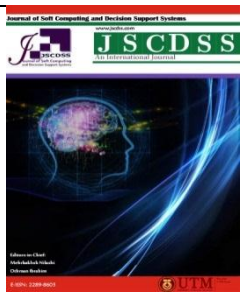
An International Journal
JSCDSS
http://www.jscdss.com
Vol.4 No.1 February 2017: 7-15
Article history:
Accepted 28 February 2017
Published online 28 February 2017

Journal of Soft Computing and Decision Support Systems



E-ISSN: 2289-8603

Encryption and Decryption Analysis of the RSA Digital Signature Based on MD5 and SHA Hash Functions Using Strong Prime

Abdelmajid Hassan Mansour [1,*]
[1] University of Jeddah, Faculty of Computers and Information Technology, Department of Information Technology, Khulais, Jeddah, Saudi Arabia, 21921

*** Corresponding author email address**: majidemam@gmail.com

Abstract

RSA digital signature is the most common public key crypto system that used widely on data security. The encryption and decryption time computation of the signature generation and verification is still a big problem an important issue that challenging the RSA security. This paper analyses the encryption and decryption time of the RSA Digital Signature based on the hash functions MD5, SHA-160, SHA-256, and SHA-512. The private key and public key of the RSA generated by using the "Strong prime", then compare it with the original RSA method. The main goal of the proposed scheme is to optimize and speed up the process of encrypting and decrypting time on a variable length of message, and different hash functions. This will overcome the problem of processing time and computational overheads of the RSA digital signature system.

Keywords: RSA digital signature, Private key, Public key, Encryption, Decryption, Strong prime, Hash function, Message digest.

1. Introduction

A digital signature is a cryptographic algorithm which includes the process of signature generation and signature verification. A signer uses the generation process to create a digital signature on the data, and the verifier verifies the authenticity of the signature by using the verification process. The private key is used to generate the signature and must remain secret, while the public key is on the verification process (Bhala et al., 2011). Digital signatures are widely used in various applications such as electronic commerce, banks, distributing software, and in detecting forgery or tampering. They are corresponds of handwritten signatures which can be transmitted within a computer network. Only the signer of the message can make the signature, and the other people can recognize easily as belonging to the signer. The digital signature has three types of services such as (Gola et al., 2014):

1.1 Authentication is the process of verifying the messages received is come from valid source.

1.2 Message integrity is process of authenticating the contents at the signature time and it did not altered during transfer.

1.3 Non-repudiation means the signer cannot claim they did not signed the message.

The digital signature provides an intermediary of integrity checking. This is done in order to provide assurance for the verifier that the data was in real was sent by the assumed entity (Ali, 2015). In the Digital signature verification they require the holder of the signature to have the private key for message signing and the public key for verification message of authenticity. The essential goal of the Digital signature is verifying that the message was not been altered during transit after it was signed and giving a confidence of sent by expected party to the receiver (Jafaar and Samsudin, 2010). Fig. 1 illustrates how the Digital Signature works from process of Signature Generation to Signature Verification.

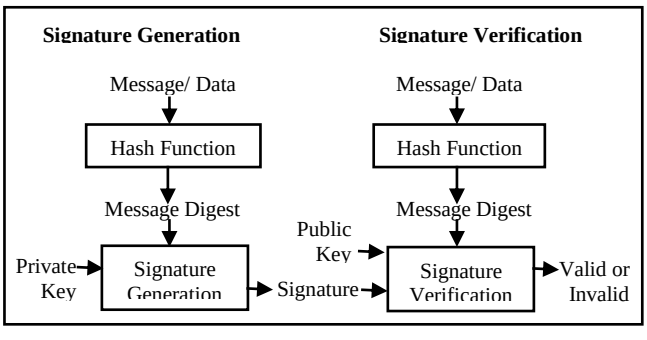


Fig. 1. Digital Signature Process

2. RSA Digital Signature

The RSA digital signature algorithm was developed by Ronald Rivest, Adi Shamir and Leonard Adelman at

Massachusetts Institute of Technology (MIT) in 1977. The RSA concept is depend on the big numbers of factorization which means that the largest sequence of numbers you have. They provide a strong security, due to its complexity and the use of large keys an adversary should not be able to break it by the factorization. RSA is used to encrypting and decrypting the data and also used for signing and/or verifying the data. The security of the RSA signature and encryption are partly dependent on the choosing of the hash function that is used to compute the signature (Ali, 2015). So that, the security assumption was depend on the complexities of factorizing a large composite integer n = p*q, which p and q are distinct large primes (Pon et al., 2005).

RSA is also known as asymmetric digital signature algorithm they uses a pair of keys, one of the keys which is used to sign the data that it can be verified with the other key only. RSA is based on one way function. The idea of RSA is that it is relatively the prime numbers can be easily multiplied but much more difficult to factorize. The multiplication process can be computed in polynomial time while factoring time can grow according to the size of the numbers. The RSA digital signature algorithm steps are shown as follows (Vijay et al., 2012):

2.1 Key Generation:

The following are the steps of key generation process:

2.1.1 Generate two large prime, p and q.
2.1.2 Calculate $n = p \times q$ and $\emptyset = (p-1) \times (q-1)$.
2.1.3 Select an integer e, where $1 < e < \emptyset$, and gcd $(e, \emptyset) = 1$.
2.1.4 Calculate d, that satisfying $1 < d < \emptyset$, where $e \times d \bmod \emptyset = 1$.
2.1.5 (e,n) are the public key and (d,n) are the private key.

