УДК 004.056.55

ИССЛЕДОВАНИЕ АЛГОРИТМОВ КРИПТОГРАФИИ В СИСТЕМАХ КОНТРОЛЯ ОКРУЖАЮЩЕЙ СРЕДЫ

Н.Л. Корепанова, М.А. Лебедева, Л.О. Павленко

ФГАОУ ВО «Севастопольский государственный университет»
РФ, г. Севастополь, ул. Университетская, 33
E-mail: *nat270702@gmail.com*

Представлены математические модели криптографии для защиты данных от несанкционированного доступа и исследование основных характеристик их эффективности.
Ключевые слова: информационная безопасность, криптография, криптоанализ, симметричные и ассиметричные криптосистемы, блочные шифры, потоковые шифры, шифры гаммирования.

Введение. Для наблюдения за параметрами среды, подверженной неблагоприятным техногенным и антропогенным воздействиям, их оценки и планирования природоохранных мероприятий используют системы экологического мониторинга. Различают глобальный (биосферный), региональный (геосистемный) и локальный (биоэкологический) мониторинг. Основу экологического мониторинга составляют автоматизированные информационные системы (АИС), которые предназначены для получения, хранения, обработки и оценки данных о состоянии атмосферы, недр, водных и наземных объектов [1]. АИС представляет собой совокупность информационно-поисковой системы, автоматизированной системы обработки данных, прогнозно-диагностической системы и системы управления. Данные АИС получает по специальным каналам связи от датчиков, выполняющих экспедиционные, наземные, морские наблюдения, наблюдения из космоса. Одним из принципов построения таких систем является принцип безопасности, который предполагает защищенный обмен данными между всеми элементами системы. Для обеспечения безопасности передаваемой и сохраняемой информации в состав АИС экологического мониторинга целесообразно включать систему защиты информации, в основе которой лежат криптографические алгоритмы преобразования информации.

Постановка задачи. В настоящее время криптография связана с решением проблем конфедециальности, неделимости, идентификации и ответственности. Так же современная криптография включает в себя разделы управления ключами, получение скрытой информации и квантовую криптографию.

Обеспечение конфиденциальности настроено на решение задачи защиты данных от изучения с их содержанием лиц, не имеющих права доступа к ним.

Под определением неделимости понимается обеспечение невозможности неразрешенной замены данных третьей стороной. Для нее необходим критерий нахождения любых действий над данными. К манипуляциям с данными относятся: вставка, удаление и замена. Решение этой задачи предполагает создание средств, направленных на сообщение лицу, не имеющему доступ к передаваемым данным, ошибочной информации. Для этого в шифруемую информацию вносится избыточность. Достигается она добавлением к сообщению проверочного набора, который вычисляется с помощью специального алгоритма и играет роль контрольной суммы для проверки целостности полученного сообщения [1].

Идентификация обеспечивает разработку методов подтверждения подлинности сторон и передаваемых данных в процессе информационного взаимодействия. Данные, передаваемые по каналу связи, должны быть опознаны по источнику, времени создания, пересылки, содержанию и т.д.

Под задачей избегания отказа от авторства подразумевается устранение

возможности отказа субъектов от некоторых из совершенных ими действий.

Квантовая криптография основывается на идее квантового распределения ключа лежащего в ее основе. При практическом применении для передачи сообщения происходит объединение квантового распределения ключа и симметричного шифрования [2].

Систематизация шифров по различным признакам В качестве начального признака, по которому производится систематизация шифров, используется тип преобразования, осуществляемого с открытым текстом при шифровании. Если фрагменты открытого текста заменяются некоторыми их равноценными фрагментами в шифрованном тексте, то соответствующий шифр относится к классу шифров замены. Если буквы открытого текста при шифровании только меняются местами друг с другом, то данный шифр относится к шифрам перестановки. С целью повышения надежности шифрования шифрованный текст, полученный применением некоторого шифра, может быть еще раз зашифрован с помощью другого шифра. Такие композиции различных шифров приводят к третьему классу шифров, которые обычно называют композиционными шифрами. В результате получаем первый уровень классификации шифров [3].

