**Лабороторна работа №2**

**Тема:** Дослідження “Шифру Тритеміуса”

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

**Короткі відомості:**

Шифром Тритеміуса називається система шифрування, розроблена Іоганном Тритемія. Являє собою вдосконалений шифр Цезаря, тобто шифр підстановки. За алгоритмом шифрування, кожен символ повідомлення зміщується на символ, який відстає від даного на деякий крок. Тут крок зміщення робиться змінним, тобто залежним від будь-яких додаткових чинників.

Наприклад, можна задати закон зміщення у вигляді лінійної функції (рівняння шифрування) позиції шифруємої літери. Сама функція повинна гарантувати цілочисельне значення. Пряма функція шифрування повинна мати зворотну функцію шифрування, теж цілочисельну.

Вважається удосконаленим шифром Цезаря

Формула для шифру:

***L = (m+k) mod N***

***L****-*номер зашифрованої букви в алфавіті,

***m***-порядковий номер букви шифрованого тексту в алфавіті,

***k****-*число зсуву,

***N****-*кількість букв в алфавіті*.*

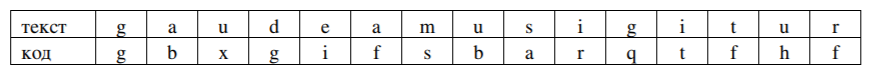
Число зсуву  ***k*** *(*крок зсуву) в даному випадку змінна величина, функціонально залежить від позиції символу в повідомленні. Залежність може бути різною, наприклад, лінійною або квадратичною.

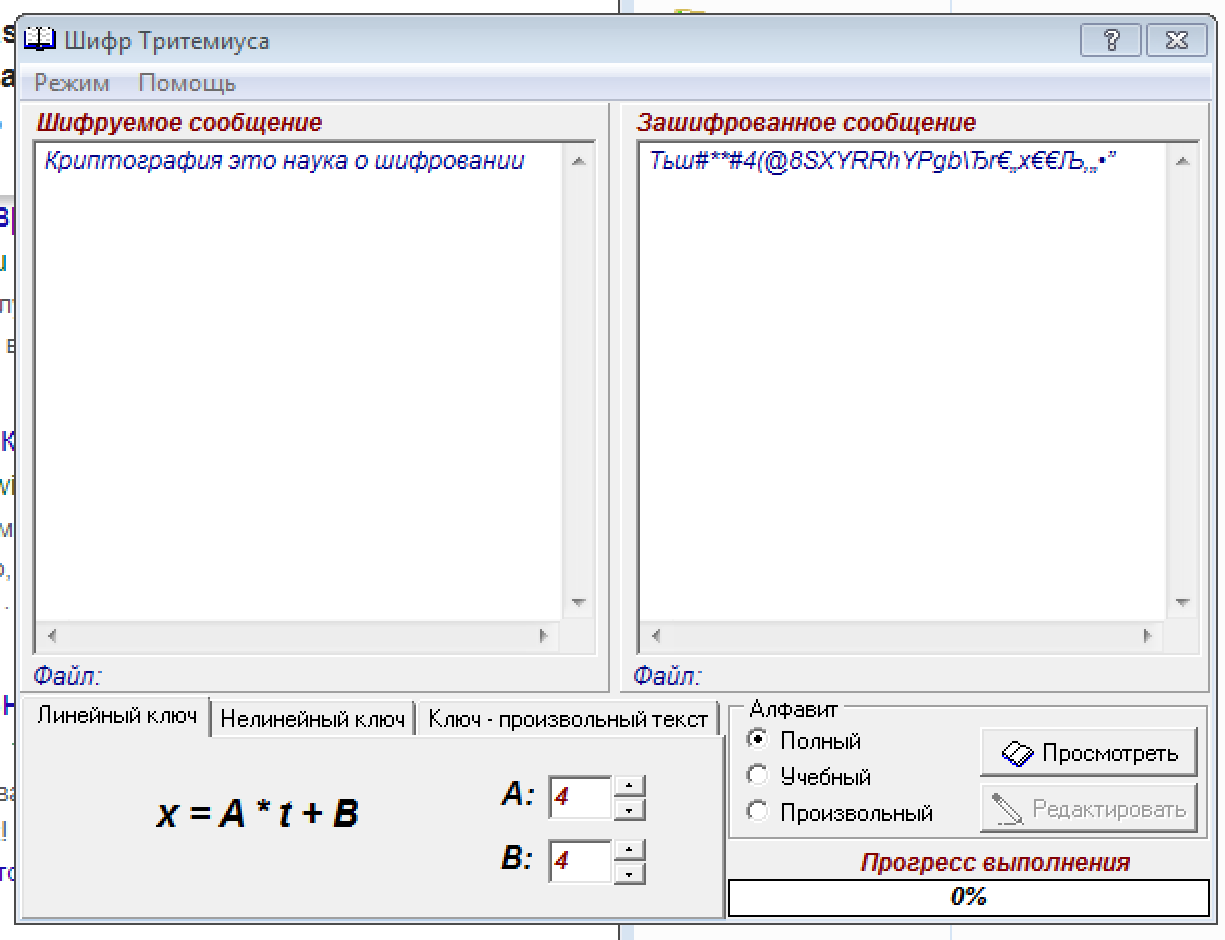
***k = A\*p + B*** *(лінійна залежність).*

***A, B*** – ключі (можуть бути будь які вибрані числа але вони повинні бути цілими).

***p*** – позиція літери в повідомленні

Приклади:





**Висновок:** Шифр Тритеміуса можна віднести до шифру заміщення це покращений шифр Цезаря який відрізняється кроком зміщення. Крок зміщення задається функцією і текстом. Тип ключа в Тритеміуса задається з обмеженим об’ємом текста, стійкість забезпечується секретним ключем.