International Journal of Engineering & Technology, 7 (2.14) (2018) 289-292

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

A Novelty Methods of Cryptography Algorithms Into Layered Cipher Encryption and Decryption

A Antoni[1*], Solly Aryza[2], Azmi Rizki Lubis[1], Bonar Harahap[1], Mahrani Arfah[1]

[1]Faculty of Engineering, Universitas Islam Sumatera Utara, Medan, Indonesia
[2]Faculty of Engineering, Universitas Pembangunan Panca Budi, Medan, Indonesia
**Corresponding author E-mail: antonigtg @ft.uisu.ac.id*

Abstract

Encryption is one method used to protect or maintain the data. Data that has encrypted will be kept confidential where the contents of the data are altered, so it does not correspond to the actual data. To be able to read data that has been encrypted earlier required a process called decryption. In the science of cryptography, the data will be safeguarded consists of three main components, that is the message that will be read (plaintext), the keys to perform cryptographic techniques (Key), and a random signal that is unreadable (ciphertext). Testing is done by sending the data in the form of words or sentences by using a secret key. Results of analysis of data from tests performed show that with the incorporation of some algorithm plated confidentiality of information can be safer because it takes several different stages to solve.

***Keywords:** algorithm, cryptography, decryption, encryption*

1. Introduction

By rapid growth of communication world, especially in the field of information such as data, images, audio or video, we need a system that can maintain the confidentiality of such information. Security is a standard requirement and becomes essential, the secrecy of data requires a security mechanism that can deal with the confidentiality of such information[1]–[5].

Encryption is the process of scrambling method or means of securing the information to make such information can not be read without any specialized knowledge[6]–[8]. Encryption can be used for security purposes, but other techniques are still needed to make communications secure[9]–[11], mainly to ensure the integrity and authentication of a message[12], [13]. For example, the information system [14]–[18] need the encryption for security the system. This study was conducted to analyze a method of encryption-decryption so that it becomes a multi-layered password that aims to improve the security of information.

2. Cryptography

Cryptography is a science which studies how to keep data or messages remain secure when transmitted from the transmitter to the receiver without interference from third parties[19]. According to Bruce Scheiner[20] in his book "Applied Cryptography," cryptography is the science and art of keeping distributing messages to stay safe or secure.

Besides these terms, there is also another meaning that cryptography is the study of mathematical techniques that relate to aspects of information security such as data confidentiality, data validity, data integrity, and authentication of data [21].The beginning of cryptography is understood as the science of hiding messages [22], but over the times until today, the notion of cryptography evolved into a science of mathematical techniques used to solve security issues such as privacy and authentication [23]. There is four fundamental purpose of the science of cryptography is that also the security aspect of information [24], namely:

a. Confidentiality is a service which is used to keep the contents of the data of anyone but who has the authority or the secret key to unlock the information that has been encoded.
b. Data integrity is associated with preservation of unauthorized data changes. To maintain data integrity system should have the ability to detect data manipulation by those who are not entitled to insertion, deletion, and other data entry into the actual data.
c. Authentication is associated with the identification or recognition, either as a whole of systems or the information itself. Two parties communicating must be introduced themselves. Information sent through the canal must be authenticated authenticity of the contents of the data, delivery time, and others.
d. Non-repudiation or non-denial is an attempt to prevent the denial of the delivery or the creation of information by the parties that send or make such information.

A. Main process in Cryptography

1) Encryption is the process by which information or data before it is transmitted, it is converted into a form that can hardly be recognizable as information initially using a specific algorithm.
2) A description is the opposite of encryption that reshapes disguised as the initial information.

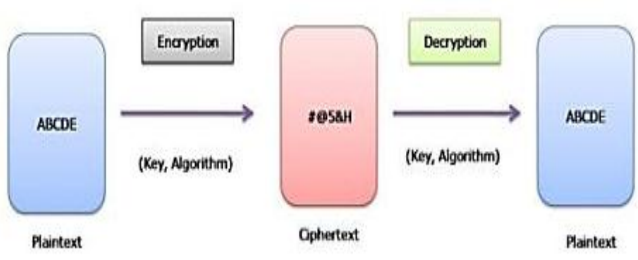


Fig.1: Basic Cryptography Illustration

B. The Term in Cryptography

Here are the terms used in cryptography:

1) Plaintext (M) is a message to be sent (containing the original data).
2) Ciphertext (C) is an encrypted message (encrypted) which is the result of the encryption.
3) Encryption (Function E) is the process of converting plaintext into ciphertext.
4) Decryption (Function D) is the process of conversion of ciphertext into plaintext, so that it becomes the initial data or original data.
5) Key is a secret number, which is used in the encryption and Decryption process.

