Jurnal Mantik, 7 (2) (2023), ISSN 2685-4236 (Online)

Published by:Institute of Computer Science (IOCS)

Jurnal Mantik

Journal homepage: www.iocscience.org/ejournal/index.php/mantik

Implementation of academy information database security using the blowfish method on the Medicom Campus

Jonas Franky Rudianto Panggabean[1], Leliana Harahap[2], Sartika Dewi Purba[3], Kamson Sirait[4], Sutrisno Situmorang[5]

[1,2,3,4,5]Akademi Informatika dan Komputer Medicom, Indonesia

A R T I C L E I N F O

Article history:

Accepted Jun 22, 2023
Revised Jul 07, 2023
Accepted Jul 21, 2023

Keywords:

Blowfish Algorithm;
Database;
Decryption;
Encryption.

ABSTRACT

Data is an authentic fact or evidence which must be stored and kept secure in order to avoid unwanted disturbances or threats. To avoid threats from parties who abuse or are not responsible, there are many ways to secure data, one way to do this is to create an encryption method. Methods of data security can be seen from the confidentiality of data against a threat that can be used with the blowfish algorithm. Blowfish is a 64-bit block chipper with variable key length. This algorithm can encrypt data in text form. This encryption produces ciphertext that is easy to understand and understand. Ciphertext is changing the form of text into codes that are difficult to understand and can be returned to their original position if using the same key when the data is encrypted. Data encryption techniques in databases are one of the steps used to secure and maintain data confidentiality. With this database encryption, code can be generated so that people who do not have access rights cannot access the database because the key has been generated. Database is a storage place for collections of data and information. The entire academy information system is stored in the database. Therefore, to maintain the security of the academy information database on the Medicom campus, cryptography with the Blowfish algorithm is needed. In this regard, the authors are very interested in carrying out an implementation of a document data / information security with cryptographic techniques using the Blowfish and Base64 algorithm methods. This algorithm technique was chosen because modern cryptography is a symmetric key in the form of a block cipher. This built Blowfish algorithm can encrypt text in text form. Encryption is done using a certain key, resulting in ciphertext.

Corresponding Author:

Kamson Sirait
Manajemen Informatika,
Akademi Informatika dan Komputer Medicom,
Jalan Darat No 74, Medan, Sumatera Utara, 20153, Indonesia.
Email: kamsonsirait@gmail.com

1. INTRODUCTION

Advances in technology today have a huge impact on various aspects of life, especially in the field of information and communication in storing data. In the development of technology, of course communication and information are very important. Therefore, security is needed to maintain the confidentiality of information from parties who do not have access rights. With the rapid advancement of technology, crime rates often vary. The Medicom campus has a lot of information that must be kept confidential so that irresponsible people don't know about it. If important information is known by irresponsible parties, it will harm the campus.

The Medicom campus has a lot of important data stored in a computer system. To store data into a computer, security is needed to ensure that the data is safe. Because data is very vulnerable to a crime or theft of important information by irresponsible parties (Alfikri Z. F., Studi dan Analisis Dua Jenis Algoritma Block Cipher, 2011). Therefore, so that data cannot be stolen or retrieved by other parties that have been stored, a method with the latest technology is needed to secure data on computer systems.

In the previous study, the encryption or description application had a good function and was implemented on an Android phone. Its function is to transform data into incomprehensible contents with the blowfish algorithm with a key of 72 bits or 9 characters and takes 1.49*108 years to break the computational speed (Siswo Wardoyo, 2016).

Data security using the PHP programming language is to hide PHP scripts so that unauthorized parties don't copy or modify the scripts. The integrity of the application that has been described will be better maintained. Because scripts in PHP applications cannot be re-read, unless the script has not been encrypted (Ahmad Timbul Sholeh, 2013).

