ЛАБОРАТОРНА РОБОТА № 3

ТЕМА: ШИФРУВАННЯ ДАНИХ МЕТОДОМ ГАМІЮВАННЯ.

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

ТЕОРЕТИЧНІ ВІДОМОСТІ

Алгоритм шифрування:

1. Нумеруємо букви вибраного алфавіту для шифрування.
2. Кожному символу M вихідного повідомлення ставимо у відповідність номер m з вибраного алфавіту.
3. Конструюємо 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 XOR ПВЧ. Тут l - код символу криптограми, ПВЧ - випадковий номер гами для символу M.

Алгоритм розшифрування:

1. Генеруємо гаму за допомогою секретного ключа.
2. Виконуємо гаміювання криптограми.
3. Перекодовуємо повідомлення з цифрового виду в символьний відповідно до обраного алфавіту.

ПОРЯДОК ВИКОНАННЯ РОБОТИ

1. Ознайомитись з шифруванняv 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.