3. Introduction Type of Cryptography

Cryptographic algorithms can be classified into two types based on its development, namely the classical cryptography and modern cryptography.

a. Classical Cryptographic Algorithm

This algorithm is used since before the era of computerization and mostly uses a symmetric key technique. The method to hide the message is to use the technique of substitution or transposition or both [25]. Substitution technique is to replace the characters in plaintext into other characters that the result is ciphertext[26]. While transposition is the technique of changing plaintext into ciphertext by means of permutations of character. It is a complex combination of both is underlying the formation of a wide range of modern cryptographic algorithms[27].

b. Modern Cryptographic Algorithms

This algorithm has a more complex difficulty level, and the strength is in key[28]. This algorithm uses a binary symbol because it follows the digital computer processing operations. Thus requiring a basic form of knowledge of mathematics to master it.

Cryptographic algorithms can be classified into two types based on the key, the symmetric algorithms and asymmetric algorithms.

a. Symmetric Algorithms

These algorithms are called symmetric because it has the same key in the encryption and decryption process so this algorithm also often called single-key algorithm or one-key algorithms. Key in this algorithm is confidential or private so that the algorithm is also called the secret key algorithm.

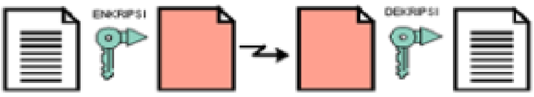


Fig.2: Symmetric Algorithms Illustration

b. Excess Symmetric Algorithms

Speed of operation is higher when compared to the asymmetric algorithm, because the speed is high enough, it can be used in real-time systems[29].

c. Symmetric Algorithms Weakness

For each delivery of messages with different user needs different keys as well, so there will be difficulties in the key management, commonly called key distribution problem.

d. Asymmetric Algorithms

This algorithm is called asymmetric because the key used for encryption is different from the key used for decryption. The key used for encryption is public key so that the algorithm is also called a public key algorithm. Whereas the key for decryption using a secret key or private key[30].

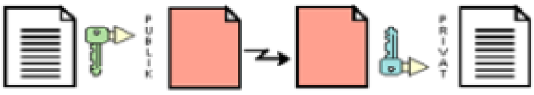


Fig.3: Asymmetric Algorithm Illustration

Asymmetric Algorithm advantages:

a. Security issues at key distribution can be better.

b. Key management problems better because fewer number of keys.

Weakness Asymmetric Algorithm:

a. The speed is lower when compared to a symmetric algorithm.

b. For the same level of security, the key used is longer than the symmetric algorithm.

At the beginning the data security with cryptography that uses the classic cryptographic algorithms are still character-based, using a pen and paper only, no computer. Classical cryptographic algorithm belongs to the symmetric key cryptography. Classic cryptographic algorithms :

a. Substitution Ciphers

b. Transposition Ciphers

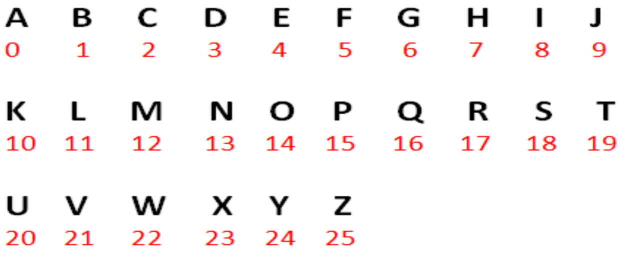
In this study the author will only discuss about Substitution Ciphers.

3.1 Substitution Ciphers

Substitution cipher change one letter or character in the message (plaintext), according to the rules of the key (key), it becomes another character in the secret password (ciphertext)[31]. Here is part of the Substitution Chipers:

1. Caesar Cipher

The simplest example of a substitution cipher is a Caesar cipher.Caesar Cipher is a substitution cipher that uses a key length of 1 characters (characters drawn from the alphabet). Usually, the parties have agreed and both know that they will use Caesar Cipher with certain characters to exchange secret messages.The sender of the message: has the original message, know the key, know how to use Caesar Cipher. He use Caesar Cipher to generate the secret password.Recipients of the message: know the key, know how to use Caesar Cipher, know the secret password. He uses the password to decode the secret in order to obtain the original message.



A	B	C	D	E	F	G	H	I	J
0	1	2	3	4	5	6	7	8	9
K	L	M	N	O	P	Q	R	S	T
10	11	12	13	14	15	16	17	18	19
U	V	W	X	Y	Z				
20	21	22	23	24	25				

Fig.4: Alphabetical Order Index

Alphabet used to build the message (plaintext) was given an index number as shown above. The characters are used as keys were also taken from the alphabet. The key will be "added" or create a "shift" character of the original message to establish a password. If when added or shifted generate an index of more than 25, the order of the index will return to 0, From Z back to A.

