INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2022, VOL. 68, NO. 3, PP. 475-481
Manuscript received July 13, 2022; revised August, 2022. DOI: 10.24425/ijet.2022.141263

Program for Simulation and Testing of Apply Cryptography of Advance Encryption Standard (AES) Algorithm with Rivest-Shamir-Adleman (RSA) Algorithm for Good Performance

Santi Pattanavichai

***Abstract*—Nowadays, information security management systems are important parts of managing a system for better handling of the information security. In scenarios and situations where safety management is done by managing protection of malwares, it is important to manage security issues properly. Cryptography is an approach which makes possible for a recipient to encrypt and decrypt the information. A combination of two different strategies for encryption and decryption in the text encoding will be transformed into the used all content. The encryption and decryption key of the content decryption key is used. There are different types of information. A number, such as finding two large prime numbers with that product. The number, the size of the RSA key is large enough to make, it's hard to pinpoint these numbers. The key, known as the RSA public key, is the most prominent open encryption. Calculations were used for information exchange. In this paper, we created a program for simulation and testing of apply cryptography of Advance Encryption Standard (AES) algorithm with Rivest-Shamir-Adleman (RSA) algorithm for better performance. In this study, this program is an application of a new algorithm to be the AES&RSA principle of using a public key instead of a private key for cryptography, and the testing of encryption and decryption for the AES&RSA algorithm resulted in time is no different on the AES algorithm and more secure encryption and decryption. The results indicated that the time needed for encoding and decoding of AES&RSA algorithm has been reduced (i.e., efficiency has been improved).**

***Keywords*—Information Security Management System (ISMS); Cryptography; Encryption; Decryption; Advance Encryption Standard (AES); Rivest-Shamir-Adleman (RSA)**

I. Introduction

NOWADAYS, information security management systems ISMS) are the one method importance in all manage system for the information security. In which safety management is in terms of managing protection about malware, it is important to manage security. ISO / IEC 27001 is the best international standard for managing corporate information security systems. They can create strategies and set directions for assessment. Measuring and preventing external threats through the standard risk management process. The aim of this standard is ISO / IEC 27001 is to provide organizations with adequate and systematic management of safety measures appropriate for the organization's operations. Initially, the organization has to do a risk analysis of the system against threats and various weaknesses in the system, and then analyze and select a control approach and protect various information appropriately and completely, in which the standard will have a guideline called the Code of Practice to be used to control various risks, while this standard also requires the organization to control the security system and a mechanism for continuous development as well and cryptography is one of the principles of the security standard in ISO 27001. Information security management system The security standard in ISO 27001 has three qualifications

1) *Cconfidentiality a feature that information will not be published or disclosed to unauthorized persons, businesses or processes.*
2) *Integrity, properties of protecting the correctness and completeness of assets*
3) *Availability of properties that can be accessed and used on demand. The company is authorized by ISO / IEC 27001 standard to protect the organization by using 3 layers of protection:*

As information becomes more important, information-security management becomes mandatory. Therefore, all of the organizational stakeholders at each level, e.g., staff, management, and board, must be aware of information security [1].

Another interruption to data security is when certainty occurs. The information is accessed by unauthorized persons with spyware. Viruses, malware, denial-of-service attacks, or ransomware [2]. Various motives can stimulate unauthorized access. Information including abuse of authority change information about data theft activities, or /a playful reason [3].

User to access information Users who lack safety knowledge or awareness also increase their potential. For interrupting information security [4] information security. Interruptions can occur from an unlimited type of media, ranging from manual ones such as mobile flash drives. Network infrastructures such

This research was financially supported by Rajamangala University of Technology Thanyaburi, RMUTT.

Author is with Rajamangala University of Technology Thanyaburi, Information Technology Department, Thailand (e-mail: pattanavichai@gmail.com).

© The Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0, https://creativecommons.org/licenses/by/4.0/), which permits use, distribution, and reproduction in any medium, provided that the Article is properly cited.

as LAN, WAN and the Internet and various bring your own equipment options [5].

Cryptography is the peculiarity of concealing it. A way that only the intended recipient can decrypt the information. A combination of two different strategies - coding and decryption in The text encoding will be transformed into the used content image. The encryption and decryption key of the content decryption key is used. For encoding and decoding, the different cipher calculations are used that can be divided into two particular classes. - Symmetric or private key algorithms and asymmetric or public key calculation symmetric key calculations use a single key to scramble and decrypt additional information through the public key Calculation [6,7] uses two unique keys for encryption and decrypting the encryption key is known as the private key and its decryption. The key, known as the RSA public key, is the most prominent open encryption. Calculations that are used for information exchange [8].

