International Journal of New Technology and Research (IJNTR)
ISSN:2454-4116, Volume-3, Issue-8, August 2017 Pages 01-05

Encryption of Blob Field Content Using AES Algorithm on CBT (Computer Based Testing) System

Juli Rejito, Deni Setiana, Rudi Rosadi

***Abstract*— Implementation of information technology especially in CBT (Computer-Based Test) is starting to use. Confidentiality matter stored in the database becomes the main thing that must be considered because the questions used in the test should not publish both from test participants (clients) as well as from a database manager (administrator). In this paper will be presented one alternative security solutions matter stored in blob field database that contains the encoded image, so the original content that matter will only be read when using the actual application. Technical encryption used to take advantage of symmetric encryption that is raised in the application form entry question bank as tools incorporate a matter also functions for encryption of content matter, on the other hand, the used of applications CBT used by the user to work also functions as the decrypted content question. Proof of the encryption result is shown with direct access to blob field matter content stored in the database using database access interface.**

Index Terms—CBT (Computer Based Testing), blob field, encryption, decryption, database, question bank

I. INTRODUCTION

Test execution using paper or *paper based test* (PBT) in the traditional tests are now starting to switch to a system of the computer-based test *(CBT-Computer Based Testing)* either via the internet using a web interface, as well as *a desktop* interface utilizes the client-server technology. The test system using paper is considered to have many shortcomings, among others, the cost of duplication, prone to leakage and relatively less safe, require operational high-cost operational, require a long time for processing and others.

Computer-based testing has become prevalent and offers many advantages [1] [2]. For example, "computer-based tests can provide new, valid and reliable goals for traditional or new competencies" [3].

Also, the computer allows testing to be done anytime and anywhere [4] and can increase the motivation of the test participants [5]. Computer-based exams also provide financial benefits by requiring fewer resources both from human resources and less paper/paper used [6].

Implementation of the computer-based test in Indonesia in the past 5 years it began to be applied as in UNBK (National Exam Computer Based), on the level of upper secondary education, admission selection of civil servants (Panselnas) and CBT-SBMPTN *(Computer Based Testing* - Selection of Joint Entrance State High Country) all over Indonesia. Computer-based exams are applied using several interfaces that vary depending on the developer of the application by considering the advantages and disadvantages of each.

The most important thing in the implementation of the CBT-based test system is that the system must be real time, fast and secure. Security questions on the CBT exam system into a separate demand due to the number of limitations and anticipation required against the leakage that allows occurring when the system is used, both from the client side and database server.

To solve this problem, it is necessary safeguards created problems that would be guaranteed confidentiality about both sides of the application will access the matter and regarding the database manager *(administrator)*. One alternative that allows for the dimple-mounted and is by securing an issue of content stored in a *blob-field* on the database server using encryption matter.

Encryption is a standard technique for encoding data to secure data. Many encryption techniques that have been developed by previous investigators including *plane bit encryption*, fuzzy PN codes based encryption color image, standard DES and others with varying degrees of success for the anticipated break-ins and other features [7].

The security of digital data at this time has become an important part since data communications products are growing rapidly and more openly [8, 9]. The techniques described by some researchers are implemented in the form of applications provide data security functions so that data cannot be accessed and transferred on the network and the media that allows to open it.

The purpose of this study is to provide high security of digital data stored in the blob field server database and keep the data from the parties who will utilize it for the purpose that is not good in the implementation of the CBT exam. Another goal is to get the encryption algorithm and its security features and maintain data from the losses caused by the decryption process that is easy to use.

II. AES ENCRYPTION ALGORITHM

There are quite some encryption algorithms used to safeguard information in a variety of techniques that can safeguard data security, its complexity and its ability to withstand attacks and vary widely between algorithms with other algorithms. The main component of the encryption process is the content of the algorithm that will be used as the core purpose of encryption in different ways. Popular algorithms that are widely used include DES, Triple DES,

Juli Rejito, Department Computer Science, Padjadjaran University, Bandung, Indonesia
Deni Setiana, Department Computer Science, Padjadjaran University, Bandung, Indonesia
Rudi Rosadi, Department Computer Science, Padjadjaran University, Bandung, Indonesia

RC2, RC4, Blowfish, Twofish and Rijndael (AES). The basic information of the most popular encryption algorithms is shown in Table 1 [10].