Если ключ шифрования и ключ дешифрования совпадают, то такие шифры называют симметричными, если же ключи не совпадают – асимметричными.

Симметричные криптосистемы подразделяют на поточные и блочные системы. Поточные системы реализуют шифрование отдельных символов открытого сообщения. Блочные же системы выполняют шифрование блоков фиксированной длины, составленных из подряд идущих символов сообщения.

Ассиметричные криптосистемы относятся к блочным шифрам. При их использовании можно легко организовать передачу конфиденциальных данных в сети с большим количеством пользователей.

Следующий уровень классификации шифров представляется одноалфавитными (поточные шифры простой замены), многоалфавитными и шифрами гаммирования. Наибольшее распространение получили поточные шифры простой замены. Это объясняется тем, что их шифрованные величины и шифрованные обозначения совпадают с алфавитом открытого текста. Ключом такого шифра является подстановка на множестве, верхняя строка которой представляет собой свойственную последовательность букв алфавита, а нижняя – систематически перемещаемую или случайную последовательность букв. Помимо явного задания (в виде двустрочной записи) ключ может быть задан некоторой формулой.

Любой многоалфавитный шифр представляет собой совокупность шифров простой замены, каждая из которых используется для шифрования очередной шифрованной величины в соответствии с вспомогательной последовательностью. Она определяется выбранным ключом и открытым текстом. Принципиально один многоалфавитный шифр отличается от другого лишь способом образования распределения. На практике используются в основном поточные многоалфавитные шифры, среди которых выделяются два больших подкласса – шифры, реализуемые дисковыми шифраторами и шифры гаммирования (гомоморфные шифры).

В основе шифров гаммирования лежит метод «наложения» ключевой последовательности – гаммы – на открытый текст. «Наложение» заключается в посимвольном (побуквенном) сложении или вычитании по тому или иному модулю. Хотя данные шифровой системы относятся к многоалфавитным системам замены, эти шифры имеют целый ряд особенностей. Благодаря простоте своей технической реализации и высоким криптографическим качествам, эти шифры получили широкое распространение и применение.

Шифры гаммирования. Сам термин «гаммирование» подразумевает под собой преобразование исходного текста, при котором символы исходного текста складываются с символами последовательности (гамма). В качестве гаммы может быть использован любой ряд случайных символов. Процедуру совмещения гаммы с исходным текстом можно

осуществить двумя способами. При первом способе символы исходного текста и гаммы заменяются цифровыми эквивалентами, которые затем складываются по модулю k, где k – число символов в алфавите. При втором методе символы исходного текста и гаммы представляются в виде двоичного кода, затем соответствующие разряды умножаются по модулю [3].

Гомоморфное шифрование широко используется в криптографии благодаря своим математическим методам защиты информации. Следует выделить такую задачу как вычисления над зашифрованными данными. Данные хранятся в зашифрованном виде. Для выполнения вычислений над ними данные можно расшифровать, произвести некоторые операции, а результат обратно зашифровать. Но для таких операций необходима защищенная аппаратура и меры по хранению секретных ключей. Вычисления над зашифрованными данными дают возможность избежать этих проблем.

Гомоморфное шифрование И НЕ включает в себя операции сравнения и реализует лишь некоторый набор операций. В случае, когда операндами являются биты, может быть реализован базис И, ИЛИ, НЕ, а для числовых операндов – операции сложения и умножения. Такую систему вычислений над зашифрованными данными можно было бы легко осуществить, если бы существовала функция шифрования, гомоморфная сразу относительно двух операций: И и ИЛИ для булевых операндов, сложение и умножение для числовых. Однако, вопрос о существовании таких функций гомоморфного шифрования, также как и вопрос о существовании системы вычислений над зашифрованными данными, остается нерешенным [4].

Областью применения гомоморфного шифрования являются удаленные системы хранения данных.

Главным понятием в гомоморфных системах с асимметричным ключом шифрования является понятие односторонней функции.

Под односторонней функцией понимается эффективно вычисляемая функция, для обращения к которой (т.е. для поиска хотя бы одного значения аргумента по заданному значению функции) не существует эффективных алгоритмов.

