

Diffie-Hellman Algorithm for Securing Medical Record Data Encryption keys

1st Ermatita

Computer Science Faculty
Sriwijaya University
Palembang, Indonesia
ermatita@unsri.ac.id

2nd Yugo Bayu Prastyo

Computer Science Faculty
Universitas Pembangunan Nasional
Veteran Jakarta
Jakarta, Indonesia
yugobprastyo@gmail.com

3rd I Wayan Widi Pradnyana

Computer Science Faculty
Universitas Pembangunan Nasional
Veteran Jakarta
Jakarta, Indonesia
wayan.widi@upnvj.ac.id

4rd Muhammad Adrezo

Computer Science Faculty
Universitas Pembangunan Nasional
Veteran Jakarta
Jakarta, Indonesia
muhammad.adrezo@upnvj.ac.id

Data security is an issue that must be a concern in the current era of information technology. Medical data in the form of medical digital images is also important data to protect its security. This is to avoid being used by irresponsible parties. This data security can apply data encryption. The application of this encryption is by developing a medical digital image security that uses a combination of the advanced encryption standard (AES) algorithm in the data encryption process and the Diffie-Hellman algorithm in the key exchange process to maintain the security and confidentiality of medical images. The AES algorithm is used in the encryption and decryption process, while the Diffie-Hellman algorithm is used to secure the key of the AES algorithm. The results of this research showed that the combination of AES and Diffie-Hellman algorithms succeeded in securing medical images. Diffie-Hellman algorithm will generate different keys which are then used as AES keys. In this research, the Diffie-Hellman algorithm will produce a key which will be combined with the encryption key from the AES algorithm. In addition, the Diffie-Hellman algorithm is used for security in the exchange process and key generation.

Keywords—*Cryptography, Medical Image, Advanced Encryption Standard (AES) Algorithm, Diffie-Hellman Algorithm, Encryption, Decryption*

I. INTRODUCTION

The development of information technology is increasingly advanced. This progress has also had an impact on data security. Data security needs to be a concern, especially on access to information. This affects data security and integrity. Medical data is sensitive personal data. This is explained in Law Number 29 Year 2004 Article 46 paragraph 1 [2], the file containing documents and records related to the patient's identity, examination, action, service and treatment applied to the patient is a medical record. (Indonesia, Undang-Undang, 2004). Whereas in the Indonesian Medical Council Medical Record Manual, it is further explained that the documents included in the medical record are X-rays and other laboratory results. (Konsil Kedokteran Indonesia 2006, p.3). MRI (Magnetic Resonance Imaging) images are laboratory results that detect the patient's body condition in more detail. Security of the data contained in the MRI image so that the data is not publicly known and then used by unauthorized parties, it takes a measure to protect the image. Image security that can be done on medical images is by using cryptographic

techniques. The type of cryptographic security that can be used is the symmetric type algorithm with AES. However, there is a weakness in the symmetrical type algorithm, namely that the keys used in the encryption and decryption processes are the same key. Therefore it is necessary to secure the key of the AES algorithm. One of the AES algorithms that can be used to secure keys is the Diffie-Hellman algorithm. This algorithm is often used as a security in the key exchange process. Diffie-Hellman algorithm is a data security solution that can be used in cryptography. Several researchers have done data security using the Diffie-Hellman Algorithm: Parth Sehgal, et Al, 2013 used a random parameter to make algorithm more efficient. They used this method for random parameter generates new shared keys for each message that is exchanged between sender and receiver [3]. Another research conducted by Aryan et al. They are extending the Diffie - Hellman algorithm by using the concept of the Diffie - Hellman algorithm to get a stronger secret key and that secret key is further exchanged between the sender and the receiver so that for each message, a new secret shared key would be generated [4]. Aditi Bhattacharjee et all research about the combined cryptography algorithm is proposed for message exchanging using a secret shared key, which will be used in RSA algorithm to modify the value of N to avoid the mathematical attack[5]. Ahmad Abusukhon et, all, they are a modified TTIE algorithm called the Diffie Hellman Text-to-Image Encryption algorithm (DHT) [6]. This research uses the Diffie-Hellman Algorithm to generate a key which will be combined with the encryption key from the AES algorithm. In addition, the Diffie-Hellman algorithm is used for security in the key exchange and generation process.

