УДК 003.26

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

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

ПОСТРОЕНИЕ ЭЛЕКТРОННОЙ ПОДПИСИ НА ОСНОВЕ ТРАНСЦЕНДЕНТНЫХ ЧИСЕЛ

***Аннотация*:** Статья посвящена распространенному во все времена способу защиты информации при её передаче – шифрованию и цифровой подписи на основе применения трансцендентных чисел как значений трансцендентных функций. Указана криптостойкость алгоритма шифрования и построения цифровой подписи на основе значений трансцендентных функций.

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

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

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

CONSTRUCTION OF ELECTRONIC SIGNATURE BASED ON TRANSCENDENT NUMBERS

***Abstract*:** The article focuses on the best-time way to protect information when it is transmitted - encryption and digital signature based on the use of transcendent numbers as values of transcendental functions. The crypto-resilience of the encryption and digital signature algorithm based on the values of transcendental functions is specified.

***Keywords*:** Cryptography, symmetrical encryption, open key encryption, transcendent numbers, digital signature, crypto resistance.

Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией, которая используется для определения лица, подписывающего информацию [1]. Электронная подпись формируется в результате криптографического преобразования информации с использованием закрытого ключа. Такая подпись позволяет не только идентифицировать владельца ключа, а также установить отсутствие искажения информации в электронном документе.

Первой и наиболее известной во всем мире конкретной системой ЭЦП стала система RSA, математическая схема которой была разработана в 1977 г. в Массачуссетском технологическом институте США.

Сначала необходимо вычислить пару ключей (секретный ключ и открытый ключ). Для этого отправитель (автор) электронных документов вычисляет два больших простых числа P и Q, затем находит их произведение $N = P \cdot Q$ и значение функции $\varphi(N) = (P-1)(Q-1)$. Далее отправитель вычисляет число E из условий: $E \leq \varphi(N), НОД\big(E, \varphi(N)\big) = 1$ и число D из условий: $D < N, E \cdot D \equiv 1(mod\ \varphi(N))$.

Пара чисел (E, N) является открытым ключом. Эту пару чисел автор передает партнерам по переписке для проверки его цифровых подписей. Число D сохраняется автором как секретный ключ для подписывания [2].

Недостатки алгоритма цифровой подписи RSA.

1. При вычислении модуля N, ключей E и D для системы цифровой подписи RSA необходимо проверять большое количество дополнительных условий, что сделать практически трудно. Невыполнение любого из этих условий делает возможным фальсификацию цифровой подписи со стороны того, кто обнаружит такое невыполнение. При подписании важных документов нельзя допускать такую возможность даже теоретически.

2. Для обеспечения криптостойкости цифровой подписи RSA по отношению к попыткам фальсификации на уровне, например, национального стандарта США на шифрование информации (алгоритм DES, уже устаревший), т.е. 10^{18}, необходимо использовать при вычислениях N, D и E целые числа не менее 2^{512} (или около 10^{154}) каждое, что требует больших вычислительных затрат, превышающих на 20...30% вычислительные затраты других алгоритмов цифровой подписи при сохранении того же уровня криптостойкости. В последнее время количество битов рекомендуется в количестве 1024 и, даже, 2048. В декабре 2019 года разложено на множители полупростое число 796 битов. Сложность разложения на множители очень быстро возрастает при росте разлагаемого числа.

3. Цифровая подпись RSA уязвима к так называемой мультипликативной атаке. Иначе говоря, алгоритм цифровой подписи RSA позволяет злоумышленнику без знания секретного ключа D сформировать подписи под теми документами, у которых результат хэширования можно вычислить как произведение результатов хэширования уже подписанных документов [2].

Более надежный и удобный для реализации на персональных компьютерах алгоритм цифровой подписи был разработан в 1984 г. американцем арабского происхождения Тахером Эль Гамалем. В 1991 г. НИСТ США обосновал перед комиссией Конгресса США выбор алгоритма цифровой подписи Эль Гамаля в качестве основы для национального стандарта[2]. Основан на невозможности в приемлемое время решить задачу определения дискретного логарифма.

Для того чтобы генерировать пару ключей (открытый ключ - секретный ключ), сначала выбирают некоторое большое простое целое число P и большое целое число G, причем $G < P$. Отправитель и получатель подписанного документа используют при вычислениях одинаковые большие целые числа P (~10^{308} или ~2^{1024}) и G (~10^{154} или ~2^{512}), которые не являются секретными.

Отправитель выбирает случайное целое число X, $1 < X \leq (P-1)$, и вычисляет $Y = G^X mod\ P$.

