# Комп’ютерний практикум №2

**Тема:** Шифр Тритеміуса.

**Мета:** Розробити криптосистему на основі шифру Тритеміуса.

**Шифр Тритеміуса** - вдосконалений шифр Цезаря, в якому кожен символ повідомлення зміщується на символ, який відстає від даного на деякий **крок**. Але крок зміщення робиться змінним, тобто залежним від будь-яких додаткових чинників. Наприклад, можна задати закон зміщення у вигляді лінійної функції позиції літери, що шифрується, або за допомогою використання гасла – текстового рядка, який багаторазово записується під текстом повідомленням.

Таким чином, шифрування і розшифрування для шифру Тритеміуса можна виразити наступними рівняннями:

y=(x+k)mod n;

x=(y+n−(kmod n))mod n,

де x-символ відкритого тексту, y - символ шифрованого тексту, n – потужність алфавіту.

Крок зміщення k розраховується:

* За лінійним рівнянням k = Ap + B;
* за нелінійним рівнянням k = A 2 + Bp + C;
* за гаслом.

Тут *p* - позиція букви в повідомленні. Ключем шифрування виступають відповідно коефіцієнти вказаних рівнянь та гасло.

**Хід виконання роботи**

1. Модифікуйте **інтерфейс** криптографічної системи симетричного шифрування з лабораторної роботи №1, забезпечивши можливість використання в якості ключа:
2. 2-вимірного вектору для зберігання коефіцієнтів лінійного рівнянняшифрування,
3. 3-вимірного вектору для зберігання коефіцієнтів лінійного рівняння шифрування,
4. Текстового рядка(гасла).
5. Доповніть систему класів з лабораторної роботи №1 класами та методами, необхідними для реалізації симетричного шифрування методом Тритеміуса, передбачивши в них методи валідації ключа, валідації шифрування і розшифрування даних.
6. Виконайте тестування роботи системи.