Advances in Intelligent Systems Research, volume 172
Sriwijaya International Conference on Information Technology and Its Applications (SICONIAN 2019)

Blowfish–RSA Comparison Analysis of the Encrypt Decrypt Process in Android-Based Email Application

Dwi Yuny SYLFANIA[1*], Fransiskus Panca JUNIAWAN[2], LAURENTINUS[3], and Harrizki Arie PRADANA[4]

[1]*dysylfania@atmaluhur.ac.id, Department of Computer Science, STMIK Atma Luhur, Pangkalpinang, Indonesia*
[2]*fransiskus.pj@atmaluhur.ac.id, Department of Computer Science, STMIK Atma Luhur, Pangkalpinang, Indonesia*
[3]*laurentinus@atmaluhur.ac.id, Department of Computer Science, STMIK Atma Luhur, Pangkalpinang, Indonesia*
[4]*harrizkiariep@atmaluhur.ac.id, Department of Computer Science, STMIK Atma Luhur, Pangkalpinang, Indonesia*
**Corresponding author: dysylfania@atmaluhur.ac.id*

ABSTRACT
Email is a service that used to send text, message, or letter to someone electronically. However, addressing the email at network possibility to be intercepted, read, even modified by another side. As a result, there is no guarantee for confidentiality and accuracy of information. There is a way to deal with information security threats in email, that is using cryptography. However, in addition to security, the rapidity factor becomes a consideration in selecting cryptographic algorithms that will apply. In this study will be implemented Blowfish algorithm and RSA algorithm into the sending and receiving emails process based on Android application. Both algorithms will be analysed and compared in terms of encryption and decryption rapidity to determine which algorithm has excellent speed. Blowfish algorithm chose due to having superior swiftness and made the best solution compared to other symmetric algorithms. RSA algorithm selects because the rapidity is superior to the different asymmetric algorithms. Testing by calculating how high encryption and decryption process from both algorithms with the same key length and same message characters. Time measurement performed by ten times, then take the average value to get a consistent one. The results of this study are the Blowfish algorithm has the superior rapidity than RSA algorithm. From the test results, it proved that for the encryption process, Blowfish was 178,958% faster than RSA. Conversely, RSA is 63.131% slower than Blowfish. For the decryption process, the same result obtains, namely Blowfish, which is faster than 420.44188% compared to RSA. Instead, RSA is 80.3399% slower than Blowfish.
Keywords: *RSA, Blowfish, cryptography, email, android*

INTRODUCTION

Sending the data process in a network will possible to be read by people who are not responsible, as eavesdroppers. Some security threats are no longer occur when data is exchanged using mobile storage media, but when the data via a telecommunications line. Information's exchange occurs in the computer network at any time. Besides, it allows the other party can be intercepted, and changed data send to the data that sent will be altered or even disappear and not deliver to the recipient. Security information in the email is indispensable. To deal with information security threats in the email is by using cryptography. The cryptography implementation in securing email has many been done by the other side, either by using symmetric and asymmetric cryptography. To decide the cryptographic algorithms that will apply in data systems security, it has to consider the protection against brute force cryptanalyst and the rapidity. At this time there is a wide range of symmetric and asymmetric cryptographic algorithm. If an algorithm believed to steady but slow in the process of encoding, then it will not be selected by the user. Consideration of this rapidity will be an advantage if the use of cryptographic algorithms engages the computer networks, especially in a client-server architecture. In this study will be implemented Blowfish algorithm and RSA algorithm into the sending and receiving emails based on Android application. Both algorithms will be analysed and compared in terms of encryption and decryption rapidity to determine which algorithm that has the extraordinary speed. Blowfish algorithm chose due to having superior swiftness and made the best solution compared to other symmetric algorithms. RSA algorithm selects because the rapidity is preferred rather than the different asymmetric algorithms [1]. The aim of this study is to determine which algorithm that have superior swiftness between encryption and decryption in sending and receiving email application based on Android using Blowfish and RSA.

