УДК *003.26*

Р. Ю. Шлаустас [1]***, Е. Е. Калинская*** [1]

[1] *Иркутский государственный университет путей сообщения, г. Иркутск, Российская федерация*

КРИПТОГРАФИЧЕСКОЕ ПРИМЕНЕНИЕ ТРАНСЦЕНДЕНТНЫХ ФУНКЦИЙ

Аннотация: *Статья посвящена распространенному во все времена способу защиты информации при её передаче – шифрованию. В статье впервые предлагается алгоритм шифрования, основанный на применении в качестве ключей длинных непериодических последовательностей цифр, представляющих собой трансцендентные числа. Данный метод шифрования объединяет в себе признаки алгоритмов симметричного шифрования, алгоритмов шифрования с открытым ключом, а также обладает чертами совершенного шифра. В ходе опытной реализации алгоритм показал высокую скорость работы.*

Ключевые слова: *Криптография, симметричное шифрование, шифрование с открытым ключом, трансцендентные числа.*

R. Yu. Shlaustas [1]***, E. E .Kalinskaya*** [1]

[1] *Irkutsk State Transport University, Irkutsk, the Russian Federation*

CRYPTOGRAPHIC APPLICATION OF TRANSCENDENTAL FUNCTIONS

Abstract: *The article is devoted to the widespread at all times method of information security during its transmission – encryption. The article for the first time proposes an encryption algorithm based on the use of long non-periodic sequences of numbers that represent transcendental numbers as keys. This encryption method combines the features of symmetric encryption algorithms, public key encryption algorithms, and has the features of a perfect cipher. During the experimental implementation, the algorithm showed high speed.*

Keywords: *Cryptography, symmetric encryption, public-key encryption, transcendental numbers.*

Криптография изучает и применяет различные методы шифрования информации — обратимого преобразования исходной информации на основе секретного алгоритма или ключа в шифрованный текст.

Традиционная криптография использует симметричные криптосистемы, в которых шифрование и дешифрование проводится с использованием одного и того же секретного ключа. Наиболее распространенные их них — это алгоритмы DES, AES, ГОСТ 28147-89, Camellia, Twofish, Blowfish, IDEA, RC4 и ряд других [1,2,3,4,5]. Наиболее важным требованием к симметричному шифру является полная утрата всех статистических закономерностей исходного сообщения. Другое требование, которое также имеет место, — это изменение даже одного бита в исходной информации приводит к полной перестройке шифрограммы. Третье свойство симметричных систем — это отсутствие линейности.

Другое направление криптографии — применение несимметричных (двухключевых) криптосистем. Примеры их — системы RSA, Elgamal (Эль-Гамаль), Диффи-Хелмана [1,2,3,4,5]. Основа этих методов — невозможность за приемлемое время получить разложение на множители больших, в несколько сотен цифр, чисел или решить задачу дискретного логарифмирования также для очень больших оснований и показателей.

Третье направление — бесключевые алгоритмы построения дайджестов исходной информации — хэш значений. Здесь также имеется множество различных алгоритмов. Их примеры — хэш-функции MD4, MD5, MD6, SHA-1, SHA-2, ГОСТ Р 34.11-2012 («Стрибог») [2,3,5].

Существующие методы криптографического преобразования информации используют ключи определенной длины [6]. Алгоритмы шифрования часто состоят из некоторого множества шагов. Например, алгоритмы, построенные на основе сетей Фейстеля или близких к ним (DES, AES, ГОСТ-89 и др.), применяют на каждом раунде преобразования ключей пре-

дыдущего раунда по определенному закону [3,5] Выполнение этой операции требует определенного времени.

Избавиться от такого преобразования можно, если в качестве ключей каждого раунда применить числа, являющиеся отрезками значения трансцендентных функций в некоторой рациональной точке. Среди таковых можно отметить такие элементарные функции как показательные, логарифмические или тригонометрические. Из их теории известно [7,8], что значения этих функций представляются непериодическими последовательностями цифр (кроме некоторых характерных значений аргумента).