Число Y является открытым ключом, используемым для проверки подписи отправителя. Число Y открыто передается всем потенциальным получателям документов.

Число X является секретным ключом отправителя для подписывания документов и должно храниться в секрете.

Схема цифровой подписи Эль Гамаля имеет ряд преимуществ по сравнению со схемой цифровой подписи RSA:

1. При заданном уровне стойкости алгоритма цифровой подписи целые числа, участвующие в вычислениях, имеют запись на 25% короче, что уменьшает сложность вычислений почти в два раза и позволяет заметно сократить объем используемой памяти. Хотя в последнее время это преимущество несколько отходит на задний план из-за наличия у современных компьютеров большого объема памяти и значительного увеличения производительности.

2. При выборе модуля P достаточно проверить, что это число является простым и что у числа (P-1) имеется большой простой множитель (т.е. всего два достаточно просто проверяемых условия).

3. Процедура формирования подписи по схеме Эль Гамаля не позволяет вычислять цифровые подписи под новыми сообщениями без знания секретного ключа (как в RSA).

Однако алгоритм цифровой подписи Эль Гамаля имеет и некоторые недостатки по сравнению со схемой подписи RSA. В частности, длина цифровой подписи получается в 1,5 раза больше, что, в свою очередь, увеличивает время ее вычисления.

Алгоритм цифровой подписи *DSA* (*Digital Signature Algorithm*) предложен в 1991 г. в НИСТ США для использования в стандарте цифровой подписи DSS (Digital Signature Standard). Алгоритм DSA является развитием алгоритмов цифровой подписи Эль Гамаля и К.Шнорра.

Отправитель и получатель электронного документа используют при вычислении большие целые числа: G и P – простые числа, L бит каждое ($512 \leq L \leq 1024$); q – простое число

длиной 160 бит (делитель числа (P-1)). Числа G, P, q являются открытыми и могут быть общими для всех пользователей сети.

Отправитель выбирает случайное целое число X, 1 < X < q. Число X является секретным ключом отправителя для формирования электронной цифровой подписи.

Затем отправитель вычисляет значение $Y = G^X mod\ P$.

Число Y является открытым ключом для проверки подписи отправителя и передается всем получателям документов.

По сравнению с алгоритмом цифровой подписи Эль Гамаля алгоритм DSA имеет следующие основные преимущества:

1. При любом допустимом уровне стойкости, т.е. при любой паре чисел G и P (от 512 до 1024 бит), числа, генерируемые в ходе алгоритма, имеют длину по 160 бит, сокращая длину подписи до 320 бит.
2. Сокращено время вычисления подписи.
3. Сокращен объем памяти и время вычисления.

Отечественный стандарт цифровой подписи обозначается как ГОСТ Р 34.10-94. Алгоритм цифровой подписи, определяемый этим стандартом, концептуально близок к алгоритму DSA В нем используются следующие параметры:

p - большое простое число длиной от 509 до 512 бит либо от 1020 до 1024 бит;

q - простой сомножитель числа (p-1), имеющий длину 254...256 бит;

a - любое число, меньшее (p-1), причем такое, что $a^q \bmod p = 1$;

x - некоторое число, меньшее q;

$y = a^x \bmod p$.

Кроме того, этот алгоритм использует однонаправленную хэш-функцию H(x). Стандарт ГОСТ Р 34.11-94 определяет хэш-функцию, основанную на использовании стандартного симметричного алгоритма ГОСТ 28147-89.

Первые три параметра p, q, a являются открытыми и могут быть общими для всех пользователей сети. Число x является секретным ключом. Число y является открытым ключом.

В отечественном стандарте ЭЦП параметр q имеет длину 256 бит. Западных криптографов вполне устраивает q длиной примерно 160 бит. Различие в значениях параметра q является отражением стремления разработчиков отечественного стандарта к получению более безопасной подписи.

Этот стандарт вступил в действие с начала 1995 г.

Принципиальным моментом в системе ***ЭЦП*** является невозможность подделки ЭЦП пользователя без знания его секретного ключа подписывания.

Каждая подпись содержит следующую информацию:

- дату подписи;
- срок окончания действия ключа данной подписи;
- информацию о лице, подписавшем файл (Ф.И.О., должность, краткое наименование фирмы);
- идентификатор подписавшего (имя открытого ключа);
- собственно цифровую подпись.

Электронная подпись может быть реализована по одному из представленных алгоритмов на рисунке 1. В качестве хэш-функции может использоваться алгоритм хеширования SHA-256. Шифрование производиться с помощью алгоритма с применением трансцендентных функций описанному в предыдущей статье [3].

