Journal of Technology and Computer (JOTECHCOM)
Vol. 1, No. 4, November 2024, pp. 1~8
ISSN: 3048-0477 (Media Online)

Implementation of RSA Cryptography Algorithm in Data Encryption for Location Manipulation Based on IP Address

Muhammad Bintang Harahap[1], Amrullah[2]
[1,2]Muhammadiyah University of North Sumatra, Indonesia
[1,2]Information Technology, Faculty of Computer Science and Information Technology, Muhammadiyah University of North Sumatra, Indonesia
[1]muhammadbintang.2112@gmail.com, [2]amrullah@umsu.ac.id

Article Info

Article history:

Received October 14, 2024
Revised October 30, 2024
Accepted November 01, 2024

Keywords:

Data Security
Geolocation
IP Address
RSA Algorithm

ABSTRACT

This research enhances data security for geolocation information derived from IP addresses using RSA encryption. In today's digital era, protecting sensitive data is crucial, as personal information is often transferred and stored electronically. Encryption is a key security method that transforms readable data (plaintext) into unreadable code (ciphertext) without the correct decryption key, thereby safeguarding it from unauthorized access. The RSA algorithm, specifically with a 2048-bit key length, has proven effective in securing geolocation data against brute-force attacks, ensuring that only authorized users with the correct decryption key can access the information. This study confirms that RSA encryption allows encrypted geolocation data to be stored safely in databases, maintaining data confidentiality and integrity. Ultimately, this research contributes to the understanding of RSA cryptography's application in data encryption for IP-based location data, offering a reliable method to prevent data manipulation and unauthorized access.

Corresponding Author:

Muhammad Bintang Harahap
Muhammadiyah University of North Sumatra
Email: muhammadbintang.2112@gmail.com

1. INTRODUCTION

In this digital age, data security is of paramount importance, where personal and sensitive information is often sent and stored electronically. This research focuses on improving the security of geolocation data obtained from IP addresses through the use of RSA encryption algorithm. One effective method of protecting data is through encryption, which converts the original data into an unreadable form without the right encryption key. One mechanism to improve data security is to use encryption technology. The data stored in the database is altered in such a way that it cannot be easily read. So encryption is a process done to secure data (called plaintext) into hidden data (called ciphertext).

One of the solutions needed is to apply the RSA algorithm, which RSA (Rivest Shamir Adleman) is one of the popular public key algorithms used and even today the RSA algorithm is still considered safe is an extension of the Caesar cipher, which multiplies the plaintext by a value and adds it with a shift. Data fraud can be overcome by utilizing the RSA method in encrypt and descript. Therefore, a security system is needed that is able to maintain data confidentiality from other threats carried out by irresponsible parties. By utilizing the RSA algorithm, the system will encrypt the original data inputted by the researcher into ciphertext using the key, then send it to other people or colleagues. For the reception of the original data is decrypted into plaintext using the key also by the recipient so that the delivery of information or utilization of information through the security of the RSA algorithm becomes younger understood by the recipient or user. (Ulfah Indriani, Ommi Alfina, 2021). From some of the problems described above, researchers are interested in conducting research with the title “Implementation of RSA Cryptography Algorithm in Data Encryption for Location Manipulation Based on IP Address”.

2. METHOD

2.1. Rivest Shamir Adleman (RSA)

RSA is one of the Public Key Cryptosystems that is very often used to provide confidentiality to the authenticity of digital data. The security of encryption and decryption of this data model lies in the difficulty of factoring a very large modulus n. In cryptography, RSA is an algorithm for public key encryption. It was the first known algorithm best suited for signing and encryption and one of the first major discoveries in public-key cryptography. RSA is still widely used in electronic commerce protocols and is believed to be highly secure due to its long key lengths and sophisticated implementations. (Rezki & Siahaan, 2021).