Так же присутствует функция-ловушка, так называется односторонняя функция, для которой обратную функцию вычислить довольно просто, если имеется некоторая дополнительная информация, и сложно, если такой информации нет.

Примером такой функции может служить алгоритм RSA, поддерживающий только одно свойство гомоморфности – операцию умножения. Вычислить произведение двух целых чисел очень просто, однако эффективных алгоритмов для выполнения обратной операции (разложения числа на целые сомножители) – не существует. Обратное преобразование возможно лишь, если известна, какая-то дополнительная информация.

Математическая модель алгоритма RSA. Алгоритм RSA является наиболее распространенной системой шифрования с открытым ключом и стандартом асимметричного шифрования, основанным на вычислительной сложности задачи факторизации больших целых чисел. На практике данный алгоритм, как и многие другие, не используют от начала и до конца самостоятельно. Алгоритм RSA часто используется вместе с алгоритмом секретного ключа типа DES для шифрования сообщения ключом RSA через цифровой конвертер. RSA может применяться для подтверждения идентификации другого человека. Это возможно благодаря тому, что каждый зарегистрированный пользователь криптосистемы имеет свой уникальный закрытый ключ, к которому ни у кого нет доступа. Именно это делает возможным уникальную идентификацию. Считается, что единственными способами расшифровать зашифрованные данным ключом RSA можно восстановлением исходной информации по ее криптограмме или вычислением закрытого ключа по ее открытому ключу.

Вся сложность нахождения секретного ключа в данном алгоритме основана на разложении модуля n на простые множители. Следовательно, надо выбирать большие целые числа p и q так, чтобы задача разложения была сложной в

вычислительном плане. Для этого необходимо соблюдать определенные требования [5]. Большие целые числа p и q должны не сильно отличаться друг от друга, но в то же время не должны быть слишком близкими друг к другу и быть достаточно большими. Так же желательно, чтобы наибольший общий делитель чисел p-1 и q-1 был небольшим. На данный момент самые большие простые числа, которые можно разложить на множители известными методами, содержат 140 десятичных знаков. Поэтому, большие целые числа в системе RSA должны содержать не менее 100 десятичных знаков [1].

Модуль n вычисляется путем перемножения больших целых чисел n=pq. Необходима осторожность в выборе модуля. Для обеспечения стойкости систем среднего срока действия, рекомендуют брать модули шифрования порядка 1024 битов. Для систем большого срока действия следует выбирать модули, состоящие из 2048 битов [6].

Одну из важных ролей в алгоритме RSA играет функция Эйлера $\phi(n)$, которая позволяет реализовать криптографическую систему с открытым ключом. Это функция натурального аргумента n и равна количеству целых чисел на отрезке от 1 до n, взаимно простых с n. Эту функцию достаточно легко вычислить, если знать разложение числа n на простые множители. Но именно это разложение и составляет наиболее трудоемкую часть вычислений [6]. Функция Эйлера вычисляется на этапе генерации пары открытого и секретного ключа. Вычисляется по следующей формуле

$$\phi(n) = (p-1)(q-1). \qquad (1)$$

Вторым компонентом открытого ключа является число e ($1<e<\phi(n)$), которое называется открытой экспонентой. Оно должно быть взаимно простое со значением функции Эйлера. В большинстве случаев в качестве открытой экспоненты берут простые числа, содержащие малое количество бит, например числа Ферма (3, 17 и 65537). Так же надо учитывать, что при выборе небольшого числа e или такого, что в его двоичной записи будет мало единиц, это может значительно ослабить безопасность алгоритма, зато увеличить скорость шифрования. В данных исследованиях используется показатель степени e = 65537. Значение этого числа достаточно велико для криптостойкости и в то же время мало по сравнению с разрядностью ключа. Так же нужно учитывать, что если на основе одной и той же открытой экспоненты небольшой величины шифруется несколько связанных между собой сообщений, то есть высокая вероятность удачного «взлома» этих сообщений.