Table 1. The Most Popular Encryption Algorithm

Algorithm	Key Size	Block Size	Rounds
DES	56-bits	64-bits	16
RC2	128-bits	64-bits	16 mix 2 mashing
RC4	Variable	Variable	Unknown
Blowfish	128-bits	64-bits	16
Towfish	(128, 192, 256) - bits	128-bits	16
3-DES	(112,168)- bits	64-bits	48
AES (Rijndael)	(128, 192, 256) - bits	128-bits	10, 12 or 14

The AES algorithm encrypts a 128-bit plaintext block (M), into a 128-bit ciphertext block (C), using a chip key (K key) that is between 128-bit, 192-bit or 256-bit. Differences in key lengths make up the key names AES-128, AES-192, and AES-256. The AES algorithm ran in a matter of bytes and based on the block size of the input, output and key represented in 32-bit words equals 4 bytes.

The AES algorithm encryption process consists of 4 types of bytes transformations, namely SubBytes, ShiftRows, Mixcolumns, and AddRoundKey. At the beginning of the encryption process, the input that has been copied into the state will undergo byte transformation AddRoundKey. After that, the state will undergo SubBytes, ShiftRows, MixColumns, and AddRoundKey repeatedly transforms as much as Nr. This process in the AES algorithm is called a round function.

The last round is somewhat different from the previous rounds where in the last round, the state did not undergo the MixColumns transformation. Illustration of AES encryption process can be described as in Figure 1 below:

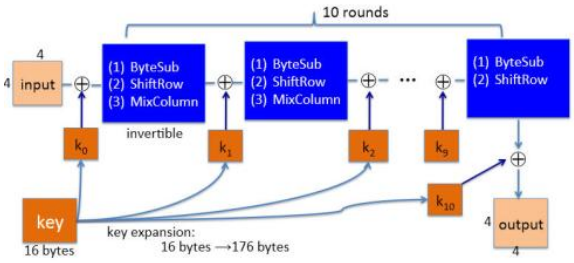


Figure 1. AES Algorithm

The AES algorithm encryption process consists of 4 types of bytes transformations, namely SubBytes, ShiftRows, Mixcolumns, and AddRoundKey. At the beginning of the encryption process, the input that has been copied into the state will undergo byte transformation AddRoundKey. After that, the state will experience SubBytes, ShiftRows, MixColumns, and AddRound Key repeatedly transforms as much as Nr. This process in the AES algorithm is called a round function. The last round is somewhat different from the previous rounds where in the last round, the state did not undergo the MixColumns transformation.

The steps of the AES-128 encryption algorithm can be written as follows:

1. Addroundkey
2. Nr -1 times as many rounds, a process carried out in each round is SubBytes, ShiftRows, MixColumns, and AddRoundKey.
3. The final round is the process for the last round that includes SubBytes, ShiftRows, and AddRoundKey.

Pseudecode encryption algorithm AES, written as follows:

```
Encrypt(byte in[4*Nb], byte out[4*Nb],
word_w[Nb*(Nr+1)]
begin
    byte state[4,Nb];
    state = in;
    AddRoundKey(state, w[0,Nb-1]);
    for i = 1 to Nr-1 stepsize 1 do
        SubBytes(state);
        ShiftRows(state);
        MixColumns(state);
        AddRoundKey(state,w[round*Nb,(round+1)*Nb-1]);
    end for
    SubBytes(state);
    ShiftRows(state);
    AddRoundKey(state,w[round*Nb,(round+1)*Nb-1]);
    Out = state;
end
```

The cipher transform can be reversed and implemented in the opposite direction to produce an easy-to-understand inverse cipher for the AES algorithm. AES-128 decryption process can be written as follows:

1. Addroundkey
2. Nr -1 times as many rounds, and in each round do process: InveShiftRows, Inv SubBytes, AddRoundKey and InvMi xColumns
3. The final round is the process for the last round that includes InvShiftRows, InvSub Bytes, and AddRoundKey.