There are some other works from the related field, which shows the performance of RSA and Blowfish algorithm. VHDL implements the hybrid RSA and Blowfish encryption technique. The proposed hybrid technique has both symmetric and asymmetric properties. Thus, the algorithm is secure, and authentication enabled process which provides better security for cloud computing. Therefore, a hybrid algorithm is successfully implemented by using VHDL and synthesized all the elements [2]. Another studies using RSA as a security method in the application of BEM Chairman election in institute [3] and improving SMS security in applications with RSA security methods [4]. As a comparison, Blowfish encryption and decryption is faster than AES and RSA because it takes the lowest processing time, and the AES algorithm is more rapid than RSA algorithm in terms of encryption and

decryption speed. Besides, symmetric algorithms provide high security with high speed on encryption and decryption, and an asymmetric algorithm can provide high protection but with more processing time [5]. The objective of this paper is to provide a comparative analysis of flexible cryptographic implementations. The selected researches, obtained through a systematic literature review process, have been classified into three design categories, it's crypto processors, crypto coprocessors, and multicore crypto processors [6].

Technical controls which make LDAP security component for cloud computing and proposed system contribution is a security architecture that provides a flexible security model with data compression algorithm and two-way encryption algorithm by SHA and AES algorithm, and it offers more security for users and cloud providers [7]. Proposed visual cryptography depending on some complex computations like AlGamal and RSA algorithm which gives more protection than the traditional methods which using only XOR operation, producing multiple shares to increase security for the image during transferring it over the network [8]. A new hybrid cryptography algorithm is proposed using Blowfish, RSA, and SHA-2 algorithms. The combination of the symmetric and asymmetric algorithm provides efficiency to the proposed system. The proposed method offers high security on data transmission over the internet using an SHA-2 algorithm [9]. Blowfish is best in terms of memory requirement and has least for encryption and decryption time than RSA. AES has a strong avalanche effect, so it can prefer for application where privacy and integrity of the message are of top priority [10][11]. The comparison of two popular cryptographic techniques (AES and RSA) made by calculating the buffer size of images, where AES more efficient in both encryption and decryption, for the given set of data [12].

Fusion encryption algorithm it's a new concept where merge DES and RC4. It uses one-time encryption method and its suitable for the business encryption of network terminal equipment which has only limited resources. The fusion encryption algorithm can choose one key or two fundamental modes [13]. The technique proposed for image encryption and decryption with random selective selection and Blowfish algorithm, the method selected refine part and encrypt decrypt block, the encryption and decryption time of proposed technique is better, and encryption and decryption results calculated by the proposed technique are better as compared standard methods [14]. Security framework to secure essential and unimportant portion of the message to overcome the uncertainty, where applied on Amazon EC2. The results showed that the proposed method gives better performance according to encryption time, throughput than full encryption, and gives a feasible solution for securing big data [15]. The security mechanism for keeping data ensure at the cloud with three steps. First, using MD5 and encrypted OTP for secure authentication. Next, enhanced the security of data using Cloud Broker and RSA, Blowfish, and AES. Afterward, verified the integrity of data stored at cloud provider using SHA2. The proposed system has reduced the complexity, processing cost, which increases the overall efficiency of the system [16]. DES algorithm better uses to send the encrypted files without change the file size. Whereas if there is a time constraint, they would be better to use algorithms like AES or RSA rather than DES [17]. DES and 3DES text data cryptographic method can be implementing on the application of ACOS3 smart card data writing process and data reading process in NFC - based systems. The execution time of the entering and the reading process data using an intelligent card DES cryptography method is faster than using 3DES cryptography [18]. Modified Blowfish algorithm performs better than the LZW algorithm in terms of total time to encrypt and decrypt. Modified Blowfish is significantly faster to encrypt Bangla and English text than LZW. However, LZW is found to be quicker to decrypt Bangla text than modified Blowfish algorithm [19]. Elliptical Curve Cryptography (ECC) and Homomorphic are combined to provide encryption. This technique used to store data in a suitably secure and safe manner to avoid intrusions and data attacks meanwhile it will reduce the cost and time to save the encrypted data in the cloud storage [20].