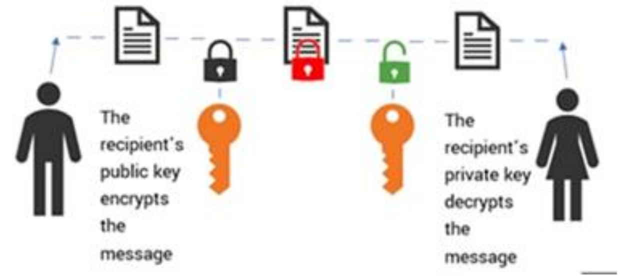

The recipient's public key encrypts the message
The recipient's private key decrypts the message

Figure 1. Example of Private and Public Keys

2.2. Steps of Rivest Shamir Adleman (RSA)

RSA (Rivest-Shamir-Adleman) algorithm is an asymmetric key cryptography algorithm used for encryption and decryption of messages. This algorithm uses a public key and a private key, where the public key is used for encryption and the private key is used for decryption. The workings of the RSA algorithm include several stages, namely:

a. Key expansion: Choose two large primes p and q, and calculate n = p x q. Also calculate m = (p-1) x (q-1).
b. Choosing e: Choose e that is prime relative to m, and e must not equal 1.
c. Selecting d: Selects d that is relatively prime to m, and d must not equal 1.
d. Encryption: Calculating the public key (e, n), and using the public key to generate the encryption message (c).
e. Decryption: Calculates the private key (d, n), and uses the private key to generate the decryption message (m).

The RSA algorithm is widely used in digital data security, such as electronic commerce protocols, digital signatures, pay TV authentication, SSL protocols, and electronic card security. The security of the RSA algorithm lies in the exponential process, and factoring a number into 2 prime numbers which until now took a long time to do the factoring. (Rezki & Siahaan, 2021).

2.3. Research Procedure

This research has several stages, namely goal definition, literature study, data processing, algorithm implementation, testing in encrypting data, and conducting testing and evaluation.

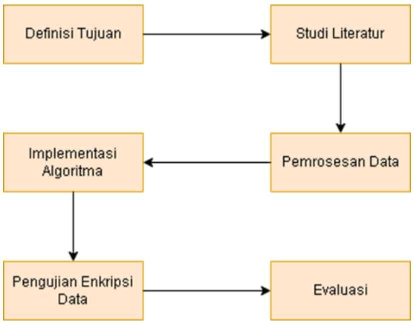


Figure 2. Research procedure

2.4. Flowchart

Flowchart of RSA algorithm implementation in data encryption This flowchart describes the steps needed to know how to work on implementing the RSA algorithm in data encryption.

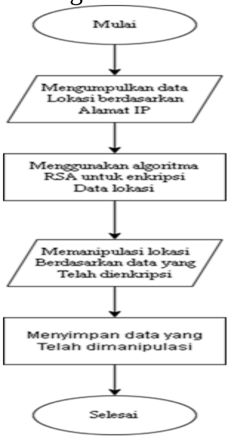

Mulai
Mengumpulkan data Lokasi berdasarkan Alamat IP
Menggunakan algoritma RSA untuk enkripsi Data lokasi
Memanipulasi lokasi Berdasarkan data yang Telah dienkripsi
Menyimpan data yang Telah dimanipulasi
Selesai

Figure 3. Flowchart of RSA algorithm implementation on data encryption

The flowchart systematics above are as follows:

a. Start: The process starts.
b. Collects location data based on IP address: Location data is collected based on the IP address.
c. Using RSA algorithm for encryption of location data: The location data that has been collected is then encrypted using the RSA algorithm.
d. Manipulate the location based on the encrypted data: The encrypted location data is processed and manipulated.
e. Storing the manipulated data: The data that has been manipulated and remains in an encrypted state is stored in the storage system.
f. Finish: The end point of the process.

3. RESULTS AND DISCUSSION

3.1. Manual Calculation and Using Python on RSA Algorithm Based on IP

This manual calculation of the RSA algorithm based on IP will explain how to perform a manual calculation of the RSA algorithm based on IP specifically. Starting from key generation, encryption process and description process.

a. IP Encryption and Description Process with RSA Algorithm
   1) Creating an RSA Key Pair:
      a) Choose two different large primes (p and q).
      b) Calculate n = p*q.
      c) Calculate φ(n) = (p - 1) * (q - 1).
      d) Choose an integer e such that gcd(e, φ(n)) = 1.
      e) Calculate d = e^-1 mod φ(n).
      f) The pair (e, n) is the public key, and (d, n) is the private key.
b. IP encryption:
   1) Convert the IP address (in decimal form) to an integer (e.g. by binary conversion).
   2) Ensure that the resulting integer is smaller than n.
   3) Perform encryption with the formula:

      Ciphertext = plaintext^e mod n

      Where: ciphertext is the encrypted IP address, while plaintext is the IP address in integer form, e is the public key and n is the modulus.
c. Manual Calculation Process of IP Address with RSA Algorithm:
   The IP address we want to encrypt is 114.122.5.15
   First, we will convert each part of the IP to binary:

114 → 01110010
122 → 01111010
5 → 00000101

15 → 00001111

Then we will combine them all into one:

01110010 01111010 00000101 00001111

Then we will convert this binary to decimal:

01110010 01111010 00000101 00001111 = 192.059.7311

Then we will convert the IP address to a whole number

IP address 114.122.5.15 we will convert it to a single integer.