2. Atbash Cipher

Another classic example is the Atbash Cipher. This Atbash Cipher permute letters from front to back so back to front as shown below:

Message : ABCDEFGHIJKLMNOPQRSTUVWXYZ
Chiper: ZYXWVUTSRQPONMLKJIHGFEDCBA

By using a password Atbash, ZENIUS message will be AVMRFH password. The recipient only needs to swap the order of the letter behind it. Atbash name is derived from its first use in Hebrew letters, the Aleph-Tav-Shin-Beth, the first, last, second and penultimate in Hebrew. If the name in roman letters or less will be Azby.

3. Polyalpabetic Cipher

Vigenere Cipher is included in polyalpabetic substitusion cipher. The new algorithm is widely known that 200 years later by the inventor cipher is then called Vigenere Cipher.Vigenere Vigenere Cipher used to encrypt the Square, each row in the square states ciphertext letters obtained by Caesar Cipher[32].
Examples of application of Vigenere Cipher

Plaintext	: THIS PLAINTEXT
Key	: sonysonysonys
Ciphertext	: LVVQ HZNGFHRVL

If the key length is shorter than the length of the plaintext, then the key is repeated periodically. In this case the key "sony" repeated as long as its plaintext.
Basically each letter is Caesar cipher encryption with different keys.
c(‘T’) = (‘T’ + ‘s’) mod 26 = L
T = 20 and s= 19 ◊ (20+19)%26=13 ◊ L
c(‘H’) = (‘H’ + ‘o’) mod 26 = V, ect

4. Result Analysis

In this case I try to incorporate some of the passwords in order to establish a password also called a streak password, for example, after do the Atbash Cipher than encrypted it again by the Polyalphabetic Cipher.

a. Encryption Process

Data submitted following the results of tests performed:

HAFIZHATUL AHLA

This message consists of 14 characters.

Step 1: Using Atbash Cipher, it will be obtained

Plain Text	: HAFIZHATUL AHLA
Cipher Text	: SZURASZGFO ZSOZ

Step 2 : Using Caesar Cipher, where the cipher text in step 1 will be plain text in step 2. Chiper text in step 2 is obtained by using key E.

Table 1. Key Of E and Chiper Text

plain text	S	Z	U	R	A	S	Z	G	F	O		Z	S	O	Z
	18	25	20	17	0	18	25	6	5	14		25	18	14	25
key, E = 5	5	5	5	5	5	5	5	5	5	5		5	5	5	5
	23	30	25	22	5	23	30	11	10	19		30	23	19	30
chiper text	X	E	Z	W	F	X	E	L	K	T		E	X	T	E

The purpose of the key, E = 5 is the numerical value of each letter in the plain text character summed with 5. If when added or shifted generate an index of more than 25, the order index should return to 0.

Step 3: is the last step of the process is to use Polyalphabetic Cipher, where the cipher text in step 2 will be plain text, cipher text obtained by using key SUN.

Table 2. Chiper Text Using Key Sun

plain text	X	E	Z	W	F	X	E	L	K	T		E	X	T	E
	23	4	25	22	5	23	4	11	10	19		4	23	19	4
key, SUN	S	U	N	S	U	N	S	U	N	S		U	N	S	U
	18	20	13	18	20	13	18	20	13	18		20	13	18	20
	23	4	25	22	5	23	4	11	10	19		4	23	19	4
	18	20	13	18	20	13	18	20	13	18		20	13	18	20
	41	24	38	40	25	36	22	31	23	37		24	36	37	24
min 26	15	24	4	14	25	10	22	5	23	11		24	10	11	24
chipper text	P	Y	E	O	Z	K	W	F	X	L		Y	K	L	Y

The way to obtain the cipher text in the last step is the same as Caesar Cipher, by summing the index number. Key used (SUN) consists of three characters, while the message (XezwfxeLkt exte) consists of 14 characters, we can redo the key so that the key character length = length of character messages. This applies to all cases, in which the length of the key characters are not the same as the character length messages.

b. Decryption Process

Decryption is done by reversing the encryption process with the following stages:

Step 1: cipher text is decrypted by subtracted with key (SUN), so that the results will show the plaint text.

