Mantik Journal, 8 (1) (2024), ISSN 2685-4236 (Online)

Published by:Institute of Computer Science (IOCS)

Jurnal Mantik

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

Data security using low bit encoding algorithm and rsa algorithm

Yusuf Ramadhan[1], Suhardi[2], Yuda Aditama[3]
[1,2,3]Department of Computer Science, Science and Technology, North Sumatra State Islamic University, Indonesia

A R T I C L E I N F O

Article history:

Received Feb 25, 2024
Revised Feb 27, 2024
Accepted Mar 05, 2024

Keywords:

Decryption;
Encryption;
LBE;
RSA;
Security.

ABSTRACT

Ensuring the security of messages and information is paramount in today's digital era. This study proposes a combined approach using the RSA algorithm for cryptography and the Low Bit Encoding (LBE) algorithm for steganography to enhance security measures. The security process involves encrypting plaintext messages into ciphertext, which are then embedded into MP3 audio files as cover objects. Evaluation is conducted by measuring the Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) of the stego audio. Research findings indicate an MSE value of approximately 0.6 and a PSNR of 62.2 dB, indicating high-quality audio files. The integration of these algorithms offers a robust security level, ensuring effective message confidentiality. This research contributes to a deeper understanding of cryptography and steganography techniques in safeguarding sensitive information during digital communication.

This is an open access article under the CC BY-NC license.

Corresponding Author:

Yuda Aditama,
Department of Computer Science, Science and Technology,
North Sumatra State Islamic University,
Jl. Golf Course, Kampung Tengah, Pancur Batu District, Deli Serdang Regency, North Sumatra 20353.
Email: yudaaditama17@gmail.com

1. INTRODUCTION

Information security is a major concern in exchanging messages and information in the current digital era. However, with the increasing complexity of cyber threats, a robust approach is needed to protect the confidentiality and integrity of data transmitted online(Lorien & Wellem, 2021).

Two techniques commonly used to improve information security are cryptography and steganography. Cryptography involves the use of algorithms to secure messages by converting them into a format that cannot be understood without the appropriate key(Arbin & Hariyanto, 2022). On the other hand, steganography allows hiding messages in seemingly ordinary media.

Based on previous research by (Zalukhu, Azanuddin, & Murniyanti, 2022)entitled "Information Security Applications Using the Least Significant Bit (LSB) Method and the Advanced Encryption Standard (AES) Cryptographic Algorithm". In this research, an application that can be used to protect text-based data is being developed by researchers. The secret text will first be encoded using the AES algorithm in the final application, then the encoded results will be inserted into the image using the LSB algorithm (Hakim, n.d.).

Another research by (Gunawan, I. 2021) entitled Using the LSB and Vigenere Algorithms to Secure Data Through Digital Image Patterns. The Vigenere algorithm can be used to encode text in this research, and the LSB algorithm can be used to insert the results into digital images.

Based on the conclusions obtained in previous research, in this research, to secure confidential information, researchers will use the RSA and Low Bit Encoding (LBE) algorithms to encode and insert information into an image. Where the secret message will be secured using the RSA algorithm and then inserted into a cover file using the LBE algorithm. The audio file will serve as a cover file for the message insertion procedure. The algorithm for encrypting public keys is called RSA. One of the first significant discoveries in the field of public key cryptography, this algorithm was the first to be recognized as the best for encryption and signing.

The group of asymmetric algorithms includes the RSA algorithm. Algorithms that use an encryption key that is different from the decryption key are known as asymmetric algorithms. Public key and private key are the two keys used in this algorithm. LBE, also known as Least Significant Bit (LSB), is a technique that is often used in steganography techniques. According to (Purba et al., 2021), "The least significant bit or commonly known as low bit encoding is one of the methods commonly used in steganography techniques for audio and image file types." Since LBE changes in cover files are very difficult to find, this method is very good and widely used. The LBE method does not use keys during the insertion and extraction phases of the process. The system works by inserting the message bits into the previous cover file bits.

Based on previous research, it can be concluded that cryptography and steganography methods can be combined to improve information security. where information will be encoded using cryptographic methods and then inserted into a medium to hide secret messages from other individuals (Zalukhu, Syahra, & Syahputra, 2020).

