A Hybrid Solution for Confidential Data Transfer Using PKI, Modified AES Algorithm and Image as a Secret Key

Aye Aye Thinn
Cyber Security Research Lab
University of Computer Studies, Yangon
Yangon, Myanmar
ayeayethinn@gmail.com

Mie Mie Su Thwin
Cyber Security Research Lab
University of Computer Studies, Yangon
Yangon, Myanmar
drmiemiesuthwin@ucsy.edu.mm

Abstract

Nowadays the provision of online services by government or business organizations has become a standard and necessary operation. Transferring data including the confidential or sensitive information via Internet or insecure network and exchange of them is also increased day by day. As a result, confidential information leakage and cyber threats are also heightened. Confidential information trading became one of the most profitable businesses. Encrypting the data is a solution to secure the data from being exposed. In this paper, we would like to propose a solution for the secure transfer of data using symmetric encryption, asymmetric encryption technologies and Key Generation Server as a mixed hybrid solution. A Symmetric encryption, modified AES algorithm, is used to encrypt data. Digital certificate is used both for data encryption and digital signing to assure data integrity. Key generation server is used to generate the second secret key from the publicly recognized information of a person and this key is used as a second secret key in the modified AES. The proposed hybrid solution can be utilized in any applications that require high confidentiality, integrity of data and non-repudiation.

Keywords—*hybrid encryption, encryption, PKI, modified AES*

I. INTRODUCTION

With the rising use by businesses and government agencies of the Internet as a major communication tool, digital data sharing is increasing rapidly, leading to security breaches, cyber bullying, and cyber-attacks. Many applications or systems do not have sufficient security implementation and confidential or sensitive data are accessed by intruders or hackers. Secret sharing methods protect the sensitive data from attackers.

Today, e-Government gained more and more attention and can provide a non-stop government information service through the introduction of online applications G2C, G2B and G2G. However, there are many e-government issues that need to be examined carefully, such as security issues, e-government service requirements, e-government model, e-government strategy and policy, and e-government. [1].

Cryptography, encryption techniques and security products are introduced to provide confidentially of data. Public-key cryptography is based on the asymmetric key model. By using the public-key cryptography and digital certificates, the communicating parties can authenticate each other without sharing secret information in advance. With public-key cryptography, each person gets a pair of keys, a public key and a private key. The public key is published by each user, while the private key is kept secret [2]. With the support of X.509 digital certificates in servers as well as browsers and many other communication equipment, digital certificates are used for authentication. It becomes a security solution for Internet or intranet applications to provide data integrity and confidentiality of the data.

For symmetric key cryptography, both for encryption and decryption, only one secret key is required. Asymmetrical encryption makes use of a couple of keys, a non-public (private) key and a public key. In public key cryptography, different but related pair of secret key is used both for encryption and decryption. Both asymmetric and symmetric encryption have advantages and disadvantages. And the asymmetric encryption is slower than symmetric encryption.

A new hybrid encryption approach is used in this work which combines symmetric cryptography, asymmetric cryptography together for safe exchange of data. Asymmetric encryption is used to hide the secret key of the symmetric encryption algorithm. Symmetric encryption algorithm we used in our work is a modified version of Advanced Encryption Standard and it is named AES-R. AES-R algorithm uses two secret keys and the additional secret key will be generated by the Key Generation Server. Traditional AES key will be generated from an image. Digital signature technology is used to facilitate the data integrity and non-

repudiation. Our proposed work combines all the best of the different technologies for use in real time applications.

II. DIGITAL SIGNATURE TECHNOLOGYy

Digital signature becomes a standard for cryptographic protocol suites, and it is widely used for the proof of authenticity and non-repudiation of transactions, data integrity, and communications. Financial transaction, online banking, e-Government applications, software distributions, auditing and Contract Management Software are now using digital signatures to detect forgery or tampering of the information.

Data signature technology can ensure that: information cannot be revealed by other parties except the senders and receivers; information will not be tampered during transmission; the recipient is able to confirm the identity of the sender; sender information for their own cannot be denied [3].

A. RSA Public Key Encryption

RSA public key encryption was introduced by Ronald Rivest, Adi Shamir, and Len Adleman in 1977. It is a block cipher encryption. Unlike the symmetric key encryption, key used for encryption and decryption is different, however they are closely related.

If we denote the public key as PK and other secret key (private key) as SK, Sender as X and Receiver as Y, the RSA algorithm can be stated as below.

I. Encryption and Decryption

If the Sender X sends the plain text P to the Receiver Y, first Sender X encrypts the message P with PK of Y. The Receiver Y decrypts the cipher with his private key SK to get the plain text P, namely.

Decrypt YSK (Encrypt YPK (P)) = P

If the Y decrypts the cipher text with his public key, it cannot be restored into original plain text P.

