МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

УДК 003.26; 512.5

НОВАЯ СЕМАНТИЧЕСКИ СТОЙКАЯ СИСТЕМА ШИФРОВАНИЯ С ОТКРЫТЫМ КЛЮЧОМ НА БАЗЕ RSA[1]

В. А. Романьков

Омский государственный университет им. Ф. М. Достоевского, г. Омск, Россия

Представлена семантически стойкая система шифрования с открытым ключом на базе системы шифрования RSA. Кроме семантической стойкости, описаны другие преимущества данной системы по отношению к базовой системе RSA, в том числе возможность более широкого выбора ключей и возможность выбора ключа шифрования пользователем. Показано, что в предлагаемой системе, в отличие от RSA, для дешифрования недостаточно знания разложения модуля на множители.

Ключевые слова: *семантическая стойкость, система шифрования с открытым ключом, RSA, платформа шифрования, ключи шифрования и расшифрования, мультипликативная группа кольца вычетов, подгруппа квадратичных вычетов.*

DOI 10.17223/20710410/29/3

A SEMANTICALLY SECURE PUBLIC-KEY CRYPTOSYSTEM BASED ON RSA

V. A. Romankov

Omsk State University, Omsk, Russia

E-mail: romankov48@mail.ru

We present a semantically secure public-key cryptosystem based on the RSA cryptosystem. We describe possible preferences of the proposed cryptosystem with respect to the basic RSA cryptosystem. These preferences include a semantic security property, as well as more various choice of an encryption key, and the possibility to select this key by an ordinary user. It is shown that the knowledge of the modulus factorization does not allow to break the cryptosystem as it happens in the basic RSA.

Keywords: *semantic security, public-key cryptosystem, RSA cryptosystem, encryption platform, encryption and decryption keys, the multiplicative group of a residue ring, the subgroup of quadratic residues.*

Введение

Система RSA, введённая в обращение Роном Ривестом, Ади Шамиром и Леном Адлеманом в 1977 г. [1], является наиболее популярной криптографической системой

[1]Работа выполнена при финансовой поддержке РФФИ, проект № 15.41.04312.

с открытым ключом. Она широко используется во всём мире как для шифрования, так и для цифровой подписи. В настоящее время RSA входит во все учебники по криптографии. Ей посвящено немало статей, она выдержала множество атак. Не раз объявлялось, что система исчерпала себя, но по-прежнему подобные утверждения остаются безосновательными. Относительно системы RSA и её криптографической стойкости см. [2 – 4].

В то же время может создаться впечатление, что система RSA существует в законченном раз и навсегда зафиксированном виде. В отличие от систем, использующих дискретные логарифмы, для неё не придумано эллиптических или алгебраических аналогов. Возникает вопрос: почему так происходит? Есть ли что-то такое в самой системе RSA, что не позволяет рассматривать различные её версии, не даёт возможности использовать платформы шифрования, отличные от колец вычетов по модулю, являющемуся произведением двух (больших) различных простых чисел? Думается, что это не так. В настоящей работе предложены достаточно простые и естественные способы разнообразить формы использования системы RSA и дан краткий анализ новых возможностей. Мы оставляем в стороне различные технические вопросы, связанные с правильным выбором параметров системы, тонкостями её имплементации и т. п. Основное внимание будет сосредоточено на вопросах общего характера.

В дальнейшем $\mathbb{Z}_n$ обозначает кольцо вычетов по модулю n, который в данной работе является произведением двух (больших) различных простых чисел p и q. Через $\mathbb{Z}_n^*$ обозначается мультипликативная группа кольца $\mathbb{Z}_n$. Через $\mathbb{Z}^{(2)}$ обозначаем множество всех чисел, представляющихся в виде произведения двух различных простых нечётных чисел. Таким образом, $n \in \mathbb{Z}^{(2)}$.

1. Классическая версия RSA

Установка системы RSA

Платформой для системы RSA служит кольцо вычетов $\mathbb{Z}_n$, где модуль n есть произведение двух различных достаточно больших простых чисел p и q. Числа p и q являются секретными, модуль n — открытым. Из соображений секретности числа p и q выбираются случайным образом. Считается, что p и q должны быть примерно одинаковой битовой длины.

