MATICS : Jurnal Ilmu Komputer dan Teknologi Informasi ISSN : 1978-161X(p); 2477-2550(e)
Volume 16, No. 2(2024), pp 92-96 DOI : 10.18860/mat.v16i2.28893
Received : August 16th 2024; **Accepted** : August 27th 2024 ; **Avalaible Online** : September 20th 2024

Data Encryption and Security in Data Storage Management Information System Using Blowfish Algorithm

Mayang Anglingsari Putri, Denisha Trihapningsari, Anggi Gustiningsih Hapsani, Chandra Sina Putra

***Abstract*— Documents and archives are crucial components of BPAD (Badan Perpustakaan Arsip dan Dokumentasi) Malang, as its primary responsibility is the management of archives. However, the management of mail archiving and approval letters is still done manually, with no data security measures in place. This system is expected to assist in managing and documenting all messages within BPAD (National Library of Archives and Documentation) Malang, including both incoming and outgoing mail. The letters stored in the system are secured through encryption using the Blowfish algorithm, ensuring that important data is protected and safe from manipulation. This application simplifies the process of data collection, archive storage, and securing image archives in BPAD Malang by using the Blowfish algorithm, thus safeguarding the data from the risk of misuse.**

***Index Terms*— Management Information System Archiving; Blowfish.**

I. INTRODUCTION

In the current era of globalization, organizations are evolving rapidly and need to be more strategic in managing their systems. One critical area of focus is the filing system. Efficient and well-organized filing systems are essential for maintaining order, ensuring quick access to information, and supporting overall operational effectiveness as businesses grow and become more complex [1][2].

Archived data or records the information recorded in any form or medium, created, received, and maintained by an organisation in order to implement the activities. Managing the archive is not merely treat it from the technical point of recording is mere media management rather than the role of archives as a source of information. From this standpoint, it would seem useful archival value as necessary as information. Archives as archival information clearly occupy a vital position in an organisation. Archives will be needed in the whole process of organisational management activities of planning, implementation, and oversight [3].

Mail archiving information system can assist in archiving management in companies and government agencies including the one of which is BPAD (Badan Perpustakaan Arsip dan Dokumentasi) Malang. The archive is an important part of the government agencies because the main task is the management BPAD poor district archives. However, the management of mail archiving and approval letters is still done manually, and there is no data security in place. Incoming mail is stored in the form of documents and save in special storage shelves, and note the location of storage in Microsoft Access. Mail search is still done manually so that it takes a long time. The letter was BPAD could be a letter as well as request funding agencies and others.

The system can help manage and document all messages are in BPAD Malang. Both incoming and outgoing mail. Letters contained in the system is also secured by means of encryption using the Blowfish algorithm to secure data archive important letters so that data is safe and away from the risk of misuse.

Blowfish was chosen for data encryption in the Data Storage Management System because it balances speed, efficiency, and robust security. Its flexibility, with a key length of up to 448 bits, ensures strong protection for sensitive data. Being patent-free, it's an accessible and cost-effective option. Since its introduction in 1993, Blowfish has consistently proven reliable in safeguarding information, making it a trusted choice for keeping data safe from manipulation and unauthorized access.

II. LITERATURE RIVIEW

A. BPAD

There is a supporting element implementing important Malang Regency is a Library, Archives and Documentation. the task of the organization BPAD Malang as follows:

1. Implement regional government affairs in the preparation and implementation of regional policy field of Libraries, Archives and Documentation;
2. Carry out other duties given by the Regent in accordance with the duties and authority.
3. The collection, management and control of data in the form of data base and data analysis to draw up a program of activities.

Manuscript received August, 2024. (Write the date on which you submitted your paper for review.)

Mayang Anglingsari Putri author is a lecturer at the Department of Information System, Faculty of Science and Technology, Terbuka University, Indonesia. (email : mayang.anglingsari@ecampus.ut.ac.id)

Denisha Trihapningsari author is a lecturer at the Department of Information System, Faculty of Science and Technology, Terbuka University, Indonesia. (email : denisha@ecampus.ut.ac.id)

Anggi Gustiningsih Hapsari Author is a lecturer at the Department of Mathematics, Faculty of Science, Brawijaya University, Indonesia. (email : anggigustiningsih@ub.ac.id)

Chandra Sina Putra Author is a writer from the Ministry of Education and Culture of the Republic of Indonesia, Indonesia. (email: chandra.sina@kemdikbud.go.id)

B. Blowfish Algoritm

The Blowfish algorithm included in the encryption of 64-bit block Cypher with key lengths vary between 32-bit to 448-bit. The blowfish algorithm consists of two parts, namely the generation of sub-keys (KeyExpansion) and Data Encryption. Data Encryption consists of a simple function iterated (Feistel Network) as many as 16 times around. All operations are addition (addition) and XOR on a 32-bit variable. Other additional operations are four search table (lookup table) indexed array for each round [4].

