http://ejournal.seaninstitute.or.id/index.php/InfoSains
Jurnal Info Sains : Informatikan dan Sains, Volume 11, No 02 September 2021
E-ISSN.2797-7889, P-ISSN.2089-3329

Text Encoding Using Cipher Block Chaining Algorithm

[1]Sartana Sinurat, [2]Maranatha Pasaribu
[1,2] Informatics Engineering Study Program, Akademi Manajemen Informatika dan Komputer Medan Business Polytechnic (MBP)
Email : sartanasinurat20@gmail.com[1], maranata@gmail.com[2]

Keywords

Cryptography
Text Encoding
Cipher Block Chaining Algorithm

Abstract. Data confidentiality and security are critical in data communication, both for the purpose of shared security, and for individual privacy. Computer users who want their data unknown to unauthorized parties are always trying to work out how to secure the information that will be communicated or that will be stored. Protection against data confidentiality is increasing, one way is by applying cryptographic science. Cipher Block Chaining (CBC), this mode is a feedback mechanism on a block, and in this case the result of the previous block encryption is feedback into the current block encryption. The trick is to block the current plaintext in XOR first with the ciphertext block of the previous encryption result, then the result of this XOR-ing goes into the encryption function. With CBC mode, each ciphertext block is calculated not only on its plaintext block but also on the entire previous plaintext block. The author tries to co-create a text encoding to secure the data with the Cipher Block Chaining (CBC) cryptographic method.

1. INTRODUCTION

Text encoding is a science based on informatics techniques that aims to secure information such as data confidentiality and authentic entities. Data confidentiality and security are of paramount importance in data communication, both for the purpose of shared security and for individual privacy [1]. Computer users who want their data unknown to unauthorised parties always try to get around how to secure the information to be communicated or that will be submitted. Protection against secrecy is increasing, one way to encrypt encryption. Encryption is the process of converting the original message into an unreadable character. There are several encryption algorithms that can be used such as Stream Chiper, Data Encryption Standard (DES), Triple DES, Advanced Encryption Standard (AES) and so on [1]–[3].

Data confidentiality and security are critical in data communication, both for the purpose of shared security, and for individual privacy [4]. Computer users who want their data unknown to unauthorized parties are always trying to work out how to secure the information that will be communicated or that will be stored. So that protection against data confidentiality increases, one way is text encoding in encryption. Encryption is a process of converting the original message into unreadable characters. There are several commonly used encryption algorithms such as Block Cipher, Stream Cipher, Data Encryption Standard (DES), Triple DES, Advanced Encryption Standard (AES), and so on [5]. Where each algorithm has its own characteristics. While the process of converting the encryption results into the original message is called decryption. To keep very important data confidential, a cryptographic method is used that encrypts and describes the data. One of the methods that will be used in the creation of this text encoding is the Cipher Block Chaining (CBC) method, as this method is implemented at the binary digit level(bits),so the encryption process pattern cannot be read, and the encryption and decryption process takes a short time[6].

2. METHODS

In the preparation of research, very accurate and objective data is needed in order to be discussed and evaluated and concluded to better understand and understand the contents of the preparation of the report. In this accurate data collection, the authors use several methods to obtain the data.

2.1 Text encoding

Text encoding is a science that relies on mathematical techniques for dealing with information security such as confidentiality, data wholeness and authentic entities. Therefore, a process of encoding or encoding data is needed. So that the data can be maintained confidential and cannot be easily changed to maintain the integrity of the data. To ensure the security and integrity of a data, a encoding process is needed [7].

2.2 Cipher Block Chaining Algorithm

In cryptography is often found terms or terminology, such as messages (messages) is data or information that can be read and understood its meaning. Another name for the message is plaintext(plaintext) or clear text(cleartext). Messages can be data or information sent (via courier, telecommunication channels, etc.) or stored in recording media (paper, storage,etc.). Stored messages are not only text, but can be image,sound (audio),and video, or other binary files. In order for the message to be incomprehensible to the other party, the message needs to be encoded into another form that cannot be understood. The encrypted form is called a ciphertext or cryptogram that must be transformed back into plaintext in order for received messages to be read [8].

Cipher blocks are symmetric cryptographic algorithms that encrypt a single plaintext block with a certain number of bits and generate ciphertext blocks of the same number of bits. Dependence between block and build software using Cipher block chaining (CBC) Operation mode on data security by converting encrypted data into ciphertext. The basic operation of Cipher block chaining is the application of a feedback mechanism on a bit block where the result of the previous block encryption is fed back into the current block encryption process. This operation is applied to algorithms that are already operating at the bit level (0) or (1) or a group / block of bits and not characters. Keys are used to perform encryption and decryption. The key works the same as the password. Encryption and description consists of 64 bits with 128 bit keys [9].

