УДК 003.26

Богуш В. В.; Мухачев В. А., к.т.н. *(Гос. унив-т информ.-коммуникационных технологий)*

АКТУАЛЬНОСТЬ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ ЖИВУЧЕСТИ АСИММЕТРИЧНЫХ КРИПТОСИСТЕМ

Богуш В. В., Мухачов В. А. Актуальність проблеми інформаційної живучості асиметричних криптосистем. Проведено аналіз спеціальних випадків ослаблення стійкості криптосистеми RSA. Показано можливість здійснення порушень захисту інформації, при реалізації яких доведення причетності порушників є ускладненим. Обґрунтовано висновок щодо можливості розповсюдження таких порушень та актуальності досліджень з метою розробки засобів протидії загрозі на системному рівні.

Ключові слова: АТАКА ВІНЕРА, АТАКА ФРАНКЛІНА, ЖИВУЧІСТЬ, КРИПТОСИСТЕМА RSA, СТІЙКІСТЬ, ТЕОРЕМА КОПЕРСМІТА, LLL-АЛГОРИТМ

Богуш В. В., Мухачев В. А. Актуальность проблемы информационной живучести асимметричных криптосистем. Проведен анализ специальных случаев ослабления стойкости криптосистемы RSA. Показана возможность осуществления нарушений защиты информации, при реализации которых доказательство причастности нарушителей затруднено. Обоснован вывод о возможности распространения таких нарушений и актуальности исследований с целью разработки средств противодействия угрозе на системном уровне.

Ключевые слова: АТАКА ВИНЕРА, АТАКА ФРАНКЛИНА, ЖИВУЧЕСТЬ, КРИПТОСИСТЕМА RSA, СТОЙКОСТЬ, ТЕОРЕМА КОППЕРСМИТА, LLL-АЛГОРИТМ

Bogush V. V., Mukhachov V. A. An urgency of information vitality problem of asymmetric cryptosystems. The analysis of special cases of the RSA cryptosystems security weakening was fulfilled. The possibility of breaches of information security, implementation of which makes the proof of the involvement of intruders difficult was shown. The conclusion about the possibility of the spread of such violations, and the urgency of research to develop a means of countering the threat on the system level were substantiated.

Keywords: WIENER ATTACK, FRANKLIN ATTACK, VITALITY, CRYPTOSYSTEM RSA, SECURITY, KOPPERSMIT'S THEOREM, LLL-ALGORITHM

Введение. Под живучестью инфокоммуникационных систем подразумевается свойство системы адаптироваться к новой ситуации и противостоять любым вредным воздействиям, выполняя свою целевую функцию за счет соответствующего изменения структуры и поведения системы, даже при серьезных повреждениях ее частей [3].

При оценке живучести распределенных компьютерных систем различают функциональную, структурную и информационную живучесть [4].

Под *функциональной живучестью* понимается способность системы при наличии неблагоприятных воздействий выполнять с предусмотренным качеством заданную цель функционирования. *Структурная живучесть* – способность системы поддерживать в неблагоприятных условиях системную структуру, необходимую для выполнения цели функционирования с заданным качеством.

Следуя [4], *информационная живучесть* – способность системы поддерживать доступность, целостность и конфиденциальность информации на уровне, который позволяет выполнять с заданным качеством цель функционирования системы, независимо от внешних и внутренних неблагоприятных воздействий либо нарушений при использовании информационных ресурсов.

Исходя из приведенных определений, а также необходимости рассматривать живучесть в аспекте противоборствующих систем [1], под информационной живучестью криптосистемы мы понимаем её свойство адаптироваться к новой ситуации для выполнения заданной цели функционирования, а также способность активно противодействовать нарушениям при использовании информационных ресурсов и вредным воздействиям со стороны другой системы либо внешней среды.

Мы намеренно не упоминаем о допустимом снижении качества выполнения цели и динамическом изменении структуры, поскольку контролируемое прекращение работы криптосистемы является реальным средством предотвращения утечки информации, однако,

скажем, в условиях катастрофы, секретность может быть принесена в жертву необходимости оповещения населения. Поэтому мы возлагаем принятие решения о допустимом снижении качества выполнения цели на более высокий уровень информационной системы и пока не обсуждаем возможность формулировки понятия информационной живучести криптосистем в более широком аспекте.