There are different types of information. Use encryption algorithms such as AES, RSA, DES, 3DES [9,10] which is used in binary or text data. In the Cryptography Process, it is considered an important process of information security management systems (ISMS). Cryptography is the science that studies how data is stored or secure message when sending from sender to file of recipients without third party intervention accordingly. Bruce Scheiner said cryptography is the science and art of keeping messages safe [11].

In 2012, D. Chen used the Chaotic Logistic Map to generate the keys of AES algorithm, which reduces the correlation of round keys and improves the durability of the algorithm [12].

RSA works on the mathematical concept of very large factorization. A number, such as finding two large prime numbers with that product. The number, the size of the RSA key is large enough to make, it's hard to pinpoint these numbers. This makes factor very time consuming despite using well known algorithms. RSA security measures greatly depend on the size of the keys used. which adds randomness to determine the factor of the number [13,14]? In cryptography we used modified AES algorithm to encrypt data by using RSA algorithm security measures.

This paper is organized as follows. Section I introduces the topic and elaborates on the background of this study. Section II describes previous studies related to Advance Encryption Standard (AES) algorithm and Rivest-Shamir-Adleman (RSA) algorithm. Section III discusses the proposed the program for simulation of testing about apply Advance Encryption Standard (AES) algorithm with Rivest-Shamir-Adleman (RSA) algorithm, and Section IV describes the performance of simulation for testing application about apply Advance Encryption Standard (AES) algorithm with Rivest-Shamir-Adleman (RSA) algorithm and evaluation results. Finally, Section V, we discuss the conclusions and proposed future work.

II. Literature Reviews

A. *Advance Encryption Standard (AES)*

AES is a code block intended to replace 3DES for commercial applications use 128-bit blocks [15]. This 128,192 or 256-bit key size and size, the standard is based on the Rijndael algorithm [16-17], a symmetric block code AES algorithm used three different key lengths These three are called "AES-128", "AES-192" and "AES-256".

The AES (Advance Encryption Standard) algorithm is widespread to use in various fields due to its high security, efficiency, high efficiency and flexibility. The AES algorithm is packet encryption format Each time encode a plain text size. It is 128 bits, 128 bits of plain text, divided into 4*4 state matrices. Status and secret codes are obtained after several rounds of encryption has three key lengths: 16 bytes, 24 bytes, and 32. Bytes of The AES encryption process consists of four steps: SubBytes, ShiftRows, MixColumns and AddRoundKey [18].

In the first round, AddRoundKey is recognized and in around; It is mainly divided into the following steps:

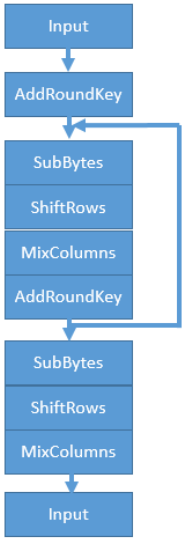

Fig.1. AES encryption algorithm flow chart

In the AES algorithm, the encryption algorithm uses a key that convert the data into unreadable encrypted text, then the decryption procedure uses the same key to convert the cipher-text. And back to original data this type of key is symmetrical. important; Other algorithms require different keys for encryption. and decoding [19].

In Final Round consists of SubBytes, ShiftRows and AddRoundKey. The precise steps involved in the algorithm can be seen in Fig. 1.

In general, the strength of a cryptographic product can be increased by increasing the number of cycles it takes to process the data. The AES standard states that the number of cycles is determined by the length of the numeric key [20,21], as shown in Table I.

TABLE I
KEY LENGTH AND THE NUMBER OF ROUNDS

Key Length	Number of Rounds (Nr)
AES-128	10
AES-192	12
AES-256	14

B. *Advance Encryption Standard (AES)*

The asymmetric RSA encryption algorithm was proposed by Ron Rivest, Ad Shamir, and Leonard Adleman in 1978 and the name consists of the initials of three scholars' surnames [22].

The security of the RSA algorithm depends on the difficulty of many important decompositions [23,24]. The principle of RSA encryption and decryption is as follows: First, the system randomly generates two large prime numbers p and q, and then uses formula (1) to find the key. private and public keys Finally, use formula (2) to encrypt and formula (3) to decrypt.

$$n = p * q, \quad \phi(n) = (p-1)(q-1) \tag{1}$$

$$\gcd(e, \phi(n)) = 1 \tag{2}$$

$$M = Cd \bmod n \tag{3}$$

When dealing with RSA, there are two families of low-cost attacks: single target. At factoring of n (to find prime numbers p and q) or directly recovering d; the other aims at decrypting an encrypted message c without knowing d. A Detailed discussion of AES vs RSA (and others) encryption algorithm) can be found in [25].

