Бородин Андрей Викторович
канд. экон. наук, доцент, заведующий кафедрой
ФГБОУ ВО «Поволжский государственный технологический университет»
г. Йошкар-Ола, Республика Марий Эл
Уразаева Полина Сергеевна
соискатель
МОУ «Лицей №11 им. Т.И. Александровой»
г. Йошкар-Ола, Республика Марий Эл

DOI 10.21661/r-469647

ОБ ОДНОМ ПОДХОДЕ К РЕШЕНИЮ ЗАДАЧИ РАЗДЕЛЕНИЯ КЛЮЧА ДОСТУПА К СЕКРЕТУ

Аннотация*: в статье предложен оригинальный протокол разделения ключа доступа к секрету. Данный протокол отличается простотой реализации и интеграцией функций расшифровки и контроля целостности секрета в одной арифметической операции. Стойкость предлагаемого протокола основывается на трудоемкости решения задачи факторизации больших целых чисел.*

Ключевые слова*: аутентификация, идентификация, информационная безопасность, криптографический протокол, разделение секрета, тест на простоту, факторизация целых чисел, целостность, шифротекст.*

Введение

Информационные технологии – основа современной экономики, а безопасность информационных технологий – залог успешного развития институтов экономики. Соответственно, одной из актуальных задач информационной безопасности является задача разграничения доступа к информации. Для решения этой задачи человечество придумало множество (порой достаточно сложных) методов идентификации и аутентификации субъектов доступа. Кроме того, в ряде случаев, для повышения безопасности целесообразно право доступа к некоторым видам информации разделять между несколькими субъектами (обычно двумя: «two-man rule» [10], однако возможны иные ситуации [9]).

Целью данной работы является разработка простого и стойкого метода разделения ключа доступа к секрету между конечным количеством субъектов доступа, таким образом, чтобы доступ к секрету был возможен лишь при предъявлении частей ключа всеми соответствующими владельцами.

Методология исследования

Методологической базой данного исследования являются результаты современной теории чисел. В частности, были использованы результаты аналитической теории чисел о распределении простых чисел [4; 7] и оценки сложности алгоритмов факторизации больших целых чисел, полученные на основе анализа алгоритмов конструктивной части этой теории [3].

Для оценки наличия элементов новизны в данном исследовании использованы справочные материалы по прикладной криптографии, собранные и обобщенные Брюсом Шнайером [9].

Базовая идея

Предлагаемый протокол разделения секрета прост. Пусть s – секрет и пусть, для простоты, $s \in \mathbb{P}$. Здесь $\mathbb{P}$ – множество всех простых чисел. Предположим, мы хотим разделить право доступа к секрету между членами множества I. Для этого каждый член i этого множества конфиденциально предлагает некоторое случайно полученное простое число p_i в качестве своей части ключа, $p_i \in \mathbb{P}$, $i \in I$. Секрет сохраняется в виде шифра $c = s \times \Pi_{i \in I} p_i$.

Теперь для получения доступа к секрету s каждый член множества I конфиденциально в произвольном порядке предъявляет свою часть ключа, и компьютер легко реализует вычисление

$$s = \frac{c}{\Pi_{i \in I} p_i}.$$

Заметим, что при условии $\log_2 s > l$, $\log_2 p_i > l$, $i \in I$, где l – число порядка 200, атака на шифр c методом факторизации оказывается для современных компьютеров трудно разрешимой задачей.

При $l = 2000$ такую задачу факторизации можно считать практически не разрешимой в достаточной перспективе развития технического прогресса

человечества [3; 9]. Учитывая, что ограничение $s \in \mathbb{P}$ в данном протоколе легко преодолевается, предложенное решение поставленной задачи можно считать вполне работоспособным. Более того, данный шифр автоматически обеспечивает контроль целостности секрета по условию $s \in \mathbb{P}$ в предположении атаки в форме изменения c.