Pseudocode decryption algorithm AES, written as follows:

```
Decrypt(byte in[4*Nb], byte out[4*Nb],
word_w[Nb*(Nr+1)]
begin
    byte state[4,Nb];
    state = in;
    AddRoundKey(state, w[Nr*Nb,(Nr+1)*Nb-1]);
    for i = Nr-1 to 1 stepsize -1 do
        InvShiftRows(state);
        InvSubBytes(state);
        AddRoundKey(state,
        w[round*Nb,(round+1)*Nb-1]);
        InvMixColumns(state);
    end for
    InvShiftRows(state);
    InvSubBytes(state);
    AddRoundKey(state, w[0,Nb-1]);
    Out = state
```

end

III. IMAGE QUALITY MEASUREMENT

Measurements with this model are widely used because of the ease of calculation, have a physical understanding and mathematically easy to use for optimization purposes, although not very useful in matching visual quality. This measurement consists of several formulas that MAE (Maximum Absolute Error), MSE (Mean Square Error), RMSE (Root Mean Square Error), SNR (Signal to Noise Ratio), and PSNR (Peak Signal to Noise Ratio) [11].

A. *Maximum Absolute Error* (*MAE*)

MAE is the highest value of the absolute value difference between the input image $f(x,y)$ and the output image $g(x,y)$. *MAE* calculation is mathematically written in equation form:

$$MAE = max|f(x,y) - g(x,y)| \quad (1)$$

where $f(x,y)$ is the value of the initial / original image intensity in the position *(x, y)* and $g(x,y)$ is the value of the image's intensity in the position (x, y).

B. *Mean Square Error* (*MSE*)

MSE is the average value of squared error between the input image $f(x,y)$ to the output image $g(x,y)$, where both of the images have the same values. Good MSE values are where the value near zero ($MSE \approx 0$) [6]. Mathematically *MSE* value calculation using the equation

$$MSE = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}[f(x,y) - g(x,y)]^2 \quad (2)$$

where M,N are the width and height of the image, $f(x,y)$ is the initial image intensity use values/position (x, y) and $g(x,y)$ native to the image of the intensity value at the position (x, y).

C. *Peak Signal to Noise Ratio* (*PSNR*)

PSNR is a value of the ratio between the maximum image reconstruction results with square root value of *MSE* or equal to the value of *RMSE* [6]. For 8-bit image pixel, the maximum value is 255. The criteria of image quality will be better if the result of the greater *PSNR* values and mathematically generated from *MSE* value shown in the equation:

$$PSNR = 10\ log_{10}\left[\frac{255^2}{MSE}\right]\ dB \quad (3)$$

IV. RESEARCH OBJECT AND IMPLEMENTATION

Objects used in this study is the CBT system on the selection test of prospective students all public universities in Indonesia with the number of universities as much as 73 university followed by 20,860 participants. The built-in architecture based on a secure remote access model consists of three parts: the access authority of the database, the master-slave database and the encryption of the database content decryption. The encrypted database content residing on the central server is redirected to the local database located at the maximum test 1 hour before the execution of the test. The network architecture is depicted in Figure 2.