II. RESEARCH METHODOLOGY

In the preparation of this research, data and information are needed that can be used as support in proving the material and discussion. Following figure shows stages and methods that are carried out in the research.

A. Problem Definition

The author observes the problems that exist in the field of data security, especially regarding the security of medical digital images. Based on the author's observations, problems related to medical data were found, including:

1. High level of vulnerability to medical digital image theft.
2. There is no security against digital medical images sent to patients.

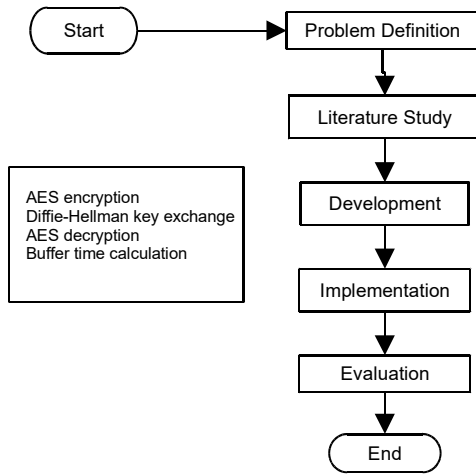


Fig. 1. Research Methodology

3. The high level of vulnerability to leakage of medical digital images in the process of sending data between the hospital and the patient.

Based on the above problems, the authors conducted research to secure medical digital images with a combination of the AES algorithm and the Diffie-Hellman key exchange method. This combination of algorithms was chosen to solve data security problems and minimize data leakage during the information transfer process.

B. Literature Study

Current studies has develop references being used by this research. Muhammad Zunaidi and Suharsil [8] aims to solve the security problem in the insertion of secret messages through digital images. By using the steganography technique, secret messages will be inserted into the image using the LSB method. The first thing to do is encrypt the message using the AES algorithm. In this case the secret message is "MuhammadAjiPraye", then encrypted with the key "A5r1S4m5UARrT111". Once encrypted, the plaintext will be 16 bytes or 128 bits ciphertext. The next step is to insert the ciphertext into a "contrast.bmp" image measuring 640x246 pixels using the LSB method. The results of this study found that messages encrypted using the AES algorithm were random and difficult to crack. In addition, the encrypted message can still be decrypted according to the encryption key so that the resulting message remains intact.

Metrilitna Br Sembiring [9] aims to analyze the security of the encryption and decryption results using elliptic curve cryptography in the key exchange process using the Diffie-Hellman algorithm. This elliptic curve cryptography uses two keys, namely the public key and the private key. The public key is generated by multiplying the private key with a generator point "G" in an elliptic curve. These points are then used in the key exchange process in the Diffie-Hellman algorithm. The results of this study found that eleptic curve cryptography provides a higher level of security because in the encryption process, the plaintext will be transformed into points in an elliptic curve before encryption. Then, the encryption process is carried out using the addition rule on the

elliptic curve. This level of security is also strengthened by the results of the application of the Diffie-Hellman algorithm, the algorithm will assign a third point (shared private key) to both users in the key exchange process.

Bin Pan, Yu Tian, Tian-shu Zhou, Feng Wang, and Jingsong Li [1] aims to analyze the ability of three encryption methods with the AES, RSA, and RSA-MurmurHash3 algorithms. In this study, the researcher wants to analyze each method by providing an object in the form of a medical image that must be encrypted. From the eight images given, the result is AES to be the algorithm with the best encryption speed. In addition, AES is able to reduce the image size without destroying the image quality. However, AES has a weakness which is the key. The AES encryption key is the same key for decryption, so if a key leak occurs, data confidentiality and security cannot be maintained.

Santosh Kumar B. J., Roshni Raj V. K., and Anjali Nair [10] aims to analyze the process of securing medical image data using cryptographic techniques using the RSA and AES algorithms. The two algorithms will be compared to get an assessment of which algorithm is better, seen from the time needed in the encryption and decryption process. Both of these algorithms will be given the same image data and then will be encrypted using each of these algorithms. The results of this study indicate that the time required for the RSA algorithm to encrypt data is longer than the AES algorithm. In the decryption process, the RSA algorithm also takes longer than the AES algorithm. In addition, the time and performance generated by the AES algorithm are more stable than the RSA algorithm. From these results, it can be concluded that the AES algorithm is better than the RSA algorithm in terms of speed and stability of the data encryption and decryption process.

