Лабораторна №4

Тема: Шифрування з відкритим ключем на основі задачі рюкзака

Мета: Ознайомитись з принципами побудови асиметричних криптосистем

Базові відомості

Першим алгоритмом для узагальненого шифрування з відкритим ключем став алгоритм рюкзака, розроблений Ральфом Меркле і Мартіном Хеллманом. Алгоритм демонструє можливість застосування задачі рюкзака (NP-повної проблеми) в криптографії з відкритими ключами. Задачу 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), і n, для якого $\Sigma a_i x_i = S$ (1 <= i <= n)?

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.

Суперзростаюча послідовність B = (b_1,b_2 ,..., b_n) - це послідовність, в якій кожній член більше суми всіх попередніх членів, тобто $b_i > \sum b_j$, j<i. Наприклад, послідовність {1,3,6,13,27,52} є суперзростаючою, а {1,3,4,9, 15,25} - ні. Розв’язання задачі рюкзака для суперзростаючої послідовності знайти легко, використовуючи такий алгоритм:

Введення: натуральне число n>1, натуральне число S, суперзростаюча послідовність натуральних чисел B = (b_1,b_2 ,..., b_n).

Виведення: набір чисел xi з (0,1), i ≤ n, для якого Σaixi = S (1 <= i <= n)

Крок 1. Покласти i=n.

Крок 2.Порівняти S з найбільшим числом послідовності bi: якщо S< bi, то xi=0, інакше xi=1.

Крок 3. Зменшити S на bi, якщо xi=1.

Крок 4. Покласти i=n-1.

Крок 5. Якщо i>1, перейти до кроку 2, в іншому випадку повернути набір чисел xi.

Не суперзростаючі, або нормальні, рюкзаки представляють собою важку NP-проблему - швидкого алгоритму для них не знайдено. Алгоритм Меркле-Хеллмана заснований на цій властивості.

В якості закритого ключа вибирається суперзростаюча послідовність B = (b_1,b_2 ,..., b_n) та натуральні числа m> Σb_i, і t≡1(mod m). За ними будується послідовність нормального рюкзака A = (a_1,a_2 ,..., a_n) за наступним алгоритмом:

Введення: натуральне число n>1, суперзростаюча послідовність натуральних чисел B=(b_1, b_2 ,..., b_n), натуральні числа m> Σb_i, і t≡1(mod m).

Виведення: A = (a_1,a_2 ,..., a_n).

Крок 1. Покласти i=1.

Крок 2. Знайти a_i=b_i*t mod m.

Крок 3. Покласти i=i+1.

Крок 4. Якщо i>n, повернути A, в іншому випадку перейти до кроку 2.

Відкритий ключ A=(a_1, a_2 ,..., a_n) використовується для шифрування за таким алгоритмом:

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=$p_{i1}p_{i2}\ldots p_{in}$.

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)

Зашифроване повідомлення може розшифрувати власник закритого ключа, скористувавшись наступним алгоритмом:

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

Виведення: відкрите повідомлення p.

Крок 1. Знайти таке дійсне t^{-1}, що $tt^{-1} \equiv 1 (\text{mod } m)$.

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

В принципі рішення задачі рюкзака 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.

Хід виконання роботи

1. Відшукайте в Інтернет-ресурсах чисельний приклад з використання «рюкзачного» алгоритму (наприклад, в Вікіпедії) та опрацюйте його.
2. Розробіть інтерфейс криптографічної системи для шифрування з використанням задачі рюкзака, передбачивши окремий діалог для формування відкритого ключа.
3. Розробіть методи, які б забезпечували:
   a. Генерацію пари «відкритий –закритий» ключі.
   b. Шифрування з використанням відкритого ключа.
   c. Розшифрування з використанням закритого ключа. При цьому значення t^{-1} вважати відомим.
4. Перевірте правильність роботи системи на основі використання даних з чисельного прикладу.

Додаткові завдання:

1. Ознайомтесь з можливостями он-лайн калькулятора для знаходження взаємно обернених чисел, використайте його для t^{-1} за відомими t і перевірте правильність функціонування системи в загальному випадку.
2. Ознайомтесь з розширеним алгоритмом Евкліда для знаходження взаємно обернених чисел і модифікуйте створений програмний код, додавши метод з реалізацією цього алгоритму і використання його для знаходження t^{-1} за відомими t і m.