Для генерации закрытого ключа необходимо вычислить число d, называемое закрытой экспонентой. Она мультипликативно обратная к закрытой экспоненте по модулю функции Эйлера

$$de = 1 \pmod{\phi(n)}. \qquad (2)$$

Обычно, закрытая экспонента вычисляется при помощи расширенного алгоритма Евклида, заключающегося в нахождении наибольшего общего делителя двух простых чисел.

Пара (n, e) является открытым ключом шифрования, а пара (n, d) представляет секретный ключ.

Для шифрования сообщения генерируется случайный сеансовый ключ m. Шифруем сеансовый ключ c при помощи открытого ключа

$$c = E(m) = m^e \bmod n. \qquad (3)$$

Если сеансовый ключ имеет длину от 0 до n-1, то он представляется в виде целого сообщения, если сеансовый ключ больше модуля n, то необходимо разбить шифруемый текст на блоки, каждый из которого является некоторым числом $b \epsilon Z_n$ [1]. Текст шифруется при помощи сеансового ключа симметричным алгоритмом

$$M_A = D_m C. \qquad (4)$$

Для дешифровки данных необходимо применить закрытый ключ (d, n) следующим образом

$$m = D(c) = c^d \bmod n. \qquad (5)$$

Расшифровывается сообщение при помощи сеансового ключа симметричным алгоритмом по следующей формуле

$$C = E_m (M_A). \qquad (6)$$

Шифрование не приводит к увеличению размера сообщения. Само сообщение и шифртекст остаются целыми числами в диапазоне от 0 до n-1.

Различают полностью гомоморфные и частично гомоморфные алгоритмы криптозащиты. Рассматриваемый алгоритм относится к частично гомоморфным алгоритмам. Такие алгоритмы позволяют одновременно рассматривать только одну операцию, или сложение или умножение. Алгоритм RSA является гомоморфной системой по операции умножения. Операцию сложения в данном алгоритме реализовать невозможно. Для операции умножения необходимо иметь модуль n и открытую экспоненту шифрования. Тогда функция шифрования имеет вид [7]

$$E(x) = x^e \bmod n. \quad (7)$$

Следовательно, гомоморфизм по умножению выглядит следующим образом

$$E(m1)\,E(m2) = m1^e\, m2^e \bmod n = (m1\, m2)^e \bmod n = E(m1\, m2). \quad (8)$$

Математическая модель алгоритма Пэйе. Изначально этот алгоритм относился к вероятностным криптосистемам с открытым ключом и основан на сложности задачи факторизации сложного числа, состоящего из произведения двух больших целых чисел. Кроме того было осуществлено улучшение данного алгоритма за счет нового предложенного метода увеличения эффективности и безопасности алгоритма, благодаря верифицируемым перестановкам [1].

Так же как и в алгоритме RSA для начала необходимо сгенерировать два больших целых числа p и q. Большие целые числа p и q должны не сильно отличаться друг от друга, но в то же время не должны быть слишком близкими друг к другу и быть достаточно большими. Так же желательно, чтобы наибольший общий делитель чисел p-1 и q-1 был небольшим.

Модуль n вычисляется путем перемножения больших целых чисел n=pq. Необходима осторожность в выборе модуля. Для обеспечения стойкости систем среднего срока действия, рекомендуется брать модули шифрования порядка 1024 битов. Для систем большого срока действия следует выбирать модули, состоящие из 2048 битов [6].

Первым компонентом закрытого ключа является λ. Она равна наименьшему общему кратному произведению чисел p-1 и q-1. Вычисляется по формуле

$$\lambda = \mathrm{lcm}(p-1)(q-1). \quad (9)$$

Выбранная λ считается корректной, если выполняется сравнение

$$u = 1 \bmod n. \quad (10)$$

Генерируется случайное целое число g, такое что $g \epsilon Z^*n2$ и вычисляется второй компонент закрытого ключа μ по формуле

$$\mu = (L(g^{\lambda} \bmod n^2))^{-1} \bmod n, \quad (11)$$

где L имеет значение

$$L = \frac{u-1}{n}. \quad (12)$$

Пара (n, g) является открытым ключом шифрования, а пара (λ, μ) представляет секретный ключ.

