RESEARCH ARTICLE OPEN ACCESS

E-Document Safety AtUniversity Of Buana Perjuangan Karawang Using Qr Code Using Encryption Blowfis Method

Agung Susilo Yuda Irawan*, Tohirin Al Mudzakir**, Kiki Ahmad Baihaqi***, Cici Emilia Sukmawati****,Candra Zonyfar*****

*(Pascasarjana Ilmu Komputer, University Of Budi Luhur, Jakarta)
**(Pascasarjana Ilmu Komputer, University Of Budi Luhur, Jakarta)
***(Pascasarjana Ilmu Komputer, University Of Budi Luhur, Jakarta)
****(Pascasarjana Ilmu Komputer, University Of Budi Luhur, Jakarta)
*****(Pascasarjana Ilmu Komputer, University Of Budi Luhur, Jakarta)

----------**********----------

Abstract:

Academic information systems (SIAK) on a college employee was very helpful in terms of improving the services, many activities are carried out in the system starting from the Exchange that is casual are important and confidential. in the academic information system E-Document that is important and should be maintained its authenticity. E-Document Exchange that high intensitasnya not cover the possibility of causing vulnerability to theft, forgery of documents by a party which is not a responsible course would be bad. This need for awareness to all stakeholders in terms of securing an E-Document so that its authenticity remains awake. some of the ways that can be applied in E-Document security one way to secure E-Document with encryption on the document. The research on the algorithms used is various algorithms blowfish, blowfish or openPGP encryption Cipher4 is included in the symmetric cryptosystem. Blowfish algorithms are created to be used on computers that have large microprocessor (32 bit upward with the large data cache) and combined with a QR Code. QR Code itself began to be developed in 1994 by denso wave that aims to convey information quickly and get quick responses. For the process of testing conducted the first two processes, testing randomness encryption using the Avalanche Effect and user acceptance testing using User Acceptance Tersting.

Keywords **—academic information systems, encryption, description, Algorithm blowfish, E-Document, QR Code.**

----------**********----------

I. INTRODUCTION

The development of information technology in the field of education gave birth to the formation of several applications of information systems, among others: Academic information systems, E-learning, E-library, E-just my assesment, the E-tutor, the portal can help students, lecturers, staff, and was also President at a College in performing tridharma colleges and improve the quality of service and learning.

The activities of the academic Information system still requires media documentation hard or soft coppycoppy as output. coppy soft or digital documents resulting from the application of the academic information system interactions with students, administrative staff as well as other parties who are related.

The number of benefits of academic information system makes many tape high in indonesia, using and developing the academic information system. With the exchange of data and information that is

extremely high intensitasnya not closing the possibility is no data or information that is important and has a confidentiality must be maintained until it is accepted by the party entitled. Data or information that secret usually becomes the target of the parties are not responsible for stolen or modified. This makes the need for awareness of the system administrator to implement a high security on the file or files to be posted or downloaded by the user, so that the file or files that are sent to a secure original. many ways to safeguard such information, data or one example with the techniques of cryptography (encryption and description) of the data or information before files or information is sent.

II. THEORETICAL BASIS

A. Information Security

Information security is an effort to protect the information assets that are owned. Which is the protective measures to ensure the sustainability of the business, minimizing the risk that mingkin may occur and maximizing a benefit of investment and business opportunities. Achieve security itself can do a few different ways and strategies that can both do together or in combination with another. Each security strategy of information system has the focus and specific purpose in accordance with their needs [1].

B. Digital Signature

A digital signature is a message contains numbers that are dependent on some secre (secret) the confidentiality that is known only by the signer (signing of messages) and in addition, it also depends on the content of the message is signed [2].

A Digital Signature or digital signature is a mechanism that serves to replace the manual signature on a paper document to digital which contained security process [3]

C. Cryptography

In the terminology of algorithms is a logical sequence of steps in the menyesaikan concern that are arranged symmetrically. Keriptografi algorithm is the logical step step how to hide the contents of the message from people who are not the right

Cryptography is the science that studies how to keep data or message for safe when sent from the sender to the receiver or otherwise without any interference from the party not entitled to

1) Blowfish Algorithm

Blowfish or OpenPGP. Cipher4 encryption is included in the Symmetric Cryptosystem. (Schneier, 1996) Blowfish algorithms are created to be used on computers that have large microprocessor (32 bit upward with the large data cache). Blowfish is a block cipher which also means

during the process of encryption and Blowfish description, work by dividing a message into blocks of bits of the same length with the size, i.e. 64-bit key length to vary that encrypts data in 8 bytes blocks. When there is a message that is not a multiple of 8 bytes then the message will be added an extra bit-bit (padding) so the size of each block are the same. Blowfish algorithm consists of two parts: key expansion and data encryption.

