International Journal of Basic and Applied Science 10 (3) (2021) 91-98

Published by: IOCSCIENCE

International Journal of Basic and Applied Science

Journal homepage: www.ijobas.pelnus.ac.id

Comparison of Performance Rot13 and Caesar Cipher Method for Registration Database of Vessels Berthed at P.T. Samudera Indonesia

Risman
Department of Computer Science, Faculty of Faculty of Engineering and Computer Science
Universitas Potensi Utama, Indonesia

Article Info

***Article history*:**

Received Sep 9, 2021
Revised Oct 26, 2021
Accepted Nov 05, 2021

***Keywords*:**

Database ;
Chryptography ;
ROT13 ;
Chaesar Chiper.

ABSTRACT

Database security is a very important aspect of an information system. A general information is onlyintended for certain groups. Therefore, it is very important for a company to prevent database leakage sothat the information contained in it does not fall to unauthorized people. Cryptographic technique is an alternative solution that can be used in database security. One way to maintain the security of the database is to use encryption techniques. The method used to secure the database is encryption using the ROTI3 and Caesar Cipher methods. Both of these methods have advantages in processing speed. For thisreason, the author will compare the use of the two algorithms above in terms of the encryption and decryption process time.

Corresponding Author:

Risman,
Department of Computer Science,
Faculty of Faculty of Engineering and Computer Science Universitas Potensi Utama, Indonesia
JL. KL. Yos Sudarso Km. 6,5 No. 3-A, Kota Medan, Sumatera Utara 20241, Indonesia
Email: anaklabuhan@gmail.com

1. INTRODUCTION

Cryptographic algorithms are divided into two major groups, namely symmetric algorithms and asymmetric algorithms. The symmetric algorithm uses a secret key that is shared by both the sender and the receiver. The asymmetric algorithm has two different keys, namely a public key and a different private key for the encryption and decryption process. Examples of symmetric algorithms are Caesar Cipher and ROT13 algorithms. The author tries to apply and make comparisons between the two methods mentioned above in data security because each cryptographic algorithm has its own complexity that affects the performance of the algorithm. The comparison of the performance level can be seen from the speed of the data encryption process between the Caesar cipher and ROT13 methods. The processing time is influenced by various aspects of the computer equipment and the data being processed. Algorithms that have fast processing times are preferred in processing large data. Therefore, the calculation of the algorithm analysis is needed to determine the performance based on the processing time of the algorithm being analyzed.[1] The ability to access and provide data quickly and accurately becomes very essential for an organization, whether in the form of commercial organizations (companies), universities, government institutions, or individuals

(personal). This is made possible by developments in the field of computer technology and telecommunications.

PT Samudera Indonesia Tbk ("Samudera Indonesia"/"the Company") is an integrated cargo transportation and logistics company established in 1964. Samudera Indonesia has 5 business lines: Samudera Shipping, Samudera Logistics, Samudera Ports, Samudera Property, and Samudera Services to provide high quality service to customers. Supported by 4,000 employees, more than 40 subsidiaries and offices in various parts of Indonesia and Asia, Samudera Indonesia is committed to providing the best solutions in cargo transportation and logistics[2].

The ship's arrival and arrival procedures have been regulated in the transportation service law. In order to facilitate and speed up service users who will register their ships, the Directorate General of Sea Transportation has built an online ship registration service application system. The application of this online ship registration service application is carried out as an effort to respond to community demands for technological developments and information disclosure to accelerate services, especially in the field of ship registration so that the Ministry of Transportation can further accelerate services to ship owners. The application that has been launched is the Sipariban application. This application is used to provide information on ship services at the Port of Belawan[3], such as a list of ships that are leaning on and waiting to dock, data on docks that are ready to dock, as well as waiting times for ships and the estimated time of docking ships at the Port of Belawan.

In this application there is information on ship data that will lean on a port that has previously been registered by the company or ship owner, and that information becomes very important and can be misused for certain purposes and can be detrimental to the ship owner company if their ship information data is misused[4] . Important information such as the identity of the ship and the owner's personal identity stored in the database is important data that is dangerous if known by others. Therefore, the author assumes that it is a problem that must be solved by making an implementation of securing the docking ship registration data, to maintain the security and confidentiality of the data in a database, several safeguards are needed to make the data unreadable or understandable by just anyone, except by the rightful recipient, several ways have been developed to deal with this security problem, one of which is a data encoding technique known as cryptography.

