в праве для обеспечения суверенного интернет пространства. Ведь если мы зададимся вопросом о том является ли наш Интернет суверенным? Вероятно, последует ответ, нет. Поскольку на данный момент большинство российских компаний, среди которых Сбербанк, Госуслуги, Яндекс, используют сервисы американских Big Tech компаний (Google, Facebook, Amazon, Microsoft). И в том случае, если мы не имеем в настоящее время отечественных сервисов, готовых заменить зарубежные аналоги, то мы должны обеспечить безопасность персональных данных законодательным путем, защитив тем самым права и свободы граждан в данной области как от внутренних посягательств, так и внешних угроз.

Список литературы

1. Характеристика состояния преступности в Российской Федерации за январь — декабрь 2020 года [Электрон. ресурс]. — Режим доступа: https://мвд.рф/reports/item/22678184/.
2. **Жуков А.З.** Основные проблемы правового регулирования интернет-отношений в российской федерации / А.З. Жуков // Проблемы экономики и юридической практики. — 2018. — № 5.
3. **Анисимова А.С.** Правовое регулирование интернета: основные пробелы и направления деятельности государства / А.С. Анисимова // Юридический вестник ДГУ. — 2020. — Т. 33. — № 1.
4. **Пономарев Д.В.** Отдельные аспекты совершенствования законодательства в области противодействия незаконному использованию персональных данных пользователей социальных сетей / Д.В. Пономарев, Е.А. Гужов, В.А. Иноценко // Юристъ-Правовъдъ. — 2014. — № 6,2014(67).
5. **Слесарев Ю.В.** Проблемы правового регулирования размещения информации в социальных сетях / Ю.В. Слесарев, А.В. Лосяков // Балтийский гуманитарный журнал. — 2016. — Т. 5. № 2(15).
6. **Исаев А.С.** Правовые основы организации защиты персональных данных: учеб. пособие / А.С. Исаев, Е.А. Хлюпина. — СПБ., 2014.
7. Состояние преступности в России за январь декабрь 2020 года.

ОПРЕДЕЛЕНИЕ УСЛОВИЙ ПРИМЕНИМОСТИ АЛГОРИТМА ШИФРОВАНИЯ RSA ДЛЯ КЛЮЧЕЙ ШИФРОВАНИЯ ДЛИНОЙ МЕНЕЕ 256 БИТ

DETERMINATION OF THE CONDITIONS OF APPLICABILITY OF THE RSA ENCRYPTION ALGORITHM FOR ENCRYPTION KEYS WITH A LENGTH OF LESS THAN 256 BIT

Дадашов Ильяс Октаевич

Студент 2-го курса ИАТЭ НИЯУ МИФИ отделения Ядерной физики и технологий, направление подготовки — ядерная физика и технологии

Dadashov Il'jas Oktaevich

2nd year student of IATE NRNU MEPhI of the Department of Nuclear Physics and Technology, direction of training — nuclear physics and technology

Гужва Дмитрий Вадимович

Студент 2-го курса МГТУ им. Н.Э. Баумана факультета Специального машиностроения, направления подготовки — робототехнические системы и мехатроника

Guzhva Dmitrij Vadimovich

2nd year student of M.V. N.E. Bauman Faculty of Special Mechanical Engineering, areas of training — robotic systems and mechatronics

Аннотация: *В основе проекта лежит изучение проблемы работы алгоритма шифрования RSA с применением разработанной программой для шифрования информации. В рамках проекта была разработана методика получения открытых ключей шифрования в приложении Microsoft Excel.*

Ключевые слова: Алгоритм, безопасность, методика, ключи шифрования.

Abstract: *The project is based on the study of the problem of the RSA encryption algorithm using the developed program for encrypting information. Within the framework of the project, a method was developed for obtaining public encryption keys in Microsoft Excel.*

Keywords: Algorithm, security, technique, encryption keys.

Введение

На сегодняшний день для защиты цифровой информации применяются симметричные и асимметричные системы шифрования. Работа симметричные криптосистем основана на использовании определённого ключа, который может шифровать и дешифровать информацию (рис. 1). Наиболее распространённым алгоритмом симметричных криптосистем является алгоритм шифрования AES, который получил широкое распространение во многих программных продуктах, таких как активаторы

WinZip, WinRAR, 7zip; системы бэкапа (Backup4all, Handy Backup, Acronis True Image и т.п.).