Blowfish uses a subkey that is huge, must be computed before encryption processes and data descriptions. The algorithm that Feistel network implements the Blowfish consists of 16 rounds. The input element is 64 bit, X for the Groove encryption algorithms Blowfish method described as follows:

1. The initial form P-array is 18 (P1, P2, ..., P18), each of which is 32-bit. The P array consists of eighteen 32bit key subkeys: P1, P2, ..., P18
2. The shape of the S-box as much as 4 pieces each 32-bit value that has 256 entries. Four 32-bit S-box each having 256 entries:
   $S_{1.0}, S_{1.1}, S_{1.2}, \ldots\ldots\ldots\ldots, S_{1.255}$
   $S_{2.0}, S_{2.1}, S_{2.2}, \ldots\ldots\ldots\ldots, S_{2.255}$
   $S_{3.0}, S_{3.1}, S_{3.2}, \ldots\ldots\ldots\ldots, S_{3.255}$
   $S_{4.0}, S_{4.1}, S_{4.2}, \ldots\ldots\ldots\ldots, S_{4.255}$
3. Plaintext that is encrypted is assumed as the plaintext input, taken as many as 64-bit, and if less than 64-bit then we add bitnya, so that in operation later in accordance with the data.
4. The results of the retrieval of yesteryear shared 2, 32-bit first called 32-bit XL, the second is called the XR.
5. Next do the operation XL = XL xor Pi XR = a and F (XL) xor XR.
6. The result of the operation above in Exchange for XL and XR XR be be XL.
7. Do 16 times, looping to do again the process of exchanging the XL and XR.
8. In the process of doing surgery for XR = XR xor P17 XL = XL xor and P18.

9. The last process reunite XL and XR so being 64 bit back
   The function F as in the formula:

   The subkeys are calculated using the Blowfish algorithm, its method is as follows:

Bagi XL menjadi empat bagian 8-bit: a, b, c, d.

$$F(x_L) = ((S_{1,a} + S_{2,b} \bmod 2^{32}) \oplus S_{3,c}) + S_{4,d} \bmod 2^{32}$$

1. First of allinilialisasi the P-array and then four S-box in a sequence with a fixed string. This string consists of digits of Pi hexadesimal.
2. XOR P1 with 32-bit first key, XOR P2 with 32-bit both of the keys and so on for every bit of the key (P18). Repeat until the entire bit key against the P-array in XOR with the bit key.
3. Enkrip all strings using the Blowfish algorithm with zero subkeys as described in step (1) and (2).
4. Replace P1 and P2 with the output of step (3).
5. Enkrip the output of step (3) with the Blowfish algorithm with the modified sub keys.
6. Replace P3 and P4 with the output of step (5).
7. Continue the process, replace entire elements of the P-array, then the whole of the fourth S-box sequence, with an altered output continuously from Blowfish algorithm.

a. QR Code

QR Code, is short for Quick Response Code is a two-dimensional image that has the ability to store a data, especially in the form of text. QR Code is the development of a barcode which was originally one of the dimensions into two dimensions. QR Code also has the ability to store data larger than the barcode [4].

QR Codes are usually small white square with the inside there is a black geometric shapes, although currently there is a QR Code and widely used as brand a product. The information can be encoded on a QR Code, among others, URL, phone number, SMS messages, V-cards as well as text [5]

2) Avalanche effect

Avalanche effect is a desired output of the encryption algorithm. The output is in the form chipertext. The result of the encryption is said to be good when the input 1 bit changes on the plaintext or keys to generate major changes in output. Avalanche effect is the usual test parameters used to describe the level of security on a symmetric key and cryptographic hash functions. This test is done to see the level of security of cryptographic algorithms [6].

Avalanche effect can be used as metriks to analyze the performance and security of a cryptographic encryption algorithm. Avalanche effect is calculated according the formula:

$$Avalanche\ Effect = \frac{\text{the number of bit changes}}{\text{the total number of bits chiperteks}} \text{x } 100\%$$

In general the bit in the ciphertext will experience a change of the number of bits in the plaintext of 50%. An avalanche effect is said to be good if the resulting bit changes ranged from 43-60%. The more bit changes that occur will lead to increasingly difficult the cryptographic algorithms to solve.