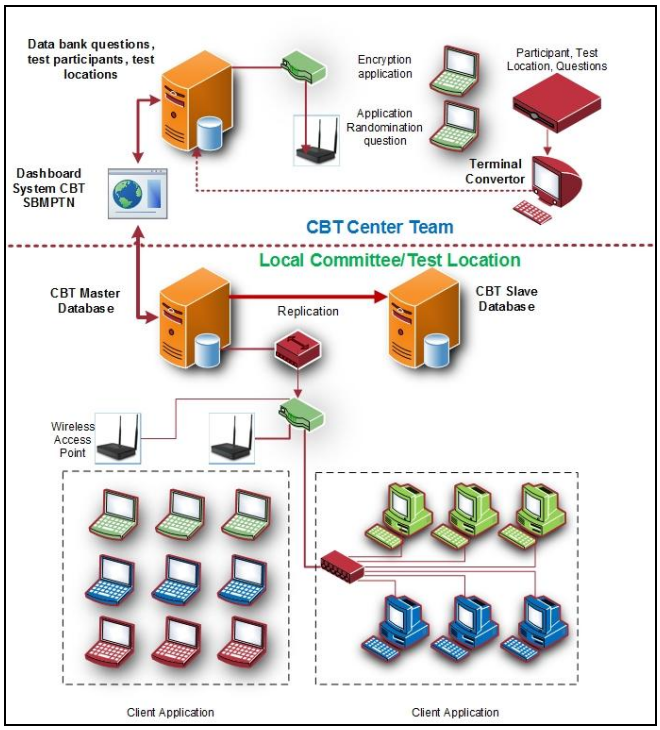


Figure 2. Network Architecture

From the figure can also be explained that there is two execution team of test that is CBT team center and the local committee which is one unit of the team for executor team of the test.

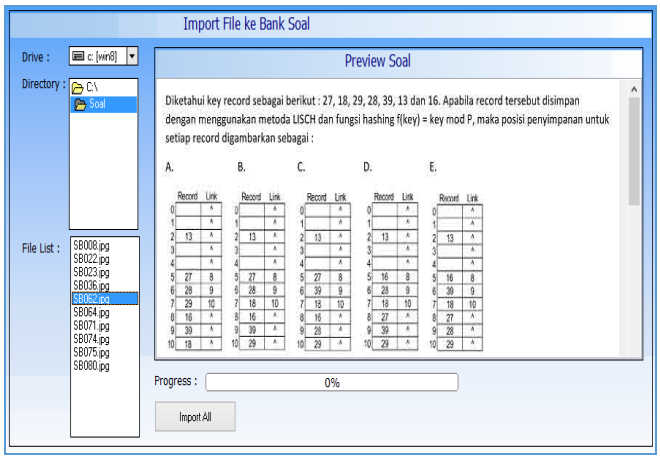


Figure 3. Server Application Interface

The implementation of the CBT exam is held together at the same time for all examinees. Exam participants using client applications that will access the local database as well as in the application there is the process of decrypting the exam questions. The results of the next test sent back to the central server and then performed data processing to get the best ranking of each course of each college. The interface built in this research is applied in two side that is server side and client side. The application that is applied on the server side is enabled to enter data problem into the database blob field, as well as functioning as an encryption process of the

data file about the prepared in the form of JPG image file. The encryption of the file in the form of binary file is then entered into a database record of the question bank using SQL insert query. The display interface is shown in Figure 3.

. For exam questions by participants using the CBT exam application which at once functioned as a decryption process of binary files stored in the database following pointer problem to be done by the participants. Data record retrievers use SQL select query operations and are displayed in the form of interfaces as shown in Figure 4.

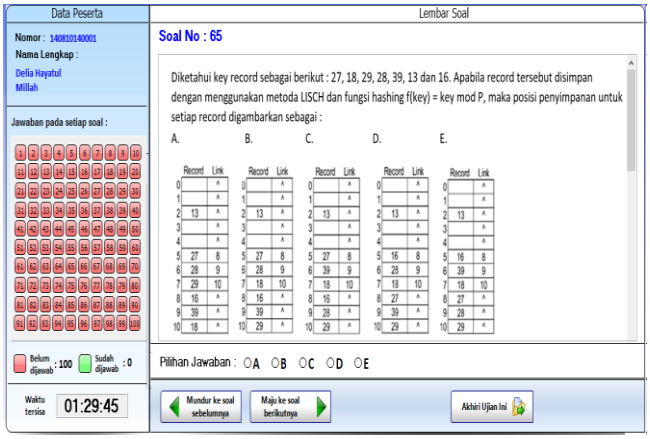


Figure 4. Client Application Interface

Figure 4 shows one part of the server application interface used for the test encryption process that will directly store the encrypted results into the database server's database blob.

