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) mod n x=(y+n−(k mod n)) mod 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 шифром 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). [https://ru.stackoverflow.com/questions/589116/Шифр-Цезаря-организовать-выдачу-полного-перебора](https://ru.stackoverflow.com/questions/589116/%D0%A8%D0%B8%D1%84%D1%80-%D0%A6%D0%B5%D0%B7%D0%B0%D1%80%D1%8F-%D0%BE%D1%80%D0%B3%D0%B0%D0%BD%D0%B8%D0%B7%D0%BE%D0%B2%D0%B0%D1%82%D1%8C-%D0%B2%D1%8B%D0%B4%D0%B0%D1%87%D1%83-%D0%BF%D0%BE%D0%BB%D0%BD%D0%BE%D0%B3%D0%BE-%D0%BF%D0%B5%D1%80%D0%B5%D0%B1%D0%BE%D1%80%D0%B0)

2. Розширте можливості системи, забезпечивши можливість шифрування даних в будь-якому форматі, а не тільки текстових.