Conversion method:

1) Split each octet of the IP address.
2) Multiply each octet by the corresponding power of 256, and then sum the results.

   Example:

   a) IP address. 114.122.5.15
   b) Octets 114, 122, 5, 15

   The calculation:

   IP_to_int = $(114 \times 256^3) + (122 \times 256^2) + (5 \times 256) + 15$

   Steps:

   1. $114 \times 256^3 = 114 \times 16777216 = 1912602624$
   2. $22 \times 256^2 = 122 \times 65536 = 7995392$
   3. $5 \times 256 = 1280$
   4. $15 = 15$

   Add it all up:

   IP_to_int = $1912602624 + 7995392 + 1280 + 15 = 1920597311$

d. RSA Steps

1) Step 1 is to select the values of p and q
   a) $p = 17$
   b) $q = 23$
2) Step 2 is to calculate n
   a) $n = p \times q$
   b) $n = 17 \times 23 = 391$
3) Step 3 is to calculate $\phi(n)$
   a) $\phi(n) = (p - 1) \times (q - 1)$
   b) $\phi(n) = (17 - 1) \times (23 - 1) = 16 \times 22 = 352$
4) Step 4 select e
   a) Choose e such that gcd $(e, \phi(n)) = 1$
   b) $e = 13$ (already coprime with 352)
5) Step 5 calculates d
   a) Use the Extended Euclidean Algorithm to find d:
   b) $d = e^{-1} \bmod \phi(n)$
   c) $13d = 1 \bmod 352$
   d) Using the Extended Euclidean algorithm:
      1 $352 = 27 \times 13 + 1$
      2 $1 = 352 - 27 \times 13$
      3 $d = 325$
      4 So $d = 325$

e. Encryption Process

1) We convert the IP address 114.122.5.15 into decimal (here I use 114 for this encryption calculation):
2) Plaintext = 114
3) Encryption formula: Ciphertext = plaintext^e mod n
4) Ciphertext = $114^{13} \bmod 391$

   The calculation uses the modular exponentiation method to calculate $114^{13} \bmod 391$:

   a) $114^1 \bmod 391 = 114$
   b) $114^2 \bmod 391 = 12996 \bmod 391 = 93$
   c) $114^4 \bmod 391 = 93^2 \bmod 391 = 8649 \bmod 391 = 47$
   d) $114^8 \bmod 391 = 47^2 \bmod 391 = 2209 \bmod 391 = 254$
   e) $114^{13} \bmod 391 = 114 \times 93 \times 47 \times 254 \bmod 391$

Combine the result with the exponent in binary form (1101):

$114^{13} = 114^{8+4+1} = 114^{8}. 114^{4}. 114 \bmod 391$

$114^{13} = 254.47.114 \bmod 391$

a) $254 \times 47 \bmod 391 = 11938 \bmod 391 = 11938 - 30 \times 391 = 208$

b) $208 \times 114 \bmod 391 = 23712 \bmod 391 = 23712 - 60 \times 391 = 252$

So, ciphertext = 252

f. Process Description

1) Description: plaintext = ciphertext^d mod n

2) Plaintext $252^{325} \bmod 391$

Using the modular exponentiation method to perform calculations.

