УДК 003.26:004.056.5

ИСПОЛЬЗОВАНИЕ RSA АЛГОРИТМА ДЛЯ ОБЕСПЕЧЕНИЯ ЗАДАЧ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В СОВРЕМЕННЫХ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

Артем Жилин, Александр Корнейко, Владимир Мохор

В наше время для решения задачи криптографической защиты информации, особенно в информационно-телекоммуникационных системах, широко применяют асимметричные криптоалгоритмы, среди которых RSA алгоритм стал наиболее популярным. Существующие публикации в основном раскрывают порядок применения RSA алгоритма, его примитивов в составе других криптоалгоритмов, анализируют стойкость этих криптосистем. При этом эти публикации не дают комплексной характеристики применения RSA алгоритма. Проанализированные источники показывают, что RSA алгоритм и порядок его применения описаны в ряде международных, национальных и отраслевых стандартов. Также в статье представлены конкретные примеры использования RSA алгоритма в протоколах информационно-телекоммуникационных систем, аппаратном и программном обеспечении для реализации задач криптографической защиты информации. Проведенный анализ показывает, что не смотря на появление в последние годы новых, более совершенных асимметричных криптоалгоритмов, RSA алгоритм остается достаточно широко представленным в современных информационно-телекоммуникационных системах для обеспечения задач криптографической защиты информации, в том числе и в нашей стране, что вызывает необходимость его более детального изучения.

Ключевые слова: *RSA алгоритм, ассиметричный криптоалгоритм, криптографическая защита информации.*

В настоящее время широкое применение в средствах криптографической защиты информации (КЗИ), используемых в информационно-телекоммуникационных системах (ИТС) для защиты информации, находят асимметричные криптоалгоритмы (АКА), которые используются в ИТС, как правило, для: распределения ключей, шифрования передаваемых ключей и формирования общего секретного ключа; обеспечения задач аутентификации абонентов и электронной цифровой подписи (ЭЦП); генерации криптографически сильных псевдослучайных последовательностей; генерации параметров ключевых массивов, используемых для создания ключей средств КЗИ и др. [3].

Среди всего разнообразия АКА криптоалгоритм RSA (Rivest-Shamir-Adleman) является наиболее распространенным в зарубежных криптосистемах – он стал стандартом де-факто для многих криптографических приложений [3, 11]. Существующие публикации [11] в основном раскрывают порядок применения RSA алгоритма, его примитивов в составе других криптоалгоритмов, анализируют стойкость этих криптосистем. При этом эти публикации не дают комплексной характеристики сфер применения RSA алгоритма. В связи с этим **целью данной работы** является анализ использования RSA алгоритма для обеспечения задач криптографической защиты информации в современных информационно-телекоммуникационных системах.

Так, использование RSA алгоритма для обеспечения задач КЗИ в ИТС рекомендовано рядом международных и национальных стандартов, например, ISO/IEC 11166-2:1994, 18033-2:2006 и 9796-2:2010, IEEE Std 1363-2000 и 1363a-2004, PKCS #1, RFC 2437, ANSI X9.44, FIPS 186-3:2009, ITU-T X.509, PEM и др. [18, 19, 12, 7, 20, 16, 13]. Кроме этого RSA алгоритм рекомендован некоторыми стандартами банковских систем электронных платежей S.W.I.F.T и ANSI X9.31, белорусским стандартом СТБ 34.101.22-2009 и австралийским стандартом управления ключами AS2805.6.5.3 [14, 6, 15].

Кроме того, в большинстве зарубежных стран, включая США и страны Евросоюза, RSA алгоритм находит широкое использование в различных средствах и технологиях КЗИ современных ИТС, в том числе и в тех, которые используются в интересах государственных структур. В Украине RSA алгоритм для обеспечения задач криптографической защиты секретной и служебной информации не допущен, однако, национальным стандартом ДСТУ ETSI TS 102 176-1:2009 оговорена возможность использования RSA алгоритма в национальных ИТС для реализации процедур ЕЦП [4]. В настоящее время RSA алгоритм используется в программном обеспечении таких фирм как Lotus Notes и Delrina PerForm Pro, встроен в операционные системы (ОС), разработанные компаниями Microsoft, IBM, Apple, Sun Digital и Novell [10, 22, 17, 9, 5].