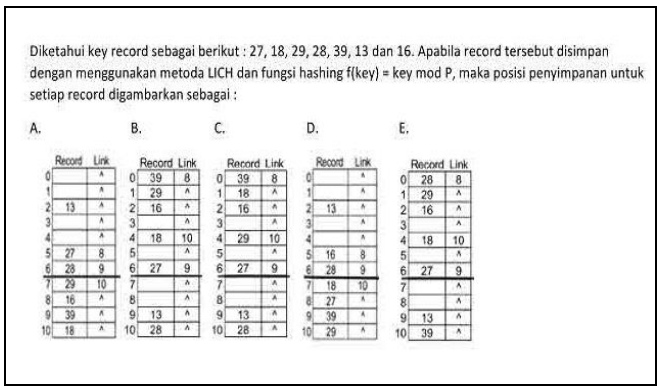
The object of research utilized in the form of a test file in the form of JPG file containing a combination of text and image consists of 100 pieces of JPG files with 10 sample data from this research object shown in table 2.

Table 2. Research Objects

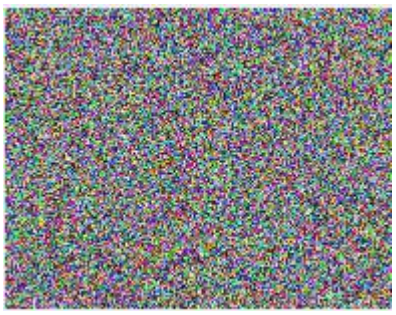
No	Filename	Content	Byte	Pixels
1	SB008.jpg	Text & equations	35.977	816x1056
2	SB022.jpg	Text & code program	39.637	816x1056
3	SB023.jpg	Text & equations	32.538	816x1056
4	SB036.jpg	Text & code program	33.521	816x1056
5	SB062.jpg	Text & images	41.633	816x1056
6	SB064.jpg	Text & images	41.221	816x1056
7	SB071.jpg	Text & images	38.281	816x1056
8	SB074.jpg	Text & images	34.339	816x1056
9	SB075.jpg	Text & images	34.388	816x1056
10	SB080.jpg	Text & diagram	38.105	816x1056

V. TEST RESULT AND DISCUSSION

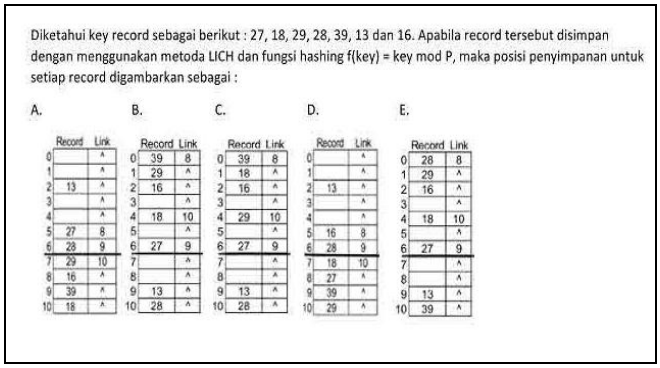
The process of encrypting the test file will generate a binary image (file encryption) that will be inserted into the blob field database. At the time the examinees do the test, the binary file is decrypted back into the image of the problem that appears on the client application interface. Figure 5 shows the original file, the encrypted file in the form of binary files and decryption files.



(a) Original File



(b) File encryption (binary)



(c) File decryption

Figure 5 Sample questions, encryption, and decryption

Table 3. File size, encryption, and decryption

No	Filename	File size		
		Original	Encryption	Decryption
1	SB008.jpg	35.977	35.992	34.489
2	SB022.jpg	39.637	41.117	41.117
3	SB023.jpg	32.538	32.552	32.538
4	SB036.jpg	33.521	33.544	30.631
5	SB062.jpg	41.633	41.656	45.353
6	SB064.jpg	41.221	41.240	45.171
7	SB071.jpg	38.281	38.296	38.534
8	SB074.jpg	34.339	34.360	32.247
9	SB075.jpg	34.388	34.408	32.361
10	SB080.jpg	38.105	38.120	38.293

The results of the test file size resulting from the encryption process and decryption of the CBT exam for the above 10 sample files are shown in table 3.