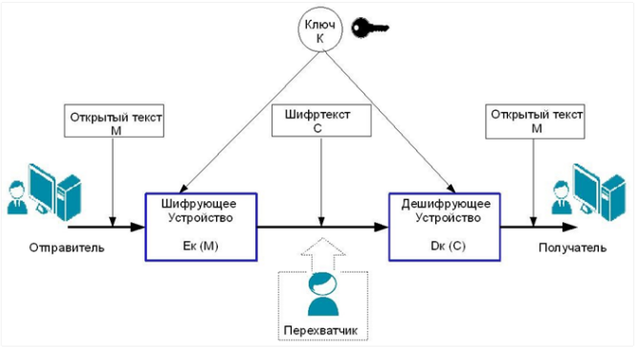

Рис. 1. Схема работы симметричных криптосистем

В ассиметричных криптосистемах шифрования используются два типа ключей: открытый — для шифрования информации, который может передаваться по незащищённому каналу связи и закрытый — для дешифрования информации (рис. 2).

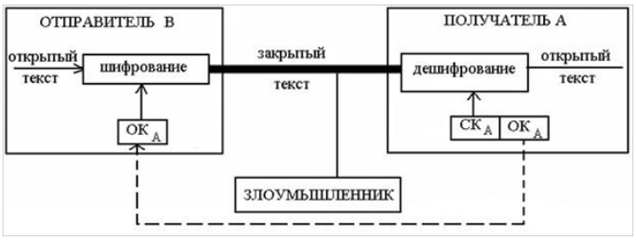

Рис. 2. Схема работы асимметричных криптосистем

Алгоритм RSA является самым распространённым алгоритмом шифрования с открытым ключом в мире и одним из самых копируемых программных продуктом в истории [5]. Он применяется для шифрования информации в операционных системах Windows, в программных продуктах компании Mozilla Firefox и т.д.

Работа алгоритма основана на действии факторизации. Для генерации ключа шифрования находят произведение двух чисел, следовательно, для того, чтобы взломать зашифрованное сообщение необходимо знать значения этих чисел, что можно сделать только путём факторизации. Однако при достаточно больших значениях чисел, даже самым мощным компьютером понадобиться несколько лет, для выполнения факторизации числа (рис. 3), что делает алгоритм шифрования RSA более криптостойким по сравнению с AES.

С развитием технологий появляется всё больше различных приложений, созданных рядовыми пользователями интернета. Как правило в таких приложениях либо применяют симметричные криптосистемы, что делает их не такими устойчивыми, как в случаях применения асимметричных криптосистем, либо вопросу безопасности информации вовсе не уделяется внимание.

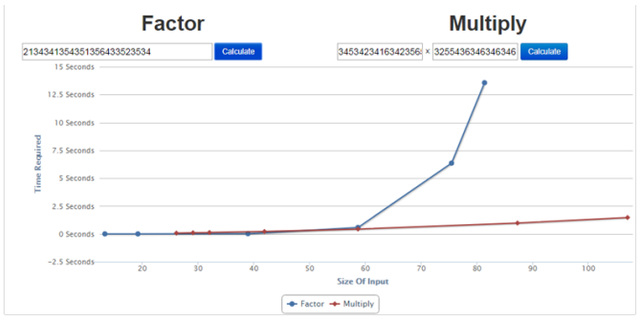

Рис. 3. График зависимости времени факторизации и умножения числе в зависимости от размера чисел

Основной проблемой применения асимметричных криптосистем в таких приложениях является сложность их структуры, а также использование длинных ключей шифрования, в результате чего, такие системы работают медленнее, чем симметричные. Для сравнения, длина ключей шифрования алгоритма RSA — 1024–2048 бит, а средняя скорость его работы — 1 Мбит/с, в то время, как у алгоритма AES длина ключа составляет 128–256 бит, средняя скорость работы — 150 Мбит/с.

Мы предполагаем, что можно увеличить скорость работы алгоритма шифрования RSA, сделав его применимым для рассматриваемых программных продуктов и тем самым увеличить защищённость информации в сравнении с использованием алгоритмов симметричных криптосистем таких как AES.

В таких приложениях нет необходимости использовать стандартную длину ключа 1024–2048 бит, так как, в большинстве случаев, они предназначены для локального пользования, что не требует настолько высокого уровня надёжности. Следовательно, можно использовать более короткие ключи шифрования, повышая скорость работы алгоритма. Конечно, можно увеличить и скорость работы алгоритмов симметричных криптосистем, уменьшив длину их ключа, но в таком случае они станут не криптостойкими.

Однако, при использовании коротких ключей, стандартных условий функционирования алгоритма RSA[6] — не достаточно, и алгоритм может работать некорректно, в результате чего возникаем необходимость в установлении дополнительных условий для корректной работы алгоритма при коротких ключах шифрования (ключи длинной менее 256 бит).

Определение дополнительных условий для применения коротких ключей шифрования

Исследование проводилось в собственных программах, написанных на языке программирования C++, которые выполняли шифрование и дешифрование числового сообщения (сообщение, которое со-

держит в себе число) по алгоритму шифрования RSA. В ходе исследования было зашифровано и расшифровано более 500 тысяч числовых сообщений, при различных значениях взаимно простых числе *p* и *p* [7], используемых для нахождения открытого ключа. Рассматривались такие числа *p* и *q* что *q* > *p*.