In this research, we combine these two techniques: RSA for cryptography and Low Bit Encoding (LBE) for steganography. RSA is a public key cryptographic algorithm that allows encryption and decryption of messages using the appropriate public and private keys(Mojisola, Misra, Falayi Febisola, Abayomi-Alli, & Sengul, 2022). Meanwhile, LBE is a steganography technique in which information is embedded in bits that have low value in media, such as MP3 audio files, without significantly changing the sound quality(Anitha, Saravanan, & Chandrasekar, 2023).

This research involved several short and concise methodological stages. First, the message is encrypted using the RSA algorithm. Next, the encrypted message is inserted into an MP3 audio file using the LBE algorithm. The results are then tested to ensure the success of the process and ensure that the sound quality of the resulting files remains high(Huang & Han, 2024).

It is hoped that by combining these two techniques, this research will make a significant contribution to improving information security in the exchange of messages and information in online environments.

This introduction will be followed by further explanation of the methods used, expected results, and potential implications of this research in the context of information security.

Cryptography is a science related to information security techniques through the transformation of data into a format that cannot be understood without proper key knowledge. One of the commonly used cryptographic algorithms is RSA (Rivest-Shamir-Adleman), a public key cryptographic algorithm that allows the use of public keys for encryption and private keys for decryption(Abdelwahab, Hussein, Hamed, Kelash, & Khalaf, 2021; Huang & Han, 2024; Osamor & Edosomwan, 2021).

Steganography is the science concerned with hiding secret information in seemingly non-suspicious media. The steganography technique used in this research is Low Bit Encoding (LBE), where information is embedded in bits that have low value in

the selected media, such as MP3 audio files (Mohamad, Din, & Ahmad, 2021). This technique allows hiding messages without disturbing the original quality of the media.

RSA is a very commonly used public key cryptography algorithm. The working process involves generating a public key and private key pair, where the message can be encrypted with the public key and can only be decrypted by the recipient with the corresponding private key (Abid et al., 2023). The security of RSA is based on the difficulty in factoring large integers(Ariyus, Kurniasih, & Profesi, 2021).

Low Bit Encoding is a steganography technique in which information is embedded in bits that have a low value in the selected media, such as an MP3 audio file. This technique allows efficient message hiding without disrupting the original quality of the media. The process involves replacing the bits that have low values with bits from the message to be inserted(Santoso, 2021).

Message Encryption with RSA: The first stage is message encryption which will be secured using the RSA algorithm. The message is converted into an unintelligible form without the appropriate key using the public key(Pahrizal, 2019).

Message Insertion with LBE: After the message is encrypted, the next stage is to insert the encrypted message into an MP3 audio file using the LBE algorithm. Information is inserted in bits that have low value in the media without changing the original quality of the media(Sihotang, Efendi, Zamzami, & Mawengkang, 2020).

After the insertion process is complete, the resulting audio file will be tested to ensure the success of the process and to ensure that the sound quality of the resulting file remains high. Testing involves calculating Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) to evaluate the sound quality of the modified files(Lubis & Dafitri, 2023).

By understanding the theoretical basis and stages of this methodology, researchers can design and implement appropriate methods to secure and hide messages in MP3 audio files using a combination of RSA and LBE algorithms (Ulva, 2021).

2. RESEARCH METHOD

In this research, the first step is to choose the dataset that will be used in the research. This dataset can be an MP3 audio file which will be used as a medium to store the inserted message. Next, the message to be inserted into the audio file is prepared. This message is then encrypted using the RSA algorithm to increase its security(Annisa, Seta, & Falih, 2022).

The RSA algorithm is implemented to encrypt messages that have been prepared previously. This encryption process uses a public key that complies with the RSA algorithm. The RSA encryption process is carried out using mathematical formulas that have been specified in the RSA algorithm. Each character in the message is converted into a numeric value according to the ASCII standard, then encrypted using a public key(Osamor & Edosomwan, 2021).