Blowfish in the algorithm used many subkeys. These keys must be calculated or generated in advance before the data encryption or decryption [5][6]. In the Feistel network, Blowfish have 16 iterations, is a 64-bit input data elements or call it "X". To perform the encryption process steps are as follows[7]:

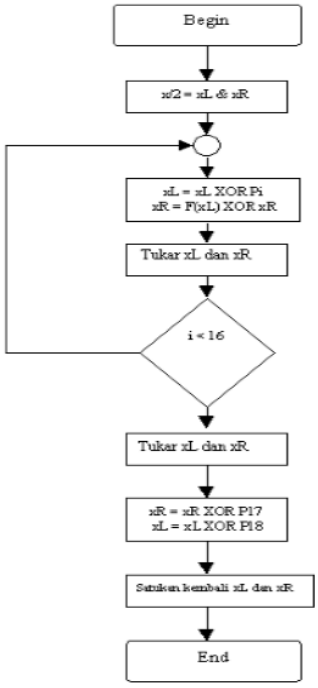

Figure 2.1 Flowchart Blowfish encryption process

Encryption process from the image above, is described as follows:

1. P-array of as many as 18 pieces (P1, P2, P18 .....) each worth 32-bit.Array msing P consists of eighteen key 32-bit subkey:
   $P_1,P_2,.....,P_{18}$
2. S-box of 4 pieces each worth 32-bit which has input 256. Four 32-bit S-boxes each having 256 entries
   $S_{1,0},S_{1,1},.....,S_{1,255}$
   $S_{2,0},S_{2,1},.....,S_{2,255}$
   $S_{3,0},S_{3,1},.....,S_{3,255}$
   $S_{4,0},S_{4,1},.....,S_{4,255}$
3. plaintext to be encrypted is assumed as an input, the plaintext taken as many as 64-bit, and if less than 64-bits then we add bits, so that in later operations in accordance with the data [8].
4. Results of earlier decision divided by 2, 32-bit first so-called XL, 32-bit second is called XR.
5. Next do the operation xor Pi XL = XL and XR = F (XL) xor XR
6. The results of the above operas are exchanged XL XR and XR becomes XL.
7. Do as much as 16 times, looping the 16th to do again the process of exchange of XL and XR.
8. At the 17th through surgery for XR = XR xor P17 and P18 XL = XL comply.
1. The final process re-XL and XR unit so that a 64-bit back.

Table 2.1 Table XOR

P	Q	HASIL
F	F	F
F	T	T
T	F	T
T	T	F

Then to find the function F is as follows: For XL, into four 8-bit parts: a, b, c and d.

$F(XL)=((S1,a + S2,b \bmod 2^{32})xor S3,c) + S4,c \bmod 2^{32}$

Subkey is calculated using the Blowfish algorithm, the method is as follows:

1. First is a initialization P-array and then the four S-boxes in order, with a fixed string. This string consists of the hexadecimal digits of Pi.
2. XOR P1 with the first 32-bit key, XOR P2 with the second 32-bit key and so on for each bit of the key (until P18) Repeat on the key bits until the entire P-array XORed with key bits.
3. Encrypt all zero string with the Blowfish algorithm, using the subkeys described in steps (1) and (2).
4. Replace P1 and P2 with the output of step (3).
5. Encrypt the output of step (3) with the Blowfish algorithm with the modified subkeys.
6. Replace P3 and P4 with the output of step (5).
7. Continue the process, replacing all elements of the P-array, then all four S-boxes in order, with the output kontiyu changing Blowfish algorithm.

III. DISCUSSION

In this study, researchers tried to apply the blowfish algorithm to secure an image archive. Before performing the encryption process, the image file must first change into the form of a string that can be calculated using the Blowfish algorithm, there are several ways you can do, such as taking the RGB values at each pixel of the image, this method has the disadvantage that the result file encode it so great , because each pixel has 3 independent value, while the other way and more practical is to use BASE64 encoding, in addition to the results file that is much smaller encode process is so much lighter because the machine does not need to read every detail pixel.