Based on previous research, there is an activity to protect websites from SQL Injection. By securing the website, the website can be disguised from threats. Then the integrity of a URL must be encrypted so that the SQL Injection method cannot interfere with the URL (Aziz, 2016)

In Java programming, the security for the Blowfish method is an algorithm that cannot be patented because it has a large enough key and a variety of keys. The Blowfish algorithm is more optimal because it has more than 5 Kb of memory and has key secrecy. The concept in encryption and description is a very good way to keep data confidential by foreigners or those who do not have access rights. So that data security in information databases can be safe because of the existence of modern cryptographic methods with symmetric keys in the form of cipher blocks (Mohammad, 2012).

What is a requirement for system security is prevention by changing opportunities to be smaller by unauthorized users (N. Fahriani, 2019). Encryption of documents has also been implemented using cryptography (F. N. Pabokory, 2020). Base64 is an algorithm for converting data encoding and decoding into ASCII format which is the method used to encode binary data (S. Supiyandi, 2020). If the data we have is interesting, it will be of concern to many people who will become the target of crime, to secure it, a base 64 URL is needed so that it is not easily disturbed by SQL Injection (Nugraha, 2021). The banking world has also implemented cryptography in the cash machine security system (Dewanti, 2019). The Merkle-Hellman algorithm uses an asymmetric algorithm and has 2 main keys, namely the private key and the public key (Hadriansa, 2021).

Rapidly evolving technology now has data descriptions that can be used by all parties to keep data confidential. Therefore technological advances are needed for data security or what is called cryptography (Rio, 2011). The science that studies encryption techniques is called cryptography (Alfikri, 2019).

Security with the blofish algorithm is a way to increase database security with the MySql command. This algorithm was chosen in this study because it can work with computers that are easy to use with program code programmers (Utomo, 2017). With this application, the database is considered important in order to maintain security from people who are not entitled to know the contents of the database (Sumartini, 2019). Explained that for database encryption, the thing to do is to select the database to be encrypted, then the table names and fields appear (Yeni Yanti, 2021).

One of the impacts of technological advances is having storage media that can be shared so that it makes it easier for other parties to be able to access communications. Therefore, security is needed to protect information from irresponsible parties, so the DES, AES, IDEA and Blowfish algorithms are needed. It aims to compare the performance of the algorithms in terms of speed, data size and results of data encryption (Donzilo, 2018).

According to the terminology, cryptography is the science and art of keeping messages secure when messages are sent from one place to another (Ariyus, 2018). If you exchange messages (eg letters) with other people, then you certainly want the messages you send to reach the intended party safely (Munir, 2006). This algorithm is made by encrypting text. This encryption is done with a certain key and produces a ciphertext.

2. RESEARCH METHOD

2 Data Security

Data security on a computer is a way to avoid crimes on the system. This security is like protecting physical data, access rights, viruses and software. In making computer security, the aspects of confidentiality, integrity, authentication, non-repudiation and availability must be considered (Dominic, 2012). Electronic data security, but with its nature that is not truly random, it is necessary to do proper engineering to get an adequate level of data security (Mansoor, 2020). A combination of algorithms (CEST Cryptography) can be applied to the database of a system to increase the security of the database (Cendra Wadisman, 2020).

2.1 Cryptography

Cryptography comes from the Greek, namely cryptós which means "secret" (hidden) and gráphein which means "writing" (writing). So, cryptography means "secret writing" (secret writing). The definition put forward by Bruce Schneier , cryptography is the science and art of keeping messages secure (Cryptography is the art and science of keeping messages secure). CrypTool 2.1 can be seen that the combination of SHA1 and Knapsack is not successfully described or decoded like the original text (Nurmi Hidayasari, 2022). The problem that is easy to solve is hidden by hiding the suprincreasing sequence by multiplying modulo and permuting (Mayuni, 2021).

There are 2 types of data security methods, namely Cryptography using the Advanced Encryption Standard (AES) algorithm and Steganography using Command/DOS and displaying color in digital images based on research that a color is a combination of three basic colors, namely Red, Green, Blue (Nandar Pabokory, 2015).

