RSA Public Key Cryptography Algorithm – A Review

Article *in* International Journal of Scientific & Technology Research · July 2017

CITATIONS
95

READS
30,628

2 authors:

Shireen Nisha
University of Fiji
4 PUBLICATIONS **109** CITATIONS
SEE PROFILE

Mohammed Farik
University of Fiji
31 PUBLICATIONS **374** CITATIONS
SEE PROFILE

RSA Public Key Cryptography Algorithm – A Review

Shireen Nisha, Mohammed Farik

Abstract: This paper aims to review RSA, examine its strengths and weaknesses, and propose novel solutions to overcome the weakness. RSA (Rivest, Shamir, and Adleman) is one of the best cryptographic algorithms in use today that ensures secure communication over networks.

Index Terms: Algorithm, Cryptography, Cypher text, Private Key, Public Key, RSA.

1 Introduction

NETWORKS are a must for any company to achieve competitive advantage; however, all communication over any network, mainly the Internet needs to be secure to prevent breach of confidential and sensitive data. An IBM sponsored benchmark study carried out by Ponemon Institute for the past 11 years highlights the alarming boost (see Fig. 1) in the average cost of data breach globally (ACoDBG) each year with 2016 being $4 million [1], a 29 percent increase since 2013 [2].

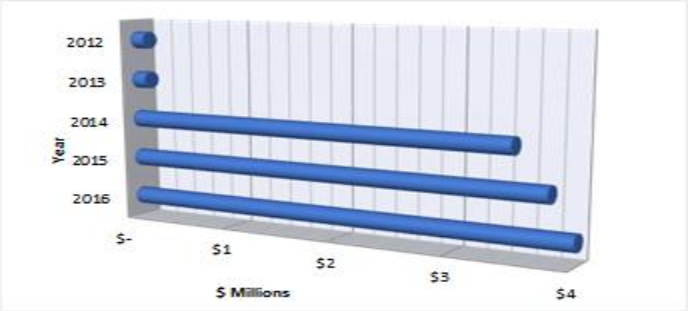

Fig 1: *Global average cost of data breach from years 2012 to 2016. Data from Ponemon Institute reports for the years 2012 [3], 2013 [3], 2014 [4], 2015 [5] and 2016 [1].*

Networks aren't just used by businesses but also by home users. Hence, network security is of utmost importance. This brings in cryptography, as a major component enabling secure communications over networks. Cryptography looks at methods of hiding the actual message from unintended recipients by scrambling the data via an algorithm. The first proven use of cryptography dates back to 1900 B.C, Ancient Egypt, when a document writer used irregular hieroglyphs (writing system using a combination of graphics, symbols and alphabet) while copying a document [6]. Modern cryptography algorithms offer more security than the ancient ones and can be divided into 3 categories, namely secret key, public key and hash functions. The focus of this paper is public key cryptography (PKC) algorithm.

- *Shireen Nisha is currently pursuing masters degree program in Information Technology in the School of Science and Technology at the University of Fiji. E-mail: shireenn@unifiji.ac.fj*
- *Mohammed Farik (Member IEEE) is a Lecturer in Information Technology in the School of Science and Technology at the University of Fiji. E-mail: mohammedf@unifiji.ac.fj*

The rest of the paper is organized as follows: the next section looks at literature review on RSA algorithm as the most widely used PKC algorithm, section 3 looks at current usage of RSA, section 4 highlights the strengths and weakness of RSA, while section 5 briefly discusses the recommendations to mitigate some of the identified drawbacks. Lastly, section 6 concludes the paper and discusses about future works in this area.

2 RSA Public Key Cryptography

Known also as asymmetric encryption, PKC works on the concept of dual keys. While the recipients' public key is used to encrypt the message, the private key is used for decryption, so there is no need to share a secret key as required in secret key (symmetric) cryptography [6]. PKC is largely used for authentication, non-repudiation, and key exchange [7]. The most widely used PKC algorithm in the world today, Rivest, Shamir, and Adleman algorithm (RSA) [6], [7], [8], [9] is considered superlative in comparison with algorithms such as the symmetric key Advanced Encryption Standard (AES) [8] and the asymmetric Goldwasser and Micali (GM) algorithms [7]. Officially launched in 1977 and named with the surname initials of inventors Ron Rivest, Adi Shamir, and Leonard Adleman, RSA is actually a set of two algorithms; key generation, the most complex part used to produce the public and private keys, and RSA function evaluation which looks at encrypting and decrypting [10]. Fig. 2 explains how the public and private key is generated. Fig. 4 shows the methods of encrypting plaintext and decrypting a ciphertext using the two keys.