Так, например, этот АКА используется в составе файловой системы шифрования EFS (Encrypting File System) семейства ОС Windows разработки корпорации Microsoft: Windows XP SP2, Windows 2000 SP4 (Server, Professional), Windows Server 2003, Windows Vista (Business, Enterprise, Home Encrypting File System Basic, Home Premium, Ultimate), Windows 2008 Server, Windows 7 (Enterprise and Professional). Система EFS использует архитектуру Windows CryptoAPI и предоставляет возможность обеспечивать КЗИ, хранящейся на разделах с файловой системой NTFS, для обеспечения несанкционированного доступа при физическом доступе к компьютеру и его дискам [14]. В зависимости от версии ОС Windows в системе EFS для шифрования данных при помощи симметричных алгоритмов 3DES, DESX или AES используются ключи шифрования файла FEK (File Encryption Key). Список используемых ключей FEK хранится в специальном атрибуте, который называется DDF (Data Decryption Field). Список ключей FEK также хранится вместе с файлом в специальной области EFS, которая называется DRF (Data Recovery Field). В составе EFS RSA алгоритм используется для создания и извлечения DDF и DRF (рис. 1) [10].

В более ранних версиях ОС Windows, выпущенных до Windows 7, наряду с ключами длиной 1024 и 2048 бит используются также 512-битовые ключи RSA. Начиная с ОС Windows 7 по умолчанию в файловой системе EFS используется 2048-разрядный ключ RSA, однако существует возможность выбора вместо него 1024-, 4096-, 8192- или даже 16384-разрядного ключа RSA [10].

Наличие таких длин RSA ключей в ОС Windows 7 с SP1, Windows Server 2008 с SP1 позволило Федеральной службе по техническому и экспортному контролю Российской Федерации (РФ) сертифицировать эти ОС на соответствие Федеральному Закону «О Защите персональных данных». Их разрешается использовать при создании автоматизированных систем класса защищенности 1Г включительно и при создании ИТ-систем персональных данных до 2 класса включительно [22].

RSA алгоритм используется в составе ИТС многих правительственных подразделениях США, включая ЦРУ, НАСА, департаменты обороны, труда и госслужбы, хотя детально порядок его использования в них нигде в открытых источниках не рассматривается. Из открытых источников известно. Что крупные корпорации выбрали RSA для внутреннего использования, среди них такие компании как Boeing, Shell Oil, DuPont, Raytheon, и Citicorp.

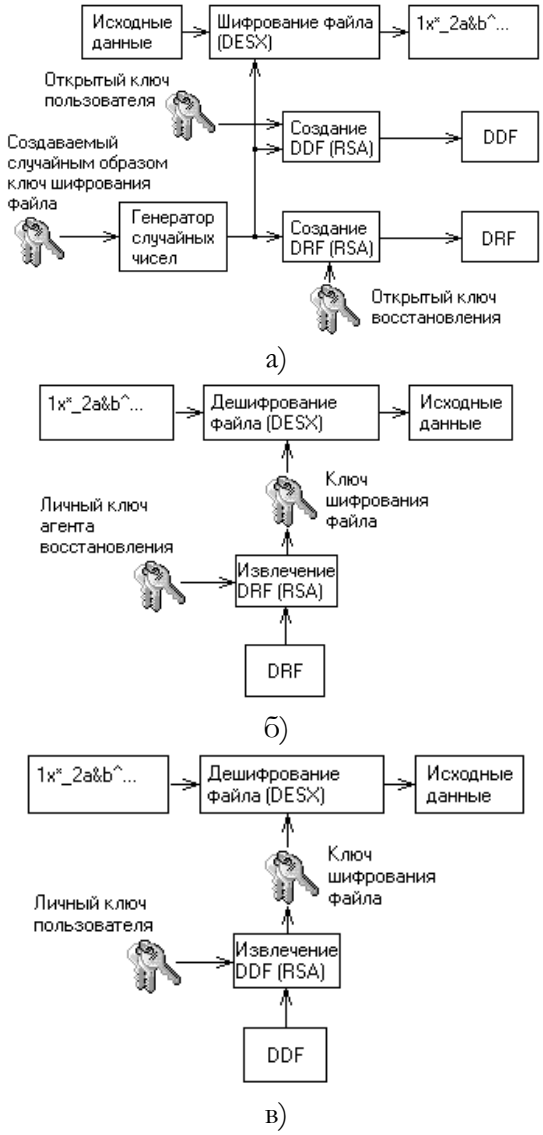

Рис. 1 Принцип использования RSA алгоритма в системе EFS Windows CryptoAPI на этапах зашифрования (а), расшифрования (б) и восстановления (в) данных [10]

