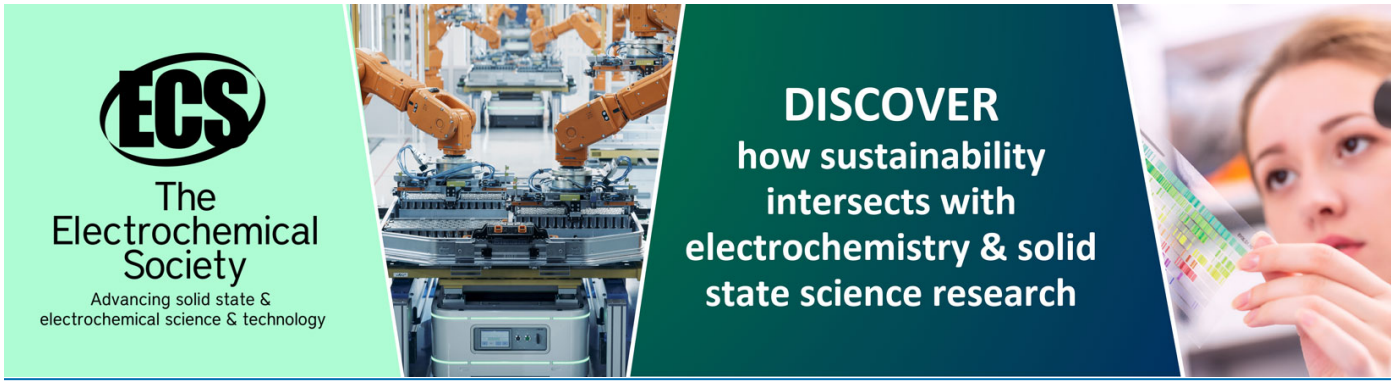
Implementation of Digital Signature Using Aes and Rsa Algorithms as a Security in Disposition System af Letter



IOP Conf. Series: Materials Science and Engineering **180** (2017) 012055 doi:10.1088/1757-899X/180/1/012055

Implementation of Digital Signature Using Aes and Rsa Algorithms as a Security in Disposition System af Letter

H Siregar, E Junaeti*, and T Hayatno

Departemen Penddikan Imu Komputer, Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam, Universitas Pendidikan Indonesia

*enjun@upi.edu

Abstract. Activities correspondence is often used by agencies or companies, so that institutions or companies set up a special division to handle issues related to the letter management. Most of the distribution of letters using electronic media, then the letter should be kept confidential in order to avoid things that are not desirable. Techniques that can be done to meet the security aspect is by using cryptography or by giving a digital signature. The addition of asymmetric and symmetric algorithms, i.e. RSA and AES algorithms, on the digital signature had been done in this study to maintain data security. The RSA algorithm was used during the process of giving digital signature, while the AES algorithm was used during the process of encoding a message that will be sent to the receiver. Based on the research can be concluded that the additions of AES and RSA algorithms on the digital signature meet four objectives of cryptography: Secrecy, Data Integrity, Authentication and Non-repudiation. Keywords: Mail, Digital Signature, Cryptography, AES and RSA algorithms.

1. Introduction

Activity correspondence, both electronic and non-electronic, has an important role in activities in an agency or company, even some of them set up a special division to handle issues related to the letter management. Mail archive management form non-electrically done manually, while for electronic mail management can be done using email client. To prevent things that are not desirable, such as a leak or a change the contents of the letter, then the letters security must be safeguarded. The safety of a non-electronic letter is located on the packaging, while the electronic mail security can be maintained by providing a digital signature or by using cryptography [1], [7], [11].

Vishnu Wendanto [2] used a digital signature and RSA algorithms on the disposition system of letter. Security letter safeguarded by performing encryption on the file name of the letter, but there was no security for the contents of the letter itself. According to Ibnu et al. [3] digital signature was one solution to data security methods were good because they have the accuracy of a high enough value to a change in data. Ibn Berliyanto G. A., Amir Hamzah, and Suwanto Raharjo provided digital signatures used algorithm CRC32 on transcripts as authentication data. Setiyo Aji Sukarno [4] developed an application securing digital documents used digital signatures with RSA and AES algorithms, as well as the invisible watermarking. The output of their research was the image that had been encrypted and a file containing digital signature verification. However, the research applies to

files with jpg format only. Application development had not reached the process of key management, so that the whole key management was managed by the entity who did data exchange.