After the message is encrypted with RSA, the next stage is to insert the encrypted message into an MP3 audio file using the Low Bit Encoding (LBE) algorithm. This insertion process is carried out by replacing the low value bits in the audio file with bits from the encrypted message. This is done so that message insertion does not interfere with the original audio quality(Patana, Alikodra, Mawengkang, & Hamdani Harahap, 2023). After the insertion process is complete, the resulting audio file will be tested to ensure the success of the process and to evaluate the sound quality of the resulting file. Testing involves calculating Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) to evaluate the sound quality of modified audio files. These calculation formulas are taken from related literature in the field of audio signal processing(Usanto, 2022).

For MSE and PSNR calculations, the formulas used are as follows, Mean Square Error (MSE):

$$\text{MSE} = \frac{1}{N} \sum_{i+1}^{N} \big(I(i,j) - K(i,j)\big)2 \quad (1)$$

Peak Signal to Noise Ratio (PSNR):

$$PSNR + 10.log_{10} \left(\frac{MAX^2}{MSE}\right) \quad (2)$$

Where I(i,j) are pixels from the original image, while K(i,j) are the resulting values from the resulting image, and N is the total number of pixels(Andika, 2021).

3. RESULTS AND DISCUSSIONS

The encryption and decryption process used by RSA is based on modular arithmetic and prime numbers. Both the encryption key and the decryption key are integers. Although the encryption key is secret, it is not hidden and can be accessed by the general public. Consequently, the encryption key is also referred to as the public key. Along with the encryption key, a number of prime numbers are used to create the description key. Factoring non-prime numbers becomes more challenging the larger the number. The RSA algorithm becomes more powerful the more difficult the factorization is(Christian, Sitorus, & Nirmala, 2023). The flowchart of the RSA cryptographic algorithm encryption process can be seen in Figure 1.

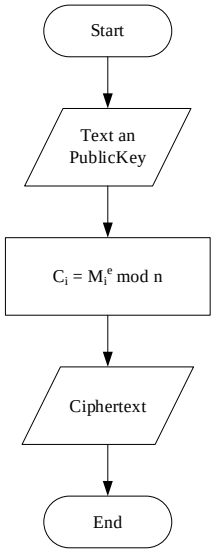

Figure 1. Flowchart Enkripsi Algoritma RSA

Figure 1 above is an illustration of the RSA Encryption Algorithm Flowchart process that will be used in this research using existing equations.

In this research, the process of securing data in the form of messages in text form which can be letters, numbers and symbols will be carried out into a digital image using a combination of the RSA algorithm and the LBE algorithm. The research flow that will be developed is to use the RSA algorithm to secure messages to produce ciphertext which will then be inserted into an audio file using the LBE algorithm. The output that will be produced by the application is an audio file that has confidential information in it. The information in the audio file can then be extracted using the application built in this research.

Where the text will be encrypted using the RSA algorithm and then the encryption results will be inserted into the audio file using the LBE algorithm. There are 5 steps in securing and inserting text into an audio file, including the following:

a. RSA algorithm encryption process.

The encryption and decryption process used by RSA is based on modular arithmetic and prime numbers. Both the encryption key and the decryption key are integers. Although the encryption key is secret, it is not hidden and can be accessed by the general public. Consequently, the encryption key is also referred to as the public key. Along with the encryption key, a number of prime numbers are used to create the description key. Factoring non-prime numbers becomes more challenging the larger the number. The RSA algorithm becomes more powerful the more difficult the factorization is.

In the process of calculating the RSA Encryption Algorithm, the first stage is determining the text and keyword values from the public, with the data sample to be tested, namely the keyword = EVERYTHING, then changing the plaintext to be encrypted in the decimal system (ASCII encoding) EVERYTHING = 69 86 69 82 89 84 72 78 71, after getting the decimal coding system value, the keyword value is broken down into 7 blocks of 3 digits, as follows:

x1 = 698 x4 = 984 x7 = 071
x2 = 669 x5 = 727
x3 = 828 x6 = 378

The plaintext blocks above are encrypted using the formula Ci = Mi e mod n as follows:

69861 mod 551 = 3= y1
66961 mod 551 = 177 = y2
82861 mod 551 = 429 = y3
98461 mod 551 = 374 = y4
72761 mod 551 = 206 = y5
37861 mod 551 = 233 = y6
07161 mod 551 = 383 = y7

So the result of the resulting ciphertext is y = 3 177 429 374 206 233 383, after getting the ciphertext value, then carry out the LBE Algorithm calculation process.

b. LBE Algorithm insertion process.