Table 3. Polyalphabetic Cipher Decryption Results

Ci-phertext	P	Y	E	O	Z	K	W	F	X	L		Y	K	L	Y
	15	24	4	14	25	10	22	5	23	11		24	10	11	24
plus 26	15	24	4	14	25	10	22	5	23	11		24	10	11	24
key, SUN	18	20	13	18	20	13	18	20	13	18		20	13	18	20
	23	4	25	22	5	23	4	11	10	19		4	23	19	4
plain text	X	E	Z	W	F	X	E	L	K	T		E	X	T	E

Step 2: Use the plain text in step 1 as cipher text Caesar Cipher and than decrypt it with key E = 5. Resulting Decryption as follows:

Table 4. Caesar Cipher Decryption Results

chiper text	X	E	Z	W	F	X	E	L	K	T		E	X	T	E
key, E = 5	23	4	25	22	5	23	4	11	10	19		4	23	19	4
	5	5	5	5	5	5	5	5	5	5		5	5	5	5
back to 25	18	25	20	17	0	18	25	6	5	14		-1	18	14	-1
plain text	S	Z	U	R	A	S	Z	G	F	O		Z	S	O	Z

Step 3 is the final stage of the decryption process, by using plain text in Caesar Cipher as a cipher text and using Atbash Cipher will be obtained:

Chiper Text : SZURASZGFO ZSOZ
Plain Text : HAFIZHATUL AHLA

5. Conclusion

The conclusions that can be drawn from this study are:

a. Whereas by merging multiple layered confidentiality algorithm information may be safer because it takes several different stages to solve.
b. Classical cryptography algorithm focuses on the power of secrecy. With intent algorithms used (which means if the algorithms used are known then the message is clear "leaky" and can know its contents by anyone who knows the algorithm).
c. Cryptography is a science which studies how to keep data or messages remain secure when transmitted from the sender to the receiver without interference from third parties.
d. Encryption is the process by which information or data to be transmitted, is converted into a form that can hardly be recognizable as information initially using a specific algorithm.
e. Decryption is the process of restoring the original data so that it can be read or understood back.

References

[1] S. Aryza, M. Irwanto, Z. Lubis, A. P. U. Siahaan, R. Rahim, and M. Furqan, "A Novelty Design Of Minimization Of Electrical Losses In A Vector Controlled Induction Machine Drive," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 300, p. 012067, 2018.

[2] R. Rahim, "Man-in-the-middle-attack prevention using interlock protocol method," *ARPN J. Eng. Appl. Sci.*, vol. 12, no. 22, pp. 6483–6487, 2017.

[3] R. Rahim *et al.*, "Combination Base64 Algorithm and EOF Technique for Steganography," *J. Phys. Conf. Ser.*, vol. 1007, p. 012003, Apr. 2018.

[4] R. Rahim *et al.*, "Combination Vigenere Cipher and One Time Pad for Data Security," *Int. J. Eng. Technol.*, vol. 7, no. 2.3, pp. 92–94, 2018.

[5] E. Kartikadarma, T. Listyorini, and R. Rahim, "An Android mobile RC4 simulation for education," *World Trans. Eng. Technol. Educ.*, vol. 16, no. 1, pp. 75–79, 2018.

[6] R. Rahim, D. Adyaraka, S. Sallu, E. Sarimanah, and M. M. Rahman, "Tiny encryption algorithm and pixel value differencing for enhancement security message," *Int. J. Eng. Technol.*, vol. 7, no. 2.9, pp. 82–85, 2018.

[7] R. Rahim, D. Adyaraka, S. Sallu, E. Sarimanah, and A. Hidayat, "An application data security with lempel - ziv welch and blowfish," *Int. J. Eng. Technol.*, vol. 7, no. 2.9, pp. 71–73, 2018.

[8] R. Rahim, H. Nurdiyanto, A. S. Ahmar, D. Abdullah, D. Hartama, and D. Napitupulu, "Keylogger Application to Monitoring Users Activity with Exact String Matching Algorithm," *J. Phys. Conf. Ser.*, vol. 954, no. 1, 2018.

[9] H. Nurdiyanto and R. Rahim, "Enhanced pixel value differencing steganography with government standard algorithm," in *2017 3rd International Conference on Science in Information Technology (ICSITech)*, 2017, pp. 366–371.

[10] R. Rahim, H. Winata, I. Zulkarnain, and H. Jaya, "Prime Number: an Experiment Rabin-Miller and Fast Exponentiation," *J. Phys. Conf. Ser.*, vol. 930, no. 1, p. 012032, Dec. 2017.

[11] H. Nurdiyanto, R. Rahim, and N. Wulan, "Symmetric Stream Cipher using Triple Transposition Key Method and Base64 Algorithm for Security Improvement," *J. Phys. Conf. Ser.*, vol. 930, no. 1, p. 012005, Dec. 2017.

