Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 10, Issue. 4, April 2021, pg.132 – 138

Encryption and Decryption (File Cryptography with AES and RSA for Mobile Based on Android)

Ahire Mitali[1]; Sayyed Ayesha[2]; Kadri Kaynat[3]; Aher Tuika[4]; Prof. Priti Kudal[5]
[1,2,3,4]Student, Department of Computer Engineering, Guru Gobind Singh Polytechnic, Indira Nagar Nashik
[5]Lecturer, Department of Computer Engineering, Guru Gobind Singh Polytechnic, Indira Nagar Nashik
[2] Sayyedayesha906@gmail.com
[3] kaynatkadri423@gmail.com
[4] shrimantganesh@gmail.com
[1] mitaliahire9767@gmail.com
DOI: 10.47760/ijcsmc.2021.v10i04.018

Abstract: The users of mobile based on android were increasing currently even now mobile was almost the same computer one of which could be used to be done by every users mobile was save the individual important data. Saving the data on mobile was very risk because become hackers' target. That was the reason of researchers want to add cryptography which the combination between Advance Encryption System (AES) dan Ron Rivest, Adi Shamir dan Len Adleman (RSA). The result of the second method above could do cryptography data on mobile. With different encryption time where the file size; 25.44 KB, encryption time 4 second, 200 KB, 5 second, 600 KB 7 second, 2.29 MB, 10 second. Where decryption 25.44 KB, encryption 2 second, 200 KB, 1.5 second, 600 KB 2.5 second, 2.29 MB, 2.7 second.

1. Introduction

Mobile which was using application of android will be needed to satisfy social expectations which was connecting and social needs now days the reason of increasing Smartphone usage. One of the leader of
Smartphone was Google Android system operation. It can be possible that Android will be installed on many phones in the near future [1-3].Android has every system smartphone operation, security was one of attention mobile users nowadays, smartphone mobile very often

© 2021, IJCSMC All Rights Reserved

virus attack etc [4]. Every person was using Smartphone like PC to save private our individual and data PC to save and individual data or secret.

Smartphone become the main point of hackers attack particularly android operation system of Smartphone. The previous researchers have done the comparison RSA, AES and DES and the result of this research showed that AES and DES needed little time and little memory, while RSA needed the long time and the using big memory, but in the giving strong key than DES and AES method [5]. The previous researchers have done in connecting algorithm of DES and RSA and showing stronger than using one method only [6-12]. Based on increase in mobile application in many platforms, security was the most necessary in issue, monitoring, security, reliability and accurate [13]. The previous researchers have ever done research to compare AES and RSA to encrypt the data in web [14-15].

In this research, there would be make an application that did the security data in mobile that android with RSA and AES method, the application could be download in play store so it was easier to Smartphone user to download on the individual mobile and developing the previous EKG.

2. Method

The RSA algorithm is the most popular and proven asymmetric key cryptographic algorithm; it can contrary to password attack to present. RSA comes from the founder name, the first algorithm encryption and digital signature. The security is in the two prime number count math from two big of the number. In RSA, two algorithm number used to making two public and private key. It was hard to know the original message from the signal key. It was safe from brute force attack too [16-19].

3. Algorithm Advanced Encryption

AES standard was block cipher where the length of this block was 128 bit. AES enable to three the different key long: 128, 192 or 256 bit. Encryption consists of 10 rounds processing to 128 key bit, 12 round for 192 bit and 14 round for 256 bit. Every round processing consists of one single – byte substitution based on steps, wisdom-line, step permutation, wisdom column mix step and beside of the general round.

The four steps were running in different encryption and decryption. It was not the same like DES, algorithm different decryption based on substantial from algorithm encryption. Even though from all steps were the same step that used in encryption, the steps that done was different with before [20-21]. All the planning of algorithm was public (not a secret) the long of key flexible; 128, 192 and 256 bit, the block measure that encryption was 128 bit, algorithm could be implicated in software or hardware [22].