Here is an example of the original image file string is still in the process or can be called raw data

Figure 3.1 The original image file

After getting this string file, begin the process encoded using base64 encoded, the following is an example of its string

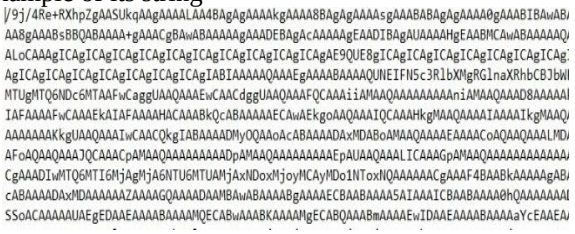

Figure 3.2 BASE64 encoding results

The blowfish algorithm has an arithmetic process. So the result is to change the character of the fruit each encode the BASE 64 decimal digits into the form by the ASCII characters. Here is an example of the results.

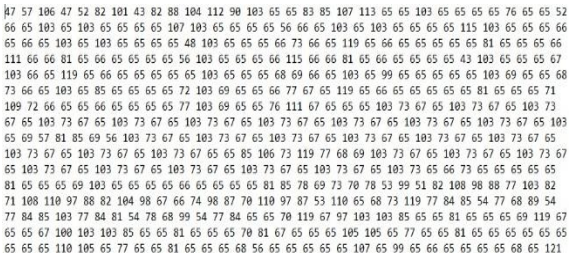

Figure 3.3 plaintext files

Decimal digits into plaintext or Preliminary data will be encrypted with Blowfish algorithm. The next process before encryption starts is counting subkeys, namely 18 pieces PBOX 32bit and 32bit 4 pieces of 256 entries sbox. Sub Keys is a row of numbers pi classified

A. Calculating Sub Keys

The following is an example of the first 50 series of numbers pi

1415926535 8979323846 2643383279 5028841971 6939937510

PBOX contains 32 bit binary number, if any one decimal-value 8 bit, then the fruit PBOX or sbox worth 4 decimals.

Categorize each 4 decimals into 1 piece PBOX as many as 18, and then four groups that each group sbox sbox each have 256, so the total should be grouped as follows:

$$18+(4 \times 256)=1042 \text{ Buah}$$

The next step is XOR every decimal of each PBOX & SBOX the decimal key

Table 3.1. calculate subkeys

Key	3	5	2	7
	XOR			
Pbox1	1	4	1	5
Pbox2	9	2	6	5
Pbox3	3	5	8	9
Etc. To All SBOX….				

The results of XOR PBOX And KEY

Pbox1	2	1	3	2
Pbox2	10	7	4	2
Pbox3	0	0	10	14
Etc. To All SBOX….				

The next step, replace the value PBOX and sbox which originally was a series of numbers such as pi into the XOR results table above, so PBOX and sbox will always change with the key.

B. Encryption process

Process time to process 64-bit Blowfish algorithm, if a decimal is 8 bits, it mean classify every 8 digit decimal plaintext Becoming One, example numbers image at plaintext differences, ON Figure 3.8, the following examples of calculation 64 bit first plaintext

Tabel 3.2 Calculation 64 bit first plaintext

X LEFT				X RIGHT			
47	**57**	**106**	**47**	**52**	**82**	**101**	**48**
2	1	3	2	21	27	18	10
45	56	105	45	33	73	119	58
Repeat 16 X							
49	70	124	4	57	58	104	39
5	1	2	1	3	2	10	6
52	**71**	**126**	**5**	**58**	**56**	**98**	**33**

Tabel 3.2 first roun F(X) Calculation

Sbox 1 [45]	5	13	3	7	
Sbox 2 [56]	4	13	5	4	
	9	26	8	11	total
Sbox 3 [105]	7	2	7	15	
	14	24	15	4	xor
Sbox 4 [45]	7	3	3	6	
F(X) Rotation 1	**21**	**27**	**18**	**10**	total

The calculation of F (x) is performed each iteration except on lap 17, the following is example the result of the encryption or called by CiperText

```
52,71,126,5,58,56,98,33
92,115,125,66,93,80,106,83
80,86,116,71,93,71,99,87
110,96,4,92,81,92,79,75
94,95,69,94,77,78,64,98
112,83,38,110,116,126,90,76
94,95,69,94,77,78,64,98
84,75,78,88,118,90,72,79
94,95,69,94,77,78,64,98
```

