Utility Software Design to Comprehend The Cryptography Cast-128 Method

Nopriadi*, Akbar Iskandar2, Listia Utami2 and Okma Yandri3
1Department of Information System, Universitas Putera Batam, Batam, Indonesia
2Department of Informatics, STMIK AKBA, Makassar, Indonesia
3Department of Civil Engineering, Universitas Musi Rawas, Indonesia
* nopriadi.jamil@gmail.com

Abstract. At present, data security techniques known as cryptography are influential and widely used. There are lots of cryptographic algorithms. The main problem faced by a student taking this course is they difficult to understand the procedures of a cryptographic algorithm due to its complexity and involves many calculations. CAST is a block ciphers belonging to the family of DES (Data Encryption System) that uses substitutions and permutations (known as Substitution Permutation Network or SPN) in key calculations and encryption and decryption processes. The CAST algorithm has two versions, namely CAST-128 and CAST-256 where both are distinguished by the length of the used key. The maximum Key length allowed in CAST is 128 bits or 16 characters. In addition CAST-128 allows key sizes to vary from 40 bits to 128 bits with the addition of 8-bits. While the length of plain text that can be encrypted and decrypted is 64 bits (8 characters) and supports all types of plain text. This study describes the procedures of CAST-128, the design of encryption procedures from CAST-128, calculations from the Key Schedule using Substitution Boxes (S-Boxes), how the CAST-128 encryption and decryption algorithms work, the results of the implementation of the CAST-128 algorithm created a program that also functions as a learning program to understand the CAST-128 algorithm with the process of key formation, CAST-128 algorithm encryption and decryption.

1. Introduction
Cryptography often used in data security [1][2][3]. One of these methods was the CAST-128 method wherever understood this method is difficult. This is due to the many steps that must be done such as the number of substitutions, bitwise functions, operating modes, and added iterations in the encryption and decryption process [4], [5][6]. At present there is not much software that can function as a medium of learning cryptographic methods [7][8].

For this reason, the researcher tried to offer a step to understand the working concept of CAST-128 by developing the teaching software that related with that method. The teaching software is designed by utilizing visual programming facilities so the CAST-128 method can be easily understood and become more interactive.

2. Related Works
CAST is a block ciphers belonging to the family of DES (Data Encryption System) that uses substitutions and permutations (known as Substitution Permutation Network or SPN) in key
calculations and encryption and decryption processes [9][10][11]. The CAST algorithm itself has two versions, namely CAST-128 and CAST-256 where both are distinguished by the length of the key used. The maximum Key length allowed in CAST is 128 bits or 16 characters. In addition CAST-128 allows key sizes to vary from 40 bits to 128 bits with the addition of 8-bits [12]. While the length of plain text that can be encrypted and decrypted is 64 bits (8 characters) and supports all types of plain text.

3. Research Methodology

3.1. Design Stage
Data collection is carried out by researchers in library where researchers take materials and sources related to the topics discussed by searching in books, articles, lecture materials, and websites that are on the Internet[13]. The data obtained comes from a website that discusses cryptographic data compression algorithms and the CAST-128 method.[14] Data analysis techniques form for examples of CAST-128 method calculations both for the encryption process and decryption process [15]. This application was developed using the Rapid Application Development (RAD) methodology with the following stages:

a. Collect various data and information related to the program to be designed.
b. Planning is the stage of planning the application design that will be created and collected
c. Algorithms used in designing applications.
d. The prototype is to make the user interface form based on the planning stages above.
e. Analysis is to do an analysis of the prototype that is designed if there is an error, then made a correction.
f. Design is to design an improved prototype using one programming language that supports RAD [9]. At this stage of design if there are discrepancies, steps can be repeated in the prototype and analysis section.
g. Implementation is to implement a prototype that has been designed, perform testing and repair.

In this requirements analysis part system was decomposed on what requirements are needed so this learning program can be designed and available at any facility. At this stage testing is carried out on a system designed using various input strings to obtain the desired results..

3.2. Block Cipher
Block cipher is a form of symmetry key encryption algorithm (secret key cryptography) that transforms a particular block of data from the plaintext into one block of ciphertext data with the same block length [16][17]. This transformation takes place through the use of a secret key provided by the user. Decryption is also done by using reverse transformation from one block of ciphertext data back to one block of plaintext data with the same key and block length. The block length is called a block size where the block size can vary such as 16-bit, 32-bit, 64-bit, 128-bit, or 256-bit. The properties possessed by encryption and decryption techniques such as ECB (Electronic Code Book), CBC (Cipher Block Chaining), CFB (Cipher Feedback Block), and OFB (Output Feedback Block) [18][19].

In ECB mode each plaintext block is encrypted independently with block cipher [14] [15]. ECB mode has the same level of security as a block cipher. Each identical plaintext block produces identical ciphertext blocks. The speed of each encryption operation is identical to the speed of the block cipher. The ECB can easily carry out parallel processes to produce higher performance. However, it is unfortunate that there is no process before a block be read (except for key formation).

