, char in enumerate(cipher.upper()):
        if char.isalpha():
            shift = ord(key[i % len(key)]) - 65
            result += chr((ord(char) - 65 - shift) % 26 + 65)
        else:
            result += char
    return result


# ====================================================
# Program Utama
# ====================================================

print("=== Tugas Mini Kriptografi 02 ===")
print("Implementasi Caesar & Vigenère Cipher\n")

# Baca input dari file
try:
    with open('input.txt', 'r') as f:
        lines = [line.strip() for line in f.readlines() if line.strip()]
except FileNotFoundError:
    print("⚠️ File 'input.txt' tidak ditemukan.")
    exit()

# Parameter Cipher
shift = 3
key = "LEMON"

# Siapkan file output
with open('output.txt', 'w') as f:
    f.write("=== Hasil Tugas Mini Kriptografi 02 ===\n\n")

    # Proses tiap baris teks dari file input
    for i, text in enumerate(lines, start=1):
        f.write(f"Plaintext [{i}]: {text}\n")

        # Caesar Cipher
        c_cipher = caesar_encrypt(text, shift)
        c_plain = caesar_decrypt(c_cipher, shift)
        f.write(f"  Caesar Encrypt : {c_cipher}\n")
        f.write(f"  Caesar Decrypt : {c_plain}\n")

        # Vigenere Cipher
        v_cipher = vigenere_encrypt(text, key)
        v_plain = vigenere_decrypt(v_cipher, key)
        f.write(f"  Vigenère Key   : {key}\n")
        f.write(f"  Vigenère Encrypt : {v_cipher}\n")
        f.write(f"  Vigenère Decrypt : {v_plain}\n\n")

print("✅ Proses selesai! Hasil tersimpan di 'output.txt'")
```

Hasil:

```
C:\Users\LENOVO\Documents\Kriptografi\Tugas Mini>C:/Users/LENOVO/miniforge3/Scripts/activate

(base) C:\Users\LENOVO\Documents\Kriptografi\Tugas Mini>conda activate base

(base) C:\Users\LENOVO\Documents\Kriptografi\Tugas Mini>python cipher_tugasmini.py
=== Tugas Mini Kriptografi 02 ===
Implementasi Caesar & Vigenère Cipher

✅ Proses selesai! Hasil tersimpan di 'output.txt'

(base) C:\Users\LENOVO\Documents\Kriptografi\Tugas Mini>
```

2) Isi input.txt

input - Notepad

File Edit Format View Help