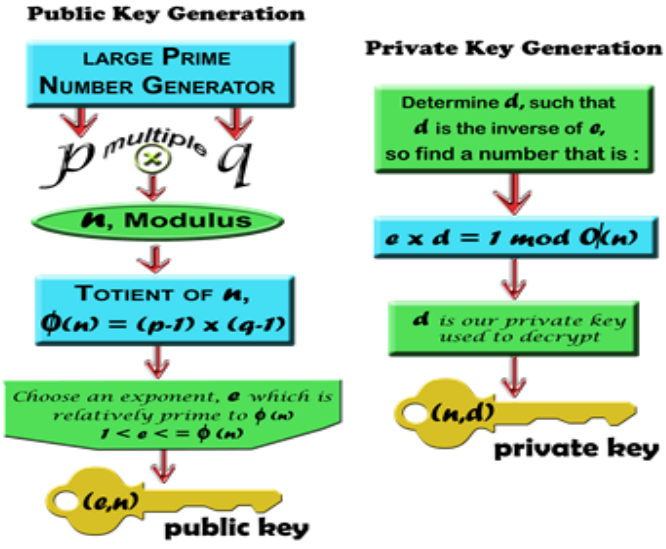

Fig 2: *RSA Public Key and Private Key Generation Method*

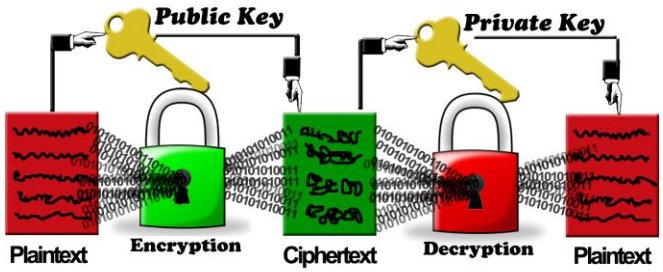

Fig 3: *RSA Encryption and Decryption Methods*

RSA Security Inc. had a 17 year hold on RSA algorithm patent from 1983 till its expiry in 2000, however, the company surprisingly released its claim on the patent two weeks before the expiry date, making RSA available to the public domain, prompting a major competitor, Baltimore Technologies into free giveaway of a version of its Keytools developer tool kit which uses RSA algorithm and had cost developers $10,000 to $20,000 until now [11]. The patent years saw more than 800 licensed customers and development of over 1,000 applications, including the likes of Microsoft Windows, Netscape Navigator, Intuit Quicken, Lotus Notes, PGP, Cisco Systems Inc., routers, credit cards, iPhone text messaging, making web connections, and hundreds of other products/services to protect trillions of transactions [9], [11], [12], [13].

