Jurnal Minfo Polgan
Volume 11, Nomor 1, Mater 2022
e-ISSN : 2797-3298
p-ISSN : 2089-9424

Playfair Cipher Algorithm in Learning Media

Subhan Hafiz Nanda Ginting[1)], M. Rhifky Wayahdi[2)], Surya Guntur[3)]
[1)2)]Universitas Battuta, Indonesia
[1)]subhanhafiz16@gmail.com, [2)]muhammadrhifkywayahdi@gmail.com, [3)]guntur@polgan.ac.id

Abstrak :
The level of security and confidentiality of information / data becomes very important in the era of increasingly sophisticated and developing technology. Cryptographic methods can be one solution to overcome problems in the level of security and confidentiality of information. However, knowledge about cryptography is still a lot of audiences who do not know and understand its use in securing the secrets of information, for that we need an application which presents a learning media that is expected to help provide knowledge from cryptography. This study implements a learning media application that discusses a Playfair Cipher classic cryptographic method, a cryptographic technique that encrypts bigrams using a matrix table consisting of 25 letters in it, text that can be encrypted in the form of alphabet letters on the system that has been tested. The results of the encryption and decryption of the text do not have spaces or symbols in it, the application of playfair cipher cryptographic learning media is aimed at computer students as a tool to better understand the playfair cipher cryptographic material.

Kata kunci :
Playfair Cipher ; Cryptography; Learning Media

INTRODUCTION

The development of communication and information technology at this time experiencing very rapid growth. Advances in information technology provide many advantages for human life, especially in the field learning, at the present time learning media are very widely used.

Learning media is a tool for teaching and learning. Everything which can be used to stimulate thoughts, feelings, attention and ability or learning skills so as to encourage the process study. One of the learning media is about computer security. Computer security is information security that is applied to computers and networks where one form of computer security is Cryptography. In computer lectures, cryptography is one of the courses that's taught and is very important for computer students to know about Cryptography. Cryptography is the study of techniques mathematics related to aspects of information security, such as data confidentiality, data integration, and data authentication. With cryptography data or information will be gated security from computer criminals. The problem that we often encounter in cryptography is a lack of explanation about cryptography and the steps of working on cryptography as well with learning media that only presents material without telling the process of its use, so that many students are less interested in deeper into learning about cryptography, especially for Playfair Cipher cryptography. Playfair Cipher is a classic cryptographic algorithm that belongs to in the polygram cipher, where the plaintext is converted into a polygram form and processes decryption encryption is done for the polygram. The cryptographic key is 25 the letters arranged in a 5x5 square by eliminating the letter J of the alphabet. The possible keys are 25, the arrangement of the keys in the square expanded by adding a sixth column and a sixth row. Sixth line is the first row, while the sixth column contains the first column. On Generally, the key is a series of words that are easy to understand.

Based on the results of data collection that I did among students there are still students who only know about cryptography, as well with knowledge of the Playfair Cipher algorithm, many of the students did interested if Playfair Cipher cryptography is made in the form of a medium learning Therefore, the authors will make learning applications for students especially Playfair Cipher cryptography learning, making this application using Microsoft Visual Studio 2010 with the VB.Net programming language,

*penulis korespondensi

e-ISSN : 2797-3298
p-ISSN : 2089-9424

where this application will display material about cryptography and Playfair Cipher step of the encryption. From the problems described above, the author raises the title research " Implementation of the Playfair Cipher Algorithm in learning media". The hope is that in the world of lectures the application is useful in increasing student interest in learning, especially in learning cryptography

RESEARCH METHOD

The playfair cipher algorithm is a classic encryption method that is very difficult to manually cryptanalyze. Even so, Playfair can be solved by using the information on the frequency of Bigram appearances. An important component in the Playfair algorithm is the cipher table used to encrypt and decrypt the default table introduced by Playfair which is a table in the form of a matrix of size (5x5) which contains the capital letters of A-Z by eliminating J (E. Haodudin Nurkifli, 2014). The use or function of the base64 algorithm is to hide confidential data so that it is not known by third people.

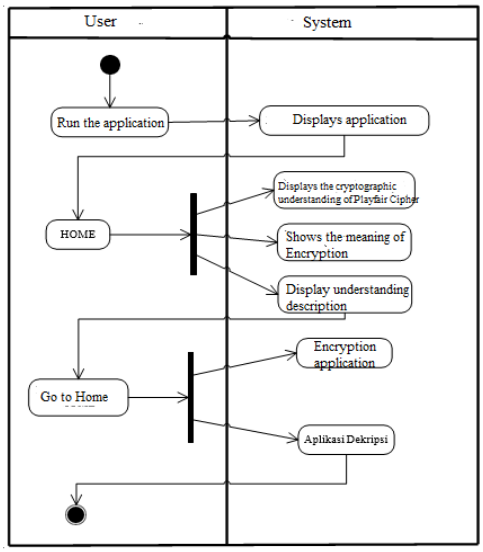
The application of the playfair cipher algorithm in making this cryptography learning application is done by collecting materials related to cryptography, the playfair cipher algorithm and so on. In this learning application. The understanding of cryptography will be applied, the understanding of the playfair cipher algorithm and examples of the encryption process and text descriptions using the playfair cipher algorithm and in the application later The encryption process and data descriptions are displayed so that students or users understand how to encrypt and describe data using the Playfair Cipher algorithm.