Слева на рис.1 документ пересылается в открытой форме. Важно лишь то, что документ будет прислан в неискаженной форме и когда не требуется скрывать его содержание.

Справа на рис. 1 приведена передача документа в зашифрованной форме. Дополнительно шифруется его хэш-дайджест.

Вместо алгоритма SHA-256 может быть применен какой-либо другой с достаточно устойчивым к взлому методом.

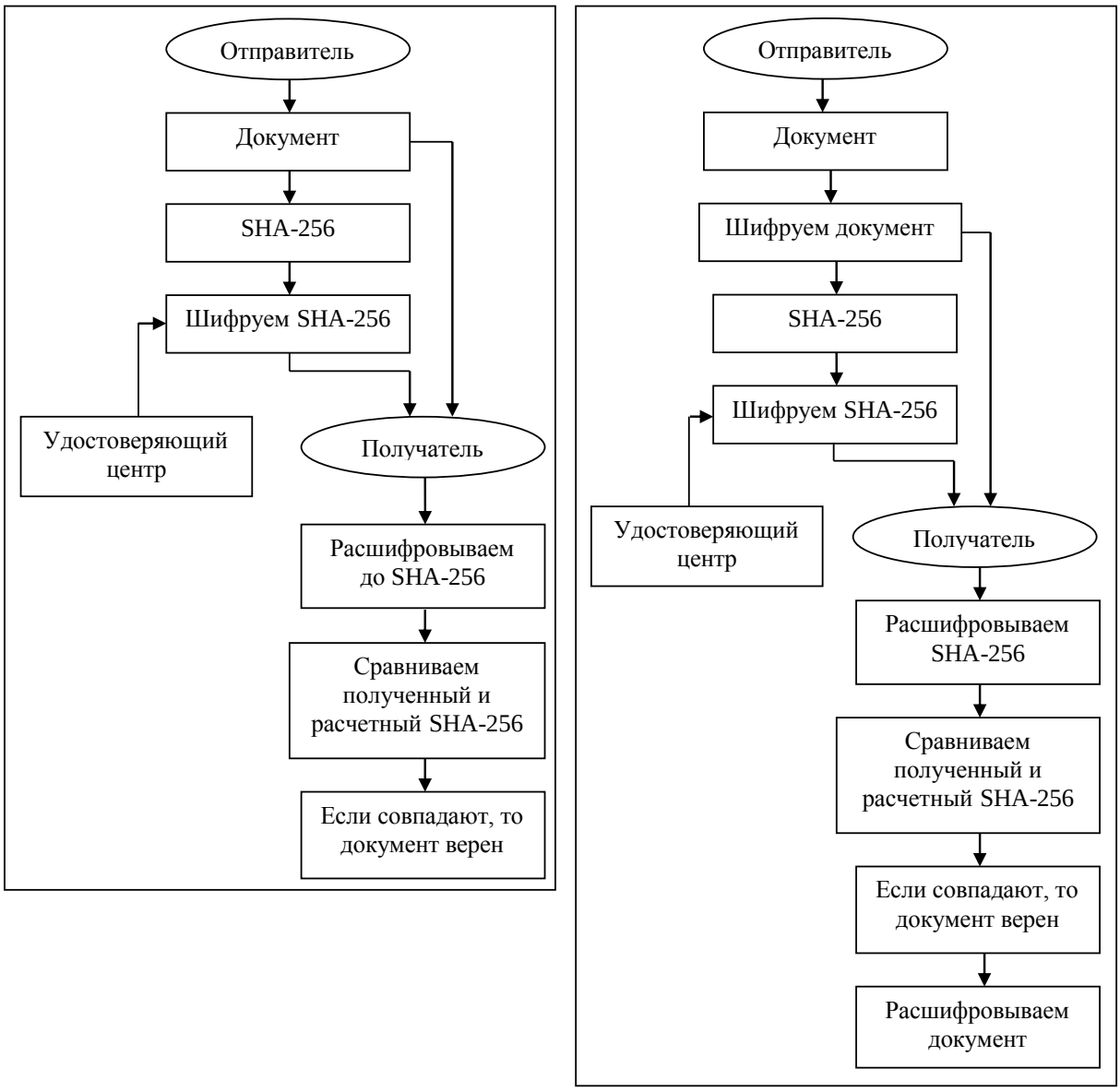

Рисунок 1

Для подтверждения подлинности отправителя может быть применен цифровой сертификат, представляющий собой приложение к электронному сообщению, применяемое в целях защиты, в основном для проверки того, что отправитель сообщения является тем, за кого он себя выдает, и предоставляющее получателю возможность зашифровать ответ.
Лицо, желающее отправить зашифрованное сообщение, обращается для получения цифрового сертификата к уполномоченной организации по цифровым сертификатам **(CA — Certificate Authority).** Удостоверяющий центр выпускает зашифрованный цифровой сертификат, содержащий открытый ключ заявителя и много другой идентификационной информации. Сама организация предоставляет собственный открытый ключ для всеобщего доступа с помощью публикаций в открытой печати или в Internet. Эти ключи также могут быть сформированы с помощью алгоритма из [3].

