References

1. Maslov O.N. *Ekologicheskiy risk i elektromagnitnaya bezopasnost* [Environmental risks and electromagnetic safety]. Moscow, IRIAS Publ., 2004. 330 p.
2. *Gigienicheskie trebovaniya k personalnyim elektronno-vyichislitelnyim mashinam i organizatsiya rabotyi. SanPiN 2.2.2/2.4.1340-03*. [Hygienic requirements for personal computers and the organization of work] Moscow, Rospotrebnadzor, 2003.
3. Maslov O.N. *Sluchaynyie antennyi: teoriya i praktika* [Random antenna: theory and practice]. Samara. PGUTI-OFORT, 2013. 480 p.
4. *Metodyi kompleksnogo kontrolya bezopasnosti informatsii na ob'ektah telekommunikatsionnyih sistem organov gosudarstvennogo upravleniya* [Methods of the complex control of information security at the facilities of government telecommunication systems]. Moscow, UDP RF Publ., 2009. 368 p.

Received 25.08.2015

УДК 004.056

АНАЛИЗ УЯЗВИМОСТЕЙ АЛГОРИТМА ВЫЧИСЛЕНИЯ СЕКРЕТНОГО КЛЮЧА В КРИПТОСИСТЕМЕ RSA

Алексеев А.П.
Поволжский государственный университет телекоммуникаций и информатики, Самара, РФ
E-mail: apa_ivt@rambler.ru

Описываются результаты анализа алгоритма формирования, открытого и закрытого ключей в асимметричной криптосистеме RSA (Rivest, Shamir, Adleman). Показано, что компрометация криптосистемы RSA возможна не только путем факторизации большого целого числа. При значениях функции Эйлера кратной 10 появляется вероятность появления ключей близнецов, когда сформированные открытые экспоненты оканчиваются цифрами 1 или 9. Приводится доказательство восьми лемм, содержащих теоретическое обоснование возникновения ключей близнецов. Рекомендовано для защиты криптосистемы от уязвимости при формировании ключей делать проверку на полное совпадение открытого и закрытого ключей.

Ключевые слова: криптография, асимметричная криптосистема, уязвимость, секретный ключ, открытый ключ, функция Эйлера, лемма, простое число, четное число, нечетное число, числа Ферма.

Введение. Постановка задачи

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: передача приватной информации по незащищенным каналам связи без предварительной передачи секретных ключей с помощью курьеров [3], цифровая подпись финансовых документов [4].

На базе RSA реализована известная почтовая программа PGP [5]. Взлом криптосистемы RSA затруднен вычислительной сложностью факторизации большого целого числа, являющегося произведением простых чисел. При формировании открытого ключа из множества допустимых значений рекомендуют формировать его по случайному закону [7; 11; 13]. В некоторых источниках предлагают использовать открытые ключи, которые содержат малое число единиц при их представлении в двоичной системе счисления [8]. Это позволяет повысить скорость шифрования, так как уменьшается число операций возведения в степень. В других источниках рекомендуют использовать числа Мерсенна и Ферма [6] и малые нечетные числа [10; 12].

Рассмотрим случаи, когда использование некоторых из перечисленных рекомендаций приводит к появлению уязвимостей в криптосистеме.

Теоретическое обоснование

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

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

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:

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

Из соотношения (1) по вычисленному значению функции Эйлера $\varphi(r)$ и значению s требуется найти такое значение t, при котором целочисленное деление величины $s\,t$ на $\varphi(r)$ даст остаток 1. Открытая экспонента s и модуль r образуют открытый ключ, а числа t и r – закрытый ключ. Для проведения анализа уязвимостей криптосистемы RSA рассмотрим несколько лемм.

Лемма 1. Функция Эйлера $\varphi(r)$ является четным числом.

Доказательство. Функция Эйлера вычисляется по формуле (2). Все простые числа нечетные, поэтому функция Эйлера, равная произведению двух четных чисел, является четным числом.

