# Комп’ютерний практикум №4

**Тема:** Книжковий шифр.

**Мета:** Розробити криптосистему на основі використання віршованого фрагменту в якості ключа шифрування.

**Базові відомості**

**Книжковий шифр** - вид шифру, в якому кожен елемент відкритого тексту (кожна буква або слово) замінюється на показник(наприклад: номерсторінки, рядки і стовпці) аналогічного елемента в додатковому тексті-ключі.

Суть методу книжкового шифру - це вибір будь-якого тексту з книги, де номери слів починаються на певну букву або координати (рядок, номер в рядку) самих букв виступають в якості шифру вихідного повідомлення. При цьому одній вихідної букві може відповідати декілька символів.

Відомо кілька різновидів книжкового шифру. Найбільш простим з них є

*шифрування з використанням вірша (віршований шифр)*.

У віршованому шифрі ключем є заздалегідь обумовлений вірш, яке записується в прямокутник узгодженого розміру. Цей прямокутник є ключовою сторінкою книжкового шифру.

**Алгоритм віршованого шифрування:**

1. Вибрати вірш для використання в якості ключа шифрування.
2. Пронумерувати всі стовпчики і рядки вибраного ключа шифрування двозначними цифрами: CC/SS відповідно.
3. Символу M вхідного повідомлення поставити у відповідність 4-значний код CС/SS такого ж вибраного випадково символу ключа шифрування. Тут чисельник кожного дробу - номер рядка, а знаменник - номер стовпчика.
4. Код CС/SS занести до шифрограми і додати кому.
5. Повторити п.п.3-4 для кожного символу повідомлення, що шифрується.

**Алгоритм розшифрування з використанням вірша:**

1. Для елемента коду CС/SS криптограми визначити номер стовпчика CС і рядка SS зашифрованого символу.
2. Знайти в ключі шифрування символ, що знаходиться на перетині CС колонки і SS-рядка.
3. Записати знайдений символ в якості розшифрованого символу.
4. Повторити п.п.1-3 для кожного елементу коду, відокремленого за допомогою ком.

Так в одному з таємних листувань революціонерів, ключем шифру був вірш Н. А. Некрасова «Школьник»: «Ну, пошел же ради бога ...». Вірш вписувався в квадрат розміром 10на10, якщо в рядку було більше 10 букв, то зайві літери викидалися:



Так, слово «Сообщите» по такій таблиці можна було зашифрувати декількома способами: «4/3,5/2, 8/6, 2/3, 1/5, 7/7, 10/1, 6 / 2 ... » або « 10/9, 1/4, 8/3, 5/5, 1/5, 8/8, 9/9, 6/2 ...» і т. д. Так як в таблиці відсутня літера «Щ», то замість неї використовується літера «Ш», але це ніяк не заважає розшифровці повідомлення.

Помітною перевагою книжкового шифру є відсутність проблем, пов'язаних з підготовкою і передачею секретного ключа, адже кодовий текст відразу існує в кількох примірниках. Проте цей шифр нестійкий до частотних методів криптоаналізу.

**Хід виконання роботи**

1. Розробіть інтерфейс криптографічної системи для реалізації шифрування з використанням вірша.
2. Доповніть систему класів з попередніх лабораторних робіт класами та методами, необхідними для шифрування і розшифрування віршованим шифром.
3. Виконайте тестування роботи системи.