Для шифрования сообщения выбирается случайное значение r, $r \epsilon Z^*_n$. Зашифровываем сообщение по формуле

$$c = g^m r^n \bmod n^2. \quad (13)$$

Для дешифровки данных необходимо принимаем зашифрованный текст $c \epsilon Z^*_{n^2}$ и дешифруем сообщение следующим образом

$$m = L(c^{\lambda} \bmod n^2)\mu \bmod n. \quad (14)$$

Алгоритм Пэйе относится к алгоритмам вероятностного шифрования. Из всех известных алгоритмов с открытым ключом, он обладает наиболее интересными гомоморфными свойствами [4]:

– произведение двух криптограмм является суммой соответствующих открытых текстов, при дешифровании криптограммы $E(k,m1)E(k,m2) \bmod n^2$ будет получен открытый текст m1 + m2 mod n;

– ту же сумму можно получить, умножив криптограмму E(k,m1) на gm2, т.е. при дешифровании криптограммы $E(k,m1)\ g^m 2 \bmod n^2$ будет получен открытый текст m1 + m2 mod n;

– открытый текст, содержащийся в криптограмме, можно умножить на константу d, возведя эту криптограмму в

степень d, т. е. при дешифровании криптограммы $E(k,m)^d \bmod n^2$ будет получен открытый текст $dm \bmod n$. В частности, в качестве константы d можно задать другой открытый текст m и тем самым получить криптограмму произведения mm' mod n.

Математическая модель алгоритма Эль-Гамаля. Алгоритм Эль-Гамаля фактически является одним из вариантов метода выработки открытых ключей Диффи-Хеллмана. Данный алгоритм является алгоритмом с открытым ключом и его криптографическая стойкость основана на сложности проблемы вычисления дискретных логарифмов в конечном поле [1]. В настоящее время эта задача практически не реализуема для значений p, содержащих более 150 десятичных знаков. Так же желательно, чтобы число p-1 содержало большой простой делитель. Алгоритм может быть использован для шифрования, цифровой подписи и согласования общего ключа.

Данный алгоритм лежит в основе стандартов электронной цифровой подписи в США (DSA) и в России (ГОСТ Р 34.10-94).

К достоинствам алгоритма Эль-Гамаля можно отнести вероятностный характер шифрования, так как схемы вероятностного шифрования имеют большую стойкость в сравнении со схемами с детерминированным процессом шифрования. В системе Эль-Гамаля можно почти на порядок увеличить скорость шифрования и дешифрования сообщения, чем у алгоритма RSA с тем же по размеру открытым ключом из-за большей степени криптостойкости. К недостаткам данного алгоритма можно отнести удвоение длины шифрованного текста. Также алгоритм Эль-Гамаля в изначальном варианте беззащитен против атак с выбором шифротекста. Поэтому обычно применяют модифицированные алгоритмы шифрования. Но, не смотря на это, Эль-Гамаль сможет выстоять против атаки с выбором открытого текста, если считать, что задача Диффи-Хэллмана сложна для решения [6].

Для генерации открытого и секретного ключей осуществляются следующие операции, выбирается большое простое число p. Далее генерируется целое число g, которое является первообразным корнем от p. Затем выбирается целое число x такое которое должно быть больше единицы, но меньше p. Число y, является частью открытого ключа и вычисляется по следующей формуле [6]

$$y = g^x \bmod p. \qquad (15)$$

В открытый ключ записываются значения (p,g,y). Открытым ключом является x.

Из выше перечисленного следует, что в системе Эль-Гамаля для построения открытого ключа достаточно найти какое-нибудь случайное число и сделать сравнительно не сложные вычисления в арифметике остатков, когда в системе RSA каждый пользователь должен генерировать два больших простых числа для определения ключевой пары, что является довольно громоздкой задачей [7].