From the results of the summary of the previous research above, the advantages and various variations of the application of both blowfish and RSA algorithms have been described and elaborated. However, which algorithm has not been determined, which is faster in terms of encryption time and decryption. For this reason, this research was conducted to prove it.

METHOD

In this study, an Android-based email sending and receiving application will create by applying the Blowfish and RSA algorithms. The analysis and comparison of the two algorithms do in terms of algorithm speed, namely the speed of the encryption and decryption process. The shorter the time needed in the encryption and decryption process, the algorithm is the most superior algorithm. The Blowfish and RSA algorithms are applied in an Android-based email sending and receiving the application.

The data used in this study is in the form of text data. The data will be encrypted and decrypted, where the size of the data amount and critical length are the same for the two algorithms. The size of the data is from 100 to 1000 characters, and the key length is 256 bits — time measurement by using a timer in the application. The duration of the encryption and decryption process will calculate the difference between the end time and the start time. Because processor performance is unstable during time measurement, testing is done ten times for each number of characters, and then the average value is taken to get a consistent time. The results of the time measurement are plotting into the Cartesian graph between the data size and the time it made. The results of this study are expected to determine the superior algorithm between Blowfish and RSA algorithms. The steps of research consist of 4 steps, namely identification of system requirements, determine cryptographic methods, design system, and testing and implementation — the four stages described in Figure 1 as below.

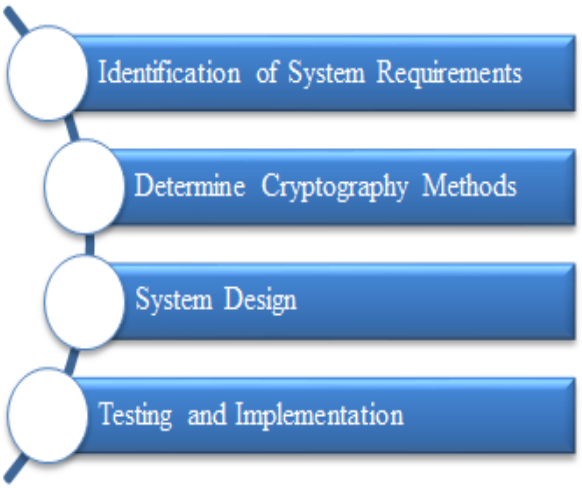


Figure 1. Research State

RESULTS

System Design

This study builds an Android-based application for sending and receiving an email by implementing Blowfish and RSA algorithm. Analysis and comparison of both algorithms performed in terms of the rapidity encryption and decryption. Shorter the time needed in the encryption and decryption process, then the algorithm is superior. Blowfish and RSA algorithm is applied in one Android-based application sending and receiving the email. The data used in this study is the text. The data will be encrypted and decrypted, which measure the amount of data and critical length the same for both algorithms — the size of the amount of data from 100 up to 1,000 characters. And an essential range of 256 bits. Time measurement is done using a timer that is in the application. The distance of the encryption and decryption process will be calculated from the start until the end time. Therefore, the performance of the processor is not stable during the measurement period, then tested ten times each for any number of characters, then take the average value to obtain a consistent time. The measurement results plotted into a Cartesian graph between the size of the data with the time required — the results of this study to define which algorithm is superior among Blowfish and RSA. Figure 2 describes the design of the application to be built using the Blowfish algorithm.