Public key-based encryption algorithms use two types of keys for encryption and decryption. For this reason, these algorithms are referred to as asymmetric encryption algorithms. For secure data communication between sender and receiver, the recipient will generate a private and public key. Then the recipient sends the public key to the sender via a secure medium and asks him to initiate communication. Now, using the public key sender encrypts the data and sends a key message to the recipient. with the help of the respective private key. The recipient will decrypt the code message and receive the original message. The entire procedure is shown in Fig. 2 as a flow diagram [26,27].

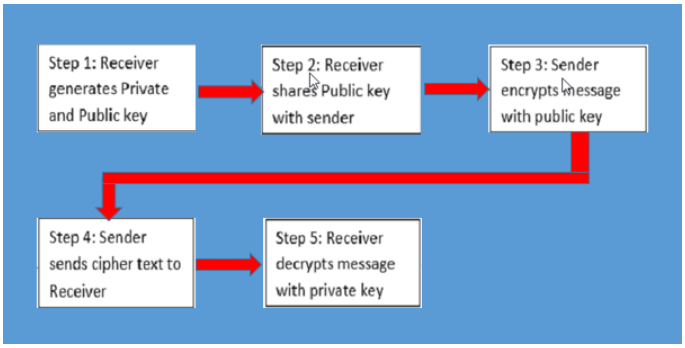

Fig.2. AES encryption algorithm flow chart

III. The Working Structure AES & RSA Joint Algorithm

In this paper, we study the using the AES algorithm in combination with the RSA algorithm, RSA encryption is an asymmetric key encryption algorithm [28]. In cryptography using knowledge of modular arithmetic, public-key cryptography is the most widely used encryption in electronic transactions. Nicks such as identity verification. In digital signature and e-commerce, encryption requires a public key and a private key generated from random numbers. and brought through the process of RSA algorithm [29-30] is shown in Fig. 3.

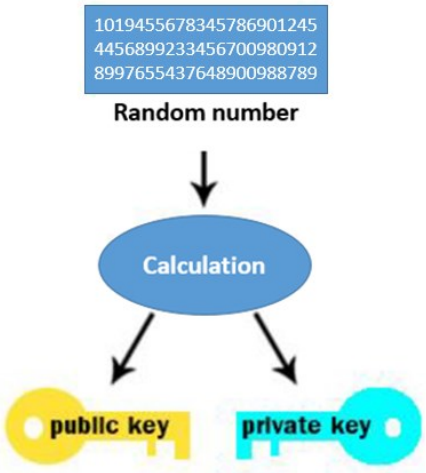

Fig.3. RSA Encryption Procedure

The public key is the one that can be published and shared, but the private key is only available to the recipient. In other words, each person can use the same public key to encrypt, but the decryption depends on the private. the recipient's key to decrypt is shown in Fig. 4.

