Комп’ютерний практикум №1

Тема: Шифр Цезаря

Мета: Розробити криптосистему на основі шифру Цезаря

Базові відомості

Шифр Цезаря - один з найдавніших шифрів, названий на честь римського імператора Гая Юлія Цезаря, який використовував його для секретного листування. При шифруванні кожен символ замінюється іншим, віддаленим від нього в алфавіті на фіксоване число позицій.

Якщо зіставити кожному символу алфавіту його порядковий номер, то шифрування і розшифрування можна виразити формулами модульної арифметики:

$y=(x+k) \bmod n$ $x=(y+n-(k \bmod n)) \bmod n$, де x - символ відкритого тексту, y - символ шифрованого тексту, n - потужність алфавіту, а k - ключ.

З прикладами використання шифру Цезаря можна ознайомитись на чисельних сайтах відповідної тематики, наприклад:
https://ciox.ru/caesar-cipher http://questhint.ru/shifr-tsezarya/
http://hostciti.net/calc/it/cipher-ceaser.html

Хід виконання роботи

1. Розробіть інтерфейс криптографічної системи симетричного шифрування, передбачивши в ньому використання меню та/або панелі інструментів для виконання таких команд:
    a. створення, відкривання, збереження, друкування файлів,
    b. шифрування і розшифрування файлів українською та англійською мовами,
    c. виведення відомостей про розробника та
    d. виходу з системи.

2. Розробіть систему класів для реалізації симетричного шифрування методом Цезаря, передбачивши в них методи валідації ключа, валідації, шифрування і розшифрування даних.
3. Виконайте тестування роботи системи.

Додаткові завдання:

1. Доповніть розроблену систему модулем для атаки на шифр Цезаря методом «грубої сили» (перебору).
2. Розширте можливості системи, забезпечивши можливість шифрування даних в будь-якому форматі, а не тільки текстових.