В последние годы в правительственных учреждениях США с целью обеспечения требованиям стандарта Suite B, определенным АНБ США для защиты секретной информации, в файловой системе EFS ОС Windows вместо RSA алгоритма рекомендованы к использованию алгоритмы ECC (Elliptic Curve Cryptography). Однако файловая система EFS последних версий Windows поддерживает работу в смешанном режиме одновременно алгоритмов ECC и RSA, что позволяет обеспечить обратную совместимость с файлами EFS, созданными в предыдущих версиях Windows.

Корпорация Novell начиная с ОС NetWare 4.x для обеспечения криптографических задач зашифрования ключей и создания ЭЦП широко использует RSA алгоритм. В последних версиях этой ОС за счет использования программного модуля NICI (Novell Internation Cryptografy Infrastructure) используется RSA алгоритм с длинами ключей 1024, 2048 или 4096 бит [17].

В системе управления базами данных (СУБД) Oracle для авторизации пользователей в модуле Oracle Advanced Security используются RSA алгоритм, а для зашифрования данных – алгоритмы Triple-DES и RC4 [9]. Данная СУБД допущена к использованию в государственных учреждениях США. СУБД Oracle также получила от Гостехкомиссии при Президенте РФ сертификат на соответствие классу защищенности 1В. Уровень защищенности серверов БД Oracle позволяет использовать их в системах обработки информации, хранящих государственную тайну РФ. На данный момент не существует СУБД, которая бы получила сертификат Гостехкомиссии РФ более высокого класса защищенности. СУБД Oracle также обладает Аттестатом соответствия уровня требования безопасности, установленным приказом МО РФ, что позволяет ей быть использованной на объектах это ведомства.

RSA алгоритм также широко используется в сетевых Internet-технологиях, в частности, он входит в такие сетевые протоколы как SSL/TLS, SSH и IPsec, защищенные протоколы электронной почты S/MIME и PGP/MIME, протокол передачи информации через заполняемые формы на web страницах HTTPS (Hypertext Transfer Protocol Secure) и др. [5].

Так, например, RSA алгоритм используется в протоколе SSL (Secure Sockets Layer), который обеспечивает конфиденциальность обмена данными на транспортном уровне между клиентом и сервером, использующими TCP/IP соединения, и в протоколе TLS (Transport Layer Security), который принят как стандарт RFC и разработан на основании протокола SSL 3.0. В этих протоколах RSA алгоритм может применяться для процедуры аутентификации сервера/клиента, обмена ключами и проверки их подлинности. Современные версии протоколов SSL/TLS поддерживают длину RSA ключа 512…4096 бит, при этом по умолчанию в OpenSSL используются ключи длиной 512 бит [5].

В современных версиях протокола сеансового уровня SSH (Secure SHell) OpenSSH и SSH-2, которые доступны большинству сетевых ОС, включая Mac OS, Linux и BSD, и позволяют проводить удаленное управление ОС и тунелирование TCP соединений, RSA алгоритм ЭЦП с ключами длиной 1024, 2048 и 4096 бит используется, как правило, в процедуре аутентификации сеанса сервера [5].

В протоколах сетевого уровня IPsec (Internet Protocol Security) RSA алгоритм используется наряду с алгоритмами DSA или ECDSA при аутентификации [5]. По умолчанию в IPsec устанавливаются RSA ключи длиною 1024 бит.

В протоколе S/MIME (Secure/Multipurpose Internet Mail Extensions), разработанном компанией RSA Data Security, который добавляет сервисы КЗИ посредством инкапсуляции в протокол электронной почты MIME зашифрованных объектов и объектов ЭЦП, в том числе за счет RSA алгоритма [5]. А современные версии PGP (Pretty Good Privacy) поддерживают RSA ключи длиной 512…4096 бит [5].