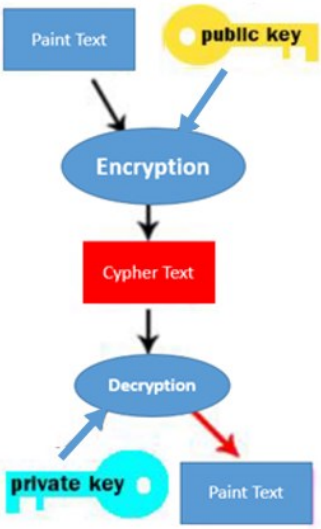

Fig.4. RSA Decryption Procedure

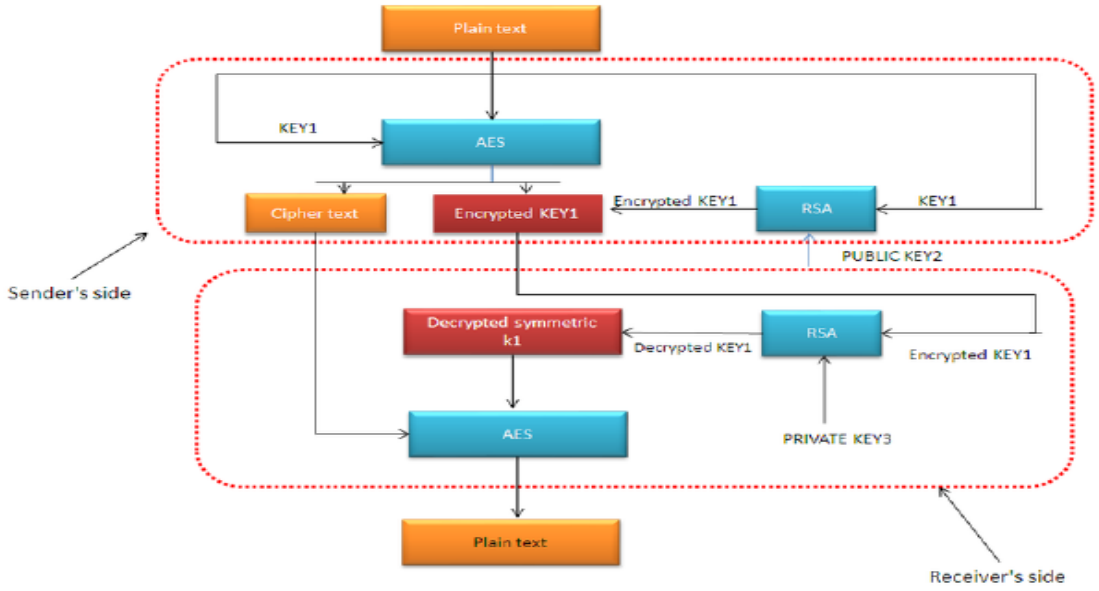

Fig.5. Working Combined AES&RSA Algorithm

We will use the two algorithms together to encrypt and decrypt using the methods and steps as shown in Figure 6. It can be seen that plaintext is used to encrypt using AES algorithm and key. of AES to encrypt with RSA algorithm and then send public key and encrypted data to the destination. The destination has private key to decrypt using RSA algorithm to decrypt the key of AES. AES, where the AES algorithm is intended for data encryption and decryption purposes and RSA is used to encrypt and decrypt the AES key, is shown in Fig 5.

We design and implement AES and AES apply RSA encrypt decryption system by using software with NetBeans Program and test and correct the correctness of the program in order to improve and develop it to be suitable for real use in simulation program.

```
            Key secretKey = new SecretKeySpec(key.getBytes(), "AES");
            Cipher cipher = Cipher.getInstance("AES");
            cipher.init(cipherMode, secretKey);

            FileOutputStream outputStream;
            try (FileInputStream inputStream = new FileInputStream(inputFile)) {
                byte[] inputBytes = new byte[(int) inputFile.length()];
                inputStream.read(inputBytes);
                byte[] outputBytes = cipher.doFinal(inputBytes);
                outputStream = new FileOutputStream(outputFile);
                outputStream.write(outputBytes);
            }
            outputStream.close();

        } catch (NoSuchPaddingException | NoSuchAlgorithmException
                | InvalidKeyException | BadPaddingException
                | IllegalBlockSizeException | IOException ex) {
            throw new CryptoException("Error encrypting/decrypting file", ex); // check for errors
        }
    }

}
```

Fig.6. Source Code for receiving files for AES encryption and decryption algorithm

Source Code for receiving files for AES encryption and decryption algorithm is shown in Fig 6.

```
 * This method is called from within the constructor to initialize the form.
 * WARNING: Do NOT modify this code. The content of this method is always
 * regenerated by the Form Editor.
 */
@SuppressWarnings("unchecked")
// <editor-fold defaultstate="collapsed" desc="Generated Code">
private void initComponents() {

    btnchooser = new javax.swing.ButtonGroup();
    jButton1 = new javax.swing.JButton();
    jButton2 = new javax.swing.JButton();
    jLabel1 = new javax.swing.JLabel();
    btnchoose = new javax.swing.JButton();
    txttotalenc = new javax.swing.JLabel();
    txtlocation = new javax.swing.JTextField();
    jLabel2 = new javax.swing.JLabel();
    jScrollPane1 = new javax.swing.JScrollPane();
    txtenc = new javax.swing.JTextArea();
    txttotaldec = new javax.swing.JLabel();
    jScrollPane2 = new javax.swing.JScrollPane();
    txtdec = new javax.swing.JTextArea();
    rdbtnAES = new javax.swing.JRadioButton();
    rdbtnAESRSA = new javax.swing.JRadioButton();

    setDefaultCloseOperation(javax.swing.WindowConstants.EXIT_ON_CLOSE);

    jButton1.setText("Encrypt");
    jButton1.addActionListener(new java.awt.event.ActionListener() {
        public void actionPerformed(java.awt.event.ActionEvent evt) {
            jButton1ActionPerformed(evt);
        }
```