Figure 2 illustrates a message (plain text) will be encrypted by A using the private key that has been agreed by both parties. The timing counted from the beginning of the encryption process until ciphertext generated. SMTP port will continue the ciphertext to the server and accepted by the IMAP port. The ciphertext is received and decrypted by B using the private key that has agreed in advance. The timing counted from the start of the decryption process until it results in the plain text. The design of the application to be built using the RSA algorithm, described in Figure 3.

Figure 3 illustrates a message (plain text) will be encrypted by A using the public key B. The timing counted from the beginning of the encryption process until ciphertext generated. The SMTP port will continue the ciphertext to the server and accepted by the IMAP port. Then, the ciphertext is received and decrypted by B using the private key. The timing counted from the start of the decryption process until it results in the plain text.

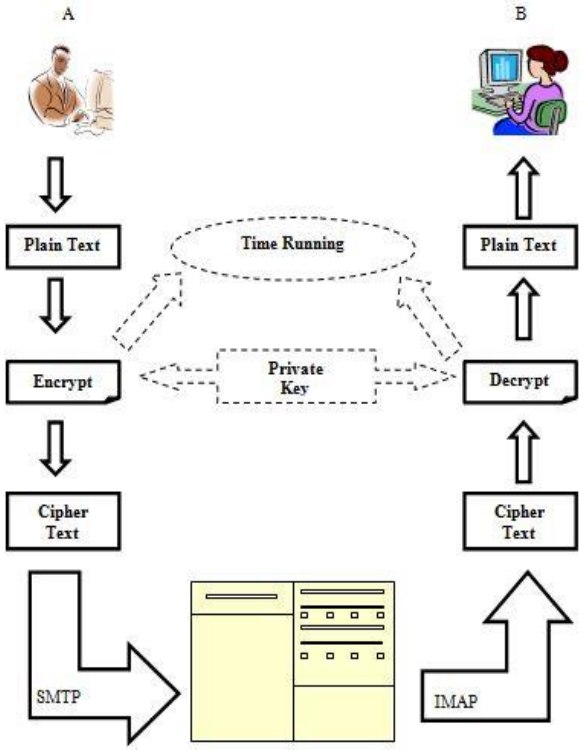


Figure 2. Blowfish System Design

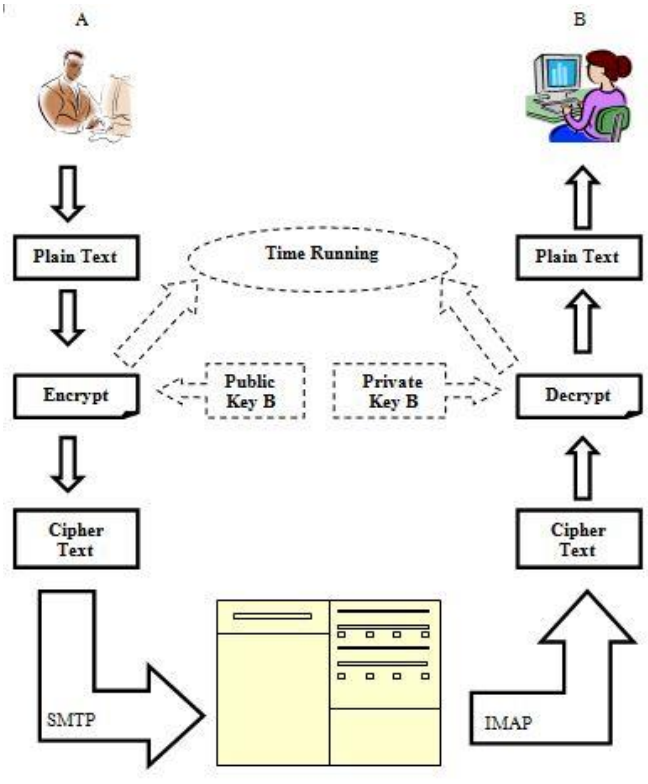
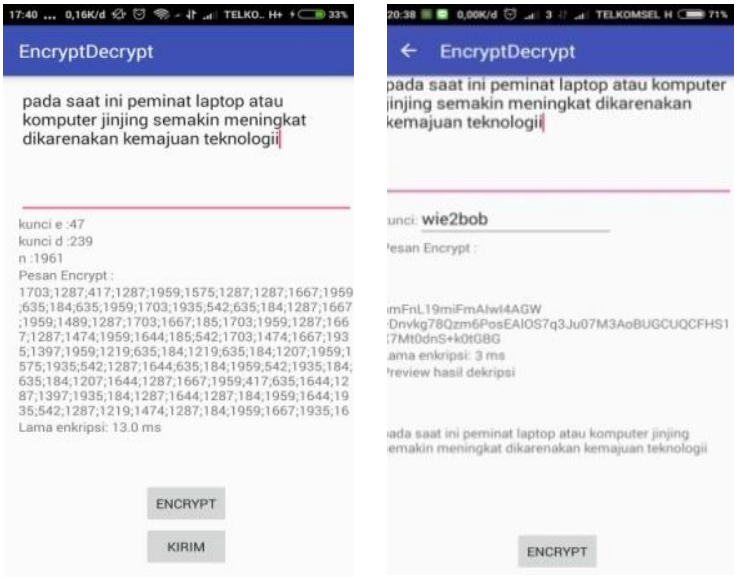