2.2 Signature Generation:

The following are the steps of signature generation process:

2.2.1 Apply Hash function H(m) create message digest.
2.2.2 Use the private key d to calculate the signature $s = \mathrm{H}(m)^d mod\ n$.
2.2.3 The signature of the message m is s that will be sent with the message m to recipient.

2.3 Signature Verification:

The following are the steps of the signature verification process:

2.3.1 Using the public key e, and calculate $= \mathrm{s}^e mod\ n$.
2.3.2 Calculate the message digest of the signed message.
2.3.3 If the two message digests are identical, then the signature is valid.

2.4 Prime number:

A prime number is act as a positive integer number that is greater than 1 which their positive divisors integer is only 1 and itself (Menezes et al., 1996). A prime is defined as a positive integer number p that having just so two positive of divisors, namely 1 and p. An integer n is called composite integer if n > 1 and n is not prime. (The number 1 is considered not prime and not composite.) Thus, an integer n is composite if and only if it admits a nontrivial factorization n = ab, where a, b are integers, each strictly between 1 and n (Crandall and Pomerance, 2000).

2.5 Definition:

An integer $p \geq 2$ is called to be a prime if its positive divisors are only 1 and p. otherwise, p is called composite (Menezes et al., 1996).

2.6 Definition:

A prime number p is said to be a strong prime if the integers r, s, and t exist such that satisfying the following three conditions are (Menezes et al., 1996):

2.6.1 $p-1$ has a large prime factor, denoted r.
2.6.2 $p+1$ has a large prime factor, denoted s.
2.6.3 $r-1$ has a large prime factor, denoted t.

3. Related work

RSA digital signature algorithm is the most popular public key cryptography system that used widely in an internet Application, there are several studies and researches have been proposed on RSA for efficiency of encryption and decryption time computation. Gola et al. (2014) showed from the conclusion that the modified RSA digital signature technique provides the security during data transfer as compared with the old RSA digital signature scheme. They satisfied and improved the security and performance of digital signature. Vijay et al. (2012) concluded that the new variant of digital signature algorithm which based on the prime factorization and xth root is secure enough versus various attacks, and the performance of it comparatively equivalent to the most of the digital signature algorithms that are depend on multiple hard problems. However, the proposed methodology is not secure against Chosen-message attack like RSADSA. Meng and Zheng (2015) concluded by analyzing the short exponent of the RSA with a small parameter, they found that the birthday attack against short exponent may cause the RSA variant insecure, they show that if $e > \sqrt{k}(p+q)$, then N can be factorized in both time and space complexity of $\bar{O}(\sqrt{k})$. Sarkar and Maitra (2010) shown from conclusion that RSA is weak when there are available two encryption exponents for the same modulus and the unknown decryption exponents of the RSA are less than $N^{0.416}$. They achieved further improvements when some amount of MSBs of the decryption exponents is identical (but unknown). From the conclusion of Sarkar and Maitra

An International Journal JSCDSS E-ISSN: 2289-8603

(2010) proved that if n are of many decryption exponents that was used with the same RSA modulus N, then RSA becomes insecure when $d_i < N^{\frac{3n-1}{4n+n}}$ for each $i, 1 \leq i \leq n,$ and $n \geq 2$. Varalakshmi et al. (2015) proposed work that uses four large prime numbers instead of two prime and they proved that the proposed algorithm is highly secure and not easily breakable as compared to RSA and the modified RSA algorithm. From the result is the key generation time of ESRKGS is so higher than the traditional RSA. The higher generation time of the key in turn increases the required time to break the system, and the time of encryption and decryption of ESRKGS is higher than RSA but significantly less than the other modified RSA that uses four primes. Thus there is not much overhead or burden on the system. Pallipamu et al. (2014) were concluded that the RSA digital signature using Algorithm for Secure Hashing-160 (ASH160) consumes less CPU time in the encryption process but a little bit more time in decryption process. While in the security point of view the ASH160 is stronger than the SHA1 and RIPEMD160 algorithms. Zhu and Li (2008) concluded the advance solution to the safety problems related to the technology of digital signature in E-Commerce they offering identity certification to those who take part in E-Commerce activities, which prevents all kinds of potential safety hazards. The study and application of the digital signature technology in China has a disparity with international level. Mahto et al. (2016) concluded that ECC outperforms in terms of operational efficiency and security over RSA. They suggested that ECC may be most favourable for memory constraints devices like Smart-Phone, Palmtop PC. For the security analyses strength of ECC and RSA over input data of 8 bits, 64 bits, 256 bits of using random keys that depend on the NIST recommendation. Okeyinka et al. (2015) observed that the RSA is superior to the Elgamal on the overall assessment, it is not as efficient as Elgamal when the rate of data decryption is considered. It is therefore fathomable that a platform that will hybridize both approaches may yield a more efficient technique than either the Elgamal or RSA algorithm. Hence efforts at designing a hybrid algorithm of these two techniques are strongly recommended as candidates for further research work.