At this stage the ciphertext resulting from the encryption process using the RSA algorithm is converted into binary form. Next, the binary data is inserted into the bytes of the selected audio file. The process for inserting ciphertext is as follows:

Convert the ciphertext value into a binary value with the following calculations:

3 = 11
177 = 10110001
429 = 110101101
374 = 101110110
206 = 11001110
233 = 11101001
383 = 101111111

The results of the bit representation of the ciphertext have the highest number of bits of 9 digits, so in order to simplify the extraction process, the bit representation that

has a number of digits less than 9 will be added with the value 0 on the left so that it has the same number of digits without changing the value of the ciphertext the. Thus becoming :

3 = 000000011
177 = 010110001
429 = 110101101
374 = 101110110
206 = 011001110
233 = 011101001
383 = 101111111

Next, the ciphertext that has been converted into binary form will be inserted into the binary audio file by replacing the last audio file binary bit with the ciphertext binary bit. Then as an example the representation of the bits after the header tag of an audio file is taken(Yu & Kim, 2020). The binary audio file that will be used is as follows:

Table 1. Binary audio files tested

Binary audio					
00000000	00000110	01100111	01101011	01010100	01001001
01010100	00110010	00000000	00000000	00000000	00001111
00000000	00000000	00000000	01010011	01101000	01101111
01101111	01110100	01101001	01101110	01100111	00100000
01010011	01110100	01100001	01110010	01110011	01010100
01010000	01000101	00110001	00000000	00000000	00000000
00000110	00000000	00000000	00000000	01001011	01000001
01010010	01010101	01010100	01010100	01000001	01001100
01000010	00000000	00000000	00000000	10100011	00000000
00000000	00000001	11111111	11111110	01000010	00000000
01101100	00000000	01110101	00000000	01100101	00000000

c. LBE Algorithm Extraction Process

The resulting stego audio file which has text data in it can be extracted using the LBE algorithm. The extraction process is carried out per byte of data on the audio file. Then the audio file will search for and combine the secret message from the beginning to the last sentence so that all sentences are arranged according to the original message.

Table 2. Binary Audio results after processing

Binary Audio Results					
0000000**0**	0000011**0**	0110011**0**	0110101**0**	0101010**0**	0100100**0**
0101010**0**	0011001**1**	0000000**1**	0000000**0**	0000000**1**	0000111**0**
0000000**1**	0000000**1**	0000000**0**	0101001**0**	0110100**0**	0110111**1**
0110111**1**	0111010**1**	0110100**0**	0110111**1**	0110011**0**	0010000**1**
0101001**1**	0111010**0**	0110000**1**	0111001**1**	0111001**0**	0101010**1**
0101000**1**	0100010**1**	0011000**0**	0000000**1**	0000000**1**	0000000**0**
0000011**0**	0000000**1**	0000000**1**	0000000**0**	0100101**0**	0100000**1**
0101001**1**	0101010**1**	0101010**0**	0101010**0**	0100000**1**	0100110**1**
0100001**1**	0000000**0**	0000000**1**	0000000**0**	1010001**0**	0000000**1**
0000000**1**	0000000**0**	1111111**1**	1111111**1**	0100001**1**	0000000**1**
0110110**1**	0000000**1**	0111010**1**	00000000	01100101	00000000

In the table above are the results obtained after the chiptext insertion process was carried out, by replacing the last binary bit with the chiptext binary bit which is marked in bold and underlined. Next is the process for carrying out LBE Algorithm extraction calculations.