В результате нестабильной работы алгоритма при коротких ключах шифрования наблюдаются следующие ошибки:

1. Информация может быть неправильно зашифрована:

- Сообщение m шифруется само в себя (*c* = *m*), что не имеет смысла.
- Сообщение m шифруется в ноль (*c* = 0) что в дальнейшем приведёт к неправильному дешифрованию зашифрованного сообщения.

2. Информация может быть неправильно дешифрована:

- Зашифрованное сообщение с при расшифровки не принимает исходное значение шифруемого сообщения *m*, что может привести к потери информации.

В результате исследования определено и сформулировано дополнительное условие, которое позволяет корректно работать алгоритму RSA при использовании коротких ключей шифрования:

$$m \in [2; q-1] \quad (1)$$

$$m \neq a\,n, \quad (2)$$

$$m \neq a\,n + 1 \quad (3)$$

где m — шифруемое числовое сообщение;

n = *p q*;

a = 1, 2, 3, …

Условия 1–3 также применимы при *q* < *p*: *m* ∈ [2; *p*–1].

Таким образом, алгоритм шифрования RSA становится применим для ключей шифрования длинной менее 256 бит при одновременном соблюдении стандартных и дополнительных (1–3) условий, что позволяет увеличить скорость его работы.

Разработка алгоритмнов для нахождения всех доступных значений открытого ключа

Дальнейшее исследование проводилось программе для работы с электронными таблицами Microsoft Excel 2016 по методическому указанию «Основы кодирования и криптографии»[3] для разработки алгоритма, позволяющего получить все возможные значения открытой экспоненты *e* при фиксированных значениях чисел *p* и *q*. Что даёт возможность выбирать наиболее оптимальный вариант параметра надёжность — быстродействие для определённых задач (чем больше длина ключа, тем больше криптостойкость, чем меньше длина ключа, тем выше скорость работы алгоритма). Были проведены расчёты для более 250 тысяч различных значения закрытой экспоненты *d*. На основе полученных результатах были разработаны два алгоритма генерации открытой экспоненты *e*.

Алгоритм 1. Формула = ОСТАТ(F4*$F4;$C$2) протягивается на следующие значения графы «степень» стоящих после значения e. Формула может протягиваться на неограниченное количество ячеек (количество возможных ячеек определяются вычислительной мощностью ПК). После чего с определённой периодичностью обнаруживаются столбцы, которые в своих ячейках будут содержать такие значения зашифрованного сообщения, как и в столбце под значением *e*. Следовательно, значения числа в графе «степень» над такими столбцами будут значениями открытой экспоненты (рис. 4).

Алгоритм 1 применим, если при переводе числа n в двоичную систему счисления, оно будет содержать в себе не более одного нуля.

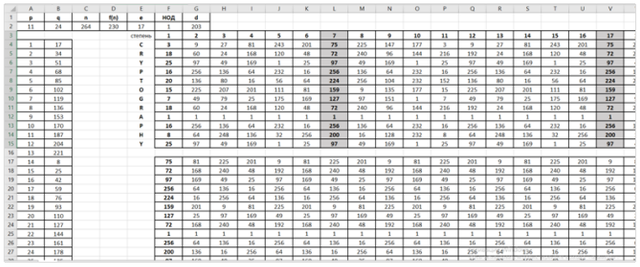

Рис. 4. Пример Алгоритма 1

Алгоритм 2. Самостоятельно подбираются первые четыре значения открытой экспоненты e (значения экспоненты e начинаются с малых чисел (односоставные числа), поэтому подобрать эти числа не составит проблемы, которая требовала бы отдельного решения). Затем все действия повторяются так же, как и в алгоритме 1. Но уже с определённой периодичности будут обнаруживаться парные колонки, которые содержать в себе значения зашифрованного текста (рис. 5). Алгоритм 2 применим, если при переводе числа n в двоичную систему счисления, оно будет содержать в себе более одного нуля.

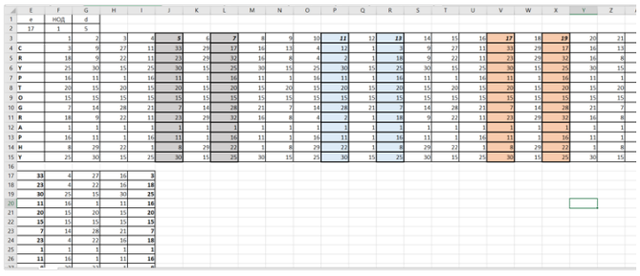

Рис. 5. Пример Алгоритма 2 — значения парных колонок *J* и *L* повторяются через 9 колонок в *V* и *X* (аналогично с парными колонками P и R)

Недостаток алгоритма 1 и алгоритма 2 заключается в том, необходимо выполнять всё «в ручную» путём построения таблиц с формулами.

