MERGING OF AMSCO WITH RSA ALGORITHM FOR MESSAGE SECURITY

Ei Ei Myint[1], Thin Thu Thu Tun[2], Sabai Win [3]

[1,2] Information Technology, Technological University (Monywa), Monywa, Myanmar
[3] University of Computer Study (Myitkyina), Myitkyina, Myanmar

Abstract

The art and science of keeping message security is referred to as cryptography. It means hidden writing, the practice of using encryption to conceal text. The need of message security over communication channel is increased to high extent. In order to keep the security and confidentiality of message, encryption techniques can be used. Nowadays, hybridization is used by merging two or more techniques to develop a new and improved form. The proposed system develops a hybrid approach by merging symmetric Amsco cipher and asymmetric RSA algorithm to enhance message security. The system evaluates the performance of algorithms by using the time consumption, memory usage and the avalanche effect. The proposed RSA-Amsco algorithm will cover the weakness of Amsco because of its avalanche effect. The RSA-Amsco is more secured than original RSA, because it consists of one additional Amsco's transposition function.

Keyword: Security, RSA, Amsco, Hybridization

1.INTRODUCTION

The transmission of data and information over the public network is very essential aspect. So, the exchange of information has become more desired and a big challenging task. It is necessary to concentrate on the security of the information. In order to get security requirements, different methods (symmetric, asymmetric and hash) of the mathematical cryptography have been developed for data encoding and decoding. Encryption is one of the most effective data security methods which focus on a series of general objectives: confidentiality, integrity, and authentication. One of the ways to strengthen the secureness of cryptography is the hybrid encryption that combines one algorithm with the other. There are many ways to design the hybrid algorithm, combining symmetric and symmetric cryptography, combining symmetric and asymmetric cryptography, or combining asymmetric and hash cryptography, or perhaps there is another way. Hybrid cryptography merges the best advantages of multiple ciphers.

M G Ristiana, and et al. [1] presented hybrid algorithm of RSA and one time pad cryptography. Chipertext from the algorithm was not only one, but there were two chipertext. Chipertext from plaintext was guaranteed by one time pad key, and chipertext from one time pad key was guaranteed by RSA public key because the secureness was guaranteed. The algorithm would cover the weakness of one time pad cryptography by the RSA Crytography. Mahbuba Begum, and et al. [2] proposed a hybrid cryptosystem using DNA, one time pad and RSA. The hybrid approach was to generate a random secret key for a symmetric cipher, and then this key was encrypted via an asymmetric cipher. In this cryptosystem, each letter of the alphabet was transformed into a various combination of the four bases which make up the human deoxyribonucleic acid (DNA). The encryption and decryption time were measured for different plaintext size.

Gaurav R. Patel, and Prof. Krunal Panchal [3] introduced hybrid approaches by combining RSA and DiffieHellman algorithms. RSA was used for encryption and decryption process. The Diffie Hellman was used to generate the secret key. In this model, bitwise XOR operation was added to increase the complexity of the message after the message was converted into cipher text. The encryption and decryption time were compared for RSA and the hybrid model. They concluded that this model is more secured than RSA, because of XOR concept. Dr. Sheetalrani R. Kawale [4] developed the hybrid

cryptography using RSA and DES algorithm for providing better message security. RSA was used to perform key encryption and DES was used for data encryption. Various approaches (RSA-AES, RSA-3DES, RSA-DES) were compared based on ciphering time and memory consumption. They concluded that combination of DES and RSA is the most efficient algorithm among all the respective hybrid techniques.

2. BACKGROUND THEORY

In this section, the operation of RSA algorithm is presented and the about of Amsco cipher is described in detail.

2.1. RSA algorithm

RSA is a public key algorithm invented by Rivest, Shamir and Adlemanin 1978. Public key cryptography refers to a cryptographic system requiring two separate keys, one of which is secret and one of which is public. The RSA cryptosystem is based on the dramatic difference between the ease of finding large primes and the difficulty of factoring the product of two large prime numbers. The key used for encryption is different from the key used for decryption, but the two parts of the key pair are mathematically linked. The algorithm is based on modular exponentiation [5].

The structure of algorithm is described as follows:

- Select two random prime integers: p and q.
- Compute n and Φ (n): n = pq and Φ (n) = (p – 1)(q – 1).
- Choose an integer e, 1 < e < Φ (n) such that: gcd(e, Φ (n)) = 1 (where gcd means greatest common denominator)
- Compute d, 1 < d < Φ such that: ed ≡ (1 mod Φ (n)).
- The public key is (n, e) and the private key is (n, d), the values of p, q and Φ (n) are private, e is the public or encryption exponent, d is the private or decryption exponent [6].

