Combination Of Rot13 Cryptographic Algorithm And Ecb (Electronic Code Book) In Data Security

Reni Rahmadani[1*], Bagoes Maulana[2], Muhammad Dominique Mendoza[3], Andreas Pratama Partogu Hutabarat[4], Larson Carstein Raja Aritonang[5]

{renirahmadani@unimed.ac.id[1]}

PTIK-FT, Universitas Negeri Medan, Medan, Indonesia

Abstract. Computer security is an important thing in the world of information technology. However, it rarely gets the attention of developers, even computer security is assumed to be a secondary/tertiary requirement for information systems. Nowadays, data encryting algorithms are increasing and; Of course this is related to the term cryptography. Several methods are usually used in this cryptographic system, namely the classical system and the public key system. Among the various algorithms; Existing cryptography, ROT13 algorithm and electronic code book (ECB) are used to solve data security cases. ROT13 is a shift cipher, which is a type of encryption; a simple one in which a ciphertext is created by taking a plain text message and (moving forward in the alphabet) a number of letters. The ECB algorithm is used to randomly encrypt files, and if the ECB algorithm is run with parallel processors, each processor can encrypt or decrypt different plaintext blocks.

Keywords: Cryptographic Algorithm, ROT13 Cryptographic Algorithm, ECB (Electronic Code Book).

1 Introduction

Security issues are one of the important aspects of information systems. However, it often gets less attention from the owners and managers of information systems, even information system problems are considered the second or even last in a series of important matters relating to information systems. Several methods have been developed to overcome this security problem, and one of the methods used to overcome this problem is to use cryptography algorithms[1].

In cryptography the data (plaintext) is converted into a password (ciphertext) using a certain key[2]. For this reason, the confidentiality of this key is important for the success of this encryption. Several methods can be used in this cryptographic system, namely traditional/classical systems and public/modern key systems. In traditional cryptography systems, plaintext uses the same key to be the ciphertext, while public key cryptography systems use two different keys[3][4]. Among the various cryptographic algorithms available, the ROT13 algorithm and the electronic code book (ECB) are used to complete the information system security course.

ROT13 is a shift cipher, which is a simple type of encryption in which the ciphertext is created by taking a plain text message and (moving forward in the alphabet) a number of letters[5]. Its name stands for "13 rounds". This is also a type of password replacement, as one letter is replaced by another[6]. The uniqueness of ROT13 lies in its opposite. Since the alphabet is 26 letters and shift is 13 letters, A stands for N and vice versa. However, it doesn't encode numbers or punctuation, which gives it some limitations.

ACEIVE 2022, October 20, Medan, Indonesia

DOI 10.4108/eai.20-10-2022.2328872

ROT13 can be easily translated without any tools. If there is a code ROT13, just write the letters A-M on a piece of paper, and write the letters N to Z below. It can then replace the letters accordingly, so if the ciphertext has the letter A, 20 plain text is N, and vice versa.

ROT13 is very precisely implemented with the ECB (Electronic Code Book) algorithm, with the condition that each record consists of the same number of discrete blocks. The ECB algorithm is used to randomly encrypt files, and if the ECB algorithm is run with parallel processors, each processor can encrypt or decrypt different plaintext blocks[7].

The ECB algorithm used is a cryptographic algorithm that has been modified so that even though the same plaintext is encrypted, the resulting ciphertext blocks are different. This is to avoid plaintext redundancy as one of the weaknesses of the ECB cryptographic algorithm.

2 Research Method

The ROT13 cryptographic algorithm (Rotate 13) is an advanced form of the Caesar Cipher method where the modified thing is the amount and direction of displacement[8]. ROT13 is commonly used on UNIX operating systems. The ROT13 encryption system replaces a letter with a letter that is 13 positions above it[9]. While the ROT13 decryption system, where a character moves back 13 times. For example, the letter "A" is replaced by the letter "N", the letter "B" is replaced by the letter "O", etc. Here is the ROT13 encryption formula.

E = ROT13 (P)

While the ROT13 decryption formula is as follows.

D = ROT13 (P)

Electronic Code Book (ECB) is a cryptographic method that is a block cipher, where each character (plaintext) will be partitioned / split into blocks and then encrypted to produce ciphertext[10]. XOR is an Exclusive OR logic gate, that is, it only evaluates to TRUE (1) when one of the premises is TRUE (1).

