**Лабороторна работа №1**

**Тема роботи:** Дослідження “Шифру Цезаря”

**Мета:** Відпрацювання та закріплення теоретичних відомостей криптоалгоритму “Шифр Цезаря”

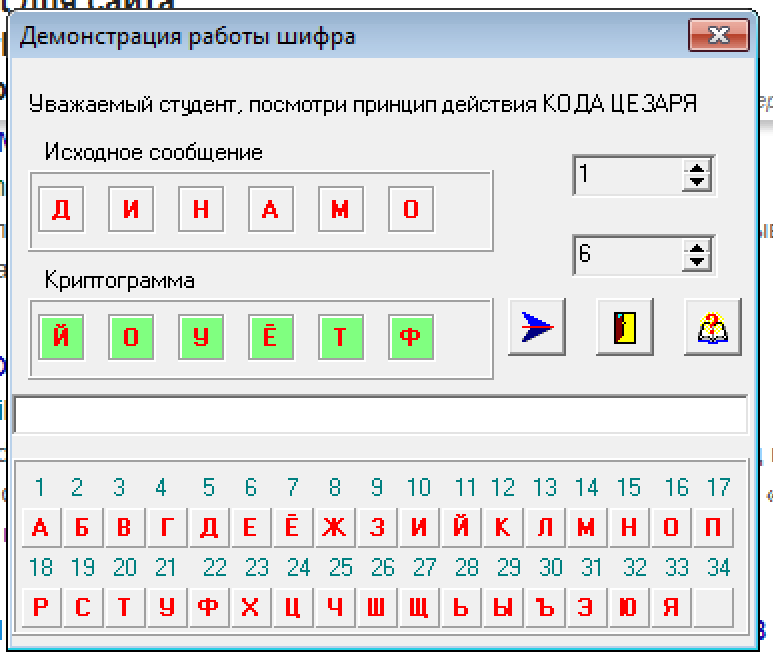
**Короткі відомості:**

Шифром Цезаря називається симетричний алгоритм шифрування підстановками. Використовувався римським імператором Юлієм Цезарем для приватного листування.

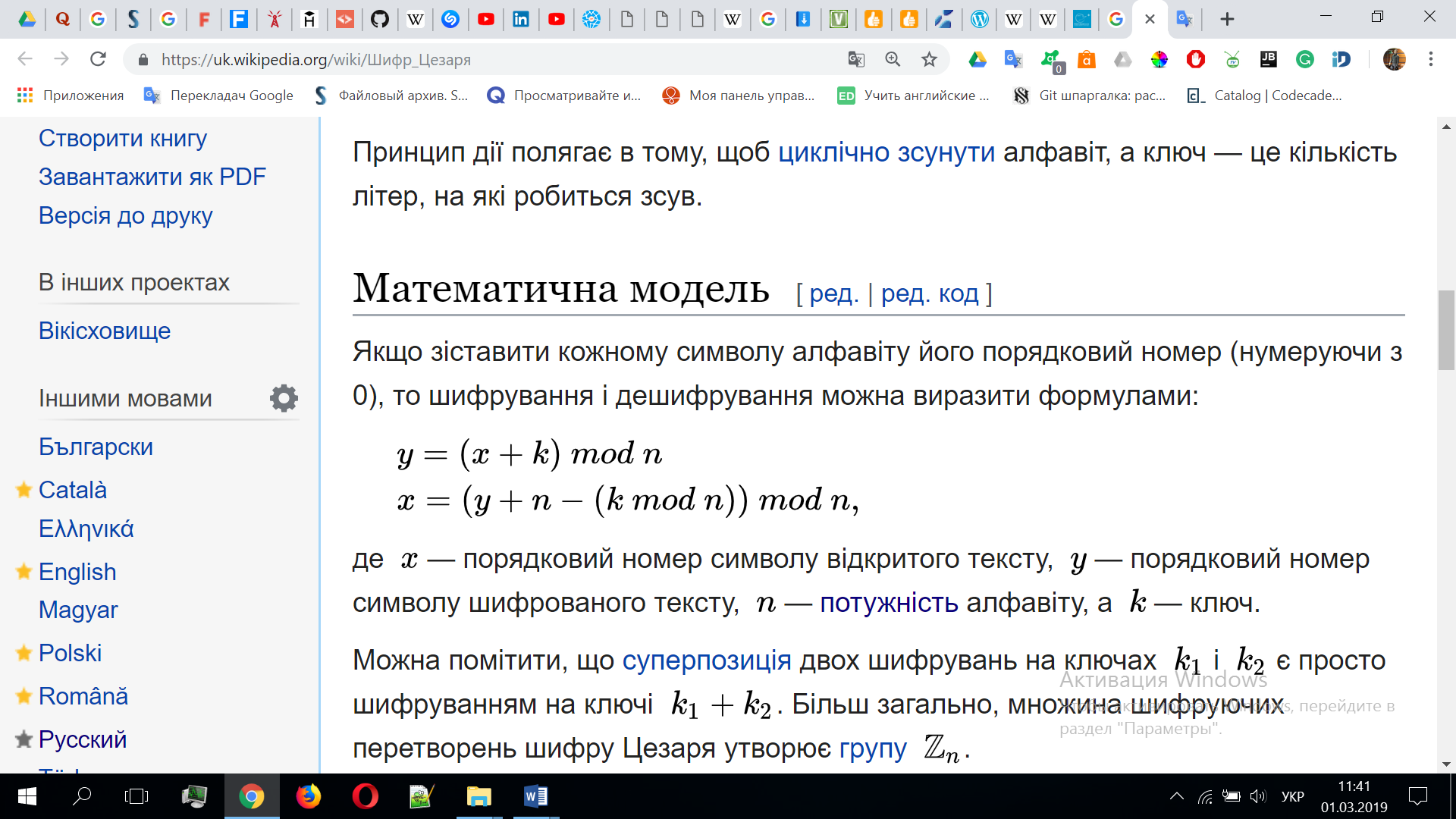
Принцип полягає в тому, щоб циклічно зсунути алфавіт на якусь кількість літер.

Ключем буде виступати ця кількість літер, на які робиться зсув.

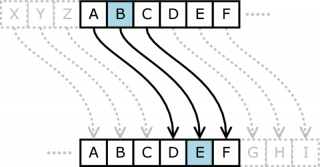


Зразок работи алгоритму  


Якщо порівнювати по кожному символу алфавіту його порядковий номер (починаючи з 0 ), то шифрування і дешифрування можна виразити :



Де ***x***- порядковий номер символу відкритого тексту, ***y*** *-* порядковий номер символу шифрованого тексту, ***n*** - потужність алфавіту, а ***k*** *-* {\displaystyle ~k}ключ.



**Висновок:** Шифр Цезаря не має практично ніякого застосування в даний час, оскільки він легко зламується. Шифр Цезаря має замало ключів — на одиницю менше, ніж літер в абетці. Тому перебрати усі ключі не складає особливої роботи. Також зламати шифр Цезаря можна, як і звичайний підстановочний шифр, у зв'язку з тим, що частота появи кожної літери в шифртексті збігається з частотою появи у відкритому тексті. Також шифр Цезаря можна зламати застосовуючи метод частотного криптоаналізу.