3.3. Algoritma
Algorithms are steps, gradual and specific sequences of problems. This algorithm then translated into programs using certain programming languages. Algorithms are used to analyze and explain the sequence and relationship between the activities to be taken. In addition the algorithm also functions to solve a problem so the desired goal achieved.
3.4. Iterated Block Cipher (Block Cipher with Iteration)

Iterated Block Cipher encrypts a plaintext block process has several rounds[20] [21]. In each round of transformation (also known as round function) applied to the data using sub key. The sub key set is usually determined from the key provided by the owner with a special function. The number of turns in an iteration depends on the level of security desired and considers the efficiency of time. In general, an increase of the number turns will increase security, but for some techniques the number of turns is needed to achieve a sufficient level of security.

Feistel Cipher is a special form of Iterated Block Cipher where the ciphertext is obtained from the plaintext by using repeated transformations or the same spin function. Feistel Ciphers are often referred to as DES-like ciphers. In the feistel cipher, the text being encrypted is broken down into two equal parts, namely Left and Right. The Round function is applied to one of the pieces using a sub key and the results are XORed with the other pieces. Then both the left and right pieces are exchanged. Each round follows the same pattern, except for the last round where there is no more data exchange. [22]

4. Result and Discussion

4.1. Design

In the design section will be explained regarding the design of the program. In this section we will explain the design of the display (form design) and the design of a module that contains functions. The design of the program form is done in the Visual Basic environment. [23]

In general, the program can carry out encryption operations on strings and other parts separately are used to explain the cryptographic theory and the procedures of the CAST-128 algorithm so that in general this program can be used as a special learning program for the CAST-128 method.

The form designed includes: menu form, learning form, CAST-128 algorithm form, encryption form, decryption form, key generation form, tutorial form 1, and tutorial form 2 and tutorial form 3. Especially the three forms mentioned at the end are used to teach cryptographic theory, operations used at CAST-128, and the theory of encryption and decryption algorithms from CAST-128. This has the purpose that the user who after reading the topics in these three forms can immediately try with various key values, plain text, and cipher text on the next form, namely the encryption form, the decryption form, and the key generation form. [24]

First, the form was designed is the menu form. The design form of this form can be seen in Figure 4.1. This form is also called the main form because from this form other forms can be accessed. Each display to another form when the user closes the form, the display will be returned to this form. [25]

In general, this form is formed by using graphic components such as labels, command buttons, and picture boxes. Parts made using labels are texts that have captions such as "MAIN MENU", "STMIK IIBBI Medan 2011", and "Program Designed by: Bayu Sunanda". In addition, the layout shows that two boxes are picture box objects that will be placed on the image to beautify the form. The other three command buttons function as buttons that have the following functions:

1. The button with the caption "Learning" is used to call the learning menu form.
2. The button with the caption "CAST Algorithm" 128 "is used to call the third menu form.
3. The button with the "Exit" caption is used to exit the program.

4.2. Use Case Module Design

The Module Function is useful for declaring all functions related to encryption and decryption operations and key generation. These functions include the rotate and shift, number conversion functions and number conversion functions such as decimal to binary or vice versa, decimal to hexadecimal or vice versa. The design of this module also involves writing code and the results of all the functions above stored in one modMain.bas file.
4.3. How to Run the Program
To use this software, run the CAST128.EXE file, the form menu will display. To access certain parts of the program, click on the desired button, for example:

1. Operation at CAST - 128: section on learning operations at CAST-128
2. CAST-128 Encryption and Decryption Algorithms: CAST-128 key formation, encryption, and decryption algorithms.
3. Key Generation: to look at learning CAST-128 sub key forming algorithms.
4. Encryption: to see the learning of the CAST-128 encryption algorithm.
5. Decryption: to see learning CAST-128 decryption algorithms.
6. Exit: to exit this program.

5. Conclusion
From the results of the research made, the researcher can draw conclusions include:
1. With the CAST 128 learning software that showed how to calculate the key formation process, the encryption process, and the CAST-128 decryption stages, the CAST-128 algorithm is easier to understand.
2. The encryption and decryption process used the same form because CAST-128 encryption is only different in the use of and variable functions.
3. The output of this program can be used to analyze the CAST 128 algorithm.