В настоящей статье рассматривается такие стороны проблемы информационной живучести асимметричной криптосистемы, как снижение ее стойкости на основе использования частных случаев дешифрования и возможность организации условий для затруднения доказательства причастности нарушителей к утечке информации.

Целью статьи является обоснование актуальности разработки подхода, обеспечивающего противодействие таким (внедренным) нарушителям, имеющих, скажем, доступ к формированию сообщений, выбору открытых ключей, длин секретных ключей, либо обладающего другими полномочиями, способствующими осуществлению следующей угрозы со стороны двух участников: нарушителя и исполнителя.

1. Нарушитель организовывает утечку информации за счет создания условий, позволяющих исполнителю после получения (перехвата) криптограммы с подсказкой, восстановить открытый текст нужного сообщения либо дешифровать криптосистему аналитическим путем.

2. Одновременно обеспечивается защита информации от третьих лиц.

3. При выявлении утечки информации доказательство причастности злоумышленников затруднено вследствие разделения их ролей и различного характера действий, а также использованием для защиты информации дополнительных секретных параметров.

Разделение ролей приводит к тому, что хотя нарушитель и создает условия для утечки информации, эта информация защищена, пока исполнитель не осуществит дешифрование криптограммы на основе дополнительных данных. В частности, правонарушение может неопределенное время оставаться незавершенным. Кроме того, подобные каналы утечки может организовать любой представитель группы из имеющих необходимые полномочия сотрудников, а возможностей для использования схем с подсказками потенциально достаточно много.

Основные криптоатаки. Хотя частные случаи снижения стойкости известны для всех типов асимметричных криптосистем, мы рассмотрим криптосистему RSA (аббревиатура от фамилий авторов системы – Rivers, Shamir, Adleman), для которой покажем, что соответствующие основные криптоатаки достаточно просты. Потенциально это может привести к неконтролируемому потоку их усовершенствований и модификаций.

Известным свойством криптосистемы RSA является зависимость ее стойкости от свойств сомножителей модуля. При необоснованном выборе этих сомножителей возможно частичное либо полное дешифрование криптосистемы за счет факторизации модуля.

Наиболее эффективным общим методом факторизации чисел, доступным в открытой литературе, является т. н. общий метод решета числового поля NFS (Number Field Siev), использующий свойства идеалов колец алгебраических чисел. В настоящее время эффективность метода находится на уровне факторизации RSA-модулей разрядности 1024 бита. Подобный подход используется также для решения задачи дискретного логарифмирования[2, гл. 3; гл. 5]. Однако NFS не приспособлен для использования дополнительной информации о значении части разрядов сомножителей RSA-модуля, взаимосвязи открытых текстов или длин ключей.

Далее мы рассмотрим возможность использования такой информации для снижения стойкости криптосистемы RSA со стандартными параметрами e, d, и n, где $n = pq$, p и q – большие простые числа, $p < q < 2p$, $ed = 1 \bmod \varphi(n)$, $\varphi = \varphi(n) = (p-1)(q-1)$, $e < \varphi$.

Случаи снижения стойкости системы RSA, без прямой факторизации модуля, сводятся к особенностям ключей и связям между открытыми текстами сообщений.

Атака Франклина [9]. При зашифровании сообщений с известной по модулю n разностью на стойкость криптосистемы может влиять величина открытого ключа.

Пусть $e=3$, m_1, m_2- линейно связанные открытые сообщения: $m_2 = m_1 + h \bmod n$, соответствующие шифртексты равны $a = m_1^e \bmod n$, $b = m_2^e \bmod n$ и значение $h \neq 0 \bmod n$ известно. Таким образом, два многочлена $g(x) = x^3 - a$ и $f(x) = (x+h)^3 - b$ имеют общий корень $x = m_1 \bmod n$. Отсюда следует, что m_1 является корнем наибольшего общего делителя (НОД) $D(x)$ указанных многочленов.

Можно показать, что в нашем случае условие взаимной однозначности шифра позволяет легко определить корень полинома $D(x)$ в случае, когда его кратность больше единицы.

С большой вероятностью выполняются также следующие условия обратимости по модулю n некоторых элементов, при которых $D(x) = ux + v$ и существует u^{-1} по модулю n: НОД$(h,n)=1$ и НОД$(2h^3 - a + b, n) = 1$. При этих условиях корень x_0 полинома $D(x)$ может быть выражен в виде

$$x_0 = m_1 = \frac{h(2a + b - h^3)}{2h^3 - a + b} \ .$$

Таким образом, достаточно прибавить к тексту известное значение h «вслепую», знание $m_1 + h \bmod n$ для восстановления сообщения не требуется.