III. RANCANGAN SISTEM DAN APLIKASI

A. Research Methods

Research methodology to be used in this research is engineering, where researchers use a technique of cryptographic Blowfish and combined with QR Code. As for the plot description of this research process systematics poured in fig 1 as follows:

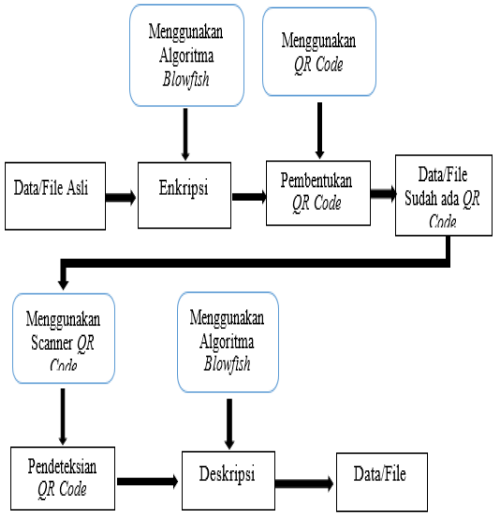

Fig. 3.1 Alur SistemPengamanan Data

B. Research Steps

Steps in research for realizing preliminary hypothesis with the techniques contained in the framework of thought

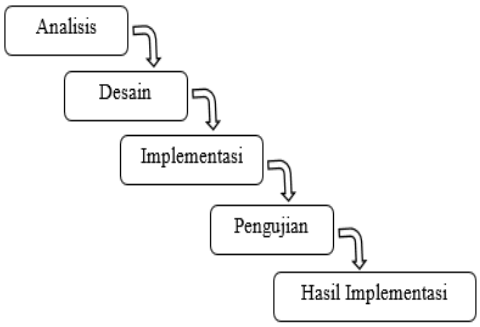

Fig. 2Langkah-langkahpenelitian

1) System Flow

The flow of the process used in this study are presented in Figure 4.1.

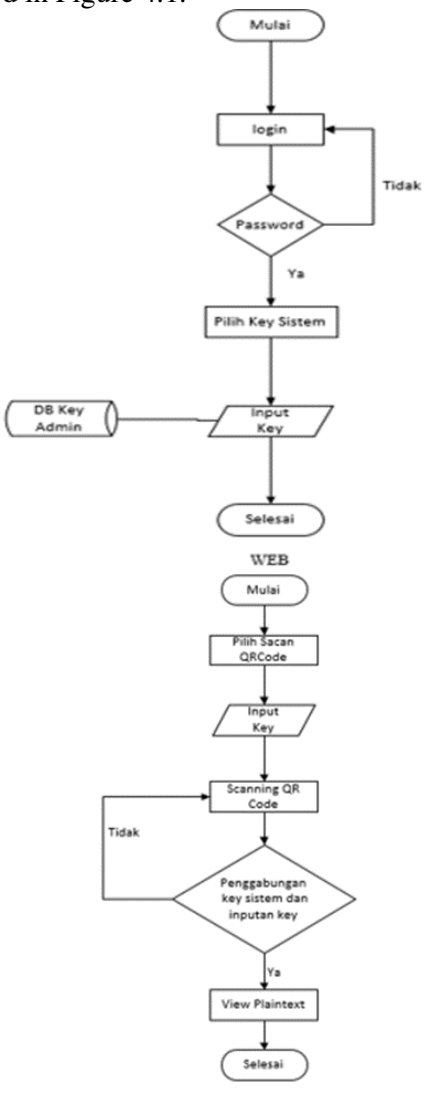

Fig. 3 Flow Reaserach

IV. RESULTS AND DISCUSSION

On this research implemented in two systems, the system's first web-based application used by admin to create the public key that will be disseminated to key supervisory examinations, while the second android-based system application used by the supervisor of tests of scan barcode. Following is the display of flow implementations:

A. Web Interface design application and android application

1. Web Application

the application of web-based application built using the java programming language.