Лемма 2. Множество чисел открытой экспоненты s состоит из множества нечетных чисел.

Доказательство. В соответствии с алгоритмом формирования ключей для асимметричной криптосистемы числа s должны быть взаимно простыми с четными числами $\varphi(r)$, поэтому числа s будут обязательно нечетными.

Лемма 3. Секретная экспонента t является нечетным числом.

Доказательство. В соответствии с выражением (1) целочисленное деление произведения $s\,t$ на четное число $\varphi(r)$ должно дать остаток равный единице. Это возможно только при нечетных значениях произведения $s\,t$. В соответствии с леммой 2 число s является нечетным. Произведение $s\,t$ будет нечетным только при нечетных 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 практического формирования 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. Можно ожидать, что 25% ключей формируются 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 $s\,t$ 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 $\varphi(r) = 440$, $s = 27$. Расчет секретной экспоненты с помощью обобщенного алгоритма Евклида 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), дает число, у которого последняя цифра 1. В этих случаях число $s \cdot t - 1$ будет кратно 10.

Пример 3. Пусть $\varphi(r) = 120$, $s = 19$. Расчет 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), дает число, у которого последняя цифра 1. В этих случаях число $s\,t - 1$ будет кратно 10.

Пример 4. Пусть $\varphi(r) = 120$, $s = 31$. Расчет дал $t = 31$.

Леммы 7 и 8 указывают на снижение криптостойкости в рассмотренных случаях (последние цифры открытой и закрытой экспоненты 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 ключей, оканчивающихся цифрами 1 или 9, составляет 0,125. При этом некоторая

часть секретных ключей полностью совпадет с открытыми ключами.

Экспериментальное подтверждение

Рассмотренная гипотеза о возможности совпадения открытых и закрытых ключей была проверена расчетным путем с помощью математической системы Mathcad.

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 уязвимостей (например 14401, 14591, 15391). В последнем случае анализировались только ключи, оканчивающиеся на единицу.

Вывод

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 закрытого ключей. Очевидно, что совпадающие ключи не должны быть использованы. Среди существующих рекомендаций по выбору открытой экспоненты следует считать предпочтительным использование чисел Ферма.

Литература

1. Rivest R., Shamir A., Adleman L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems //Communications of the ACM. New York, USA: ACM, V. 21, №2, Feb. 1978. – P. 120-26. doi: 10.1145/359340.359342
2. Diffie W., Hellman M. New Directions in Cryptography // IEEE Trans. Inform. Theory IT-22, Nov. 1976. – P. 644-654. doi: 10.1109/TIT.1976.1055638
3. Алексеев А.П., Орлов В.В. Стеганографические и криптографические методы защиты информации. Самара: Изд-во ПГУТИ, 2010. – 330 с.
4. Алексеев А.П. Информатика для криптоаналитиков. Самара: Изд-во ПГУТИ, 2015. – 376 с.
5. Алексеев А.П. Информатика 2015. М.: СОЛОН-Пресс, 2015. – 400 с.
6. RSA. Википедия, свободная энциклопедия. https://ru.wikipedia.org/wiki/RSA. (д.о. 01. 08. 2015).
7. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – Изд-во ТРИУМФ, 2002. – 816 с.
8. Смарт Н. Криптография. М.: Техносфера, 2006. – 528 с.
9. Введение в криптографию. Под ред. В.В. Ященко. Спб.: Питер, 2001. – 288 с.
10. Фергюсон Н., Шнайер Б. Практическая криптография: Пер. с англ. М.: ИД «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.

