Instal : Jurnal Komputer

E-ISSN: 2808-683X
Edisi : Volume 15 Nomor 01 | June 2023

Available online at https://journalinstal.cattleyadf.org/index.php/Instal/index

COMPARISON OF RSA AND ROT13 METHODS FOR TEXT FILE CONFIDENTIALITY

Rano Irawan[1], Abdul Halim Hasugian[2], Sulindawaty[3]
[1,2,3]Universitas Islam Negeri Sumatra Utara

A R T I C L E I N F O

Keywords:

Cryptography
RSA and ROT13
Maintain data security

ABSTRACT

The word cryptography comes from the Greek: krupto (hidden or secret) and grafh (writing), meaning "secret writing". In the past, cryptography could be interpreted as the science and art of maintaining the security of data or messages by encoding them in a form whose meaning could no longer be understood. In its development, cryptography is not only meant to encrypt data or messages, but also to maintain the security of data or messages. The research carried out by researchers is a type of research and development (R&D). The R&D research method is a research method used to produce certain products and test the effectiveness of these products. R&D is a process or steps to develop a new product or improve an existing product, which can be accounted for. At this stage, encryption and decryption testing of each algorithm will be carried out on text data with a number of characters varying between 10 to 100 characters and the output What will be displayed is the encryption result in the form of a ciphertext file and the running time. 1. The implementation of the RSA cryptographic algorithm was successful and the resulting system runs according to the algorithm used and the encrypted plaintext can be returned to its original form.

Corresponding Author:
Rano Irawan
Universitas Islam Negeri Sumatra Utara
Email: ranoirawan271197@gmail.com

INTRODUCTION

The word cryptography comes from the Greek: krupto (hidden or secret) and grafh (writing), meaning "secret writing". In the past, cryptography could be interpreted as the science and art of maintaining the security of data or messages by encoding them in a form whose meaning could no longer be understood. In its development, cryptography is not only defined as encrypting data or messages, but also maintaining the security of data or messages. The development of information technology today makes it easy to communicate and provide various information. But with this convenience, people forget that data security and privacy are important things in communication. As technology develops, the ease of sending information has risks and negative impacts, namely the security of information on the data sent. Because not just anyone can access data, including text that has been selected

Page : 347-351

Doi. https://doi.org/10.54209/jurnalinstall.v16i03.223

because it is confidential and public. Meanwhile, applications such as WhatsApp, BBM, Facebook have a low level of security. To minimize these concerns, cryptography was born, namely the science of encoding and decoding data or making it disguised.

METHODS

to carry out the text data encryption process. In its work, the research procedure used is as follows:

1. Literature study

This research is carried out by the author by searching for journals and ebooks, to study and collect references and basic theories while studying various articles and journals on the internet.

2. Data Collection

Carry out data collection and review of the resulting data from the interview stage to sources regarding security measures for data that are used as reference material for the system that is being created.

3. Sand design and application development

At this stage of application design and development, an analysis of the appropriate procedures for the research in this case and text data is carried out so that the application which is the result of the research can achieve its objectives. The design created is then implemented in the SMS programming language. sVisual sBasic s.NET s2010.

4. Test sTry sApp

The testing stage is carried out while the application is being developed. This is so that the application can be ensured that it is running well, and if there is an error it can be detected.

5. Writing reports

Documentation is available at every stage of the design, up to drawing conclusions from the results of data analysis, and then being compiled to be used as a research report.

RESULTS AND DISCUSSION

The data needed in this research is text data. At the data analysis stage, text data input and stamp design are carried out. Then simplify the Rivest Shamir sAdleman (RSA) and Rotate 13 (ROT13) algorithms in all applications to perform encryption and decryption. There are several program stages carried out, namely: s