This study used a combination of asymmetric and symmetric cryptographic algorithms, i.e. algorithms RSA and AES-128 algorithms. The RSA algorithm is an asymmetric cryptographic algorithm that has a key length in bits that can be set so that the longer the bit the more difficult to solve because of the difficulty of factoring the very large two numbers, but it takes a long time for the decryption process, while AES algorithm is a symmetric algorithm that uses a block cipher [1]. During the encryption and decryption process, AES-128 algorithm doing ten cycles transformation functions, i.e. Add Round Key, Sub Byte, Shift Rows and Mix Column [6]. The study was conducted to see the effect of the combination of digital signatures with RSA and AES algorithms to the disposition system of letter based cryptographic purposes, namely Secrecy, Data Integrity, Authentication and Non-repudiation [6], [8], [9], [10], [11], [12].

2. Digital Signature Scheme

This study used digital files with jpg format because they can be opened with a standard platform or application that has been provided by the computer operating system. RSA algorithm was used to secure the key when the process of digital signature was given to sign that the messages sent had legality. The RSA algorithm was used to meet the objectives of cryptographic i.e. authentication and non-repudiation [5], [7]. 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 [12], [13, 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 [1]. Modification made to add the encryption process of the message therein. 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 [1], [6]. 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. Modification of digital signature scheme was described by Figure 1.

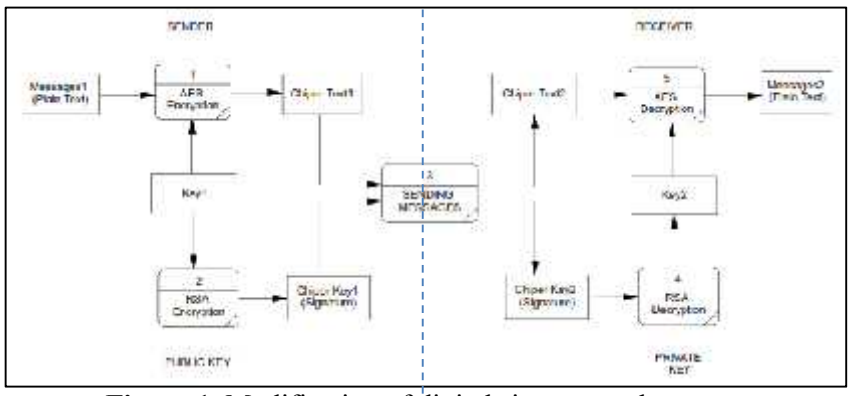


Figure 1. Modification of digital signature scheme

Figure 1 shows that messages encrypted by AES algorithm to generate cipher text that would be sent to the receiver and stored in the database. AES key that used was a combination of eight digit number of the sender identity and eight digit number of the date of sending letter. Then the key used in the encryption algorithm AES would be encrypted using the RSA algorithm to generate cipher key or digital signature and would be stored in the database. RSA algorithms have two keys i.e. public key and private key [1], [6]. In this research, the two keys used were generated from two prime numbers

between 2 and 2000, which was chosen randomly. The recepient would be decrypt the signature to generate a key that would be used to decrypt the messages.

3. Testing

Figure 2 shows an example of message that woud be encrypted, result of encryption of message, and result of decryption of message. The keys used were:

- AES key (plain text) : 1957122620160805
- Public key for RSA : (7, 1728239)
- Private key for RSA : (739543, 1728239)