© 2021, IJCSMC All Rights Reserved

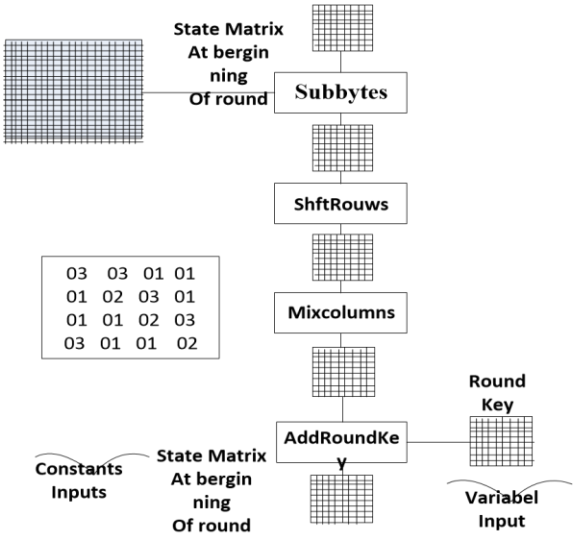

Figure 1. Input For Single AES Around [23].

4. Design and development

Figure 2 was explain how the process of giving key toward data with RSA and AES method. The first step done was determining the file that key giving. After the data was determine so the next was the process of key RSA and AES method.

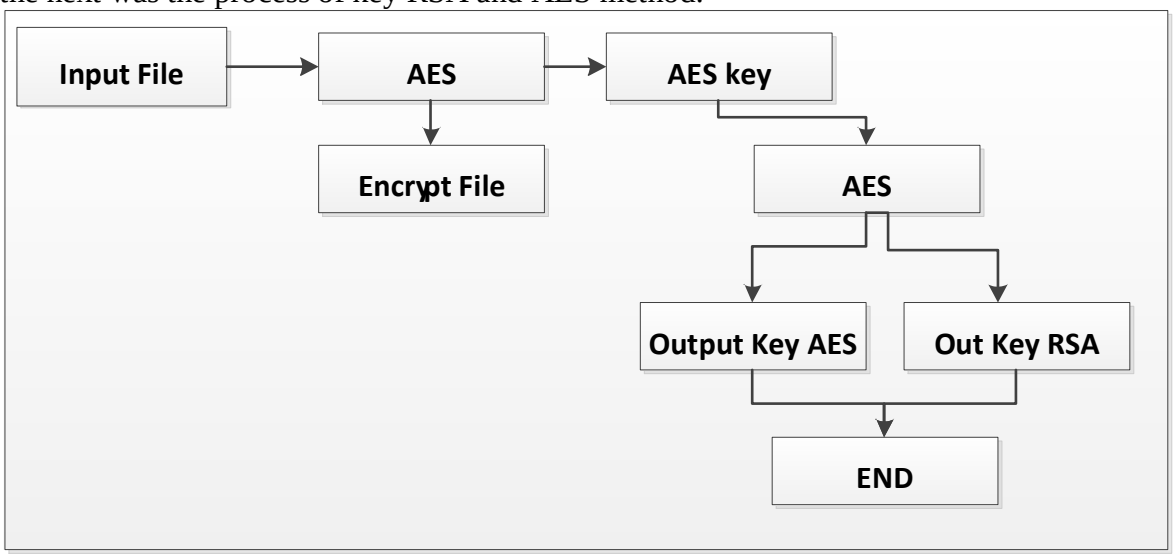

Figure 2. The Combined Block Diagram Method Of RSA And AES

Figure 3 was explain how the process of giving key toward data with RSA and AES method. The first step done was determining the file that key giving. After the data was determine so the next was the process of key RSA and AES method.