4. Proposed Scheme

RSA digital signature is a public key cryptosystem, the security and efficiency of RSA digital signature algorithm is based on the use of a large prime number, and the difficulty of analyzing the prime numbers for Encryption and decryption on the process of signature generation and verification. There are several studies and efforts have been done in past to solve the prime factorization problem and the encryption and decryption computation time of the signature generation and verification process. In this paper we analyze the computation time of encryption and decryption process of the RSA Digital Signature based on the hash functions MD5, SHA-160, SHA-256, and SHA-512. Using the concept of a "Strong Prime" numbers, state that $p = 2p_0 + 1$, $q = 2q_0 + 1$ where p_0 and q_0 are prime numbers, to generate the private and public key, and compare it with the original method of key generation of the RSA Digital Signature using different message length of "64, 256, 512, 768,1024, 1536, 1728, and 2048 bytes". In order to show and find out the variations analysis of the encryption and decryption time computation, and getting a good results of the improvement that optimize the key generation strategy, and overcomes the processing time & computational overheads of the RSA system. The proposed methodology of RSA digital signature moves throw three phases, as follows:

4.1 Key generation:

In this phase, the signer generates the private & public key according to the following steps:

4.1.1 Generate two large random primes p_0 and q_0.
4.1.2 Calculate $p = 2p_0 + 1$, $q = 2q_0 + 1$.
4.1.3 Calculate $n = p \times q$ and $\emptyset = (p-1) \times (q-1)$.
4.1.4 Select an integer e, where $1 < e < \emptyset$, and gcd $(e, \emptyset) = 1$.
4.1.5 Calculate d, that satisfying $1 < d < \emptyset$, where $e \times d \bmod \emptyset = 1$.
4.1.6 (e,n) are the public key and (d,n) are the private key.

4.2 Signature Generation:

The signature generation is calculated through the following steps:

4.2.1 Apply Hash function H(m) create message digest.
4.2.2 Use the private key d to calculate the signature $s = H(m)^d mod\ n$.
4.2.3 The signature of the message m is s that will be sent with the message m to recipient.

4.3 Signature Verification:

The Signature verification is done through the following steps:

4.3.1 Obtains the public key (n, e).
4.3.2 Receives the message (m) and its signature (s) from the signer.
4.3.3 Using the public key e, and calculate $= s^e mod\ n$.
4.3.4 Calculate the message digest of the signed message.
4.3.5 If the two message digests are identical, then the signature is valid.

5. Results

The proposed scheme was tested and analyzed using the "Strong Prime" for generating the private key and public key on a different variable message length of 64, 256, 512, 768, 1024, 1536, 1728, 2048 bytes, using different hash functions of "MD5, SHA-160, SHA-256, SHA-512, compared with the original RSA digital Signature algorithm, and the analysis done by using different statistical method. The analysis showing the variation of

An International Journal JSCDSS E-ISSN: 2289-8603

how much time it taken by using the concept of "Strong Prime" for generating the private key and public key compared with the original RSA algorithm to encrypt and decrypt the different message lengths using different hash functions of MD5, SHA-160, SHA-256, SHA-512. The mean time of encryption by the original RSA algorithm record a little time variation from small message size up to large message size compared with the use of strong prime key generation. But it can see that the time encryption using the "Strong Prime" is slightly less than that of original RSA keys for the message size larger than 1024 bytes. Tables 1-7 and Figs. 2-12 present the results of analysis of the proposed scheme.

Table 1
One-Sample Statistics for Encryption

	N	Mean	Std. Deviation	Std. Error Mean
Message Length	64	4.500000000	2.3094010768	.2886751346
Hash Function	64	10.863850344	18.7642212053	2.3455276507

Table 2
Paired Samples Correlations for Encryption

		N	Correlation	Sig.
Pair 1	Message Length & Hash Function	64	.372	.003

Table 3
Cross tab Case Processing Summary for Encryption

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Message Length * Hash Function	64	100.0%	0	.0%	64	100.0%

Table 4
One-Sample Statistics for Decryption

	N	Mean	Std. Deviation	Std. Error Mean
Message Length	64	4.500000000	2.3094010768	.2886751346
Hash Function	64	.031610250	.0250026318	.0031253290

Table 5
Paired Samples Correlations for Decryption

		N	Correlation	Sig.
Pair 1	Message Length & Hash Function	64	.963	.000

Table 6
Case Processing Summary for Decryption

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Message Length * Hash Function	64	100.0%	0	.0%	64	100.0%

Table 7
One-Sample Test for Decryption

	Test Value = 0					
			Sig.		95% Confidence Interval of the Difference	
	t	df	(2-tailed)	Mean Difference	Lower	Upper
Message Length	15.588	63	.000	4.5000000000	3.923128775	5.076871225
Hash Function	10.114	63	.000	.0316102500	.025364778	.037855722

