# ЛАБОРАТОРНА РОБОТА № 8

## ТЕМА: МЕТОД АСИМЕТРИЧНОГО ШИФРУВАННЯ, ЩО ГРУНТУЄТЬСЯ НА ЗАДАЧІ РЮКЗАКА

## МЕТА: НАДАТИ ПРОГРАМНУ РЕАЛІЗАЦІЮ АСИМЕТРИЧНОЇ КРИПТОСИСТЕМИ НА ОСНОВІ ДАНОГО МЕТОДУ

### ТЕОРЕТИЧНІ ВІДОМОСТІ

Проблему рюкзака можна сформулювати так:

Нехай задано множину натуральних чисел A = ($a_1$,$a_2$ ,..., $a_n$) і натуральне число S. Потрібно встановити, чи існує такий набір чисел $x_i$ з (0,1), i ≤ n, для якого $\Sigma a_i x_i$ = S (1 <= i <= n)?

В принципі рішення завжди може бути знайдено повним перебором підмножин A і перевіркою, яка з їх сум дорівнює S. Але при великих n доведеться перебрати $2^n$ варіантів. Навіть для n = 300 пошук серед $2^{300}$ підмножин не піддається обробці.

Ідея побудови системи шифрування на основі проблеми рюкзака полягає у виділенні деякого підкласу задач про укладання рюкзака, що розв'язуються порівняно легко – задачі «суперзростаючого» рюкзака, і "маскування" задач цього класу за допомогою деякого перетворення параметрів під загальний випадок. Параметри підкласу визначають секретний ключ, а параметри модифікованої задачі - відкритий ключ.

Алгоритм шифрування:

Введення: натуральне число n>1, послідовність натуральних чисел A=($a_1$, $a_2$ ,..., $a_n$), вхідне повідомлення p.

Виведення: шифротекст C.

Крок 1. Представити p у вигляді бінарної послідовності.

Крок 2. Розбити отриману бінарну послідовність на n-розрядні блоки $p_i=p_{i1}p_{i2}...p_{in}$.

Крок 3. Зашифрувати кожний блок за допомогою перетворення $C_i = \Sigma\, p_{ij} \cdot a_j$, j = 1 ... n.

Крок 4. Отримати шифротекст C= ($C_1$; $C_2$; ...; $C_i$)

Алгоритм розшифрування:

Введення: натуральне число n>1, суперзростаюча послідовність натуральних чисел B=( $b_1$, $b_2$ ,..., $b_n$), натуральні числа m> $\Sigma b_i$, і $t \equiv 1 \pmod m$, шифротекст C= ($C_1$; $C_2$; ...; $C_i$).

Виведення: відкрите повідомлення p.

Крок 1. Знайти таке дійсне $t^{-1}$, що $tt^{-1} \equiv 1 \pmod m$.

Крок 2. Для кожного блоку шифротексту обчислити $C_i' \equiv t^{-1}C_i \pmod m$.

Крок 3. Розв'язати задачу «суперзростаючого» рюкзака для B і кожного $C_i'$, отримавши відповідну бінарну послідовність $p_i$ з n бітів.

Крок 4. Шляхом декодування $p_i$ отримати текст повідомлення p.

Секретний ключ алгоритму складається з елементів $B=( b_1, b_2 ,..., b_n)$, m, t.

Відкритий ключ алгоритму утворюють елементи $A=(a_1, a_2 ,..., a_n)$, де $a_i= t\ b_i \bmod m$.

## ПОРЯДОК ВИКОНАННЯ РОБОТИ

1. Ознайомитись з методом асиметричного шифрування на основі задачі рюкзака.
2. Побудувати блок-схему алгоритму шифрування.
3. Написати програму для шифрування та розшифрування за допомогою даного методу, передбачивши в ній можливості вибору:
    a. Файлу.
    b. Алфавіту (наприклад, англійський та український).
    c. Ключа.
4. Підготувати звіт про виконання роботи. Звіт оформлюється у вигляді документу Word з такою структурою:
    a. титульний лист,
    b. тема і мета роботи,
    c. опис алгоритму роботи програми у вигляді блок-схеми або UML- діаграм (класів, діяльності тощо),
    d. функціональні можливості програми (основні і додаткові),
    e. фрагмент програмного коду, що реалізує базову функціональність,
    f. особливості програмної реалізації окремих функцій.
5. Електронну копію звіту відправити за адресою: George@aprodos.kpi.ua.