Метод Франклина применим также при полиномиальных зависимостях между сообщениями, однако открытые показатели, все-таки, должны быть низкими.

Если нарушитель имеет возможность сформировать подобные сообщения, то для их передачи можно использовать следующий элементарный прием.

Пусть $k-$ секретное большое число, взаимно простое с e, а $m-$ открытый текст сообщения. Нарушитель вычисляет криптограммы $m^e \bmod n$, $m^k \bmod n$ и передает их исполнителю. Заранее зная k, исполнитель находит сначала x, y, при которых $xe - yk = \pm 1$, а затем определяет m: $m^{ex} m^{-ky} (\bmod n) = m^{\pm 1} (\bmod n)$.

Понятно, что этот прием можно развить за счет усложнения структуры данных и их взаимосвязей. Однако необходимо скрыть несанкционированную передачу информации.

Скрытые каналы. Систематическое изучение скрытых каналов передачи информации средствами криптографии начинается с 80-х годов XX века. Соответствующие протоколы существуют для различных типов асимметричных криптосистем.

Пример 1. Воспользуемся схемой цифровой подписи Онга-Шнорра-Шамира [5, гл.23.3].

Скрытая информация содержится в блоках r, s цифровой подписи практически произвольного сообщения M_1. Нарушитель может любым путем передать r, s и M_1 независимо друг от друга, т.к. в наших условиях полная схема цифровой подписи не нужна.

Пусть необходимо отправить скрытое сообщение M, с помощью маскирующего сообщения M_1. Выберем случайный секретный вычет $k \bmod n$, взаимно простой с n, известный нарушителю и исполнителю. Ограничения, состоящие в том, чтобы M и M_1 были взаимно просты с n, очевидно, легко выполнимы.

При наличии $r = 2^{-1}(M_1 M^{-1} + M) \bmod n$ и $s = k 2^{-1}(M_1 M^{-1} - M) \bmod n$, мы получим M, т.к. $r^2 - s^2 k^{-2} = (r + sk^{-1})(r - sk^{-1}) = (M_1 M^{-1}) M = M_1 \bmod n$, откуда $M = M_1 (r + sk^{-1})^{-1} \bmod n$.

Пример 2. Рандомизированные цифровые подписи типа Эль Гамаля.

Если нарушитель и исполнитель доверяют друг другу секретные ключи своих цифровых подписей, то уравнение цифровой подписи и подписанное сообщение позволяют вычислить рандомизатор, который и является скрытой информацией для соответствующего абонента.

Наконец, структуру каналов можно усложнить, например, используя симметричные криптосистемы.

Приведенные примеры показывают разнообразие параметров и сложность выявления структуры скрытых каналов связи.

Атака Винера [6]. Эта атака использует относительно короткую длину секретного ключа $d < (1/3)n^{1/4}$ и основана на диофантовом приближении вещественного числа α рациональной дробью с помощью разложения α в т.н. цепную дробь. Приближение состоит в построении числителя и знаменателя несократимой рациональной дроби x/y, такой, что $|\alpha - x/y| < 1/2y^2$. Точность приближения определяется значением y и числом α. В условиях нашей задачи α будет рациональной дробью: $\alpha = a/b$.

Числитель и знаменатель дроби x/y находятся среди пар (x_i, y_i), которые строятся, исходя из значений (a,b), по рекуррентным формулам. Дроби x_i/y_i называются подходящими к α.

Известно, что всякая несократимая рациональная дробь x/y, удовлетворяющая неравенству $|\alpha - x/y| < 1/2y^2$, есть подходящая дробь к числу α.

Рассматриваемая атака основана на том, что интересующие нас числа (x, y) образуют подходящую дробь к известному числу e/n. Остается только проверять некоторые простые условия, чтобы отобрать нужную подходящую дробь.

В соответствии с требованиями к параметрам RSA, $p < q < 2p$, откуда $p < \sqrt{n}$.

