Київський національний університет імені Тараса Шевченка
Факультет комп’ютерних наук та кібернетики
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації

Лабораторна робота №10
“Алгоритм відкриття математичного сейфу”
Виконали студенти 3-го курсу
Групи ІПС-32

Роботу виконали:
Ольховатий Ігор
Ковальов Володимир
Тряско Софія
Цілинко Олександр
Бондар Юлія
Волик Артем

Київ 2023

Завдання:

Задається мат сейф за допомогою матриці 2 на 3 (2 рядки 3 символи) за модулем k як простим так і складеним. Побудувати алгоритм який дозволяє відкрити математичний сейф.

Розв'язання:

Розглянемо перший випадок, що модуль k є простим числом

Нехай $X = ||x||_{ij} - \text{шуканий розв'язок}$ Розглянемо вектор стовпчик

$x^T = (x_{11}, x_{12},.., x_{1n},.., x_{m1},..., x_{mn})$ Це вектор який отриманий послідовним записом рядків матриці X

Тоді задача пошуку x зводиться до розв'язку СЛАР

$Bx + a = 0\ (mod\ k)$ у кільці G_k. Вектор a формується аналогічним чином з матриці початкових зсувів. Матриця B в загальному випадку має такий вигляд

$$\begin{pmatrix} \Im_n & E_n & E_n & \dots & \dots & E_n \\ E_n & \Im_n & E_n & \dots & \dots & E_n \\ E_n & E_n & \Im_n & \dots & \dots & E_n \\ \dots & \dots & \dots & \dots & \dots & \dots \\ E_n & E_n & E_n & \dots & \dots & \Im_n \end{pmatrix}$$

Матриця $\Im_n$ матриця розміру $n * n$ яка складається з 1.

$E_n - \text{одинична матриця розміру } n * n$

Тоді для нашої задачі матриця B має вигляд

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Нехай вектор стовпчик a має вигляд $\begin{bmatrix} a_{11} \\ a_{12} \\ a_{13} \\ a_{21} \\ a_{22} \\ a_{23} \end{bmatrix}$

Тепер просто розв'язуємо дану систему

Спочатку шукаємо обернену матрицю B в цьому кільці(за допомогою будь-якого відомого алгоритму)

$$\begin{bmatrix} \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{5}{8} & \frac{-3}{8} & -\frac{3}{8} \\ \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{-3}{8} & \frac{5}{8} & -\frac{3}{8} \\ \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{-3}{8} & \frac{-3}{8} & \frac{5}{8} \\ \frac{5}{8} & \frac{-3}{8} & \frac{-3}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} \\ \frac{-3}{8} & \frac{5}{8} & \frac{-3}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} \\ \frac{-3}{8} & \frac{-3}{8} & \frac{5}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} \end{bmatrix}$$

Тоді розв'язок системи x має вигляд

$x_{11} = -(\frac{1}{8}a_{11} + \frac{1}{8}a_{12} + \frac{1}{8}a_{13} + \frac{5}{8}a_{21} - \frac{3}{8}a_{22} - \frac{3}{8}a_{23})$

$x_{12} = -(\frac{1}{8}a_{11} + \frac{1}{8}a_{12} + \frac{1}{8}a_{13} - \frac{3}{8}a_{21} + \frac{5}{8}a_{22} - \frac{3}{8}a_{23})$

$x_{13} = -(\frac{1}{8}a_{11} + \frac{1}{8}a_{12} + \frac{1}{8}a_{13} - \frac{3}{8}a_{21} - \frac{3}{8}a_{22} + \frac{5}{8}a_{23})$

$x_{21} = -(\frac{5}{8}a_{11} - \frac{3}{8}a_{12} - \frac{3}{8}a_{13} + \frac{1}{8}a_{21} + \frac{1}{8}a_{22} + \frac{1}{8}a_{23})$

$x_{22} = -(\frac{-3}{8}a_{11} + \frac{5}{8}a_{12} - \frac{3}{8}a_{13} + \frac{1}{8}a_{21} + \frac{1}{8}a_{22} + \frac{1}{8}a_{23})$

$x_{23} = -(\frac{-3}{8}a_{11} - \frac{3}{8}a_{12} + \frac{5}{8}a_{13} + \frac{1}{8}a_{21} + \frac{1}{8}a_{22} + \frac{1}{8}a_{23}$

Якщо припустити, що $k \neq 2,$ то елемент 8 має обернений і розв'язок системи коректний

Якщо k ***– складене число***

Тут виконується все аналогічно, але в самому кінці елемент 8 може не мати оберненого якщо $k -$ парне. Якщо k -непарне, то елемент 8 має обернений. І цей розв'язок є коректним

Тестування

Розглянемо 2 випадки для $k -$ простого і 2 випадки для $k -$ складеного

1) $k = 7$

Нехай $a = (1, 2, 1, 0, 4, 5)$

Тоді розглянемо розв'язок

Елемент $1/8 = 1$

$x_{11} = a_{11} + a_{12} + a_{13} + 5a_{21} - 3a_{22} - 3a_{23} = 1 + 2 + 1 + 5 * 0 - 3 * 4 - 3 * 5 = 4 - 12 - 15$