The resulting stego audio file which has text data in it can be extracted using the LBE algorithm. The extraction process is carried out per byte of data on the audio file. Then the audio file will search for and combine the secret message from the beginning to

the last sentence so that all sentences are arranged according to the original message. The process of compiling message bits into ciphertext:

000000011 = 3
010110001 = 177
110101101 = 429
101110110 = 374
011001110 = 206
011101001 = 233
101111111 = 383

d. RSA Algorithm Decryption Process

At this stage, carry out a calculation process in the description process to produce plaintext values again using the equation formula Mi = Ci d mod n. The description is carried out using the private key d = 1019. The ciphertext blocks are described as follows:

31019 mod 551 = 698 = x1
1771019 mod 551 = 669 = x2
4291019 mod 551 = 828 = x3
3741019 mod 551 = 984 = x4
2061019 mod 551 = 727 = x5
2331019 mod 551 = 378 = x6
3831019 mod 551 = 71 = x6

Finally, the original plaintext is recovered x = 698 669 828 984 727 378 71. After getting the original plaintext value, we break it into blocks of 2 digits to get the ASCII value of the plaintext becomes: 69 86 69 82 89 84 72 73 78 71= EVERYTHING.

e. PSNR Value Calculation

To be able to carry out calculations on the MP3 stego, first calculate the MSE (Mean Square Error) with equation 1. The calculation can be explained as follows, In the previous data, the result of the addition or (Σ) of $|| I(i) - K(i) ||^2$ in the first 30 bytes is 20, so the MSE value can be calculated using the formula:

$$MSE = \frac{1}{n}\sum_{i=0}^{n-1} || I(i) - K(i) ||^2$$

$$= \frac{1}{30} x18$$

$$=0.6$$

From the calculation above, the MSE value is 0.6. Next, the PSNR value will be calculated using the formula 2. Where MAX_I bits per sample in the MP3 file signal. Because each byte in the MP3 sample has a value of 8, the MAX value can be calculated using the formula:

$MAX_I = 2^I - 1$
$= 2^8 - 1$
$= 255$

$PSNR = 20 \log_{10} \frac{255}{\sqrt{0.6}}$
$= 20 \log_{10} (311.5)$
$= 20 * 3.11 = 62.2$

From these calculations, the PSNR value of Stego audio is 62.2 dB and the MSE value is 0.6. The stego audio is declared good because it complies with the PSNR value requirements, where the audio will be better if it has a PSNR value above 30dB.

The design of an image data security application using a combination of the low bit encoding algorithm and the RSA algorithm was built using Android Studio software.

The design of the flow of using the menu in the application being designed can be seen in the following flowchart. The embedding flowchart describes the flow of using the menu in the application in carrying out the encryption process and inserting data into the image.

In this research, an application has been produced that can be used to secure data in the form of text into an audio file. The process of securing and inserting text into audio files is carried out using the RSA algorithm and LBE algorithm(Sutejo, 2021). By using this application, users can use audio files to protect information before it is sent to other parties. The following are the results of application testing when run on an Android smartphone. The testing carried out is in the form of running the application and displaying the pages contained in each menu in the application resulting from this research. Application testing results are as follows:

Figure 3. Research Application Testing Results

In the picture above is the result of the design and test results of the system built using the University word sample resulting in an MSE process of 0.000108 and a PSNR of 87.841966 with a work process time of 0.003652 seconds, with the accuracy value of data similarity after encrypting the data amounting to 98% accurate similarity in the system being built. In this research, an application has been produced that can be used to secure data in the form of text into an audio file. The process of securing and inserting text into audio files is carried out using the RSA algorithm and LBE algorithm. By using this application, users can use audio files to protect information before sending it to other parties. The research results obtained can be compared with previous research results where previous research did not contain PSNR calculations which is a benchmark for comparing file quality, while the results presented in This research includes the comparative aspect of calculating PSNR values between initial or original audio and stego audio which has been processed to get the same results and good data security.

4. CONCLUSION

The conclusion from the research findings is that the RSA algorithm has proven effective in encrypting and decrypting messages using public and private keys. Insertion of an encrypted message into an audio file (.mp3) using the LBE algorithm was successful for messages 10 characters long, but failed for 50 and 100 character lengths with audio bit rates of 64 Kbps, 128 Kbps, 192 Kbps, and 320 Kbps, resulting in the application

becomes unresponsive. However, audio files with encrypted messages still maintain good quality with PSNR values above 30dB and maintain original sound quality. The contribution of this research is to expand understanding of the use of RSA and LBE algorithms in the context of information security on audio media and provide practical guidance for developing applications that integrate cryptographic and steganographic techniques in securing messages and information on Android-based platforms. Suggestions for further development include adding features to secure other types of files such as videos and images, as well as expanding research to improve the security of data obtained from document files. Thus, this research not only provides valuable insights for the academic world in the field of information security, but also provides practical contributions that can be applied in the development of information security applications in the future.