a) $252^{1} \bmod 391 = 252$

b) $252^{2} \bmod 391 = 63504 \bmod 391 = 162$

c) $252^{4} \bmod 391 = 162^{2} \bmod 391 =26244 \bmod 391 = 47$

d) $252^{8} \bmod 391 = 47^{2} \bmod 391 = 2209 \bmod 391 = 254$

e) $252^{16} \bmod 391 = 254^{2} \bmod 391 = 64516 \bmod 391 = 101$

f) $252^{32} \bmod 391 = 101^{2} \bmod 391 = 10201 \bmod 391 = 35$

g) $252^{64} \bmod 391 = 35^{2} \bmod 391 = 1225 \bmod 391 = 52$

h) $252^{128} \bmod 391 = 52^{2} \bmod 391 = 2704 \bmod 391 = 358$

i) $252^{256} \bmod 391 = 358^{2} \bmod 391 = 128164 \bmod 391 = 270$

Combining results

$252^{325} = 252^{256}. 252^{64}. 252^{4}. 252^{1} \bmod 391$

a) $358 \times 35 \bmod 391 = 12530 \bmod 391 = 12530 – 32 \times 391 = 18$

b) $18 \times 8 \bmod 391 = 144 \bmod 391 = 144 – 0 \times 391 = 144$

So, plaintext = 114

g. Conclusion

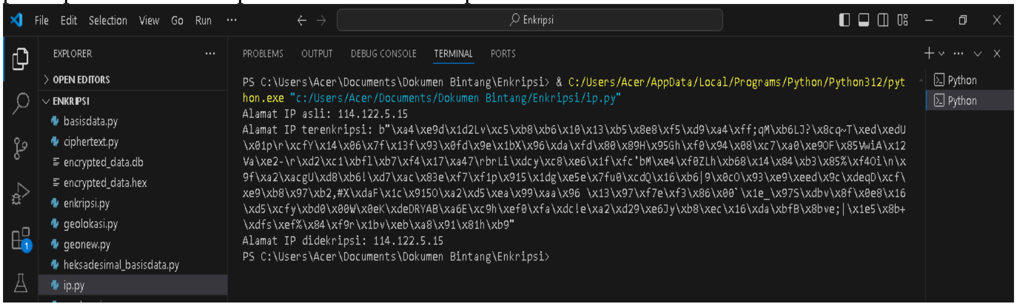
After doing manual calculations and having obtained the results of calculations with the appropriate modular exponentiation method, the results:

1) Ciphertext 252

2) Plaintext 114

3.2. Implementation of Encryption on IP Addresses with RSA Algorithm

This implementation is done to encrypt IP addresses using the RSA algorithm. RSA is an asymmetric encryption algorithm that uses a pair of keys, namely a public key and a private key, for the data encryption and description process. This implementation aims to protect IP address information from unauthorized access.



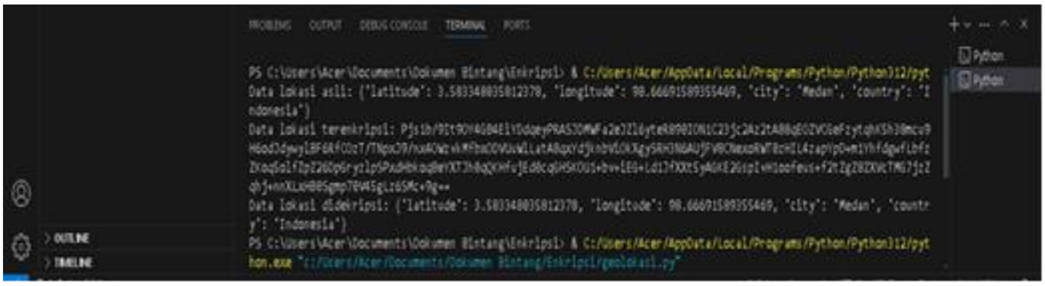
```
PS C:\Users\Acer\Documents\Dokumen Bintang\Enkripsi> & C:/Users/Acer/AppData/Local/Programs/Python/Python312/pyt
hon.exe "c:/Users/Acer/Documents/Dokumen Bintang/Enkripsi/ip.py"
Alamat IP asli: 114.122.5.15
Alamat IP terenkripsi: b"\xa4\xe9d\x1d2Lv\xc5\xb8\xb6\x10\x13\xb5\x8e8\xf5\xd9\xa4\xff;qM\xb6LJ?\x8cq~T\xed\xedU
\x01p\r\xcfY\x14\x06\x7f\x13f\x93\x0fd\x9e\x1bX\x96\xda\xfd\x80\x89H\x95Gh\xf0\x94\x08\xc7\xa0\xe9OF\x85WwiA\x12
Va\xe2-\r\xd2\xc1\xbfl\xb7\xf4\x17\xa47\rbrLi\xdcy\xc8\xe6\x1f\xfc'bM\xe4\xf0ZLh\xb68\x14\x84\xb3\x85%\xf4Oi\n\x
9f\xa2\xacgU\xd8\xb6!\xd7\xac\x83e\xf7\xf1p\x915\x1dg\xe5e\x7fu0\xcdQ\x16\xb6|9\x0cO\x93\xe9\xeed\x9c\xdeqD\xcf\
xe9\xb8\x97\xb2,#X\xdaF\x1c\x915O\xa2\xd5\xea\x99\xaa\x96 \x13\x97\xf7e\xf3\x86\x00`\x1e_\x97S\xdbv\x8f\x0e8\x16
\xd5\xcfy\xbd0\x00W\x0eK\xdeDRYAB\xa6E\xc9h\xef0\xfa\xdc!e\xa2\xd29\xe6Jy\xb8\xec\x16\xda\xbfB\x8bve;|\x1e5\x8b+
\xdfs\xef%\x84\xf9r\x1bv\xeb\xa8\x91\x81h\xb9"
Alamat IP didekripsi: 114.122.5.15
PS C:\Users\Acer\Documents\Dokumen Bintang\Enkripsi>
```

