Implementation of Security with Login Data using the Electronic Code Book Algorithm

Muhammad Iqbal Panjaitan
Informatics Management Study Program, Akademi Manajemen Informatika dan Komputer Imelda, Indonesia

Article Info

Article history:

Received, Okt 09, 2018
Revised, Nov 22, 2018
Accepted, Dec 12, 2018

Keywords:

Security,
Cryptography,
Electronic code book algorithm.

ABSTRACT

Currently, the security of stored data has become an absolute requirement. Security against computer networks connected to the database is no longer safe because data leaks can be caused by irresponsible people. The results of this program can be used to secure data. One of the cryptography that is suitable for securing the data is the Electronic Code Book algorithm because the Electronic Code Book cryptography is suitable for encrypting a password in a login data. The program results show that the Electronic Code Book (ECB) algorithm is suitable for this security, because it can encrypt the password in the login data.

Corresponding Author:

Muhammad Iqbal Panjaitan,
Informatics Management Study Program,
Akademi Manajemen Informatika dan Komputer Imelda,
Jl. Kol. Yos Sudarso No.45 AB, Glugur Kota, Kec. Medan Baru, Kota Medan, Sumatera Utara 20115.
Email: iqbalpj87@gmail.com

1. INTRODUCTION

Security for data stored in databases has become an absolute requirement. Security against computer networks connected to the database is no longer safe, because data leaks can be caused by irresponsible people or parties who are directly related to the database must find a way to secure data without the intervention of the database administrator[1].

In the field of cryptography, there are two very important or main concepts, namely encryption and decryption. Encryption is the process in which information or data to be sent is converted into a form that is almost unrecognizable as initial information by using a certain algorithm. Decryption is the opposite of encryption in that it converts the disguised form back into the original information[2]. A message or data that is still original and has not been encrypted is known as plaintext. Then after disguising it by means of an encoding, this plaintext is called ciphertext. The process of disguising it from plaintext to ciphertext is called encryption (encryption), and the process of returning from ciphertext to plaintext back is called decryption[3].

Cryptography can be used to secure data. Therefore, database users need help to meet the security needs of the data they store. One of the efforts to secure the information system that can be done is cryptography[4]. Cryptographic techniques can be used to ensure document security. One that can be used is data encryption and decryption, or in other words, encoding the data so that only the person concerned knows the contents of the data. Electronic Code Book cryptography is a strong algorithm and has been declared safe until now[5].

2. RESEARCH METHOD

In carrying out this research, clear and structured stages are needed, in order to facilitate the process, it is necessary to make a diagram design such as the diagram below:

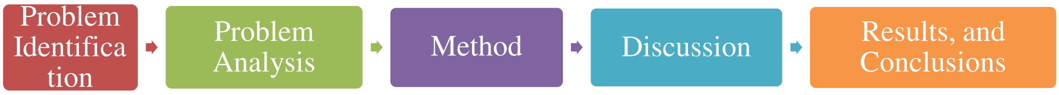


Figure 1. Diagram of Methods and Research Stages

In the stages of the research method, the author conducted interviews with experts to obtain symptoms of worms in livestock.

2.1. Basic theory

A. Cryptography

Cryptography comes from Greek. According to this language, the word cryptography is divided into two, namely crypto and graphia. Crypto means secret (secret) and graphia means writing (writing). According to terminology, cryptography is the science and art of maintaining the security of messages when they are sent from one place to another. In its development, cryptography is also used to identify message sending with digital signatures and the authenticity of messages with digital fingerprints[6].

B. Algorithm Electronic Code Book (ECB)

ECB mode is the simplest mode. ECB operates by breaking the original text of size N x n bits into N blocks with each block of size n bits (according to the block size of the encryption system), then each block is encoded with the key, and the same encryption algorithm. For decryption, the same thing is done using the decryption algorithm[7].

In ECB mode of operation, if the original text is not an exact multiple of the encoding system block size, padding is required. Padding is the addition of a few bytes to the last block of the original text so that it has the correct size multiple of the block size. The array of bytes used for padding can be either an empty byte or an array with a constant such as byte 80 followed by byte 00[8].

