УДК 004.056

Уязвимости алгоритма вычисления секретного ключа в криптосистеме RSA

Алексеев А. П.

Постановка задачи: *во многих публикациях отмечается, что неверный выбор параметров шифра RSA может привести к уменьшению его криптостойкости. В некоторых случаях открытый и закрытый ключи могут полностью совпасть и тогда абонент случайно опубликует секретный ключ.* ***Целью работы*** *является доказательство возможности формирования ключей близнецов, когда открытый и закрытый ключ полностью совпадают.* ***Используемые методы****: возможность формирования ключей близнецов теоретически обоснована с помощью восьми лемм. Наличие ключей близнецов подтверждено проведёнными расчётами с помощью математической системы Mathcad. При проведении расчётов были рассмотрены функции Эйлера, кратные десяти, и открытые экспоненты, которые оканчивались цифрами 1 и 9.* ***Новизна:*** *показано, что при значениях функции Эйлера, кратных десяти, существует вероятность открытой публикации секретного ключа, если открытая экспонента оканчивается на цифры 1 или 9. Функция Эйлера формируется кратная десяти, если хотя бы одно простое число оканчивается единицей.* ***Результат****: расчётным путём подтверждена возможность формирования ключей близнецов.* ***Практическая значимость****: полученные результаты позволяют повысить криптостойкость шифра RSA путём проверки на совпадение сформированных открытых и закрытых ключей и тем самым предотвратить атаку на ключи близнецы.*

Ключевые слова: *асимметричная криптосистема RSA, уязвимость, секретный ключ, открытый ключ, функция Эйлера, лемма, простое число, чётное число, нечётное число, числа Ферма.*

Актуальность

Криптосистему RSA разработали R. Rivest, A. Shamir, L. Adleman [1], а саму концепцию шифрования с помощью открытого ключа предложили W. Diffie и M. Hellman [2].

Асимметричная криптосистема RSA широко используется в современных инфокоммуникационных системах благодаря своим несомненным достоинствам. Положительными свойствами этой криптосистемы являются возможность передачи приватной информации по незащищённым каналам связи без предварительной передачи секретных ключей с помощью курьеров [3] и обеспечение цифровой подписи финансовых документов [4]. На базе RSA реализована известная почтовая программа PGP [5]. Многие фирмы выпускают микросхемы, которые аппаратно реализуют криптосистему RSA [7].

Постановка задачи

В работах [9, 10] отмечается, что для формирования ключей необходимо использовать простые числа, длины которых должны быть примерно одинаковые. Для предотвращения факторизации модуля разрядность простых чисел в настоящее время должна быть не менее 1024…4096 бит [8, 10].

В ряде публикаций отмечается, что недопустимо использовать открытую экспоненту малой разрядности [10, 14]. При формировании открытой экспоненты из множества допустимых значений рекомендуют формировать её по случайному закону [7, 11, 13]. В некоторых источниках предлагают

использовать открытые экспоненты, которые содержат малое число единиц при их представлении в двоичной системе счисления [7], например, 3, 17, 65537. Это позволяет повысить скорость шифрования, так как уменьшается число операций возведения в степень. В других источниках рекомендуют использовать числа Мерсенна, Ферма [6] и малые нечётные числа [10, 12].

Использование некоторых из перечисленных рекомендаций может привести к появлению уязвимостей в криптосистеме RSA. Взлом криптосистемы возможен путём проведения атаки на наличие ключей близнецов.

Теоретическое обоснование

Известно, что расчёт секретной экспоненты t в криптосистеме RSA осуществляется с помощью сравнения [1]:

$$s \cdot t \equiv 1(\mathrm{mod}(\varphi(r)), \quad (1)$$

здесь s – число взаимно простое с $\varphi(r)$, так называемая открытая экспонента; r – произведение двух простых чисел p и q (модуль); $\varphi(r)$ – функция Эйлера, которая вычисляется по формуле:

$$\varphi(r) = (p-1)\cdot(q-1). \quad (2)$$

Из соотношения (1) по вычисленному значению функции Эйлера $\varphi(r)$ и выбранному значению s требуется найти такое значение t, при котором целочисленное деление величины $s \cdot t$ на $\varphi(r)$ даст остаток 1.