Сообщение в данном алгоритме является ненулевым элементом поля $m \epsilon F^*_p$. Для того чтобы зашифровать сообщение для начала выбирается сессионный ключ, который представляется случайным целым числом k. Оно должно быть взаимно простым с числом p-1. После выбора сессионного ключа вычисляются числа a и b, которые являются шифртекстом. Таким образом, получается, что зашифрованное сообщение в двоичном виде в два раза длиннее исходного сообщения.

$$a=G^K \bmod p, \qquad (16)$$

$$b=Y^K M \bmod p. \qquad (17)$$

Необходимо отметить, что при каждом шифровании применяется свой сессионный ключ. Поэтому, шифруя одно и то же сообщение два раза и больше, получаем разные шифротексты.

Чтобы расшифровать пару данных (a, b) производим следующие преобразования

$$M=b(a^x)^{-1} \bmod p = ba^{(p-1-x)} \bmod p. \qquad (18)$$

Алгоритм Эль-Гамаля является алгоритмом вероятностного шифрования. Его функция шифрования гомоморфна относительно операции умножения от-

крытых текстов. Криптограмма произведения может быть вычислена как попарное произведение криптограмм сомножителей. Если E (y,m1)=(y^{r1}m1,g^{r1}) и E(y,m2)=(y^{r2}m2, g^{r2}), то E(y,m1m2) можно получить в следующем виде

$$E(y,m1m2))=(y^{r1}y^{r2}m1m2,g^{r1}g^{r2}). \quad (19)$$

Результаты исследоваий алгоритмов криптографии. Для исследования алгоритмов криптографии была создана программная система на языке программирования Java. С помощью системы производилось двустороннее криптопреобразование над данными произвольной длины, обладающее механизмом преобразования паролей и ключей и системой транспортного кодирования по вышепредставленным алгоритмам.

Критерием эффективности явилось минимум времени на операции гомоморфных свойств (сложение и умножение), минимум времени на шифрование и дешифрование сообщений и надежность криптосистемы. В алгоритме RSA операция сложения не реализовывалась, т.к. данная функция является частично гомоморфной относительно операции умножения. Исходными данными являлся традиционный текстовый файл, а выходными данными дешифрованный текст и его характеристики с точки зрения системы криптозащиты. Ограничений на используемую среду передачи данных не накладывались.

Результаты эксперементальных исследований, в которых менялось количество символов в тестируемых сообщениях, сведены в табл. 1.

На рис. 1 представлены диаграммы «Шифрования» и диаграмма «Умножение» для тестового набора включающего 100 символов. Для операции сложения нет смысла строить диаграмму т.к. эту операцию выполняет только алгоритм Пэйе. Операция сложения представлена на рис. 2 в виде графика зависимости времени, потраченного на операцию сложения от количества символов в тексте.

На рис. 3 отображена графическая зависимость времени, за которое выполняется работа всего алгоритма от количества символов в текстовом файле. На рис. 4 отображена зависимость времени, за которое выполняется операция умножения от количества символов в текстовом файле.

Как видно из табличных данных и графиков, при небольшом объеме текста меньше всего времени на работу всего алгоритма занимает у алгоритма Эль-Гамаля, его преимущество перед алгоритмом RSA составляет 4,24%. При большем объеме текста (от 3000 символов) эта разница составляет 0,44%. При рассмотрении операции умножения наименьшее время показывает алгоритм RSA. При небольшом объеме текста, алгоритм RSA показывает результат на 39,54% лучше, чем алгоритм Эль-Гамаля. Рассматривая объемы текста более 2000 символов, этот процент сокращается до 2,75%. Алгоритм Пэйе показывает худшие результаты в обоих случая. Но его преимуществом является то, что он может реализовать оба гомоморфных свойства.

Заключение. Использование криптозащиты является необходимым условием обеспечения безопасности в системах экологического мониторинга. В связи с развитием вычислительной техники, появлением новых методов анализа криптографических алгоритмов важнейшей задачей является создание криптографических систем, обладающих высокой стойкостью к криптоанализу [8]. К таким алгоритмам относятся алгоритмы RSA, Пэйе и Эль-Гамаля. Проектирование АИС экологического мониторинга на базе этих алгоритмов позволит повысить эффективности защиты данных. В дальнейшем предполагается исследовать алгоритмы криптографии на основе нейронных сетей. Поскольку в таких системах секретной информацией являются как параметры нейронной сети, так и криптографический ключ, то по сравнению с традиционной криптографией пространство ключей возрастает, что приводит к увеличению криптостойкости системы.

