Technoarete Transactions on Advances in Computer Applications (TTACA)
Vol-2, Issue-1, March 2023
e-ISSN: 2583-3472

A Study on Digital Signatures with Privacy Factor

Omkar Pattnaik [1*], Lopamudra Bisoyi [2], Sasmita Pani [3], A.S.Srinivas [4], Priti Rai [5], Ashutosh Sahoo [6]

[1, 3] Assistant Professor, Computer Science and Engineering, Government College of Engineering, BPUT, Keonjhar, Odisha, India
[2, 4, 5, 6] Final Year Student, Computer Science and Engineering, Government College of Engineering, BPUT, Keonjhar, Odisha, India
*Corresponding Author Email: omkar29in@gmail.com

Abstract

The safety, authenticity, and integrity of different electronic mechanisms, including e-government, online education, e-commerce, and electronic voting, are essential to their success. The transmitting of information within people and end viewers are very much essential now a days. To meet all these requirements, sensitive data should be digitally signed by the individual who sent it and absolutely confirmed by the person who is to receive it, as digital signature methods are essentially difficult cryptographic techniques which form the message in plain text format. The standard of functionality of these electronic services varies depending on various factors like key size, complexity of computation, privacy criteria, specific to the application variations, etc. In order to obtain the best outcomes, we have carefully reviewed the standard digital signature schemes in this paper.

Keywords

Authenticity, Digital Signature, Integrity, Public Key etc.

INTRODUCTION

In current scenario, various kinds of data are transferred across the internet containing some of the information that is highly confidential, which needs a high security. Various techniques and algorithms are used to maintain security of the data from third party. This is known as Cryptography, that is the branch of cryptology, that deals with the designing of algorithms for encryption and decryption. A Digital Signature is a significant type of authentication using a public-key cryptographic system. Digital signatures should not be jumbled with an Electronic Document, that is a Digital Certificate containing digital signatures of proceeding Certifying Authority. It combines a public key and an identity key that is used for verifying that the public key belongs to a specific individual or entity [1].

Digital Signature is one of the most important tools for the implementation of secure and truthful sign. Communications between partners is a significant issue that can not be secured by the traditional physical method of signature. Hence, we are using digital signature that provides appropriate background for secure communication using various schemes. Digital signature increases efficiency, security, services along with signing and verification capabilities. It improves the group working and company security maintenance using cryptography [2]. Physical signature can be forged easily whereas the digital signature is a full-proof method. Realizing the importance and necessity of digital signature, numerous governments have passed laws to empower the utilization of digitally signed documents rather than paper documents.

In today's world digital signature are implemented in most of the fields such as government, health care, manufacturing, financial services, and cryptocurrency [3]. While talking about security in digital signature, the CIA triad is one of the most important among them. CIA stands for confidentiality, integrity, and availability. Integrity is maintained when there is no data corruption and availability means that the data should be readily available to users but maintaining confidentiality in digital signature is tiresome [4] [5]. To ensure confidentiality we can encrypt the entire message using the recipient's public key. Since public-key cryptography requires rigorous computations, it is necessary to speed up these computations by using either efficient software algorithms or special purpose hardware [6] [7].

Different approaches like RSA algorithm, MD-5, SHA are used to provide security in digital signature [8]. In digital signature computation two techniques are used, those are Symmetric key Cryptosystem and Public key Cryptosystem [9] [10]. In symmetric key system, a secret key is used that is known only to the sender and the proposed receiver. Due to increase in number of user pairs, it becomes difficult in generation, distribution, signing, verification, and management of the key pairs [11] [12].