Поскольку $ed = 1 + k\varphi$ и $e < \varphi$, то $\frac{k}{d} < 1$ и НОД$(k,d) = 1$, следовательно, дробь k/d несократима. Кроме того, из условия $d < (1/3)n^{1/4}$ следует, что $k < (1/3)n^{1/4}$.

Очевидно, $\varphi = n + 1 - (p + q)$, то есть, $n - \varphi < 3p < 3\sqrt{n}$. К тому же, $\varphi < n$, следовательно,

$$\left|\frac{e}{n} - \frac{k}{d}\right| = \frac{|ed - kn|}{nd} = \frac{|1 + k(\varphi - n)|}{nd} < \frac{k(n - \varphi)}{nd} \le \frac{3k\sqrt{n}}{nd} = \frac{3k}{dn^{1/2}}.$$

Умножая числитель и знаменатель правой части неравенства на $n^{1/2}$ и учитывая, что $k < d < (1/3)n^{1/4}$, получим $\frac{3kn^{1/2}}{dn} < \frac{n^{1/4}n^{1/2}}{dn} = \frac{1}{dn^{1/4}}$. Поскольку и подавно $2d < n^{1/4}$, то

$$\left|\frac{e}{n} - \frac{k}{d}\right| < \frac{1}{dn^{1/4}} < \frac{1}{2d^2}.$$

Таким образом, k/d – одна из дробей, подходящая к e/n, откуда определяется вариант пары (k,d). Равенство $ed = 1 + k\varphi$, дает значение φ, затем определяем p и q.

Если факторизация не удалась, то вычисляем следующую подходящую дробь и т.д.

Данный подход расширен на значения $d < n^{\beta}$, где $\beta < 0{,}292$ [10], а также применим для более широкого диапазона значений ключа d, если часть его разрядов, скажем, старшая половина, известна.

В наших условиях атака Винера представляет угрозу факторизации любого RSA-модуля.

Действительно, если при построении криптосистемы нарушитель сможет, якобы непреднамеренно, задать для ключа $\tilde{d}$ короткую длину, получить ключ $\tilde{e}$, а затем, даже не ознакомившись с $\tilde{d}$, от ключей отказаться, то условия атаки Винера будут выполнены для

незадействованной пары ключей, но для действующего RSA-модуля, который при известном $\tilde{e}$ может быть факторизован.

Разработка подобных методов показала, что для дешифрования отдельных сообщений, как и для факторизации модуля, иногда достаточно частичной информации о параметрах криптосистемы, а это позволяет использовать приближенные решения уравнений, которым такие параметры удовлетворяют.

Редукция базиса решетки и LLL-алгоритм. Факторизация RSA при наличии неполной информации об одном из сомножителей модуля и использует алгоритм редукции базиса решетки [13], за которым, по первым буквам фамилий авторов, закрепилось название LLL-алгоритм. Этот алгоритм был предложен авторами для факторизации полиномов с рациональными коэффициентами и успешно применен для решения ряда задач криптоанализа и теории чисел.

В частности, применение LLL-алгоритма для поиска корней полиномиальных сравнений по нефакторизованному модулю позволило разработать ряд атак, снижающих стойкость криптосистемы RSA[11].

Хотя доказательство корректности LLL-алгоритма является громоздким, его структурная схема достаточно проста. Мы приведем лишь сведения, необходимые для обоснования многообразия возможностей и доступности принципов его применения.

Подмножество L_m вещественного n-мерного пространства R^n называется целочисленной решеткой, а число m - ее рангом, если $L_m = \left\{ \sum_{i=1}^{m} r_i b_i ; r_i \in Z \right\}$, где $b_1, \ldots, b_m$ – линейно независимы. Система векторов $b_1, \ldots, b_m$ называется базисом решетки,.

Решетка ранга n называется полной решеткой. Ей соответствует базис $b_1, \ldots, b_n \in R^n$.

Если матрица U состоит из базисных векторов, $U = (b_1, \ldots, b_m)$, то детерминантом Грама системы векторов $b_1, \ldots, b_m$ называется величина $\Gamma(b_1, \ldots, b_m) = \det(U^T U)$.

Детерминант Грама системы $b_1, \ldots, b_m$ линейно зависимых векторов равен нулю. Если $b_1, \ldots, b_m$ – линейно независимы, то $\Gamma(b_1, \ldots, b_m) > 0$.