Decrypt YPK (Encrypt YPK (P)) $\neq$ P

The security for RSA public key cryptography depends on how difficult it is to calculate the private key SK from the public key PK. This calculation is equivalent to a lump sum for the decomposition into two prime number multiplication factor. So far, no matter with what kind of hardware and software, decomposing a lump sum to two qualitative factors is extremely difficult. So the RSA public key encryption algorithm is still very safe [3]. As the hardware technology is improving and the unceasing research and improvement made to the RSA algorithm, RSA algorithm has been widely used by various applications to date.

III. MODIFIED ADVANCED ENCRYPTION STANDARD (AES-R)

To get better performance in encryption time, the proposed work will use a standard symmetric encryption algorithm. As the AES is the standard of now and it is sturdy sufficient to face the attacks, our proposed security solution used modified version of the AES algorithm, called AES-R. Detail design and implementation of AES-R can be seen in the research paper [4]. The encryption process of AES-R algorithm can be seen in Fig. 1.

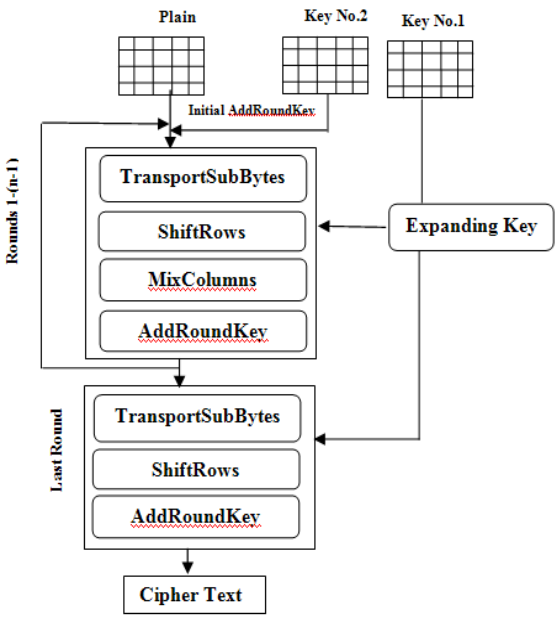

Figure 1. Encryption of AES-R

The decryption process of AES-R can be seen in Fig. 2.

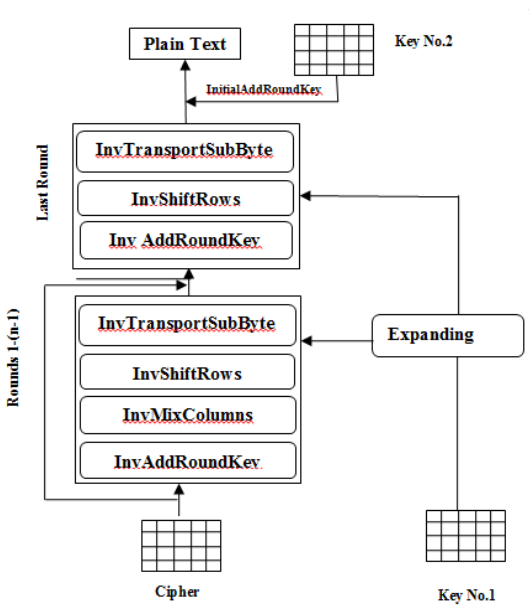

Figure 2. Decryption of AES-R

The reason AES is chosen for modification is that it can work with different key sizes and block sizes. According to the AES statement, it can accept only a block size of 128 bits and a choice of three keys; 128, 192, 256 bits [5].

IV. DESIGN OF PROPOSED WORK

Our proposed work is a combined solution that brings symmetric encryption, Public Key Infrastructure (PKI) and key generation server together.

Because symmetric encryption is faster than asymmetric encryption and since it can be implemented with hardware or software, our proposed solution has used the symmetric encryption to reduce the time for encryption. Among the symmetric encryption algorithms, AES has been a standard until now and because of its good performance, our proposed work has modified AES and proposed AES-R algorithm.

Today, the legislation of many countries recognizes an electronic document as a legal document, i.e. the same legal status as the paper documents. PKI has been established in many countries to make online identification available for online services. Certification Authorities (CAs) issue digital certificates to subscribers and the subscribers use their digital certificates for identification, authorization and digital signature signing. Currently, digital signature is the only answer used for non-repudiation of the document signer and data integrity. For that reason, our proposed work has been using digital signature technology to verify the validity of documents, and the Signer cannot refuse the transaction.

As described in Fig. 1 and Fig. 2 of AES-R algorithm, AES-R algorithm requires two secret keys. Key-1 will be used for key expanding and to generate the round keys. An image file will be used as secret key (i.e. Key-1) after it is converted into a SHA256 hash value. The flowchart of how the image will transform into a secret key(SHA256 hash) is shown in the Fig. 3.