Получатель зашифрованного сообщения использует *открытый ключ CA* для дешифровки цифрового сертификата, прилагаемого к сообщению, убеждается в том, что сертификат действительно выпущен организацией CA, а затем получает открытый ключ отправителя и идентификационную информацию (напомним, что эти данные хранятся вместе с сертификатом). Имея эту информацию, получатель может отправить зашифрованный ответ. Органи-

зация СА выполняет в этом процессе исключительно важную роль, поскольку действует в качестве посредника между заинтересованными сторонами.

Если посмотреть на рис. 1, то этот сертификат может быть присоединен перед формированием хэша SHA-256, как левого, так и правого способов.

Абсолютно стойкий шифр

Клод Шеннон в 1945 году в одной из своих работ ввел понятие абсолютно стойкого шифра, а также доказал, что абсолютно стойкий шифр должен обладать определенными свойствами[4]. Шенноном было доказано, что примером абсолютно стойкого алгоритма является шифр Вернама (одноразовый блокнот). Иными словами, корректное использование шифра Вернама не даёт злоумышленнику никакой информации об открытом тексте (любой бит сообщения он может лишь угадать с вероятностью 1/2) [4].

Абсолютно стойкий шифр — шифр, характеризующийся тем, что криптоаналитик принципиально не сможет извлечь статистическую информацию относительно выбираемых ключей из перехватываемого шифротекста:

- ключ генерируется для каждого сообщения (каждый ключ используется только один раз);
- ключ статистически надёжен (то есть вероятности появления каждого из возможных символов равны, символы в ключевой последовательности независимы и случайны);
- длина ключа равна или больше длины сообщения;
- исходный (открытый) текст обладает некоторой избыточностью (что является критерием оценки правильности расшифровки).

Криптографический алгоритм с применением трансцендентных чисел в качестве ключа удовлетворяет вышеперечисленным условиям, благодаря свойствам трансцендентных чисел. Трансцендентное число (трансцендентные функции) – представляет собой бесконечную, не периодичную последовательность. В алгоритме ключ формируется для каждого сообщения благодаря тому, что есть возможность выбирать начальное значение, а именно начальный номер первой цифры числового значения трансцендентного числа. Второе условие достигается благодаря тому, что трансцендентное число обладает не периодичной последовательностью. Благодаря тому, что трансцендентное число бесконечно, можно зашифровать сообщение любой длины, таким образом, выполняется третье условие.

Стойкость алгоритма с применением трансцендентных функций обусловлена тремя основными составляющими:

- Неизвестна применяемая трансцендентная функция, для которой известны представления в виде бесконечных рядов. Таковых функций, приведенных в [12, 13], несколько тысяч. У авторов [13] имеется еще несколько книг, освященных данной тематике. Таким образом, множество общеупотребительных книг будет $10^{\alpha}, \alpha = 4.$
- Неизвестна позиция цифр в представлении значения функции. Можно заранее вычислить порядка $10^{\beta}, \beta = 6$ цифр. Используя представления в виде рядов от рациональных значений аргументов, достаточно просто вычислить любое число десятичных знаков. Например, число π или e известны со многими десятками миллионов знаков (больше 10^8 десятичных знаков).
- Выбирая аргумент трансцендентной функции в виде рационального числа, можно построить множество таких значений. Для числителя и знаменателя количество таких значений можно взять по $10^{\gamma}, \gamma = 10$.