Fig.7. Source Code to encrypt the common algorithm AES&RSA by encrypting the key and sending the key to the destination

Source Code to encrypt the common algorithm AES&RSA by encrypting the key and sending the key to the destination is shown in Fig 7.

```
    };

    pack();
}// </editor-fold>

private void jButton1ActionPerformed(java.awt.event.ActionEvent evt) {
    if (rdbtnAES.isSelected())
    {
        String filename = txtlocation.getText();
        File outputFile = new File("EncryptedFiles/Encrypted.AES");
        File inputFile = new File(filename);
        byte [] keyaes = null;
        try {
            keyaes = Files.readAllBytes(Paths.get("Onekey/secretKey"));
        } catch (IOException ex) {
            Logger.getLogger(Main.class.getName()).log(Level.SEVERE, null, ex);
        }
        String key = new String(keyaes);
        long starttime = System.currentTimeMillis();
        try {
            AES.encrypt(key, inputFile, outputFile);
        } catch (CryptoException ex) {
            Logger.getLogger(Main.class.getName()).log(Level.SEVERE, null, ex);
        }
        try {
            byte [] s = Files.readAllBytes(Paths.get("EncryptedFiles/Encrypted.AES"));
            String txt = new String(s);
            txtenc.setText(txt);
        } catch (IOException ex) {
            Logger.getLogger(Main.class.getName()).log(Level.SEVERE, null, ex);
        }
```

Fig.8. Source Code for the interface page for encryption and decryption. and timing for encoding and decoding

Source code for the interface page for encryption and decryption. and timing for encoding and decoding is shown in Figure 8.

IV. The Working Structure AES & RSA Joint Algorithm The Performance Of Simulation For Testing Application About Apply Advance Encryption Standard (AES) With Rivest-Sharmir-Adleman(RSA) Algorithm

1. The operation of process 1

To choose AES and AES&RSA algorithm is shown in Fig 9.

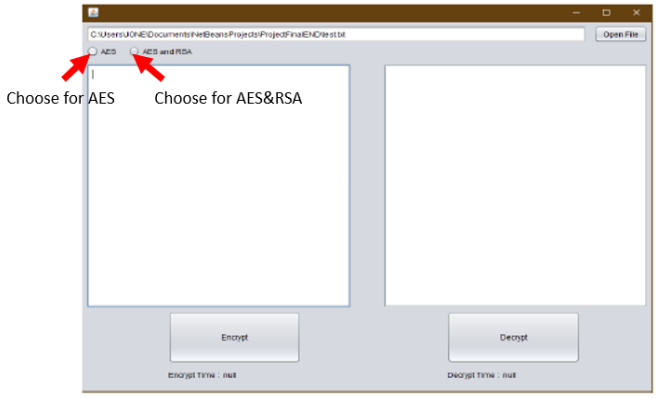

Fig.9. The choosing AES and AES&RSA algorithm

2. The operation of process 2

To encrypt is performed using the AES algorithm is shown in Fig 10.

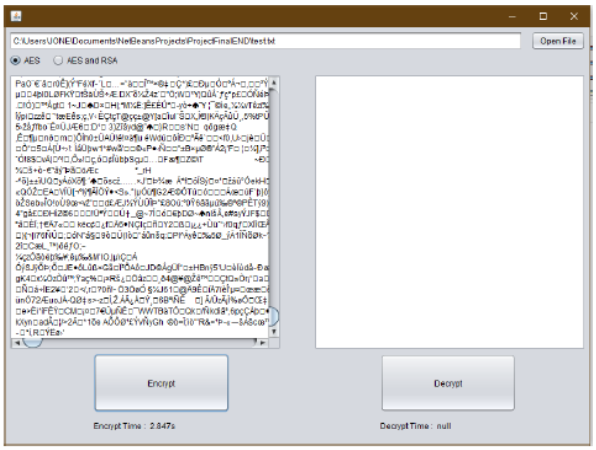

Fig.10. The process of the AES Algorithm in Encryption

3. The operation of process 3

To decrypt is performed using the AES algorithm. is shown in Fig 11.