После выбора p и q, однозначно определяющих модуль n и платформу $\mathbb{Z}_n$, вычисляется функция Эйлера $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1)$. Её значение сохраняется в секрете.

Напомним, что $\varphi(n)$ равно числу натуральных чисел, не больших n и взаимно простых с n. Записываемые этими числами вычеты, и только они, являются обратимыми по модулю n, то есть обратимыми в кольце $\mathbb{Z}_n$. Значит, $\varphi(n) = |\mathbb{Z}_n^*|$ является порядком группы $\mathbb{Z}_n^*$ обратимых вычетов кольца $\mathbb{Z}_n$.

Далее выбирается ключ зашифрования e — целое число в пределах $2 \leqslant e \leqslant \varphi(n)-1$, такое, что e и $\varphi(n)$ взаимно простые. В дальнейшем e используется как открытый ключ зашифрования (экспонента зашифрования).

Однозначно вычисляется число d, такое, что $ed = 1 \pmod{\varphi(n)}$. Вычет $d = e^{-1} \bmod \varphi(n)$ является обратным элементом к e в группе $\mathbb{Z}_{\varphi(n)}^*$.

Число d является секретным и используется в дальнейшем в качестве ключа расшифрования (экспоненты расшифрования). Оно эффективно вычисляется по e и $\varphi(n)$ расширенным алгоритмом Евклида.

Открытые данные: модуль n и ключ зашифрования e.

Секретные данные: параметры p и q, значение функции Эйлера $\varphi(n)$, ключ расшифрования d.

Алгоритмы зашифрования и расшифрования

Для передачи своего сообщения m, представленного как элемент кольца $\mathbb{Z}_n$, корреспондент Алиса должна знать открытый ключ (n, e) корреспондента Боба, которому предназначено данное сообщение. Сообщение m записывается своим стандартным значением, то есть $0 \leqslant m \leqslant n-1$. Зашифрованное сообщение c вычисляется по правилу

$$c = m^e \bmod n. \tag{1}$$

При этом для вычета c, передаваемого по открытой сети, используется его стандартное значение, то есть $0 \leqslant c \leqslant n-1$.

Чтобы расшифровать сообщение, Боб использует свой секретный ключ расшифрования d, выполняя следующее действие:

$$c^d = m^{ed} = m \pmod{n}. \tag{2}$$

Справедливость равенства (2) в случае обратимого вычета m следует из формулы Эйлера $m^{\varphi(n)} = 1 \pmod{n}$. Если m необратим, равенство (2) также имеет место (см., например, [5]).

Криптостойкость системы RSA основывается на трудности решения задачи о разложении на множители больших чисел вида $n = pq$. Эта задача решается уже сотни лет, но эффективный алгоритм разложения в общем случае так и не найден. Если потенциальный взломщик или нелигитимный пользователь сумеет найти числа p и q, он сможет вычислить ключ d и читать все сообщения, предназначенные в данной системе Бобу. Известно также (см., например, [6, с. 94–95]), что по ключу d можно, используя метод Монте-Карло, вычислить параметры p и q, что полностью разоблачает и делает непригодной к использованию установленную Бобом систему.

Из приведённых рассуждений, однако, не следует, что криптостойкость системы RSA равносильна трудноразрешимости проблемы разложения чисел вида $n = pq$ на множители. Известны атаки, в которых использованы другие соображения (см., например, [7]). Возможно, что существует ещё не найденный универсальный способ прочтения сообщения m без вычисления секретных параметров p, q и ключа расшифрования d. Но это только предположение.