В настоящее время RSA алгоритм также широко используется в ряде популярных прикладных программ. Например, в программном продукте Skype, обеспечивающем IP-телефонию, при установке соединения данные шифруются при помощи алгоритма AES (Advanced Encryption Standard), для передачи 256 бит ключа которого, в свою очередь, используется RSA алгоритм с 1024-битным ключом. Открытые ключи пользователей сертифицируются центральным сервером Skype при входе в систему с использованием 1536 или 2048-битных сертификатов RSA [1].

RSA алгоритм используется в Internet стандарте для почты с повышенной секретностью PEM (Privacy-Enhanced Mail), который одобренный Советом по архитектуре Internet (Internet Architecture Board, IAB). Сообщения в PEM шифруются алгоритмом DES в режиме CBC. Проверка подлинности, обеспечиваемая средством проверки целостности сообщения (Message Integrity Check, MIC), использует MD2 или MD5. Симметричное управление ключами может применять либо DES в режиме ECB, либо тройной DES с двумя ключами (так называемый режим EDE). Для управления ключами PEM также поддерживает сертификаты открытых ключей, используя RSA (длина ключа до 1024 битов) и стандарт X.509 для структуры сертификатов [5].

В аппаратном исполнении RSA алгоритм реализуются в защищенных телефонах, в сетевом оборудовании, в смарт-картах и электронных ключах (так называемых токенах) [3, 5].

В последние годы для аппаратного обеспечения функционирования RSA алгоритмов под управлением ОС Windows в системные платы современных ПЕОМ, как правило, встраивают микроконтроллеры TPM (Trusted Platform Module), которые производятся компаниями Atmel, Broadcom, Infineon Technologies AG (например, чип Infineon SLE66 CL PE), Intel, National Semiconductor, Sinosun, STMicroelectronics, Nuvoton, ITE и др. [21]. Стандартизация выработки ключей и их шифрование RSA алгоритмом в TPM модулях обеспечивается ISO/IEC 11889:2009 и TPM руководством. В настоящее время TPM модулями оснащены более 300 млн. компьютеров во всем мире.

В банковско-финансовой сфере для обеспечения безопасности денежных переводов и платежей, передачи служебной информации, организации электронного документооборота с возможностью ЭЦП используется аппаратно-программные средства, содержащие протоколы защищенной передачи информации на основе использования криптосистемы RSA.

Например, RSA алгоритм применяется в международной банковской системе информации и платежей S.W.I.F.T. Так, при обмене сообщениями между пользователями для обеспечения конфиденциальности и подлинности, а также для контроля над целостностью сообщений система S.W.I.F.T. рекомендует применять алгоритм проверки достоверности, который реализован в системе в виде службы обмена двусторонними ключами (BKE), основанном на стандарте ISO/IEC 11166-2:1994, который использует криптосистему RSA.

Еще в 2004 году компаниями MasterCard Worldwide и Visa Int. были утверждены единые требования к системам перечисления электронных платежей, использования банковских и платежных терминалов, формализованные в PCI PIN Security Requirements, PCI PIN Entry Device Requirements, PCI PIN Entry Device Evaluation Vendor Questionnaire и PCI Derived Test Requirements. Они предусматривали использование протокола защищенных электронных транзакций SET (Secure Electronic Transaction), где RSA алгоритм с длиной модуля в диапазоне от 320 до 2048 используется для шифрования PIN транзакций между терминалом и сервером банка [2]. В 2008 году Советом по безопасности индустрии платежных карт (PCI SSC) был принят новый стандарт безопасности платежных приложений PA DSS (Payment Application Data Security Standard), в соответствии с которым RSA алгоритм с длиной модуля не менее 1024 бит является обязательным для использования при передаче PIN-кода с платежных карт на терминалы.

В финансовых организациях на территории Украины, участвующих в Национальной системе массовых электронных платежей, в средствах защиты информации применяются механизмы строгой аутентификации и формирования (проверки) ЭЦП на базе RSA алгоритма [8]. RSA используется для защиты информации между сервером баз данных банка и его САБ, а также между ГПЦ и Расчетным банком. Длина используемого ключа зависит от персонального программного модуля генерации ключей, который выдается банкам территориальным управлением Национального банка Украины и в настоящее время, как правило, составляет не менее 1024 бит.