The remainder of this paper is organized as follows. In Section 2, Literature Survey is elaborated in tabular form**.** Section 3 provides an idea on background of digital signature working technique. Section 4 describes the different digital signature privacy scheme. Section 5 includes conclusion and future work.

e-ISSN: 2583-3472

LITERATURE SURVEY ON DIGITAL SIGNATURE SCHEMES

SL.NO	NAME	AUTHOR	PUBLISHER	SUMMARY
1	A comprehensive study on digital signature	J. Chandrashekhara, Anu V B, Prabhavati H, Ramya B R	**IJIRCST, 2021**	In cryptographic protocols, Digital signature techniques are generally used to provide authentication, delivery and agreement authenticated key. It provides the most secure data during online transaction. Apart from non-repudiation, other factors like cost and time-efficiency, imposing industry standards, flexibility etc had also been taken into consideration.
2	Digital signature scheme for information non-repudiation in blockchain: a state of art review.	Weidong Fang, Wei Chen, Jun Pei, Weiwei Gao, Guohui Wang	**Springer, 2020**	A digital signature schemes are an operative approach to accomplish non-repudiation. As one of the most promising technologies, Blockchain is widely in use. The features of the digital signature and blockchain is to promise non-repudiation of the information.
3	The study of digital signature authentication process	Unnati Patel, Ashaben Patel, Falguni Suthar	**ISSN, 2019**	With the advancement of internet, digital signature becomes gradually more important for security because of its integrity and privacy factors. Digital signature schemes promise three properties information security. Approaches of digital signature affixed by a single user have been defined and used widely.
4	Security system analysis in combination method: RSA encryption and digital signature Algorithm.	Farah Jihan Aufa, Endroyono, Achman Affandi	**IEEE 2018**	Researchers have combined RSA-1024 with DSA-512 since it has a rapid computation time. This combined method can encrypt messages as well as provide digital signatures.
5	Analysis of digital signature algorithm for authentication and privacy of digital data	Dimple Bansal, Manish Sharma, Ayushi Mishra	**IJCA,2017**	The author described how hash has a role in secure digital signature and described how authenticity is provided to digital data using digital signature. Also proposed idea about various DSA like 'Edward curve DSA, DSA based on x^{th} root problem, and modified ElGammal over RSA.
6	A new e A new efficient digital signature algorithm based on block cipher	Mr Prasun Kumar Mitra, Mr Debashis Hati, Mr Partha Haldar	**IJOURNALS, 2016**	The author has determined the technique which has least time complexity for the creation of digital signature. Some algorithms are also discussed based on block cipher and the algorithm are compared based on least execution time. **MATLAB** is used as a tool in this experimental study
7	An Introduction to digital signature scheme	Mehram Alidoost Nia, Ali Sajedi, argo Jamshidpey	**arXiv, 2014**	The author has given comparing view on different signature scheme to optimize signing procedure. Different schemes like Batch, forward-secure, Blind and Proxy scheme are discussed and compared based on security, verification, difficulty, and efficiency.

SL.NO	NAME	AUTHOR	PUBLISHER	SUMMARY
8	Research on digital Signature based on Digital Certificate	Yong Huang, Fugui Chen, Peixin Qu	**SCIRES,2014**	The objective of the paper is how to avoid illegal tampering and trading each-others identity using digital signature and ensure five major concern like confidentiality, integrity, authenticity, availability, and non-repudiation.
9	Design and Implementation of Digital Signature	K. Ramya, K. Suganya	**IJERT, 2013**	This paper proposes the algorithm of Digital signature and has also given a brief idea about supported algorithms like RSA and hashing algorithms.
10	Robust RSA for Digital Signature	Mr. Virendra Kumar, Mr. Puran Krishen Koul	**IJCSI, 2011**	The whole algorithm with each step is described here with additional challenges. The RSA algorithm suffers from Multiplicative Property, Integer Factorization. The failure of RSA algorithm means, the imitating of the digital signatures of a Certifying Authority could be computationally viable. This would result in the fake digital signature certificate generation, thus defeating the actual purpose of the employment of certifying authorities in public rejection of E-commerce.

DIGITAL SIGNATURE BACKGROUND

Digital Signature

The signer to denyigital signatures are playing an important role is internet application in business transaction, electronic mail etc. Digital signature makes it impossible for sender to disagree about signing the data. This can also be referred as maintaining non-repudition [13]. The basic idea about implementing digital signature of documents is not to veil what a message declares but somewhat to verify that, it is originated from a specific sender [14].