© 2021, IJCSMC All Rights Reserved

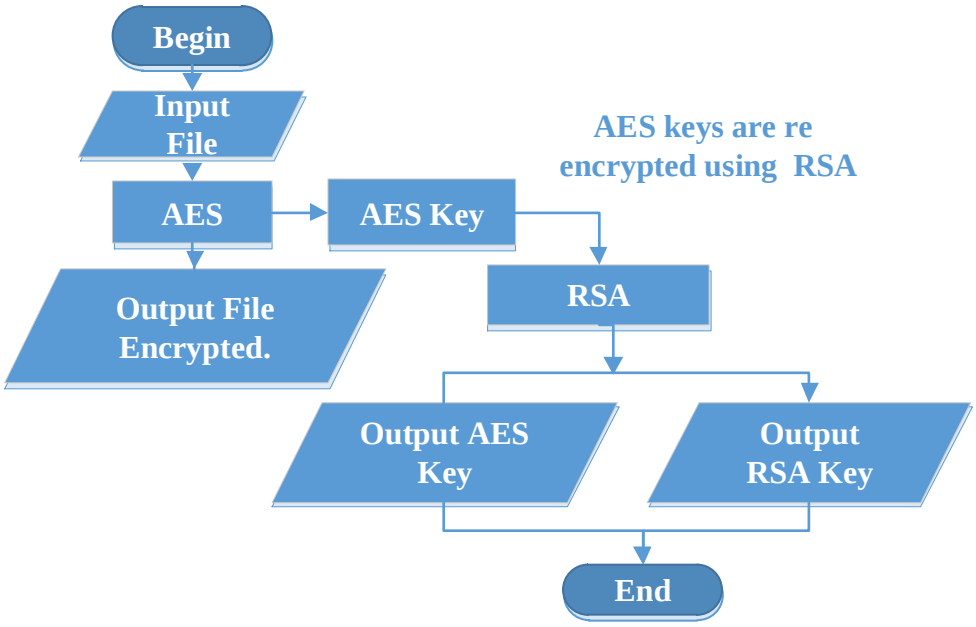

Figure 3. Flowchart Encryption

The user insert the file in file system will be decrypt, RSA private, and AES. The system would be decrypted by AES using RSA private, AES that has decrypted would be use to decrypt file, the file that has been decrypted would be export.

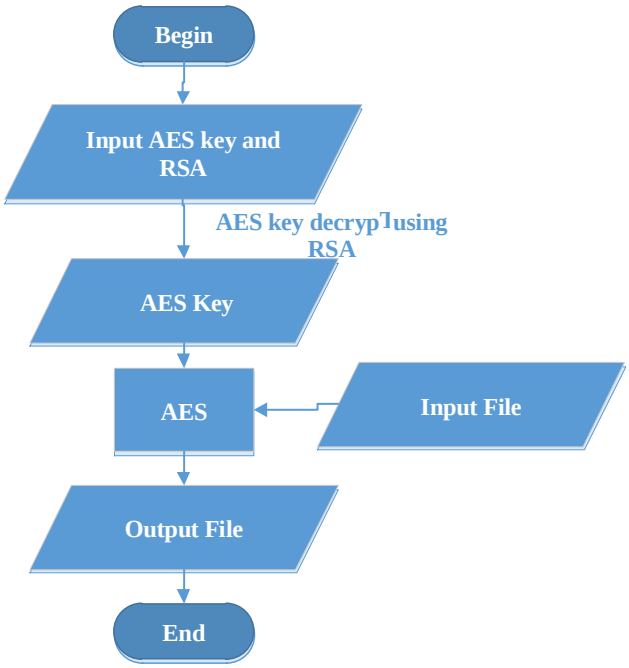

Figure 4. Flowchart Decryption

5. Discussion

Figure 5 was explained how the process of making RSA and AES in file that has been determined. The first process was download of application in play store, second step installation process, third step has run and could choose the file which encryption, fourth step choosing the encryption file, fifth step showing the file performance that has been determined.

© 2021, IJCSMC All Rights Reserved

Based on result of this research could be seen how the process of cryptography in android system. Therefore, found the file first would be encrypting, after it assign the number in increasing key based on algorithm which applied, whereas the key would be used in opening file that has been encrypting become decrypting. Below could be seen in figure 6 the file that have been encryption figure 7 was file that has been encryption in safety file which was used android system.