REFERENCES

Abdelwahab, O. F., Hussein, A. I., Hamed, H. F. A., Kelash, H. M., & Khalaf, A. A. M. (2021). Efficient Combination of RSA Cryptography, Lossy, and Lossless Compression Steganography Techniques to Hide Data. *Procedia Computer Science*, *182*(2), 5–12. https://doi.org/10.1016/j.procs.2021.02.002

Abid, R., Iwendi, C., Javed, A. R., Rizwan, M., Jalil, Z., Anajemba, J. H., & Biamba, C. (2023). An optimised homomorphic CRT-RSA algorithm for secure and efficient communication. *Personal and Ubiquitous Computing*, *27*(3), 1405–1418. https://doi.org/10.1007/s00779-021-01607-3

Andika, S. (2021). Implementasi Algoritma Freivlds Untuk Pembangkitan Kunci AlgoritmaRSA Pada Pengamanan Data Video. *Pelita Informatika : Informasi Dan Informatika*, *10*(2), 70–77.

Anitha, S., Saravanan, S., & Chandrasekar, A. (2023). Trust management based multidimensional secure cluster with RSA cryptography algorithm in WSN for secure data transmission. *Measurement: Sensors*, *29*(May), 100889. https://doi.org/10.1016/j.measen.2023.100889

Annisa, S., Seta, H. B., & Falih, N. (2022). Model Pengamanan Berkas Menggunakan Kriptografi Asimetris RSA Dan Algoritma Kompresi PPM Pada File Curriculum Vitae (CV). *Informatik : Jurnal Ilmu Komputer*, *18*(2), 177. https://doi.org/10.52958/iftk.v18i2.4669

Arbin, S., & Hariyanto, E. (2022). APPLICATION OF CRT (CHINESE REMINDER THEOREM) TO SPEED UP THE PROCESS OF DATA SECURITY ON IMAGE FILES. *Jurnal Sean Institute*, *10*(2), 1312–1320.

Ariyus, D., Kurniasih, J., & Profesi, D. E. (2021). Modifikasi Kunci Simetris Caesar Cipher dan OTP Menggunakan Algoritma Genetika Pada Steganografi. *CSRID (Computer Science Research and Its Development Journal)*, *11*(1), 34. https://doi.org/10.22303/csrid.11.1.2019.34-43

Christian, C., Sitorus, S. H., & Nirmala, I. (2023). Implementasi Algoritma RSA Dan One Time Password (OTP) Untuk Pengamanan Data Pengguna dan Proses Transaksi pada Website E-Commerce. *Coding: Jurnal Komputer Dan Aplikasi*, *11*(1), 62–72.

Hakim, S. A. (n.d.). Implementasi advanced encryption standard pada sistem repository berbasis online studi kasus: Pt Bprs Al Salaam Amal Salman. Fakultas Sains dan Teknologi UIN Syarif Hidayatullah Jakarta.

Huang, H., & Han, Z. (2024). Computational ghost imaging encryption using RSA algorithm and discrete wavelet transform. *Results in Physics*, *56*(November 2023), 107282. https://doi.org/10.1016/j.rinp.2023.107282

Lorien, A., & Wellem, T. (2021). Implementasi Sistem Otentikasi Dokumen Berbasis Quick Response (QR) Code dan Digital Signature. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *5*(4), 663–671. https://doi.org/10.29207/resti.v5i4.3316

Lubis, I., & Dafitri, H. (2023). Analisis Kinerja Sistem Kripto kompresi Pada File Dokumen Dengan Algoritma Asimetris RSA dan Even Rodeh Code. *SNASTIKOM*, *10*(3), 1–11.