Отмеченные пункты дают $10^{\alpha+\beta+\gamma+\gamma} \approx 10^{30}$ вариантов. Кроме этого, можно предусмотреть непоследовательность выбора групп цифр для запутывания криптоаналитика. В качестве элементов запутывания можно предусмотреть сдвиги битов или вращения битов (**rcl, rcr** или подобные команды ассемблера)

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон «Об электронной подписи» от 06.04.2011 № 63-ФЗ, принят Государственной Думой 25 марта 2011 года.
2. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. //Под ред. В.Ф. Шаньгина. - 2-е изд., перераб. и доп. //Радио и связь, Москва, 2001. - 376 с.
3. Шлаустас Р. Ю., Калинская Е. Е. Криптографическое применение трансцендентных функций. / Р.Ю. Шлаустас, Е.Е. Калинская, // «Информационные технологии и математиче-ское 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: 19.12.2019)
4. Шеннон К. Теория связи в секретных системах // Работы по теории информации и кибернетике / Перевод С. Карпова. — М.: ИЛ, 1963. — 830 с.
5. Зубов А.Ю. Криптографические методы защиты информации. Совершенные шифры. М..: Гелиос АРВ, 2005. — 160 с.
6. Венбо Мао Современная криптография: теория и практика. //Издательский дом «Вильямс», Москва, 2005, – 768с.
7. А. Г. Ростовцев, Е. Б. Маховенко Теоретическая криптография. //НПО «Профессионал», Санкт-Петербург, 2016. – 478с.
8. Ш.Т. Ишмухаметов, Р.Г. Рубцова Математические основы защиты информации. Электронное учебное пособие. // КФУ, ИВМиИТ, Казань, 2012 – 139с.
9. Б.А. Фороузан Математика криптографии и теория шифрования. //ИНТУИТ, Москва, 2016. — 511с.
10. А. О. Гельфонд Трансцендентные и алгебраические числа// Государственное издательство технико-теоритической литературы, Москва, 1952 – 224 с.
11. Ю. В. Нестеренко Теория чисел//Издательский дом «Академия», Москва, 2008. – 272с.
12. И.С. Градштейн, и И.М. Рыжик Таблицы интегралов, сумм, рядов и произведений. //Изд-во «Наука», Москва, 1971. -1108с.
13. А.П. Прудников, Ю.Ф. Брычков, О.И. Маричев. Интегралы и ряды. Специальные функции. //Изд-во «Наука», Москва, 1983. – 752.

REFERENCES

1. The Federal Law “On Electronic Signature” of 06/04/2011 No. 63-FZ, adopted by the State Duma on March 25, 2011.
2. Romanets, Yu.V., Timofeev, PA, Shangin, V.F. Information security in computer systems and networks. // Ed. V.F. Shangina. - 2nd ed., Pererab. and add. // Radio and communication, Moscow, 2001. - 376 pp.
3. 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: elec-tronic 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 19/12/19]
4. Shannon K. Communication Theory in Secret Systems // Works on Information Theory and Cybernetics / Translation by S. Karpov. - M.: IL, 1963. - 830 p.
5. Zubov A.Yu. Cryptographic methods of information security. Perfect ciphers. M..: Helios ARV, 2005. - 160 pp.
6. Wenbo Mao, Modern cryptography: theory and practice. // Publishing house "Williams", Moscow, 2005, – 768pp.
7. A. G. Rostovtsev, E. B. Makhovenko Theoretical cryptography. // NPO Professional, St. Petersburg, 2016. – 478pp.
8. Sh.T. Ishmuhametov, R.G. Rubtsova Mathematical foundations of information security. Electronic textbook. // KFU, IVMiIT, Kazan, 2012 – 139pp.
9. B.A. Forousan Mathematics of cryptography and encryption theory. // INTUIT, Moscow, 2016. – 511pp.
10. A. O. Gel'fond Transcendental and Algebraic Numbers // State Publishing House of Technical and Theoretical Literature, Moscow, 1952–224 pp.
11. Yu. V. Nesterenko Theory of numbers// Publishing house "Academy", Moscow, 2008. – 272pp.

12. I.S. Gradstein, and I.M. Ryzhik Tables of integrals, sums, series and works (in Russian). Science, Moscow, 1971. -1108pp.
13. A.P. Prudnikov, Y.F. Brychkov, O.I. Marichev. Integrals and rows. Special features (in Russian). Science, Moscow, 1983. – 752pp.

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. Построение электронной подписи на основе трансцендентных чисел // «Информационные технологии и математическое моделирование в управлении сложными системами»: электрон. науч. журн. – 2020. – №1(6). – С. 37-43. DOI: 10.26731/2658-3704.2020.1(6).37-43 – Режим доступа: http://ismm-irgups.ru/toma/16-2020, свободный. – Загл. с экрана. – Яз. рус., англ. (дата обращения: 20.01.2020)

For citation

Shlaustas R.Yu., Kalinskaya E.E. Construction of the electronic signature on the basis of transcendental numbers // 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], 2020. No. 1(6). P. 37-43. DOI: 10.26731/2658-3704.2020.1(6).37-43 [Accessed 20/01/2020]