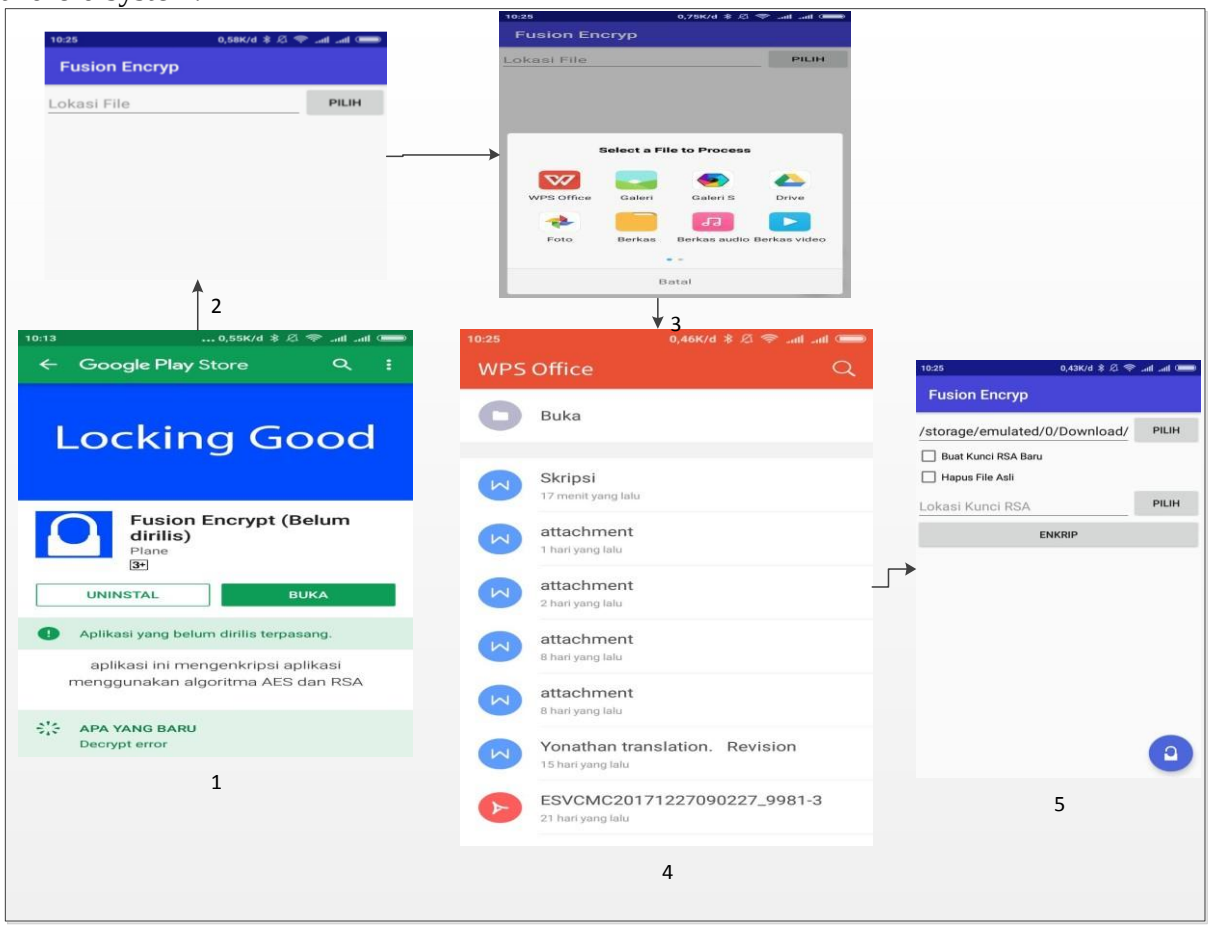

Figure 5. The process of Encrypt the File RSA and AES

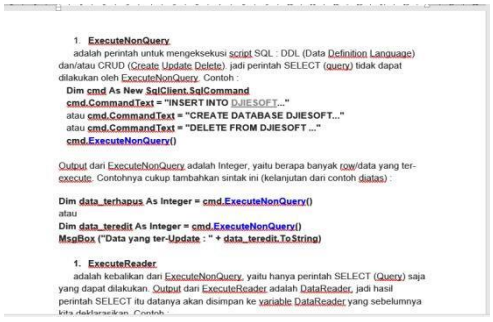

Figure 6. Before Encryption

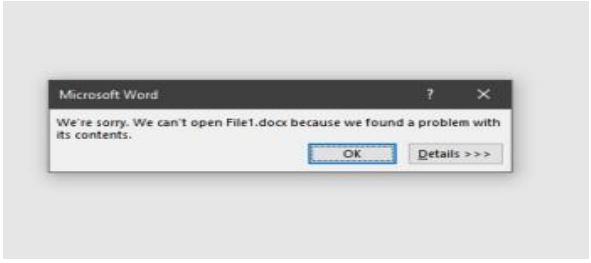

Figure 7. After Encryption

Based on the analysis process of encryption and decryption in some files which has been test from files looking from different files, so could be seen the different in encryption and decryption process which in android system from time