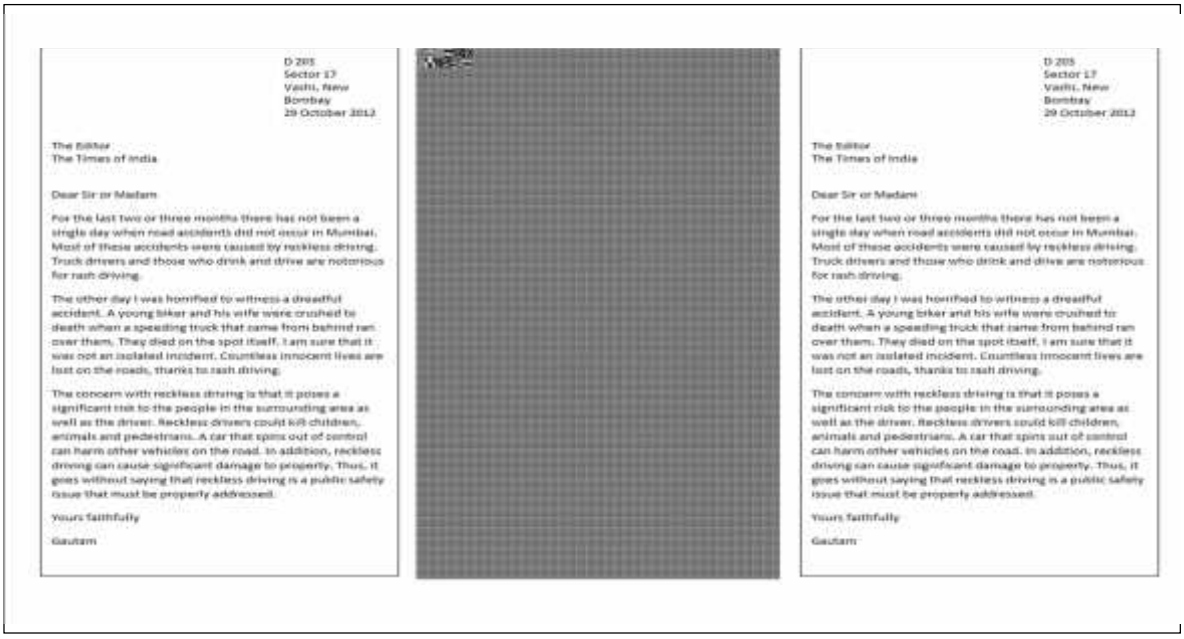


Figure 2. Sample of letter encryption using the AES algorithm

Figure 2(a) was an example of a letter with jpg format to be delivered. At the time of the encryption used AES algorithm, only the image data will be done encoding, so the results of it was still images with jpg format, which was shown in Figure 2(b). After the encryption process was complete, the image was stored on the archive server in the form of image cipher text. Figure 2(c) show the result of decryption of message.

The following forms of testing conducted to determine the research results. Tests carried out on digital signature schemes that had been made based on a modification of the attacks [14]. The image that be used in the test was the image shown in the Figure 2(a).

3.1. Addition of Single Character on Signature

The addition of one character carried out in order to saw the effect of a change in the value of the AES key toward the result of decryption of image. Suppose the character '1' was added to the signature, so the signature was:

117649 185193 148877 166375
117649 125000 125000 157464
12*1*5000 110592 117649 157464
110592 175616 110592 148877

Then the signature was decrypted with the RSA algorithm to generate AES key as follows.

19571226**?**0160805

If the key was used to decrypt the message with the AES algorithm, the result of the decryption was addressed by Figure 3.

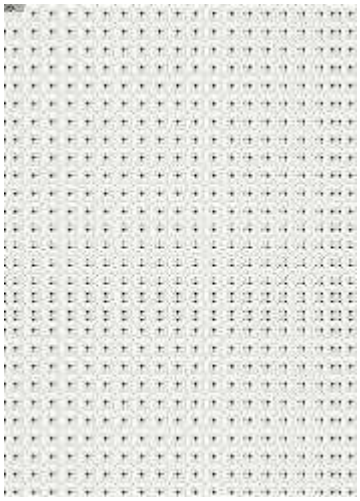


Figure 3. Result of Adding One Character

It can be seen in the Figure 3 that the result did not match the original image in the Figure 2(a) and generate a random image. This shows that the digital signature scheme was sensitive to the addition of a character in the signature.

3.2. Reduction of One Character

A reduction of one character carried out in order to saw the effect of a change in the value of the AES key toward the result of decryption of image. Suppose that character '1' on row 185 193 omitted in the signature, so the signature became

117649 **85193** 148877 166375 117649 125000
125000 157464 1215000 110592 117649
157464 110592 175616 110592 148877

Then the signature was decrypted with the RSA algorithm to generate AES key as follows.

1**?**5712262016080

If this key was used to decrypt the message with the AES algorithm, the result of the decryption was addressed by Figure 4.

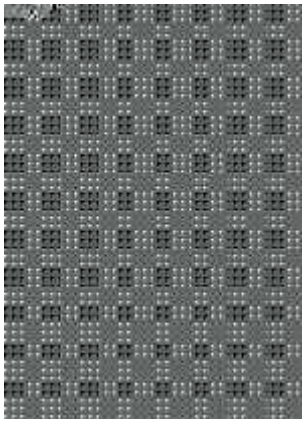


Figure 4. Result of Reduction One Character

It can be seen in the Figure 4 that the result did not match the original image in the Figure 2(a) and generate a random image. This shows that the digital signature scheme was sensitive to the reduction of a character in the signature.