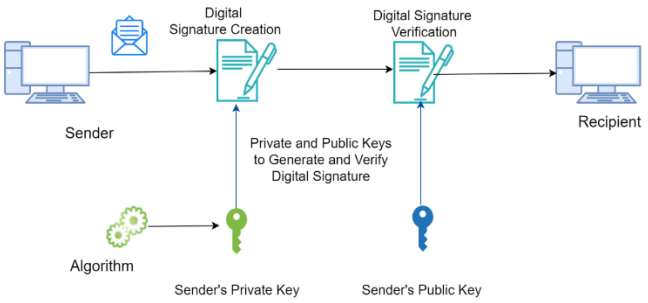

Figure 1. Model of Digital Signature [15]

Digital Signature is constructed on asymmetric key cryptography, which is primarily a mathematical application over the digitally signed document to certify its validity and integrity to its operators [16] [17]. It is also used in detection of reliability of the signed document. A Digital Signature should provide CIA (Confidentiality, Integrity, and Authentication) [15]. Digital signature algorithm comprises of Key Generation, Signature Generation and Signature Verification algorithm [18].

Process of Digital Signature

Key Generation

The key generation algorithm uniformly chooses a private key from a set of probable private keys [19] [3].

1. Let us assume a large prime ‘m’.
2. And ‘n’ be the prime divisor, such that (m - 1) mod n = 0.
3. An arbitrary integer ‘i’ is selected that (1< i < n) and (i * n) mod m = 1 as well as
   i = h {(m – 1) / n} mod m.
4. Select a private key ‘x’ such that 0<x<q.
5. Compute public key by using the formula $y = i^x \bmod p$.
6. Private key package = [m, n, i, x].
7. Public key package = [m, n, i, y].
8. Generate the hash ‘h’ of the message using Hash function [20].

Signature Generation

In signing algorithm, a signing key is used to produce a signature over raw data.

1. An arbitrary integer ‘k’ is taken, where 0 < k < q.
2. We can compute $a = \{(i^k \bmod m) \bmod n\}$
3. Compute $b = \{k^{-1} (h + x * a) \bmod n\}$
4. Hence {a, b} = Digital Signature [3].

Signature Verification

A signature can be validated by a party who has no knowledge of the signing key.

1. A verification component ‘V’ has three parameters that are: w, z_1, z_2.
2. Compute w from (b * w) mod n = 1.

e-ISSN: 2583-3472

3. Calculate z1, using z1 = (h * w) mod n
4. Calculate z2, using z2 = (a * w) mod n
5. Now V = [{(i^{u1}. y^{u2}) mod m} mod n]
6. The signature is verified if and only if V = = a [21].

Hash function

Hash function renovates a large integer length into a small, fixed length variable. In simple language we can say that hash function maps a large number or a string into a usable small integer for the index in the hash table. The output of hash function is referred as 'Message Digest' [22]. Hash function advantages in minimizing computation requirements as the signature has short and fixed length hash, which moreover increases the security level of the signature [23].

Properties of hash function

a. Collision-free.
b. Puzzle friendly.
c. Guessing input from the output is difficult.

Secure Hash Algorithm (SHA)

It is the hash functions used as a Government Standard and has been promoted by the National Institute of Standard and Technology (NIST). The successors are SHA-1, SHA-2, SHA-3 [24]. Every piece of data generates a unique hash value that is systematically unmatchable with any other piece of data [25].

Message Digest (MD)

This algorithm is developed by Ronald Rivest in the year 1989. It is used to deliver a hash function that is secured and used for a processor of 8-bits.

