МОДИФИКАЦИЯ СИСТЕМЫ RSA НА ОСНОВЕ ИДЕНТИФИКАТОРОВ ДЛЯ ЗАЩИТЫ E-MAIL

Вячеслав Олейник
Dekart Ltd.
w.oleinik@dekart.com, Dr.W.Oleinik@gmail.com

Abstract: *In this work the Identity Base Encryption (IBE) scheme, which is a public-key cryptosystem where E-mail address is a valid public key, is described. The approach based on the idea of the known cryptosystem - RSA modification for the purpose of the user permanent identifier (E-mail address) «insertion» on his public key is proposed.*

Keywords: *Identity Base Encryption, RSA, Secure E-mail.*

I. Введение

В 1976 г. была опубликована статья У. Диффи и М. Хеллмана «Новые направления в криптографии» [1], которая, по сути, открывала новое, революционное направление в криптографии. В этой работе приводится схема, в последствии названная *системой открытого распространения ключей*, или проще алгоритмом Диффи - Хеллмана. Эта система позволяет отказаться от передачи секретных ключей, т.е. позволяет обойтись без *защищённого канала* для передачи ключей, но она не устраняет необходимость *аутентификации*. Это означает, что получатель открытого ключа может быть уверен в его сохранности при передаче. Однако, у него нет оснований верить, что ключ принадлежит «верному» пользователю.

Следующей работой, внёсшей достойный вклад в криптографию с открытыми ключами, явилась статья Р. Ривеста, А. Шамира и Л. Адлмана «Метод получения цифровых подписей и криптосистем с открытыми ключами» [2]. Заметим, что хотя в названии и подчёркнута именно аутентификация, а не секретность, система RSA (образовано от первых букв фамилий авторов) не решает проблемы аутентификации открытых ключей пользователей. Аутентификация здесь означает возможность получения *цифровой подписи*, с помощью которой отправитель может заверять («подписывать») некоторые несекретные сообщения, для того, чтобы у получателя была возможность безошибочно установить отправителя.

На практике решение задачи аутентификации открытых ключей может быть осуществлено путём введения “третьей стороны” (третьего лица), в функции которой входит сертификация (подтверждение с помощью цифровой подписи) открытых ключей всех пользователей некоторой сети. Это лицо обычно принято называть Certification Authority (CA), а заверенный цифровой подписью открытый ключ пользователя – *сертификатом открытого ключ* или просто *сертификатом*. Такой подход позволяет решить основную проблему (проблему аутентификации), но порождает ряд новых проблем. В частности, открытые ключи CA в свою очередь требуют сертификации и мы в любом случае «имеем змею, кусающую себя за хвост».

Один из авторов системы RSA А. Шамир, в [3] высказал элегантную идею, которая заключалась в том, чтобы «роль открытого ключа играл идентификатор (постоянное имя) пользователя». Эта идея была подхвачена рядом авторов и развита в работах [4-8]. Но надежда, связанная с «избавлением» от некоторой третьей стороны, которой должны доверять все пользователи сети, увы, не сбылась. Главной особенностью, не позволившей решить эту проблему в указанных работах, явилось то, что идентификатор пользователя хоть и являлся прямо или косвенно открытым ключом, тем не менее, он «затрагивал» сам секретный ключ или секретную ключевую информацию.

В работах [9-10] был предложен иной подход к данной проблеме, который позволяет осуществить аутентифицированный обмен секретными ключами. Но в этих работах, по сути, проблема аутентификации открытых ключей используемых в алгоритме Диффи – Хеллмана решается с помощью алгоритма цифровой подписи (DSA), который в свою очередь требует аутентификации своих открытых ключей.

Наконец, ключевая идея, используемая в данной работе, была высказана автором в [11], и заключается в том, чтобы постоянный идентификатор пользователя не сам являлся открытым ключом, а был бы «вплетён каким-либо образом» в открытый ключ. Например, он может являться некоторым параметром для получения открытого ключа. Однако здесь обязательно должны выполняться следующие требования: идентификатор пользователя должен быть постоянным, должен однозначно определять данного пользователя и должен позволять осуществлять проверку его принадлежности. Например, для такого идентификатора идеально подходит адрес электронной почты (E-mail) пользователя.

В данной работе автор, используя вышеизложенную идею, предлагает модификацию (вариант) криптосистемы RSA, в которой проблема аутентификации открытых ключей в той или иной степени решена.

