**Лабороторна работа №4**

**Тема:** Криптоалгоритм “Шифр Штірліца” (книжковий шифр)

**Мета:** Практичне відпрацювання та закріплення теоретичних відомостей з криптоалгоритму “Шифр Штірліца” (книжкового шифру)

**Короткі відомості:**

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

Для дешифрування необхідно мати, як закритий текст, так і додатковий текст-ключ. В якості додаткового тексту часто використовували поширені книги або книги, які з великою часткою ймовірності були і у відправника і у адресата.

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 однією вихідної букві може відповідати кілька символів.

**Висновки:** У будь-якому випадку книжковий шифр дозволяє отримати зашифрований текст, який відносно важко зламати. А головне - вирішує проблему передачі ключа: сторони можуть заздалегідь домовитися про те, яка книга буде вживатися для шифрування повідомлень.