A. RSA algorithm

1. Encryption

A. Generate public and private keys

B. Enter public text data and public key.

C. Reading text data.

D. Perform encryption

E. Displays the results of ciphertext encryption.

Decryption

A. Enter ciphertext data.

B. Enter the private key.

C. Perform Decryption

D. Displays plain text as the decryption result.

2. ROT13 algorithm

Encryption

A. Enter text and key data.

B. Reading text data.

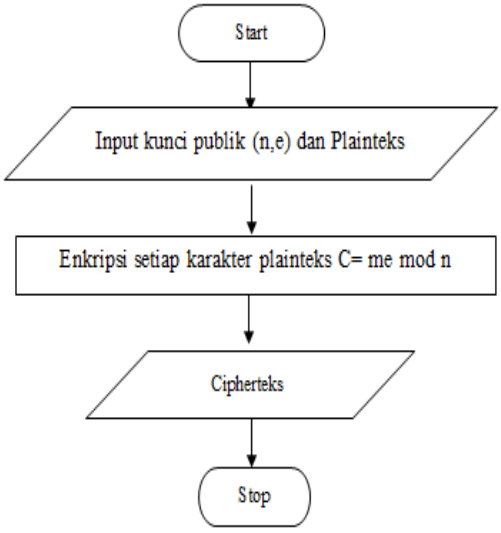
C. Perform encryption

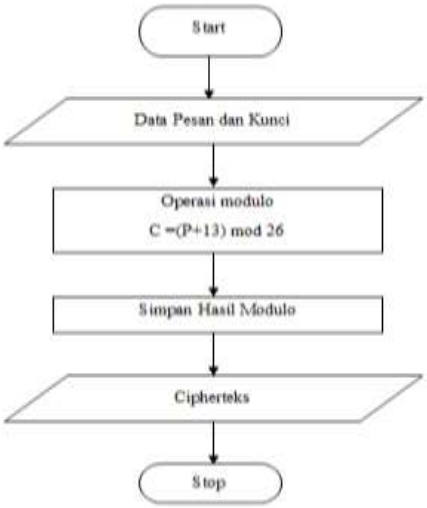
Page : 347-351

Doi. https://doi.org/10.54209/jurnalinstall.v16i03.223

D. Displays the results of ciphertext encryption.
Decryption
A. Enter the passtext and key.
B. Read ciphertext data.
C. Perform decryption
D. Displays plain text as the decryption result.

RSA and ROT13 Encryption Flowchart





Encryption results with RSA and ROT 13 algorithms

No	File	Plainteks	Cipherteks	Running time (s)
1	File-10	HARI INI BELAJAR	253,477,1072,610,210,610,1051,610,210,652,743,519,477,785,477,1072	0.015
2	File -20	HARI INI BELAJAR KRIPTOGRAFI	253,477,1072,610,210,610,1051,610,210,652,743,519,477,785,477,1072, 210,1142,1072,610,540,806,1408,1275,1072,477,918,610	0.018
3	File -30	HARI INI BELAJAR KRIPTOGRAFI RSA DAN ROT13 UNTUK	253,477,1072,610,210,610,1051,610,210,652,743,519,477,785,477,1072, 210,1142,1072,610,540,806,1408,1275,1072,477,918,610,210,1072,1429, 477,210,386,477,1051,210,1072,1408,806,987,1519,210,1163,1051,806,116 3,1142	0.016
4	File -40	HARI INI BELAJAR KRIPTOGRAFI RSA DAN ROT13 UNTUK MENGAMANKA N DATA	253,477,1072,610,210,610,1051,610,210,652,743,519,477,785,477,1072,210 , 1142,1072,610,540,806,1408,1275,1072,477,918,610,210,1072,1429,477,21 0, 386,477,1051,210,1072,1408,806,987,1519,210,1163,1051,806,1163,1142,2 10, 876,743,1051,1275,477,876,477,1051,1142,477,1051,210,386,477,806,477	0.008
5	File -50	HARI INI BELAJAR KRIPTOGRAFI RSA DAN ROT13 UNTUK MENGAMANKA N DATA RAHASIA KITA MENGGUNAKAN KUNCI PUBLIK	253,477,1072,610,210,610,1051,610,210,652,743,519,477,785,477,1072, 210, 1142, 1072, 610, 540, 806, 1408, 1275, 1072, 477, 918, 610, 210, 1072, 1429, 477, 210, 386, 477, 1051, 210, 1072, 1408, 806, 987, 1519, 210, 1163, 1051, 806, 1163, 1142, 210, 876, 743, 1051, 1275, 477, 876, 477, 1051, 1142, 477, 1051, 210, 386, 477, 806, 477, 210, 1072, 477, 253, 477, 1429, 610, 477, 210, 1142, 610, 806, 477, 210, 876, 743, 1051, 1275, 1275, 1163, 1051, 477, 1142, 477, 1051, 210, 1142, 1163, 1051, 1009, 610, 210, 540, 1163, 652, 519, 610, 1142, 210, 386, 477, 1051, 210, 1072, 477, 253, 477, 1429, 610, 477	0.008

Page : 347-351

Doi. https://doi.org/10.54209/jurnalinstall.v16i03.223

RSA and ROT13 Algorithm Testing Process Time Results

No	Nama File	Jumlah Karakter	Running Time (s)
1	File-10	16	0.0005
2	File -20	28	0.0006
3	File -30	48	0.007
4	File -40	65	0.007
5	File -50	115	0.010
6	File -60	178	0.012
7	File -70	241	0.019
8	File -80	298	0.022
9	File -90	221	0.032
10	File -100	312	0.054

