Лабораторна робота №2

Тема: Шифр Тритеміуса
Мета: Розробити криптосистему на основі шифру Тритеміуса

Базові відомості

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:

$$y=(x+k) \bmod n \qquad x=(y+n-(k \bmod n)) \bmod n,$$

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 $k = Ap^2 + Bp + C$;
- 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:
a. 2-вимірного вектору для зберігання коефіцієнтів лінійного рівняння шифрування,
b. 3-вимірного вектору для зберігання коефіцієнтів нелінійного рівняння шифрування,
c. Текстового рядка (гасла).
2. 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.
3. Виконайте тестування роботи системи.

4. Застосувати частотні таблиці для української та англійської мов для атаки.
5. Доповніть систему модулем активної атаки на шифр Тритеміуса, який би забезпечував знаходження ключа шифрування у випадку, коли зловмиснику вдалось отримати пару повідомлень «незашифроване – зашифроване».