So much information is exchanged every second on the internet. there is also a lot of theft of information by irresponsible parties. Security threats that occur to information are: (1). Interruption, Interruption is a form of threat to availability, where data is damaged so that it cannot be used anymore. The acts of destruction that can be done can be in the form of physical or non-physical damage. Physical damage is generally in the form of destruction of hard disks and other storage media and cutting network cables. While non-physical destruction in the form of deletion of certain files from the computer system. (2). Interception, Interception is a form of threat to secrecy, in which an unauthorized party has succeeded in obtaining access rights to read data/information from a computer system. Actions that are usually carried out are usually through wiretapping of data transmitted via public / public lines. Actions like this are commonly known as wiretapping in wired networking (networks that use cables as data transmission media). (3). Modification, Modification is a form of threat to integrity, in which unauthorized parties have succeeded in obtaining access rights to modify data/information from a computer system. Usually the data / information that is changed is a record from a table in the database file. (4). Fabrication, Fabrication is also a form of threat to integrity. The usual action is to imitate and enter an object into the computer system. The object that is inserted can be a file or a record that is inserted in an application program[5].

Cryptography basically consists of two processes, namely the encryption process and the decryption process. The encryption process is the process of encoding an open message into a secret message (ciphertext). This ciphertext will later be sent through open communication channels. When the ciphertext is received by the recipient of the message, the secret message is converted again into an open message through the decryption process so that the message can be read again by

the recipient of the message Anwar, (2017), In general, the encryption and decryption process can be described as follows;

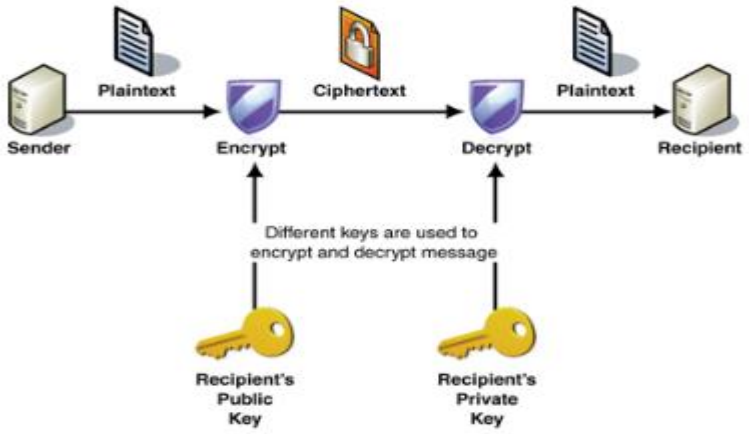

Figure 1. Chryptography flow

Cryptography is the science and art of maintaining the confidentiality of messages by encoding them into a form that can no longer be understood. In cryptography, there are two processes, namely encryption and decryption. The message to be encrypted is referred to as plaintext (plain text). So called because this information can easily be read and understood by anyone[7]. The algorithm used to encrypt and decrypt a plaintext involves the use of some form of key. A plaintext message that has been encrypted (or encoded) is known as ciphertext, Caesar Cipher ROT13 is a function that uses the Caesar code with a shift of k=13. ROT13 is designed for security on UNIX operating systems which are often used in on-line forums, serves to cloak the content of articles so that only authorized people can read them. The ROT13 encryption system this time by shifting the character forward 13 times, counting 1 is the character in front of it, and shifting the character based on the sequence of characters in the ASCII table. As a decryption, by rewinding the character 13 times. The first substitution in the world of data security was during the reign of Julius Caesar, so it was known as the Caesar Cipher, namely changing the position of the initial letter of the alphabet, Caesar cipher is also known as the Shift Cipher [8].

In cryptography, Caesar cipher, or shear cipher, Caesar cipher or Caesar cipher is one of the simplest and most well-known encryption techniques. This password includes a substitution password where each letter in plaintext is replaced by another letter that has a certain position difference in the alphabet. In Caesar Cipher, each letter is substituted with the next third letter of the same alphabetical order. In this case the key is letter shift (ie 3).

Caesar cipher is very easy to use. The essence of this cryptographic algorithm is to shift all characters in plaintext with the value the same shift. The steps taken to form a ciphertext with Caesar cipher are: (1). Determine the magnitude of the character shift used in forming the ciphertext to plaintext. (2). Changing characters in plaintext into ciphertext based on a predetermined shift. For example, it is known that shift = 3, then the letter A will be replaced by the letter D, the letter B becomes the letter E, and so on.