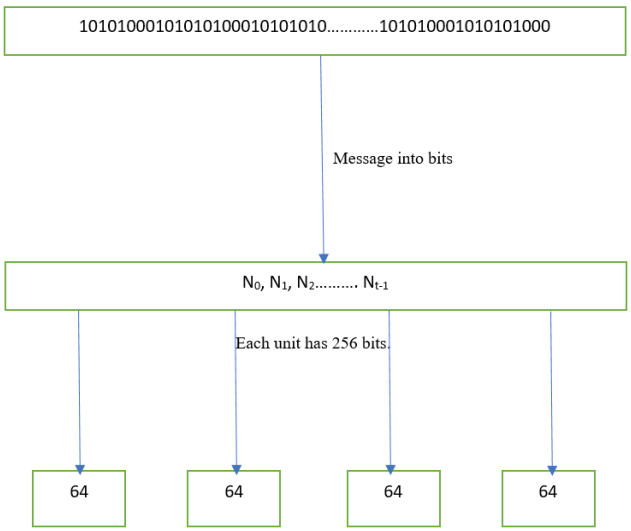

Figure 2. The MD5 Algorithm [26]

Currently message authentication process is playing a vital role in various applications such as Internet protocol (IP) related works as well as network management. Distinctive Digital Signature Schemes, have some performance overhead, which is often hefty to function with. Thus, we need to concentrate on the message-authentication built on shared secret key, which is ideally combined with the hash function [14].

Table 1. Comparison of different hashing algorithm

Hashing Algorithm	Input (in bits)	Output (in bits)
SHA-1	160	40
SHA-256	256	64
SHA-512	512	128
MD 5	128	32

DIGITAL SIGNATURE PRIVACY SCHEME

Initially a key pair is generated consisting of public key and private key of the sender. That public key is then sent to the recipient using any reliable mechanism which is not a secret necessarily. The private key is used for aligning and encryption by the sender. Then for verification process, the receiver uses the public key that is provided by the sender. Generally, the sender provides the data to the hash function which in return produces a hash value. Hash value and private key is provided to the signing algorithm, then the parameters of signature are generated [27] [28]. The signature is then appended to the data and send to the receiver, then the digital signature is verified using the verification key or public key. Then hash value is generated and used for the creation of verification parameter. The verification parameter is compared to the signature parameter and hence decided whether the signature is authentic or not. If the value is same, then it is acceptable otherwise rejected [29].

Privacy Scheme

In the current digitally signed documents, there is no provision for maintaining privacy. Anyone can view the document although they cannot modify it. Privacy can be maintained using cryptographic techniques like AES, RSA, Diffie-Hellman algorithms. Blockchain can also act as a privacy maintaining technique [30].

RSA (Rivest, Shamir, Adleman)

RSA is currently in wide use in various platforms. We can demonstrate RSA using sender and receiver. It is developed by Ron Rivest, Adi Shamir, and Len Adleman. This algorithm is used for public-key cryptography [31]. But there are also some challenges in RSA, like multiplicative property, integer factorization [32] [33]. RSA protect the data from pollution attack as well as eavesdropping attack by indicating the odds of attacker reading the original messages and imitating a effective signature for an irrelevant random packet are both unimportant purposes of Security Parameters [34]. The failure of RSA algorithm means, the imitating of the digital signatures of a Certifying Authority could be computationally viable. This would result in the fake digital signature certificate generation, thus defeating the actual purpose of the employment of certifying authorities in public rejection of E- commerce [35] [36]. RSA not only encrypt and decrypt data but also sign and verify the data packets. It does not dictate the use of a specific hash function therefore

e-ISSN: 2583-3472

the security is partially dependent on choice of hash function that is used for the computation of the signature [37].

