УДК 512.622.23:004

Рябухо О.М., Іванова К.Ю.

[1] *канд. фіз.-мат. наук, доцент, зав. кафедри алгебри, СДПУ*

[2] *студентка 5 курсу фізико-математичного факультету, СДПУ*

e-mail: kafedra_algebry_sdpu@mail.ru

РЕАЛІЗАЦІЯ ЗАДАЧІ ПОДІЛУ ТАЄМНИЦІ В МАТЕМАТИЧНОМУ ПАКЕТІ MAXIMA

В роботі проведено аналіз літератури щодо дослідження задачі поділу таємниці. Розроблено програмну реалізацію даної задачі в математичному пакеті Maxima. Проведено порівняльний аналіз програмної реалізації задачі поділу таємниці двома способами: за схемою Шаміра та схемою Асмута-Блума.

Ключові слова: *задача поділу таємниці, поліном Лагранжа, китайська теорема про остачу.*

Вступ

Криптографічна задача поділу таємниці (англ. Secret sharing) виникає у випадку необхідності забезпечення колегіальності прийняття рішення. Її суть полягає в тому, що сукупність даних, яка дозволяє повністю відновити секретний ключ (таємницю), розподіляється між членами певної групи з n осіб в такий спосіб, що кожному з них дістається доля таємниці (англ. Shadow), і подальше відновлення ключа можливе лише за присутності всіх (або певної мінімальної кількості k) членів групи. У разі невиконання цієї умови секретний ключ гарантовано не відновлюється.

Задача поділу таємниці містить два алгоритми: перший призначений для обчислення долей за заданим значенням секретного ключа (розподіл таємниці) і другий — для відновлення ключа за відомими долями (реконструкція таємниці).

Основне призначення розподілу таємниці — захист ключа від втрати. Зазвичай для захисту від втрати ключа роблять декілька копій. Зі збільшенням числа копій ключа зростає імовірність його компрометації (розголошення), якщо ж число копій мале, то зростає ризик втрати ключа, через можливість загубити його. Тому краще «розподілити» ключ між декількома особами в такий спосіб, щоб була можливість його відновлення при різних обставинах: кількома уповноваженими групами з певним складом учасників. Тим самим запобігають повної втрати ключа.

Пороговою схемою або схемою поділу таємниці називається схема, яка дозволяє «розподілити» таємницю між декількома учасниками в такий спосіб, щоб заздалегідь визначені уповноважені особи могли однозначно відновити таємницю, а неуповноважені – не отримали жодної додаткової інформації про можливе значення таємниці.

У (k, n)-порогових схемах повідомлення ділиться на n частин так, що будь-які k частини можуть відновити повідомлення.

Мета роботи: дослідити та програмно реалізувати задачу поділу таємниці за схемою Шаміра та схемою Асмута-Блума. Зробити порівняльний аналіз відповідних програм.

Загальні відомості про задачу поділу таємниці за схемами Шаміра та Асмута - Блума

Ідея порогової схеми була незалежно запропонована в 1979 році Аді Шаміром та Джорджем Блеклі. Для створення порогової схеми Шамір користувався поліноміальними рівняннями в скінченному полі [3]. Спочатку обирається просте число P, яке більше кількості можливих часток (долей) і більше найбільшої з можливих таємниць. Щоб зробити таємницю загальною, генерується довільний многочлен степеня $k-1$. Наприклад, якщо необхідно створити (6,10)-порогову схему, то генерується многочлен 5-го степеня:

$$f(x) = (ax^5 + bx^4 + cx^3 + dx^2 + hx + S) \mod P,$$

де P — це випадкове просте число, більше будь-якого з коефіцієнтів; S — таємниця (повідомлення).

Коефіцієнти a, b, c, d, h обираються випадково, вони зберігаються в таємниці і відкидаються після розподілу часток. Просте число P повинно бути опубліковане.

Частки (долі) отримуються за допомогою обчислення значення многочлену в n різних точках: $S_i = f(x_i)$.

Для відновлення таємниці необхідна наявність 6 часток (долей). Ця необхідність зумовлена тим, що для відшукання невідомих коефіцієнтів многочлену 4-го степеня з 6-ма невідомими потрібно 6 будь-яких значень часток. Трьох чи чотирьох буде недостатньо, а шести або восьми буде з надлишком. Для відновлення таємниці S за 6-ма частками S_1, S_2, S_3, S_4, S_5, S_6 будується многочлен $f(x)$ за інтерполяційною формулою Лагранжа

$$f(x) = \sum_{e=1}^{k} f(i_e) \prod_{j \neq e} \frac{x - i_j}{i_e - i_j}. \qquad (1)$$

Тоді вільний член поліному і буде таємницею $S = f(0) = a_0$.