3 Current usage of RSA

Looking at where RSA is being used today, let's take the example of ***Pretty Good Privacy*** in short PGP, a freeware created by Phil Zimmerman, providing encryption and authentication for e-mail and file storage applications across multiple platforms and it uses RSA algorithm for its key transportation [14], [15]. Many cloud service providers also use PKC for authentication. One example is ***Googles G Suite***, a brand of cloud based services that has been rated as excellent on PGMags review in February 2017, has about 3 million paid customers including large companies such as Whirlpool and PiceWaterhouseCoopers taking advantage of a collaboration-ready office suite, a website, shared calendars, mail services, chat, video conferences, social media, real-time document collaborations, and many more [16], [17]. This service has encryption at numerous stages and is enabled by default for all customers. Firstly, data access is enabled through Hypertext Transfer Protocol Secure (HTTPS) encrypted tunnels, then it uses Perfect Forward Secrecy (PFS), for which Google made headlines in 2011 for being the first to enable this feature [18], which scrambles data as it moves between their and other companies servers and it uses SSL (Secure Sockets Layer)/TLS (Transport Layer Security) for connectivity where the 256-bit TLS looks at the encryption enforcement policy which rejects all inbound and outbound mail from other mail servers if they don't use TLS [19]. A common operation in IT is RSA signature verification and many protocols such as SSH, OpenPGP, S/MIME and SSL/TLS rely on it [20]. ***SSL certificates*** are used to protect the online users' private and sensitive data. In its bids to up defenses against the growth in cryptanalysis, Google has upgraded the length of all its SSL certificates RSA encryption keys from 1024 to 2048 bits for validation and key exchange in 2013 [19], [21]. SSL, initially developed by Netscape, delivers data security incrusted between internet-based communications protocol TCP/IP and application protocols such as HTTP, Telnet, Network News Transfer Protocol (NNTP), or File Transfer Protocol (FTP) by establishing an RSA key exchange during the SSL handshake between client and server to authenticate each end of the connection [14]. Moreover, RSA is used for employee verification in many organizations. Chip based smart cards use cryptographic algorithms to ensure security by checking the PIN code [22]. Some of these cards use RSA algorithms in combination with other algorithms. For instance, ***IDPrime MD 3811 smart cards***, a single chip based dual-interface (contact and contactless ISO14443 interface) smart card developed by Gemalto is also compatible with the NFC standard already widely used by mobile devises today and is secured with both RSA and elliptic curves algorithms [23]. Another example of Gemalto's cards is the ***IDPrime PIV (personal identity verification) card v1.55*** that looks at improved identification and authentication of US Federal employees and contractors to access Federal amenities and was published as FIPS PUB – 201 [24]. Another product that uses RSA is the ***RSA SecurID,*** a two-factor authentication technology used in high-security environments to protect network resources and can be hardware authenticator (a USB token, smart card, software application residing on your smartphone or key fob) and RSA authentication manager software based tokens [25]. The authenticator generates passcodes/pin tokens which resets itself every 60 seconds making the previous token worthless. When trying to access a protected resource, users enter the passcode together with their username which are intercepted by the RSA authentication Agent and presented to the RSA SecureID system on the RSA authentication server which validates the pass code by running the same algorithm that was used to generate the passcode to check if their 8 digit output matches the one entered by the user along with the username before granting access to the remote server [26].

4 Strengths and weaknesses of RSA

One of the reason RSA has become most widely used is because it allows either of the two keys to encrypt a message and the opposite key to decrypt it, thus promising confidentiality, integrity, authenticity and non-reputability of data and electronic communications [20]. It's important to note that a weak key generation will make RSA very vulnerable to attacks therefore care must be taken to ensure that two large random prime numbers are used to calculate the modulus, n [10], which will become the public key and the private key will consist of those two primes themselves. The effectiveness of RSA algorithm comes from the fact that it's difficult to computationally factor large integers into primes [12], [20]. Multiplying the two primes is easy but performing the reverse in the form of factoring is actually hard and gets even harder as the values of p and q gets bigger [27]. Take for instance, the RSA Factoring Challenge enacted by RSA Laboratories in 1991, has many moduli still pending to be factored. On 12 December 2009, a 768-bit RSA modulus containing a 232 decimal digit number was factored by a total of 13 researchers over a span of two years using hundreds of parallel computers, a task equivalent to approximately 2000 years of computing on a single-core 2.2 GHz AMD processor [12], [27], [28]. The larger the key length of the modulus, the more time it takes to be factored. The Federal Information Processing Standards Publication (FIPS PUB) 186-4 specifies three choices for the length of the modulus, n, to be 1024, 2048 and 3072 bits [29]. RSA's strength lies in its key size, since it's not