RSA алгоритм также используется в некоторых системах электронных платежей, действующих на территории Украины, например, в Web-Money и PayPal.

Выводы. Таким образом, проведенный выше анализ показывает, что не смотря на появление в последние годы новых, более совершенных AKA, RSA алгоритм в настоящее время остается достаточно широко распространенным для обеспечения задач криптографической защиты информации. Это подтверждается как множеством актуальных стандартов, в которых описано RSA алгоритм и порядок его применения, так и его реализаций в аппаратном и программном обеспечении, в протоколах сетевых технологий.

ЛИТЕРАТУРА

[1]. Букин Максим. Skype: глобальная система персональной связи // [Электронный ресурс]. – Режим доступа: http://www.pcweek.ru/themes/detail.php?ID=73403.

[2]. Голдовский И. RSA в терминалах / И. Голдовский // ПЛАС. – 2007. – № 2 (122). – С. 13-15.

[3]. Горбенко І. Д. Прикладна криптологія: Терія. Практика. Застосування : монографія / І. Д. Горбенко, Ю. І. Горбенко. – Харків : Вид-во «Форт», 2012. – 880с.

[4]. Електронні підписи та інфраструктури (ESI). Алгоритми та параметри безпечних електронних підписів. Частина 1. Геш-функції й асиметричні алгоритми (ETSI TS 102 176-1:2007, IDT): ДСТУ ETSI TS 102 176-1:2009, 2009.

[5]. Зубок В. Ю. Безпека глобальних інформаційних систем та мереж : консп. лекцій / В. Ю. Зубок, О. В. Корнейко, Д. В. Ланде, В. В. Мохор; під. заг. ред. О. В. Корнейка. – К. : Вид-во ІСЗЗІ НТУУ «КПІ», 2010. – 162 с.

[6]. Информационные технологии. Криптография на основе алгоритма RSA: СТБ 34.101.22-2009, 2009.
[7]. Информационные технологии. Методы обеспечения безопасности. Схемы цифровой подписи, обеспечивающие восстановление сообщений. Часть 2. Механизмы на основе целочисленной факторизации: ISO/IEC 9796-2:2010, 2010.
[8]. Правила організації захисту електронних банківських документів з використанням засобів захисту інформації Національного банку України, затверджені постановою Правління Національного банку України від 02.04.2007 № 112 і зареєстровані в Міністерстві юстиції України 24.04.2007 за № 419/13686.
[9]. Технические решения для безопасности данных в ORACLE // [Электронный ресурс]. – Режим доступа: http://www.re.mipt.ru/infsec/2004/essay/2004_Technical_solutions_to_security_in_ Oracle__Popov.htm.
[10]. Шифрующая файловая система EFS Windows // [Электронный ресурс]. – Режим доступа: http://www.ixbt.com /storage/efs.html.
[11]. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – Applied Cryptography. Protocols, Algorithms and Source Code in C / Б. Шнайер. – М. : Триумф, 2002. – 816 с.
[12]. Banking. Key management by means of asymmetric algorithms. Algorithms using the RSA cryptosystem: ISO 11166-2:1994, 1994.
[13]. Digital Signature Standard (DSS): FIPS 186-3:2009, 2009.
[14]. Digital Signatures using Reversible Public Key Cryptography for the Financial Services Industry (rDSA), Appendix A: ANSI X9.31-1998. – American National Standards Institute, 1998.
[15]. Electronic Funds Transfer. – Key Management: AS 2805.6.5.3 Standarts Australia, 1990.
[16]. Key Establishment Using Integer Factorization Cryptography: ANSI X9.44-2007, 2007.
[17]. NICI 2.7.1. Cryptografhic Library FIPS 140-2 Level 2, versin 1.5 // [Электронный ресурс]. – Режим доступа: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp767.pdf.
[18]. RSA Cryptography Standard: PKCS #1 v2.1. – RSA Laboratories, 2002.
[19]. Standard Specifications for Public Key Cryptography: IEEE Std 1363-2000. – IEEE, 2000.
[20]. Standard Specifications For Public Key Cryptography- Amendment 1: IEEE 1363a-2004, 2004.
[21]. Trusted Platform Module // [Электронный ресурс]. – Режим доступа: http://ru.wikipedia.org/wiki/Trusted_Platform_ Module#cite_note-0.
[22]. Windows 7 и Windows Server 2008 сертифицированы на соответствие закону о защите персональных данных // [Электронный ресурс]. – Режим доступа: http://bda-expert.com/2011/10/windows-7-server-2008-sertificirovany-na-sootvetstvie-zakonu-o-zashhite-personalnyh-dannyh/.