II. Модифицированный вариант RSA на основе идентификаторов

В системе RSA в основе её стойкости лежит тот факт, что разложение произведения двух больших простых чисел вычислительно очень трудно. В то же время поиск таких больших простых чисел является достаточно лёгкой задачей.

Для создания секретного и открытого ключей случайным образом выбираются два простых числа p и q. Произведение этих чисел даёт двухсоставное число (модуль) $n = p \cdot q$. Используя числа p и q можно вычислить значение функции Эйлера $j(n)$, показывающее количество положительных целых чисел от 1 до n, которые взаимно просты с n

$$j(n) = (p-1)(q-1).$$

Величина $j(n)$ присутствует в теореме Эйлера, которая гласит, что если наибольший общий делитель *НОД*(x, n) = 1, то

$$x^{j(n)} \equiv 1 \,(\mathrm{mod}\, n), \tag{1}$$

где $x < n$. Это выражение в более общей форме можно записать как

$$x^{kj(n)+1} = x \,(\mathrm{mod}\, n). \tag{1a}$$

Показатель степени e случайным образом выбирается так, что

$$\gcd(e, j(n)) = 1, \tag{2}$$

т.е. e является взаимно простым со значением функции Эйлера и соответственно взаимно простым с числами $p - 1$ и $q - 1$.

Зная $j(n)$ легко вычислить (с помощью Обобщённого алгоритма Евклида) такое единственное число d, что $0 < d < j(n)$ и

$$e \cdot d \equiv 1 \,(\mathrm{mod}\, j(n)),$$

или то же самое

$$e \cdot d = k \cdot j(n) + 1, \tag{3}$$

где k = 1, 2, ..

Числа e и n являются открытым ключом системы, а число d - секретным ключом. Заметим также, что параметры p, q и $j(n)$ являются также секретными и по большому счёту должны быть "уничтожены".

Вычисление криптограммы для некоторого текста Θ выполняется на основе открытого ключа следующим образом

$$C = \Theta^e \ (\mathrm{mod}\, n). \tag{4}$$

Если криптограмму *C* возвести в степень секретного числа (ключа) *d* по модулю *n*, то в результате получится открытый текст Θ, так как

$$C^d = \left(\Theta^e\right)^d (\mathrm{mod}\, n),$$

$$\left(\Theta^e\right)^d = \Theta^{ed} (\mathrm{mod}\, n),$$

далее делаем подстановку (3)

$$\Theta^{ed} = \Theta^{kj\,(n)+1} (\mathrm{mod}\, n)$$

и, наконец, в соответствии с (1а) имеем

$$\Theta^{kj\,(n)+1} \equiv \Theta\ (\mathrm{mod}\, n).$$

Применение здесь теоремы Эйлера возможно, поскольку известно, что если *n* является произведением двух простых неравных чисел, то необходимость в условии gcd(*x*, *n*) = 1 отпадает и равенство (1, 1а) верно для всех положительных целых *x*, меньших *n*.

Применим предложенный в [11] подход к системе RSA, а именно предположим, что при выборе числа *e*, мы будем его брать не случайно, а использовать для этого постоянный идентификатор пользователя. В этом случае идентификатор будет являться частью открытого ключа пользователя, и тем самым будет осуществляться его «автоматическая» аутентификация.

Однако, одним из необходимых требований в системе RSA является то, что число *e* должно удовлетворять условию (2). Очевидно, что для того, чтобы обеспечить выполнение данного условия, мы должны вычислять и выбирать соответствующим образом как само число *e*, так и параметры *p* и *q*. Кроме этого, с точки зрения безопасности, простые числа *p* и *q* должны быть т.н. сильными простыми. Поэтому, будем выбирать простые числа *p* и *q* так, что бы $p = 2 \cdot p' + 1$, а $q = 2 \cdot q' + 1$ и так чтобы числа p' и q' были также простыми, т.е. простыми числами Софи Жермен. Не трудно видеть, что в этом случае, поскольку $j\,(n) = (p-1)(q-1)$, то для выполнения условия (2) по крайней мере, необходимо чтобы число *e* было нечётным. Для этого число *e* будем вычислять как

$$e = 2 \cdot I_i + 1, \tag{5}$$

где I_i - постоянный идентификатор *i*-го пользователя, представленный в виде числа (На практике $I_i = H(Email_i)$, где *H* – хеш-функция, $Email_i$ - E-mail адрес *i*-го пользователя). Таким образом, условие (2) в нашем случае приобретает следующий вид

