

Індивідуальне завдання №2 – 106

Розширити програмну реалізацію завд. 1 додатковою опцією шифрування, реалізувавши шифр зсуву (шифрування/дешифрування) з заданим ключем.

- На вхід програми передається величина зсуву, алфавіт в якому здійснюється шифрування (зчитується з окремого файлу), довжина блоку (якщо довжина блоку = 0, тоді файл не розбивається блоками) та текстовий файл з відкритим або зашифрованим текстом.
- Результат шифрування/дешифрування повинен записуватись у файл. Кожен блок тексту шифрується/дешифрується окремо. Розробити реалізацію алгоритмів найбільш оптимальним чином (у випадку шифрування блоками можна застосувати багатопотчність).
- Додатковою опцією програми має бути реалізований частотний криптоаналіз за допомогою якого визначається величина зсуву.
- Функціонал програми повинен бути покритий юніт-тестами.
- Заміряти час виконання алгоритмів та використання пам'яті. Перевірити роботу програми на великих текстових файлах $\geq 5\text{Mb}$.
- *Бонусною опцією програми буде розробка графічного інтерфейсу.
- Код програми завантажити у Git репозиторій.
- Поділитись на пари за бажанням для передачі зашифрованих файлів (хтось з пари шифрує, інша(ий) дешифрує за допомогою частотного криптоаналізу не знаючи ключа.).