The stages in the encryption process using the ECB algorithm:

1) Convert plaintext to binary numbers.
2) Separate the binary numbers per block where each block consists of 4 bits.
3) Specify a keyword to modify a message containing 4 bits; binary number.
4) Perform XOR Operation between plaintext and keywords.
5) Swipe left one step, then combine the results of each block.
6) Then partition it into blocks of 8 bits each.
7) Each binary block is converted to a character, the result is ciphertext (ASCII).

3 Results and Discussion

The following is an example of an encryption implementation with a combination of ROT and ECB (Electronic Code Book) cryptographic algorithms.

1) ROT 13 Cryptographic Algorithm
   Plaintext : ANDREAS
   Encryption : ROT13 (P)

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

ROT13 (ANDREAS) = **NAQERNF**

2) ECB Cryptographic Algorithm
Key = A, in hexadecimal: 41, in binary: 01000001, in decimal: 65

Table 1. Plaintext conversion to biner

Plaintext (ASCII)	**NAQERNF**													
	N		A		Q		E		R		N		F	
ASCII Conversion to Biner	01001110		01000001		01010001		01000101		01010010		01001110		01000110	
Split biner number to two block, 4 bit per block	0100	1110	0100	0001	0101	0001	0100	0101	0101	0010	0100	1110	0100	0110

XOR operation of each block pair is shown in Table 2:

Table 2. XOR operation

Plaintext XOR Key	0100	1110	0100	0001	0101	0001	0100	0101	0101	0010	0100	1110	0100	0110
	0100	0001	0100	0001	0100	0001	0100	0001	0100	0001	0100	0001	0100	0001
	0000	1111	0000	0000	0001	0000	0000	0100	0001	0011	0000	1111	0000	0111
Swipe left one step	0001	1110	0000	0000	0010	0000	0000	1000	0010	0110	0001	1110	0000	1110
Merging Result	00011110		00000000		00100000		00001000		00100110		00011110		00001110	
ASCII	RS		NULL		Space		BS		&		RS		SO	
Encryption	**RS**		**NULL**		**Space**		**BS**		**&**		**RS**		**SO**	

The following is an example of a decryption implementation with a combination of the ECB (Electronic Code Book) and ROT cryptographic algorithms.

1) ECB Cryptographic Algorithm
   a. Convert ciphertext (ASCII) to binary numbers.
   b. Partition the binary number per block, each block consisting of 4 bits.
   c. Swipe right 1 step.
   d. Perform XOR Operation between ciphertext and keywords.
   e. Then partition each block with each block containing 8 bits.
   f. Convert each binary block to; The result character is plaintext.

Table 3. Ciphertext conversion to biner and ASCII

Encryption	**RS**		**NULL**		**Space**		**BS**		**&**		**RS**		**SO**	
ASCII	RS		NULL		Space		BS		&		RS		SO	
Biner Conversion	00011110		00000000		00100000		00001000		00100110		00011110		00001110	
Partition (4 bit)	0001	1110	0000	0000	0010	0000	0000	1000	0010	0110	0001	1110	0000	1110
Swipe right one step	0000	1111	0000	0000	0001	0000	0000	0100	0001	0011	0000	1111	0000	0111
Ciphertext XOR Key	0100	0001	0100	0001	0100	0001	0100	0001	0100	0001	0100	0001	0100	0001
Result	0100	1110	0100	0001	0101	0001	0100	0101	0101	0010	0100	1110	0100	0110
Merging	01001110		01000001		01010001		01000101		01010010		01001110		01000110	
ASCII Conversion from biner	N		A		Q		E		R		N		F	

2) ROT 13 Cryptographic Algorithm
   Plaintext : NAQERNF
   Description : ROT13 (P)

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

ROT13 (NAQERNF) = ANDREAS

The advantages of the ROT13 cryptographic algorithm: the same code can be made to perform encryption or decryption[11]. Weaknesses of the ROT13 cryptographic algorithm: ROT13 is not designed with high security so it is only used for small things such as article content[12].

The advantages of the ECB cryptographic algorithm: (1) Manual encryption can be done easily[13]. This is because each plaintext block is encrypted independently so there is no need to encrypt files linearly. (2) ECB is used to encrypt data in the database (provided that each record consists of the same number of blocks)[14]. While the weaknesses of the ECB cryptographic algorithm: (1) the existence of redundancy of the plaintext portion results in encryption with the same block[15]. (2) In e-mail, messages contain redundancy of letters/words so that when encrypted they get output in the form of ciphertext patterns that can be easily found[16].