There are several goals of cryptography, one of which is to create security services like the following: a) Confidentiality of data, b) Data integrity

Cryptography has 2 important components, namely encryption and description. To convert plaintext into ciphertext and vice versa. Some terms in cryptography: (a) Message (Plaintext and Ciphertext), (b) Sender and Recipient, (c) Tapper (eavesdropper), (d) Cryptanalysis and Cryptology, (f) Encryption and Decryption, (g) Cipher and Key

2.2 Blowfish

Blowfish is a cryptographic algorithm using a key in the cipher block that is used in the encryption process with the decryption process where data is entered and output like data blocks that are 64 bits in size. Blowfish was designed by Bruce Schneier in 1993 which was intended for large microprocessors (32 bits and above with a large data cache). The algorithm can make optimizations where the key doesn't change frequently because it has sub-keys. This subkey is created by calculating it before the encryption and data description process. The key expansion section has the function of changing keys whose size can be 488 bits with several subkey arrays with a total of 4168 bytes. The process of encryption consists of several iterations of 16 iterations. Each iteration has permutations and substitutions between keys and data. This whole process uses addition and XOR operations with 32 bit variables. In addition operations there are 4 tables with each iteration (Nani, 2011). The description of using the Blowfish algorithm is the same as for encryption, except that P1, P2,..., P18 are used in reverse order. The blowfish algorithm encryption process can be seen in Figure 1 below.

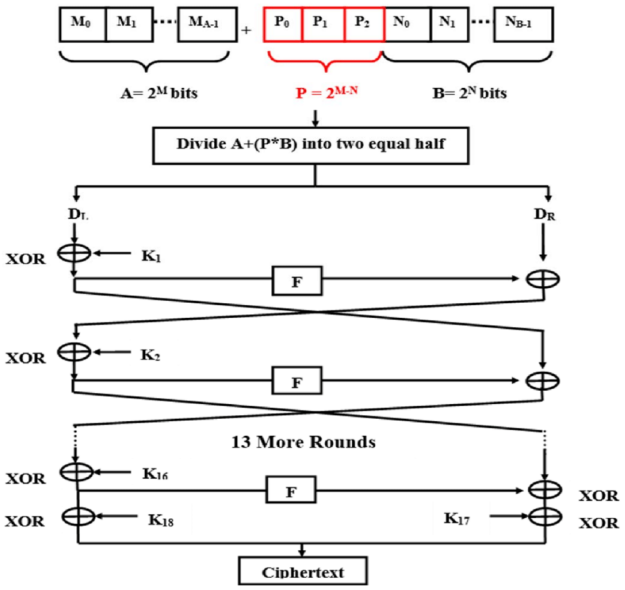

Figure 1. Blowfish Algorithm Encryption Proces

The following is Figure 2 of the F function found in the Feistel network.

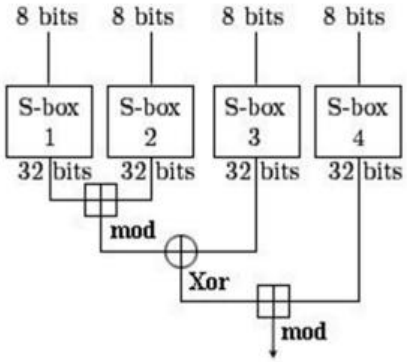

Figure 2. Schematic of the F function in the blowfish algorithm

The bowfish algorithm decryption is the same as the encryption process, except that P1, P2,..., P18 are used when the sequence is reversed. but the input is ciphertext (Schneier, 1994). The following is Figure 3 of the blowfish algorithm decryption process.

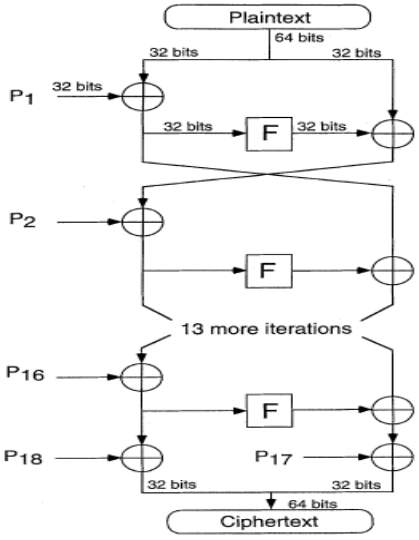

Figure 3. Blowfish Algorithm Decryption Process

3. RESULTS AND DISCUSSIONS

3.1. Application System Architecture

The Medicom campus has a cryptographic application system architecture such as data content, encrypted data to the database and description process.