C. Development

The security application that will be developed in this research is to combine the AES algorithm with the Diffie-Hellman key exchange method. This method aims to secure medical digital images using the AES algorithm and secure the key using the Diffie-Hellman key exchange method. The medical digital image that will be used in this study is a digital image from the MRI results in .jpg or .jpeg format. This data will be secured with the AES algorithm and the Diffie-Hellman key exchange method for later evaluation and assessment of the required encryption-decryption time and

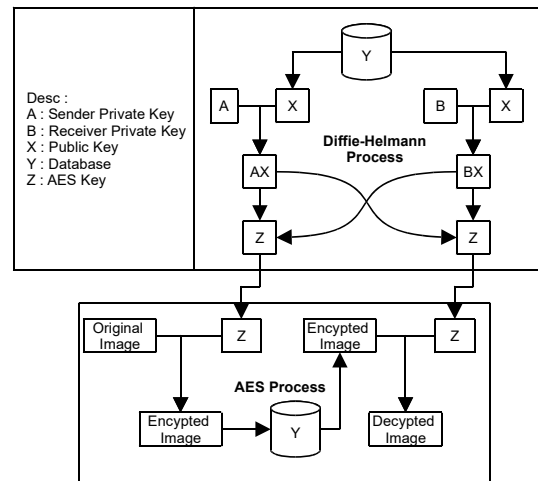


Fig. 2. Development algorithm



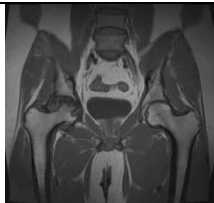
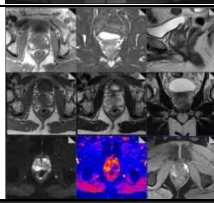
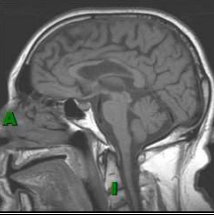
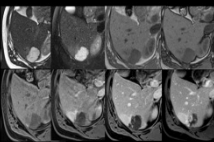
vulnerability to leakage of key data. The sender will first exchange the key with the Diffie - Hellman method. The process will generate a decryption encryption key for the AES algorithm. The encrypted image using AES is then sent to the database. The recipient will perform the decryption process using the key generated from the Diffie-Hellman method.




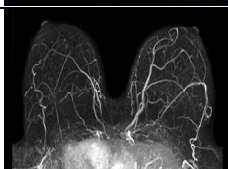
D. Implementation and Testing

The medical digital image that will be used in this study is a digital image from the MRI results in .jpg or .jpeg format. This data will be secured with the AES algorithm and the Diffie-Hellman key exchange method for evaluation and assessment of the required encryption-decryption time and vulnerability to leakage of key data. The sender will first exchange the key using the Diffie - Hellman method. The process will generate a decryption encryption key.

The samples taken were 10 samples of MRI images containing different information. The information contained in the object from the sample MRI image can be seen in **Error! Reference source not found.**

TABLE I. MEDICAL IMAGE SAMPLE

No.	Image	Object Description	Image Size
1.		MRI image of the heart	675 x 510
2.		MRI image of the knee	512 x 512
3.		MRI image of Pelvic Abdomen	638 x 680
4.		MRI image of the prostate	727 x 725
5.		MRI image of the brain	256 x 256
6.		MRI Image of liver tumours	499 x 297

No.	Image	Object Description	Image Size
7.		MRI image of the spine	308 x 500
8.		MRI Image of Adrenal Gland Disorders	530 x 336
9.		MRI image of the ankle	500 x 498
10.		MRI image of the breast	482 x 229

The image samples in table 1 will be used for research on the combination of AES and Diffie-Hellman algorithms.