Figure 3. RSA System Design

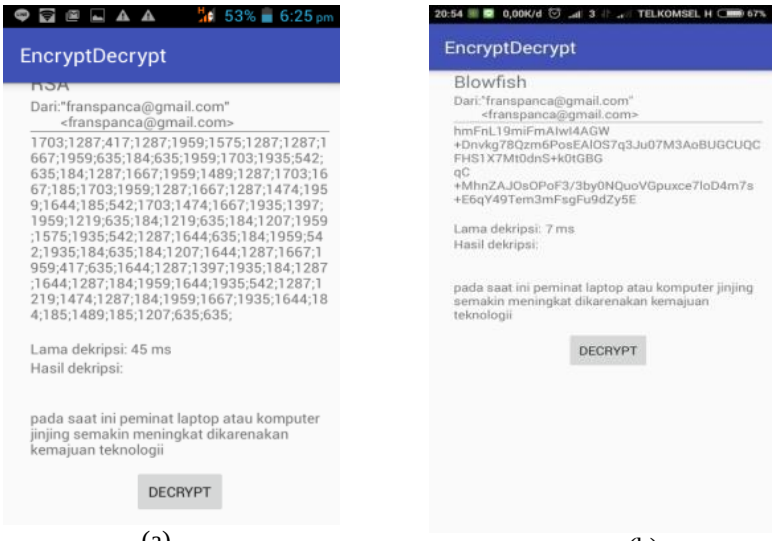
SOFTWARE TESTING

Testing is doing by comparing the rapidity of encryption and decryption Blowfish and RSA in a message with the same number of characters. The results of this test in the form of graphs. The user must first select the algorithm to use, Blowfish or RSA algorithm, then insert plain text and key. Once that process was doing, the plain text into cipher text changed. The next stage is the decryption process; at this stage, the ciphertext can access in the menu inbox. Users choose which messages to be decrypted by Blowfish or RSA algorithm, and then, users enter the key according to the selected algorithm. After the process finished, then the ciphertext will change to plain text. During the encryption and decryption process, either Blowfish or RSA algorithm, then the timer will automatically calculate the lengthy process of encryption and decryption. Figure 4 shows testing for 100 characters' encryption with Blowfish algorithm and RSA. Decryption testing the 100 character with Blowfish algorithm and RSA will be shown in Figure 5.



