

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:

$$y = (x + k) \bmod n$$

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

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

Крок зміщення k розраховується:

- за лінійним рівнянням $k = A \cdot p + B$;
- за нелінійним рівнянням $k = A \cdot p^2 + B \cdot p + C$;
- 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-вимірному вектору для зберігання коефіцієнтів лінійного рівняння шифрування,
 - b. 3-вимірному 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, шифрування і розшифрування даних.
3. Виконайте тестування роботи системи.

Додаткові завдання

1. Доповніть систему модулем активної атаки на шифр Тритеміуса, який би забезпечував знаходження ключа шифрування у випадку, коли зломиснику вдалось отримати пару повідомлень «незашифроване – зашифроване»