2. Индивидуальные и универсальные ключи

Пусть порядок $|m|$ элемента m группы Z_n^* равен t. Это означает, что наименьшая степень, в которой элемент m равен 1 в группе $\mathbb{Z}_n^*$, равна t. Тогда зашифрованное сообщение $c = m^e \bmod n$ может быть расшифровано индивидуальным ключом d_t, определяемым равенством $ed_t = 1 \pmod{t}$. Ключ d_t может оказаться существенно меньше, чем универсальный ключ расшифрования d. Он подходит для расшифрования всех зашифрованных сообщений вида g^e, таких, что $g^t = 1$ в группе $\mathbb{Z}_n^*$ (или, что то же самое, $g^t = 1 \pmod{n}$). Действительно, из равенства $ed_t = 1 \pmod{t}$ следует, что $ed_t = 1 + tl$ для некоторого целого l. Тогда $(g^e)^{d_t} = g^{ed_t} = g^{1+tl} = g \pmod{n}$. В частности, вычисление универсального ключа d, с помощью которого расшифровывается любое зашифрованное сообщение, основано на том, что для любого $g \in \mathbb{Z}_n^*$ по формуле Эйлера $g^{\varphi(n)} = 1 \pmod{n}$.

Пусть $\tau(\mathbb{Z}_n^*)$ обозначает период группы $\mathbb{Z}_n^*$, то есть наименьшее натуральное число t, такое, что $g^t = 1$ для любого элемента g группы $\mathbb{Z}_n^*$. Условие $g^t = 1 \pmod{n}$

равносильно одновременному выполнению условий $g^t = 1 \pmod p$ и $g^t = 1 \pmod q$. Так как мультипликативные группы $\mathbb{Z}_p^*$ и $\mathbb{Z}_p^*$ полей $\mathbb{Z}_p$ и $\mathbb{Z}_q$ циклические порядков $p-1$ и $q-1$ соответственно, для любого элемента g группы $\mathbb{Z}_n^*$ выполнено равенство $g^t = 1$, где $t = [p-1, q-1]$ ($[a, b]$ означает «наименьшее общее кратное чисел a и b»). Заметим, что такое t заведомо меньше, чем $\varphi(n)$, так как при больших простых p и q числа $p-1$ и $q-1$ оба чётные. Число t позволяет определить универсальный ключ расшифрования d_t, не всегда совпадающий с d.

Можно утверждать, что $[p-1, q-1]$ совпадает с периодом $\tau(\mathbb{Z}_n^*)$. Докажем это. Пусть $p-1 = \prod\limits_{i=1}^{k} p_i^{l_i}$ и $q-1 = \prod\limits_{i=1}^{k} p_i^{m_i}$ — разложения в произведения примарных множителей. Тогда $[p-1, q-1] = \prod\limits_{i=1}^{k} p_i^{r_i}$, где $r_i = \max(l_i, m_i)$, $i = 1, \ldots, k$. Достаточно доказать, что в группе $\mathbb{Z}_n^*$ найдётся элемент порядка $t = \prod\limits_{i=1}^{k} p_i^{r_i}$. Пусть $t = t_1 t_2$, где $t_1 = \prod\limits_{i \in \{1,\ldots,k\}: r_i = l_i} p_i^{r_i}$, $t_2 = \prod\limits_{i \in \{1,\ldots,k\}: l_i \neq m_i, r_i = m_i} p_i^{r_i}$. Тогда t_1 делит $p-1$ и t_2 делит $q-1$. Заметим также, что $(t_1, t_2) = 1$.

Пусть f — порождающий элемент группы $\mathbb{Z}_p^*$, h — порождающий элемент группы $\mathbb{Z}_q^*$. Элемент $g_1 = f^{(p-1)/t_1}$ имеет порядок t_1, элемент $g_2 = h^{(q-1)/t_2}$ — порядок t_2. Так как эти порядки взаимно просты, элемент $g = g_1 g_2$ имеет порядок t. Отсюда получаем требуемое утверждение.

Итак, система допускает два способа вычисления ключа расшифрования по соотношениям $ed = 1 \pmod{\varphi(n)}$ и $ed_t = 1 \pmod{\tau(n)}$ соответственно, где $\tau(n) = [p-1, q-1]$. В некоторых случаях эти ключи совпадают, иногда отличаются достаточно сильно. Например, при $p = 19$, $q = 37$, $n = 703$, $\varphi(n) = 648$, $\tau(n) = 36$ для ключа шифрования $e = 5$ получаем $d = 574$, $d_t = 29$.