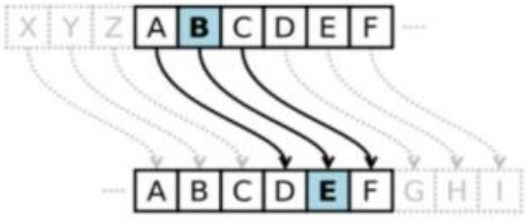

Figure 2. Chryptography flow

2. RESEARCH METHOD

2.1. Analysis Stages

Methods Data collection is carried out to analyze the results of the work of these two methods in determining the results, in the research methodology there are things that need to be underlined, namely the data collection method which is the steps for collecting data by studying literature/library, literature study is used to obtain supporting theories for the application. will be made, namely by collecting reference materials from books, articles, journals, papers and internet sites related to the achievement of research objectives, then the author conducts data analysis[9], and at this stage aims to collect data directly obtained either directly with the interview stage or indirectly requested from PT.Samudera Indonesia, for securing the registration database for the Ship docking, after that the author carried out the design of the System design where the user interface design and application program structure were from the PT. Samudera Indonesia office, a careful methodology t and effectively will produce accurate and valid steps so that they can answer the desired results from the user and especially for PT. Samudera Indonesia in determining the security of the docking ship registration database, this aims to make it easier for operators to secure the database[10].

System analysis is the initial phase in designing a system. This analysis aims to understand and describe clearly what must be done in the process of designing a system[11]. In this study, system analysis is divided into problem analysis, needs analysis and process analysis, The data cryptography process is an important step in conducting classification analysis which aims to clean data from elements that are not needed to speed up the classification process. below is a flowchart of the preprocessing stages of the data used.

At this stage, an analysis of the comparison of two cryptographic algorithm methods is carried out. The flowchart of the Caesar Cipher Algorithm Encryption process in this study will be shown in the picture ;

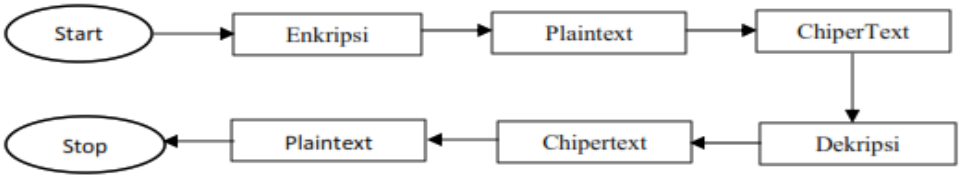

Figure 3. Chryptography process flow.

In cryptography, the process of encoding plaintext into ciphertext is called encryption. While the process of returning ciphertext to plaintext is called decryption. The parameters used for the transformation of encryption and decryption are called keys Munir, (2006). According to Paar and Pelzl (2010), cryptography aims to provide security services as follows:

a) Confidentiality. Information is kept confidential from all unauthorized parties.
b) Integrity. Allows the recipient of the message to check that the data was not modified during transmission; The intruder cannot replace the wrong message with the real one.
c) Authentication. Allows the recipient of the message to confirm the authenticity of the data; intruders cannot impersonate someone else[12].
d) Non-repudiation. Each communicating entity cannot reject or deny the data that has been sent or received

At this stage the authors perform an analysis of the comparison of the two cryptographic algorithm methods, the analysis of the comparison of these two methods to determine the easiest method to be carried out by the PT operator. Indonesia Samudera in determining the security of the docking ship

database, the following authors show the Flowchart of the Caesar Cipher Algorithm Encryption process

3. RESULTS AND DISCUSSION

3.1. Sedimentation

In the analysis of this result process the author will apply the Caesar Cipher and ROT13 cryptographic algorithms, the user who acts as the sender of the message will make a comparison by randomizing the message text with the ROT13 method, so before doing the encryption it must be known in advance that the ROT13 method is a system where letters are replaced with letters that are 13 positions away from it. For example, the letter "A" is replaced by the letter "N", the letter "B" is replaced by the letter "O", and so on

Table. 1 ROT13 substitution

A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

In the mathematical formula can be written as follows;

C = ROT13 (P) (2.1)

Example :

C = ZNTVFGRE

P = MASTER

To restore it back to its original form (decryption), the ROT13 encryption process is carried out twice.