easy to factor large primes, however encrypting with larger modulus has certain negatives associated with it, particularly when dealing with mobile devices as it requires more computing power and battery resource usage for key generation thus impairing device performance [20]. Most hardware and software in compliance with FIOS PUB 186-4 [29] are moving from the first choice of key length to the second and are having a minimum of 2048 bits as being secure but with increase in computing power, more efficient factoring algorithms and advances in cryptanalysis techniques, the ability to crack these keys also increases [20]. A major hurdle to RSA cryptosystems is the enabling company's inability to accept that a problem does exist in the key length and the unwillingness of upgrading to keep up with the computing power of the current and possible future devices. An example from the past highlights this negligence. Chosen in 1980s, and broken in 2000, a 320-bit RSA modulus for Carte Bleue, is surely a mark of severe ineffectiveness on the part of the organization that oversaw security for 33 million French credit cards [30], [31]. After 2 years of failed attempts to convince the company of the serious flaws, Serge Humpich, a 36 year-old engineer purchased some metro tickets with fake cards and sent prove to the credit card company in attempts to sell his idea, however he was convicted to 10 months suspended sentence [30], [31]. The use of acoustic cryptanalysis is another challenge looming over the security offered by cryptography. A team of researchers, including Adi Shamir, a co-inventor of RSA, carried out an acoustic cryptanalysis attack on the popular GnuPG software which is a complete and free implementation of the OpenPGP standards and have successfully determined a 4096-bit RSA key within an hour, using the sound generated by the computer during the decryption of some chosen cipher texts [20], [32].

5 Recommendations

Several recommendations needs to be highlighted in relation to RSA cryptography. While the strength of RSA lies in the large prime number based keys, it's also causing RSA to be slower compared to other algorithms in terms of key generation. One example is the JSCAPE MFT Server, a platform independent server that consolidates all file transfer processes into a single easy to use application which requires users to choose between two supported key algorithms: RSA or digital signature algorithm (DSA) during the process of generating a public-private keypair in PGP [33]. Generally encryption happens at client end while decryption on the server side. Let's say that in the JSCAPE server the client side machine is slower and server more powerful then RSA is used for server keys as it has smaller computational requirements for encryption, thereby encrypting faster, however, if server is slower than DSA is used as there is a need for server keys that have smaller computational requirements for decryption, thus impacting the start of the session only [33]. Same goes for authentication which entails of signing on the client side and verification on the server side. If client machines are slow then DSA is used and if slower server then RSA is used for verification, yet again difference of speed is at the start of the process [33]. Another example is elliptic curve cryptography (ECC), which is seen as more suitable for mobile apps than RSA because of its ability to generating faster and smaller keys using lower computing power [20]. Current trends suggest an escalated adaptation and shift towards mobile computing. According to the digital in 2017 global overview report, there are about 4.92 billion global mobile users in 2017 [34], and is predicted to move to three quarters of the world's population, by 2020 [35], therefore RSA algorithms needs to adapt to key generation techniques that not just offers the current strength but even more stronger keys which can't be cracked by quantum computers, however focus should be on doing all this within the computation power limits offered by smartphone and smart applications batteries. As the development of quantum computing gains momentum there is a huge question mark hanging on viability of RSA. Some cryptographers are unconvinced about quantum computing been a threat to current encryption tools assuming that it should be many years before they have to worry about quantum computing. Again the denial factor comes into play. Cryptographers are showing fewer signs of concern and expect that no real progress will be made in quantum crypto before 2031 [36], however, the Shor algorithm, a quantum step having the ability to factorize large numbers was used by an MIT physicist and electrical engineer, Isaac Chuang, in 2001 to factor the number 15, but he wasn't able to scale up his five-atom quantum computer system to factor anything more complicated [9]. Even though he wasn't able to have a functional quantum computer of the necessary size to crack RSA encryption yet, Chuangs experiment points out the threat that such a computer poses to cryptographic systems [9]. In line with this comes the news of the Ireland's top young scientist and technologist of 2017, Shane Curran, a 16 year old student at Terenure College, who anticipated the impact quantum computing will have on current cryptographic methods and created qCrypt, a quantum-encrypted data storage solution is resistant to attacks by quantum computers [37], [38].

6 Conclusion

Even though RSA is the most used cryptography algorithm today, it has certain limitations which need to be taken into consideration for RSA to continue to be the best and research has to be done into making RSA quantum resistant. There is a need now more than ever for studies to be conducted in the area of quantum encryption methods resistant to quantum computers as it will soon replace the current encryption systems. Development of qCrypt isn't enough, but it's a start. However, we need more research into quantum resistant encryption systems.

References

[1] Ponemon Institute, "2016 Cost of Data Breach Study: Global Analysis," Ponemon Institute, North Traverse, 2016.

[2] B. L. Jr., "Cybersecurity: CNBC.com," CNBC, 15 June 2016. [Online]. Available: http://www.cnbc.com/2016/06/14/cost-of-data-breaches-hits-4-million-on-average-ibm.html. [Accessed 22 March 2017].