Таким образом, выбирая заранее какую-либо трансцендентную функцию, совсем не обязательно из элементарных, значение ее аргумента, а также начальную цифру в представлении ее значения, можно сформировать последовательность ключей каждого раунда. При этом на каждом раунде даже можно усложнить задачу шифрования, выбирая разные длины последовательностей.

Можно предложить и более простой вариант применения трансцендентных чисел, как значений трансцендентных функций, подобно методу Вернама [1,9].

Такой алгоритм будет отвечать положениям совершенного шифра [1]. Это следует из того факта, что длина исходной информации и длина ключевой будут иметь близкие значения.

Отметим, что принимающей стороне необходимо передать лишь номер трансцендентной функции, значение аргумента, начальный номер первой цифры ее числового значения и, возможно, длину употребляемой последовательности цифр или то, как она может меняться от раунда к раунду.

В этом плане, предлагаемый алгоритм имеет черты симметричного алгоритма и, одновременно, черты алгоритма шифровании с открытым ключом, так как необходимая информация для дешифрования может быть передана в открытой форме.

Возникает лишь две проблемы.

Первая из них — как получить длинные последовательности цифр, представляющих значения функций. Данная задача легко решается. Для этого достаточно применить один из математических пакетов (например, MAPLE или Mathcad [10]). Они позволяют вычислить значения многих трансцендентных функций с большим числом десятичных знаков. Для других функций можно написать программы вычисления значений на основе рядов, представляющих функцию для рациональных значений аргумента с необходимым количеством десятичных цифр. Еще один вариант возникает при использовании специальных типов данных в языках программирования Pascal ABC или C++ (типа BigInteger).

Вторая проблема — тайное хранение информации о применяемых трансцендентных функциях. Информацию о трансцендентных функциях, их аргументах, длинах значений этих функций можно передать абонентам один раз. По мере необходимости проводить ее корректировку через некоторые промежутки времени. Естественно, требуется предпринять определенные меры по безопасному хранению такой информации.

В качестве примера применения трансцендентных чисел была составлена программа на Delphi 7. Исходная информация может быть набрана пользователем в окно редактирования слева, либо выбрана из текстового файла после нажатия соответствующей кнопки. Результат шифрования поступает в файл, однако, если открыть его в текстовом редакторе, прочесть ничего не удастся, будут видимы так называемые “кракозябры”. Для дешифрования нужно выбрать файл с криптограммой, ввести правильную ключевую информацию и нажать нужную кнопку. Результат поступает в окно слева и еще в файл, так как можно шифровать файлы любой структуры, не обязательно текстовые.

В качестве трансцендентного числа взято число $\pi = 3{,}14159265\ldots$ с 345 знака. На рис. 1 приведен пользовательский интерфейс программы.