Для проведения анализа уязвимостей криптосистемы RSA рассмотрим несколько лемм.

Лемма 1.

Функция Эйлера $\varphi(r)$ является чётным числом.

Доказательство.

Функция Эйлера вычисляется по формуле (2). Все простые числа, используемые в криптографии, нечётные, поэтому функция Эйлера, равная произведению двух чётных чисел, является чётным числом.

Лемма 2.

Множество чисел открытой экспоненты s состоит из множества нечётных чисел.

Доказательство.

В соответствии с алгоритмом формирования ключей для асимметричной криптосистемы RSA числа s должны быть взаимно простыми с чётными числами $\varphi(r)$ [1], поэтому числа s будут обязательно нечётными.

Лемма 3.

Секретная экспонента t является нечётным числом.

Доказательство.

В соответствии с выражением (1) целочисленное деление произведения $s \cdot t$ на чётное число $\varphi(r)$ должно дать остаток, равный единице. Это возможно только при нечётных значениях произведения $s \cdot t$. В соответствии с леммой 2 число s является нечётным. Произведение $s \cdot t$ будет нечётным только при нечётных значениях t.

Лемма 4.

Функция Эйлера кратна 10, если хотя бы одно простое число модуля (p или q) оканчивается на 1.

Доказательство.

Используемые в практической криптографии простые числа могут оканчиваться только цифрами 1, 3, 7 и 9. Единственное простое число, которое оканчивается на 5 – это само число 5. Однако оно слишком мало для формирования реальных криптографических ключей. В соответствии с формулой для вычисления функции Эйлера (2) произведение указанных сомножителей будет кратно 10, если хотя бы одно простое число оканчивается на 1.

Считая, что формирование простых чисел происходит по случайному закону, можно ожидать, что 40% ключей создаётся при значениях функции Эйлера, кратной 10.

Лемма 5.

Если $\varphi(r)$ кратно 10, а число s оканчивается цифрой 7, то число t оканчивается цифрой 3.

Доказательство.

Так как произведение указанных чисел s и t будет оканчиваться единицей, то в результате вычитания единицы из произведения $s \cdot t$ будет получено число, кратное 10.

Таким образом, величину t нужно искать среди чисел, у которых последняя цифра 3, например, 3, 13, 23 и т.д.

Пример 1.

Пусть $\varphi(r) = 440$, $s = 27$. Расчёт секретного ключа с помощью обобщённого алгоритма Евклида [12] дал $t = 163$.

Лемма 6.

Если $\varphi(r)$ кратно 10, а число s оканчивается цифрой 3, то число t оканчиваться цифрой 7.

Доказательство.

Доказательство аналогично доказательству леммы 5.

Итак, величину t нужно искать среди чисел, оканчивающихся на цифру 7, например, 7, 17, 27 и т.д.

Пример 2.

Пусть $\varphi(r) = 440$, $s = 23$, тогда $t = 287$.

Лемма 7.

Если $\varphi(r)$ кратно 10, а s оканчивается цифрой 9, то последняя цифра числа t должна быть 9.

Доказательство.

Только произведение двух чисел, оканчивающихся цифрами 9 (при s, оканчивающимся на 9), даёт число, у которого последняя цифра 1. В этих случаях число $s \cdot t$-1 будет кратно 10.

Пример 3.

Пусть $\varphi(r) = 120$, $s = 19$. Расчёт дал $t = 19$.

Лемма 8.

Если $\varphi(r)$ кратно 10, а s оканчивается цифрой 1, то последняя цифра числа t должна быть 1.

Доказательство.

Только произведение двух чисел, оканчивающихся цифрами 1 (при числе s, оканчивающимся цифрой 1), даёт число, у которого последняя цифра 1. В этих случаях число $s \cdot t-1$ будет кратно 10.

Пример 4.

Пусть $\varphi(r) = 120$, $s = 31$. Расчёт дал $t = 31$.