E. Encryption and Decryption Key Generation Process

The encryption key generation process begins by applying the Diffie-Hellman algorithm. This process is in the form of an exchange of two agreed-upon public key values between the sender and receiver. In this system, the public key is not inputted manually, but has been generated by the system as the address code of the user. In addition, the sender and receiver each hold a private key which is not shared with others. Furthermore, these public keys will be exchanged and then entered into the Diffie-Hellman formula. This process will generate a new key with the same value between the sender and receiver without having to exchange information about the value of the key. Then after getting the key value from the Diffie-Hellman algorithm, the key will be used to generate the final key for the AES algorithm. The generation of the final key involves three value variables, namely the sender's public key, the receiver's public key, and the key from the Diffie-Hellman algorithm. The combination formula used in the formation of the AES-128 encryption key is as follows:

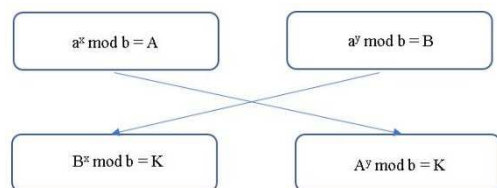


Fig. 3. Diffie-Hellman formula process description

$$E_{AES} = \alpha(5) + K(6) + \beta(5)$$

XAES = AES Encryption Key
 a = Sender User Address Code
 b = Recipient User Address Code
 K = Diffie-Hellman Combination Codes

In the formula above, there is a "K" value generated from the Diffie-Hellman algorithm process. This value is obtained by discussing the formula as shown in Figure 3 dan Table 2.

a = Sender User Address Code
 b = Recipient User Address Code
 K = Diffie-Hellman Combination Codes
 x = Sender's Private Key Value
 y = Recipient's Private Key Value

Following table shows example of code and key being used for simulation.

TABLE II. VARIABLE VALUE INFORMATION

No	Information	Value
1.	Sender User Address Code	123456
2.	Recipient User Address Code	654321
3.	Sender's Private Key Value	112123
4.	Recipient's Private Key Value	334322

Based on the processes and values in table above, the system automatically generates the user's address code when registering for the first time. This code is then used as the public key for the Diffie-Hellman process. When the image is to be sent, the system will first perform two calculation processes, namely "ax mod b = A" and "Ay mod b = K", the process of calculating these values is as shown in Figure 4.

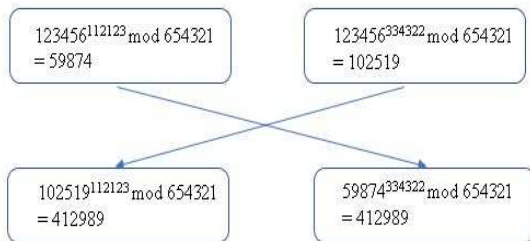


Fig. 4. Diffie-Hellman Key Value Exchange Process

The key generated from the Diffie-Hellman algorithm is 412989, this key is then entered into the variable "K". The next step is to take the first 5 characters from the values "a" and "b" to be used in the generator variable "XAES". The value of "K" which was obtained earlier is "412989" converted into hexadecimal form. The conversion results will also be used in the final key generation process "XAES". Taking the values of "a" and "b" as many as 5 characters aims to maintain key security when user data leaks occur in the database. If the user data contained in the database is leaked, the AES key is not immediately known because the value used in this algorithm is not the original value of the variables "a" and "b" but a cut from the values "a" and "b". Meanwhile, the process of changing the key generated from the Diffie-Hellman algorithm which is initially a number into hexadecimal characters and then formed into a new variable with a length of 6 characters aims to complicate message security attacks with the

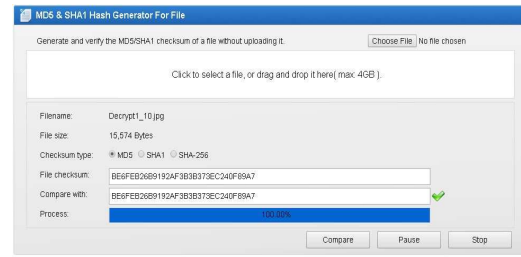


Fig. 5. Checksum comparison

bruteforce method. With the combination of numbers and letters, there are more possibilities for character arrangement to form a key with a length of 16 characters. The value change process in the final key generation process can be seen in table 3.

TABLE III. VALUE CHANGES IN THE AES KEY GENERATION PROCESS

Variable	Initial Score	Hexadecimal Convert	New Variable Memory	End Score
Sender address code (a)	123456	Not performed	5 char	12345
Receiver address code (b)	654321	Not performed	5 char	65432
Diffie-Hellman Key (k)	412989	64D3D	6 char	64D3D6
AES Final Key	Not Yet generated	Not performed	15 char	1234564D3D665432