Заключение

Нами было разработана методика применения алгоритма шифрования RSA с использованием ключей шифрования длиной менее 256 бит, что позволяет оптимизировать его для применения в программных продуктах, предназначенных для локального пользования.

Разработаны алгоритмы, вычисляющие все возможные значения открытой экспоненты e при фиксированных значениях взаимно простых чисел *p* и *q*. Таким образом, при разработке программных продуктов можно выбирать оптимальный размер открытого ключа под требуемые задачи, используя приведённые алгоритмы. Ведутся разработки по созданию программы, которая будет компенсировать текущие недостатки алгоритма 1 и алгоритма 2.

Ведётся разработка программы, которая будет выполнять шифрование информацию по алгоритму AES для того, чтобы можно было провести полный сравнительный анализ между алгоритмами AES в котором будут использоваться ключи шифрования стандартной длины и алгоритма RSA с применением коротких ключей шифрования. Завершение разработки планируется по 15.03.2021.

Ведётся разработка тестового приложения на смартфоны в котором будет применятся созданная программа, шифрующая информацию по алгоритму RSA с использованием коротких ключей. После чего будут проведены окончательные тесты по применению алгоритма шифрования RSA в таких приложениях.

Список литературы

1. Системы шифрования с открытыми ключами. Основы криптографии / А.П. Алферов, А.Ю. Зубков, А.С. Кузьмин [и др.]. — М.: Гелиос АРВ, 2002, — С. 310–322.
2. **Diffie W., Hellman M.E.** New Directions in Cryptography // IEEE Trans. Inf. Theory / F. Kschischang — IEEE, 1976. — Vol. 22, Iss. 6. — P. 644–654. — DOI:10.1109/TIT.1976.1055638
3. Основи кодування та криптографії / В.В. Швиров. — Луганськ: ДЗ «ЛНУ імені Тараса Шевченко», 2014. — С. 58–64.
4. **Дадашов И.О.** Исследование применимости алгоритма шифрования RSA для ключей шифрования различной длины / И.О. Дадашов // Будущее атомной энергетики — AtomFuture 2019. — Обнинск, 2019. — С. 143–145.
5. Алгоритм шифрования RSA[Электрон. ресурс]. — Режим доступа: http://www.e-nigma.ru/stat/rsa (Дата обращения-10.11.2019).
6. Описание алгоритма шифрования RSA [Электрон. ресурс]. — Режим доступа: http://teh-box.ru/informationsecurity/algoritm-shifrovaniya-rsa-na-palcax.html (Дата обращения: 11.12.2017).
7. Алгоритм шифрования RSA [Электрон. ресурс]. — Режим доступа: https://www.youtube.com/watch?v=vooHjWxmcIE&t=717s.

ВОПРОСЫ ОПРЕДЕЛЕНИЯ ПРАВОВОЙ ПРИРОДЫ БИТКОИНА

QUESTIONS OF DETERMINING THE LEGAL NATURE OF BITCOIN

Архипова Арина Сергеевна

Студентка (магистрант) Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)

Arhipova Arina Sergeevna

Student (undergraduate) of the Moscow State Law University named after O.E. Kutafina (Moscow State Law Academy)

Аннотация. *Предполагается, что для правового анализа любого явления, прежде всего, стоит разобраться с терминологией и природой появления этого явления, а также его свойствами и механизмами функционирования. В связи с этим, в первой части статьи будут предприняты попытки раскрыть основные понятия криптографической индустрии, причины возникновения и популярности такого явления, как Биткоин, его свойства и механизмы функционирования, а также способы его получения и использования. Во второй части статьи будет проведен правовой анализ Биткоина и возможностей его законодательного регулирования.*

Ключевые слова: цифровая валюта, криптовалюта, биткоин, блокчейн, майнинг, государственное регулирование, правовое регулирование.

Abstract. *It is assumed that for the legal analysis of any phenomenon, first of all, it is necessary to understand the terminology and the nature of the appearance of this phenomenon, as well as its properties and mechanisms of functioning. In this regard, the first part of the article will attempt to interpret reveal the basic concepts of the cryptographic industry, the reasons for the emergence and popularity of such a phenomenon as Bitcoin, its properties and mechanisms of functioning, as well as ways to obtain and use it. The second part of the article will attempt on legal analysis of Bitcoin and the possibilities of its legislative regulation.*

Keywords: digital currency, cryptocurrency, bitcoin, blockchain, mining, government regulation, legal regulation.