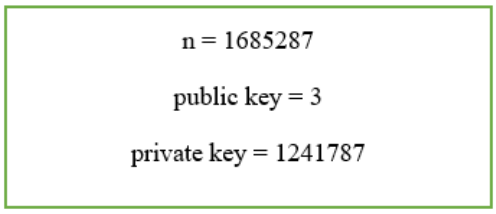

Figure 3. Key used in RSA. [38]

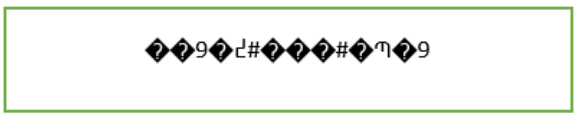

Figure 4. Result of decryption. [38]

Here is a simple example of RSA functioning using different keys in fig-3 and if we try to decrypt the message then it will show result like shown in fig-4 which is hard to read [39]. RSA uses 3 processes to implement a successful digital signature that is key generation, digital signature generation(fig-5) and digital signature verification(fig-6). Digital Signature generation process:

- Digital signature algorithm is utilised to produce a digital signature.
- A record that is signed by keys produced by algorithms.
- The private key of the sender is used to sign a document and produce a signature.
- Hash value is generated from the document by applying a hash function then private key encrypts this hash value.
- The document which is produce by the Digital Signature Algorithm encryption is mentioned as digitally signed document, after that this document will send over the network or to receiver end.

Digital Signature Verification process:

- The identical hash function is applied to decrypt the hash using the public key of the sender at the receiver end.
- If both hash value matched, then the signature is properly validated.
- So, the message can be accepted otherwise it is rejected.

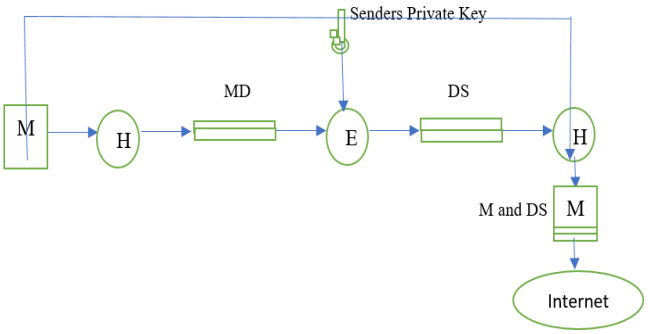

Figure 5. Digital Signature Generation Process [39]

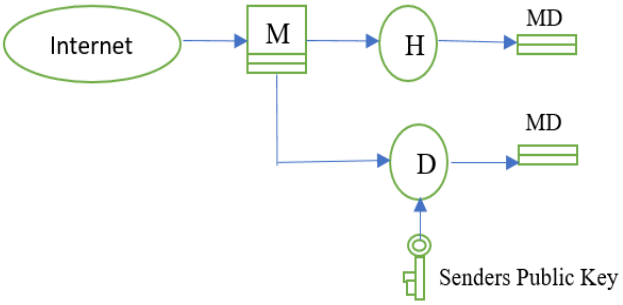

Figure 6. Digital Signature Verification Process [39]

AES (Advanced Encryption Standard)

This is amongst the most widely adopted encryption algorithm. It uses symmetric block cipher for key generation. The length of the key determines the number of rounds in AES. It has various key lengths of 128, 192, 256 bits. AES encryption process uses a refining procedure that depends on the number of the chord used. The relationship between the key length and the number of rounds is as follows [40].

Table 2. Number of Key Lengths and rounds.

AES Key Length (bits)	Number of Round (Nr)
128	10
192	12
256	14

There are 4 steps in this algorithm that are byte substitution, shift rows, mix columns, add round keys. It is executed in software and hardware all over the world to encrypt delicate data. In this algorithm the computations are performed on bytes instead of bits. Various applications are using AES algorithm like, wireless security, processor security, SSL/TSL and file encryption etc [38]. AES algorithm can reserve the privacy and integrity of data in Message Transfer Process.

Diffie-Hellman

Diffie-Hellman is an asymmetric encryption algorithm which was published in 1976 which is named after Whitfield Diffie and Martin Hellman. It is a protocol used for key-exchange, that enables communication between two parties over public channel to establish a mutual secret. Here the key size the same as the authentication certificate (1024-2048 bits) [31].