No	Nama File	Jumlah Karakter	Running Time (s)
1	File-10	16	0.0005
2	File -20	28	0.0006
3	File -30	48	0.007
4	File -40	65	0.007
5	File -50	115	0.010
6	File -60	178	0.012
7	File -70	241	0.019
8	File -80	298	0.022
9	File -90	221	0.032
10	File -100	312	0.054

CONCLUSION

Based on the analysis, design and testing of Rivest Shamir Adleman (RSA) and ROT13 (Rotate13) research algorithms in encrypting text files, several conclusions were obtained: The implementation of the RSA scriptography algorithm has been successfully carried out and the resulting system runs according to the algorithm used and the encrypted text can be returned to its original form. Based on the graph of the relationship between encryption process time and plaintext size, it shows that there is an influence on the speed of the encryption process based on the total length of plaintext in each algorithm. Based on the graph of the relationship between encryption process time and decryption process time, it

Page : 347-351

Doi. https://doi.org/10.54209/jurnalinstall.v16i03.223

shows that the time used does not have much difference. Based on changes in sciphertext results during testing, the use of the RSA and ROT13 scriptography algorithms here is relatively simple and very simple to secure text.

REFERENCES

1. Agustina, A. N. & Aryanti, Nasron. 2017. Document Security Using the Web-Based Rsa (Rivest Shamir Adleman) Method. Proceedings of the 3rd UNISBANK National Multi-Discipline Seminar & Call For Papers.
2. Andriyani, S. Y. 2019. Implementation of Shamir Adleman's Rivest cryptographic algorithm and Myszkowski transposition algorithm and Fibonacci code compression algorithm. Thesis Faculty of Computer Science and Information Technology.
3. Aresta, R. M., Pratomo, E. W., Geraldino, V., Santoso, J. D. & Mulyatun, S. 2020. Implementation of ROT 13 Multi Encryption on Whatsapp Symbols. Journal of Information System Management e-ISSN: 2715-3088 Vol 2., No. 1. (2020).
4. Arifah, P. N. & Basuki, W. A. 2017. Implementation of Caesar Chiper Cryptography Using Matlab R2013a. UNY Mathematics and Mathematics Education Seminar 2017.
5. Budiharto, W. & Lisangan, C. E.. 2012. VB.NET Programming Applications. Publisher: Elexmedia Komputindo Gramedia Jakarta Edition 1.
6. Girsang, N. D., Santoso, M. H., Wahyudi, A. & Sitorus, B. A. 2019. Combination of Shamir Adleman's Rivest Transposition Cryptography Algorithm and Route Cipher. Proceedings of the National Information Technology Seminar Volume 2 Number 1 November 2019.
7. Jogiyanto, HM. 2010. Analysis and design of Information Systems, Kawan Pustaka, Jakarta.
8. Latifah, R., Ambo, S. N. & Kurnia, S. I. 2017. Modification of the Caesar Chiper and Rail Fence Algorithms to Increase the Security of Alphanumeric Text and Special Characters. 2017 National Science and Technology Seminar, Faculty of Engineering, Muhammadiyah University, Jakarta 1-2 November 2017.
9. Munir, M. 2006, Cryptography, Publisher: Informatika Bandung
10. Pabokory, F. N., Astuti, I. F. & Kridalaksana, A. H. 2016. Implementation of Cryptographic Data Security in Text Messages, Document File Contents, and Document Files Using the Advanced Encryption Standard Algorithm. Mulawarman Informatics Journal Vol. 10 No. February 1 2015. Computer Science Study Program, FMIPA, Mulawarman University.
11. Ratna, D. 2018. Implementation of the Rail Fence Chiper Algorithm in 2-Dimensional Image Data Security. Pelita Informatics Journal, Volume 7, Number 1, July 2018 ISSN 2301-9425 (Print Media) Page: 38-42.
12. Setyaningsih, E, Iswahyudi, C. & Widyastuti, N. 2011. Super Encryption Concept to Increase Image Data Security. SNASTI 2011. Pg. 7-10.
13. Setyaningsih, E. 2015. Cryptography & Its Implementation Using Matlab. Yogyakarta: Andi Publishers. Vol 1, Pg. 250.
    Singh, A., Nandal, A. & Malik, A. 2012. Implementation of Caesar Cipher with Rail Fence for Enhancing Data Security. International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE) Vol 2, Issue 12: Pg. 78-82.