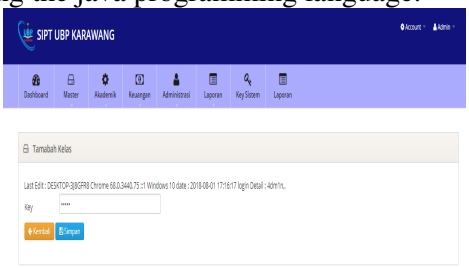

Fig. 4 Web Application

2. Android Application

Android-based applications are created using the java programming language and xml

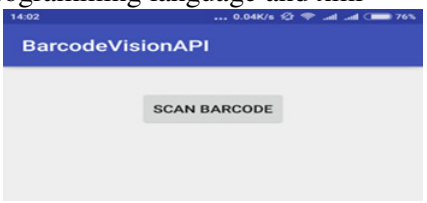

Fig. 5 Android *Application Design Home*

Fig. 6 the design of the input key

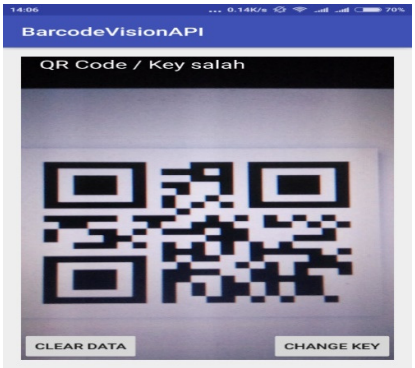

Fig. 7 design of scan QR Code

B. Testing

In the testing phase of this research uses two testing, testing the first testing the strength of the encryption process after ciphertext randomness using the Avalanche effect, while the second testing testing against the acceptance of the user using the User Acceptance Testing techniques.

1. Avalanche Effect

Pada test of randomness this ciphertext performed 20 times experiment with parameters varying sample that is based on the large file size, the length of the ciphertext characters and a different key.

TABLE I
TRIAL RESULTSQUESTIONNAIRE CALCULATION

No	Nama Data/File	Panjang *Plaintext* (bit)	Panjang *key*	Perubahan bit	*Avalanche Effect*
1.	Ujicoba 1	70	37	384	44.4
2.	Ujicoba 2	70	51	396	45.8
3.	Ujicoba 3	68	48	452	52.3
4.	Ujicoba 4	69	70	411	47.6
5.	Ujicoba 5	69	75	383	44.3
6.	Ujicoba 6	72	91	431	44.9
7.	Ujicoba 7	67	100	392	45.4
8.	Ujicoba 8	76	129	390	45.1
9.	Ujicoba 9	87	165	484	43.2
10.	Ujicoba 10	69	200	367	42.5
11.	Ujicoba 11	72	210	410	42.7
12.	Ujicoba 12	69	226	398	46.1
13.	Ujicoba 13	78	244	440	45.8
14.	Ujicoba 14	71	252	415	43.2
15.	Ujicoba 15	74	299	406	42.3
16.	Ujicoba 16	72	309	418	43.5
17..	Ujicoba 17	69	322	398	46.1
18.	Ujicoba 18	73	354	412	42.9
19.	Ujicoba 19	75	366	398	46.1
20.	Ujicoba 20	70	398	372	43.1
Nilai Rata-Rata Avalanche Effect					44,9%

2. User Acceptance Testing

In this study the delivry of as many as 19 questionnaire respondents, the questionnaire back as many as 19 questionnaires, so as there is no questionnaire that flawed or incomplete questionnaires so that all eligible to be processed. So the rate of return the questionnaires from respondents is 100% of the questionnaires have been returned all of his. Then return the questionnaire in its entirety in the amount of 100%.

1. Kuesionerr analysis results

After doing the calculation of questionnaires to the 19 people the respondents obtained the results of the questionnaire, as follows:

a. Analysis of the first question

From the above table it can be seen that the amount of the value of the 19 respondents to the first question is 66. The average value is 66/19 = 3.47. A percentage value is 3.47 x 100

b. Analysis of the second question

From the above table it can be seen that the amount of the value of the 19 respondents to the first question is 62. The average value was 62/19 = 3.26. A percentage value is 3.26 x 100 = 89.47%

c. analysis of the third question

From the above table it can be seen that the amount of the value of the 19 respondents to the first question is 68. The average value was 68/19 = 3.58. A percentage value is 3.58 x 100 = 86.84%

d. fourth question Analysis

From the above table it can be seen that the amount of the value of the 19 respondents to the first question is 62. The average value was 62/19 = 3.26. A percentage value is 3.26 x 100 = 81.58%

