

Лабораторна робота №6

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 $A = (a_1, a_2, \dots, a_n)$ і натуральне число S . Потрібно встановити, чи існує такий набір чисел x_i з $(0,1)$, $i \leq n$, для якого $\sum a_i x_i = S$ ($1 \leq i \leq n$)?

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.

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 $B = (b_1, b_2, \dots, b_n)$ – це послідовність, в якій кожний член більше суми всіх попередніх членів, тобто $b_i > \sum_{j < i} b_j$. Наприклад, послідовність $\{1, 3, 6, 13, 27, 52\}$ є суперзростаючою.

Розв'язання задачі рюкзака для суперзростаючої послідовності знайти легко, використовуючи такий алгоритм:

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

Виведення: набір чисел x_i з $(0,1)$, $i \leq n$, для якого $\sum a_i x_i = S$ ($1 \leq i \leq n$)

Крок 1. Покласти $i=n$.

Крок 2. Порівняти S з найбільшим числом послідовності b_i : якщо $S < b_i$, то $x_i=0$, інакше $x_i=1$.

Крок 3. Зменшити S на b_i , якщо $x_i=1$.

Крок 4. Покласти $i=n-1$.

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

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 $B = (b_1, b_2, \dots, b_n)$ та натуральні числа $m > \sum b_i$, $i \equiv 1 \pmod{m}$. За ними будується послідовність нормального рюкзака $A = (a_1, a_2, \dots, a_n)$ за наступним алгоритмом:

Введення: натуральне число $n > 1$, суперзростаюча послідовність натуральних чисел $B = (b_1, b_2, \dots, b_n)$, натуральні числа $m > \sum b_i$, $i \equiv 1 \pmod{m}$.

Виведення: $A = (a_1, a_2, \dots, a_n)$.

Крок 1. Покласти $i=1$.

Крок 2. Знайти $a_i = b_i \cdot t \bmod m$.

Крок 3. Покласти $i=i+1$.

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

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

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

Виведення: шифротекст C .

Крок 1. Представити p у вигляді бінарної послідовності.

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

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

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

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

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

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 $C'_i \equiv t^{-1}C_i \pmod{m}$.

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:
 - а. 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 калькулятор](#) 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

