IJITEB
Vol. 2
No. 2
2020

International Journal of Information Technology and Business

http://ejournal.uksw.edu/ijiteb

AES (Advanced Encryption Standard) and RSA (Rivest–Shamir–Adleman) Encryption on Digital Signature Document: A Literature Review

Keywords :
Watermarking, Digital Signature, AES, RSA, Literature Review

Abstract : Distributed digital documents, it can utilize cryptographic methods to provide confidentiality, data integrity, authentication and non repudiation services. Watermark in this case serves as authentic proof of ownership of the data or document, and its existence should not damage or change the contents or counter of digital data or digital documents. The RSA and AES encryption methods in digital signatures are appropriate to be taken as a reliable method. But a unique biometric key idea emerged, one of which was used to authenticate users.

1. Introduction

The process of distributing data digitally through electronic media both online or locally and online is greatly facilitated in terms of the process of exchanging data, but behind this convenience there are several vulnerabilities and security threats that might occur. Moreover, if the digital document distributed is important or has a purchase value or the data document has confidential content. To maintain the confidentiality of distributed digital documents, it can utilize cryptographic methods to provide confidentiality, data integrity, authentication and non repudiation services. Cryptographic methods only provide data security services at the time of the distribution process, and therefore need another service that is useful to protect the copyright of the document or digital data.

One of the services that can be used to protect copyright is by providing a watermark, watermarking in improving copyright documents. Watermark in this case serves as authentic proof of ownership of the data or document, and its existence should not damage or change the contents or counter of digital data or digital documents. The watermark method that will be reviewed includes the AES and RSA method. In this literature review, the emphasis is more on the comparison between several developments from the watermarking method that have been previously researched and used. The purpose of this literature review is to find out which method is most appropriate when used to encrypt photos and text documents in the future.

1.1. Previous Research

Research that discusses the application of digital signatures to approve the authenticity of e-voting entitled "Implementation of Digital Signature Group Blind in the Regional Head Election Voting System". E-voting is one solution to the choice of a conventional voting system, in e-voting the role of human beings is replaced by computers for calculating dams, so that errors in counting can be minimized. To enable the secrecy of this e-voting system to use cryptography which consists of a group of digital signatures which are variations of digital signatures built on the RSA algorithm. Through data encryption, this system regulates candidate data that has been chosen by the voters, so that confidentiality is still chosen. in the research of the e-voting system implemented, the blind digital signature group was used when sending data from institutions in the process of regional head selection to authenticate the requested data [1]. Subsequent research has the title "Digital Document Security Application Development Using the Advanced Encryption Standard Algorithm, RSA Digital Signature and Invisible Watermarking" digital document security can also use watermaking techniques, this technique provides protection against unauthorized use of digital material, but to eliminate suspicion from the parties those who do not have access rights to digital watermaking materials can be used invisible watermaking [2]. A signature is a tool used to legalize or as a marker that a document is original from the first party (the maker) or not. This applies to real documents in this case printed or written documents. Next what if the document or file is digital. At this time digital media is not a common

[*] Corresponding authors
e-mail addresses : yudist9612@gmail.com

thing anymore, almost all business activities and everyday use the internet. So from the study entitled "Safeguarding Digital Land Certificates Using Digital Signature SHA-512 and RSA" concluded it was necessary to replace the signatures made in digital form to legalize digital documents. There are three main processes in digital signatures, namely the process of getting a summary of the contents of a document, the process of encoding a summary, and finally the process of inserting an encrypted summary. The process of summarizing a document content can be done using a hash function, the output of a hash function is called a hash value [3]. "*Big module RSA signature algorithm is very popular these years*". The writer of research entitled "Research and Implementation of Four-prime RSA Digital Signature Algorithm" try proposed a four-prime Chinese Remainder Theorem (CRT)-RSA digital signature algorithm in this paper. The Hash function SHA 512 is used to make message digest. Large number are optimized modular exponentiation with CRT combining in Montgomery algorithm. This experiment shows that RSA method got good performance. The security analysis shows higher signature efficiency on resistance of common attacks [4]. Proof of the authenticity of the image and increased security to prove the authenticity of the image must be developed, one of them is by using a digital signature.