Use cases describe the sequence of activities carried out by actors and the system to achieve a specific goal. A Use Case presents an interaction between actors and the system and describes the expected functionality of a comparison system.

1. RESULTS AND DISCUSSION

The results of the design of the Playfair Cipher Cryptography learning media application are sorted from discussion, encryption and decryption. The discussion serves to present material about Playfair Cipher Cryptography, encryption is used to convert plaintext (text to be encrypted) into ciphertext (text that has been encoded), and decryption is used to return ciphertext to plaintext. The following is a display of the results and discussion of the Playfair Cipher Cryptography learning media application.

The main form is the overall Playfair Cipher Cryptography Learning Media Application interface, where to use this learning media application you can go through the main form interface. In the main form there is a strip menu, namely, the file menu which consists of profiles, and exits, the discussion menu, the application menu which consists of Encryption and Decryption and the help menu. For more details, the main form display can be seen in the following image:



*penulis korespondensi

e-ISSN : 2797-3298
p-ISSN : 2089-9424

Figure 1. Activity Diagram Initial Application Display

This encryption form functions to convert plaintext messages into ciphertext forms, so that the plaintext messages cannot be known. The things that can be done in this encryption form are inputting the text, then encrypting the text then we can clean the text that we have encrypted then we can exit the encryption form and return to the main form.

In the process of encrypting plaintext into ciphetext, we first input the text which we will encrypt in the input textbox, then input the keyword which will be the key in encrypting the message, then press the encrypt button, the plaintext we input will turn into ciphertext which will appear in the output textbox.

This decryption form serves to convert the ciphertext message back into plaintext form, so that the message can be read again. The things that can be done in this Decryption form are inputting the text, then decrypting the text then we can clean the text that we have described then we can exit the decryption form and return to the main form.

Blackbox testing is a software testing method that focuses on the functionality side, especially on application input and output (whether it is in accordance with what is expected or not). The testing or testing phase is one of the stages that must be in a software development cycle (other than the design or design stage). The following is the system testing with the black box testing method which is presented in the following black box testing table:

No	Scenario Testing	The results are expected	Result Testing	Conclusion
1	*Discussion strip menu*	The application processes the Discussion Strip Menu then a form appears discussion	As expected	*Valid*
2	*Application Strip Menu*	*Click the Extract Strip menu, an Encryption and Decryption form will appear*	As expected	*Valid*
3	*Menu Strip File*	*Selected Strip File menu will appear Profile form*	As expected	*Valid*
4	*Menu Strip Help*	*Strip Help menu is selected will appear Help form*	As expected	*Valid*

Table 1.Black Box Testing Main Form Testing Results

*penulis korespondensi

e-ISSN : 2797-3298
p-ISSN : 2089-9424

No	Scenario Testing	The results are expected	Result Testing	Conclusion
1	*Button Encrypt*	When the Encryption button is selected, the system will perform the Encryption process, a message box will appear which will display all input and a matrix table will appear to produce ciphertext	As expected	*Valid*
2	*Button Clear*	When the Button is clicked it will clean up display on the form	As expected	*Valid*
3	*Button Home*	When the Home Button is selected it will return to the Main Form	As expected	*Valid*

Table 2. Black Box Testing Results for Encryption Form

No	Scenario Testing	The results are expected	Result Testing	Conclusion
1	*Button Decrypt*	When the Decrypt button is selected, the system will perform the decryption process, a message box will appear which will display all input and a table will appear matrix	As expected	*Valid*
2	*Button Clear*	When the Button is clicked it will clear the display on the form	As expected	*Valid*
3	*Button Home*	When the Home Button is selected it will return to the Main Form	As expected	*Valid*

Table 3. Black Box Testing Results Form Description

*penulis korespondensi

e-ISSN : 2797-3298
p-ISSN : 2089-9424

CONCLUSION

By providing complete and lightweight cryptographic material to be understood in a learning medium with an attractive appearance, students will be more interested in learning about cryptography.
By presenting complete and easy-to-understand material in the form of text or images, as well as with examples of calculations on Playfair Cipher Cryptography, students will more easily understand and understand Playfair Cipher Cryptography. By creating a learning media that has an attractive appearance, it will increase student interest in using learning media as a medium for enhancing knowledge