Blockchain

Blockchain in digital signature is employed for the verification of the user's impression of the transaction. It uses the private key for signing of the digital transaction whereas the public key is used to authorize the sender. Blockchain along with digital signature ensures the safety of our identity that is genuine and authenticated [30]. Digital signing in blockchain aims to authenticate transactions. Each node in the network verifies the submitted transaction and then makes an informed decision asking the whole network to add

e-ISSN: 2583-3472

on it. The main advantage is that, in the event of a dispute, we can prove whether our document has been tampered or not [37].

CONCLUSION AND FUTURE SCOPE

In this paper we have focused on several schemes of digital signatures that will secure the document properly. The digital signatures along with privacy schemes is addressed in this paper which also enable the confidentiality. Here, we not only focused on the traditional cryptography methods, but also have emphasized the importance of new emerging technologies on cryptography for both digital signature and encryption implementation.

The main objective of this paper is to provide a basic idea on different schemes of digital signatures with privacy parameter to the researchers. In future we will plan to simulate the digital signatures with RSA and AES scheme to check the standard of confidentiality maintained.

REFERENCES

[1] Ravneet Kaur, Amandeep Kaur, “Digital Signature”, Springer, 2012.
[2] I Built a Tool to Sign Contracts on Smart Contracts Without Using Your Private Key | by Lina Nada Maach The Innostation Publication, Jan 15, 2002.
[3] A. Sinha, K. Singh, “A technique for image encryption using digital signature”, Optics Communications, vol. 218, no. 4-6, pp. 229–234, 2003.
[4] D. Bhattacharya, N. Bansal, A. Banaerji and D. R. Chowdhury, "A near optimal S-box design", Information Systems Security, Lecture Notes in Computer Science, vol. 4812, pp. 77–90, 2007.
[5] Nidhi Sethi,Deepika Sharma “A novel method of image encryption using logistic mapping”, International Journal of Computer Science Engineering, vol. 01, no. 2, pp. 115-119, 2012.
[6] Aloka Sinha, Kehar Singh, “A technique for image encryption using digital signature”, Optics Communications, 2003.
[7] Shahzad Alam, Amir Jamil, Ankur Saldhi, Musheer Ahmad, “Digital Image Authentication and Encryption using Digital Signature”, ICACEA 2015.
[8] V. Vapnik, "Statistical Learning Theory", John Wiley, 2008.
[9] Paris Kitsos, Nicolas Sklavos, Odysseas G. Koufopavlou, “An efficient Implementation of the digital signature algorithm”, ICECS, 2002.
[10] Z. Zalevsky, D. Mendlovic, U. Levy, G. Shabtay, Opt. Commun. 180 (2000)
[11] Niels Ferguson and Bruce Schneier, Practical Cryptography, Wiley, 2003. IEEE P1363 Standard Specifications for Public Key Cryptography, IEEE, November.
[12] Mr. Hemant Kumar, Dr.Ajit Singh, An Efficient Implementation of Digital Signature Algorithm with SRNN Public Key Cryptography, IJRREST, June 2012.
[13] R.Gennaro and P.Rohatgi, How to sign digital streams, presented at Proceedings of CRYPTO’97, Santa Barbara, CA, 1997.
[14] Kefa Rabah, “Secure Implementation of Message Digest, Authentication and Digital Signature”, Information Technology Journal, 2005.
[15] Weidong Fang, Wei Chen, Wuxiong Zhang, Jun Pei, Weiwei Gao, Guohui Wang, “Digital signature scheme for information non-repudiation in blockchain: a state of art review.”, EURASIP Journal on Wireless Communications and Networking,2020.
[16] https://www.simplilearn.com/tutorials/cryptography-tutorial/digital-signature-algorithm
[17] https://www.tutorialspoint.com/cryptography/cryptography_digital_signatures.htm
