Cryptography Programming Exercise

I chose the Caesar Cipher algorithm from the blog. Here's the Python program that takes a short piece of text and encrypts it. Additionally, it can read a text file, encrypt its contents, and save the encrypted text as another file. python Copy Edit

Users > george.koridze > Desktop > Essex > SSD > ePortfolio > Unit8 > Caesar_Cypher.py > ...

```python
import os

def caesar_cipher_encrypt(text, shift):
    """
    Encrypts text using Caesar Cipher with a given shift.
    :param text: The plain text to encrypt.
    :param shift: Number of positions to shift the alphabet.
    :return: Encrypted text.
    """
    encrypted_text = ""
    for char in text:
        if char.isalpha():
            start = ord('A') if char.isupper() else ord('a')
            encrypted_text += chr((ord(char) - start + shift) % 26 + start)
        else:
            encrypted_text += char
    return encrypted_text


def encrypt_file(input_file, output_file, shift):
    """
    Encrypts the contents of a file and saves the encrypted version.
    :param input_file: Path to the input text file.
    :param output_file: Path to save the encrypted file.
    :param shift: Shift value for Caesar Cipher.
    """
    if not os.path.exists(input_file):
        print(f"Error: {input_file} not found!")
        return

    with open(input_file, 'r') as file:
        plaintext = file.read()

    encrypted_text = caesar_cipher_encrypt(plaintext, shift)

    with open(output_file, 'w') as file:
        file.write(encrypted_text)

    print(f"Encrypted text saved to {output_file}")


```

```python
# Example usage
if __name__ == "__main__":
    print("Caesar Cipher Encryption")

    # Encrypt user-provided text
    sample_text = input("Enter the text to encrypt: ")
    shift_value = int(input("Enter the shift value (integer): "))
    encrypted = caesar_cipher_encrypt(sample_text, shift_value)
    print(f"Encrypted Text: {encrypted}")

    # Encrypt a file
    input_path = "sample.txt"  # Replace with your text file path
    output_path = "encrypted_sample.txt"  # Output file
    encrypt_file(input_path, output_path, shift_value)

```

Output:

```
george.koridze@MBP-GK-QQXJPGK7P4 unit8 % /usr/local/bin/python3 /Users/george.koridze/Desktop/Essex/SSD/ePortfolio/Unit8/Caesar_Cypher.py
Caesar Cipher Encryption
Enter the text to encrypt: Hello!
Enter the shift value (integer): 3
Encrypted Text: Khoor!
Error: sample.txt not found!
```

Answers:

1. Why did you select the algorithm you chose?

I selected the **Caesar Cipher** because:

- It is a foundational encryption method and easy to implement.
- It demonstrates the concept of substitution encryption effectively.
- Though simple, it provides an opportunity to explore encryption and its implementation in Python.

2. Would it meet the GDPR regulations? Justify your answer.

The **Caesar Cipher does not meet GDPR requirements** because:

- GDPR requires encryption methods that ensure a high level of data security. Caesar Cipher is highly insecure and vulnerable to brute-force attacks or frequency analysis.
- It lacks the robustness of modern encryption algorithms like AES (Advanced Encryption Standard) or RSA.
- Caesar Cipher is primarily used for educational purposes or low-security requirements.

To comply with GDPR, stronger encryption like AES-256 should be employed, as it meets industry standards for protecting personal and sensitive data.