REFERENCES

[1]. Bukin Maxim. Skype: The global personal communications, [electronic resource]. Mode access: http://www.pcweek.ru/themes/detail.php?ID = 73403.
[2]. Goldovskiy I. RSA in terminals. PLAS , 2007, Vol. 122, No. 2, pp. 13-15.
[3]. Gorbenko I.D. Applied cryptology: theory. Practice. Application: Monograph., I.D. Gorbenko, U.I. Gorbenko., Harkiv: «Fort», 2012, 880 P.
[4]. Electronic signatures and infrastructures (ESI). Algorithms and Parameters secure electronic signatures. Part 1. Hash functions and asymmetric algorithms (ETSI TS 102 176-1:2007, IDT): State Standard of Ukraine ETSI TS 102 176-1:2009, 2009.
[5]. Zubok V.U. Security of global information systems and networks: lecture notes, V.U. Zubok, O.V. Korneiko, D.V. Lande, V.V. Mokhor., K.: publishing house of Institute of special communication and information security NTUU "KPI", 2010, 162 P.
[6]. Information technologies. Cryptography on the basis of algorithm of RSA: Natsionalny standard of Belarus 34.101.22-2009.
[7]. Information technology - Security techniques - Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms: ISO/IEC 9796-2:2010, 2010.
[8]. Terms of protect electronic banking documents using information security National Bank of Ukraine, approved by the National Bank of Ukraine of 02.04.2007 № 112 and registered with the Ministry of Justice of Ukraine from 24.04.2007 № 419/13686.
[9]. Technical solutions for data security in ORACLE, [electronic resource]. Mode access: http://www.re.mipt.ru/infsec/2004/essay/2004_Technical_solutions_to_security_in_Oracle__ Popov.htm.
[10]. The encrypting file system (EFS) in Windows, [electronic resource]. Mode access: http://www.ixbt.com /storage/efs.html.
[11]. Schneier Bruce. Applied Cryptography. Protocols, Algorithms and Source Code in C, Schneier Bruce. – M. Triumf, 2002, 816 P.
[12]. Banking. Key management by means of asymmetric algorithms. Algorithms using the RSA cryptosystem: ISO 11166-2:1994, 1994.
[13]. Digital Signature Standard (DSS): FIPS 186-3:2009, 2009.
[14]. Digital Signatures using Reversible Public Key Cryptography for the Financial Services Industry (rDSA), Appendix A: ANSI X9.31-1998., American National Standards Institute, 1998.
[15]. Electronic Funds Transfer. – Key Management: AS 2805.6.5.3 Standarts Australia, 1990.
[16]. Key Establishment Using Integer Factorization Cryptography: ANSI X9.44-2007, 2007.
[17]. NICI 2.7.1. Cryptografhic Library FIPS 140-2 Level 2, versin 1.5, [electronic resource]. Mode access:

http://csrc.nist.gov /groups/STM /cmvp/ documents/140-1/140sp/ 140sp767.pdf.
[18]. RSA Cryptography Standard: PKCS #1 v2.1. – RSA Laboratories, 2002.
[19]. Standard Specifications for Public Key Cryptography: IEEE Std 1363-2000, IEEE, 2000.
[20]. Standard Specifications For Public Key Cryptography- Amendment 1: IEEE 1363a-2004, 2004.
[21]. Trusted Platform Module, [electronic resource]. Mode access: http://ru.wikipedia.org/wiki /Trusted _Platform_ Module#cite_note-0.
[22]. Windows 7 и Windows Server 2008 сертифицированы на соответствие закону о защите персональных данных, [electronic resource]. Mode access: http://bda-expert.com/2011/10/windows-7-server-2008-sertificirovany-na-sootvetstvie-zakonu-o-zashhite-personalnyh-dannyh/.