After creating public and private keys, message is encrypted with the public key and decrypted with private key. The encryption and decryption processes of RSA are shown in Figure 1. In the encryption process, ciphertext C is obtained by the equation: $C = M^e \bmod n$, where M is the original message. In the decryption process, message M can be obtained from the ciphertext C by the equation; $M = C^d \bmod n$ [6].

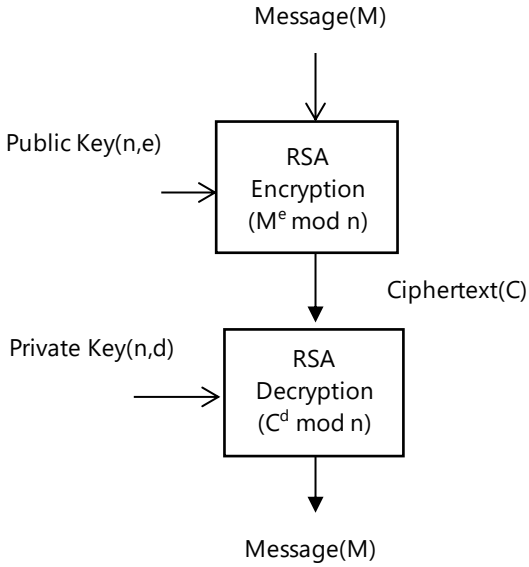

Figure 1. Encryption and Decryption Processes of RSA Algorithm

2.2. Amsco cipher

A transposition cipher, called columns permutation, is a technique to change the order of letters in a text by placing it in a grid. Amsco is a transposition cipher which adds cutting sequence. Cutting sequence may be (1, 2) that is alternation of 1 letter then 2 letters, or (2, 1) that is alternation of 2 letters then 1 letter. It is created by A. M. Scott in 19th century. It has two main components; plaintext and numeric key. The key must be maximum length of 9 and must contain the number 1to n, where n refers to length of key. For encryption, the plaintext is filled consecutive chunks of cutting sequence into n columns of a grid. The resulting permuted plaintext is read of the grid in columns, in order of the key. Then, the final ciphertext is obtained [7].

1	2	3
hy	b	ri
d	cr	y
pt	o	gr
a	h	y

Figure 2. Encryption Grid of Amsco

For decryption, the ciphertext is written in the columns of grid following the order of the columns indicated by the key with the use of cutting sequence. The plaintext is getting back by reading the grid in rows. For instance, plaintext is "hybrid cryptography" with a cutting sequence (2, 1) and key is 312. As the encryption grid of Amsco shown in Figure 2, ciphertext is "riygryhydptabcroph".

3.ARCHITECTURE OF THE SYSTEM

This session expresses the proposed Amsco-RSA algorithm and implementation of the system. And then, the results of performance analysis of algorithms are discussed in this session.

3.1. The proposed RSA-Amsco algorithm

The flowchart of the hybrid encryption process with RSA and Amsco is shown in Figure 3.

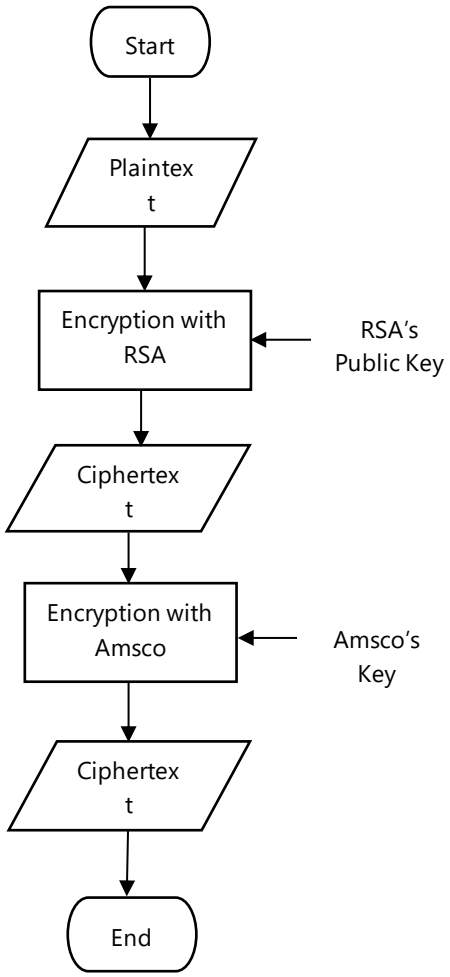

Figure 3. Hybrid Encryption Process with RSA - Amsco

A hybrid approach provides a solution that guarantees to improve the confidentiality, integrity and authenticity of the data. In order to enhance the security of the hybrid algorithm, different types of ciphers can be combined. The proposed hybrid algorithm is created by merging asymmetric RSA with symmetric Amsco cipher. For both encryption and decryption processes, double encryption and decryption functions are performed. To generate the ciphertext, the original message is encrypted in two times; first time with RSA, and next with Amsco. The decryption process is the reversed order of encryption process. To get back the original message, the ciphertext is also decrypted in two times, first time with Amsco, and next with RSA.