P = ROT13 (ROT13 (P)) (2.2)

Example :

P = MASTER

C = ZNTVFGRE

ROT13 is not designed for a high level of security. ROT13, for example, is used to cloak the contents of articles (posts) on Usenet news that smell offensive. So that only people who really want to read can see the contents. Another example of use is to cover the answer to a riddle or the like [13].

3.2. Process Analysis Results Caesar Cipher

The scientific basis of Caesar cipher is mostly mathematics which includes number theory, algebra and functions. Caesar cipher formula in general:

C = E (P) = (P + k) mod 26 (2.3)

And the decryption function is:

P = D (C) = (C - k) mod 26 (2.4)

How this cipher works can be illustrated by lining up two sets of alphabets; The cipher alphabet is arranged by sliding the regular alphabet to the right or left by a certain number (this number is called a key). For example Caesar cipher with key 3, is as follows:

Common Alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Password Alphabet: DEFGHIJKLMNOPQRSTUVWXYZABC

To encode a message, simply search for each letter you want to encode in the regular alphabet, then write the corresponding letter in the cipher alphabet [14]. To crack the password, use the opposite method, in this thesis the author takes the example of encoding a message as follows:

Plaintext: MASTER
Ciphertext: ESYAKLWJ

By encoding each letter of the alphabet with an integer: 'A'= 0 , 'B'= 1,..., 'Z'= 25, then mathematically the shift of 3 alphabetic letters is equivalent to performing a modulo operation on plaintext P to ciphertext C with the equation:

C = E (P) = (P + 3) mod 26 (2.5)

Because there are 26 letters in the alphabet. The recipient of the message returns the ciphertext again with the inverse operation, mathematically it can be expressed by the equation:

P = D (C) = (C - 3) mod 26 (2.7)

It can be noted that the function D is the inverse of the function E, namely:

D (C) = E-1 (P) (2.8)

The use of Caesar cipher can be modified by changing the number of shifts (not just 3) and also the direction of the shear. This is done to make it more difficult for people who want to intercept messages because [16], eavesdroppers have to try all combinations (26 possible slides), in this comparison the author will start with plaintext;

Plaintext : MASTER

Ciphertext : ESYAKLWJ

Where ;

P = MASTER

K = 18

Where M is ;

C = (12 + 18) mod 26

C = (30) mod 26

C = 30

C = E

Where A is ;

C = (0 + 18) mod 26

C = (18) mod 26

C = 18

C = S

Where G is ;

C = (6 + 18) mod 26

C = (24) mod 26

C = 24

C = Y

Where I is ;

C = (8 + 18) mod 26

C = (26) mod 26

C = 26

C = A

Where S is ;

C = (18 + 18) mod 26

C = (36) mod 26

C = 36

C = K

Where T is ;

C = (19 + 18) mod 26

C = (37) mod 26

C = 37

C = L

Where E is ;

C = (4 + 18) mod 26

C = (22) mod 26

C = 22
C = W

Where R is ;

C = (17 + 18) mod 26
C = (35) mod 26
C = 37
C = J

So that the ciphertext can be obtained as follows ESYAKLWJ [17], from the comparative analysis of the data, the Caesar cipher method is the safest way compared to the ROT13 method in securing databases on ships docking at PT. Samudera Indonesia, to see the results and implementation can be seen in the following chapter:

Figure 3. The Result

The performance process compares these two methods by entering the same variable (same input), the same time and will get different results, from the comparison results obtained at the same time [18], both at the same time, the encryption and description can be obtained. the same accuracy and speed, but with the existing program flow it can be seen that the security of the registration database is safer by using the Caesar Cipher Algorithm [19], because security uses the existing key, so in this case the author can conclude the performance of the two comparisons of this method that the Caesar Cipher Algorithm more secure[20],[21].

4. CONCLUSION

From the results of the research conducted, the conclusions Based on the description and explanation of the results is, The implementation of the PHP-based Caesar cipher cryptographic algorithm has been successfully carried out. The resulting system runs according to the algorithm used, Comparison for security can be done, and secondly The scrambled plaintext can be returned to its original form, and based on the graph of the relationship between the encryption process time and the plaintext size, it shows that there is no effect on the speed of processing time based on the total length of the plaintext in each algorithm, but if the length of the plantex is added, it will be seen that the security is The most effective method is to use the Caesar Cipher method, and last is based on changes in the ciphertext results in the test, the use of the Caesar cipher cryptographic algorithm is relatively safer than using the ROT13 method.