Леммы 7 и 8 указывают на снижение криптостойкости в рассмотренных случаях (последние цифры открытого и закрытого ключей обязательно совпадают). Можно предположить, что могут быть сформированы полностью совпадающие числа s и t (ключи близнецы), то есть секретный ключ может быть ошибочно опубликован абонентом. Примеры 3 и 4 подтверждают это утверждение.

Другими словами, при $\varphi(r)$ кратном десяти и открытых экспонентах, оканчивающихся цифрами 1 и 9 есть вероятность открытой публикации секретного ключа. Если величина s выбирается по случайному закону, то для $\varphi(r)$, кратных 10, вероятность формирования экспонент, оканчивающихся цифрами 1 или 9, составляет 0,2 (половина всех ключей, у которых функция Эйлера кратна десяти). При этом небольшая часть секретных ключей полностью совпадёт с открытыми ключами.

Экспериментальная проверка

Рассмотренная гипотеза о возможности совпадения открытых и закрытых ключей была проверена расчётным путём с помощью математической системы Mathcad 15. Программа для расчёта ключей приведена в Приложении 1. Для $\varphi(r)$=440 выявлено 15 уязвимостей (открытый и закрытый ключи полностью совпали, например, 241, 351, 309, 419). Для $\varphi(r)$=18240 выявлено также 15 ключей близнецов (например, 14401, 14591, 15391). В последнем случае анализировались только ключи, оканчивающиеся на единицу.

Расчёты проводились следующим образом. Выбирались простые числа, которые оканчивались цифрой 1 (в этом случае функция Эйлера будет кратна 10). Для выбранного значения функции Эйлера определялись все допустимые значения открытой экспоненты s. Для значений s, которые оканчивались цифрами 1 или 9, вычислялись секретные экспоненты t. Отмечались совпадающие значения s и t.

Фрагмент протокола выполненных вычислений приведён в таблице 1.

Таблица 1. Фрагмент протокола вычислений

$\varphi(r)$	s	t	$\varphi(r)$	s	t	$\varphi(r)$	s	t
440	21	21	18240	191	191	120	11	11
440	111	111	18240	2431	2431	120	31	31
440	131	131	18240	3041	3041	120	61	61
440	221	221	18240	5281	5281	120	71	71
440	241	241	18240	5471	5471	120	91	91
440	331	331	18240	6271	6271	120	101	101
440	351	351	18240	8321	8321			
440	89	89	18240	9121	9121			
440	109	109	18240	9311	9311			
440	199	199	18240	11551	11551			
440	219	219	18240	12161	12161			
440	309	309	18240	14401	14401			
440	329	329	18240	14591	14591			
440	419	419	18240	15391	15391			
440	439	439	18240	17441	17441			

Выводы

При практическом формировании ключей в криптосистеме RSA в случаях, когда функция Эйлера кратна 10, а открытая экспонента оканчивается цифрами 1 или 9, следует произвести проверку на полное совпадение сформированных открытого и зарытого ключей. Очевидно, что совпадающие ключи не должны быть использованы.

Для исключения возникновения ключей близнецов при формировании открытой экспоненты нужно использовать числа, которые оканчиваются на 3 или 7, например, простые числа Ферма 17, 257, 65537.

Определить теоретически число ключей близнецов не представляется возможным. Выполненный объём вычислений в настоящее время мал, поэтому пока невозможно точно определить вероятность возникновения ключей близнецов. Их число нетривиально зависит от значения функции Эйлера. В настоящее время известна только верхняя граница вероятности появления одинаковых ключей (не более 0,2). Отсутствие оценки вероятности возникновения ключей близнецов объясняется необходимостью разработки соответствующего программного обеспечения и большим временем счёта. Если используются 1024-х битные простые числа, то число возможных функций Эйлера оценивается величиной $3{,}2 \cdot 10^{616}$. Для получения статистически устойчивого результата нужна репрезентативная выборка. Понятно, что время счёта будет внушительным. Однако предотвратить формирование ключей близнецов легко. Для этого достаточно произвести сравнение открытой и закрытой экспонент. Основная цель данной работы показать наличие ключей близнецов. В дальнейшем предстоит получить количественную оценку вероятности их формирования и оценить, насколько имеющееся ограничение уменьшит пространство допустимых ключей.