$= -15 = -5 = 2$

$x_{12} = -2 = 5$

$x_{13} = -3 = 4$

$x_{21} = -5 = 2$

$x_{22} = -6 = 1$

$x_{23} = -5 = 2$

Перевіримо чи відкриває даний ключ сейф

Будемо розглядати сейф після кожної ітерації

$$\begin{bmatrix} 3 & 4 & 3 \\ 2 & 4 & 5 \end{bmatrix} \begin{bmatrix} 8 & 9 & 8 \\ 2 & 9 & 5 \end{bmatrix} \begin{bmatrix} 12 & 13 & 12 \\ 2 & 9 & 9 \end{bmatrix} \begin{bmatrix} 14 & 13 & 12 \\ 4 & 11 & 11 \end{bmatrix} \begin{bmatrix} 14 & 14 & 12 \\ 5 & 12 & 12 \end{bmatrix} \begin{bmatrix} 14 & 14 & 14 \\ 7 & 14 & 14 \end{bmatrix}$$

Дійсно даний елемент є ключем, отже алгоритм є вірним, бо перетворює матрицю на нульову, бо всі елементи кратні 7

2) $k = 13$

Нехай $a = (1, 2, 1, 0, 4, 5)$

Тоді розглянемо розв'язок

Елемент $1/8 = 5$

$x_{11} = a_{11} + a_{12} + a_{13} + 5a_{21} - 3a_{22} - 3a_{23} = 1 + 2 + 1 + 5 * 0 - 3 * 4 - 3 * 5 = 4 - 12 - 15$

$= -2 = 11$

$x_{12} = -6 = 7$

$x_{13} = -7 = 6$

$x_{21} = -12 = 1$

$x_{22} = 0$

$x_{23} = -12 = 1$

Перевіримо чи відкриває даний ключ сейф

$$\begin{bmatrix} 12 & 13 & 12 \\ 11 & 4 & 5 \end{bmatrix}\begin{bmatrix} 19 & 20 & 19 \\ 11 & 11 & 5 \end{bmatrix}\begin{bmatrix} 25 & 26 & 25 \\ 11 & 11 & 11 \end{bmatrix}\begin{bmatrix} 26 & 26 & 25 \\ 12 & 12 & 12 \end{bmatrix}\begin{bmatrix} 26 & 26 & 25 \\ 12 & 12 & 12 \end{bmatrix}\begin{bmatrix} 26 & 26 & 26 \\ 13 & 13 & 13 \end{bmatrix}$$

Дійсно даний елемент є ключем, отже алгоритм є вірним, бо перетворює матрицю на нульову, бо всі елементи кратні 13

1) $k = 15$

Нехай $a = (1, 2, 1, 0, 4, 5)$

Тоді розглянемо розв'язок

Елемент $1/8 = 2$

$x_{11} = a_{11} + a_{12} + a_{13} + 5a_{21} - 3a_{22} - 3a_{23} = 1 + 2 + 1 + 5 * 0 - 3 * 4 - 3 * 5 = 4 - 12 - 15$

$= -14 = 1$

$x_{12} = -3 = 12$

$x_{13} = -4 = 11$

$x_{21} = -10 = 5$

$x_{22} = -11 = 4$

$x_{23} = -10 = 5$

Перевіримо чи відкриває даний ключ сейф

$$\begin{bmatrix} 2 & 3 & 1 \\ 1 & 4 & 5 \end{bmatrix}\begin{bmatrix} 14 & 15 & 14 \\ 1 & 16 & 5 \end{bmatrix}\begin{bmatrix} 25 & 26 & 25 \\ 1 & 16 & 16 \end{bmatrix}\begin{bmatrix} 30 & 26 & 25 \\ 6 & 21 & 21 \end{bmatrix}\begin{bmatrix} 30 & 30 & 25 \\ 10 & 25 & 25 \end{bmatrix}\begin{bmatrix} 30 & 30 & 30 \\ 15 & 30 & 30 \end{bmatrix}$$

Дійсно даний елемент є ключем, отже алгоритм є вірним, бо перетворює матрицю на нульову, бо всі елементи кратні 15

1) $k = 25$

Нехай $a = (1, 2, 1, 0, 4, 5)$

Тоді розглянемо розв'язок

Елемент $1/8 = 22$

$x_{11} = a_{11} + a_{12} + a_{13} + 5a_{21} - 3a_{22} - 3a_{23} = 1 + 2 + 1 + 5 * 0 - 3 * 4 - 3 * 5 = 4 - 12 - 15$

$= -19 = 6$

$x_{12} = -23 = 2$

$x_{13} = -24 = 1$

$x_{21} = -10 = 15$

$x_{22} = -11 = 14$

$x_{23} = -10 = 15$

Перевіримо чи відкриває даний ключ сейф

$$\begin{bmatrix} 7 & 8 & 6 \\ 6 & 4 & 5 \end{bmatrix}\begin{bmatrix} 9 & 10 & 9 \\ 6 & 6 & 5 \end{bmatrix}\begin{bmatrix} 10 & 11 & 10 \\ 6 & 6 & 6 \end{bmatrix}\begin{bmatrix} 25 & 11 & 10 \\ 21 & 21 & 21 \end{bmatrix}\begin{bmatrix} 25 & 25 & 10 \\ 35 & 35 & 35 \end{bmatrix}\begin{bmatrix} 25 & 25 & 25 \\ 50 & 50 & 50 \end{bmatrix}$$

Дійсно даний елемент є ключем, отже алгоритм є вірним

Бо якщо підставити, то ми побачимо, що всі елементи обертаються на 0, бо всі елементи кратні 25

Література:

- Лекції з предмету “Математичні основи захисту інформації”
- http://dspace.puet.edu.ua/bitstream/123456789/2926/1/32%20%D0%94%D0%BE%D0%BD%D0%B5%D1%86%D1%8C.pdf
- http://dspace.puet.edu.ua/bitstream/123456789/2926/1/32%20%D0%94%D0%BE%D0%BD%D0%B5%D1%86%D1%8C.pdf