Figure 4. Encryption Process on IP

3.3. Implementation of Encryption on IP Addresses with RSA Algorithm

The geolocation data is done and prepared, the next step is to encrypt the data and ensure that the geolocation data is in the right format and ready to be encrypted. This encryption process starts by ensuring that the geolocation data is in the right format and ready to be encrypted. . Data that is ready for encryption includes information such as geographic coordinates (latitude and longitude), city, country, and internet service provider (ISP).

The geolocation data is encrypted using a pre-generated RSA public key. This results in an encrypted form of data that cannot be read or understood without the right decryption key. The implementation of encryption can be done using available cryptographic libraries, such as the cryptographic library in the Python programming language. This library accepts geolocation data and public key as input and produces ciphertext as output.



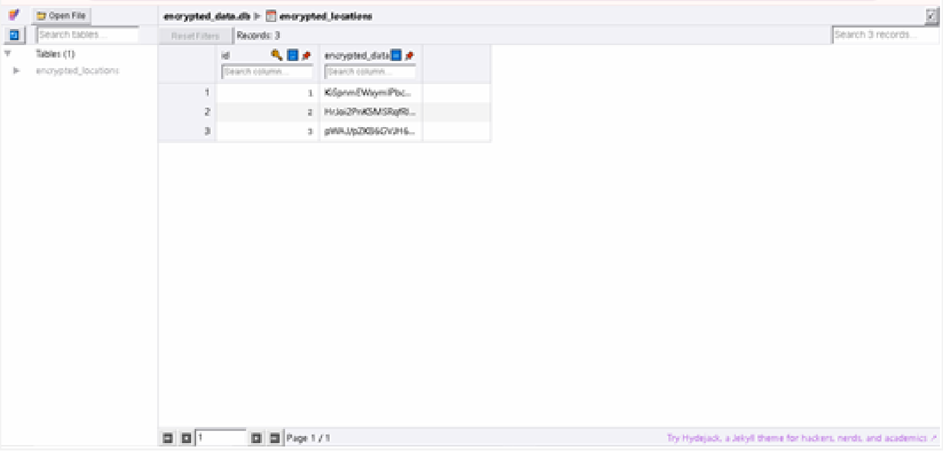
```
PS C:\Users\Acer\Documents\Dokumen Bintang\Enkripsi> & C:/Users/Acer/AppData/Local/Programs/Python/Python312/pyt
Data lokasi asli: {'latitude': 3.583348035812378, 'longitude': 98.66691589355469, 'city': 'Medan', 'country': 'I
ndonesia'}
Data lokasi terenkripsi: Pjs1b/9Dt9OY4G04E1YDdqeyPRAS3OMWFa2eJZl6yteR89OION1C23jc2Az2tA88qEOZVOGeFzytqhKSh38mcu9
H6od3dywyL8F6RfC0zT/TNpx29/nu4OWz+kMfbxOOVUuWLLatA8qxYdjknbV5OkXgySRH3N6AUjFV8ObwxoRWT8zHIL4zapYpO+m1YhfdgwfLbfz
ZXoq6olfZpZ26Dp6ryz1p5PxdHbkoqBeYXTJh8qQKHfvjEd8cqGHSKOUs+bv+1EG+Ld17fXXtSyAGKE26spI+H1oofeus+f2tZgZ8ZXWcTMG7jtZ
qhj+nnXLuH80Sgmp70V45gLz6SMc+9g==
Data lokasi didekripsi: {'latitude': 3.583348035812378, 'longitude': 98.66691589355469, 'city': 'Medan', 'countr
y': 'Indonesia'}
PS C:\Users\Acer\Documents\Dokumen Bintang\Enkripsi> & C:/Users/Acer/AppData/Local/Programs/Python/Python312/pyt
hon.exe "c:/Users/Acer/Documents/Dokumen Bintang/Enkripsi/geolokasi.py"
```