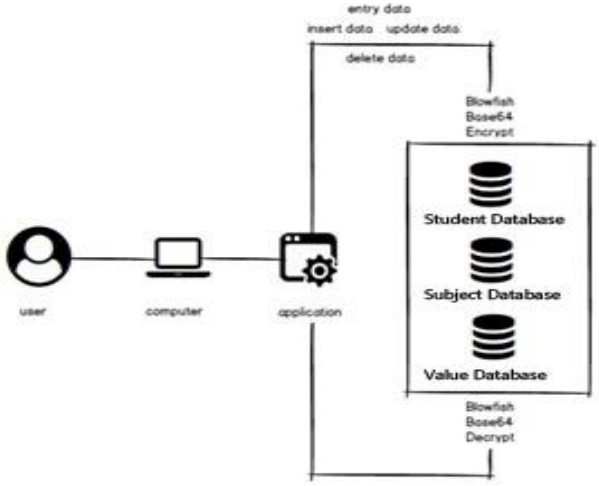

Figure 4. Application System Architecture

3.2. Database Design

a. Class Diagrams

In this class diagram, it explains the relationship between each class with details that are in one design model in a system. In this diagram describes the rules of each entity.

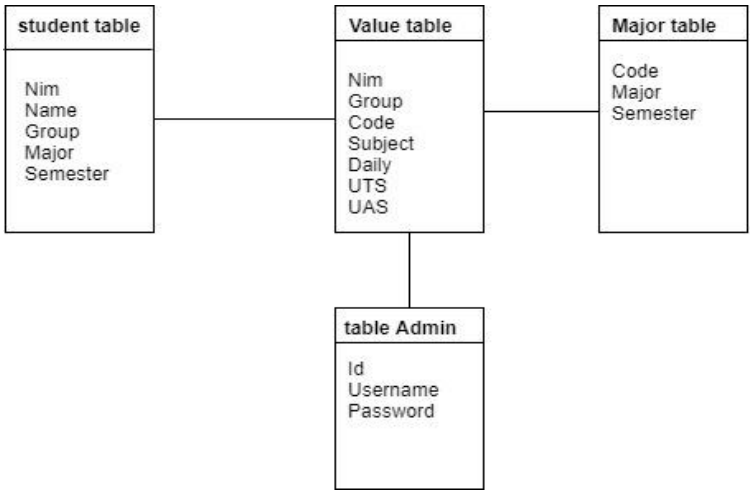

Figure 5. Class Diagrams

b. ERD (Entity Relationship Diagram)

Entity Relationship Diagram (ERD) is designed to create an overview of database models that function to facilitate users in designing databases.

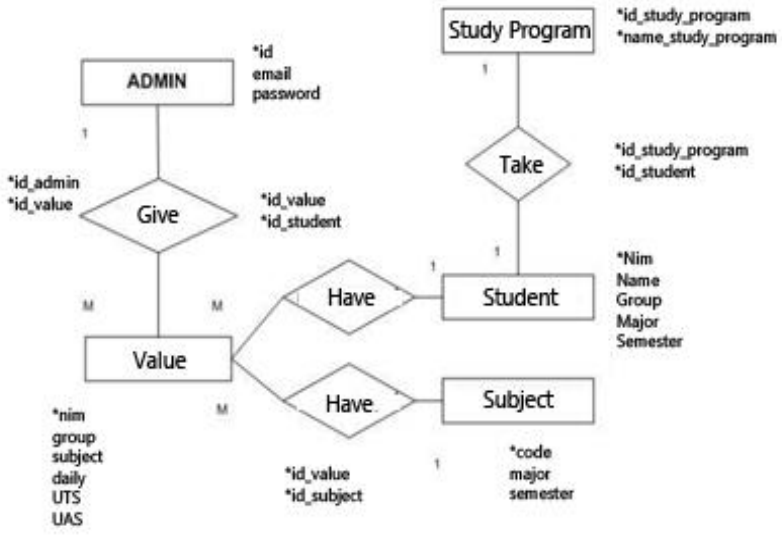

Figure 6. ERD

c. Menu Design

In the information system cryptography application on the Medicom campus which is made with several specified menus.

d. Change Data Flowchart

The application or program layer display must be clear, so that it is easily understood and understood by the user. In this application view consists of the main display page, adding data, searching, deleting and editing data.