(a) (b)

Figure 4. Encryption Testing of 100 Characters (a) RSA; (b) Blowfish



(a) (b)

Figure 5. Decryption Testing of 100 Characters (a) RSA; (b) Blowfish

DISCUSSION

This study uses two methods of the algorithm in encrypting and decrypting messages, likely Blowfish and RSA algorithm. The discussion section is dividing into two parts, namely the results of the encryption test and the results of the decryption test, with the performance results of the two algorithms in each section.

ENCRYPTION TESTING

The software testing result was showing in the chart that describes how long the process of encryption and decryption based on the number of characters from the message. Figure 6 shown encryption testing chart. Speed encryption comparison of blowfish against RSA and on the other hand, RSA to Blowfish is presenting in Table 1.

Table 1. Detail of Encryption Testing Result

Characters	Blowfish (ms)	RSA (ms)	Blowfish against RSA percentage (%)	RSA against Blowfish percentage (%)
100	3	13	333.333	76.923
200	9	25	177.778	64
300	13	36	176.923	63.889
400	16	49	206.25	67.347
500	22	57	159.091	61.406
600	27	67	148.148	59.701
700	31	75	141.935	58.667
800	35	87	148.571	59.77
900	39	97	148.718	59.794
1000	43	107	148.837	59.813
Average			178.958	63.131

The results of the graph in Figure 6 describes the length encryption process for Blowfish and RSA algorithm. The x-axis expresses the number of characters to be encrypted, and the y-axis shows the length of the encryption process in milliseconds units. Testing is performed ten times for each number of characters; the value that entered in the chart are average values. On average, Blowfish is 178.958% faster than RSA; on the other hand, RSA is 63.131% slower than Blowfish. Based on Figure 6 and Table 1, the Blowfish encryption algorithm takes much shorter than the RSA algorithm. Therefore, the Blowfish encryption algorithm is superior compared to the RSA algorithm.

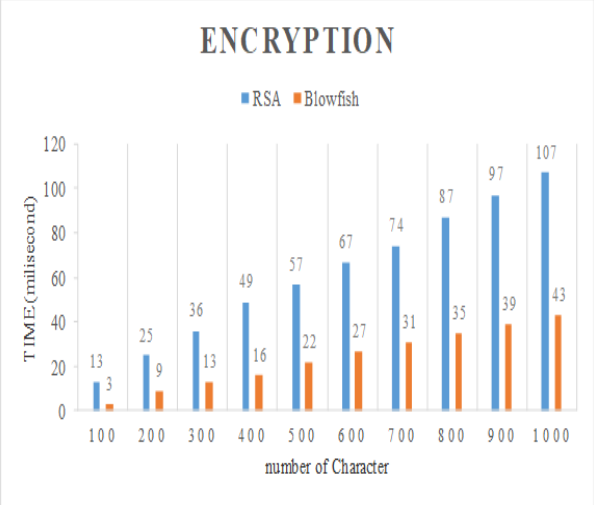


Figure 6. Encryption Testing Result

DECRYPTION TESTING

Figure 7 displays the results of testing the second decryption algorithm. Just like encryption, the decryption process needed by Blowfish is faster than RSA. Table 2 describes the speed percentage of Blowfish decryption against RSA of 420.44188%. Otherwise, RSA is 80.3399% slower than Blowfish.