The combination of three algorithms for digital signatures is made, namely: Rivest - Shamir - Adleman (RSA), Vigenere Cipher and Message Digest 5 (MD 5). The proposed method was also tested with various attacks to measure the reliability of digital signatures. Various attacks are applied such as blur, salt, and pepper, Gaussian filters. Based on the results of the attack, the smallest change that occurs in a blurring attack has a very good PSNR is 86.7532 dB [5]. Fingerprints have now been used for digital authentication, from these fingerprints you can get unique IDs to be processed into authentication for biometric technology. Now, the fingerprint biometric technology system has been planted in several smartphone products sold today, so users are allowed to unlock their smartphones simply by scanning their fingerprints into the smartphone's fingerprint sensor.The combination of all these technologies (digital signatures, biometric fingerprints, smartphones with fingerprint sensors) can trigger innovation to make a system that can make digital signatures using only fingerprints on smartphones [6]. Techniques that can be seen as cryptographic aspects or by providing signatures, digital, can produce integrity and authenticity data. The addition of asymmetrical and symmetrical algorithms, namely the RSA and AES algorithms will require large, digital signatures to secure data security. RSA is used for the process of sending digital signatures, while RSA is used for the process of encoding messages to be sent by the sender to the recipient [7].

2. Literature Review

The basic concept of cryptography to be discussed is about RSA (Rivest-Shamir-Adleman) and AES (Advanced Encryption Standard) which will be valued from the aspects of reliability and workings of the algorithm that used to deploy on digital signature.

2.1. **RSA (Rivest-Shamir-Adleman**)

RSA is an asymmetric cryptography algorithm. This algorithm is the first algorithm most appropriate for signing and encryption and one of the first major cryptographic discoveries with a public key [2] [8].

In this method, there are three main parts: key generation, encryption, and decryption process.

1) Key generation

In RSA algorithm, encryption and decryption process need a public key and private key. Here are the steps to generate the public and private key on RSA algorithm:

Step 1: Generate two prime number p and q, where $p \neq q$.

Step 2: Calculate *p* and *q* using Eq 1-3:

$$n = p \text{ x } q \qquad (1)$$

$$\Theta(n) = (p - 1) \text{ x } (q - 1) \qquad (2)$$

$$K = \Theta(n) + 1 \qquad (3)$$

Step 3: Factor the value of k to get coprime value, so the first-factor use for *e* and the second factor s the value of d.

Step 4: The public key is [*e*,n] for the sender and pair private key is [d,n] for the receiver.

2) Encryption

To encrypt the sender message (*M*) using a public key [*e*,n] that has been generated at key generation process To generate the cipher using Eq.4.

$$C = (m^e) \text{ } mod \text{ } n \qquad (4)$$

Where c is an element of the cipher (c € C), *m* is an element of the message (m € M), *e* is the public key and *n* can show at Eq.1.

3) Decryption

To decrypt the cipher (*C*), from receiver use the private key (*d* , *n*). Below is decryption process. Use Eq.5 to perform the decryption process.

$$m = (c^d) \text{ } mod \text{ } n \qquad (5)$$

Where, *m* is an element of the message (m € M), *c* as an element of the cipher (c € C), *d* is the private key. While *n* obtained from Eq.1.

2.2. AES (Advanced Encryption Standard)

AES algorithm was used for security during the process of encoding a message that will be sent to the receiver. AES algorithm used in this study to meet the objectives of cryptography i.e. secrecy and data integrity [9], [10], so the messages content was protected from actions like tapping data.

A digital signature scheme carried out in this study is a modification of the digital signature scheme using Hash function [11]. Modification made to add the encryption process of the message there in. AES algorithm serves to conceal the contents of the message that would be sent to the receiver while for the key exchange would be hidden using the RSA algorithm. The RSA algorithm was not used to encrypt messages, but encrypts the symmetric key with the message receiver's public key. This is because the way of work of RSA algorithm is slower than symmetric cryptography such as DES or AES [11], [12], [13], [14]. Therefore the message would be encrypted with a symmetric key algorithm, namely AES algorithm, while the key would be encrypted with an asymmetric algorithm i.e. RSA algorithm [2], [15], [16].

3. Result

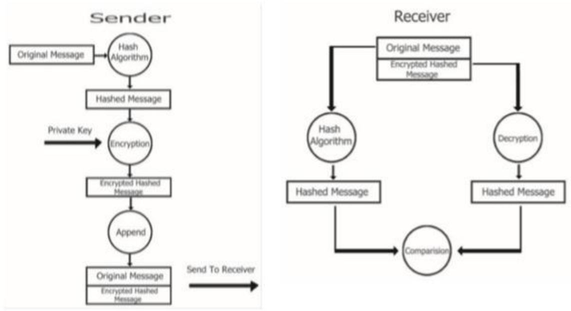

Fig 1. This is a general flow of Digital Signature

So from several studies conducted by previous researchers, the process of giving digital watermarking and signing digital signatures is more suitable using the RSA encryption method. While the AES encryption method is more suitable for encoding the results of digital signatures that have been received by the recipient of the message .