e. fifth question Analysis

From the above table it can be seen that the amount of the value of the 19 respondents to the first question is 75. The average value is 75/19 = 3.95. A percentage value is 3.95 x 100 = 98.68%

f. Analysis of the sixth question

From the above table it can be seen that the amount of the value of the 19 respondents to the first question is 59. The average value is 59/19 = 3.11. A percentage value is 3.11 x 100 = 77.63%

g. seventh question Analysis

From the above table it can be seen that the amount of the value of the 19 respondents to the

first question is 25. The average value is 25/19 = 1.32. A percentage value is 1.32 x 100 = 32.89%

h. Eighth question Analysis

From the above table it can be seen that the amount of the value of the 19 respondents to the first question is 56. The average value is 56/19 = 2.95. A percentage value is 2.95 x 100 = 73.68%

i. Analysis of the ninth question

From the above table it can be seen that the amount of the value of the 19 respondents to the first question is 24. The average value is 24/19 = 1.26. A percentage value is 1.26 x 100 = 31.58%

j. tenth question Analysis

From the above table it can be seen that the amount of the value of the 19 respondents to the first question is 61. The average value was 61/19 = 3.21. A percentage value is 3.21 x 100 = 80.26%

k. Eleventh question Analysis

From the above table it can be seen that the amount of the value of the 19 respondents to the first question is 51. The average value is 51/19 = 2.68. A percentage value is 2.68 x 100 = 67.11%

l. twelfth question Analysis

From the above table it can be seen that the amount of the value of the 19 respondents to the first question is 55. The average value was 55/19 = 2.89. A percentage value is 2.89 x 100 = 72.37%

m. Thirteenth question Analysis

From the above table it can be seen that the amount of the value of the 19 respondents to the first question is 32. The average value is 32/19 = 1.68. A percentage value is 1.68 x 100 = 42.11%

n. Fourteenth question Analysis

From the above table it can be seen that the amount of the value of the 19 respondents to the first question is 59. The average value is 59/19 = 3.11. A percentage value is 3.11 x 100 = 77.63%

o. Analysis of the fifteenth question.

From the above table it can be seen that the amount of the value of the 19 respondents to the first question is 61. The average value was 61/19 = 3.21. A percentage value is 3.21 x 100 = 80.26%

V. CONCLUSION

Based on the research that has been done, E-Document Security Engineering at the University of the world Struggle Karachi Using QR Code with Blowfish Encryption Method that has already been done, by adding an application is made are able to:

1. Secure the card test as evidenced by the presence of testing randomness encryption using the Avalanche Effect produces a value of 44.9%, which means it belongs to the category either. the results of the tests conducted already presented in table 4.6 above.
2. Make it easy for employees in the University World Struggle Karachi to certify attendance card test.

BIBLIOGRAPHY

[1] I. Riadi, "ANALISIS KEAMANAN INFORMASI BERDASARKAN KEBUTUHAN TEKNIKAL DAN OPERASIONAL MENGKOMBINASIKAN STANDAR ISO 27001 : 2005 DENGAN MATURITY LEVEL (Studi Kasus Kantor Biro Teknologi Informasi PT . XYZ)," *Semin. Nas. Teknol. Inf. Dan Multimed. 2016*, vol. 6, no. 6, pp. 6–7, 2016.

[2] L. K. Sofu Risqi Y.s, "Algoritma Digital Signature Solin Sebagai," 2016.

[3] O. K. Sulaiman, M. Ihwani, and S. F. Rizki, "Model Keamanan Informasi Berbasis Tanda Tangan Digital Dengan Data Encryption Standard (Des) Algorithm," *InfoTekJar (Jurnal Nas. Inform. dan Teknol. Jaringan)*, vol. 1, no. 1, pp. 14–19, 2016.

[4] M. P. Nugraha and R. Munir, "Pengembangan Aplikasi QR Code Generator dan QR Code Reader dari Data Berbentuk Image," *Konf. Nas. Inform. – KNIF 2011*, pp. 148–155, 2011.

[5] L. A. Muharom, "SMART PRESENSI MENGGUNAKAN QR- Code DENGAN ENKRIPSI VIGENERE CIPHER," *Univ. Muhammadiyah Jember*, vol. 13, no. 2, pp. 31–44, 2016.

[6] Nikita & Ranjeet Kaur, "a Survey on Secret Key Encryption Technique," *IMPACT Int. J. Res. Eng. Technol. (IMPACT IJRET)*, vol. 2, no. 5, pp. 7–14, 2014.