Детерминантом $d(L_m)$ решетки L_m называется значение $\sqrt{\Gamma(b_1, \ldots, b_m)}$. Детерминант не зависит от выбора базиса решетки. Если величина $d(L_m)$ сравнительно невелика, то возможны упомянутые выше криптоаналитические атаки. Для наших целей достаточно рассмотреть решетку L полного ранга.

В LLL-алгоритме используются только рациональные преобразования.

На предварительном этапе алгоритма исходный базис решетки $B = \{b_1, \ldots, b_n\}$ преобразуется в ортогональный базис B_1 с помощью процесса ортогонализации Грама-Шмидта и составляется таблица T некоторых промежуточных результатов.

В результате повторных проходов LLL-алгоритма эта таблица модифицируется, а базис B_1 трансформируется в упорядоченный базис решетки $B^* = \{b_1^*, \ldots, b_n^*\}$, длины некоторых линейных комбинаций векторов которого и элементы таблицы T удовлетворяют специальным требованиям.

Эти требования и определяют понятие редуцированности базиса B^*. При этом, конечно, базис B^* и исходный базис порождают одну и ту же решетку.

Если упомянутые требования выполняются для соответствующего базиса B_1 изначально, то базис $B = \{b_1, \ldots, b_n\}$ называется LLL-редуцированным. Такой базис обладает рядом свойств, выраженных в виде неравенств относительно эвклидовых норм входящих в него векторов.

Алгоритм редукции применим для рационального и целочисленного базисов, а также в том случае, когда лишь все скалярные произведения (b_i, b_j) рациональны.

Далее мы воспользуемся тем, что первый вектор редуцированного базиса b_1 обладает наименьшей длиной среди векторов базиса, а также оценкой $\|b_1\| \le 2^{(n-1)/4} d(L)^{1/n}$.

LLL-алгоритм дает некоторое приближение к решению задачи нахождения базиса решетки, состоящего из её коротких векторов.

Вообще говоря, применение LLL-алгоритма широко и многогранно. В отличие от специализации большинства алгоритмов, типичной для криптоанализа, LLL-алгоритм реализует идею сведения исходной задачи к поиску формулировки другой задачи, одним из решений которой является искомый параметр.

Искусство аналитика заключается в том, чтобы новая задача была легко разрешима в некотором диапазоне значений параметра, причем оценки диапазона были бы эффективными.

Покажем, как использовать LLL-алгоритм для полного дешифрования криптосистемы RSA, если исполнителю известна половина старших битов одного из сомножителей $n = pq$.

LLL-атака. Пусть $f(x)$ полином вида $f(x) = a_0 + a_1 x + \ldots + a_{t-1} x^{t-1} + x^t$.

Назовем вектором коэффициентов полинома в точке X вектор-строку вида $v(f(x), X) = (a_0, a_1 X, \ldots, a_{t-1} X^{t-1}, X^t)$.

Очевидно, $v(f(x), X) = v(f(xX), 1)$. Там, где позволяет контекст, в качестве $v(f(x), X)$ мы будем пользоваться обозначениями $v(f(xX))$, $v(f)$, или просто v. Аналогично используем обозначение эвклидовой нормы $\|v(f(xX))\|$ вектора $v(f(xX))$.

Лемма *(Howgrave-Graham).* Пусть $h(x)$, $\deg h(x) \ge 1-$ полином с целочисленными коэффициентами, количество ненулевых коэффициентов которого равно w.

Пусть x_1, X и $N > 2$ целые числа, удовлетворяющие условиям $|x_1| < X$, $h(x_1) \equiv 0 (\mathrm{mod}\, N)$ и $\|h(xX)\| < \frac{N}{\sqrt{w}}$. Тогда $x_1 -$ корень полинома $h(x)$ над полем рациональных чисел.

Доказательство. Пусть вектор $\bar{b} = v^+(h)$ получается заменой всех координат вектора $v(h)$ на их абсолютные величины, а $\bar{c} -$ вектор, все координаты которого получаются заменой ненулевых координат вектора $v(h)$ на единицы.