4. Conclusion

In encryption and decryption, the choice of key length affects the filesize of the encrypted file and also the long time the encryption process. The RSA and AES encryption methods in digital signatures are appropriate to be taken as a reliable method. But a unique biometric key idea emerged, one of which was used to authenticate users. The fingerprint user ID cannot reach because it is stored on a secure system from a smart phone. Fingerprints on smart phones can encrypt and decrypt the process by connecting to the server and calling the decrypt process.

5. References

[1] M. Yusuf and T. Rohman, "IMPLEMENTASI GROUP BLIND DIGITAL SIGNATURE DALAM SISTEM E-VOTING PEMILIHAN KEPALA DAERAH," *Semin. Nas. Inform.*, vol. 2012, no. semnasIF, pp. 75–81, 2012.

[2] A. S. Sukarno, "Pengembangan Aplikasi Pengamanan Dokumen Digital Memanfaatkan Algoritma Advance Encryption Standard , RSA Digital Signature dan Invisible Watermarking," *Lemb. Sandi Negara Jakarta*, pp. 1–8, 2013.

[3] A. S. Leonardo Refialy, Eko Sediyono, "Pengamanan Sertifikat Tanah Digital Menggunakan Digital Signature SHA-512 dan," *J. Tek. Inform. dan Sist. Inf.*, vol. 1, pp. 229–234, 2015.

[4] Z. Xiao, "Research and Implementation of Four-prime RSA Digital Signature Algorithm," 2015.

[5] C. Rsa, R. D. Ardy, O. R. Indriani, C. A. Sari, D. R. Ignatius, and M. Setiadi, "Digital Image Signature using Triple Protection Cryptosystem (RSA, Vigenere, and MD5)," pp. 87–92, 2017.

[6] E. Rahmawati, M. Listyasari, A. S. Aziz, S. Sukaridhoto, and F. A. Damastuti, "Digital Signature On File Using Biometric Fingerprint With Fingerprint Sensor On Smartphone," pp. 234–238, 2017.

[7] P. S. Lozhnikov and A. E. Sulavko, "Implementation of Digital Signature Using Aes and Rsa Algorithms as a Security in Disposition System af Letter Implementation of Digital Signature Using Aes and Rsa Algorithms as a Security in Disposition System af Letter," 2017.

[8] and S. V. P. V. R. Pallipamu, T. R. K, "Design of RSA Digital Signature Scheme Using A Novel Cryptographic Hash Algorithm," *Int. J. Emerg. Technol. Adv. Eng.*, vol. 4, no. 6, pp. 609–613, 2014.

[9] P. S. and S. S. G. S. Mewada, "Exploration of efficient symmetric AES algorithm," *2016 Symp. Colossal Data Anal. Netw.*, pp. 1–5, 2016.

[10] M. A. B. and S. A.-N. Y. A. Nasser, "AES algorithm implementation for a simple low cost portable 8-bit microcontroller," *2016 Sixth Int. Conf. Digit. Inf. Process. Commun.*, pp. 203–207, 2016.

[11] R. Munir, "Kriptografi," *Bandung, Inform.*, 2006.

[12] B. Schneier, "Applied Cryptography – Protokol, Algorithms and Source Code in C," *John Wiley Sons*, 1996.

[13] Noroozi, E., Daud, S. M. & Sabouhi, A. 2014. Enhancing Secured Data Hiding Using Dynamic Digital Signature for Authentication Purpose. Jurnal Teknologi 68.

[14] Prakash, Purohit, (2013) An Efficient mplementation of PKI architecture based Digital Signature using RSA and various hash functions (MD5 and SHA variants

[15] S. A. Jaju and S. S. Chowhan, "A Modified RSA algorithm to enhance security for digitalsignature," Computing and Communication (IEMCON), 2015 International Conference and Workshop on, Vancouver, BC, 2015, pp. 1-5.

[16] S. Mewada, P. Sharma and S. S. Gautam, "Exploration of efficient symmetric AES algorithm," 2016 Symposium on Colossal Data Analysis and Networking (CDAN), Indore, 2016, pp. 1- 5.