3.3. Changing of One Character

Changing one character conducted to saw the effect of a change in the value of the AES key toward the result of decryption of image. Let the characters '7' was converted into a character '8' in the signature, so the signature became

117649 185193 148877 166375
117649 125000 125000 15***8***464
1215000 110592 117649 157464
110592 175616 110592 148877

Then the signature was decrypted with the RSA algorithm to generate AES key as follows.

1957122 2016080

If this key was used to decrypt the message with the AES algorithm, the result of the decryption was addressed by Figure 5.

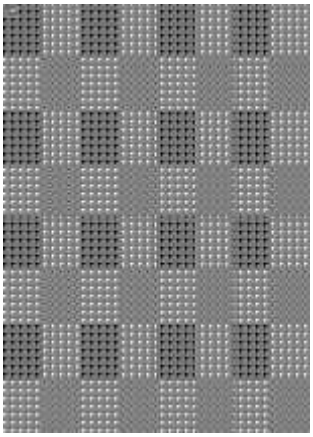


Figure 5. Results of Conversion One Character

It can be seen in the Figure 5 that the result did not match the original image in the Figure 2(a) and generate a random image. This shows that the digital signature scheme was sensitive to the conversion of a character in the signature

3.4. Using different Key

This test was done to try a case where the receiver used a different private key which was not spouses of public key used to create the signature. Suppose that the key used was

n = 1685287
public key = 3
private key = 1241787

The results of decryption with the RSA algorithm was

If this key was used to decrypt the message with the AES algorithm, the result of the decryption was addressed by Figure 6.

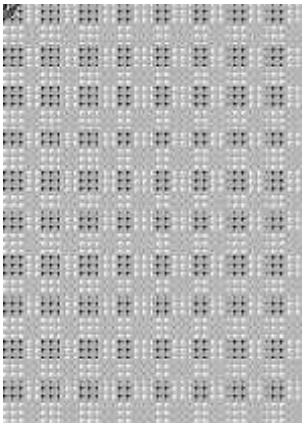


Figure 6. Results of Private Key Using different

It can be seen in the Figure 5 that the result did not match the original image in the Figure 2(a) and generate a random image. This shows that the digital signature scheme was sensitive to the use of digital signature keys.

3.5. Turn Around Time

Testing the turnaround time was a test of the execution time required of an encrypted plaintext into cipher text and decrypted cipher text back into plaintext. Tests were conducted at 5 .jpg image file with a size of 1.96 KB to 58 KB. Here were the test results turnaround times devoted by Table 1.

Table 1. Table Testing Turnaround Time

No	File name	Size (KB)		Time (second)		
		Before Encryption	After Encryption	Encryption	Decriptyon	Sum
1	image.jpg	1.96	1.96	0.188011	0.735042	0.923053
2	MUJDhs-medium.jpg	19	19	2.157123	8.337477	10.4946
3	Night-Stalker-Silhouette.jpg	31	31	3.486199	14.0658	17.552
4	sample_fc080cc07078e9b1b4db9ea6cebd081ce689ae8e.jpg	36	36	4.156238	16.79196	20.9482
5	Barathrum-Silhouette.jpg	58	58	6.754387	27.22156	33.97594

In Table 1 it can be said that the size of the file before encryption and after decryption with the AES algorithm remains the same. It showed the AES algorithm did not add or reduce the size of the file that was used, so the digital signature maintained the integrity of the message. In addition it can be said that the bigger size of the file the longer for encryption and decryption. So the time required for process of encryption or decryption was different due to the length of plaintext.

4. Results and Discussion

Here the influence of Digital Signature using AES and RSA algorithms to the four objectives of cryptograpy.

4.1. Secrecy

By performing encryption and decryption of the message was an attempt to maintain the confidentiality of messages. Only the owner of the key could only read the contents of the message. So in addition to those who did not have the key used for encryption and decryption process would not know the contents of messages sent.

Figure 2(b) shows that the encryption process of message using AES algorithm generate cipher text or encrypted messages. The cipher text shown the message had no real meaning, so the purpose of secrecy can be met.

4.2. Data integrity

Table 1 show that the size of the file before encryption and after decryption with the AES algorithm remains the same. It shows the AES algorithm did not add or reduce the size of the file that was used, so the digital signature maintained the integrity of the message. Those prevent the addition or reduction of the content of the message. In addition, as long as no one knows the RSA private key no one would be able to change the contents of the letter.

