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:

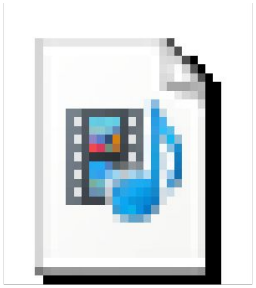
$y=(x+k) \bmod n$ $x=(y+n-(k \bmod n)) \bmod n$, де x - символ відкритого тексту, y - символ шифрованого тексту, n - потужність алфавіту, а k - ключ.

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



Óðîê ¹1 Øèôð Öåçàðÿ.mp4

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.

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

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

Варіант	Зміст	Варіант	Зміст
1	Зсув на 3 в українській абетці	16	Зсув на 18 в українській абетці
2	4	17	19
3	5	18	20
4	6	19	21
5	7	20	22
6	8	21	23
7	9	22	24
8	10	23	25
9	11	24	26
10	12	25	27
11	13	26	
12	14	27	
13	15	28	
14	16	29	
15	17	30	