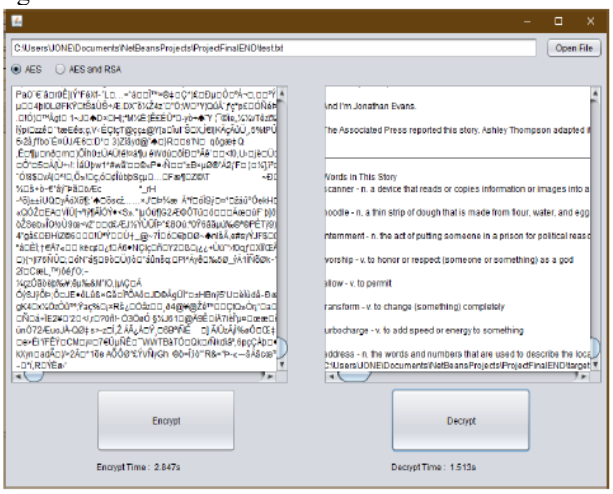

Fig.11. The process of the AES Algorithm in Decryption

4. The operation of process 4

To encrypt is performed using the AES&RSA algorithm is shown in Fig 12.

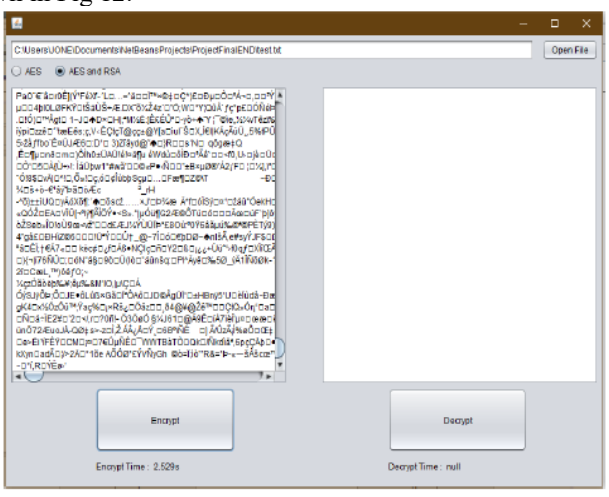

Fig.12. The process of the AES&RSA Algorithm in Encryption

In the testing, we use the file to encrypt and decrypt the file size to be 47,224 KB and there are 100 rounds of testing is shown in Fig 14.

5. The operation of process 5

The last process to decrypt is performed using the AES&RSA algorithm.is shown in Fig 13.

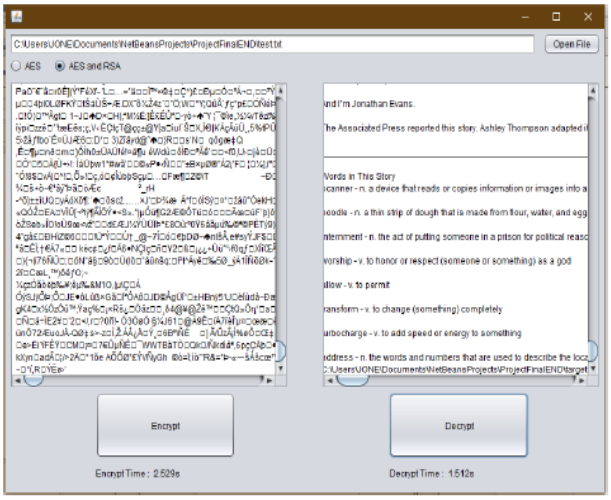

Fig.13. The process of the AES&RSA Algorithm in Decryption

Testing	Time(s)			
Key Size 128bit	AES		AES & RSA	
	Encrypt	Decrypt	Encrypt	Decrypt
1	3.547	1.891	2.973	1.447
2	2.91	1.799	2.628	1.385
3	2.653	1.646	2.551	1.411
4	2.754	1.422	2.566	1.379
5	2.785	1.617	2.533	1.373
6	2.683	1.332	2.674	1.356
7	2.407	1.462	2.58	1.368
8	2.449	1.856	2.548	1.409
9	2.146	1.878	2.529	1.41
10	2.118	1.857	2.558	1.376
91	2.662	1.435	2.621	1.431
92	2.859	1.434	2.638	1.451
93	2.895	1.484	2.68	1.436
94	2.67	1.562	2.671	1.467
95	2.81	1.441	2.864	1.436
96	2.704	1.423	2.609	1.414
97	2.631	1.441	2.647	1.447
98	2.87	1.448	2.841	1.446
99	2.628	1.444	2.623	1.426
100	2.956	1.534	2.652	1.443
Total	259.237	146.851	257.792	139.919
Averge Time	2.59237	1.46851	2.57792	1.39919