```
CRYPTOGRAPHY IS FUN
KEEP THE SECRET SAFE
PYTHON MAKES IT SIMPLE
```

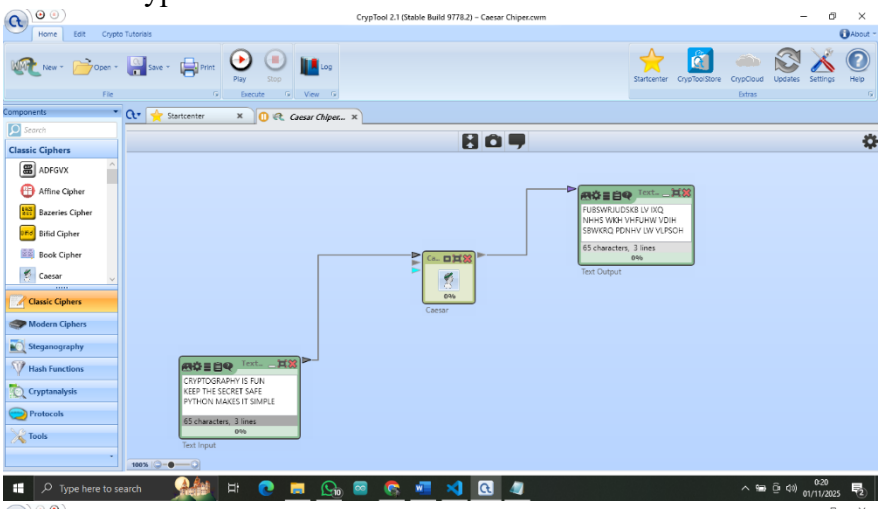
3) Output Program

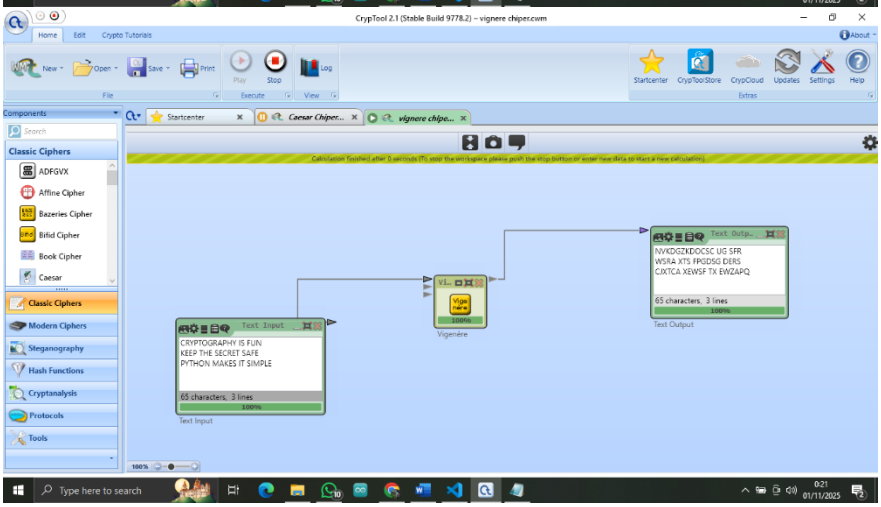
output - Notepad

File Edit Format View Help

```
=== Hasil Tugas Mini Kriptografi 02 ===

Plaintext [1]: CRYPTOGRAPHY IS FUN
  Caesar Encrypt : FUBSWRJUDSKB LV IXQ
  Caesar Decrypt : CRYPTOGRAPHY IS FUN
  Vigenère Key   : LEMON
  Vigenère Encrypt : NVKDGZKDOCSC WF JGB
  Vigenère Decrypt : CRYPTOGRAPHY IS FUN

Plaintext [2]: KEEP THE SECRET SAFE
  Caesar Encrypt : NHHS WKH VHFUHW VDIH
  Caesar Decrypt : KEEP THE SECRET SAFE
  Vigenère Key   : LEMON
  Vigenère Encrypt : VIQD ELQ FPGDSG WMTR
  Vigenère Decrypt : KEEP THE SECRET SAFE

Plaintext [3]: PYTHON MAKES IT SIMPLE
  Caesar Encrypt : SBWKRQ PDNHV LW VLPSOH
  Caesar Decrypt : PYTHON MAKES IT SIMPLE
  Vigenère Key   : LEMON
  Vigenère Encrypt : ACFVBY YOXPW WG WUACWI
  Vigenère Decrypt : PYTHON MAKES IT SIMPLE
```

4) Hasil di Cryptool





5) Analisis
   - Pada Caesar Cipher, setiap huruf bergeser +3 posisi (A→D, B→E)
   - Pada Vigenère Cipher, pola enkripsi bergantung pada kunci "LEMON", sehingga hasil lebih bervariasi.
   - Keduanya mampu melakukan proses enkripsi dan dekripsi secara otomatis.
   - Hasil dekripsi sama dengan plaintext awal → program berjalan dengan benar.
6) Kesimpulan

   Berdasarkan hasil implementasi, dapat disimpulkan bahwa Caesar Cipher dan Vigenère Cipher dapat diterapkan menggunakan Python dengan baik. Keduanya mampu melakukan proses enkripsi dan dekripsi otomatis serta menyimpan hasil ke file teks. Meskipun sederhana, cipher klasik ini menjadi dasar penting untuk memahami cipher modern seperti AES dan RSA.