

## ЛАБОРАТОРНА РОБОТА № 3

---

ТЕМА: ШИФРУВАННЯ ДАНИХ МЕТОДОМ ГАМІЮВАННЯ.

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

---

### ТЕОРЕТИЧНІ ВІДОМОСТІ

---

Шифр Трбітеміуса мав суттєвий недолік: повторюваність ключа. Метод гаміювання знімає цю проблему.

Алгоритм шифрування:

1. Нумеруємо букви вибраного алфавіту для шифрування.
2. Кожному символу  $M$  вихідного повідомлення поставити у відповідність номер  $m$  з вибраного алфавіту.
3. Конструємо генератор псевдовипадкових чисел (ПВЧ).
4. Задаємо параметри генератора ПВЧ в якості секретного ключа.
5. Генеруємо послідовність ПВЧ - гаму, для якої  $T > L$ , де  $T$  - період гами  $L$  - довжина повідомлення, що шифрується.
6. Накладаємо гаму на повідомлення, що шифрується:  $l = m (+) \text{ПВЧ}$  в  $GF(N)$ , де  $N$  - період ПВЧ, ПВЧ - випадковий номер,  $l$  - номер символу криптограми у вибраному алфавіті.
7. Перекодуємо повідомлення з цифрового виду в символьний відповідно до обраного алфавіта.

Алгоритм розшифрування:

1. Отримане повідомлення з допомогою відомого коду алфавіту перетворюється в цифровий вигляд.
2. Генеруємо гаму за допомогою секретного ключа.
3. Виконуємо повторне гаміювання криптограми (із заміною складання на віднімання).
4. Перекодуємо повідомлення з цифрового виду в символьний відповідно до обраного алфавіта.

### ПОРЯДОК ВИКОНАННЯ РОБОТИ

---

1. Ознайомитись з шифруванням даних методом гаміювання.
2. Побудувати блок-схему алгоритму шифрування.
3. Написати програму для шифрування та розшифрування за допомогою метода гаміювання, передбачивши в ній можливості вибору:
  - a. Файлу.
  - b. Алфавіту (наприклад, англійський та український).

4. Підготувати звіт про виконання роботи. Звіт оформлюється у вигляді документу Word з такою структурою: титульний лист,
  - a. тема і мета роботи,
  - b. опис алгоритму роботи програми у вигляді блок-схеми або UML- діаграм (класів, діяльності тощо),
  - c. функціональні можливості програми (основні і додаткові),
  - d. фрагмент програмного коду, що реалізує базову функціональність,
  - e. особливості програмної реалізації окремих функцій.
5. Електронну копію звіту відправити за адресою: [George@aprodos.kpi.ua](mailto:George@aprodos.kpi.ua).