An International Journal JSCDSS E-ISSN: 2289-8603

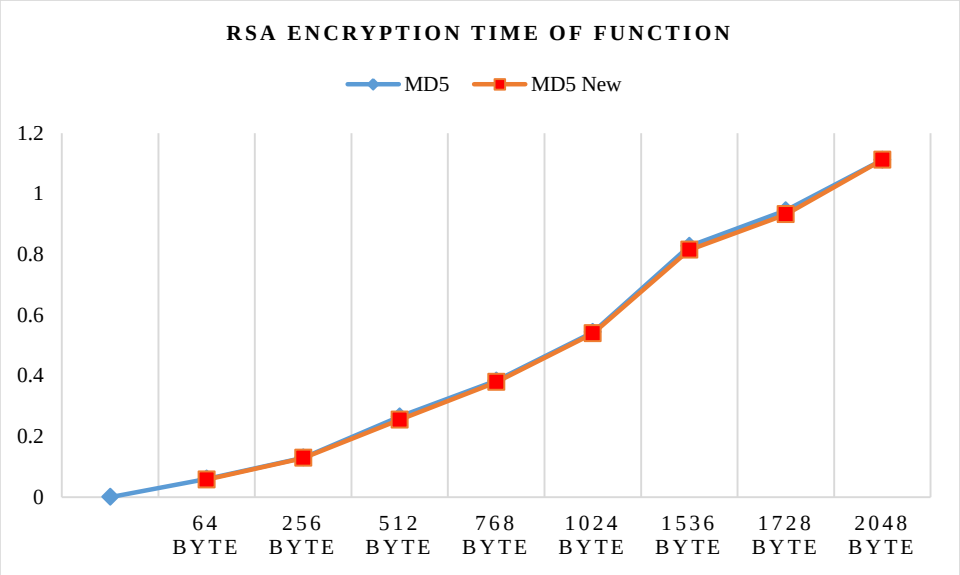


Fig. 2. RSA Encryption Time (in seconds) with MD5 Hash Function

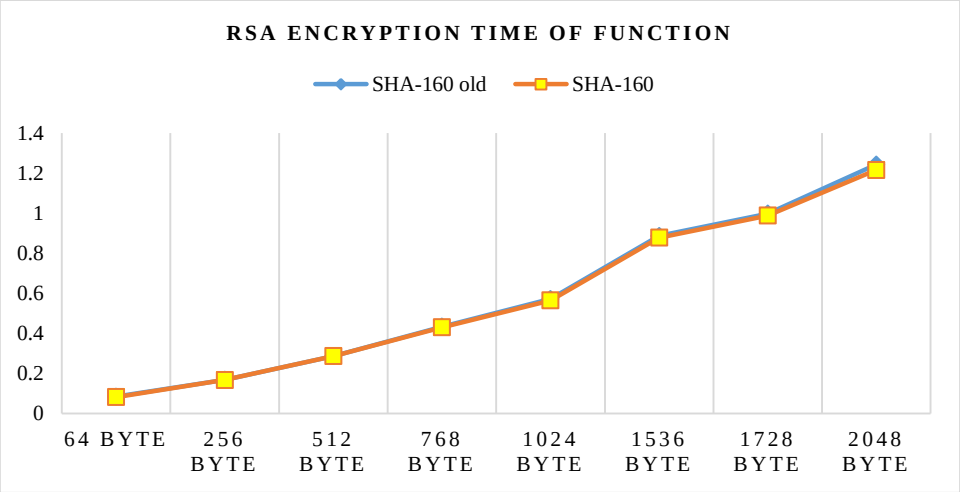


Fig. 3. RSA Encryption Time (in seconds) with SHA-160 Hash Function

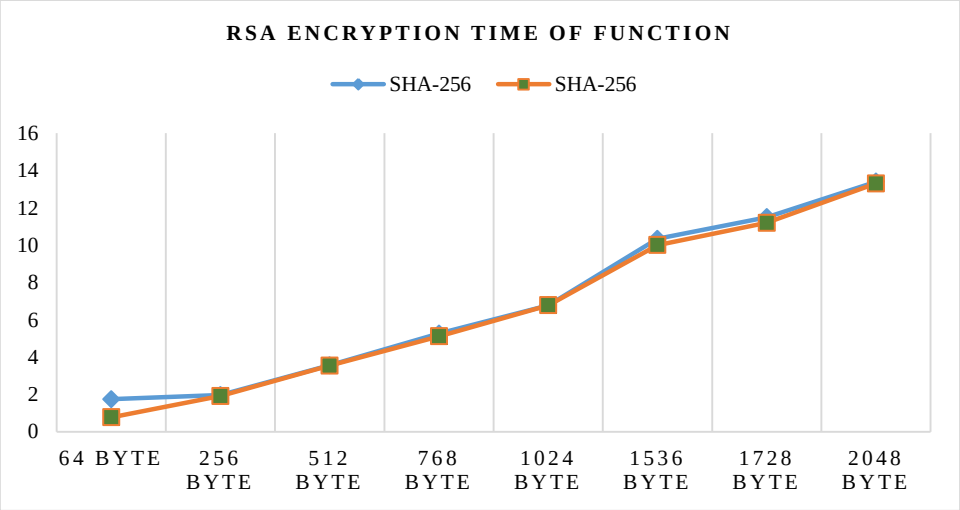


Fig. 4. RSA Encryption Time (in seconds) with SHA-256 Hash Function

An International Journal
JSCDSS
E-ISSN: 2289-8603

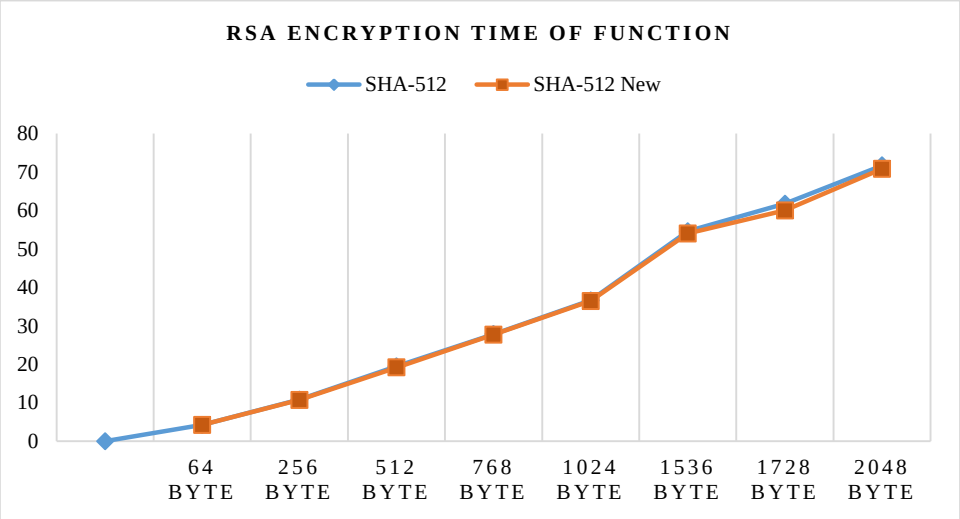


Fig. 5. RSA Encryption Time (in seconds) with SHA-512 Hash Function

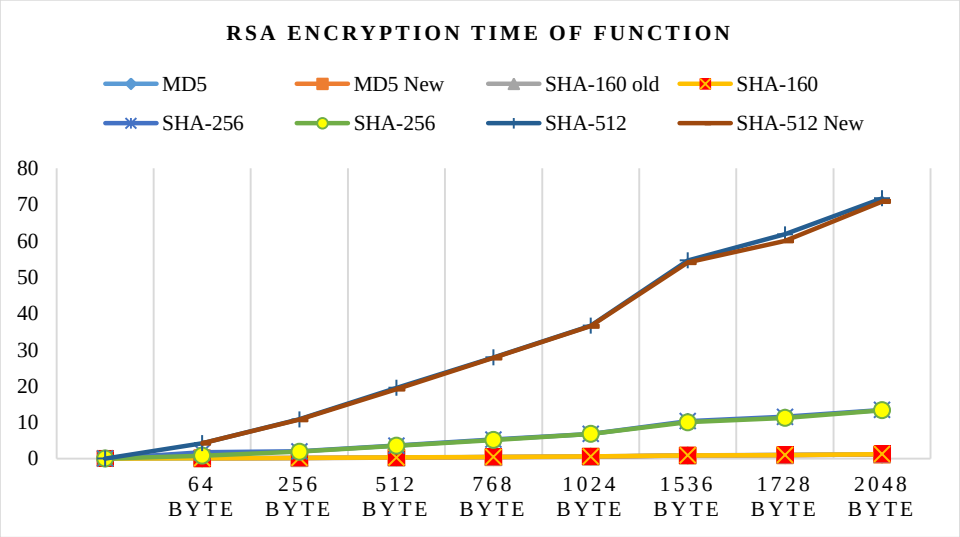