Получено 10.08.2015

Алексеев Александр Петрович, к.т.н., профессор Кафедры информатики и вычислительной техники Поволжского государственного университета телекоммуникаций и информатики. Тел. (8-846) 228-00-57. E-mail: apa_ivt@rambler.ru

ANALYSIS OF SECRET-KEY ALGORITHM VULNERABILITY IN RSA-CRYPTOSYSTEMS

Alekseev A.P.
Povolzhskiy State University of Telecommunication and Informatics, Samara, Russian Federation
E-mail: apa_ivt@rambler.ru

This work describes results of analysis of public - and private-key generation algorithms in asymmetric RSA-cryptosystems. We demonstrated that RSA-cryptosystem can be compromised not only by large number factorization. Under Euler function value is multiple to 10, there is a probability of occurrence of two same public keys, when formed open exponents end in 1 or 9. 8 lemmas are described and proven with theoretical justification of same public keys occurrence. It is recommended to produce a complete test on full match of public- and private-key during key generation to improve vulnerability protection of cryptosystem.

Keywords: cryptography, asymmetric cryptosystem, vulnerability, secret key, public key, Euler function, lemma, prime, even number, odd number, Fermat numbers.

DOI: 10.18469/ikt.2015.13.4.17

Alekseev Aleksander Petrovich, PhD in Technical Science, Professor of the Department of Information and Computer Engineering, Povolzhskiy State University of Telecommunications and Informatics, Samara, Russian Federation. Tel. +78462280057. E-mail: apa2008@rambler.ru

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. doi: 10.1145/359340.359342
2. Diffie, W., Hellman, M. New Directions in Cryptography. *IEEE Trans. Inform. Theory IT-22*, 1976, pp. 644-654. doi: 10.1109/TIT.1976.1055638
3. Alekseev A.P., Orlov V.V. *Steganograficheskie i kriptograficheskie metody zashchity informatsii: uchebnoe posobie* [Steganographic and cryptographic methods of information protection]. Samara, PGUTI Publ., 2010. 330 p.
4. Alekseev A.P. *Informatika dlya kriptoanalitikov: uchebnoe posobie* [Informatics for cryptanalysts]. Samara, PGUTI Publ., 2015. 376 p.
5. Alekseev A.P. *Informatika 2015* [Informatics 2015]. Moscow, SOLON-Press Publ., 2015. 400 p.
6. RSA. Available at: https://ru.wikipedia.org/wiki/RSA. (Accessed 1.08.2015).
7. Shnajer B. *Prikladnaja kriptografija. Protokoly, algoritmy, ishodnye teksty na jazyke Si* [Applied Cryptography. Protocols, algorithms, source code in C]. Moscow, TRIUMF Publ., 2002. 816 p.
8. Smart N. *Kriptografija* [Cryptography]. Moscow, Tehnosfera Publ., 2006. 528 p.
9. Jashhenko V.V. *Vvedenie v kriptografiju* [Introduction to Cryptography]. St. Petersburg, Piter Publ., 2001. 288 p.
10. Fergjuson N., Shnajer B. *Prakticheskaja kriptografija* [Practical Cryptography]. Moscow, Izdatelskij dom «Viljam», 2005. 424 p.
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.
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.
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.

Received 10.08.2015

УПРАВЛЕНИЕ И ПОДГОТОВКА КАДРОВ ДЛЯ ОТРАСЛИ ИНФОКОММУНИКАЦИЙ

УДК 004.8

СРАВНЕНИЕ КЛАССИФИКАЦИОННЫХ ВОЗМОЖНОСТЕЙ АЛГОРИТМОВ C4.5 И C5.0

Пальмов С.В., Мифтахова А.А.
Поволжский государственный университет телекоммуникаций и информатики, Самара, РФ
E-mail: psv@psuti.ru

В статье проводится сравнение возможностей алгоритмов деревьев решений C4.5 и C5.0 - одних из наиболее эффективных инструментов классификации интеллектуального анализа данных. Для этого были выбраны две их программные реализации – отечественная аналитическая платформа Deductor и система See5. Чтобы повысить качество сравнительного анализа, использовались три разных набора данных. Как показали результаты эксперимента, утверждения автора-разработчика обоих алгоритмов Куинлана о том, что новая версия алгоритма во всем превосходит старую, оказались несколько излишне оптимистичными. C5.0 действительно строит, как и заявлено, более компактные деревья решений, но скорость его работы осталась сопоставимой с C4.5, а достоверность