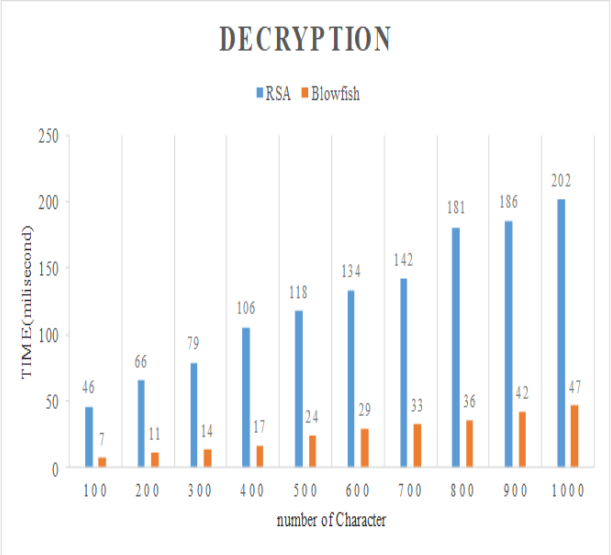


Figure 7. Decryption Testing Result

Table 2. Detail of Decryption Testing Result

Characters	Blowfish (ms)	RSA (ms)	Blowfish against RSA percentage (%)	RSA against Blowfish percentage (%)
100	7	46	557.1428571	84.7826087
200	11	66	500	83.33333333
300	14	79	464.2857143	82.27848101
400	17	106	523.5294118	83.96226415
500	24	118	391.6666667	79.66101695
600	29	134	362.0689655	78.35820896
700	33	142	330.3030303	76.76056338
800	36	181	402.7777778	80.11049724
900	42	186	342.8571429	77.41935484
1000	47	202	329.787234	76.73267327
Average			420.44188	80.3399

CONCLUSION

The conclusion of this research is the blowfish algorithm has superior rapidity than RSA, the encryption or decryption process. The number of characters will be encrypted and decrypted against encryption and decryption processes. That evident from the results of testing that the blowfish encryption process is 178,958% faster than RSA, as well as the decryption process 420.44188% faster than RSA. Conversely, in the encryption process, RSA has a slower performance of 63.131% compared to blowfish. Besides, the decryption process also has slower performance than blowfish, which is 80.3399%.

REFERENCES

[1] R. Tripathi and S. Agrawal, “Comparative Study of Symmetric and Asymmetric Cryptography”, Int. J. Advance Foundation and Research in Computer, IJAFRC 2014, vol. 1, no. 6, pp. 68–76, 2014.

[2] V. P. Bansal and S. Singh, “A Hybrid Data Encryption Technique Using RSA and Blowfish For Cloud Computing on FPGAs,” 2015 2nd IEEE Int. Conf. on Recent Advances in Engineering & Computational Sciences, RAECS 2015, no. December, 2016.

[3] F. P. Juniawan, "RSA implementation for data transmission security in BEM chairman E-voting Android based application," 2016 1st International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE), Yogyakarta, 2016, pp. 93-98.

[4] D. Y. Sylfania, F. P. Juniawan, L. Laurentinus, and H. A. Pradana, "SMS Security Improvement using RSA in Complaints Application on Regional Head Election’s Fraud," Jurnal Teknologi dan Sistem Komputer, vol. 7, no. 3, pp. 116-120, Jul. 2019.

[3] W. A. N. A. AL-Nbhany and A. Zahary, “A Comparative Study Among Cryptographic Algorithms : Blowfish , AES and RSA,” Int. Arab Conf.on Information Technology, ACIT 2016, no. December, 2016.

[4] M. Rashid, M. Imran, and A. R. Jafri, “Comparative Analysis of Flexible Cryptographic Implementations,” 2016 11th IEEE Int. Symp. on Reconfigurable Communication-centri Systems-on-Chip (ReCoSoC) 2016, 2016.

[5] K. V. Raipurkar and A. V. Deorankar, “Improve Data Security in Cloud Environment by Using LDAP and Two Way Encryption Algorithm,” 2016 IEEE Symp. on Colossal Data Analysis and Networking, CDAN 2016, pp. 1–4, 2016.

[6] A. Kadhim and R. M. Mohamed, “Visual Cryptography For Image Depend on RSA & AlGamal Algorithms,” IEEE Al-Sadiq Int. Conf. Multidisciplinary in IT and Communication Science and Applications, AIC-MITCSA 2016, pp. 195–200, 2016.

[7] D. P. Timothy and A. K. Santra, “A Hybrid Cryptography Algorithm For Cloud Computing Security,” 2017 IEEE Int. Conf. on Microelectronic Devices, Circuits and System, ICMDCS 2017, vol. 2017–Janua, pp. 1–5, 2017.