that has gotten. Below could be seen in figure 8 encryption process and figure 9 decryption which was test in some different files that

© 2021, IJCSMC All Rights Reserved

has using in cryptography with decryption and encryption process that has different file size 25.44 KB 200 KB, 600 KB, and 2.29 MB

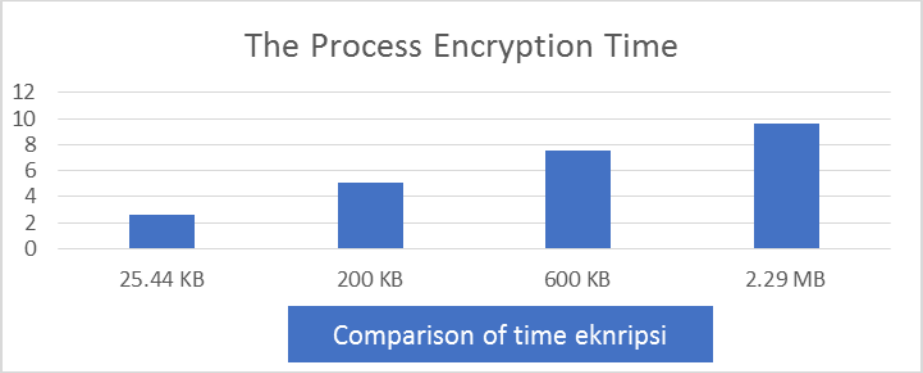

Figure 8. The process encryption time.

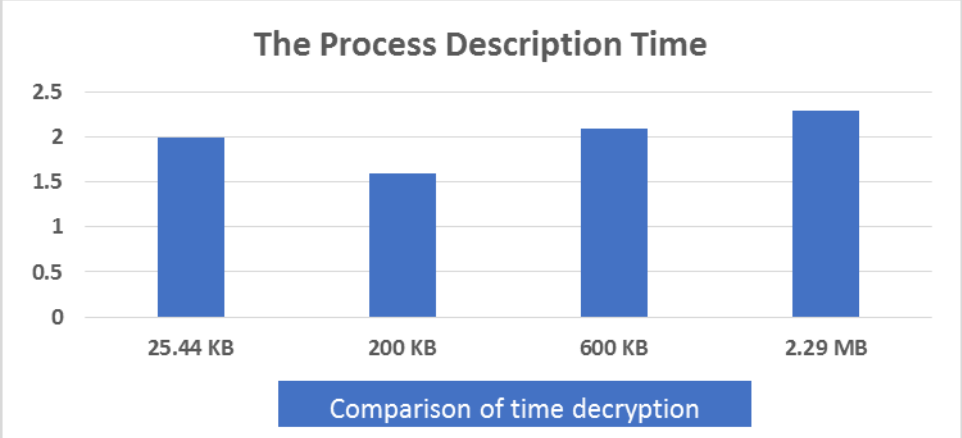

Figure 9. The process description time.