Приложение 1.

Программа на языке Mathcad 15 для формирования открытой и закрытой экспонент

Mathcad 15

Выбор простых чисел

$p1 := 97 \qquad q1 := 191$

Расчет функции Эйлера

$r1 := p1 \cdot q1 \qquad r1 = 18527$

$w1 := r1 - p1 - q1 + 1$

$w1 = 18240$

Расчет взаимно простых чисел

$ORIGIN := 1$

```
nod(a,b) := while (a ≠ 0) ∧ (b ≠ 0)
              if a ≥ b
                a ← mod(a,b)
                0
              otherwise
                b ← mod(b,a)
                0
            nod ← a + b
            nod
```

```
pr(a) := for i ∈ 2..a
           if nod(i,a) = 1
             j ← j + 1
             d_j ← i
           0
         d
```

Взаимно простые числа

$pr(18240) =$

	1
1	7
2	11
3	13
4	17
5	23
6	...

Обощенный алгоритм Евклида

a - функция Эйлера; b - открытая экспонента

$a := 18240 \qquad b := 14591$

$U := \begin{pmatrix} \overrightarrow{a} \\ 1 \\ 0 \end{pmatrix} \qquad V := \begin{pmatrix} \overrightarrow{b} \\ 0 \\ 1 \end{pmatrix} \qquad T := \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$

```
k1(a,b) := while T1 ≠ 0
             c ← U1 / V1
             q ← floor(c)
             T1 ← mod(U1, V1)
             T2 ← U2 − q·V2
             P ← T3
             P ← P + a if P < 0
             T3 ← U3 − q·V3
             U ← V
             V ← T
           P
```

t1 - секретная экспонента

t1 := k1(a,b) t1 = 1.4591 × 10^4

Литература

1. Rivest R., Shamir A., Adleman L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems // Communications of the ACM. 1978. T. 21. № 2. Pp. 120-126.

2. Diffie W., Hellman M. New Directions in Cryptography // IEEE Trans. Inform. Theory IT-22, (Nov. 1976). Pp. 644-654.

3. Алексеев А. П., Орлов В. В. Стеганографические и криптографические методы защиты информации. Самара: ИУНЛ ПГУТИ, 2010. 330 с.

4. Алексеев А. П. Информатика для криптоаналитиков. Самара: ИУНЛ ПГУТИ, 2015. 376 с.

5. Алексеев А. П. Информатика 2015. М.: СОЛОН-Пресс, 2015. 400 с.

6. RSA // Википедия, свободная энциклопедия [Электронный ресурс], 2015. URL: https://ru.wikipedia.org/wiki/RSA.html (дата обращения 1.08.2015).

7. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Издательство ТРИУМФ, 2002. 816 с.

8. Смарт Н. Криптография. М.: Техносфера, 2006. 528 с.

9. Введение в криптографию / Под общей редакцией Ященко В.В. Спб.: Питер, 2001. 288 с.

10. Фергюсон Н., Шнайер Б. Практическая криптография. М.: Издательский дом «Вильям», 2005. 424 с.

11. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. Основы криптографии. М.: Гелиос АРВ, 2002. 480 с.

12. Рябко Б. Я., Фионов А. Н. Основы современной криптографии и стеганографии. М.: Горячая линия-Телеком, 2010. 232 с.

13. Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. М.: Радио и связь, 2001. 376 с.

14. Петров А. А. Компьютерная безопасность. Криптографические методы защиты. М.: ДМК, 2000. 448 с.

References

1. Rivest R., Shamir A., Adleman L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, 1978. vol. 21. no. 2, pp. 120-126.

2. Diffie W., Hellman M. New Directions in Cryptography. IEEE *Trans. Inform. Theory IT-22*, 1976, pp. 644-654.

3. Alekseev A. P., Orlov V. V. *Steganograficheskie i kriptograficheskie metody zashchity informatsii* [Steganographic and Cryptographic Methods of Information Protection]. Samara, IUNL PGUTI Publ., 2010. 330 p. (in Russian).