3.3. Application Algorithm

a. Login Algorithm

This login algorithm explains who can access the application, before being able to access the application, you must first log in with your username and password on the main menu display of the application.

b. Dashboard Algorithm

This view explains the main application menus, such as student data, grade data, course data, and logout. Each menu has a different appearance and function according to its function.

c. Shown Algorithm

This view displays data that has been encrypted and returns to the original text on student data.

d. System Process Algorithm

In this view, it describes the system in the encryption process, explaining how the encryption process works until the processed cipher text appears.

e. Process Algorithm System Description Blowfish

In this algorithm process, it explains how to process the description to get the original text or plaintext.

3.4. Implementation And Testing Solutions

a. Testing Method

The black box method is a way to check the function of input and output in programs and applications. The process to be carried out to produce comparable output values.

b. b. Input Data

The input data is used as a comparison in entering data into the cryptographic system database. The method used to check is to calculate the amount of time it takes to process the encryption and description in the application program.

c. Encryption Table

In testing, we will discuss which tables can be encrypted. Which serves to check the original data before encryption.

d. Table Description

In the description table, checks are made to original data such as student names.

3.5. Screen Display

In the display of the encryption layer and description of the Medicom campus information data, it starts from the initial display to finish / log out.

a. Login Form Screen Display

This view serves to enter into the main menu application. Those who can enter this application are those who are given access. To be able to enter the main menu, you must fill in the username and password data. If it is wrong, an error notification will appear or the username or password is wrong.

Figure 7. Login display

b. Dashboard Menu Screen Display

This screen will appear when you have successfully logged in. This view contains all the menus that will be processed.

4. CONCLUSION

The results of the analysis that has been carried out from the problem and resolved, it can be concluded that website-based database security with the blowfish and base 64 methods is very important because with this method it can protect database security. Database security is done using the blowfish method and base 64 managed to create an encryption code that is built in text form. Encryption is done using a certain key, resulting in an incomprehensible and unintelligible ciphertext. The ciphertext can be changed back to its original state if it is decrypted using the same key at the beginning when encrypting the database.

ACKNOWLEDGEMENTS

Thanks to AMIK Medicom, Foundation, Director, Management and all AMIK Medicom employees at Jalan Darat No.74 Medan

REFERENCES

Ahmad Timbul Sholeh, E. G. (2013). MENGAMANKAN SKRIP PADA BAHASA PEMOGRAMAN PHP DENGAN MENGGUNAKAN KRIPTOGRAFI BASE64 . *Jurnal Algoritma Sekolah Tinggi Teknologi Garut* , 1-9.

Alfikri. (2019). *Studi dan Analisis Dua Jenis Algoritma Block Cipher:DES RC5.* Bandung: Sekolah Teknik Elektro dan Informatika Institut Teknologi Bandung.

Alfikri, Z. F. (2011). *Studi dan Analisis Dua Jenis Algoritma Block Cipher.* Bandung.

Ariyus, D. (2018). *Kriptografi Keamanan Data Dan Komunikasi.* Yogyakarta: Graha Ilmu.

Aziz. (2016). Penerapan Kriptografi Base64 Untuk Keamanan URL (Uniform Resource Locator) Website Dari Serangan SQL Injection. *Jurnal Algoritma*, 1-8.