[3] Ponemon Institute, "2013 Cost of Data Breach Study: Global Analysis," Ponemon Institute, North Traverse, 2013.

[4] Ponemon Institute, "2014 Cost of Data Breach Study: Global Analysis," Ponemon Institute, North Traverse, 2014.

[5] Ponemon Institute, "2015 Cost of Data Breach Study: Global Analysis," Ponemon Institute, North Traverse , 2015.

[6] G. C. Kessler, An Overview of Cryptography, Boca Raton: Auerbach Publications, 2017.

[7] N. Priya and M. Kannan, "Comparative Study of RSA and Probabilistic Encryption," International Journal Of Engineering And Computer Science, vol. 6, no. 1, pp. 19867 - 19871, January 2017.

[8] H. B. Pethe and S. R. Pande, "Comparative Study and Analysis of Cryptographic Algorithms," International Journal of Advance Research in Computer Science and Management Studies, vol. 5, no. 1, pp. 48-56, 1 January 2017.

[9] A. Nordrum, "Tech-Talk: IEEE Spectrum," IEEE Spectrum, 3 March 2016. [Online]. Available: http://spectrum.ieee.org/tech-talk/computing/hardware/encryptionbusting-quantum-computer-practices-factoring-in-scalable-fiveatom-experiment. [Accessed 19 March 2017].

[10] B. Steyn, "Essays: Doctrina.org," Doctrina.org, 26 May 2012. [Online]. Available: http://doctrina.org/How-RSA-Works-With-Examples.html. [Accessed 19 March 2017].

[11] A. Harrison, "Articles:Computerworld.com," Computerworld.com, 18 September 2000. [Online]. Available: http://www.computerworld.com/article/2588444/security0/rsa-encryption-patent-released.html. [Accessed 22 March 2017].

[12] E. Frenkel, "Articles: Slate.com," Slate.com, 3 June 2013. [Online]. Available: http://www.slate.com/articles/health_and_science/science/2013/06/online_credit_card_security_the_rsa_algorithm_prime_numbers_and_pierre_fermat.html. [Accessed 20 March 2017].

[13] S. Simpson, "www.laits.utexas.edu," University of Texas, 24 March 1997. [Online]. Available: http://www.laits.utexas.edu/~anorman/BUS.FOR/course.mat/SSim/algorithms.html. [Accessed 2017].

[14] S. Simpson, "www.laits.utexas.edu," The University of Texas, 1997. [Online]. Available: http://www.laits.utexas.edu/~anorman/BUS.FOR/course.mat/SSim/life.html. [Accessed 23 March 2017].

[15] C. Bradford, "Blog: StorageCraft.com," StorageCraft Technology Corporation, [Online]. Available: https://www.storagecraft.com/blog/5-common-encryption-algorithms/. [Accessed 23 March 2017].

[16] B. Darrow, "PointCloud: Fortune.com," 1 February 2017. [Online]. Available: http://fortune.com/2017/01/31/google-g-suite/. [Accessed 20 March 2017].

[17] E. Mendelson, "Review: PCMag.com," Ziff Davis, LLC. PCMag Digital Group, 28 February 2017. [Online]. Available: http://www.pcmag.com/review/352023/google-g-suite. [Accessed 20 March 2017].

[18] P. Higgins, "Deeplinks Blog: Electronic Frontier Foundation," Electronic Frontier Foundation, 28 August 2013. [Online]. Available: https://www.eff.org/deeplinks/2013/08/pushing-perfect-forward-secrecy-important-web-privacy-protection. [Accessed 23 March 2017].

[19] Google, "Help: Support.Google.com," Google, 2017. [Online]. Available: https://support.google.com/work/answer/6056693?hl=en&ref_topic=6055719. [Accessed 23 March 2017].

[20] M. Rouse, "Network Security: Searchsecurity.techtarget.com," Searchsecurity.techtarget.com, November 2014. [Online]. Available: http://searchsecurity.techtarget.com/definition/RSA. [Accessed 19 March 2017].

[21] S. McHenry, " Blogs: Security.googleblog.com," Google, 23 May 2013. [Online]. Available: https://security.googleblog.com/2013/05/changes-to-our-ssl-certificates.html. [Accessed 23 March 2017].