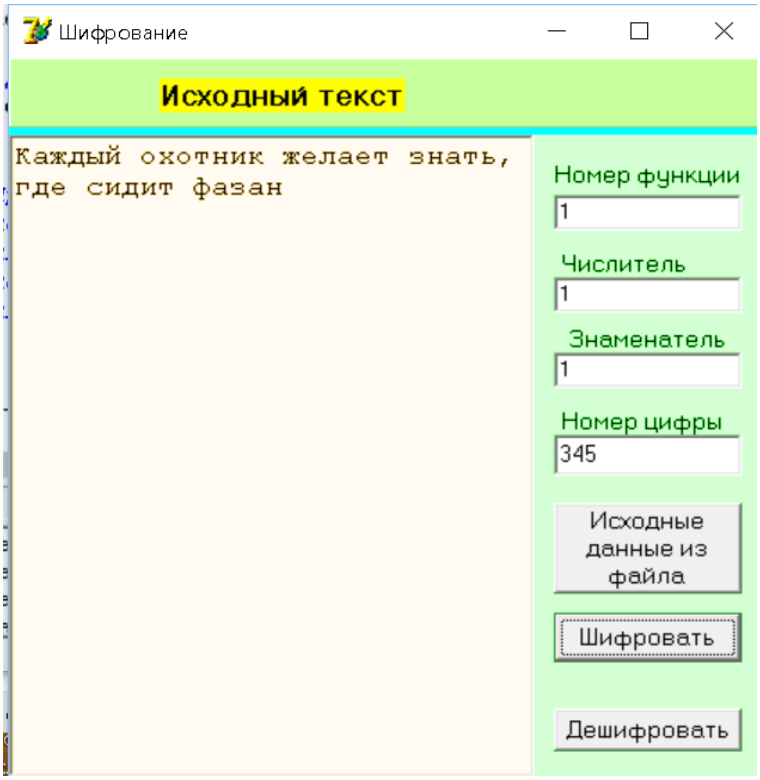

Рис. 1. Графический интерфейс программы шифрования/дешифрования

Порядок действий в программе следующий:

1. Считываются четыре символа;
2. Осуществляется их конкатенация в четырехбайтную величину;
3. Считываются 10 цифр, начиная с 345 цифры трансцендентного числа;
4. Из первых девяти цифр генерируется четырехбайтная величина;
5. Из десятой цифры вдвигаются три бита в число из четвертого шага;
6. С полученными двумя числами осуществляется операция XOR;
7. Результат сохраняется в файл;
8. Операции 1-7 проводятся до исчерпания исходной информации.

Отметим, что операции 4-5 нужны для получения 32-битной величины. Если имеется двоичное представление ключевой информации, то вместо шагов 3-5 достаточно считать 32 бита и превратить их в 32-битное число.

Так как длина исходной информации в общем случае не кратна 4, то можно записать в ее начало зашифрованное значение длины исходной информации длиной 4 байта, как это реализовано в программе, и при расшифровке последней группы байтов, учитывая этот факт, оставить нужное число байтов. При шифровании последний блок дополняется до 4-х байтов.

Отметим, длина криптограммы будет в этом случае кратна 4.

Оценка скорости вычислений также легко проводится. Достаточно провести операцию шифрования/дешифрования много раз. Так, для заданной в примере информации проведенное 1000 раз шифрование с перезаписью файла заняло всего **2-4 секунды** на машине с частотой процессора около 2Ггц в зависимости от типа центрального процессора**.** Большая часть этого времени уходит на операции с дисковым файлом. Избавиться в случае длинной исходной информации от многочисленных файловых операций можно путем использования оперативной памяти или отображаемых в память файлов, когда запись на диск будет проводиться всего один раз. Сказанное позволяет говорить, что предлагаемый метод окажется значительно быстрее даже при программной реализации, чем многораундовые симметричные алгоритмы и, тем более несимметричные системы.

Два других преимущества — легко допускает распараллеливание, исходный файл разбивается на части, каждая их них шифруется в своем Thread'е (потоке исполнения). Наконец, зашифрованный блок из 4 байтов может быть передан сразу вне зависимости от других.

Большей стойкости к взлому можно добиться путем повторного применения шифрования с ключом, начинающимся с другой позиции трансцендентного числа, либо применения более сложных приемов запутывания.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. А. Г. Ростовцев, Е. Б. Маховенко Теоретическая криптография. //НПО «Профессионал», Санкт-Петербург, 2016. – 478с.

2. Ш.Т. Ишмухаметов, Р.Г. Рубцова Математические основы защиты информации. Электронное учебное пособие// КФУ, ИВМиИТ, Казань, 2012 – 139с.

3. Г.В. Басалова Основы криптографии//ИНТУИТ, Москва, 2016. — 281с.

4. Б.А. Фороузан Математика криптографии и теория шифрования. //ИНТУИТ, Москва, 2016. — 511с.

5. О.Н.Жданов В.В.Золотарев Методы и средства криптографической защиты информации// СибГАУ, Красноярск, 2007. – 217 с.