В 1983 році в роботах С. Асмута, Д. Блума та М. Міньота були описані інші підходи до розв'язання задачі поділу таємниці. Вони запропонували в якості вихідної бази обрати кільце цілих чисел. В цьому кільці в якості таємниці пропонувалося брати деяке ціле число, а в якості часткової таємниці учасника — його конгруенцію за деяким модулем. Відновлення таємниці в таких системах відбувається шляхом розв'язання системи конгруенцій, найчастіше, за допомогою китайської теореми про лишки. Такі схеми називаються модулярними.

Для (k, n)-порогової схеми обирається велике просте число p, більше S. Потім обираються числа, менші p – $d_1, d_2, \ldots, d_n$, для яких:

1) значення d_i впорядковані за зростанням, $d_i < d_{i+1}$;
2) всі числа послідовності $d_1, d_2, \ldots, d_n$ попарно взаємнопрості;
3) $d_1 \cdot d_2 \cdot \ldots \cdot d_k > p \cdot d_{n-k+2} \cdot d_{n-k+3} \cdot \ldots \cdot d_n$.

Щоб розподілити частки, спочатку обираємо випадкове число r та обчислюємо $s = S + rp$. Частками (долями) є $s_i \equiv s \mod d_i$. Об'єднавши будь-які k часток, можна відновити S, використовуючи китайську теорему про лишки. Для довільних k чисел $s_{i_1}, \ldots, s_{i_k}$ єдиним розв'язком системи конгруенцій

$$\begin{cases} x \equiv s_{i_1} \pmod{d_{i_1}} \\ \ldots\ldots\ldots\ldots\ldots \\ x \equiv s_{i_k} \pmod{d_{i_k}} \end{cases} \tag{2}$$

буде таємний ключ s.

Процедура відновлення ключа неможлива для меншої ніж k кількості часток. Так для довільних $k-1$ чисел $s_{i_1}, \ldots, s_{i_{k-1}}$ система

$$\begin{cases} x \equiv s_{i_1} \pmod{d_{i_1}} \\ \ldots\ldots\ldots\ldots\ldots \\ x \equiv s_{i_{k-1}} \pmod{d_{i_{k-1}}} \end{cases}$$

матиме безліч розв'язків.

Програмна реалізація задачі поділу таємниці в пакеті Maxima

Алгоритм поділу таємниці $S \in Z_P$ за схемою Шаміра

1. Обирається n різних, ненульових елементів з Z_P.
2. Випадковим чином в Z_P обираються $k-1$ елементи $a_1, \ldots, a_{k-1}$.

3. Для кожного $1 \leq i \leq n$ обчислюються $S_i = f(x_i)$, де

$$f(x) = S + \sum_{j=1}^{k-1} a_j x^j \mod P.$$

4. Кожний учасник $1 \leq i \leq n$ отримує долю $(S_i,\ P)$.

Алгортм відновлення таємниці за наявними 6-ма частками.

1. Будуємо поліном Лагранжа за формулою 1.
2. Знаходимо його значення при $x = 0$, отримаємо таємницю $S = f(0)$.

Алгоритм поділу таємниці $S \in Z_P$ за схемою Асмута-Блума

1. Обирається просте число P та n взаємно простих чисел.
2. Перевіряються умови: $\forall i : d_i > P,\quad d_1 < \ldots < d_i < \ldots < d_n$ та $d_1 \cdot \ldots \cdot d_k > P \cdot d_{k+1} \cdot \ldots \cdot d_n$.
3. Обирається випадкове число r та обчислюється $s = S + rP$.
4. Обчислюються частки за формулою $s_i = s \mod d_i$.

Алгортм відновлення таємниці за наявними 6-ма частками.

1. Будуємо систему конгруенцій виду 2 та розв'язуємо її за допомогою китайської теореми про лишки.
2. Відновлюємо таємницю як розв'язок системи конгруенцій 2.