[8] P. Semwal and M. K. Sharma, “Comparative Study of Different Cryptographic Algorithms For Data Security in Cloud Computing,” IEEE Proc. - 2017 3rd Int. Conf. on Advances in Computing Communication and Automation. (Fall), ICACCA 2017, vol. 2018–Janua, pp. 1–7, 2018.

[9] M. Nazeh, A. Wahid, A. Ali, B. Esparham, and M. Marwan, “A Comparison of Cryptographic Algorithms : DES , 3DES , AES , RSA and Blowfish for Guessing Attacks Prevention,” J. Comput. Science Applications and Information Technology, vol. 3, no. 2, pp. 1–7, 2018.

[10] B. J. Santhosh Kumar, R. V. K. Roshni, and A. Nair, “Comparative Study on AES and RSA Algorithm For Medical Images,” Proc. 2017 IEEE Int. Conference on Communication and Signal Processing, ICCSP 2017, vol. 2018–Janua, pp. 501–504, 2018.

[11] Z. Y. Hong, Z. P. Qiu, S. L. Zeng, S. De Wang, and M. Sandrine, “Research on Fusion Encryption Algorithm For Internet of Things Monitoring Equipment,” Proc. - 14th IEEE Int. Symp. on Pervasive System, Algorithms and Networks, I-SPAN 2017, 11th Int. Conf. on Frontier of Computer Science and Technology FCST 2017 3rd Int. Symp. of Creative Computing ISCC 2017, vol. 2017–Novem, pp. 425–429, 2017.

[12] A. Kaur and G. Singh, “A Random Selective Block Encryption Technique For Secure Image Cryptography Using Blowfish Algorithm,” IEEE Proc. Int. Conf. on Inventive Communication and Computational Technologies, ICICCT 2018, no. Icicct, pp. 1290–1293, 2018.

[13] A. S. Sakr, P. M. El-Kafrawy, H. M. Abdullkader, and H. M. Ibrahem, “An Efficient Framework For Big Data Security Based on Selection Encryption on Amazonec2,” 1st IEEE Int. Conf. on Computer Applications & Information Security, ICCAIS 2018, pp. 1–5, 2018.

[14] G. Singh and M. Garg, “Enhanced Cloud Security Using Hybrid Mechanism of RSA, AES and Blowfish Data Encryption With Secure OTP,” Int. J. of Computers and Technology, vol. 18, pp. 7364–7380, 2018.

[15] T. Subbulakshmi, S. Bhardwai, P. Ranjan, and K. Antony John, “Enhanced SPK Encryption Algorithm For File Encryption Using Java,” Proc. 2nd Int. Conf. on Intelligent Computing and Control Systems, ICICCS 2018, no. Iciccs, pp. 235–239, 2019.

[16] Ratnadewi, R. P. Adhie, Y. Hutama, A. Saleh Ahmar, and M. I. Setiawan, “Implementation Cryptography Data Encryption Standard (DES) and Triple Data Encryption Standard (3DES) Method in Communication System Based Near Field Communication (NFC),” J. of Physics Conf. Ser., vol. 954, no. 1, 2018.

[17] S. Akhter and M. B. Chowdhury, “Bangla and English Text Cryptography Based on Modified Blowfish and Lempel-Ziv-Welch Algorithm to Minimize Execution Time,” 1st IEEE Int. Conf. on Robotics, Electrical and Signal Processing Techniques, ICREST 2019, pp. 96–101, 2019.

[18] P. Saravanan, H. Kumar R, A. T, and B. Narayanan, “Hybrid Cryptosystem Using Homomorphic Encryption and Elliptic Curve Cryptography Algorithm,” i-manager ’s J. on Computer Science, vol. 7, no. 1, p. 2019, 2019.