4 Conclusions

The ROT13 cryptographic algorithm (Rotate 13) is an advanced form of the Caesar Cipher method where the modified thing is the amount and direction of displacement. ROT13 is commonly used on UNIX operating systems. The ROT13 encryption system replaces a letter with a letter that is 13 positions above it. While the ROT13 decryption system, a character moves back 13 times. The advantage of ROT13 is that the same code can be made to perform encryption and decryption. The advantages of the ECB cryptographic algorithm: (1) Manual encryption can be done easily, because each plaintext block is encrypted independently so there is no need to encrypt files linearly. (2) ECB is used to encrypt data in the database with the condition that each record consists of the same number of blocks.

References

[1] Venkatachalam, K., Prabu, P., Almutairi, A., & Abouhawwash, M. (2021). Secure biometric authentication with de-duplication on distributed cloud storage. *PeerJ Computer Science*, 7, e569.

[2] Xu, H., Thakur, K., Kamruzzaman, A. S., & Ali, M. L. (2021). Applications of Cryptography in Database: A Review. In 2021 IEEE International IOT, *Electronics and Mechatronics Conference (IEMTRONICS)* (pp. 1-6). IEEE.

[3] Raghunandhan, K. R., Shetty, S., Aithal, G., & Rakshith, N. (2018). Enhanced RSA algorithm using fake modulus and fake public key exponent. *In 2018 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT)* (pp. 755-759). IEEE.

[4] Rahmadani, R., & Hutahaean, H. D. (2020). Implementation Of Pohlig-Hellman Algorithm And Steganography Combination Of First Of File (Fof) And End Of File (EOF) For File Security: Implementation Of Pohlig-Hellman Algorithm And Steganography Combination Of First Of File (Fof) And End Of File (EOF) For File Security. *Jurnal Mantik*, 4(1), 14-19.

[5] Duffany, J. L. (2019). Developing cybersecurity skills in intermediate programming courses. In *Proceedings of the LACCEI International Multi-Conference for Engineering, Education and Technology* (pp. 24-26).

[6] Hondro, R. K., & Fau, A. (2018). Perancangan Aplikasi Penyandiandengan Algoritma ROT13 dan Triangel Chain Chipher (TCC). *Jurnal Mahajana Informasi*, 3(2).

[7] Tarigan, P. T. (2020). Use of Electronic Code Book (Ecb) Algorithm in File Security. *Jurnal Info Sains: Informatika dan Sains*, 10(1), 19-23.

[8] Holden, J. (2018). *The mathematics of secrets: cryptography from caesar ciphers to digital encryption.* Princeton University Press.
[9] Risman, R. (2021). Comparison of Performance Rot13 and Caesar Cipher Method for Registration Database of Vessels Berthed at PT Samudera Indonesia. *International Journal of Basic and Applied Science,* 10(3), 91-98.
[10] Tarigan, N. M. B., & Panjaitan, M. I. (2018). Implementation of Security with Login Data using the Electronic Code Book Algorithm. Login: *Jurnal Teknologi Komputer*, 12(2), 36-39.
[11] Filipova-Petrakieva, S., & Shopov, S. (2021, September). Educational Windows Presentation Foundation and XAML Application for Information Protection based on the Cryptographic Methods–part II. In *2021 13th Electrical Engineering Faculty Conference (BulEF)* (pp. 1-8). IEEE.
[12] Fischer, T. (2019, November). I Wrote my Own Ransomware; did not make 1 iota of a Bitcoin. *In In Depth Security Vol. III: Proceedings of the DeepSec Conferences* Vol. 3, p. 139). BoD–Books on Demand.
[13] Shahbazi, K., & Ko, S. B. (2020). High throughput and area-efficient FPGA implementation of AES for high-traffic applications. *IET Computers & Digital Techniques*, 14(6), 344-352.
[14] Panagiotou, P., Sklavos, N., Darra, E., & Zaharakis, I. D. (2020). Cryptographic system for data applications, in the context of internet of things. *Microprocessors and Microsystems,* 72, 102921.
[15] Naouel, S., Zakarya, B. A. M., & Badr, B. (2021). Optimization of the symmetric encryption mode ECB dedicated to securing medical data. *Journal of Electrical and Electronics Engineering*, 14(1), 48-52.
[16] Bhattacharya, S. (2019). Cryptology and information security-past, present, and future role in society. *International Journal on Cryptography and Information Security* (IJCIS), 9(1/2).