In table 3, the values a and b are not converted into hexadecimal numbers, only the K values are converted. In filling the memory of the new variable K in the combination process, there is a rule that the number of characters must be 6. The rules in the combination process are shown in the following line of code:

```
int hkdhex;
String hkdhex1 = hkdhex;
String sub_hkd = null;
String kdf = null;
String hkdhex = Integer.toHexString(kd);
if (kdhex.length() > 6)
    (String sub_kdhex = kdhex.substring(0, 6);
    kdhex = new sub_kdhex.getText());
else if (kdhex.length() < 6)
    (String sub_hkd =
    String.join(hkdhex, hkdhex, hkdhex1, hkdhex1, hkdhex);
    String dhf = sub_hkd.substring(0, 6);
else (kdhex.length() = 6)
    (String kdf = kdhex.getText());
```

The results of the rules obtained will produce a combination of 5 characters from the sender's address code, namely the variable "a", plus 6 characters from the result of the Diffie-Hellman key that has been processed, namely the variable "K", then added with 5 characters from the code. recipient address is variable "b". The process will produce a final key totaling 16 characters, namely "1234564D3D665432". Furthermore, this key will be used in the image encryption and decryption process.

III. RESULTS AND DISCUSSION

Quality of compression method is performed in some steps, including: filesize comparison, histogram analysis, checksum comparison.

When viewed from following table, images with different encryption key values change in size with the same value. This shows that the characters used as keys in the encryption

process do not affect the size of the encrypted image file as long as the length of the key characters used is the same.

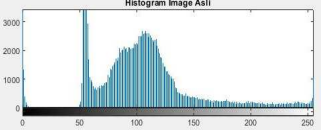
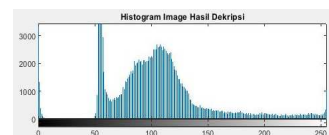
TABLE IV. FILESIZE COMPARISON

No.	Name	Key	Org Size (Bytes)	Enc'd Size	Dec'd Size	Diff (%)
1	Img 1	1234564D3D665432	33,579	33,584	33,579	0,015
2	Img 1	23096E1CBE155168	33,579	33,584	33,579	0,015
3	Img 2	1234564D3D665432	62,236	62,240	62,236	0,006
4	Img 2	23096E1CBE155168	62,236	62,240	62,236	0,006
5	Img 3	1234564D3D665432	52,268	52,272	52,268	0,008
6	Img 3	23096E1CBE155168	52,268	52,272	52,268	0,008
7	Img 4	1234564D3D665432	87,854	87,856	87,854	0,002
8	Img 4	23096E1CBE155168	87,854	87,856	87,854	0,002
9	Img 5	1234564D3D665432	18,230	18,240	18,230	0,055
10	Img 5	23096E1CBE155168	18,230	18,240	18,230	0,055
11	Img 6	1234564D3D665432	82,402	82,416	82,402	0,017
12	Img 6	23096E1CBE155168	82,402	82,416	82,402	0,017
13	Img 7	1234564D3D665432	44,096	44,112	44,096	0,036
14	Img 7	23096E1CBE155168	44,096	44,112	44,096	0,036
15	Img 8	1234564D3D665432	18,750	18,752	18,750	0,011
16	Img 8	23096E1CBE155168	18,750	18,752	18,750	0,011
17	Img 9	1234564D3D665432	162,411	162,416	162,411	0,003
18	Img 9	23096E1CBE155168	162,411	162,416	162,411	0,003
19	Img 10	1234564D3D665432	15,574	15,584	15,574	0,064
20	Img 10	23096E1CBE155168	15,574	15,584	15,574	0,064
Avg of size diff.						0,022

The results of the histogram test show that there is no difference between the initial image histogram and the decrypted image histogram, this indicates that the decryption process was successfully carried out without damaging the quality of the image. The histogram shows the frequency of the pixel intensity value on a scale of 0 - 255. The same histogram between the initial image and the decrypted image shows that in the decryption process, the encrypted image that previously experienced changes in its pixel value can be returned to its original pixel value. such as the initial image pixel value.

This proves that the data integrity of the image can be maintained by using a combination of AES and Diffie-Hellman algorithms. This is because in the decryption image there is no damage or change in value when compared to the initial image.