6. Result

Based on result of cryptography file has been done with AES and RSA could give cryptography in kinds of files in mobile. There were size of file data that have done in test. It found the different encryption. Some of file size 25.44 KB, encryption time 4 second, 200 KB, 5 second, 600 KB 7 second, 2.29 MB, 10 second. Where decryption 25.44 KB, encryption 2 second, 200 KB, 1.5 second, 600 KB 2.5 second, 2.29 MB, 2.7 second.

ACKNOWLEDGEMENT

Our deepest gratitude goes to my Guide Prof. P.B. Kudal (Lecture, Department of Computer Engineering, Guru Gobind Singh Polytechnic, Nashik) for her immense patience in dealing with our doubts and providing the required guidance and suggestions. She has always been prompt and quick in sharing views and advising at various stages of the dissertation work. We would also like to express our sincere gratitude to Prof. G.R.Jagtap (Head Of Department, Computer Engineering, Guru Gobind Singh Polytechnic, Nashik) who had been very supporting to allowing me the liberty to independently pursue the work.

© 2021, IJCSMC All Rights Reserved

CONCLUSION

As we toward a society where automated information resources are increased and cryptography will continue to increase in importance as a security mechanism. Electronic networks for banking, shopping, inventory control, benefit and service delivery, information storage and retrieval, distributed processing, and government applications will need improved methods for access control and data security. The information security can be easily achieved by using Cryptography technique. DES is now considered to be insecure for some applications like banking system. there are also some analytical results which demonstrate theoretical weaknesses in the cipher. So it becomes very important to augment this algorithm by adding new levels of security to make it applicable. By adding additional key, modified S-Box design, modifies function implementation and replacing the old XOR by a new operation as proposed by this thesis to give more robustness to DES algorithm and make it stronger against any kind of intruding. DES Encryption with two keys instead of one key already will increase the efficiency of cryptography.

References

[1]. Muneer Ahmad Dar and Javed Parvez Evaluating Smartphone Application Security: A Case Study on Android, International Journal of Advance Research, IJOAR .org ISSN 2320-9194, Volume 1, ISSN 2320-9194.

[2]. Tiwari Mohini, Srivastava Ashish Kumar and Gupta Nitesh Review on Android and Smartphone Security, Research Journal of Computer and Information Technology Sciences, ISSN 2320 – 6527, Vol. 1(6), 12-19, November (2013).

[3]. Zhiyi F, Ying W, Zelin D and Fan Y. (2013) The Research on NSSC Key Service Mechanism in Mobile Network, 2nd International Conference on Science and Social Research (ICSSR 2013).

[4]. Bin Liu, and Bevan M. Baas (2013) "Parallel AES Encryption Engines for Many-Core Processor Arrays " Journal IEEE Transactions on Computers, 2(3), 536-547.

[5]. Das Debasis, MisraRajiv. "Programmable Cellular Automata Based Efficient Parallel AES Encryption Algorithm". International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011, pp. 204.

[6]. Rohan Rayrikar,Sanket Upadhyay and Priyanka Pimpale,"SMS Encryption using AES Algorithm on Android", International Journal of Computer Applications Vol.

[7]. Kalpana Parsi, Singaraju Sudha. "Data Security in Cloud Computing using RSA Algorithm". International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278-5841, Vol 1, Issue 4, September 2012.

[8]. Padmapriya, Dr.A, Subhasri, P. "Cloud Computing: Security Challenges & Encryption Practices". International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 3, Issue 3, March 2013, pp. 257.

[9]. Padmapriya, Dr.A, Subhasri, P. "Cloud Computing: Security Challenges & Encryption Practices". International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 3, Issue 3, March 2013, pp. 257.

[10]. Prashanti.G, Deepthi.S & Sandhya Rani.K. "A Novel Approach for Data Encryption Standard Algorithm". International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume - 2, Issue - 5, June 2013, pp. 264.

[11]. Singh Narjeet, Raj Gaurav. "Security On Bccp Through Aes Encryption Technique". International Journal Of Engineering Science & Advanced Technology Volume-2, Issue-4, 813 – 819. pp. 817

© 2021, IJCSMC All Rights Reserved