Таблица 1. Результаты исследований

Количество символов	Алгоритм	Шифрование, мс	Гомоморфные свойства	
			Сложение, мс	Умножение, мс
50	RSA	531	-	15
	Пэйе	1061	390	421
	Эль-Гамаль	468	-	216
100	RSA	542	-	17
	Пэйе	1295	499	531
	Эль-Гамаль	486	-	227
250	RSA	643	-	24
	Пэйе	2090	905	920
	Эль-Гамаль	472	-	216
300	RSA	556	-	24
	Пэйе	2247	983	998
	Эль-Гамаль	455	-	206
400	RSA	610	-	26
	Пэйе	2714	1232	1217
	Эль-Гамаль	591	-	207
520	RSA	584	-	37
	Пэйе	3307	1513	1529
	Эль-Гамаль	452	-	205
670	RSA	717	-	29
	Пэйе	4776	2322	2166
	Эль-Гамаль	527	-	237
700	RSA	611	-	88
	Пэйе	4702	2196	2222
	Эль-Гамаль	473	-	213
1000	RSA	671	-	35
	Пэйе	6308	2830	3141
	Эль-Гамаль	521	-	226
1500	RSA	619	-	39
	Пэйе	9711	4794	4571
	Эль-Гамаль	472	-	211
2000	RSA	591	-	48
	Пэйе	11544	5453	5782
	Эль-Гамаль	463	-	204
2050	RSA	599		49
	Пэйе	12289	6130	5875
	Эль-гамаль	545	-	208
3000	RSA	585	-	68
	Пэйе	17640	8493	8866
	Эль-Гамаль	494	-	207
4500	RSA	656	-	121
	Пэйе	25766	12880	12589
	Эль-Гамаль	618	-	231
5000	RSA	661	-	135
	Пэйе	27563	13519	13741
	Эль-Гамаль	609	-	237