Приведённые рассуждения наталкивают на мысль построения подсистемы данной системы RSA, позволяющей использовать ключи зашифрования, которые не могут быть таковыми для всей системы. В частности, оказалось возможным использовать в качестве e чётные числа, более того — степени двойки. Более подробно об этом говорится далее.

3. Новая семантически стойкая система шифрования с открытым ключом на базе RSA

Перейдём к описанию основной системы шифрования, предлагаемой в данной работе.

Установка: платформа шифрования

Пусть $n = pq \in \mathbb{Z}^{(2)}$. В качестве платформы для системы шифрования выбираем кольцо вычетов $\mathbb{Z}_n$.

Пусть M — подгруппа мультипликативной группы $G_n = \mathbb{Z}_n^*$, $r = |M|$ — её период (или порядок). Можно также использовать любое число r, делящееся на период подгруппы M. Считаем, что множество всех возможных сообщений m совпадает с M. Таким образом, M выступает в роли пространства сообщений.

Выберем другую подгруппу $H \leqslant G_n$ периода (или порядка) t, взаимно простого с r. В качестве t также можно взять любое число, делящееся на период подгруппы H и взаимно простое с r.

Данные n, M, H открыты. Данные p, q, r, t секретны.

Установка: ключи

Ключ зашифрования e — любое натуральное число, взаимно простое с r. Ключ расшифрования $d = td_1$ вычисляется из равенства

$$(te)d_1 = 1 \pmod{r}.$$

Это можно сделать, так как te и r — взаимно простые числа. Ключ e открытый, d — секретный.

Алгоритм зашифрования

Для того чтобы передать по незащищённой сети сообщение $m \in M$, Алиса выбирает случайный элемент $h \in H$ и вычисляет элемент $hm \in G_n$. Передача имеет вид

$$A : c = (hm)^e \bmod n \to B.$$

Алгоритм расшифрования

Боб расшифровывает полученное сообщение следующим образом:

$$B : c^d = m \bmod n.$$

Объяснение правильности расшифрования

Так как $ed = 1 \pmod{r}$, найдётся целое число k, такое, что $ed = 1 + rk$. Тогда

$$c^d = (hm)^{ed} = (h^t)^{ed_1} m^{1+rk} = m \pmod{n}.$$

Выбор и задание составляющих системы

Кроме обычных рекомендаций, касающихся системы шифрования RSA, нужно определить подгруппы H и M. Предлагается задавать эти подгруппы своими порождающими элементами. Например, они могут быть циклическими подгруппами $H = \text{гр}(h)$ и $M = \text{гр}(g)$, для задания которых достаточно определить элементы h и g взаимно простых порядков t и r соответственно.

Одним из эффективных способов выбора циклических подгрупп заданного порядка является следующая процедура, неоднократно описанная в разных источниках (см., например, [5]). Генерируется простое число p. Для этого выбирается простое число p_1. Случайным образом выбирается чётное число s в интервале $p_1 \leqslant s \leqslant 4p_1 + 2$. Полагаем $p_2 = p_1 s + 1$. Далее случайным образом ищется число a в интервале $2 \leqslant a \leqslant p_2 - 1$, удовлетворяющее условиям

$$a^{p_2 - 1} = 1 \pmod{p_2}, \quad (a^s - 1, p_2) = 1.$$

Если это удалось сделать, то p_2 простое. Мы либо останавливаемся, полагая $p = p_2$, либо продолжаем процесс с p_2 вместо p_1. Известно, что при простом p_2 вероятность выбора подходящего a не меньше $1 - 1/p_1$. Если после достаточного числа проверок число a с нужными свойствами подобрать не удаётся, меняем s. Практика показала, что найти указанным способом простое число удаётся с вероятностью близкой к 1. Таким образом строятся сколь угодно большие простые числа.

Заметим, что в этом построении при достаточно большом p_1 можно выбирать s с любым заранее заданным делителем r. Если при этом получается простое p, то r делит $s = p - 1$. В мультипликативной группе $\mathbb{Z}_p^*$ есть элемент g_1 нужного порядка r. Найти его можно известными способами, в том числе практическими. Для получения

элемента g порядка r в группе G_n достаточно составить и решить по китайской теореме об остатках систему сравнений

$$\begin{cases} g = g_1 \pmod p, \\ g = 1 \pmod q, \end{cases}$$

где q — другой простой множитель модуля n.