4. Alekseev A.P. *Informatika dlya kriptoanalitikov.* [Informatics for Cryptanalysts]. Samara, IUNL PGUTI Publ., 2015. 376 p. (in Russian).

5. Alekseev A. P. *Informatika 2015* [Informatics 2015]. Moscow, SOLON-Press Publ., 2015. 400 p. (in Russian).

6. RSA. *Vikipedija* [RSA. Wikipedia, the free Encyclopedia]. Available at: https://ru.wikipedia.org/wiki/RSA (Accessed 1 August 2015).

7. Schneier B. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. New York, John Wiley & Sons, Inc. Publ. 792 p. 1996.

8. Smart N. *Cryptography: An Introduction*. New York, McGraw-Hill Companies Publ., 433 p. 2004.

9. Jashhenko V. V. *Vvedenie v kriptografiju* [Introduction to Cryptography]. Sankt Peterburg, Piter Publ., 2001. 288 p. (in Russian).

10. Ferguson N., Schneier B. *Practical Cryptography*. New York, JohnWiley&Sons Publ., 432 p. 2003.

11. Alferov A. P., Zubov A. Ju., Kuzmin A. S., Cheremushkin A. V. *Osnovy kriptografii* [Basics of Cryptography]. Moscow, Gelios ARV Publ., 2002. 480 p. (in Russian).

12. Rjabko B. Ja., Fionov A. N. *Osnovy sovremennoj kriptografii i steganografii* [The Foundations of Modern Cryptography and Steganography]. Moscow, Gorjachaja linija-Telekom Publ., 2010. 232 p. (in Russian).

13. Romanec Ju. V., Timofeev P. A., Shangin V. F. *Zashhita informacii v kompjuternyh sistemah i setjah* [Protecting Information in Computer Systems and Networks]. Moscow, Radio i svjaz Publ., 2001. 376 p. (in Russian).

14. Petrov A. A. *Kompjuternaja bezopasnost. Kriptograficheskie metody zashhity* [Computer Security. Cryptographic Methods of Protection]. Moscow, DMK Publ., 2000. 448 p. (in Russian).

Статья поступила 9 августа 2015 г.

Информация об авторе

Алексеев Александр Петрович - кандидат технических наук, доцент, старший научный сотрудник. Профессор кафедры информатики и вычислительной техники. Поволжский государственный университет телекоммуникаций и информатики. Область научных интересов: криптография; стеганография; информатика; контрольно-измерительная техника; дефектоскопия. Тел.: +7(846)228 00 57. E–mail: apa_ivt@rambler.ru

Адрес: 443013, г. Самара, ул. Льва Толстого, 23.

Vulnerabilities Algorithm for Computing the Secret Key in the RSA Cryptosystem

Alekseev A. P.

Purpose. *In many publications indicates that the wrong choice of parameters RSA encryption may reduce the reliability of his. However, no mention of the fact that the public key and private key, in some cases, can completely match the subscriber and then publish the private key. The aim is to prove the possibility of forming twin keys where public and private keys are the same.* ***Methods.*** *The possibility of forming the twin keys theoretically justified with eight lemmas.* ***Novelty****. It is shown that for values of Euler's function, a multiple of ten, there is a possibility of publication of the private key, if the public key numbers ending in 1 or 9.* ***Results****. By calculation confirmed the possibility of the formation of the twin keys.* ***Practical relevance.*** *The results will improve RSA cryptographic cipher by checking for a match generated public and private keys.*

Key words: asymmetric cryptosystem RSA, vulnerability, private key, public key, Euler function, Lemma, a prime number, an even number, odd number, the number of Farms.

Information about Author

Alekseev Aleksandr Petrovich - Ph.D. of Engineering Sciences, Associate Professor, Senior Research Officer. Professor at the Department of Computer Science and Engineering. Povolzhye State University of Telecommunications and Informatics. Field of research: cryptography; steganography, computer science; testing and measuring equipment; flaw detection. Tel.: +7(846)2280057. E–mail: apa_ivt@rambler.ru

Address: Russia, 443013, Samara, L. Tolstogo Street, 23.