Рис. 1. Диаграмма времени работы алгоритма

Рис. 2. Время, потраченное на операцию сложения

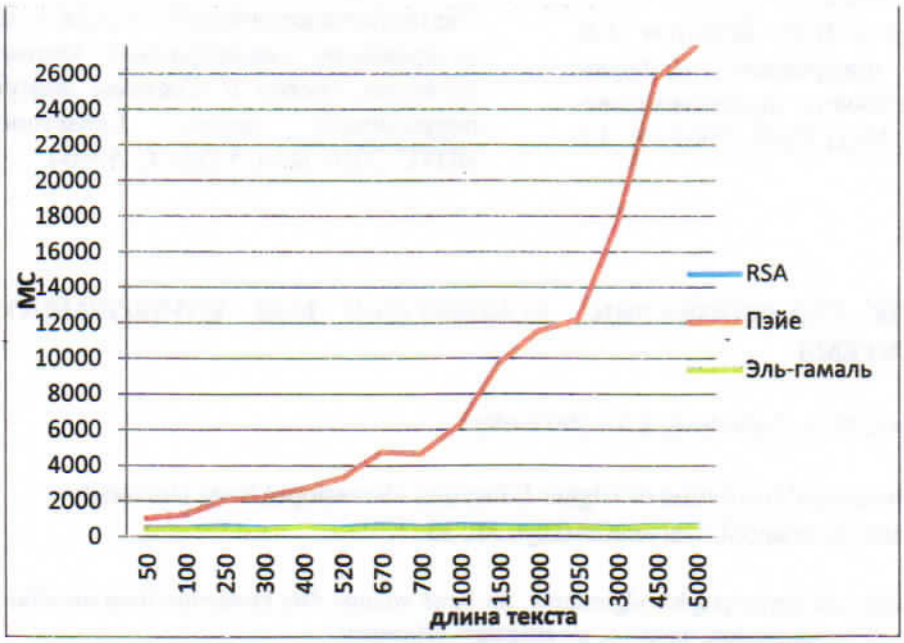

Рис. 3. Время, потраченное на работу всего алгоритма

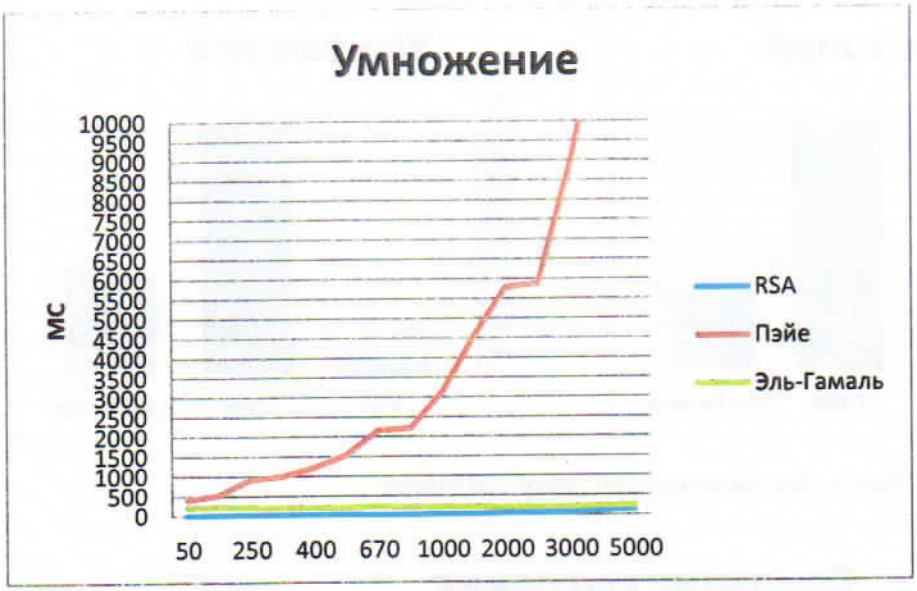

Рис. 4. Время, потраченное на операцию умножения

СПИСОК ЛИТЕРАТУРЫ

1. *Алферов А.П., Зубов А.Ю., Кузьмин А.С.* Основы криптографии. М.: Гелиос АРВ. 2002. 480 с.
2. *Килин С.Я.* Квантовая криптография: идеи и практика. Минск: Беларуская навука, 2007. 391 с.
3. Введение в криптографию / под общ. ред. В.В. Ященко. 4-е изд., доп. М.: МЦНМО, 2012. 348 с.
4. *Варновский Н.П., Шокуров А.В.* Гомоморфное шифрование // Труды Института системного программирования РАН. М.: ИСП РАН. 2007. Т. 12. С. 27–36.
5. *Rivest R. L., Shamir A., Adleman L.* A method for obtaining digital signatures and public key cryptosystems // Commun. ACM. 1978. V. 21, No 2. P. 120–126.
6. *Смарт Н.* Криптография. М.:Техносфера, 2005. 528 с.
7. *Молдованян Н.А., Молдованян А.А.* Введение в криптосистемы с открытым ключом: учебное пособие. СПб.: Лань. 2005. 285 с.
8. *Корепанова Н.Л., Лебедева М.А.* Системно-теоретический подход к проектированию симметричных крптографических систем // Системы контроля окружающей среды. Севастополь: ИПТС. 2016. Вып. 5 (25). С. 59–64.

ANALYSIS OF CRYPTOGRAPHIC ALGORITHMS FOR ENVIRONMENTAL CONTROL SYSTEMS

N.L. Korepanova, M.A. Lebedeva, L.O. Pavlenko

Federal State Educational Institution of Higher Education «Sevastopol State University»
Russian Federation, Sevastopol, Universitetskaya St., 33

Mathematical models and cryptographic algorithms for large volume data protection from unauthorized access, generation of pseudorandom numbers, investigation efficiency.

Keywords: information security, cryptography, cryptanalysis, symmetric cryptosystems, block ciphers, ciphers XOR.