Заметим, что построение простого числа p описанной процедурой можно осуществлять, получая в итоге не только простое число p, но и разложение на множители порядка $p-1$ мультипликативной группы поля $\mathbb{Z}_p^*$. Это даёт возможность строить подгруппы в $\mathbb{Z}_p^*$ заданных порядков.

Можно предложить и другой выбор простого числа, когда берутся числа вида $2s+1$ нужного размера и проверяются на простоту известными вероятностными алгоритмами. Здесь также можно контролировать разложение $p-1$ на множители. Заметим, что упомянутые два способа являются основными для построения простых параметров в криптографии.

Можно построить несколько элементов $g_1, \ldots, g_l$ соответствующих заданных порядков $r_1, \ldots, r_l$. Тогда порождённая ими подгруппа $\text{гр}(g_1, \ldots, g_l)$ имеет период r, делящий $[r_1, \ldots, r_l]$. Этого достаточно для задания подгруппы M. Аналогичным способом можно задавать и подгруппу H.

Свойства построенной системы шифрования

— Система является семантически стойкой. Это обеспечивается тем, что одно и то же сообщение $m \in M$ передается t различными случайно определяемыми способами. Поэтому, имея два сообщения m_1 и m_2, а также зашифрованное сообщение $(hm)^e \bmod n$, потенциальный взломщик не может определить, какое из двух сообщений зашифровано. Это одно из определений семантической стойкости.

— Ключом зашифрования e может быть любое число, взаимно простое с r. Если, например, r — простое число, то можно допустить выбор ключа e самим пользователем. Действительно, пользователь может выбирать из интервала с правой границей, заведомо меньшей r. Да и в общем случае при большом неизвестном простом r вероятность случайного выбора числа e, делящегося на r, пренебрежимо мала.

— Для компрометации предлагаемой системы шифрования недостаточно знания параметров p и q.

Объясним последнее из перечисленных свойств.

Заметим, что проблема определения порядка произвольного элемента группы $\mathbb{Z}_n^*$ влечёт решение проблемы RSA, то есть определение зашифрованного сообщения m по $c = m^e \bmod n$. Значит, эту проблему можно считать трудноразрешимой. Знание параметров p и q также не позволяет вычислять порядки элементов группы $\mathbb{Z}_n^*$ за полиномиальное время; это возможно только при знании разложений $p-1$ и $q-1$. Действительно, можно сделать так, что $p-1 = 2n'$, $n' = p'q'$, где p' и q' — большие различные простые числа. Если уметь вычислять порядки случайных элементов мультипликативной группы $\mathbb{Z}_n^*$, то можно получить разложение n'.

При знании p и q можно вычислить $hm \bmod n$ и попытаться определить множители h и m. Эту задачу также можно рассматривать как трудноразрешимую. Например, если взять в качестве M подгруппу квадратичных вычетов в группе $\mathbb{Z}_n^*$, проблема вхождения в которую традиционно рассматривается как трудноразрешимая, то при наличии способа определения множителей h и m можно определить по $hm \bmod n$

принадлежность этого элемента к подгруппе квадратичных вычетов. Это происходит только в случае, когда $h = 1 \pmod{n}$.

Если всё же потенциальному взломщику системы удастся определить параметр t, то для нахождения m ему придётся решать обычную проблему RSA. Заметим, что предлагаемая схема шифрования сводится к RSA при выборе в качестве H единичной подгруппы, а в качестве M — всей мультипликативной группы $\mathbb{Z}_n^*$.

4. Шифрование на подгруппе квадратичных вычетов

Представляется естественной следующая версия RSA, которую назовём *квадратичной подсистемой* RSA.