Figure 5. Geolocation encryption and description process

3.4. Storage of Encrypted Data in the Database

After the encryption and description process is complete and the geolocation data has been converted into ciphertext, the next step is to securely store this encrypted data in the database. This encrypted data storage is done because it aims to be able to maintain the integrity and confidentiality of the data, and can ensure that only parties who have authorized access can access the data.

The encrypted data is stored in a database designed for data security. This database can be a relational database management system (RDBMS) such as MySQL or PostgreSQL. Here I use the SQLite database to be able to store encrypted data, SQLite is a database that does not require a separate server to carry out its functions, unlike MySQL or PostgreSQL which require a server.



	id	encrypted_data
1	1	K6pnmEWaymiPbc...
2	2	HrJai2PnKSMSRqfRl...
3	3	pWAJ/pZK86GVJH6...

Figure 6. Data Encryption SQLite Database

4. CONCLUSION

This research can provide several points of conclusion in the implementation of encryption and description based on IP addresses, namely as follows:

1. The results of this research show that the RSA algorithm can be implemented well to be able to encrypt data based on the IP address obtained. The encryption process uses the RSA public key which is able to convert data into ciphertext that cannot be read without the right description key.
2. The results of this study prove that the RSA algorithm can ensure that geolocation data is encrypted properly, so that it can only be accessed by parties who have a valid description key. By using SQLite in securing encrypted data cannot be accessed by unauthorized parties so as to increase data security.
3. The implementation of the RSA algorithm using python to encrypt and decrypt data based on IP addresses has been successfully carried out. The python programming language provides various libraries and modules that can facilitate the implementation of RSA cryptography. Tests conducted in this study using the python programming language can show that python is an effective and efficient tool.

ACKNOWLEDGEMENTS

I would like to express my deepest gratitude to my supervisor who has provided guidance and advice in the process of writing this journal. With his help, I was able to complete this writing well.

REFERENCES

[1] Ade, B. (2022). Rancang Bangun Sistem Absensi Berbasis Face Id di Bank Mandiri Sungai Rumbai dengan Bahasa Pemograman Python. *Journal of Vocational Education and Information Technology (JVEIT)*, *3*(2), 65–70. https://doi.org/10.56667/jveit.v3i2.715

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

[3] Ardhiansyah, M., Noris, S., & Andrianto, R. (2020). *Modul Jaringan Komputer Universitas Pamulang* (Nomor 1).

[4] Chafid, N., & Soffiana, H. (2022). Impelementasi Algoritma Kriptografi Klasik Caesar Untuk Rancang Bangun Aplikasi E-Voting Berbasis Web (Studi Kasus : Sman 10 Tangerang). *Jurnal Ilmiah Sains dan Teknologi*, *6*(2), 133–145. https://doi.org/10.47080/saintek.v6i2.2249

[5] Fauzi, R. (2023). Implementasi Algoritma Kriptografi Elgamal Untuk Pesan Rahasia Berbasis Web Di Markas Pmi Kota Tangerang. *50 |Jurnal Ilmu Komputer JIK*, *VI*(03), 50–54.

[6] Feraldi, R., Khairuna, A., Hasan, M. A., Rezky, R., & Ramadhan, H. (2021). Kombinasi Algoritma Kriptografi Caesar Cipher Dan Permutation Cipher Untuk Pesan Teks Menggunakan Python. *Riau Journal of Computer Science*, *7*(1), 76–86.

[7] Harun Alfirdaus, M., Tahir, M., Enno Dewanti, N., Ardianto, R., Nur Azurah, N., Firman Cahyono, N., & Informatika, P. (2023). Perancangan Aplikasi Enkripsi Deskripsi Mengunakan Metode Caesar Chiper Berbasis Web. *Jtmei)*, *2*(2), 64–76.

[8] Ii, B. A. B., & Teori, L. (2016). *android yang diberi nama Gerbang Otomatis.apk. Dihubungkan dengan*. *2014*, 7–16.

[9] Ilmiah, J., & Indonesia, M. (2023). *Mutiara*. *1*(1), 204–214.