TABLE V. HISTOGRAM ANALYSIS

Image Histogram	Image Size	Notes
 <p>Fig. 6. Original Image</p>	256 x 256 px 96 x 96 dpi 18KB	There is no change between the original image and the decrypted image. The decryption process does not destroy the authenticity of the image.
 <p>Fig. 7. Decrypted Image</p>	256 x 256 px 96 x 96 dpi 18KB	

In this section, the checksum value of the initial image is tested, the encrypted image uses key 1, the encrypted image uses key 2, the decrypted image uses key 1, and the decrypted

image uses key 2. This test aims to check whether the each image has a difference caused by the encryption and decryption process. If there is a change, the checksum value of each image will also be different. This test is done by uploading the image file to a checksum checking website.

Following result are sample of checksum comparison of some images (1 & 2) having processed for each stages (encrypt with key 1 & 1, decrypt with key 1 & 2).

TABLE VI. CHECKSUM COMPARISON RESULT

Img	Stage	Checksum Val	Different/Similar
1	Orig	12373C285B9C60E00A2CF0BE84CAE11C	-
	Enc.Key1	0F9885C3CD228E89645C4AB50653B248	Dif
	Enc.Key2	7FB02B800C9B637A23DF4F82EF092DF5	Dif
	Dec.Key1	12373C285B9C60E00A2CF0BE84CAE11C	Sim
2	Dec.Key2	12373C285B9C60E00A2CF0BE84CAE11C	Sim
	Orig	C9BF87C934C667B5FBF1DD1B70CECBC9	-
	Enc.Key1	8B6AD5F096B9FD5083DAD37F296C3E01	Dif
	Enc.Key2	FE2C386C7B12EA52B34EBE091293F3DD	Dif
2	Dec.Key1	C9BF87C934C667B5FBF1DD1B70CECBC9	Sim
	Dec.Key2	C9BF87C934C667B5FBF1DD1B70CECBC9	Sim

IV. CONCLUSIONS

Diffie-Hellman algorithm can improve data security. This is because the keys used for the encryption and decryption process do not need to be exchanged in the public channel, so that the level of key leak vulnerability can be minimized. Diffie-Hellman algorithm will be a bridge in the key exchange process.

REFERENCES

- Bin Pan, Yu Tian, Tian-shu Zhou, Feng Wang, Jing-song Li, 2015, 'Study on Image Encryption Method in Clinical Data Exchange', International Conference on Information Technology in Medicine and Education, 2015.
- Indonesia, Undang – undang 2004, Undang – undang Republik Indonesia nomor 29 tahun 2004 tentang Praktik Kedokteran, Jakarta.
- Parth Sehgal, Nikita Agarwal , Sreejita Dutta, P.M.Durai Raj Vincent, "Modification of Diffie-Hellman Algorithm to Provide More Secure Key Exchange," International Journal of Engineering and Technology (IJET), Vols. Vol 5 No 3 Jun-Jul 2013 , pp. 2498-2051, 2013.
- C. K. a. D. R. V. P. M. Aryan, "Enhanced diffie-hellman algorithm for reliable key exchange," IOP Conference Series: Materials Science and Engineering, vol. 263(017) 042015 , pp. 1-8, 2017.
- C. K. D. B. D. R. V. P. Aditi Bhattacharjee, "Hybrid security approachby combining diffie-hellman and RSA algorithms," International Journal of Pharmacy and Technology, vol. Vol. 8 | Issue No.4, pp. 26560-26567, 2016.
- M. N. A. Z. M. & B. A. Ahmad Abusukhon, "A hybrid network security algorithm based on Diffie Hellman and Text-to-Image Encryption algorithm," Journal of Discrete Mathematical Sciences and Cryptography, Vols. Volume 22, 2019 , no. Issue 1, pp. 65-81, 2019.
- Maude et al, "Magnetic Resonance Imaging Of The Brain In Adults With Severe Falciparum Malaria", 2014,. Malaria Journal, vol.3, p. 177-185.
- Zunaidi, M & Suharsil, 2018, 'Pengamanan Citra Digital Menggunakan Kombinasi Antara Algoritma AES dan Metode LSB', Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD, Vol.1, No.2, July 2018, p.36-50.
- Metrillitna, BS, 2015, 'Elliptic Curve Cryptography (Ecc) Pada Proses Pertukaran Kunci Publik Diffie-Hellman', vol.6, no.1, June 2015, p. 25-33.
- Kumar Santosh, BJ, Raj Roshni, VK, & Nair, A, 2017, 'Coparative Study on AES and RSA Algorithm for Medical Images', International Conference on Communication and Signal Processing, April 20