Развитие базовой идеи

Основным ограничением базовой идеи является условие простоты секрета: $s \in \mathbb{P}$. Для преодоления этого ограничения достаточно заметить, что согласно теореме о распределении простых чисел [4; 7] они встречаются достаточно часто, например, если искать простое число среди идущих одно за другим n-битовых натуральных чисел, то оно обязательно встретится в среднем в пределах $\lceil n \ln 2 \rceil$ шагов.

Таким образом, если мы имеем секрет s_0, $s_0 \notin \mathbb{P}$, то достаточно найти простое число s в последовательности $(s_0 + k)_{k=1,2,\ldots}$ и применить базовую идею к этому числу. Для проверки чисел на простоту удобно использовать комбинацию из нескольких элементарных тестов [3]: метода пробных делений на несколько сот первых простых чисел и теста на псевдопростоту в нескольких десятках значений базы. Обычно такого объема тестов достаточно. С вычислительной точки зрения – это относительно простая задача. Теперь процессу разделения секрета достаточно депонировать число $\Delta s = s - s_0$ вместе с шифром или предоставить его любому непустому подмножеству множества субъектов доступа I.

Предъявление значений p_i, $i \in I$, и Δs означает возможность восстановления секрета:

$$s_0 = \frac{c}{\Pi_{i \in I} p_i} - \Delta s. \quad (1)$$

Атака на этот шифр, все так же как и в базовом случае, сводится к проблеме факторизации c, как для отдельного субъекта хранения секрета, так и для

внешнего злоумышленника. Контроль целостности секрета сводится к проверке условий

$$c \equiv 0 \left(\mathrm{mod}\, \Pi_{i \in I}\, p_i \right) \quad (2)$$

и

$$\frac{c}{\Pi_{i \in I}\, p_i} \in \mathbb{P}.$$

Заметим, что проверка условия (2) является побочным эффектом выполнения операции деления в формуле (1).

Повышение стойкости протокола

Важно отметить слабую сторону предложенного протокола: в отдельных случаях факторизация c может оказаться существенно менее трудоемкой задачей, нежели решение этой задачи в общем случае. Рассмотрим эту ситуацию подробнее.

Если $c \equiv 0 \left(\mathrm{mod}\, q \right)$, $q \in \mathbb{P}$, и $q - 1$ разлагается на степени лишь небольших простых чисел, то факторизация c существенно упрощается [3]. Для преодоления этой уязвимости можно организовать процесс, состоящий из следующих шагов:

1. поиск (например, первого) простого числа $s_1 = s_0 + k_0$ в последовательности вида $\left(s_0 + k \right)_{k = 0, 1, \ldots}$;

2. поиск (также, например, первого) простого числа $s_{j+1} = 2 r_j\, s_j + 1$ в последовательности вида $\left(2 r\, s_j + 1 \right)_{r = 1, 2, \ldots}$, этот шаг повторяется m раз – для $j = 1, 2, \ldots, m$.

Если положить $s = s_{m+1}$, применить базовую идею и депонировать вместе с шифром c числа k_0, r_j, $j = 1, 2, \ldots, m$, то предъявление субъектами чисел p_i, $i \in I$, позволит восстановить секрет.

Передавать числа k_0, r_j, $j=1,2,\ldots,m$, субъектам разделения секрета в данном случае потенциально не безопасно, так как практическая разрешимость системы включений

$$\begin{cases} s_1 = s_0 + k_0 \in \mathbb{P}, \\ s_{j+1} = 2r_j s_j + 1 \in \mathbb{P}, \quad j=1,2,\ldots,m \end{cases}$$

относительно s_j, $j=0,1,\ldots,m$, требует дальнейшего исследования.

Новизна результатов исследования

Поиск принципов построения протокола разделения секрета, аналогичных предлагаемым в данной статье, в справочнике Брюса Шнайера [9] (по состоянию на 2016 год) результатов не дал. На сайте Брюса Шнайера и на ресурсах, по ссылкам с этого сайта, аналогов также найдено не было. Не дал результатов и поиск по известным авторам этой статьи другим русско- и англоязычным ресурсам сети Internet, посвященным криптографии. Все это позволяет сделать предположение о возможной существенной новизне изложенных результатов.