ВИКОРИСТАННЯ RSA АЛГОРИТМУ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЗАДАЧІ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ В СУЧАСНИХ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

У наш час для вирішення задачі криптографічного захисту інформації, особливо в інформаційно-телекомунікаційних системах, широко застосовують асиметричні криптоалгоритми, серед яких RSA алгоритм став найбільш популярним. Існуючі публікації в основному розкривають порядок застосування RSA алгоритму, його примітивів у складі інших криптоалгоритмов, аналізують стійкість цих криптосистем. При цьому дані публікації не дають комплексної характеристики застосування RSA алгоритму. Проаналізовані джерела показують, що RSA алгоритм і порядок його застосування описані в ряді міжнародних, національних і галузевих стандартів. Також у статті представлені конкретні приклади використання RSA алгоритму в протоколах інформаційно-телекомунікаційних систем, апаратному та програмному забезпеченні для реалізації завдань криптографічного захисту інформації. Проведений аналіз показує, що не дивлячись на появу в останні роки нових, більш досконалих асиметричних криптоалгоритмів, RSA алгоритм залишається досить широко представленим в сучасних інформаційно-телекомунікаційних системах для забезпечення завдань криптографічного захисту інформації, зокрема й в нашій країні, що й викликає необхідність його більш детального вивчення.
Ключові слова: RSA алгоритм, асиметричний криптоалгоритм, криптографічний захист інформації.

USING RSA ALGORITHM FOR PROBLEMS OF CRYPTOGRAPHIC PROTECTION OF INFORMATION IN MODERN INFORMATION&TELECOMMUNICATION SYSTEMS

In our time, asymmetric cryptoalgorithms are widely used in solving the problem of cryptographic protection of information, especially in information and communication systems, they include RSA algorithm that has become the most popular. Existing publications mainly reveal the application of RSA algorithm, its primitives in other cryptoalgorithms, analyzing the stability of these cryptosystems. Besides, these publications do not provide a comprehensive description of the applications of RSA algorithm. Analyzed sources shows that RSA algorithm and the procedure for its application are described in a number of international, national and industry standards. This article also presents specific examples of using RSA algorithm in the protocols of information and telecommunication systems, and in hardware and software for the realization of cryptographic protection. The analysis shows that despite the appearance of new and more sophisticated asymmetric encryption algorithms in recent years, RSA algorithm is still widely represented in modern information and telecommunication systems to provide cryptographic security problems, including in our country, as it calls for a more detailed study.
Index Terms: RSA algorithm, an asymmetric encryption algorithm, cryptographic protection of information.

Жилін Артем Вікторович, кандидат технічних наук, провідний науковий співробітник Науково-дослідного центру Інституту спеціального зв'язку та захисту інформації НТУУ «КПІ».
E-mail: jhartem@i.ua.
Жилин Артём Викторович, кандидат технических наук, ведущий научный сотрудник Научно-исследовательского центра Института специальной связи и защиты информации НТУУ «КПИ».
Zhylin Artem, Ph.D. in Eng., Senior Research Fellow of the Research Center, Institute of Special Communication and Information Security of NTUU «KPI».

Корнейко Олександр Васильович, кандидат технічних наук, доцент, заступник Голови Державної служби спеціального зв'язку та захисту інформації України.
E-mail: kav@dsszzi.gov.ua.
Корнейко Александр Васильевич, кандидат технических наук, доцент, заместитель Председателя Государственной службы специальной связи и защиты информации Украины.
Korneiko Oleksandr, Ph.D. in Eng., Associate Professor, State Service of Special Communication and Information Protection of Ukraine Deputy Chairman.