Figure 3.4. Ciper Text

C. Decryption Process

For the calculation of the decryption process exactly the same as the above calculation, which changed only order PBOX beginning of PBOX 18th and end at the PBOX 0, if the above calculation of the initial data is the plaintext then the decryption process is the initial data of course is the CiperText, the following is example the calculations

Tabel 3.4. The first 64-bit decryption process

X LEFT				X RIGHT			
52	**71**	**126**	**5**	**58**	**56**	**98**	**33**
5	1	2	1	21	23	15	5
49	70	124	4	47	47	109	36
Ulangi 16 kali							
45	56	105	45	62	85	97	50
2	1	3	2	10	7	4	2
47	**57**	**106**	**47**	**52**	**82**	**101**	**48**

Tabel 3.5. The calculation of F (x) decrypt at first round

Sbox 1 [49]	4	4	4	1	
Sbox 2 [70]	4	13	0	2	
	8	17	4	3	total
Sbox 3 [124]	7	6	1	1	
	15	23	5	2	xor
Sbox 4 [4]	6	0	10	3	
F(X) Rotation 1	**21**	**23**	**15**	**5**	total

IV. IMPLEMENTATION

The results of the implementation of management information system archiving using blowfish algorithm As Security Archive Picture at BPAD Malang and illustrated in full and restructuring by using the programming language PHP and HTML [9]. HTML and PHP language used to build web pages. HTML is a markup language that is commonly used because of its ease of use. [10] [11]. HTML and PHP has the function of which can determine the format of a text, create lists, create links to other documents, insert images, and can display information in tabular form [12] [13].

The first page contain of mail storage and finding a letter in the Management Information System Archiving Using Blowfish algorithm As BPAD Security Archive Picture at Malang

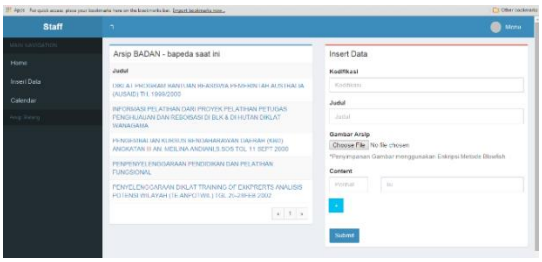

Figure 4.1 Saving image data

This system there is a menu to add a data archive which includes codification letter, title, image archive, content. The content here are dynamic and can be added as needed.

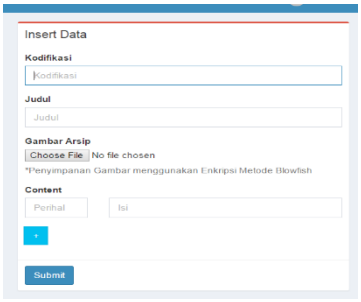

Figure 4.2 data input

The next step is directly select titles from the archive you want to view by pressing the picture archives show. And it will go to the security page where staff must input the code to see the archived data so that the data truly safe

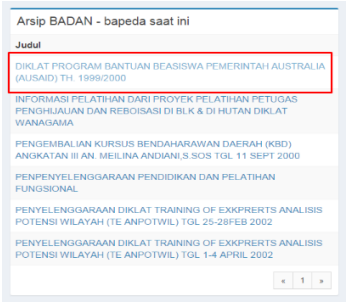

Figure 4.3 archive data entry

Input code to see the data, this page is used for securing data media images.

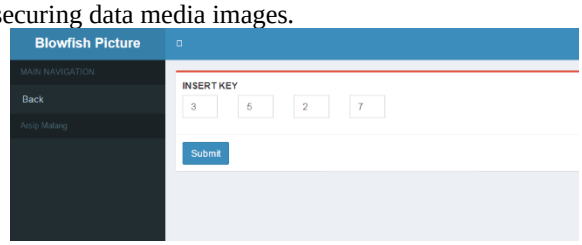

Figure 5.13 see a data

If you correctly fill the key is, here use the key 3527 then the data was successfully processed by the system will display the image data as below.