Key-2 is an additional secret key for AES-R. To produce Key-2 of our solution, a Key Generation Server will be used. Key Generation Server will accept the user's publicly identifiable data such as public key of digital certificate, e-ID number, Passport number or e-mail as input and then it generates a secret key. Both the sender and the receiver require Key Generation Server to generate the secret key before they encrypt or decrypt the data.

A. Encryption

For the encryption, the process will perform as shown in the Fig. 4 where P is plain text, H(P) is hash of plain text, SKS is Secret Key generated from Key Server, KEY-1 is secret key of AES-R algorithm generated from the input image, C(P) is cipher of plain text P, C(KEY-1) is cipher of the KEY-1 and Rpk is public key of Receiver.

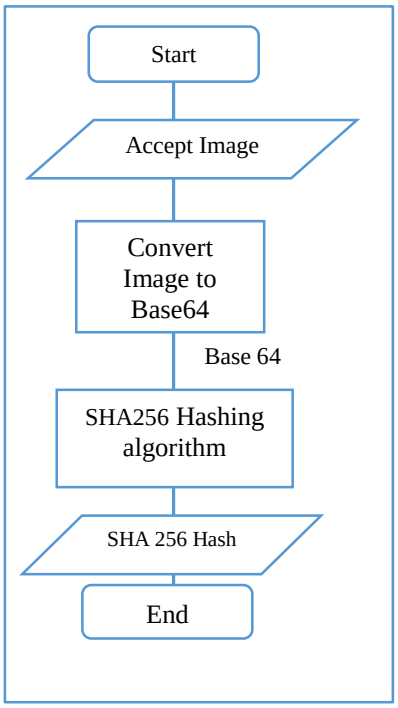

Figure 3. SHA25 Hash Generation from an Image File

To begin with, digital signature algorithm uses plain text P to generate H(P), where H(P) is the digital signature of the plain text. For confidentiality of the data, AES-R is used to encrypt the plain text by using KEY-1 and second secret key(SKS). For the confidentiality of the KEY-1, it is again encrypted with the public key of the Receiver so as to be decrypted with private key of the Receiver.

Finally, when all the encryption processes are finished, (H(P), C(P), C(KEY-1)) will be sent to the Receiver. Fig. 4 shows the encryption process done in the proposed solution.

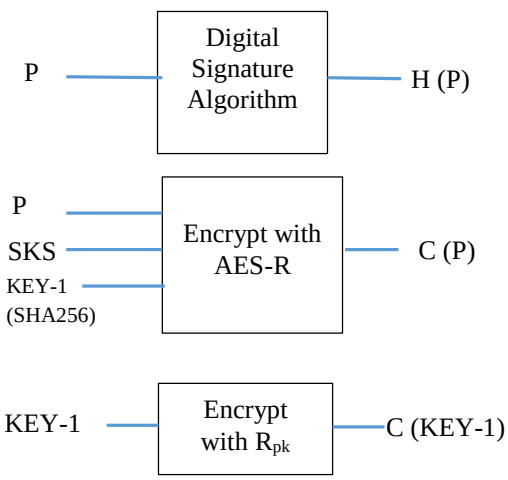

Figure 4. Encryption Process

B. Decryption

When the receiver has received the message (H(P), C(P), C(KEY-1)), the decryption process will be performed as shown in the Fig. 5. Here, Rsk is private key of Receiver and H(P)' is the new hash value generated by P after decryption by AES-R.

In the decryption process, C(KEY-1) is decrypted first to get the KEY-1. Then, KEY-1 together with secret key generated by the Key Generation Server (SKS) and C(P) are used and decrypted to get the plain text P. To verify the integrity of the data, Hash of P is generated again and we get H(P)'. Then two hash values, H(P)' and H(P), are compared. If they are equal or identical, signature is valid and data is not altered during transfer. Otherwise, the message shall be discarded.

The identical of two hash values also guarantees that data is really sent by the Sender. Fig. 5 shows the decryption process done in proposed solution.

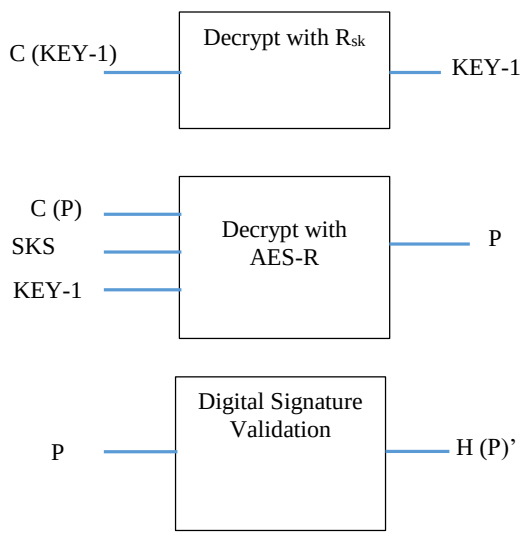

Figure 5. Decryption Process

C. Advantages of Proposed Solution

The advantages of our proposed solution are described briefly in below paragraphs.