Установка квадратичной подсистемы RSA

При выборе параметров p и q на них накладывается дополнительное требование: они должны иметь вид $p = 4k + 3$ и $q = 4l + 3$. В качестве платформы шифрования выбирается подгруппа $Q_n \leqslant \mathbb{Z}_n^*$, состоящая из всех квадратичных вычетов группы $\mathbb{Z}_n^*$. Так как каждый элемент $g \in Q_n$ имеет в точности четыре различных корня второй степени, порядок подгруппы Q_n равен нечётному числу $t = \varphi(n)/4 = (2k + 1)(2l + 1)$. Более того, при таком выборе простых чисел возведение в квадрат определяет биективное отображение группы Q_n на себя. Следовательно, извлечение квадратных корней в группе Q_n однозначно. При знании параметров p и q процесс извлечения квадратных корней в группе $\mathbb{Z}_n^*$ и проверки их на принадлежность подгруппе Q_n может быть организован эффективно. Если указанные параметры неизвестны, извлечение корней равносильно разложению модуля на множители. Проверка принадлежности вычета группе Q_n в этом случае также представляется трудноразрешимой задачей.

В качестве ключа шифрования на группе Q_n выбирается любое натуральное число e, взаимно простое с её порядком t. Например, можно взять $e = 2^s$, где s — произвольное натуральное число. Ключ расшифрования d получается из соотношения $ed = 1 \pmod{t}$.

Алгоритмы шифрования и расшифрования

Шифрование осуществляется обычным способом. Зашифрованное сообщение c для $m \in Q_n$ вычисляется по формуле (1). В качестве ключа зашифрования e можно брать любое число, взаимно простое с порядком подгруппы Q_n. Если выбирается нечётный ключ e, то условие на параметры p и q (остаток 3 при делении на 4) можно не накладывать. В особом случае получается

$$c = m^{2^s} \bmod n.$$

Если $e = 2^s$, то расшифрование можно осуществить и другим способом, последовательно извлекая s квадратных корней, начиная с c, оставляя для дальнейших вычислений тот из корней, что принадлежит Q_n. Знание параметров p и q позволяет проводить такой процесс эффективно. В основном мы рассматриваем такую возможность как чисто теоретическую. Указанный способ шифрования можно сравнить с известной системой шифрования Рабина [8]. Основное отличие состоит в том, что платформой шифрования в предлагаемой системе служит не вся группа $\mathbb{Z}_n^*$, а только её подгруппа квадратичных вычетов Q_n. В системе Рабина используется возведение в квадрат, но для любого вычета $m \in \mathbb{Z}_n^*$. Расшифрование даёт четыре варианта для m, из которых только один является правильным. В предлагаемой системе можно использовать возведение в любую степень вида $2^s l$, где l взаимно просто с $\varphi(n)/4$, расшифрование однозначно. Для зашифровывания произвольного $m \in \mathbb{Z}_n^*$ можно использовать следующие соображения.

Замечание 1. Элементы подгруппы Q_n — полные квадраты. Если мы хотим передавать любые сообщения m в пределах от 0 до $n-1$, как это делается в RSA, можно использовать теорему Лагранжа о представлении любого натурального числа m в виде суммы четырёх квадратов $m_1^2 + m_2^2 + m_3^2 + m_4^2$. Известно, что нахождение такого представления для произвольного m эффективно. Остается передать слагаемые, по которым сообщение восстанавливается однозначно. Для упрощения можно даже передать любой квадрат $u^2 \leqslant m$ и открытым способом разницу $m - u^2$.

Использование квадратичной подсистемы RSA имеет ряд отличий, которые можно в определённом смысле считать преимуществами:

— возможность использования чётных ключей шифрования;
— возможность использования ключей шифрования вида 2^s, которые могут выбирать пользователи подсистемы RSA, а не только её владелец;
— ключи вида 2^s могут меняться от раунда к раунду. Это, например, позволяет передавать одинаковые сообщения в разных видах, что даёт возможность обеспечить семантическую секретность;
— расшифрование при использовании ключей вида 2^s можно осуществлять одной и той же программой вычисления квадратных корней в группе Q_n. Отличие только в s — числе шагов работы программы. Процесс расшифрования может быть организован без знания этого параметра;
— шифрование в квадратичной подсистеме можно включить как часть системы, описанной в предыдущем пункте: подгруппу Q_n можно выбрать в качестве фигурирующей там подгруппы M.

Последнее из приведённых свойств представляется наиболее важным для приложений.