2.3. Enkripsi and Cipher Block Chaining Description

Encryption is the process of converting messages or data into passwords which is one of the processes of cryptography. Encoded data is an input file and by using a key, it is converted into an unreadable encryption file. The purpose of this encryption is to hide data or information from unauthorized persons [10], [11].

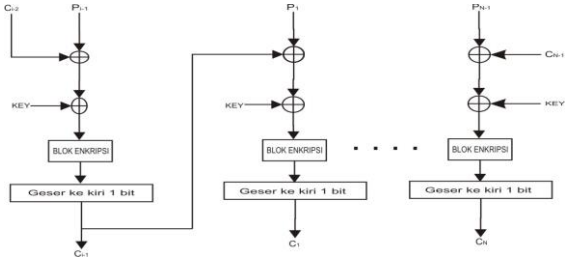

Figure 1 : Encryption Scheme with CBC Algorithm

Text encoding is a science that relies on mathematical techniques to deal with information security such as confidentiality, data integrity and authentic entities.

3. RESULTS AND DISCUSSION

In the encryption process, block cipher uses several mathematical functions, including permutation function and substitution function, so that confussion and diffusion in cipher block are fulfilled. The term confucius and diffusion was introduced by Claude Shannon in 1949. According to him, confucius and diffusion are things that should be considered in cryptographic systems, because it can prevent cyptanalysis, especially those based on statistical analysis

3.1 Encryption Process

The arrangement of Cipher block chaining algorithm in the encryption process is as follows:

Plaintext : WITH YOU

Cipherteks: EXGLGDUPD

P_1:01000010,01010101,01000100,01001001, 01000100,01000001,01001101,01000001

key : C

K= 01000011

Intialization Vektor : Z

W (C_0) =010111010

01000010, 01010101, 01000100, 01001001, 01000100, 01000001, 01010010, 01001101, 01000001

P8 P9

$C_1 = P_1 \oplus C_0$
= 01000010 ⊕ 01011010
= 01000010
= 00011000 ⊕ K
= 00011000 ⊕ 01000011
= 01011011 ⇨ 10110110

$C_2 = P_2 \oplus C_1$
= 01010101 ⊕ 10110110
= 01010101
= 11100011 ⊕ K
= 11100011 ⊕ 01000011
= 10100000 ⇨ 01000001

$C_3 = P_3 \oplus C_2$
= 01000100 ⊕ 0100001
= 01000100
= 00000101 ⊕ K
= 11100011 ⊕ 01000011
= 10100000 ⇨ 01000001

$C_4 = P_4 \oplus C_3$
= 01001001 ⊕ 10001100
= 11000101
= 11000101 ⊕ K
= 11000101 ⊕ 01000011
= 10000110 ⇨ 00001101

$C_5 = P_5 \oplus C_4$
= 01000100 ⊕ 00001101
= 01001001
= 01001001 ⊕ K
= 01001001 ⊕ 01000011
= 00001010 ⇨ 00010100

$C_6 = P_6 \oplus C_5$
= 01000001 ⊕ 00010100
= 01010101
= 01010101 ⊕ K
= 01010101 ⊕ 01000011
= 00010110 ⇨ 00101100

$C_7 = P_7 \oplus C_6$
= 01010010 ⊕ 00101100
= 01111110
= 01111110 ⊕ K
= 01111110 ⊕ 01000011
= 00111101 ⇨ 11101000

$C_8 = P_8 \oplus C_7$
= 01001101 ⊕ 01111010
= 01001101
= 01001101 ⊕ K
= 00110111 ⊕ 01000011
= 01110100 ⇨ 11101000

$C_9 = P_9 \oplus C_8$
= 01000001 ⊕ 11101000
= 01000001
= 01000001 ⊕ K
= 10101001 ⊕ 01000011
= 11101010 ⇨ 11010101

3.2 Process Description

While the arrangement of Cipher block chaining algorithm in the description process is as follows:

C_1 = 10110110, 01000001, 10001100, 00001101, 00010100, 00101100,

C1 C2 C3 C4 C5 C6

01111010, 11101000, 11010101

C7 C8 C9

$P_1 = C_1 \oplus C_0$
= 10110110
= 10110110 ⊕ 01011010
= 00000001
= 00000001 ⊕ K
= 00000001 ⊕ 01000011
= 01000010