6. [Электронный ресурс] URL: https://studfiles.net/preview/2886463/page:8/ (дата обращения: 09.01.2019).

7. А. О. Гельфонд Трансцендентные и алгебраические числа// Государственное издательство технико-теоритической литературы, Москва, 1952 – 224 с.

8. Ю. В. Нестеренко Теория чисел//Издательский дом «Академия», Москва, 2008. – 272с.

9. Венбо Мао Современная криптография: теория и практика//Издательский дом «Вильямс», Москва, 2005, – 768с.

10. [Электронный ресурс] URL: https://compress.ru/article.aspx?id=16152 (дата обращения: 09.01.2019).

REFERENCES

1. A. G. Rostovtsev, E. B. Makhovenko, Theoretical cryptography. // NPO "Professional", St. Petersburg, 2016. – 478p.

2. Sh. T. Ishmukhametov, R. G. Rubtsova Mathematical bases of information protection. Electronic textbook// KFU, IVMiIT, Kazan, 2012 – 139p.

3. G.V. Basalova, Fundamentals of Cryptography // INTUIT, Moscow, 2016. - 281 p.

4. B. A. Forouzan Mathematics of cryptography and encryption theory. //INTUIT, Moscow, 2016. - 511c.

5. O. N. Zhdanov V. V. Zolotarev Methods and means of cryptographic protection of information// of SibSAU, Krasnoyarsk, 2007. - 217 p.

6. [Electronic resource] URL: https://studfiles.net/preview/2886463/page:8/ (date: 09.01.2019).

7. A. O. Gel'fond Transcendental and Algebraic Numbers // State Publishing House of Technical and Theoretical Literature, Moscow, 1952–224 p.

8. Yu. V. Nesterenko Theory of numbers// Publishing house "Academy", Moscow, 2008. – 272p.

9. Wenbo Mao, Modern cryptography: theory and practice// Publishing house "Williams", Moscow, 2005, – 768p.

10. [Electronic resource] URL: https://compress.ru/article.aspx?id=16152 (date: 09.01.2019).

Информация об авторах

Шлаустас Ромас Юргевич — к. ф.-м. н., доцент кафедры «Информационные системы и защита информации», Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: shlaustas@gmail.com

Калинская Екатерина Евгеньевна — магистрант., кафедра «Информационные системы и защита информации», Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: ekaterina.kalinskaya@mail.ru

Authors

Shlaustas Romas Yurgevitch — Ph.D., in phisics and mathematics, Assistant Professor of "Information Systems and Information Protection", Irkutsk State Transport University, Irkutsk, e-mail: shlaustas@gmail.com

Kalinskaya Ekaterina Evgen'evna — undergraduate, "Information Systems and Information Protection", Irkutsk State Transport University, Irkutsk, e-mail: ekaterina.kalinskaya@mail.ru

Для цитирования

Шлаустас Р. Ю., Калинская Е. Е. Криптографическое применение трансцендентных функций. / Р.Ю. Шлаустас, Е.Е. Калинская, // «Информационные технологии и математическое моделирование в управлении сложными системами»: электрон. науч. журн. – 2019. – №2. – С. 69-73 – Режим доступа: http://ismm-irgups.ru/toma/23-2019, свободный. – Загл. с экрана. – Яз. рус., англ. (дата обращения: 19.06.2019)

For citation

Shlaustas R.Yu., Kalinskaya E.E. *Kriptograficheskoye primeneniye transtsendentnykh funktsiy* [Cryptographic application of transcendental functions] // *Informacionnye tehnologii i matematicheskoe modelirovanie v upravlenii slozhnymi sistemami: ehlektronnyj nauchnyj zhurnal* [Information technology and mathematical modeling in the management of complex systems: electronic scientific journal], 2019. No. 2. P. 69-73 – Access mode: http://ismm-irgups.ru/toma/23-2019, free. – Title from the screen. – Language Russian, English. [Accessed 19/06/19]