Из неравенства Шварца $|(\bar{a}, \bar{b})| \le \|\bar{a}\| \cdot \|\bar{b}\|$ следует $(\bar{c}, \bar{b}) \le \sqrt{w} \cdot \|\bar{b}\|$, откуда

$$|h(x_1)| = \left|\sum_i a_i x_1^i\right| \le \sum_i |a_i X^i| = (\bar{c}, v^+(h(xX))) \le \sqrt{w}\|h(xX)\| < \sqrt{w}\frac{N}{\sqrt{w}} = N .$$

Поскольку $h(x_1) \equiv 0 (\mathrm{mod}\, N)$ и $-N < h(x_1) < N$ то $h(x_1)$ принадлежит системе абсолютно наименьших вычетов, в которой существует только одно число сравнимое с нулём – рациональный нуль, поэтому $x_1 -$ рациональный корень $h(x)$.

Теперь мы сможем решить сравнение вида $f(x_1) \equiv 0 (\mathrm{mod}\, N)$, если среди линейных комбинаций полиномов вида $G(x, N) = x^k f(x) + N^l s(x)$ найдем полином $h(x)$, у которого имеется тот же рациональный корень равный x_1, а коэффициенты по абсолютной величине достаточно малы, чтобы использовать предыдущую лемму.

Линейным комбинациям полиномов $G_i(x, N)$ соответствуют линейные комбинации векторов $v(G(xX, N))$. Если среди этих векторов выбрать линейно независимые, например, за счет степеней полиномов, то они образуют базис решетки и не исключено, что $b_1 -$ вектор

наименьшей длины редуцированного базиса решетки – подойдет в качестве вектора коэффициентов $v(h(xX))$. Это можно узнать из приведенной выше оценки для $\|b_1\|$.

Обычно векторы $v(G)$ выбирают так, чтобы $d(L)$ можно было легко вычислить теоретически.

Идею применения LLL-алгоритма покажем, следуя [8; 12; 14].

Рассмотрим RSA модуль $N = pq$, где p – число размером $2k$ битов, $p < q < 2p$ и пусть старшие k битов p образуют число p_1, которое известно. Пусть $p = p_1 + x_1$, где оценка младших разрядов $0 < x_1 < X$ дана. Понятно, что $X < 2^k$ и $p_1 \geq 2^{2k-1}$.

Вычислим число $q_1 = \left\lfloor \frac{N}{p_1 + X} \right\rfloor = \frac{N}{p_1 + X} - \varepsilon$, где $0 < \varepsilon < 1$.

Очевидно, $q_1 < q < \frac{N}{p_1}$ и $q < q_1 + \left(\frac{N}{p_1} - q_1 \right) < q_1 + \frac{N}{p_1} - \frac{N}{p_1 + X} + \varepsilon = q_1 + \frac{NX}{p_1(p_1 + X)} + \varepsilon$.

Откуда $q < q_1 + \frac{N}{(p_1 + X)} \frac{2^k}{p_1} + \varepsilon < q_1 + (q_1 + \varepsilon) \frac{2^k}{2^{2k-1}} + \varepsilon$ и $q_1 < q < q_1 + \frac{q_1}{2^{k-1}} + \varepsilon \left(1 + \frac{1}{2^{k-1}} \right)$.

Следовательно, примерно $k-2$ старших разрядов q_1 совпадают со старшими разрядами числа q. Поэтому даже $k+1$ старших разрядов q можно считать известными за счет небольшого числа повторений алгоритма, а рассуждение можно применить и для нечетного размера p.

Рассмотрим полином $f(x) = x + p_1$. Очевидно, $f(x_1) \equiv 0 (\mathrm{mod}\, p)$, при $x_1 = p - p_1 \approx \sqrt{p}$, но для определения корня лемма не подходит, т.к. p неизвестно и непосредственно манипулировать коэффициентами векторов, содержащими множители вида p^t невозможно. Поэтому воспользуемся степенями N, чтобы получить другое полиномиальное сравнение по модулю p^t с малым корнем.

Выберем полиномы $N^t, N^{t-1} f(x), N^{t-2} f^2(x), \ldots, N^2 f^{t-2}(x), N f^{t-1}(x)$, количество которых равно t, а также полиномы $f(x)^t, x f(x)^t, x^2 f^t(x), \ldots, , x^{k-t} f(x)^t$.

Общее количество выбранных полиномов равно $k+1$ и для каждого такого полинома число x_1 является корнем по модулю p^t (но для не всех – по модулю N).