REFERENCES

[1] E. Haodudin Nurkifli.2014. Modifikasi Algoritma Playfair Dan Menggabungkan Dengan Linear Feedback Shift Register (LFSR). Jurusan Teknik Informatika, Ilmu Komputer, Universitas Singaperbangsa Karawang.
[2] Sumandri.2017. Studi Model Algoritma Kriptografi Klasik dan Modern. Program Studi Pascasarjana Pendidikan Marematika, Universitas Negeri Yogyakarta.
[3] E. Haodudin Nurkifli.2014. Modifikasi Algoritma Playfair Dan Menggabungkan Dengan Linear Feedback Shift Register (LFSR). Jurusan Teknik Informatika, Ilmu Komputer, Universitas Singaperbangsa Karawang.
[4] Ginting SHN, Sawaluddin, Nababan EB. Performance improvement of ant colony optimization algorithm using multi-attribute rating simple technique exploiting ranks. International Journal of Research and Review. 2020; 7(2): 150-154.
[5] Hafiz Nanda Ginting , S., Rhifky Wayahdi, M., & Syahputra , D. (2020). IMPLEMENTATION OF SIMPLE ADDITIVE WEIGHTING (SAW) ALGORITHM IN DECISION SUPPORT SYSTEM FOR DETERMINING WORKING AREA FOR COOPERATIVE. *INFOKUM*, *9*(1), 7-10. Retrieved from http://infor.seaninstitute.org/index.php/infokum/article/view/74
[6] S. Hans, R. Johari and V. Gautam, "An extended Playfair Cipher using rotation and random swap patterns," 2014 International Conference on Computer and Communication Technology (ICCCT), Allahabad, 2014, pp. 157-160, doi: 10.1109/ICCCT.2014.7001485.
[7] P. Murali and G. Senthilkumar, "Modified Version of Playfair Cipher Using Linear Feedback Shift Register," 2009 International Conference on Information Management and Engineering, Kuala Lumpur, 2009, pp. 488-490, doi: 10.1109/ICIME.2009.86.
[8] K. Jia, J. Chen, M. Wang and X. Wang, "Practical-time Attack on the Full MMB Block Cipher," International Association for Cryptologic Research, 2010
[9] S. V.U.K and K. Shirisha, "A Block Cipher Involving a Key Matrix and a Key bunch Matrix, Supplemented with Mix," International Journal Of Engineering And Science, vol. II, no. 9, pp. 37-43, 2013.
[10] A. Joux, Algorithmic Crypanalysis, United States: CRC Press, 2009.
[11] J. Seberry, Cryptography: An Introduction to Computer Security (Advances in Computer Science Series), Prentice Hall, 1989.
[12] A. Alam, S. Khalid and M. Salam, "A Modified Version of Playfair Cipher Using 7," IJCTE, pp. 626-628, 2013.
[13] Andrew S. Tanenbaum, Networks Computer, 5th edition, Pearson Education, ISBN-10: 0132553171.
[14] Aftab Alam, Sehat Ullah, Ishtiaq Wahid, & Shah Khalid, “Universal Playfair Cipher Using MXN Matrix”. International Jourrnal of Advanced Computer Science, Vol.1, No.3, Pp.113-117, Sep.2011.
[15] Ravindra Babu K, S.Uday Kumar, A. Vinay Babu, I.V.N.S. Aditya, P.Komuraiah, “An Extension to Traditional Playfair Cryptographic Method”. International Journal of Computer Applications (0975 – 8887), Volume 17- No.5, March 2011.
[16] Muhammad Salam, Nasir Rashid, Shah Khalid, Muhammad Raees Khan, “A NXM Version of 5X5 Playfair Cipher for any Natural Language (Urdu as Special Case)”. World Academy of Science, Engineering and Technology 73 2011.
[17] Muhammad Salam, Nasir Rashid, Shah Khalid, Muhammad Raees Khan, “A NXM Version of 5X5 Playfair Cipher for any Natural Language (Urdu as Special Case)”. World Academy of Science, Engineering and Technology 73 2011.
[18] G. Sivagurunathan, V. Rajendran, & T. Purusothaman “Classification of Substitution Ciphers using Neural Networks,” (March, 2010) International Journal of Computer Science and Network Security, vol. 10, no. 3, pp. 274-279.
[19] Poonam. G, "A comparison of memetic & tabu search for the cryptanalysis of simplified data encryption standard algorithm", International Journal of Network Security & Its Applications (IJNSA), Vol.1, No 1,pp34-42

*penulis korespondensi

e-ISSN : 2797-3298
p-ISSN : 2089-9424

[20] Shiv Shakti Srivastava & Nitin Gupta , Security aspects of the Extended Playfair cipher. IEEE International Conference on Communication Systems and Network Technologies, p144-147,2011.

*penulis korespondensi