[10] Rezki, R., & Siahaan, R. F. (2021). Rancang Bangun Sistem Keamanan Data Digital dengan Metode RSA Berbasis Dekstop. *Jurnal Mahajana Informasi*, *6*(2), 32–40.

[11] Rumetna, M. S. (2021). Kombinasi Gnu Privacy Guard Dan Hamming Distance Untuk Keamanan Email Serta Jalur Sertifikasi Combination of Gnu Privacy Guard and Hamming Distance for Email Security and Certification Paths. *Elektro Luceat [November]*, *7*(2), 151–160.

[12] Studi, P., Informatika, T., Sains, F., Teknologi, D. A. N., Islam, U., & Syarif, N. (2021). *Evaluasi Kinerja Routing Protocol Ripng Dan Ospfv3 Pada Ipv6 Menggunakan Protocol Fhrp (Hsrp Dan Glbp)*.

[13] TRIANA, F. (2020). *Implementasi Caesar Cipher Cryptography Dan Least Significant Bit-2 (Lsb-2) Steganography Untuk Keamanan Data Berbasis …*. 8–42. http://eprints.polsri.ac.id/10054/

[14] Ulfah Indriani, Ommi Alfina, N. S. (2021). *Penerapan Algoritma Rsa Dan Affine Cipher Dalam Keamanan File Ms Word*. *01*(02), 95–100. http://repository.potensi-utama.ac.id/jspui/handle/123456789/5074

[15] Waruwu, S. H., & Hondro, R. K. (2024). *Analisis dan Implementasi Modifikasi Algoritma Kriptografi GOST Menggunakan Blum Blum Shub Generator Pada Sistem Pengamanan Login Pada Website*. *01*(03), 30–46.

[16] Martiano, M., & Sary, Y. Cryptography Generator for Prevention SQL Injection Attack In Big Data.

[17] Syaifuddin, M., Amrullah, A., Ginting, R. I., Iswan, M., & Hutagalung, J. (2022). Project-based learning on cryptographic using lms. *JURTEKSI (Jurnal Teknologi dan Sistem Informasi)*, *8*(2), 147-152.

[18] Hafizah, H., Tugiono, T., Panjaitan, Z., Amrullah, A., & Setiawan, D. (2023). APPLICATION OF THE MOORA METHOD IN THE DECISION SUPPORT SYSTEM FOR SELECTING THE BEST FONT AUTHORS ON ABLY CREATIVE FONT. *Journal of Science and Social Research*, *6*(1), 255-262.

[19] Syafutra, T. R., Khairil, K., & Suryana, E. (2022). The Implementation Of Modern Cryptography On Document Data Security. *Jurnal Media Computer Science*, *1*(2), 287-294. [20] Ii, B. A. B. (2021). *Bab ii tinjauan pustaka*. *Dm*, 7–23.

[20] Sari, M., Purnomo, H. D., & Sembiring, I. (2022). Cryptographic Algorithm for SMS Security System on Android. *Journal of Information Technology*, *2*(1), 11-15.

[21] Abella, F. A. (2022). IMPLEMENTATION OF CRYPTOGRAPHY USING AES-128 ALGORITHM. *Jurnal Ilmu Komputer (JIKOMP)*, *1*(1).

[22] Permana, A. A., & Nurnaningsih, D. (2020). Application Of Cryptography With Data Encryption Standard (Des) Algorithm In Picture. *JIKA (Jurnal Informatika)*, *4*(2), 82-87.

[23] Kuncoro, A. P., Mustofa, D., Krisbiantoro, D., & Tarwoto, T. (2023). DIGITAL DATA SECURITY WITH APPLICATION OF CRYPTOGRAPHY AND DATA COMPRESSION TECHNIQUES. *Jurnal Teknik Informatika (Jutif)*, *4*(5), 995-999. [24] Di, B., Bangunan, T., Mas, A., Algoritma, M., Saputra, A., Sari, H. L., & Sartika, D. (2023). *Implementasi Metode Association Rule Mining Pada Penjualan*. *2*(4), 709–718.

[24] Royani, M. R., & Wibowo, A. (2020). Web service implementation in logistics company uses JSON web

token and RC4 cryptography algorithm. *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, *4*(3), 591-600.

[25] Yuniati, T. (2020). Secure Electronic Payment Methods for Online Shopping Based on Visual Cryptography. *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, *4*(2), 319-328.