[12] R. Rahim, M. Dahria, M. Syahril, and B. Anwar, "Combination of the Blowfish and Lempel-Ziv-Welch algorithms for text compression," *World Trans. Eng. Technol. Educ.*, vol. 15, no. 3, pp. 292–297, 2017.

[13] A. Putera, U. Siahaan, and R. Rahim, "Dynamic Key Matrix of Hill Cipher Using Genetic Algorithm," *Int. J. Secur. Its Appl.*, vol. 10, no. 8, pp. 173–180, Aug. 2016.

[14] A. S. Ahmar, Rusli, and A. Rahman, "Steps in Designing Queue and Interview Process using Information System: A Case of Re-registration of New Students in Universitas Negeri Makassar," *Asian J. Technol. Manag.*, vol. 9, no. 1, pp. 52–57, 2016.

[15] A. S. Ahmar, R. Hidayat, D. Napitupulu, R. Rahim, Y. Sonatha, and M. Azmi, "eConf: an Information System to Manage the Conference," *J. Phys. Conf. Ser.*, vol. 1028, no. 1, p. 012044, 2018.

[16] D. Lazim *et al.*, "Information Management and PSM Evaluation System," *Int. J. Eng. Technol.*, vol. 7, no. 1.6, pp. 17–19, 2018.

[17] A. Iskandar, E. Virma, and A. S. Ahmar, "Implementing DMZ in Improving Network Security of Web Testing in STMIK AKBA," *Int. J. Eng. Technol.*, vol. 7, no. 2.3, pp. 99–104, 2018.

[18] F. A. A. Fauzy *et al.*, "Registration system and UTM games decision using the website application," *Int. J. Eng. Technol.*, vol. 7, 2018.

[19] D. Abdullah, R. Rahim, D. Apdilah, S. Efendi, T. Tulus, and S. Suwilo, "Prime Numbers Comparison using Sieve of Eratosthenes and Sieve of Sundaram Algorithm," in *Journal of Physics: Conference Series*, 2018, vol. 978, no. 1, p. 012123.

[20] S. Bruce, *Applied cryptography*. 1996.

[21] "Implementation of Modified Median Filtering Algorithm for Salt & Pepper Noise Reduction on Image," *Int. J. Sci. Technoledge*, pp. 2321–919, 2016.

[22] H. Aspan and S. Aryza, "Dear Sir/Madam, Elpina, Henry Aspan, Solly Aryza This is to inform you that after a rigorous review process, our review panel has reached a decision about your paper! "," no. January, p. 76318, 2018.

[23] Indar Sugiarto, Thiang Thiang, and Timothy Joy Siswanto, "Disain dan Implementasi Modul Akuisisi Data sebagai Alternatif Modul DAQ LabVIEW," *J. Tek. Elektro*, vol. 8, no. 1, pp. 30–37, 2008.

[24] W. Diffie, W. Diffie, and M. E. Hellman, "New Directions in Cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[25] R. Sadikin, "Kriptografi Untuk Keamanan Jaringan dan Implementasinya dalam Bahasa Java," p. 2012, 2012.

[26] I. Halik and Y. Prayudi, "Studi dan Analisis Algoritma Rivest Code 6 (RC6) dalam Enkripsi/Dekripsi Data," *Stud. Dan Anal. Algoritm. Rivest Code 6 Dalam Enkripsi/Dekripsi Data*, vol. 6, no. D, pp. 149–158, 2005.

[27] S. Hesari and M. B. N. Sistani, "Efficiency improvement of induction motor using fuzzy-genetic algorithm," *30th Power Syst. Conf. PSC 2015*, no. November, pp. 210–216, 2017.

[28] D. Wirdasari, "Prinsip Kerja Kriptografi dalam Mengamankan Informasi," *Saintikom*, vol. 5, no. 2, pp. 174–184, 2008.

[29] M. Ebrahim, S. Khan, and U. Bin Khalid, "Symmetric Algorithm Survey: A Comparative Analysis," vol. 61, no. 20, pp. 12–19, 2014.

[30] T. Bala, "Asymmetric Algorithms and Symmetric Algorithms : A Review," no. Icaet, pp. 1–4, 2015.

[31] D. Putra *et al.*, "IMPLEMENTASI ALGORITMA RC4 DAN PLAYFAIR CIPHER Permutasi Untuk S-Box," *Pelita Inform.*, vol. 16, pp. 328–334, 2017.

[32] R. Morelli and R. Walde, "Evolving Keys for Periodic Polyalphabetic Ciphers," no. Rubin 1995, pp. 445–450, 1997.