Рассмотрим теперь вектор-строку $\tilde{v}$, содержащую $k+1$ нулей, элементы которой пронумерованы слева направо с нуля, а нумерация сопоставлена со степенями $x^0 = 1, x^1, x^2, \ldots, x^k$ переменной x. Пусть $G(x, N)$ – очередной по порядку полином, из выбранных ранее, а $v(G) = v(G(xX, N))$ – соответствующий ему вектор коэффициентов в точке X.

Запишем каждый элемент $a_i(X, N)$ вектора $v(G)$ на место координаты вектора $\tilde{v}$, номер которой соответствует степени переменной в терме $a_i(X, N) x^i$ многочлена $G(xX, N)$.

Запишем вектор-строку $\tilde{v}$ в качестве очередной строки матрицы $\tilde{B}$. В итоге, получим невырожденную нижнюю треугольную $(k+1) \times (k+1)$ матрицу вида:

$$\tilde{B} = \begin{pmatrix} N^t & 0 & 0 & 0 & 0 \\ N^{t-1} p_1 & N^{t-1} X & 0 & \cdots & 0 \\ * & * & \ddots & \ddots & \ddots \\ \vdots & \vdots & \ddots & X^{k-1} & 0 \\ * & * & * & * & X^k \end{pmatrix}, \quad \det \tilde{B} = \prod_{i=1}^{t} N^i \prod_{i=1}^{k} X^i = N^{\frac{t(t+1)}{2}} X^{\frac{k(k+1)}{2}}.$$

Теперь, рассматривая строки $\widetilde{B}$ как базисные вектора целочисленной решетки L, с помощью LLL-алгоритма получаем редуцированный базис $B = b_1, \ldots, b_{k+1}$, с детерминантом $d(L) = \det \widetilde{B}$ и вектором b_1, длина которого удовлетворяет оценке $\|b_1\| \le 2^{k/4} d(L)^{1/(k+1)}$.

По построению, компоненты вектора b_1 имеют вид $a_i X^i$ и ему можно поставить в соответствие полином $h(x)$, для которого $v(h(x), X) = b_1$.

Поскольку $\sqrt{N/2} < p$, для применения леммы достаточно выполнения более слабого неравенства $\|b_1\| \le 2^{k/4} d(L)^{1/(k+1)} < \frac{p^t}{\sqrt{k+1}} < (N/2)^t (k+1)^{-1/2}$.

Если оно выполняется, то находим x_1 и, следовательно, p.

В общем случае можно использовать целочисленный полином $f(x)$ степени $d > 1$ со старшим коэффициентом равным единице, такой, что $f(x_1) = 0 \bmod N$, для чего применяется следующая теорема.

Теорема (Coppersmith). Пусть $0 < \varepsilon < \min(0.18, 1/d)$, $f(x_1) = 0 \bmod N$ и $|x_1| < \frac{1}{2} N^{\frac{1}{d} - \varepsilon}$.

Тогда x_1 можно определить за полиномиальное по $1/\varepsilon, d$ и $\log(N)$ время.

Доказательство теоремы конструктивно и использует решетку, построенную исходя из полиномов $G_{i,j}(x) = N^{h-1-j} f(x)^j x^i$, где $0 \le i \le d-1$, $0 \le j \le h-1$.

Здесь $|x_1| < X = \frac{1}{2} N^{\frac{1}{d} - \varepsilon}$, $h > 1$, $h \approx \frac{1}{\varepsilon d}$ – ближайшее целое к $\frac{1}{\varepsilon d}$.

Заключение. Существует направление исследований, в рамках которого предлагаются и совершенствуются разнообразные атаки, применимые для ослабления асимметричных криптосистем. Соответствующая тематика для криптосистемы RSA достаточно полно представлена в [11; 14].

Рассмотренная в статье ситуация существенно отличается от модели т.н. оспариваемого шифрования (Deniable encryption) [7], в которой состав преступления подтверждается, исходя из содержания переписки законного пользователя (например, террористическая угроза). В случае оспариваемой криптографии нарушитель выбирает криптосистему и способ построения двух ключей для расшифровки одного шифртекста в два разных смысловых сообщения. При вынужденном предъявлении ключа властям нарушитель предъявляет ключ, соответствующий сообщению, в котором нет компрометирующих данных.

Мы не рассматриваем данное направление, поскольку возможность существования подобных уникальных ключей, является неотъемлемым свойством криптосистемы и характеризует ее с точки зрения надежности, но не живучести.