Fig. 6. RSA Encryption Time (in seconds) with all Hash Function

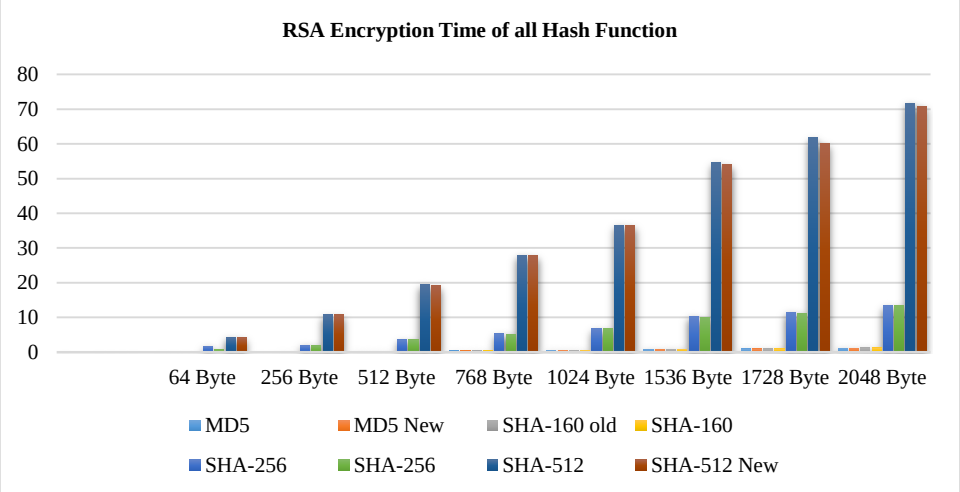


Fig. 7. RSA Encryption Time (in seconds) with all Hash Function

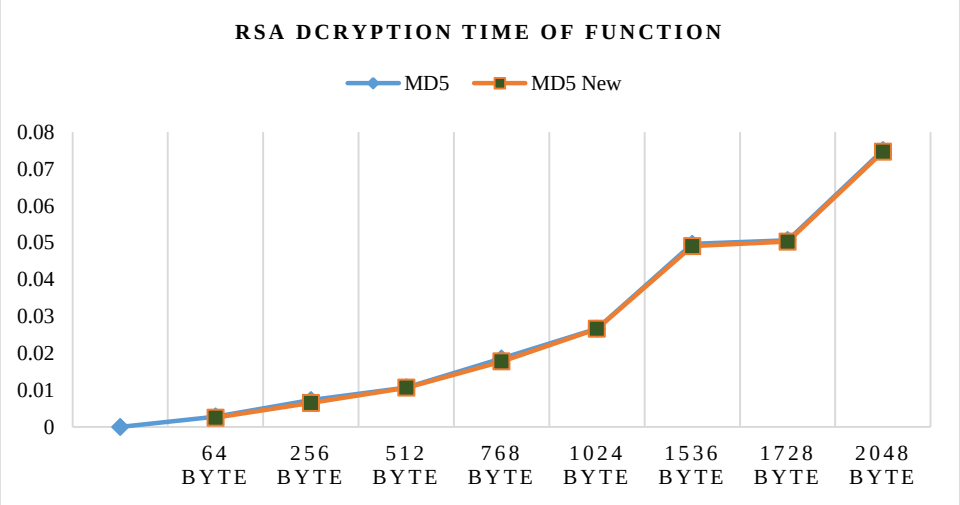


Fig. 8. RSA Decryption Time (in seconds) with MD5 Hash Function

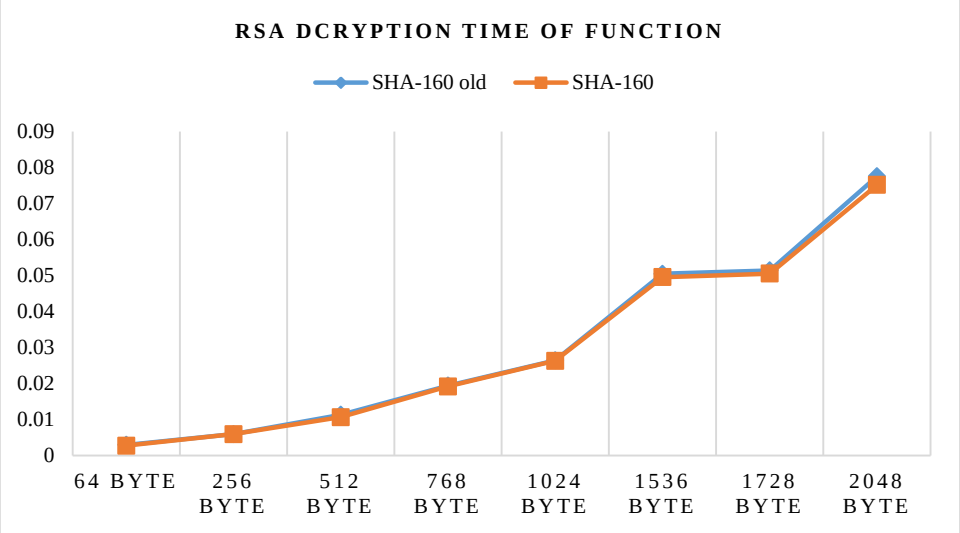


Fig. 9. RSA Decryption Time (in seconds) with SHA-160 Hash Function

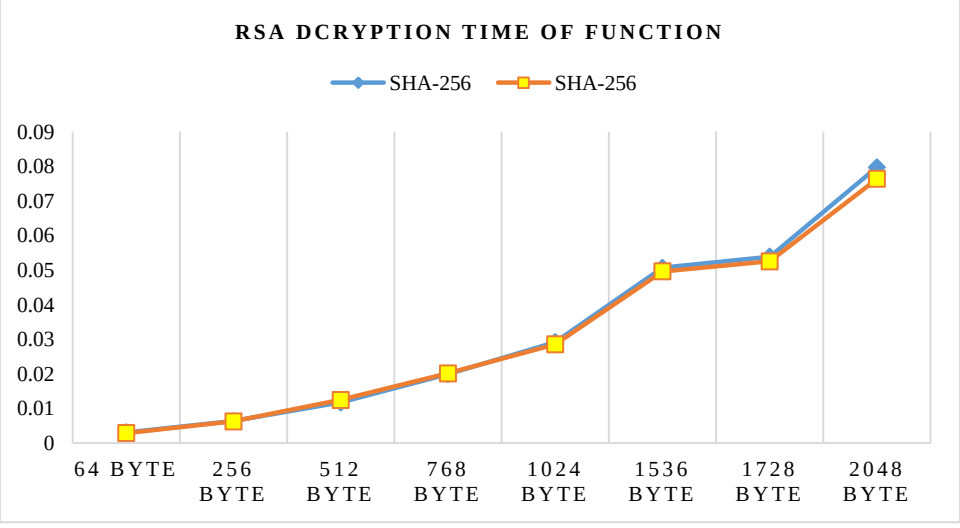


Fig. 10. RSA Decryption Time (in seconds) with SHA-256 Hash Function

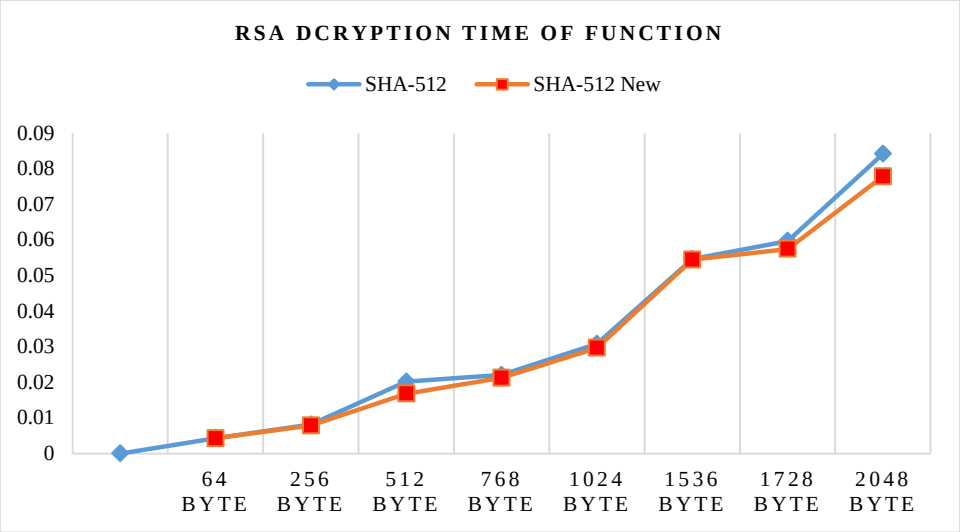


Fig. 11. RSA Decryption Time (in seconds) with SHA-512 Hash Function

