

## ЛАБОРАТОРНА РОБОТА № 4

---

ТЕМА: ШИФРУВАННЯ ДАНИХ З ВИКОРИСТАННЯМ ЛІТЕРАТУРНОГО ФРАГМЕНТУ.

МЕТА: ОЗНАЙОМИТИСЬ З МЕТОДОМ ШИФРУВАННЯ ДАНИХ НА ОСНОВІ ЛІТЕРАТУРНОГО ФРАГМЕНТУ І НАДАТИ ЙОГО ПРОГРАМНУ РЕАЛІЗАЦІЮ

---

### ТЕОРЕТИЧНІ ВІДОМОСТІ

---

Даний метод симетричного шифрування передбачає використання в якості ключа фрагменту літературного фрагменту.

Алгоритм шифрування:

1. Вибрати певну сторінку достатньо відомого літературного твору для використання в якості ключа шифрування.
2. Пронумерувати всі стовпчики і рядки вибраного ключа шифрування двозначними цифрами: CC SS відповідно.
3. Символу М вихідного повідомлення поставити у відповідність 4-значний код CCSS такого ж вибраного випадково символу ключа шифрування.
4. Код CCSS занести до шифрограми і додати пробіл.
5. Повторити п.п.3-4 для кожного символу повідомлення, що шифрується

Алгоритм розшифрування:

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

### ПОРЯДОК ВИКОНАННЯ РОБОТИ

---

1. Ознайомитись з шифруванням даних з використанням літературного фрагменту.
2. Побудувати блок-схему алгоритму шифрування.
3. Написати програму для шифрування та розшифрування на основі літературного фрагменту, передбачивши в ній можливості вибору:
  - а. Файлу з літературним фрагментом .
  - б. Алфавіту (наприклад, англійський та український).

4. Підготувати звіт про виконання роботи. Звіт оформити у вигляді документу Word з такою структурою: титульний лист, тема і мета роботи, блок-схема алгоритму методу, програмний код.
5. Електронну копію звіту відправити за адресою: [George@aprodos.kpi.ua](mailto:George@aprodos.kpi.ua).