3.2. Implementation of the system

In this section, the encryption and decryption of RSA-Amsco algorithm is implemented with the help of Java Programming Language. In encryption process, the plaintext message can be encrypted by entering inputs (message and key) in the respective text boxes with the use of corresponding buttons. The system evaluates the processing time in milliseconds and memory usage in kilobytes to compare the original RSA and Amsco algorithms.

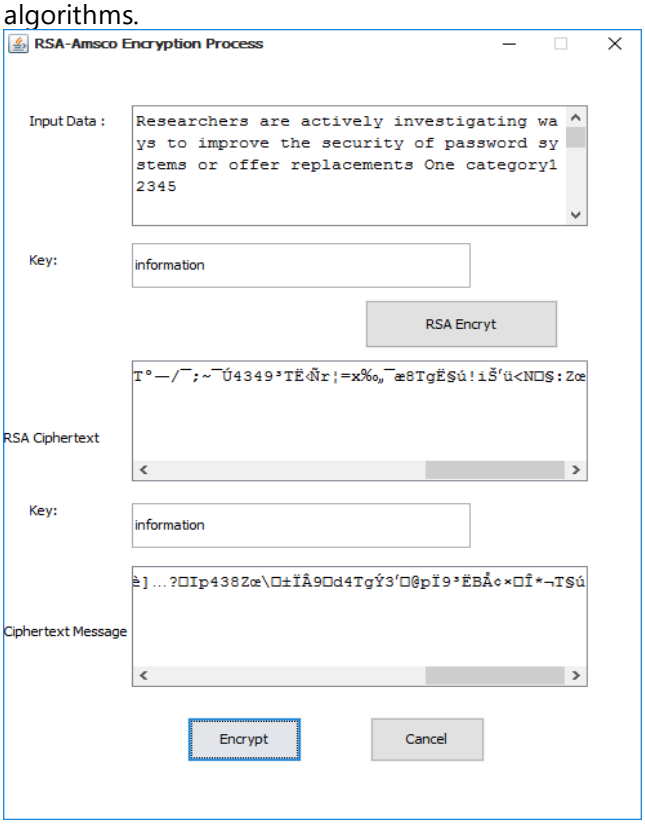

Figure 4. Encryption Process of RSA-Amsco

In RSA-Amsco encryption, the plaintext message is encrypted by the use of RSA public key with length of 1024-bit. And then, RSA ciphertext is generated. After that, this ciphertext is encrypted again by the Amsco to get the desired RSA-Amsco ciphertext. The RSA-Amsco encryption process can be seen as shown in Figure 4.
Under the decryption process, the ciphertext is decrypted with first by Amsco, and second by RSA private key to recover the original message without any changes. The RSA-Amsco decryption process and the recovered original message can be seen in Figure 5.

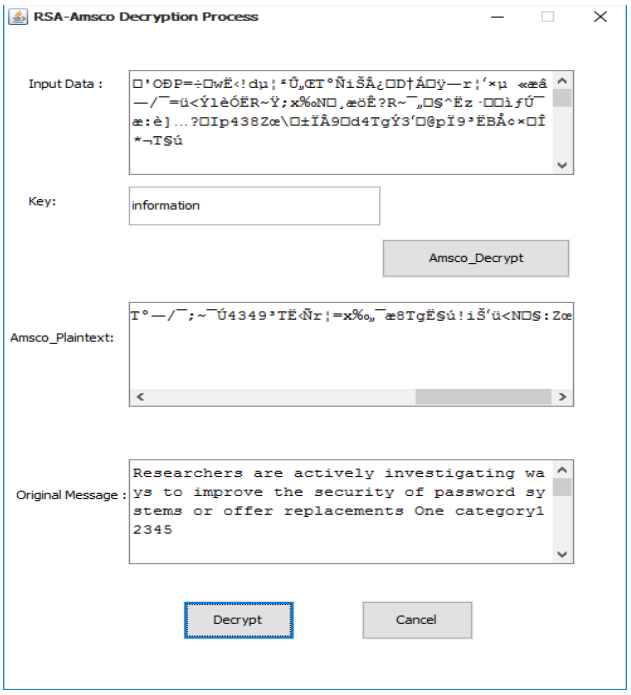

Figure 5. Decryption Process of RSA-Amsco

4. EXPERIMENTAL RESULTS

This session includes the performance comparison of RSA, Amsco and RSA-Amsco algorithms, and evaluation of avalanche effect for RSA-Amsco algorithm to prove the strength of secureness.