References
[1] A. H. Hasugian, “Implementasi Algoritma Hill Cipher Dalam Penyandian Data,” Pelita Informatika Budi Darma, vol. 4, no. 2, pp. 115–122, 2013.
[2] D. Ariyus, Pengantar Ilmu Kriptografi: Teori Analisis & Implementasi. Penerbit Andi, 2008.
[3] R. Rahim et al., “HASHING VARIABLE LENGTH APPLICATION FOR MESSAGE SECURITY COMMUNICATION,” ARPN Journal of Engineering and Applied Sciences, vol. 14, no. 1, pp. 259–264, 2019.
[4] M. Nurtanto et al., “Information media literacy to improve working concept comprehension of ignition system with contact breaker and problem-based learning,” no. February, 2019.
[5] R. El Islami, I. J. Sari, S. Sjaifuddin, M. Nurtanto, M. Ramli, and A. Siregar, “An Assessment of Pre-service Biology Teachers on Student Worksheets Based on Scientific Literacy,” Journal of Physics: Conference Series, vol. 1155, p. 012068, 2019.
[6] A. Iskandar et al., “Web based testing application security system using semantic comparison method,” in IOP Conference Series: Materials Science and Engineering, 2018, pp. 1–6.
[7] W. Diffie and M. Hellman, “New directions in cryptography,” IEEE transactions on Information Theory, vol. 22, no. 6, pp. 644–654, 1976.
[8] A. Iskandar, M. Rizal, N. Kurniasih, D. U. Sutiksmo, and A. Purnomo, “The Effects of Multimedia Learning on Students Achievement in Terms of Cognitive Test Results,” in Journal of Physics: Conference Series, 2018, pp. 1–7.
[9] J. Benaloh, “Dense probabilistic encryption,” in Proceedings of the workshop on selected areas of cryptography, 1994, pp. 120–128.
[10] C. M. Adams, “Constructing symmetric ciphers using the CAST design procedure,” Designs, Codes and cryptography, vol. 12, no. 3, pp. 283–316, 1997.
[11] A. Iskandar, E. Virma, and A. S. Ahmar, “Implementing DMZ in improving network security of web testing in STMIK AKBA,” International Journal of Engineering and Technology(UAE), vol. 7, no. 2,3 Special Issue 3, 2018.
[12] P. Junod and S. Vaudenay, “FOX: a new family of block ciphers,” in International Workshop on Selected Areas in Cryptography, 2004, pp. 114–129.
[13] D. Sudrajat et al., “Expert System Application for Identifying Formalin and Borax in Foods Using the Certainty Factor Method,” Eurasian Journal of Analytical Chemistry, vol. 13, no. 6, pp. 321–325, 2018.
[14] M. Bellare, T. Kohno, and C. Namprempre, “The secure shell (SSH) transport layer encryption modes,” 2005.

[15] M. I. Alam and M. R. Khan, “Performance and efficiency analysis of different block cipher algorithms of symmetric key cryptography,” International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 10, 2013.

[16] D. Surian, “Algoritma Kriptografi AES Rijndael,” TESLA Jurnal Teknik Elektro UNTAR, vol. 8, no. 2, pp. 97–101, 2009.

[17] A. Mousa and A. Hamad, “Evaluation of the RC4 algorithm for data encryption,” IJCSA, vol. 3, no. 2, pp. 44–56, 2006.

[18] N. R. Potlapally, S. Ravi, A. Raghunathan, and N. K. Jha, “A study of the energy consumption characteristics of cryptographic algorithms and security protocols,” IEEE Transactions on Mobile Computing, vol. 5, no. 2, pp. 128–143, 2006.

[19] T. J. Naughton, B. M. Hennelly, and T. Dowling, “Introducing secure modes of operation for optical encryption,” JOSA A, vol. 25, no. 10, pp. 2608–2617, 2008.

[20] G. Jakimoski and L. Kocarev, “Chaos and cryptography: block encryption ciphers based on chaotic maps,” IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, vol. 48, no. 2, pp. 163–169, 2001.

[21] L. Kocarev and G. Jakimoski, “Logistic map as a block encryption algorithm,” Physics Letters A, vol. 289, no. 4–5, pp. 199–206, 2001.

[22] D. Abdullah, R. Rahim, D. Hartama, A. Abdisyah, Z. Zulmiardi, and S. Efendi, “Application of Web Based Book Calculation using Deterministic Dynamic Programming Algorithm,” Journal of Physics: Conference Series, vol. 1019, p. 012040, Jun. 2018.

[23] H. J. Muhasin, R. Atan, M. A. Jabar, S. Abdullah, and S. Kasim, “Multilayered Framework to Enhance Management Information Systems Decision on Sensitive Data in Cloud Computing Environment,” JOIV: International Journal on Informatics Visualization, vol. 1, no. 4–2, pp. 179–183, Nov. 2017.

[24] Y. S. Shuen, N. Arbaiy, and Y. Y. Jusoh, “Fertilizer Information System for Banana Plantation,” JOIV: International Journal on Informatics Visualization, vol. 1, no. 4–2, pp. 204–208, Nov. 2017.

[25] and E. Ongko, O. S. Sitompul, and E. B. Nababan, and D. Abdullah, “Hybrid Approach Redefinition (HAR) Method with Loss Factors in Handling Class Imbalance Problem,” in 2018 International Symposium on Advanced Intelligent Informatics (SAIN), 2018, pp. 56–61.