[22] Maxim Integrated Products, "Tutorials: Maximintegrated.com," Maxim Integrated Products, 25 May 2012. [Online]. Available: https://www.maximintegrated.com/en/app-notes/index.mvp/id/5421. [Accessed 24 March 2017].

[23] Gemalto, "Updates: Gemalto.com," Gemalto, 2016. [Online]. Available: http://data-protection-updates.gemalto.com/files/2017/04/IDPrime3811_Plug_and_Play_Smart_Cards_PB_EN_v2_SEP082016_web.pdf. [Accessed 24 March 2017].

[24] Smartjac Industries, "Index: Smartjac.biz," Smartjac Industries, [Online]. Available: http://www.smartjac.biz/index.php/component/eshop/identity-access-products/smart-cards/gemalto-idprime/idprime-piv-card-v1-55-128k-v2,-tri-interface-legacy-name-protiva-piv-card-v1-55-on-top-wl?Itemid=0. [Accessed 24 March 2017].

[25] V. Beal, "Term: Webopedia.com," QuinStreet Enterprise, [Online]. Available: http://www.webopedia.com/TERM/R/rsa_secure_id.html. [Accessed 24 March 2017].

[26] M. Arora, "Design: Embedded.com," AspenCore, 9 November 2011. [Online]. Available:http://www.embedded.com/design/safety-and-security/4230483/Understanding-the-security-framework-behind-RSA-SecurID. [Accessed 24 March 2017].

[27] S. D. Schoen, "www.loyalty.org," Loyalty.org, [Online]. Available: http://www.loyalty.org/~schoen/rsa/. [Accessed 22 March 2017].

[28] Wikipedia, "Wikipedia," Wikipedia, 29 March 2017. [Online]. Available: https://en.wikipedia.org/wiki/RSA_numbers. [Accessed 1 April 2017].

[29] Information Technology Laboratory, "Digital Signature Standard (DSS)," National Institute of Standards and Technology, Gaithersburg, 2013.

[30] T. Leek, "Questions: Security Stack Exchange.com," Stack Exchange Inc, 24 January 2014. [Online]. Available: https://security.stackexchange.com/questions/49280/cryptography-behind-chip-based-credit-cards-smart-cards. [Accessed 24 March 2017].

[31] S. Jessel, "World: News.bbc.co.uk," BBC, 25 February 2000.

[Online]. Available: http://news.bbc.co.uk/2/hi/europe/657135.stm. [Accessed 24 March 2017].

[32] D. Genkin, A. Shamir and E. Tromer, "RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis," in Advances in Cryptology – CRYPTO 2014, Santa Barbara, 2014.

[33] J. V, "Blog: Jscape.com," JSCAPE LLC, 2 August 2014. [Online]. Available: http://www.jscape.com/blog/bid/82975/Which-Works-Best-for-Encrypted-File-Transfers-RSA-or-DSA. [Accessed 24 March 2017].

[34] S. Kemp, "Blog: We Are Social Ltd.," We Are Social Ltd, 24 January 2017. [Online]. Available: https://wearesocial.com/blog/2017/01/digital-in-2017-global-overview. [Accessed 25 March 2017].

[35] Phys.org, "News: Phys.org," Phys.org, 27 February 2017. [Online]. Available: https://phys.org/news/2017-02-bn-mobile-users.html. [Accessed 24 March 2017].

[36] J. Buntinx, "News: The Merkle," 16 Februray 2017. [Online]. Available: https://themerkle.com/ai-and-quantum-computing-pose-no-threat-to-cryptography-experts-say/. [Accessed 25 March 2017].

[37] J. Young, "News: Themerkle.com," The Merkle, 17 January 2017. [Online]. Available: https://themerkle.com/irish-teen-introduces-new-encryption-system-resistant-to-quantum-computers/. [Accessed 24 March 2917].

[38] D. Gilbert, "Technology: Iibtimes.co.uk," IBTimes Co., Ltd. , 25 January 2017. [Online]. Available: http://www.ibtimes.co.uk/unbreakable-encryption-technology-created-by-16-year-old-schoolboy-1603024. [Accessed 24 March 2017].