Table 4. Values of MAE, MSE, PSNR and Equality

No	Filename	MAE	MSE	PSNR	Equality
1	SB008.jpg	0.1711	1.4532	46.5076	99.93%
2	SB022.jpg	0.2354	1.9357	45.2525	99.91%
3	SB023.jpg	0.0000	0.0000	0.0000	100.00%
4	SB036.jpg	0.1374	1.1204	47.6370	99.95%
5	SB062.jpg	0.2450	1.6613	45.9264	99.90%
6	SB064.jpg	0.2371	1.5587	46.2033	99.91%
7	SB071.jpg	0.2032	1.6104	46.0615	99.92%
8	SB074.jpg	0.1374	0.9262	48.2740	99.95%
9	SB075.jpg	0.1377	0.9258	48.2757	99.95%
10	SB080.jpg	0.2001	1.6780	45.8830	99.92%
Average		0.1704	1.2870	42.0021	99.93%

The comparative values between the encrypted files and the decrypted results are shown in Table 4 with an average value of MAE = 0.1704, MSE = 1.2870, and PSNR = 42.0021, and an average of 99.93%. In other words, the results show that the original test subjects encrypted by the encryption process are stored in the BLOB-field database, and the decrypted file that appears in the client application has 99.93% similarity.

VI. CONCLUSION

The results of this study indicate that the origin files stored as JPG files during the encryption process in the server application position, the binary files stored in the database blob-field, as well as the decrypted files retrieved from the database have almost 100% similarity, or the origin file and Result file no significant change.

REFERENCES

[1] Clariana, R. and Wallace, P.. Paper-based versus computer-based assessment: key factors associated with the test mode effect. British Journal of Education Technology, 33(5), 593-602. 2002.
[2] Schatz, P., & Putz, B. O.. Cross-validation of measures used for computer-based assessment of concussion. Applied Neuropsychology, 13(3), 151-159. 2006.
[3] Wirth, J. Computer-based tests: alternatives for test and item design. In J. Hartig, E Klieme, & D. Leutner (Eds.), Assessment of competencies in educational contexts (pp.235–252). Göttingen: Hogrefe. 2008.
[4] Jeong, H.. A comparative study of scores on computer-based tests and paper-based tests. Behaviour & Information Technology, 33(4), 410-422. 2014.
[5] Chua, Y. P., & Don, Z. M. Effects of computer-based educational achievement test on test performance and test takers' motivation. Computers in Human Behavior, 29(5), 1889-1895. 2013.
[6] Kaya, F. & Delen, E.. A computer-based peer nomination form to identify gifted and talented students. The Australasian Journal of Gifted Education. 23(2), 29-36. 2014.
[7] Ismet Ozturk, Ibrahim Sogukpinar, "Analysis and Comparison of Image Encryption Algorithms" World Academy of Science, Engineering and Technology 3,PP.26-30, 2005.
[8] Al-Ataby A. and Al-Naima F., "A Modified High Capacity Image Steganography Technique Based on Wavelet Transform", The International Arab Journal of Information Technology, vol. 7, no. 4, pp. 358-364, 2010.
[9] Sara Tedmori, Nijad Al-Najdawi " Lossless Image Cryptography Algorithm Based on Discrete Cosine Transform", IAJIT First Online Publication vol.3, 2011.
[10] A. Lee, NIST Special Publication 800-21, Guideline for Implementing Cryptography in the Federal Government, National Institute of Standards and Technology, November 1999.
[11] Ahmet M. Eskicioglu, Paul S. Fisher, "Image Quality Measures and Their Performance" IEEE Transactions on Communication, Vol. 43, No. 12, December 1995