Cendra Wadisman, d. (2020). PENGAMANAN DATABASE MENGGUNAKAN KOMBINASI ALGORITMA (CEST CRYPTOGRAPHY) DAN Algoritma BASE64. *JURTEKSI (Jurnal Teknologi dan Sistem Informasi).*

Dewanti, F. E. (2019). Implementasi Kriptografi dalam Sistem Keamanan Anjungan Tunai Mandiri. *J. Inform. Upgris.*

Dominic, B. (2012). A Cryptographic Algorithm Based on a Pseudorandom Number Generator. *International Symposium on Symbolic and Numeric Algorithms for Scientific Computing.*

Donzilo. (2018). Perbandingan Algoritma DES,AES,IDEA, Dan Blowfish Dalam Enkripsi Dan Dekripsi Data', Jurnal Teknologi Terpadu. *Jurnal Teknologi Terpadu.*

F. N. Pabokory, I. F. (2020). Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard. *Inform. Mulawarman J. Ilm. Ilmu Komputer.*

Hadriansa, M. F. (2021). Rekayasa Aplikasi Kriptografi dengan Penerapan Kombinasi Algoritma Knapsack Merkle Hellman dan Affine Cipher. *J. Teknol. Inf. dan Ilmu Komputer*.

Mansoor, O. S. (2020). Performance Analysis of Stream and Block Cipher Algorithms. *Third International Conference on Advanced Computer Theory and Engineering (ICACTE)*.

Mayuni. (2021). Implementasi Algoritma Knapsack dan Algoritma Spritz dalam Mengamankan File. *Jurnal Teknologi dan Sistem Informasi*.

Mohammad. (2012). Implementasi Sistem Enkripsi Pengiriman Pesan Instan Java Dengan Algoritma Blowfish. *Jurnal Format*.

Munir, R. (2006). *Kriptografi.* Bandung: Informatika.

N, A. (2017). Penerapan Kriptografi Base64 Untuk Keamanan URL (Uniform Resource Locator) Website Dari Serangan SQL Injection. *Jurnal Algoritma*.

N. Fahriani, P. A. (2019). Alternatif Penanganan Jenis Serangan Pencurian Data Pada Jaringan Komputer. *Teknol. dan Rekayasa Inf*.

Nandar Pabokory, F. d. (2015). Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard. *Jurnal Informatika Mulawarman*.

Nani, P. A. (2011). *Penerapan Enkripsi Algoritma Blowfish Pada Proses Steganografi Metode EOF*. Kupang: Universitas Katolik Widya Mandira.

Nugraha, E. G. (2021). Penerapan Kriptografi Base64 Untuk Keamanan URL (Uniform Resource Locator) Website Dari Serangan SQL Injection. *J. Algoritm.*

Nurmi Hidayasari, d. (2022). Penerapan Keamanan Basis Data Dengan Menggunakan Kombinasi Teknik Enkripsi SHA Dan Knapsack. *Jurnal Nasional Industri dan Teknologi* .

Rio. (2011). *Implementasi Algoritma RSA Dan Blowfish Untuk Enkripsi Dan Deskripsi Data Menggunakan Delphi 7.* Jakarta: Fakultas Sains dan Teknologi Universitas Islam Negeri Jakarta.

S. Supiyandi, H. H. (2020). Implementasi dan Penggunaan Algoritma Base64 dalam Pengamanan File Video. *J. MEDIA Inform. BUDIDARMA*.

Schneier, B. (1994). Description of a New Variable-Length Key, 64-Bit Block Cipher. *Springer Verlag*.

Siswo Wardoyo, R. F. (2016). Aplikasi Teknik Enkripsi Dan Dekripsi File Dengan Algoritma Blowfish Pada Perangkat Mobile Berbasis Android . *SETRUM*, 2301-4652 .

Sumartini, A. R. (2019). Implementasi Kriptografi Menggunakan Metode Blowfish Dan Base 64 Untuk Mengamankan Database Informasi Akademik Pada Kampus Akademi Telekomunikasi Bogor Berbasis Web-based. *Jurnal E-KOMTEK (Elektro-Komputer-Teknik)* .

Utomo. (2017). Implementasi Algoritma Blowfish untuk Enkripsi Database Mysql pada Sistem Informasi Data Aset Berbasis Web. *Faculty of Information Technology T1 - Informatics Engineering*.

Yeni Yanti, d. (2021). Implementasi Sistem Keamanan Database Menggunakan Metode Triangle Chain. *Serambi Engineering*.