4.1. Comparison results of three algorithms

The experimental results of RSA, Amsco and RSA-Amsco algorithms are compared in this session. The performance evaluation of each algorithm can be seen as shown in Figure 6. From this Figure, comparison results can be viewed by the use of corresponding button (Time Graph, Memory Graph).

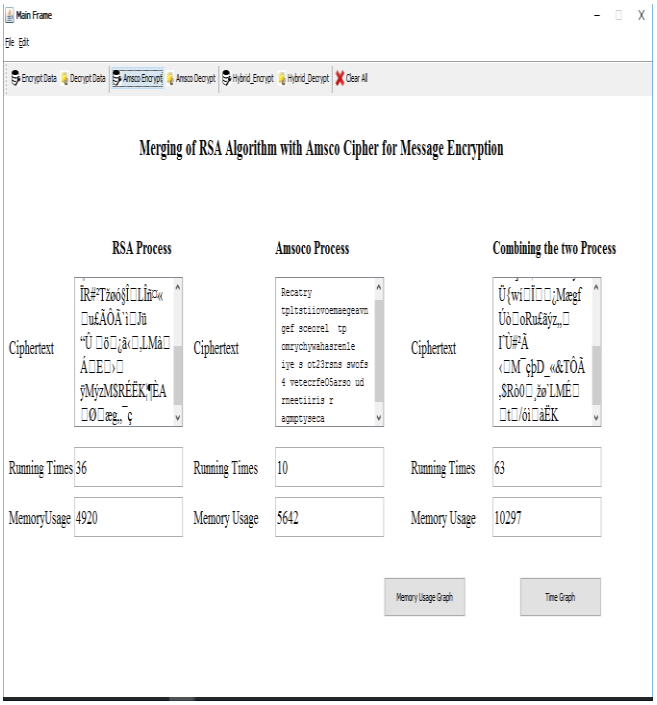

Figure 6. The Performance Evaluation of Each Algorithm

The comparison of running time can be seen in Figure 7. According to the results, the RSA-Amsco encryption takes the longest time among these three algorithms because it performs double encryption process over plaintext message, and Amsco is the fastest cipher because it performs only transposition function.

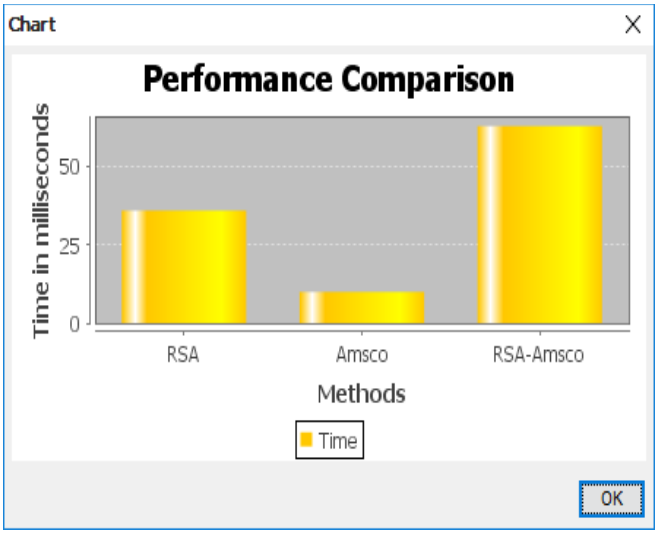

Figure 7. The Comparison of Running Time

The comparison of memory usage is illustrated as shown in Figure 8. Based on the results, the RSA-Amsco

encryption consumes the highest memory among these three algorithms.

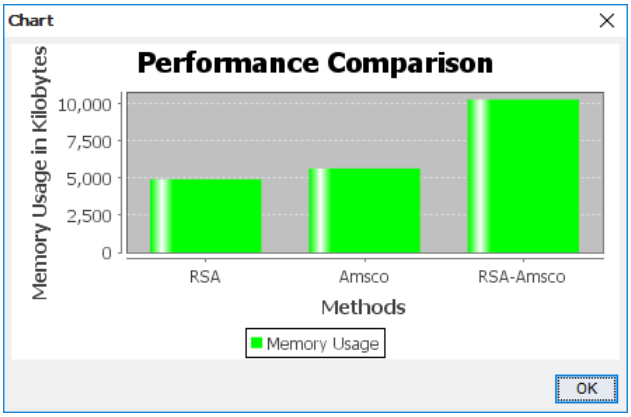

Figure 8. The Comparison of Memory Usage

4.2. Evaluation of avalanche effect

The avalanche effect is the considered necessary characteristic of cryptographic techniques, generally block ciphers and hash functions. If an input is changed slightly, the output will change significantly. In order to strengthen the quality of ciphers, such a small change in either the key or the plaintext should cause a drastic change in the ciphertext. The avalanche effect is calculated by the following equation;