Практические приложения протокола

Тривиальным приложением предлагаемого протокола являются системы электронного депонирования документов [8]. Другой тривиальной задачей, решаемой этим протоколом, может быть задача разделения пароля доступа к ресурсу между несколькими администраторами. Например, пароль доступа с правами администратора к операционной системе (ОС) сервера базы данных (БД) может быть зашифрован на трех ключах (администратора ОС, администратора БД и офицера безопасности) для обеспечения принципа «two-man rule» (с учетом различия компетенций участников) при выполнении любых разновидностей действий по администрированию системы. Для хранения ключей могут быть использованы персональные аппаратные носители.

Потенциально интересным приложением данного протокола может быть использование его в обфусцированном программном коде, когда корректная функциональность кода обеспечивается лишь при совместном наступлении нескольких событий, при этом каналы информирования о наступлении этих

событий секретны. Данный эффект может быть обеспечен множеством секретов, представляющих из себя начальный элемент циклической группы, определяющей поток команд [1].

Другой сферой потенциального использования предложенного протокола является использование его в реализациях вредоносного программного обеспечения [2], где также важны вычисления на данных из скрытых каналов.

Заключение

В среде GAP версии 4.5.6 [5, 6] был создан прототип предложенного механизма разделения ключа для доступа к секрету. Выбор среды обусловлен простотой встроенного языка программирования, а также тем, что в этой среде реализована машинная арифметика высокой разрядности, присутствует реализация достаточно эффективного алгоритма факторизации больших целых чисел, имеется API для работы с файлами. Следует отметить, что наличие в указанной среде реализации алгоритма факторизации важно с точки зрения демонстрации и изучения генезиса стойкости предложенного решения поставленной задачи.

Список литературы

1. Бородин А.В. Линейные конгруэнтные последовательности максимального периода в задачах обфускации программ // Кибернетика и программирование. – 2016. – №6. – С. 1–19.

2. Бородин А. В. Феномен компьютерных вирусов: элементы теории и экономика существования. – Йошкар-Ола: Марийский государственный технический университет, 2004. – 144 с.

3. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. – М.: МЦНМО, 2003. – 328 с.

4. Диамонд Г. Элементарные методы в изучении распределения простых чисел // Успехи математических наук. – 1990. – Т. 45. – В. 2 (272). – С. 79–114.

5. Коновалов А.Б. Система компьютерной алгебры GAP. – Запорожье: Запорожский государственный университет, 1999. – 42 с.

6. Коновалов А.Б. Система компьютерной алгебры GAP 4.4 (Brief GAP Guidebook in Russian). Редакция 3.0.2. – 07.04.2009. – 87 с. [Электронный

ресурс]. – Режим доступа: http://www.gap-system.org/ukrgap/gapbook/ manual.pdf (дата обращения: 11.02.2018).

7. Чебышев П.Л. Избранные труды. – М.: Изд-во АН СССР, 1955. – 929 с.

8. Шихалеев И.А. Экономика безопасности технологических процессов электронного депонирования документов / И.А. Шихалеев, А.М. Сокольников, А.В. Бородин // Человек, общество, природа в эпоху глобальных трансформаций: безопасность и развитие. Семнадцатые Вавиловские чтения: Материалы постоянно действующей международной междисциплинарной конференции. Ч. 2. – Йошкар-Ола: Поволжский государственный технологический университет, 2014. – С. 264–265.

9. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходный код на С. – М.: Вильямс, 2016. – 1024 с.

10. Two-man rule // Wikipedia. The Free Encyclopedia. – [Электронный ресурс] – Режим доступа: https://en.wikipedia.org/wiki/Two-man_rule (дата обращения: 12.02.2018).