Выводы. 1. Необходимость изучения организации криптосистем в аспекте живучести следует из масштабности и сложности проблемы живучести инфокоммуникационных систем в целом.

2. Наличие частных случаев ослабления и дешифрования действующих асимметричных криптосистем потенциально являются предпосылками к утечке информации и нарушению схем цифровой подписи.

3. Доступность реализации и возможность модификации соответствующих криптоатак указывает на необходимость упреждающих действий с точки зрения защиты информации, что подтверждает актуальность проблемы информационной живучести криптосистем.

4. Рассмотренные криптоаналитические атаки осуществляются с использованием человеческого фактора, поэтому активное противодействие должно организовываться при

участии человека и основываться на упреждающем изменении тактики адаптации, информационное обеспечение которой носит форму благоприятного внешнего воздействия.

С целью реализации такого подхода, в качестве отправного пункта для исследований можно использовать опыт построения инфраструктуры открытых ключей на основе цифровых сертификатов и систем антивирусной защиты удаленных пользователей.

Литература

1. Валетчик В.А. Оценка живучести противоборствующих информационно-управляющих систем / В. А. Валетчик, А. Г. Додонов, В. Г. Путятин // Реєстрація, зберігання і обробка даних. –2002. – Т. 4, № 3. – С.104-112.

2. Василенко О. Н. Теоретико-числовые алгоритмы в крипторгафии / О. Н. Василенко. – М.: МЦНМО, 2003. – 328с.

3. Додонов А. Г. Введение в теорию живучести вычислительных систем / А. Г. Додонов, М. Г. Кузнецова, Е. С. Горбачик. –К.: Наук.думка, 1990. – 184 с.

4. Сербін В. Г. Деякі аспекти живучості складних гарантоздатних комп'ютерних систем критичних умов застосування / В.Г. Сербін, А.І. Сухомлин // Математичні машини і системи. – 2011. – № 4. – С. 189-192.

5. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. / Б. Шнайер. – М.: Изд-воТРИУМФ, 2003. – 816 с.

6. Joy M. Security Analysis of RSA-type Cryptosystems [Електронний ресурс] ; A dissertation subm. for the degree of Doctor of Philosophy in Applied Science. – Université catholique de Louvain, Oct. 1997. – 110 p. // – Режим доступу : http://joye.site88.net/theses/Joye_PhD.pdf (08.08.2012).

7. R. Canetti, C. Dwork, M. Naor, and R. Ostrovsky Deniable encryption // Advances in CRYPTO '97 – Spr. Ferlag, LNCS vol. 1294 – 1997. – P.90-104.

8. D. Coppersmith Finding a small root of a univaraite modular equation // Advances in Cryptology Proceedings of EUROCRYPT'96. – Springer Ferlag, LNCS vol. 1070 – 1996. – P.155-165.

9. Don Coppersmith, Matthew Franklin, Jacques Patarin, Michael Reitert Low. Exponenet RSA withrelated messages [Електронний ресурс] // – Режим доступу: http://www.cs.unc.edu/~reiter/papers/1996/Eurocrypt.pdf (08.08.2012).

10. Durfee G. Cryptanalysis of RSA with private key d less than $N^{0,292}$ [Електронний ресурс] // – Режим доступу: http://crypto.stanford.edu/~dabo/pubs/abstracts/lowRSAexp.html (08.08.2012).

11. Glenn Durfee Cryptanalysis of RSA using algebraic and lattice methods [Електронний ресурс] ; A dissertation subm. for the degree of Doctor of Philosophy, June 2002. – 114 p. Режим доступу: http://theory.stanford.edu/~gdurf/durfee-thesis-phd.pdf. (08.08.2012).

12. Galbraith Steven D. Mathematics of Public key Cryptography Part IV: Lattices / Steven D. Galbraith – Cambridge University Press, 2012. – 640p.

13. A. K. Lenstra, H. W. Lenstra Jr., and L. Lovasz Factoring polynomials with rational coefficients // MathematischeAnnalen. – 1982. –Vol. 261(4). – P. 515-534.

14. May Alexander. New RSA Vulnerabilities Using Lattice Reduction Methods [Електронний ресурс]: // A Dissertation Thesis. – UniversitätPadeborn, Oct. 2003. – 159 p. Режим доступу: http://www.cs.uni-paderborn.de/uploads/tx_sibibtex/bp.pdf (10.08.2012).