$$\text{Avalanche Effect} = \frac{\text{Number of flipped bits in cipheretext}}{\text{Number of bits in ciphered text}}$$

Here, it is used the small changes of plaintext and key to calculate the avalanche effect. For example, the plaintext "Information Technology Engineering" and the key "engineering" are used to calculate the avalanche effect.

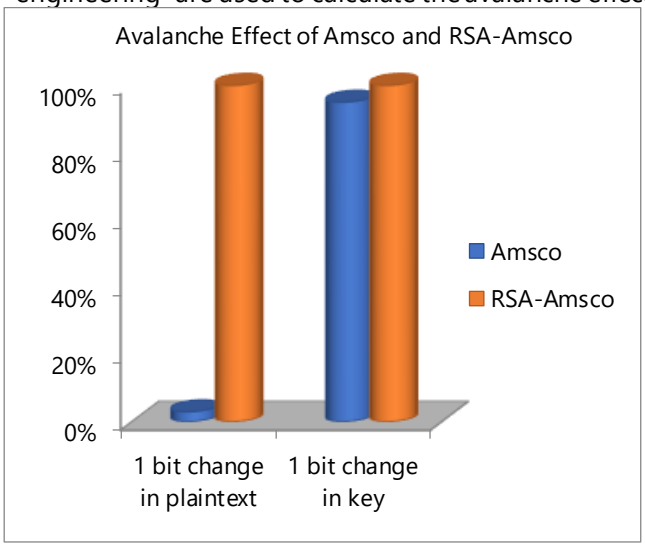

Figure 9. Evaluation Results of Avalanche Effect

In the result of changing one bit in plaintext and keeping the key constant, Amsco supports 3% avalanche effect whereas RSA-Amsco supports 100%. In changing one bit in the key and keeping the plaintext constant, Amsco has 95% whereas RSA-Amsco has 98%. In both cases, RSA-Amsco algorithm provides the higher percentage of avalanche effect. This algorithm can cover the weakness of Amsco cryptography by RSA cryptography. The evaluation results of avalanche effect are shown in Figure 9.

5. CONCLUSION

This paper presents the hybrid cryptography with the combination of RSA and Amsco cipher. RSA uses random prime numbers to generate key pair before encryption process, so it takes long time. The system calculates the performance measurement of RSA, Amsco and RSA-Amsco encryption in terms of running time and memory usage. In both comparisons, the RSA-Amsco consumes more time and memory usage as compare to original RSA because RSA-Amsco merges two different techniques of cryptography. Whereas RSA-Amsco is more secured cryptography algorithm than original RSA, because RSA-Amsco includes Amsco's transposition concept, which is more difficult for the intruder to find the plaintext from the secrete message.

6. ACKNOWLEDGEMENT

The author wants to express her thanks to the experts who have contributed towards development of the paper.

REFERENCES

[1] M G Ristiana, R Marwati and S M Gozali, "Hybrid algorithm of RSA and One Time Pad Cryptography", 2018.
[2] Mahbuba Begum, JannatulFerdush and Md. GolamMoazzam, "A Hybrid Cryptosystem using DNA, OTP and RSA", International Journal of Computer Applications (IJCA), Vol. 172 (8), 2017.
[3] Gaurav R. Patel, and Prof. KrunalPanchal, "Hybrid Encryption Algorithm", International Journal of

Engineering Development and Research (IJEDR), Vol. 2 (2), 2014.
[4] Dr. Sheetalrani R. Kawale, "Message Security Using RSA-DES Hybrid Cryptography ", IOSR Journal of Computer Engineering (IOSR-JCE), Vol. 21 (2), 2019.
[5] M. Preetha, and M. Nithya, "A Study and PerformanceAnalysis of RSA Algorithm", International Journal of Computer Science and Mobile Computing (IJCSMC), Vol. 2 (6), 2013.
[6] HüseyinBodur and Resul Kara, "Secure SMS Encryption Using RSA Encryption Algorithm on Android Message Application", 2015.
[7] MalteNuhnand Kevin Knight, "Cipher Type Detection", 2012.