The second way to fulfill the length of the original text so that it is the exact multiple of the block size is the ciphertext stealing technique. With this technique the cipher text size is the same as the original text size without the need for additional padding. For example, the last 2 blocks of the initial text are PN-1 and PN. The block size is n bits, and the final block size (PN) is m bits with m <n do the following[7]:

1. Perform X = enck (Pn-1) (PN-1 block encryption).
2. Set CN = headm (X) (The function headm (X) is to take the m leading bit X).
3. Compute Y = PN | tailn-m (X) (the function headn-m (X) is to take the n-m bits behind Y).
4. Set CN-1 = enck (Y)

3. RESULTS AND DISCUSSION

This discussion section explains in general how the Electronic Code Book (ECB) algorithm works in encrypting messages. The Electronic Code Book (ECB) algorithm has the advantage, because each plaintext block is encrypted independently, we don't need to encrypt files linearly. We can encrypt the first 5 blocks, then the blocks at the end, and go back to the middle blocks and so on.

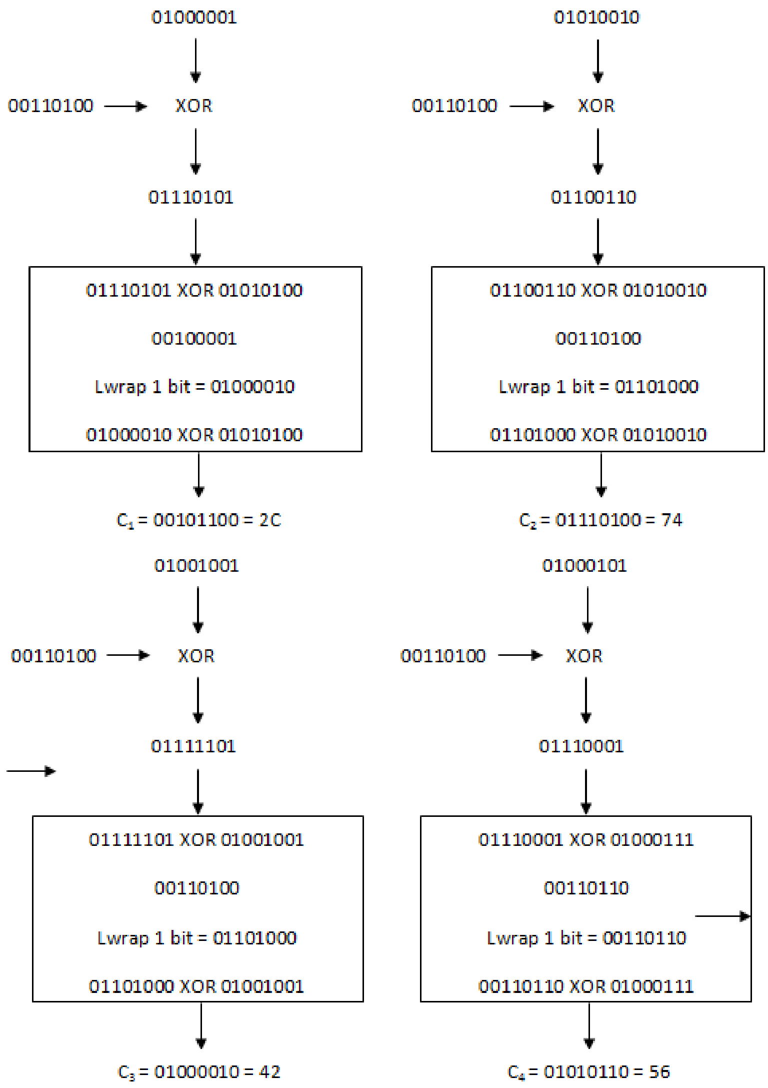
Electronic Code Book (ECB) mode is suitable for encrypting randomly accessed files, such as database files. If the database is encrypted with Electronic Code Book (ECB) mode then any record can be encrypted or decrypted independently of the other records (assuming each record consists of an equal number of discrete blocks). Error of 1 or more bits in the block ciphertext only affects the ciphertext concerned at the time of decryption. Other ciphertext blocks when decrypted are not affected by the bit error ciphertext.Based on the results of consultations and interviews with experts, the following hypothesis values are obtained:

In this mode, each plaintext block is encrypted individually and independently. Mathematically, encryption with the Electronic Code Book (ECB) algorithm is expressed as Ci = EK

(Pi) and decryption as Pi = DK (Ci). That in this case, Pi and Ci are the ith block of plaintext and ciphertext, respectively. Figure 3.1 shows the encryption of two plaintext blocks, P1 and P2 with the Electronic Code Book (ECB) algorithm, which in this case E represents the encryption function that encrypts the plaintext block using the K key.

Plaintext (in characters): DIRMAIRANI
Key (in character): BUDIDARMA
C0: 00110100 (4 in character)
Settlement:

The encryption function E used is to make the plaintext blocks 8 bits and make the key also 8 bits and then XOR the Pi plaintext block with K, then shift the bits from Pi □ K one position to the left and the wrapping results in XOR will return with the initial key.



So, the results of plaintext encryption

01000001 01010010 01001001 01000101 00100000 01001001 01010011 01001011 01000001 01001110 01000100 01000001 01010010
(DIRMAIRANI in character)

00101100 01110100 01000010 01010110 10101111 01010000 00011010 00000100 00111000 01011110 01010010 00101010 00111100
(2C744256AF501A04385E522A3C in notation HEX)

4. CONCLUSION

The password in the login data is encrypted by making the plaintext blocks 8 bits and making the key also 8 bits and then XORing the plaintext block P_i with K, then shifting the bits from $P_i \oplus K$ one position to the left and the wrapping results in XOR will return with the initial key. This login data security application was created or designed using the Microsoft Visual Studio 2008 programming language.

REFERENCES

[1] F. N. Pabokory, I. F. Astuti, and A. H. Kridalaksana, “Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard,” *Inform. Mulawarman J. Ilm. Ilmu Komput.*, 2016, doi: 10.30872/jim.v10i1.23.

[2] C. Program, S. Magister, K. Kunci, : Kriptografi, and K. Publik, “KEAMANAN DATA DENGAN METODE KRIPTOGRAFI KUNCI PUBLIK,” *J. TIMES*, 2016.

[3] Jumrin, Sutardi, and Subardin, “Aplikasi sistem keamanan basis data dengan teknik kriptografi rc4,” *semanTIK*, 2016, doi: 10.1111/cdev.12009.Mine.

[4] M. K. Harahap, “ANALISIS PERBANDINGAN ALGORITMA KRIPTOGRAFI KLASIK VIGENERE CIPHER DAN ONE TIME PAD,” *InfoTekJar (Jurnal Nas. Inform. dan Teknol. Jaringan)*, 2016, doi: 10.30743/infotekjar.v1i1.43.

[5] R. Arifin and L. T. Oktoviana, “Implementasi Kriptografi Dan Steganografi Menggunakan Algoritma RSA Dan Metode LSB,” *J. Din. Inform.*, 2013.

[6] E. Setyaningsih, “Kriptografi dan Implementasinya Menggunakan Matlab,” *Andi*, 2015.

[7] D. Rizal, T. Sutojo, and Y. Rahayu, “Implementasi Kriptografi Gambar Menggunakan Kombinasi Algoritma Elgamal Dan Mode Operasi Ecb (Electronic Code Book),” *Techno.COM*, 2016.

[8] E. Yoga and I. Kurniawan, “PENERAPAN TEORI CHAOS PADA KRIPTOGRAFI MENGGUNAKAN ALGORITMA STREAM CIPHER DAN ELECTRONIC CODE BOOK (ECB) UNTUK KEAMANAN PESAN TEKS,” *Eprints UDINUS*, 2015.