REFERENCES

[1] Abdul Kadir, 2003. Pengenalan Sistem Informasi. Andi. Yogyakarta Al-Bahra bin ladjamudin. (2005). Analisis dan Desain Sistem Informasi. Graha Ilmu: Yogyakarta.
[2] Akbar, M. (2010). "Sistem Informasi Penjualan Motor Berbasis Web". Jurusan Teknik Informatika UPN, 11–77.
[3] Amril, S. (2013). Perancangan Sistem Informasi Penjualan Sepeda Motor Honda Berbasis Web Pada Dealer PT. Nusa Motor Ponorogo. Jurusan Teknik Informatika Universitas Muhammadiyah Ponorogo.Rahmel, D. (2008). *Visual Basic.NET*. New York: McGraw-Hill
[4] AndriKristanto, 2003, *Keamanan Data Pada Jaringan Komputer*, Penerbit Gava Media, Yogyakarta.
[5] Arief S, S. (2009). Media Pendidikan: Pengertian, pengembangan dan pemanfaatannnya. Raja Grafindo Persada.
[6] Ariyanto, A. B. (2009). Simulasi Enkripsi dan Dekripsi Berbasis Algoritma Blowfish.
[7] Ariyus, D. (2008). Pengantar Ilmu Kriptografi: Teori Analisis & Implementasi. Penerbit Andi. Arti kata simulasi Kamus Besar Bahasa Indonesia (KBBI) Online. (t.t.). Diambil 26 November 2018, dari https://kbbi.web.id/simulasi.
[8] B. Nugroho. (2005). Database Relasional dengan MySQL. C.V Andi Offset: Yogyakarta. Fahmi, I. (2016). *Teori dan Teknik Pengambilan Keputusan: Kualitatif dan Kuantitatif*. Jakarta: Rajawali Pers.
[9] Basheer, S., & Sreedhar, S. (2015). Crypto View: Visual Representation of Cryptographic Algorithms. 4(11).
[10] Dian Rachmawati & Ade Candra. (2015). Implementasi Kombinasi Caesar dan Affine Cipher untuk Keamanan Data Teks. 1.
[11] Ernie. (2009). Diagram Alir (Flowchart). 14 September 2009. https://ndoware.com/diagram-alir-flowchart.html
[12] Kendall, K.E, dan J.E. Kendall, 2003, *Analisis Perancangan Sistem, Edisi-5, Jilid I* Penerbit P.T. Indeks, Jakarta.
[13] Rahmat Lianda, 2008, *Analisis dan Perbandingan Skema Digital Signature Spesial*, Penerbit ITB, Bandung.
[14] Schneiner, B., 2000, *Applied Cryptography: Protocols, Algorithm, and Source Code in C*, Penerbit Wiley, New York.
[15] G. Kidanemariam and M. Uhlmann, "Interface-resolved direct numerical simulation of the erosion of a sediment bed sheared by laminar channel flow," Int. J. Multiph. Flow, vol. 67, pp. 174–188, 2014.
[16] M. Le, S. Cordier, C. Lucas, and O. Cerdan, "A faster numerical scheme for a coupled system modeling soil erosion and sediment transport," Water Resour. Res., vol. 51, no. 2, pp. 987–1005, 2015.
[17] C. Peng, Y. Teng, B. Hwang, Z. Guo, and L.-P. Wang, "Implementation issues and benchmarking of lattice Boltzmann method for moving rigid particle simulations in a viscous flow," Comput. Math. with Appl., vol. 72, no. 2, pp. 349–374, 2016.
[18] D. R. L. Vedoy and J. B. P. Soares, "Water-soluble polymers for oil sands tailing treatment: Review," Can. J. Chem. Eng., vol. 93, no. 5, pp. 888–904, 2015.
[19] Ata, M. S., Liu, Y., & Zhitomirsky, I. (2014). A review of new methods of surface chemical modification, dispersion and electrophoretic deposition of metal oxide particles. Rsc Advances, 4(43), 22716-22732.
[20] Nore, V. N. (2013). Perancangan sistem informasi penjualan dan pemesanan produk berbasis web. Pr
[21] Krismiaji, 2005. Sistem Informasi Akutansi. UPP STIM YKPN Yogyakarta. Syafi'I, M. (2005). Aplikasi Database Dengan PHP 5 MySQL PostgreSQL Oracle. Yogyakarta: Andi.