Fig.14. 100 rounds of testing

The performance of simulation for testing application about apply Advance Encryption Standard (AES) algorithm with Rivest-Shamir-Adleman (RSA) algorithm to compare between AES algorithm and AES&RSA algorithm the time for encrypting and decrypting can be shown in Figure 26. The average time for encrypting 100 rounds of testing of AES algorithm is 2.59237 s and The average time for decrypting 100 rounds of testing of AES algorithm is 1.46851 s. The average time for encrypting 100 rounds of testing of AES&RSA algorithm is 2.57792 s and The average time for decrypting 100 rounds of testing of AES&RSA algorithm is 1.39919 s. Which the result of comparing between AES algorithm and AES&RSA algorithm, you can see the interval has a reduced value time both of the encrypting and decrypting for AES&RSA algorithm and more secure encryption and decryption.

CONCLUSION

The main objective of this paper is to study to find new algorithms in order to obtain high-security algorithms. and the time it takes to encrypt and decrypt which is not different from AES algorithm. This paper focuses on simulation of a program through encryption and decryption to compare 2 algorithms between AES algorithm and AES&RSA algorithm. In this work, we initially studied the working principles of AES and RSA algorithms, and then we created the simulation of a program based on the encryption and decryption methods.

In other words, in this study, we designed and implemented the AES and RSA algorithms and we applied the AES&RSA algorithm for encryption and decryption system by using software running with the NetBeans program. Subsequently, we tested and evaluated the accuracy of the program in order to improve and develop it to be suitable for real-life situations and scenarios. The AES algorithm was chosen because of its popularity worldwide. The RSA algorithm also was chosen because of its high security regarding the encryption and decryption processes.

However, execution speed of the commands depends on the equipment and specifications of computers used and their operating speed. In cases when a slow computer is used, the experiment may let the computer freeze both in normal mode and Safe Mode.

In the future work, we will apply this simulation program on other algorithms such as; 3DES (Data Encryption Standard), Diffie-Hellman, and TwoFish, etc., with the intention of finding the best method which can be used in testing, encryption and decryption processes resulting in the highest level of security possible.

ACKNOWLEDGEMENTS

This study was approved by the university human research ethics committee and all procedures performed in studies involving human participants were in accordance with the ethical standards of the institutional and/or national research committee and with the 1964 Helsinki declaration and its later amendments or comparable ethical standards.

Informed consent was obtained from all individual participants included in the study.

The authors report no conflicts of interest.

The author confirms sole responsibility for the following: study conception and design, data collection, analysis and interpretation of results, and manuscript preparation.

REFERENCES

[1] J. W. Candra, O. C. Briliyant, and S. R. Tamba, “ISMS planning based on ISO/IEC 27001:2013 using analytical hierarchy process at gap analysis phase (Case study: XYZ institute)”, in Proceedings of the 2017 11th International Conference on Telecommunication Systems Services and Applications, TSSA 2017, 26-27 Oct. 2017.

[2] M. Button, “Cyber Security Breaches Survey 2016”, Department for Digital Culture Media and Sport, 2018, https://doi.org/10.13140/RG.2.1.4332.6324

[3] F. G. I. T. U.S. Congress, Office of Technology Assessment, Electronic Record Systems and Individual Privacy, June, (1986) https://doi.org/10.1016/0167-4048(86)90061-1

[4] H. W. Glaspie and W. Karwowski, “Human Factors in Information Security Culture: A Literature Review”, in Proceedings of the AHFE 2017 International Conference on Human Factors in Cybersecurity, 2017, pp. 269-280.

[5] A. Retnowardhani, R. H. Diputra, and Y. S. Triana, "Security risk analysis of bring your own device (BYOD) system in manufacturing company at Tangerang", TELKOMNIKA (Telecommunication Comput. Electron. Control.), vol. 17, no. 2, 2019, pp. 753-762.

[6] A. J. Menezes, S. A. Vanstone, and P. C. V. Oorschot, Handbook of Applied Cryptography, FL, USA, CRC Press, Inc., Boca Raton, 1996.

[7] W. Diffie, and M. Hellman, "New directions in cryptography". IEEE Transactions on Information Theory, vol. 22, no. 6, 1996, pp. 644–654.

[8] R. Saxena, M. Jain, D. Singh, and A. Kushwah, "An enhanced parallel version of RSA public key crypto based algorithm using openMP", Proceedings of the 10th International Conference on Security of Information and Networks, 2017, pp. 37–42,

[9] S. Lian, Multimedia Content Encryption: Techniques and Applications, Taylor & Francis Group, LLC, 2008.