Mohamad, M. S. A., Din, R., & Ahmad, J. I. (2021). Research trends review on RSA scheme of asymmetric cryptography techniques. *Bulletin of Electrical Engineering and Informatics*, *10*(1), 487–492. https://doi.org/10.11591/eei.v10i1.2493

Mojisola, F. O., Misra, S., Falayi Febisola, C., Abayomi-Alli, O., & Sengul, G. (2022). An improved random bit-stuffing technique with a modified RSA algorithm for resisting attacks in information security (RBMRSA). *Egyptian Informatics Journal*, *23*(2), 291–301. https://doi.org/10.1016/j.eij.2022.02.001

Osamor, V. C., & Edosomwan, I. B. (2021). Employing scrambled alpha-numberic randomization and RSA algorithm to ensure enhanced encryption in electronic medical record. *Informatics in*

Medicine Unlocked, *25*(2), 100672. https://doi.org/10.1016/j.imu.2021.100672

Pahrizal, D. P. (2019). Implementasi Algoritma Rsa Untuk Pengamanan Data Berbentuk Teks. *Jurnal Pseudocode*, *III*(1), ISSN : 2355 – 5920.

Patana, P., Alikodra, H. S., Mawengkang, H., & Hamdani Harahap, R. (2023). State of human tiger conflict around Gunung Leuser National Park in Langkat Landscape, North Sumatra, Indonesia. *Biodiversitas*, *24*(2), 837–846. https://doi.org/10.13057/biodiv/d240220

Santoso, Y. S. (2021). Message Security Using a Combination of Hill Cipher and RSA Algorithms. *Jurnal Matematika Dan Ilmu Pengetahuan Alam LLDikti Wilayah 1 (JUMPA)*, *1*(1), 20–28. https://doi.org/10.54076/jumpa.v1i1.38

Sihotang, H. T., Efendi, S., Zamzami, E. M., & Mawengkang, H. (2020). Design and Implementation of Rivest Shamir Adleman's (RSA) Cryptography Algorithm in Text File Data Security. *Journal of Physics: Conference Series*, *1641*(1). https://doi.org/10.1088/1742-6596/1641/1/012042

Sutejo, S. (2021). Implementasi Algoritma Kriptografi Rsa (Rivest Shamir Adleman) Untuk Keamanan Data Rekam Medis Pasien. *INTECOMS: Journal of Information Technology and Computer Science*, *4*(1), 104–114. https://doi.org/10.31539/intecoms.v4i1.2437

Ulva, A. (2021). Implementasi Algoritma Kargers Min Cut Untuk Pembangkitan Kunci Algoritma RSA Pada Pengamanan Data Video. *Pelita Informatika : Informasi Dan Informatika*, *10*(2), 58–64.

Usanto, U. (2022). Aplikasi Enkripsi Dengan Algoritma Rivest Shami Aldeman (Rsa) Dan Parity Bit Coding Untuk File Multimedia. *Jeis: Jurnal Elektro Dan Informatika Swadharma*, *2*(2), 17–28. https://doi.org/10.56486/jeis.vol2no2.179

Yu, H., & Kim, Y. (2020). New RSA encryption mechanism using one-time encryption keys and unpredictable bio-signal for wireless communication devices. *Electronics (Switzerland)*, *9*(2), 1–10. https://doi.org/10.3390/electronics9020246

Zalukhu, K., Azanuddin, A., & Murniyanti, S. (2022). Implementasi Sistem Keamanan Database Data Pelanggaran Hukum Disiplin Prajurit Menggunakan Algoritma Advanced Encryption Standard 128 Bit Pada Pengadilan Militer I-02 Medan. *Jurnal Cyber Tech*, *1*(8).

Zalukhu, K., Syahra, Y., & Syahputra, T. (2020). Implementasi Sistem Keamanan Database Data Pelanggaran Hukum Disiplin Prajurit Menggunakan Algoritma Advanced Encryption Standard 128 Bit Pada Pengadilan Militer I-02 Medan. *J-SISKO TECH (Jurnal Teknologi Sistem Informasi Dan Sistem Komputer TGD)*, *3*(2), 138. https://doi.org/10.53513/jsk.v3i2.2419