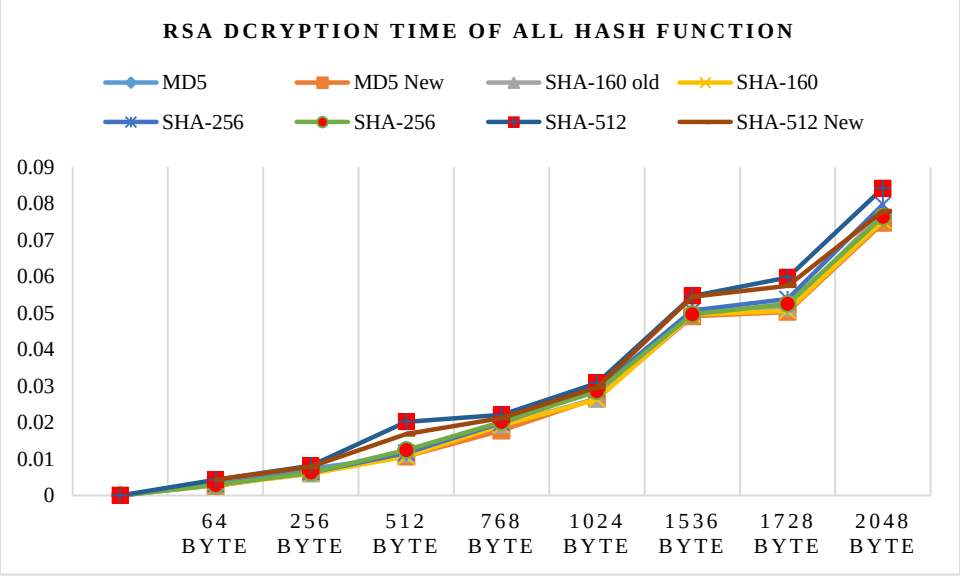


Fig. 12. RSA Decryption Time (in seconds) with All Hash Function

6. Conclusion

The proposed work has been implemented and the results are analyzed using the "Strong Prime" for generating the private key and public key on a different variable message length of 64, 256, 512, 768, 1024, 1536, 1728, 2048 byte, using different hash functions of "MD5, SHA-160, SHA-256, SHA-512, compared with the original RSA digital Signature algorithm, using different statistical method. From The analysis of experimental results obtained showed that, the encryption time taken for signature generation by using the concept of "Strong Prime" key generation is significantly less for small message size up to large message size compared with the use of original RSA key generation, in addition to increasing time on SHA-256 and SHA-512 hash function. Also the decryption time of using the "Strong Prime" is faster than that of the original RSA key generation for the message size larger than 768 byte. So that leads to the improvement and efficiency of RSA digital signature. And there is no much overhead the system.