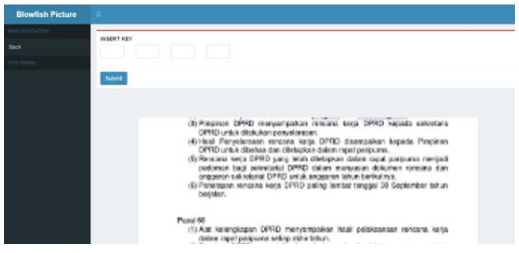

Figure 5.14 successful

If the key is loaded by staff of wrong the data is not successful at the process and will appear like the view below

Figure 5.15 WRONG key

The implemented system at BPAD has had a significant positive impact on both the organization and its users. Feedback from users shows enhanced operational efficiency, with quicker archive management and easier access to crucial documents. Users also value the system's usability, noting its intuitive and user-friendly interface. Moreover, the integration of the Blowfish algorithm for data encryption has greatly improved the security of sensitive information, safeguarding archival data from manipulation and unauthorized access. These advancements have not only increased user confidence in the system but also ensured that BPAD adheres to high security standards in managing government archives.

V. CONCLUSIONS AND RECOMMENDATIONS

A. *Conclutions*

From the discussion described in chapters 1 through 6 can be obtained several conclusions as follows:

a. With this application, can help mail archiving officers to facilitate the search process, archive storage and helps to document all the letters in BPAD Malang
b. Applications can perform image archive security at BPAD using Blowfish Algoritama, so that data is safe and away from the risk of misuse

Future research should focus on exploring and comparing additional encryption algorithms and techniques to enhance data security and efficiency. This includes evaluating emerging cryptographic methods, testing their performance in real-world scenarios, and considering their scalability and practical implementation challenges.

B. *Recomendations*

Based on this research, there are some suggestions for the development of this application is as follows:

a. using blowfish algoritama method is not the only method used in performing bpad data security at malang districts, it's best to try to compare by using the other methods in order to get a better result.

REFERENCES

[1] Jogiyanto. 2008. *Sistem Teknologi Informasi*. Yogyakarta: Penerbit ANDI.

[2] Hasugian, Jonner. 2009. *Pengantar Kearsipan*. Modul kuliah. Program Studi Ilmu Perpustakaan Fakultas Sastra Universitas Sumatera Utara.

[3] Tata Sutabri, 2005, *Sistem Informasi Manajemen*, Yogyakarta, Andi.

[4] Wilnic Izaac., Maraunuela . 2013. *Implementasi algoritma BLOWFISH padabasis data honorarium mengajar Dosen tidak tetap FTI UKSW* SALATIGA : FTI

[5] **Schneier, Bruce.1996.** ***Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish).*** Cambridge Security Workshop Proceedings

[6] Joko, Mochamad. 2009. *Amazing News Website with PHP, Ajax, dan MySQL.* Yogyakarta: Penerbit ANDI.

[7] Rosa, A.S., Shalahuddin, M., 2011. *Modul Pembelajaran Rekayasa PerangkatLunak (Terstruktur dan Berorientasi Objek)*. Bandung: Modula.

[8] Syafari, Anjar, 2007, *Sekilas Tentang Enkripsi Blowfish*, <www.ilmukomputer.com>, diakses tanggal 10 Juni 2008.

[9] Hakim, Lukmanul. 2009. *Trik Rahasia Master PHP*. Yogyakarta: Penerbit Lokomedia.

[10] Hariyanto, Bambang. 2004. *Sistem Manajemen Basis Data*. Bandung: Informatika.

[11] Madcoms. 2009. *Menguasai XHTML, CSS, PHP, & MySQL melalui DREAMWEAVER.* Yogyakarta: Penerbit ANDI.

[12] Nugraha WP, Antonius. 2010. *CodeIgniter: Cara Mudah Membangun Aplikasi PHP*. Jakarta Selatan: mediakita.

[13] Pudjo Widodo, Prabowo dan Herlawati. 2011. *Menggunakan UML*. Bandung: Penerbit INFORMATIKA.

Mayang Anglingsari Putri, is a lecture in the Department of Information System, Faculty of Science and Technology, Terbuka University, Indonesia . Mayang research interests are the Artificial Intelligence, Software Engineering, Information Systems (Business Informatics), and Human-Computer Interaction.

Denisha Trihapningsari, is a lecture in the Department of Information System, Faculty of Science and Technology, Terbuka University, Indonesia . Denisha research interests are Artificial Intelligence, information system analyst, analysis and design system, and distance education learning.

Anggi Gustiningsih Hapsani, is a lecture in the Department of Mathematics, Faculty of Science, Brawijaya University, Indonesia. Anggi research interests are Artificial Intelligence, Computer Vision, Science Data and Computer Science.

Chandra Sina Putra, is a writer at the Ministry of Education and Culture of the Republic of Indonesia, Indonesia. Chandra's research interests are Software Engineering and Human-Computer Interaction.