Приклад 1. *Нехай необхідно розділити таємницю $S = 97$ між 10 учасниками таким чином, щоб будь-які 6 з них могли відновити цю таємницю. Реалізуємо $(6, 10)$-порогову схему.*

Схема Шаміра	**Схема Асмута-Блума**
Обирається деяке просте число $P = 101$ Будуємо многочлен $f(x) = (64 \cdot x^5 + 27 \cdot x^4 + 18 \cdot x^3 +$ $+31 \cdot x^2 + 7 \cdot x + 97) \mod 101$	В якості простого числа оберемо $P = 101$ В якості взаємно простих $\forall i : i \in \{103, 107, 109, 113, 127, 131,$ $137, 139, 149, 151\}$, $i > P = 101$ $103 < 107 < 109 < 113 < 127 <$ $< 131 < 137 < 139 < 149 < 151$ $\cdot 131 > 101 \cdot 137 \cdot 139 \cdot 149 \cdot 151$ $103 \cdot 107 \cdot 109 \cdot 113 \cdot 127$ $r = 51$, $s = 5248$

Отримані долі $\{413, 49\}$, $\{432, 48\}$, $\{451, 71\}$, $\{470, 50\}$, $\{489, 78\}$, $\{508, 38\}$, $\{527, 40\}$, $\{546, 50\}$, $\{565, 24\}$, $\{584, 42\}$. Відновлення таємниці $\{432, 48\}$, $\{470, 50\}$, $\{489, 78\}$, $\{508, 38\}$, $\{565, 24\}$, $\{584, 42\}$ Будуємо інтерполяційний поліном Лагранжа $f(x) = 48 \cdot \frac{(x-470)\cdot(x-489)\cdot(x-508)}{(432-470)\cdot(432-489)\cdot(432-508)} \cdot$ $\cdot \frac{(x-565)\cdot(x-584)}{(432-565)\cdot(432-584)} + 50 \cdot \frac{(x-432)\cdot(x-489)}{(470-432)\cdot(470-489)} \cdot$ $\cdot \frac{(x-508)\cdot(x-565)\cdot(x-584)}{(470-508)\cdot(407-565)\cdot(470-584)} + 78 \cdot \frac{(x-432)}{(489-432)} \cdot$ $\cdot \frac{(x-470)\cdot(x-508)\cdot(x-565)\cdot(x-584)}{(489-470)\cdot(489-508)\cdot(489-565)\cdot(489-584)} +$ $+ 38 \cdot \frac{(x-432)\cdot(x-470)\cdot(x-489)\cdot(x-565)}{(508-432)\cdot(508-470)\cdot(508-489)\cdot(508-565)} \cdot$ $\cdot \frac{(x-584)}{(508-584)} + 24 \cdot \frac{(x-432)\cdot(x-470)\cdot(x-489)}{(565-432)\cdot(565-470)\cdot(565-489)} \cdot$ $\cdot \frac{(x-508)\cdot(x-584)}{(565-508)\cdot(565-584)} + 42 \cdot \frac{(x-432)\cdot(x-470)}{(489-432)\cdot(489-470)} \cdot$ $\cdot \frac{(x-489)\cdot(x-508)\cdot(x-565)}{(489-508)\cdot(489-565)\cdot(584-565)}$ Вільний член полінома і є таємниця	Отримані долі $\{101, 103, 98\}, \{101, 107, 5\}$, $\{101, 109, 16\}, \{101, 113, 50\}$, $\{101, 127, 41\}, \{101, 131, 8\}$, $\{101, 137, 42\}, \{101, 139, 105\}$, $\{101, 149, 33\}, \{101, 151, 114\}$ Відновлення таємниці $\{101, 107, 5\}$, $\{101, 109, 16\}$, $\{101, 113, 50\}$, $\{101, 131, 8\}$, $\{101, 139, 105\}$, $\{101, 151, 114\}$ Складемо відповідну систему конгруенцій $\begin{cases} x \equiv 5 \pmod{107} \\ x \equiv 16 \pmod{109} \\ x \equiv 50 \pmod{113} \\ x \equiv 8 \pmod{131} \\ x \equiv 105 \pmod{139} \\ x \equiv 114 \pmod{151} \end{cases}$ Розв'язавши систему конгруенцій відновимо таємницю

Порівняльний аналіз реалізованих схем

Схема Шаміра	**Схема Асмута-Блума**
Потребує генерації двох простих чисел.	Потребує генерації $2+n$ простих чисел, причому n простих чисел необхідно обрати у порядку зростання.
Кількість учасників, які можуть відновити таємницю задається одразу.	Необхідна перевірка заявлених долей на можливість відновлення таємниці.
Для обчислення долей будується поліном степеня $k-1$.	Для обчислення долей обирається випадкове число.
Обидві схеми крипостійкі до атак.	