4.3. Authentication (Authentication)

When key exchange between sender and receiver, keys encrypted and decrypted using an asymmetric RSA algorithm keys. It was intended that only the origin recipient who know the meaning of a message sent by the sender. In subsection 3.4, it could be said that by using a different private key to

decrypt the signature would cause the message be meaningless. This shows that with the RSA algorithm can meet the authentication aspect.

4.4. Non-repudiation (non-repudiation)

By doing the appropriate key generation, the sender could not deny that he had sent a message, because the digital signature was obtained from AES key value that consists of a combination of 8-digit numeric number of the sender's identity and the 8-digit numeric message delivery time. Utilization of encryption and decryption with the RSA algorithm was also intended that the receiver could not deny that the receiver was the actual receiver of the message. This showed that the digital signature could fulfill aspects of non-repudiation.

5. Conclussion

Modification of digital signature scheme by adding the message encryption key and the encryption process when sending messages and adding the decryption process and the decryption key when you receive a message was done. The accuracy of the message could be guaranteed because the digital signature was very sensitive to a change in data. The time required for the execution of the program would increase because the system would make the process of AES and RSA encryption algorithm when sending messages and make decryption algorithm AES and RSA algorithms when receiving messages.

Effect of digital signatures using algorithms AES and RSA algorithms and disposition system of letter meet the four cryptographic purposes, namely secrecy, data integrity, authentication and non-repudiation. Digital signatures could ensure the validity of the sender, the message authenticity and non-repudiation. AES algorithm could preserve the secrecy and integrity of data messages in the message delivery process. Authentication and non-repudiation can be handled by the RSA algorithm. When the exchange of keys to be used AES algorithm, the key would be encrypted and decrypted by the RSA algorithm for the purpose of authentication and non-repudiation.

References

[1] R. Munir, “Kriptografi,” Bandung, Informatika, 2006.
[2] W. Wedanto, “Sistem Mailtracking dengan Digital Signature,” Sistem Komputer STMIK-AUB Surakarta, 2013.
[3] Ibnu Berliyanto G.A, Amir Hamzah, Suwanto Raharjo, “Penerapan Digital Signature pada Transkrip Nilai Sebagai Otentikasi Data,” Intitut Sains &Teknologi AKPRIND Yogyakarta, 2014.
[4] A. S. Sukarno, “Pengembangan Aplikasi Pengamanan Dokumen Digital Memanfaatkan Algoritma Advance Encryption Standard, RSA Digital Signature dan Invisible Watermarking,” Deputi III, Lembaga Sandi Negara, 2013.
[5] G. R. The, “Studi dan Implementasi Digital Signature Menggunakan algoritma RSA dan fungsi HAVAL,” Institut Teknologi Bandung, 2010.
[6] B. Schneier, “Applied Cryptography – Protokol, Algorithms and Source Code in C,” new york, John Wiley and Sons, Inc, 1996.
[7] S. A. Jaju and S. S. Chowhan, "A Modified RSA algorithm to enhance security for digital signature," Computing and Communication (IEMCON), 2015 International Conference and Workshop on, Vancouver, BC, 2015, pp. 1-5.
[8] R. Dhagat and P. Joshi, "New approach of user authentication using digital signature," 2016 Symposium on Colossal Data Analysis and Networking (CDAN), Indore, 2016, pp. 1-3.
[9] B. Al-Hammadi, M. Shahsavari, "Certified exchange of electronic mail (CEEM) Southeastcon '99", Proceedings. IEEE, pp. 40-43, 1999.
[10] Kazuki Katagish, Tohru Asami, Yoshihiko Ebhihara, Kazuo Toraichi, Tetsuo Sugiyama, "A Public Key Cryptography-Based Enhanced Mail Gateway with the Mailing list Function",

IEEE Pacific Rim Confernece, pp. 262-265, 1999.

[11] T. R. Devi, "Importance of Cryptography in Network Security," Communication Systems and Network Technologies (CSNT), 2013 International Conference on, Gwalior, 2013, pp. 462-467

[12] 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.

[13] Y. A. Nasser, M. A. Bazzoun and S. Abdul-Nabi, "AES algorithm implementation for a simple low cost portable 8-bit microcontroller," 2016 Sixth International Conference on Digital Information Processing and Communications (ICDIPC), Beirut, 2016, pp. 203-207.

[14] Lynn Margaret Batten, "Digital Signatures," in Public Key Cryptography:Applications and Attacks , 1, Wiley-IEEE Press, 2013, pp.103-131.