[18] W.Diffie and M. E. Hellman, New directions in cryptography, IEEE Transactions on information theory, vol.22,1976. 1996.
[19] L. Buttyán, L. Dóra, F.,Martinelli, M.Petrocchi,2010. Fast certificate-based authentication scheme in multi operator maintained wireless mesh networks. Elsevier Computer CommunicationsTransform", in Proc. 7th IEEE International Symposium on Signal Processing and Information Technology (ISSPIT'07), December 2007, Egypt.
[20] G. R. Blakley, “A Computer Algorithm for Calculating the Product AB modulo M”, IEEE Transactions on Computers, Vol. C-32, May 1983.
[21] F.E.S.,Dunbar, 2002. Digital Signature SchemeVariation, presented in University of Waterloo.
[22] FIPS 180-3, Secure Hash Standard - National Institute of Standards and Technology: http://csrc.nist.gov/publications/fips/fips1803/fips1803_final.pdf
[23] Bart Preneel, “Cryptographic Hah Functions: An Overview”, ICSVC, 1993.
[24] A. Buldas and M. Saarepera, Electronic Signature System with Small Number of Private Keys, presented at 2nd Annual PKI Research Workshop, 2003.
[25] Burhan Ul Islam Khan, Rashidah Funke Olanrewaju, Malik Arman Morshidi, Roohie Naaz Mir, Miss Laiha Binti Mat Kiah, Abdul Mobeen Khan “Evolution and Analysis of Secure Hash Family”, Malaysian Journal of Computer Science, 2022.
[26] Piyush Kumar Shukla, Amer Aljaedi, Piyush Kumar Pareek, Adel R. Alharbi and Sajjad Shaukat Jama, “AES Based White Box Cryptography in Digital Signature Verification” MDPI, Sensors, 2022.
[27] Bruce Schneier, Applied Cryptography – Protocols, Algorithms and Source Code in C, Second Edition, John Wiley and Sons, New York, 1996.
[28] Mohammad A Alia, “Combining Public-Key Encryption with Digital Signature Scheme”, Al-Zaytoonah University of Jordan, 2016.
[29] Abhishek roy and sunil karforma., ‘A survey on digital signatures and its applications’, J of Comp. and I.T. Vol.3(1&2) (2012).
[30] National Institute of Standards and Technology (NIST), Digital Signature Standard, FIPS PUB 186-2, http://csrc.nist.gov/publications/fips/fips186-2/fips186- 2.pdf
[31] Clifford Cocks, A Note on 'Non-Secret Encryption’, CESG Research Report, 20 November 1973. 1993.
[32] Cetin Kaya Koc, “RSA Hardware Implementation”, RSA Laboratories, RSA Data Security, Inc., online available
[33] P. S. Chen, S. A. Hwang, and C. W. Wu, “A systolic RSA public key cryptosystem,” in Proceedings of International Symposium of Circuit and System (ISCAS’96) 1996, vol. 4, pp. 408-411.
[34] J. Li, Z. Liu, and Y. Wu "An Improved Privacy-Preserving Digital Signature Scheme Based on RSA" IEEE, 2019.
[35] C. K. Koc, "RSA hardware implementation", Technical report, RSA Laboratories, RSA Data Security, Inc., Redwood City, CA, 1995.

e-ISSN: 2583-3472

[36] Z Li Ping, S Qi Liang, and L Xiao Liang, "RSA Encryption and Digital Signature", in International Conference on Computational and Information Sciences, 2011.
[37] Abdelhamid Hassan Mansour, "Analysis of RSA Digital Signature Key Generation using Strong Prime", University of Jeddah, Saudi Arabia, 2017.
[38] H Siregar, E Junaeti, T Hayatno , "Implementation of Digital Signature Using AES and RSA Algorithms as a Security in Disposition System of Letter", 1st Annual Applied Science and Engineering Conference IOP Publishing, 2017.
[39] Venkateswara Rao Pallipamu, K. ThammiReddy, P. Sureshvarma, "Design of RSA Digital Signature Scheme Using a Novel Cryptographic Hash Algorithm" ISSN 2250-2459, 2014.
[40] Dinda Husnaa Dhiyaulhaq, Sahda Armandiva Usman, "Comparative Performance of Digital Signature Security Using Cryptography AES 192 BIT and RSA 512 BIT Algorithm Model", Journal of Advances in Information Systems and Technology, October 2020.