Описані схеми також були реалізовані в математичному пакеті Maple, в середовищі Delphi та на мові програмування PHP. Математичні пакети Maxima та Maple оперують однаковими вбудованими функціями та виконують чисельні розрахунки високої точності. Завдяки цьому, на етапі відновлення таємниці, був побудований інтерполяційний многочлен Лагранжа та розв'язана система конгруенцій за допомогою китайської теореми про лишки. Що дає можливість відновлення таємниці. Але між цими математичними пакетами є певні відмінності. При виведенні результатів команд Maxima виводить кінцевий результат, а Maple виводить поетапне виконання вказаної команди. На відміну від комерційних Maple, та Delphi математичний пакет Maxima є вільно розповсюдженою системою комп'ютерної алгебри, яка розрахована на широке коло користувачів.

Мова PHP на відміну від вище згаданих математичних пакетів є серверною мовою web-програмування і має розвинену обчислювальну частину. Наявність в мові повноцінного набору керуючих конструкцій, дозволяє реалізовувати алгоритми будь-якої складності. Синтаксис мови майже співпадає із синтаксисом мови C, тому працювати з нею може вузьке коло користувачів.

Delphi дає можливість створювати програми в стилі візуального конструювання форм, розмістивши на них будь-які візуальні елементи. Середовище Delphi має складний інтерфейс. Програма в середовищі Delphi реалізує деякий код тільки як реакцію на події, які зумовлені діями користувачів (натискання кнопок, рух миші і тому подібне).

Висновки

В статті наведені приклади реалізації задачі поділу таємниці за схемами Шаміра та Асмута-Блума в системі компютерної алгебри Maxima. Проведений порівняльний аналіз реалізованих схем в різних програмних середовищах.

Література

[1] *Берник В.* Математические и компьютерные основы криптологии / В. Берник, С. Матвеев, Ю. Харин. – М.: Новое знание, 2003. – 382 с.

[2] *Саломаа А.* Криптография с открытым ключом : [пер. с англ.] / А. Саломаа. – М.: Мир, 1995. – 318 с.

[3] *Тилборг ван Х.К.А.* Системы разделения секрета : [пер. з англ.] / ван Х.К.А. Тилборг // Основы криптологии. Профессиональное руководство и интерактивный учебник. – М.: Мир, 2006. – С. 314 – 334.

[4] *Чичкарёв Е.А.* Компьютерная математика с Maxima. Руководство для школьников и студентов / Е.А. Чичкарёв. – М.: ALT Linux, 2009. – 233 с.
[5] *Шнайер Б.* Разделение секрета : [пер. с англ.] / Б. Шнайер // Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Триумф, 2002. – С. 93 – 96.
[6] *Шнайер Б.* Алгоритмы разделения секрета : [пер. с англ.] / Б. Шнайер // Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Триумф, 2002. – С. 588 – 591.

УДК 512.53

Рябухо О.М., Турка Т.В., Литвиненко Л.П.

[1] *канд. фіз.-мат. наук, доцент, зав. кафедри алгебри, СДПУ*

[2] *асистент кафедри алгебри, СДПУ*

[3] *студентка 5 курсу фізико-математичного факультету, СДПУ*

e-mail: kafedra_algebry_sdpu@mail.ru

НАПІВГРУПА ВІДПОВІДНОСТЕЙ СКІНЧЕННОЇ ГРУПИ

Дослідження полягає у вивченні напівгрупи відповідностей скінченної групи, зокрема обчислено порядки напівгрупи відповідностей знакозмінної групи четвертого порядку $S(A_4)$ та групи кватерніонів восьмого порядку $S(Q_8)$.

Ключові слова: *напівгрупа відповідностей, порядок напівгрупи, знакозмінна група, група кватерніонів.*

Вступ

Поняття напівгрупи та відповідний термін виникли на початку XX століття, а систематичні дослідження напівгруп почалися в кінці 20-х років. До 60-х років теорія напівгруп сформувалася в область алгебри, що динамічно розвивається, з багатою проблематикою і різноманітними застосуваннями. В ці роки з'явилися і перші монографії, які цілком присвячені теорії напівгруп.

Першим задачу вивчення напівгруп відповідностей поставив Курош О.Г. в своєму курсі з теорії універсальних алгебр (див. [1]). Однак зроблено в цьому напрямку небагато. Є кілька робіт (наприклад, Іскандер [2], [3]), де вивчалася будова напівгрупи $S(G)$ як решітки відносно природного часткового порядку. Але напівгрупи відповідностей конкретних універсальних алгебр майже не досліджувалися.