Мохор Володимир Володимирович, доктор технічних наук, професор, завідуючий кафедри Кібербезпеки та застосування інформаційних систем та технологій Інституту спеціального зв'язку та захисту інформації НТУУ «КПІ».
E-mail: mokhor@rambler.ru.
Мохор Владимир Владимирович, доктор технических наук, профессор, заведующий кафедры Кибербезопасности и применения информационных сис-

тем и технологий Института специальной связи и защиты информации НТУУ «КПИ».
Mokhor Volodymyr, Professor, Doctor of Science in Eng., Head of Academic Department of Cybersecurity and the use of information systems and technologies, Institute of Special Communication and Information Security of NTUU «KPI».

УДК 004.4.056.53:004.43(031)

ОСОБЛИВОСТІ СИСТЕМИ КОНТРОЛЮ ІНФОРМАЦІЙНИХ ПОТОКІВ ВЕЛИКОГО РОЗМІРУ

Володимир Луценко, Андрій Балан

Для побудови комплексних систем захисту інформації та інших систем безпеки необхідно проводити аналіз ризиків інформації. При обслуговуванні систем передавання даних великих розмірів в оптичних лініях зв'язку нагляд за даними є складним завданням. Воно вимагає застосування нових апаратних рішень у засобах контролю, нагляду та збору даних, що є вихідною інформаційною базою майбутніх проектів. Розглянутою є проблема використання нових засобів захисту інформації при проектуванні комплексних систем захисту інформації. Головна увага приділяється методам контролю за потоками інформації великого розміру, котрі досяжні атакам кіберзлочинців. Розглядаються питання систем контролю, котрі застосовуються в Україні та за її межами, та мають функціональні властивості що дозволяють здійснювати захист від кібертероризму при їх використанні у якості засобів захисту в рамках проектів комплексних систем захисту (КСЗІ).

Ключові слова: *комплексна система захисту інформації; проект захисту; лінії зв'язку; сітьовий екран; сітьовий комплект.*

Вступ. Згідно Закону України «Про внесення змін до Закону України «Про ратифікацію Конвенції про кіберзлочинність»», що була ратифікованою 7 вересня 2005 р., в Україні органом, на який покладаються повноваження щодо створення та функціонування цілодобової контактної мережі для надання невідкладної допомоги при розслідуванні злочинів, пов`язаних з інформаційно - комп`ютерними системами (ІКС) та даними, переслідуванні осіб, що обвинувачуються у вчиненні таких злочинів, а також збирання доказів в електронній формі, є Міністерство внутрішніх справ України. Необхідність протидії кіберзлочинності визначається фактом підписання цього Закону. Масштабність проблеми може ілюструватися хоча б результатами обговорень на Конференції з питань інформаційної безпеки проведеною 9 грудня 2009 р. Американською торгівельною палатою в Україні, де присутніми були президенти торгівельних палат, посол США, генеральний директор «Майкрософт Україна», українські та зарубіжні фахівці з питань інформаційної безпеки та кіберзлочинності: представники МВС України, Федерального бюро розслідувань (FBI) та інші фахівці. Фахівці одностайні у тому, що безперервне зростання кіберзлочинності пов'язане з тим, що реалізація електронних злочинів, як правило, не є складною (95% фінансове шахрайство та крадіжки; 5% шпіонаж).

З огляду на реальні справи в Україні теза про нескладність реалізації кіберзлочинів має рацію.

Постановка проблеми. З огляду на реальні справи в Україні теза про нескладність реалізації кіберзлочинів має рацію. Такий стан підтримується тим, що не є систематизованими та врегульованими, наприклад, такі питання як:

– централізація відомостей та узгодженість дій з боку дозвольних органів, органів контролю (НКРЗ) та органів слідства про архітектуру та функціонування мереж ВОЛЗ власників «TransTeleCom», «Vympelcom», «RETN», «SMUR», «MTS», «Golden Telecom», «Romtelecom», «PanTel», «T-Com», «Matav», «GTS», «TelKolejowa». Особливо важливими при цьому є відомості щодо мережевого зв'язку з боку Польщі, Білорусі, Росії, Румунії, Молдови, Угорщини, Словаччини, загальні з Україною мережі котрих обслуговуються вищезазначеними власниками;

– фактична складність систематизації даних щодо приватних власників ліній останньої милі;

– встановлення регламенту користування трафіками на фізичних та логічних рівнях від магістралей з віддзеркаленнями на маршрутизатори, а далі на комутатори і до трафіків останньої милі;