$P_2 = C_2 \oplus C_1$
= 01000001
= 10100000 ⊕ 10110110
= 00010110
= 00010110 ⊕ 01000011
= 01010101

$P_3 = C_3 \oplus C_2$
= 10001100
= 01000110 ⊕ 01000001
= 00000111
= 00000111 ⊕ 01000011
= 01000100

$P_4 = C_4 \oplus C_3$
= 00001101
= 10000110 ⊕ 10001100

= 00001010
= 00001010 ⊕ 01000011
= 01001001

$P_5 = C_5 \oplus C_4$
= 00010100
= 00001010 ⊕ 01000011
= 00000111
= 00000111 ⊕ 01000011
= 01000100

$P_6 = C_6 \oplus C_5$
= 00101100
= 00010110 ⊕ 00010100
= 00000010
= 00000010 ⊕ 01000011
= 01000001

$P_7 = C_7 \oplus C_6$
= 01111010
= 00111101 ⊕ 00101100
= 00010001
= 00010001 ⊕ 01000011
= 01010010

$P_8 = C_8 \oplus C_7$
= 11101000
= 01110100 ⊕ 01111010
= 00001110
= 00001110 ⊕ 01000011
= 01001101

$P_9 = C_9 \oplus C_8$
= 11010101
= 11101010 ⊕ 11101000
= 00000010
= 00000111 ⊕ 01000011
= 01000001

4. CONCLUSION

Cryptography with CBC method can be used to maintain the authenticity of data (authentication) and data integrity (dataintegrity) and disguise the original message. This scheme also supports the verification process of Cryptography with the CBC method.

REFERENCE

[1] W. Zhai, "Design and application of a remote electronic communication teaching system in a network environment," *Int. J. Emerg. Technol. Learn.*, vol. 13, no. 4, 2018, doi: 10.3991/ijet.v13i04.8480.

[2] A. Prameshwari and N. P. Sastra, "Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen," *Eksplora Inform.*, vol. 8, no. 1, 2018, doi: 10.30864/eksplora.v8i1.139.

[3] W. M. Rahmawati and F. Liantoni, "Penggunaan Arnold Cat Map Dan Beta Chaotic Map Pada Enkripsi Data Citra," *J. ELTIKOM*, vol. 2, no. 2, 2018, doi: 10.31961/eltikom.v2i2.85.

[4] J. C. Das and D. De, "Qca based secure nanocommunication block cipher design based on electronic code book," *Malaysian J. Comput. Sci.*, vol. 31, no. 2, 2018, doi: 10.22452/mjcs.vol31no2.3.

[5] D. Vetri Priya and R. Kamaraj, "An invasive launch of two compendiums: Orange book and purple book by FDA," *Research Journal of Pharmacy and Technology*, vol. 11, no. 8. 2018, doi: 10.5958/0974-360X.2018.00666.2.

[6] S. Retno and N. Hasdyna, "ANALISIS KINERJA ALGORITMA HONEY ENCRYPTION DAN ALGORITMA BLOWFISH PADA PROSES ENKRIPSI DAN DEKRIPSI," *TECHSI - J. Tek. Inform.*, vol. 10, no. 2, 2018, doi: 10.29103/techsi.v10i2.858.

[7] Rusmala and D. Prasti, "Implementasi Metode Rail Fence Chiper dan Row Transposition Chiper Pada Mata Kuliah Kriptograpi," *Ilm. d'Computare*, vol. 9, 2019.

[8] A. P. Sidik *et al.*, "Teknik Xor Pada Mode Operasi Algoritma Cipher Block Chaining (Cbc) Dengan Kunci Acak Blum Blum Shub Dalam Meningkatkan Keamanan Data," *J. Mantik Penusa*, vol. 3, no. 2, 2019.

[9] R. Syahputra, "Penerapan Mode Operasi Cipher Block Chaining Dan Metode Lsb-1 Dalam Pengamanan Data Teks," *J. Pelita Inform.*, vol. 16, no. Juli, 2017.

[10] N. R. D. Pujiastuti, "Perancangan Modifikasi Kriptografi Modern CBC untuk Pengamanan Data/File Text," *e-print UAD*, 2017.

[11] D. Lombu, S. D. Tarihoran, and I. Gulo, "Kombinasi Mode Cipher Block Chaining Dengan

Algoritma Triangle Chain Cipher Pada Penyandian Login Website," *J-SAKTI (Jurnal Sains Komput. dan Inform.*, vol. 2, no. 1, 2018, doi: 10.30645/j-sakti.v2i1.51.