5. Использование общего модуля n

В литературе неоднократно объяснялось, что знание ключа расшифрования d позволяет методом Монте-Карло эффективно раскрыть секретные параметры p и q и тем самым дискредитировать данную систему RSA (см., например, [6, с. 94–95]). Однако можно представить себе некоторую сеть, пользователи которой обладают системами RSA с общим модулем n. В сеть передаются шифрованные сообщения, общие для всех пользователей; например, пользователи — отделения одной и той же организации. Раскрывать секретные параметры легитимным пользователям нецелесообразно. В этом случае имеет смысл наделять пользователей разными парами (e, d) ключей шифрования и расшифрования. В противном случае, если будет достаточно много одинаковых ключей шифрования e, нелигитимный пользователь может прочитать зашифрованное сообщение, используя китайскую теорему об остатках. Этот способ также хорошо известен (см., например, [2, с. 51; 5, с. 105]).

При наделении пользователей различными ключами шифрования, в особенности при случайном их выборе, легко возникает ситуация, когда часть этих ключей, скажем $e_1, \ldots, e_l$, окажется в совокупности попарно взаимно простой. Тогда расширенный алгоритм Евклида позволяет эффективно вычислить целые числа $k_1, \ldots, k_l$, такие, что $\sum\limits_{i=1}^{l} e_i k_i = 1$, что позволяет по соответствующему набору зашифрованных вариантов $c_i = m^{e_i} \bmod n$, $i = 1, \ldots, l$, одного и того же сообщения m восстановить это сообщение:

$$\prod_{i=1}^{l} c_i^{k_i} = m^{\sum\limits_{i=1}^{l} e_i k_i} = m \pmod{n}.$$

Такое восстановление невозможно при использовании ключей вида 2^s в квадратичной подсистеме RSA.

ЛИТЕРАТУРА

1. *Rivest R., Shamir A., and Adleman L.* A method for obtaining digital signatures and public-key cryptosystems // Comm. ACM. 1978. V. 21(2). P. 120–126.
2. *Hinek M. J.* Cryptanalysis of RSA and its Variants. Boca Raton: Chapman & Hall/CRC, 2010.
3. *Song Y. Y.* Cryptanalytic Attacks on RSA. Springer, 2008.
4. *Stamp M. and Low R. M.* Applied Cryptanalysis. Breaking Ciphers in the Real World. Hoboken: John Wiley & Sons, 2007.
5. *Романьков В. А.* Введение в криптографию. М.: Форум, 2012. 239 с.
6. *Koblitz N.* A Course in Number Theory and Cryptography. N.Y.: Springer, 1994. 235 p.
7. *Maurer U. M.* Fast generation of prime numbers and secure public-key cryptographic parameters // Cryptology. 1995. V. 8. P. 123–155.
8. *Rabin M. O.* Digitalized Signatures and Public Key Functions as Intractable as Factorization. Technical Report. Cambridge: MIT, 1979.

REFERENCES

1. *Rivest R., Shamir A., and Adleman L.* A method for obtaining digital signatures and public-key cryptosystems. Comm. ACM, 1978, vol. 21(2), pp. 120–126.
2. *Hinek M. J.* Cryptanalysis of RSA and its Variants. Boca Raton, Chapman & Hall/CRC Publ., 2010.
3. *Song Y. Y.* Cryptanalytic Attacks on RSA. Springer, 2008.
4. *Stamp M. and Low R. M.* Applied Cryptanalysis. Breaking Ciphers in the Real World. Hoboken, John Wiley & Sons, 2007.
5. *Romankov V. A.* Vvedenie v kriptografiyu [Introduction to Cryptography]. Moscow, Forum Publ., 2012. 239 p. (in Russian)
6. *Koblitz N.* A Course in Number Theory and Cryptography. N.Y., Springer, 1994. 235 p.
7. *Maurer U. M.* Fast generation of prime numbers and secure public-key cryptographic parameters. Cryptology, 1995, vol. 8, pp. 123–155.
8. *Rabin M. O.* Digitalized Signatures and Public Key Functions as Intractable as Factorization. Technical Report. Cambridge, MIT, 1979.