References

Bhala, A. S., Kshirsagar, V. P., Nagori, M. B., & Deshmukh, M. K. (2011). Performance Comparison of Elliptical Curve and RSA Digital Signature on ARM7. *In Proceedings of International Conference on Information and Network Technology (IPCSIT), Singapore. (4), (2011), pp. 58-62.*

Gola, K. K., Gupta, G., & Iqbal, Z. (2014). Modified RSA Digital Signature Scheme for Data Confidentiality. *International Journal of Computer Applications, 106 (13), (November 2014), pp. 13-16.*

Ali, A. I. (2015). COMPARISON AND EVALUATION OF DIGITAL SIGNATURE SCHEMES EMPLOYED IN NDN

An International Journal JSCDSS E-ISSN: 2289-8603

NETWORK. *International Journal of Embedded systems and Applications (IJESA). 5(2), (June 2015), p. 15-29.*

Jaafar, A. M. & Samsudin, A. (2010). Visual Digital Signature Scheme: A New Approach. *IAENG International Journal of Computer Science, 37(4).*

Pon, S. E., Lu, E. H., & Jeng, A. B. (2005). Meta-He digital signatures based on factoring and discrete logarithms. *Applied Mathematics and Computation 165, www.elsevier.com/locate/amc, pp. 171–176.*

Vijay, A., Trikha, P., & Madhur K. (2012). A New Variant of RSA Digital Signature. *International Journal of Advanced Research in Computer Science and Software Engineering, 2(10), (October 2012), pp. 366-371.*

Menezes, A. J., Oorschot, P. C. V., & Vanstone, S. A. (1996). *HANDBOOK of APPLIED CRYPTOGRAPHY.*

Crandall, R. (2000). Prime Numbers a Computational Perspective, Carl Pomerance, Second Edition, ISBN-10: 0-387-25282-7, springeronline.

Meng, X., &Zheng, X. (2015). Cryptanalysis of RSA with a small parameter revisited. *Information Processing Letters 115, Elsevier, June 2015, p. 858–862.*

Sarkar, S., &Maitra, S. (2010). Cryptanalysis of RSA with two decryption exponents. *Information Processing Letters 110, Elsevier, (December 2010), pp. 178–181.*

Sarkar, S., &Maitra, S. (2010). Cryptanalysis of RSA with more than one decryption exponent. *Information Processing Letters 110, Elsevier, (March 2010), pp. 336–340.*

Thangavel, M., Varalakshmi, M., Murrali, M., & Nithya, K. (2015). An Enhanced and Secured RSA Key Generation Scheme (ESRKGS). *Journal of information security and applications 20, www.elsevier.com/locate/jisa, pp. 3-10.*

Pallipamu, V. R., Reddy K., T., & Varma P. S. (2014). Design of RSA Digital Signature Scheme Using ANovel Cryptographic Hash Algorithm. *International Journal of Emerging Technology and Advanced Engineering, 4(6), (June 2014), pp. 609-612.*

Zhu, H., & Li, D. (2008). Research on Digital Signature in Electronic Commerce. In *Proceedings of the International Multi Conference of Engineers and Computer Scientists (IMECS), 19-21 March, (I), Hong Kong. Retrieved from http://www.iaeng.org/publication/IMECS2008.*

Mahto, D.,Khan, D. A., & Yadav, D. K. (2016). Security Analysis of Elliptic Curve Cryptography and RSA. *In Proceedings of the World Congress on Engineering (WCE), June 29 - July 1, (I), London, U.K. Retrieved from http://www.iaeng.org/publication/WCE2016.*

Okeyinka, A. E. (2015). Computational Speeds Analysis of RSA and ElGamal Algorithms on Text Data. *In Proceedings of the World Congress on Engineering and Computer Science (WCECS), October 21-23, (1), San Francisco, USA. Retrieved from http://www.iaeng.org/publication/WCECS2015.*

Author Biographies

Dr. Abdelmajid Hassan Mansour Emam. (Saraf Omra, 1977), Ph.D in Information Security, Alneelain University, Faculty of Computer Science and Information Technology, Khartoum, Sudan.

Current Address: Department of Computers and Information Technology, University of Jeddah, Faculty of Computers and Information Technology, khulais, Jeddah, Saudi Arabia.

Permanent Address: Department of Information Technology, Faculty of computer Science and Information Technology, Alneelain University, Khartoum, Sudan, E-mail: majidemam@gmail.com

An International Journal JSCDSS E-ISSN: 2289-8603