[10] R. A. Mollin, An introduction to cryptography, FL USA, CRC Press Boca Raton 2006.

[11] B. Schneier, Applied cryptography Protocols, algorithm, and source code in C, Wiley, 1996.

[12] D. C hen, D. Qing, and D. Wang "AES Key Expansion Algorithm Based on 2D Logistic Mapping[C]", / Fifth International Workshop on Chaos-Fractals Theories and Applications. IEEE Computer Society,2012, pp. 207-211.

[13] J. Bajard, and L. Imbert. "A full RNS implementation of RSA", 2004. IEEE Transactions on Computers, vol. 53, no. 6, pp. 769-774, 2004.

[14] L. Rivest, A. Shamir, and L. Adleman. "A method for obtaining digital signatures and public key cryptosystems", 1978. Communications of the ACM, vol. 21, no. 2, pp. 120-126, (Feb. 1978).

[15] Federal Information Processing Standards Publication 197(FIPS197), http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf , 2001

[16] J. aemen, and V. Rijmen, "The block cipher Rijndael", Smart Card Research and Applications, pp. 288–296, 2000.

[17] P.C. Kocher "Timing attacks on implementations of diffie-hellman, RSA, DSS, and other systems". In: Koblitz, N. (ed.) CRYPTO 1996. LNCS, vol. 1109, pp. 104–113. Springer, Heidelberg (1996).

[18] V M Silva-García, R. Flores-Carapia, C. Rentería-Márquez et al. "Generating substitution boxes with 104 non-linearity for AES using chaos[J]", Applied Mathematical Sciences, vol. 10, no. 1, pp.151-166, 2016, https://doi.org/10.12988/ams.2016.511695

[19] J. Daemen and V. Rijmen, The Design of Rijndael: AES The Advanced Encryption Standard, Springer-Verlag, 2002.

[20] R. F. Shao, Z. Chang, and Y. Zhang, "AES Encryption Algorithm Based on the High Performance Computing of GPU", 2010 Second International Conference on Communication Software and Networks, pp. 26-28, 2010, https://doi.org/10.1109/ICCSN.2010.124

[21] D. Smekal J. Frolka, and J, Hajny, "Acceleration of AES Encryption Algorithm Using Field Programmable Gate Arrays", IFAC-Papers OnLine, vol. 49, no. 25, pp. 384–389, 2016.

[22] R.L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystem", Commun. ACM, vol. 21, pp. 120–126, 1978, https://doi.org/10.1145/359340.359342

[23] J. Katz, A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, Handbook of applied cryptography., CRC press, 1996.

[24] A. Lasheras, R. Canal, E. Rodríguez, and L. Cassano, "Lightweight protection of cryptographic hardware accelerators against differential fault analysis", in: 2020 IEEE 26th International Symposium on On-Line Testing and Robust System Design (IOLTS), pp. 1–6, 2010, https://doi.org/10.1109/IOLTS50870.2020.9159720

[25] A. Barenghi, L. Breveglieri, I. Koren, and D. Naccache, "Fault injection attacks on cryptographic devices: theory", practice, and countermeasures, Proc. IEEE, vol. 100, no. 1, pp. 3056–3076., 2012, https://doi.org/10.1109/JPROC.2012.2188769

[26] R. Saxe, M. Jain, D. Singh, and A. Kushwah, "An enhanced parallel version of RSA public key crypto based algorithm using openMP", Proceedings of the 10th International Conference on Security of Information and NetworksOctobe, pp. 37–42, 2017, https://doi.org/10.1145/3136825.3136866

[27] F, Sonmez, and M. K. Abbas, "Development of a Client / Server Cryptography-Based Secure Messaging System Using RSA Algorithm", Journal of Management Engineering and Information Technology, vol. 4, no. 6, pp. 2-6., 2017

[28] R. Karri et al., "Fault-based side-channel cryptanalysis tolerant rijndael symmetric block cipher architecture", Proceedings 2001 IEEE Int. Symp. on Defect and Fault Tolerance in VLSI Systems, pp. 427-435, Oct 2001, https://doi.org/10.1109/DFTVS.2001.966796

[29] G. Singh, "A study of encryption algorithms (RSA, DES, 3DES and AES) for information security", International Journal of Computer Applications, vol. 67, no. 19, pp.33-38, 2013, https://doi.org/10.5120/11507-7224

[30] S. Pavithra and Mrs. E. Ramadevi, "Performance Evaluation of Symmetric Algorithms", Journal of Global Research in Computer Science, vol 3, no. 8, pp. 43-45, August 2012.