$$\mathrm{gcd}(e, j\,(n)) = \mathrm{gcd}(e, 4 \cdot p' \cdot q') = 1 \tag{6}$$

и ясно, что для того, чтобы оно выполнялось, необходимо и достаточно обеспечить $\mathrm{gcd}(e, p') = 1$ и $\mathrm{gcd}(e, q') = 1$. Это может быть обеспечено на этапе генерации и выбора простых чисел p' и q', т. е. путём случайного выбора простых p', q', проверки условий $\mathrm{gcd}(e, p') = 1$, $\mathrm{gcd}(e, q') = 1$ и отбрасывания того p' или q', которое не удовлетворяет этим условиям. Однако существует условие, выполнение которого обеспечивает выполнение условия (6) для любых значений I_i. Покажем этот факт. Поскольку p' и q' простые, а *e* в соответствии с (5) нечетно, то условие (6) будет выполняться всегда при условии, что

$$e = 2 \cdot I_i + 1 < p' \quad \text{и} \quad e = 2 \cdot I_i + 1 < q'. \tag{7}$$

Выполнение же последнего условия обеспечить достаточно легко на этапе практической реализации рассматриваемого здесь варианта RSA. Это можно сделать путем выбора соответствующей хеш-функции, которая бы заведомо выдавала значения I_i, удовлетворяющие условию (7).

III. Заключение

Связав, таким образом, параметр ***e*** криптосистемы RSA с постоянным идентификатором I_i пользователя ***i***, мы получаем новое качество для этой системы, а именно: это позволяет создавать на её базе секретные системы с открытыми ключами, не требующие заверки открытых ключей или параметров третьей стороной.

В данной работе мы попытались развить идею А. Шамир, высказанную им в [3], которая заключалась в том, чтобы в системах с открытым ключом «роль открытого ключа играл идентификатор пользователя». Причём, наша задача заключалась «в устранении» недостатков, обнаруженных в ряде других работ [4-7], посвящённых этой проблеме, которые заключались в том, что в них идентификатор пользователя хоть и являлся прямо или косвенно открытым ключом, тем не менее, он «затрагивал» сам секретный ключ или секретную ключевую информацию. Что не позволяло совсем отказаться от «услуг» третьей стороны, к которой должно быть доверие со стороны всех пользователей системы.

В данной работе предложен вариант модифицированной криптосистемы RSA, в котором можно отказаться от так называемой третьей стороны. Однако, этот вариант требует выполнения определенных условий: идентификатор пользователя является постоянным, он однозначно определяет конкретного пользователя и позволяет осуществлять проверку его принадлежности.

IV. Литература

1. W. Diffie and M.E. Hellman, "New Directions in Cryptography," IEEE Trans. on Info. Theory, Vol. IT-22, pp. 644-654, Nov. 1976.
2. R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Commun. of the Assoc. of Comp. Mach., vol. 21, pp. 120-126, Feb. 1978.
3. A. Shamir, Identity Based Cryptosystems and Signature Schemes. Advances in Cryptology, Crypto ’84, pp. 47-53, Springer-Verlad, 1985.
4. E. Okamoto, Proposal for Identity-based Key Distribution systems. Electronic Letter, Vol. 22, No. 24, pp. 1283-1284, 1986.
5. U. Maurer and Y. Yacobi, “Non-interactive public-key cryptography”, ***Advances in Cryptology-EUROCRYPT ’91 (LNCS 547)***, 498-507, 1991.
6. U. Maurer, “A remark on a non-interactive public-key distribution system”, ***Advances in Cryptology-EUROCRYPT ’92 (LNCS 658)***, 458-460, 1993.
7. W. Diffie, P.C. Van Oorschot, and M.J. Wiener, "Authentication and Authenticated Key Exchanges," in Designs, Codes and Cryptography, Kluwer Academic Publishers, 1992, pp. 107.
8. Олейник В. О проблеме обмена ключами на основе идентификаторов**.** Acta Academia 1998, Chisinau: Evrica, 1998, c. 26 - 38.
9. Oleinik W.L. Authenticated Diffie - Hellman Key Exchange on the Basis of DSA. The II International Conference on Microelectronics and computer Science, October 30 - 31, 1997, ICMCS'97, Vol.II, Tehnica Publishing House, Technical University of Moldova, pp. 184 - 187.
10. Олейник В. Расширение алгоритма Диффи - Хеллмана на базе DSA для аутентифицированного обмена ключами. Acta Academia 1997, Chisinau: Evrica, 1997, c. 23 - 38.
11. В. Олейник, Авто аутентификация в системах с открытыми ключами. Acta Academia 2001, Chisinau: Evrica, 2001, c. 27-35.