1. Data Confidentiality

Confidentiality is the assurance of data privacy: No one can read the data except for the intended specific entity (or entities). If data or documents are transmitted over unprotected or insecure networks, confidentiality or privacy is a basic or desired requirement [6].

The proposed solution used symmetric encryption to achieve faster performance and asymmetric encryption to securely send the secret keys to the Receiver. Our proposed solution can provide confidentiality even if the information is intercepted during transfer. It cannot be restored to its original without having two secret keys and private keys of the Receiver.

2. Data Integrity

Data integrity is the assurance of no alteration whether the data is either in transit or in the storage. A digital signature provides both data origin authentication (evidence about who originated the data) and data integrity (evidence that the data has not been altered in any way) [6].

A digital signature is depending on the message because it can be computed only by the Sender's message and requires private information. As our solution use digital Signature that facilitates authentication of messages, it guarantees that no one can forge the Sender's signature. Besides that, the Sender cannot deny a message he has sent.

Our proposed work digitally signs the data so that it can be verified later with the use of digital signature technology. In addition to that, solution can facilitate identity authentication and non-repudiation.

3. Security

As we use two secret keys and a private and public key pair to encrypt and decrypt the data, it will take longer time for hackers to find the right keys than the symmetric or asymmetric solution alone. Finding the right keys to decrypt the data will be difficult and not possible with having private key of the Receiver.

V. CONCLUSION

Today, sensitive or confidential data are transferred via Internet or insecure network for business purposes or personal affairs. By using insecure network or applications, electronic documents or information may be disclosed, counterfeited, tampered or repudiated when transfer. Confidentiality, integrity and non-repudiation become a mandatory requirement for organizations and government entities.

By using the proposed solution, secret key agreement between the Sender and Receiver is not necessary. Any public information of a person can be used as one of the secret keys. The proposed work can be implemented to secure the sensitive data, for example trade confidential data, credit card information, Government's SECRET and TOP SECRET level documents, which are transferred over insecure network. The proposed solution can be used when data is shared between two people who have conflicting interests. The solution can be used to guard against fraud and it is secure than the analog signature of today.

Implementation of this proposed work will be presented as future work and its performance and impacts

will be analyzed by the view of time taken for encryption/decryption and security analysis.

REFERENCES

[1] M. S. HWANG, C. T. Li, J. J. SHEN, and Y. P. CHU, "Challenges in e-government and Security of Information", An International Journal, Information & Security, Vol. 15, No. 1, 2004, pp. 9-20

[2] T. Elgamal, J. Treuhaft, and F. Chen, "Securing Communications on the Intranet and over the Internet", http://home.netscape.com, Netscape Communications Corp., July 1996

[3] Z.Junxuan, W. Zhong, "The Digital Signature Technology in E-commerce systems", 2009 International Conference on Electronic Commerce and Business Intelligence, 2009 IEEE, pp-16-19, DOI 10.1109/ECBI.2009.90

[4] A. A. Thinn, M. M. S. Thwin, "Modification of AES Algorithm by Using Second Key and Modified SubBytes Operation for Text Encryption", Fifth International Conference on Computational Science and Technology 2018 (ICCST), Computational Science and Technology, Lecture Notes in Electrical Engineering 481, pp. 435-444, 2018, https://doi.org/10.1007/978-981-13-2622-6_42

[5] D. Gayathri, Manjula.A., "Double Encryption Using Rijndael Algorithm for Data Security in Cloud Computing", International Journal of Emerging Technologies in Engineering Research (IJETER), Volume 5, Issue 2, pp. 1-3, February 2017, ISSN: 2454-6410, www.ijeter.everscience.org

[6] C. Adams and S. Lloyd, "Understanding PKI: Concepts, Standards, and Deployment considerations", second edition, Addison-Wesley, 2003

[7] Y. Kumar, R. Munjal, H. Sharma, "Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures", International Journal of Computer Science and Management Studies (IJCSMS), Vol. 11, Issue 03, pp. 60-63, Oct 2011, ISSN (Online): 2231-5268

[8] X. Hu, L. Ma, "A Study on the hybrid encryption technology in the security transmission of electronic documents", 2010 International Conference of Information Science and Management Engineering, IEEE Computer Society, pp. 60-63, 2010,

[9] B. Rajendra, S. N. Darade, Deshmukh, "An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds", International Journal of Science Technology Management and Research, Volume 2, Issue 4, pp. 48-53, April 2017, ISSN (online): 2456-0006