Securing the Distribution of Personnel Data in the North Sumatera Personnel Agency by Utilizing an Asymetric Cryptography Algorithm

Noprian Syahputra
Department of Information System, Universitas Muhammadiyah Sumatera Utara, Indonesia

ABSTRACT

In the context of this research, we will explore the implementation of the RSA algorithm to improve the security of personnel data distribution at BKPSU. This approach will provide additional protection to sensitive data, thereby increasing public trust and meeting established security standards. To overcome this problem, it is necessary to implement a strong and reliable security system. One suggested solution is to use the RSA (Rivest-Shamir-Adleman) asymmetric cryptographic algorithm. By implementing this algorithm, personnel data can be encrypted securely so that only authorized parties can read the information. By using the RSA algorithm, data security can be guaranteed because it is difficult for hackers to find out which private key corresponds to the public key used for encryption.

Keyword : Security, RSA, VB

Corresponding Author:
Noprian Syahputra,
Department of Information System,
Universitas Muhammadiyah Sumatera Utara,
Jalan Kapten Muktar Basri No 3 Medan 20238, Indonesia.
Email: nopriansyahputra@gmail.com

1. INTRODUCTION

In this modern digital world, data security is a crucial aspect that must be considered by organizations, especially in the context of personnel data in public institutions such as BKPSU. With more and more data security incidents occurring, the protection of personnel information should not be ignored. The RSA asymmetric cryptographic algorithm offers a robust approach to securing data by using different public and private keys. In the context of this research, we will explore the implementation of RSA algorithm to improve the security of personnel data distribution at BKPSU. This approach will provide additional protection to sensitive data, thereby increasing public trust and meeting established security standards. (Doe, J., 2022).

To solve the problem, it is necessary to implement a robust and reliable security system. One of the suggested solutions is to use the RSA (Rivest-Shamir-Adleman) asymmetric cryptography algorithm. By applying this algorithm, personnel data can be encrypted securely so that only authorized groups are able to access the information. (L. Adleman, 2022).

The RSA asymmetric cryptography algorithm is classified as one of the most commonly used cryptography algorithms to encrypt and decrypt data. It uses a combination of public and private keys, where the public key encrypts the data, while the private key is used for decryption. With the implementation of the RSA algorithm, data becomes more secure because it is difficult for hackers to figure out the private key that corresponds to the public key used for encryption.

The implementation of the RSA cryptographic algorithm in the personnel data distribution system at BKPSU is expected to provide effective protection of sensitive information. Thus, BKPSU employees and personnel data will be protected from the threat of hacking and information theft. In general, cryptography uses two techniques, namely symmetric and asymmetric. In symmetric cryptography, also known as Private Key Cryptography, the same key is used for the data encryption and decryption process (Ferdy Riza, 2018).

Based on the above problems, the authors are interested in conducting research with the title "Securing the Distribution of Personnel Data in the North Sumatera Personnel Agency by Utilizing an Asymetric Cryptography Algorithm".

2. RESEARCH METHOD

A. Research Phases

System design procedures can be described into waterfall stages, namely analysis, design, implementation, testing, maintenance.

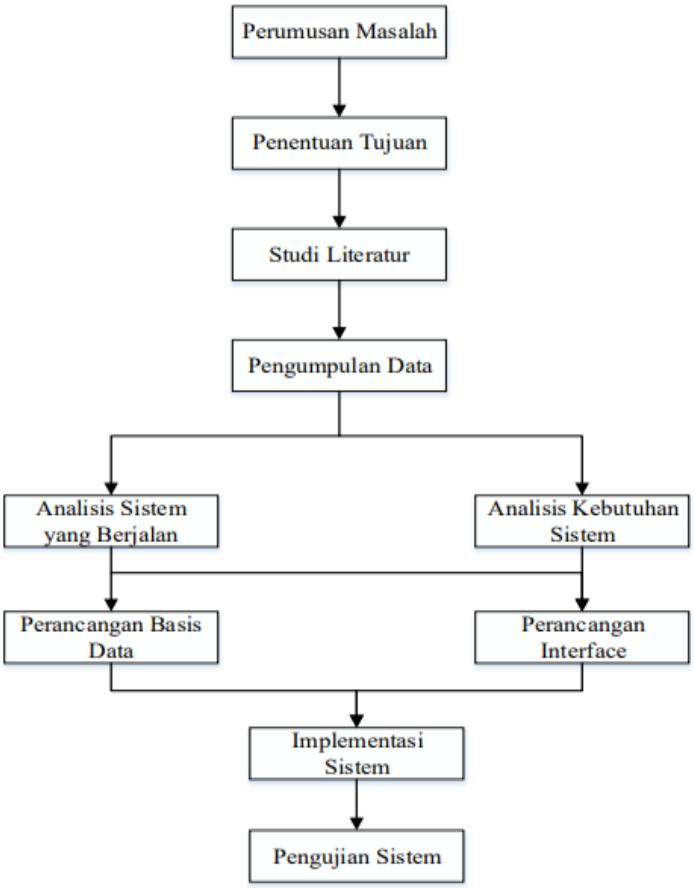

Fig 1. Waterfall Design Analysis Diagram

Design Analysis Diagram with WaterfallThe process of research activities is carried out in several stages as in Figure 1 what is expected is the development of a system for securing the distribution of personnel data at the North Sumatra Provincial Personnel Agency by utilizing the RSA Asymmetric Cryptography Algorithm.

B. Data Collection Methods

The designed system certainly requires data collection, in the data collection process there are several ways, including the following:

1) Observation, namely data and information collection carried out by direct observation to the location of the North Sumatra Provincial Civil Service Agency.
2) Interview, namely data collection by conducting questions and answers with HRD to obtain Personnel data at the Personnel Agency of North Sumatra Province.
3) Library Research, namely conducting library studies for data related to research in the form of journals and books.

C. Problem Analysis

In today's digital era, data security is a crucial aspect that must be considered by organizations, especially in the context of personnel data in public institutions such as BKPSU. With more and more data security incidents occurring, the protection of personnel information should not be neglected. The RSA asymmetric cryptographic algorithm offers a robust approach to securing data by using different

public and private keys. In the context of this research, we will explore the implementation of RSA algorithm to improve the security of personnel data distribution at BKPSU. This approach will provide additional protection to sensitive data, thereby increasing public trust and meeting established security standards. To address the problem, it is necessary to implement a robust and reliable security system. One suggested solution is to use the RSA (Rivest-Shamir-Adleman) asymmetric cryptography algorithm. By applying this algorithm, staffing data can be encrypted securely so that only authorized parties can read the information.

3. RESULTS AND DISCUSSION

A. Results

This chapter will explain the display of the results of the application that has been made, which is used to clarify the views that exist in the Security of Personnel Data Distribution at the Personnel Agency of North Sumatra Province by Utilizing the RSA Asymmetric Cryptography Algorithm. So that the results of its implementation can be seen in accordance with the results of the program that has been made. Below will be explained each display in the program.

1) Login Menu Display

The login display is the display that first appears when the program is run. Serves as a program admin username and password input form. The login display image can be shown in Figure 2:

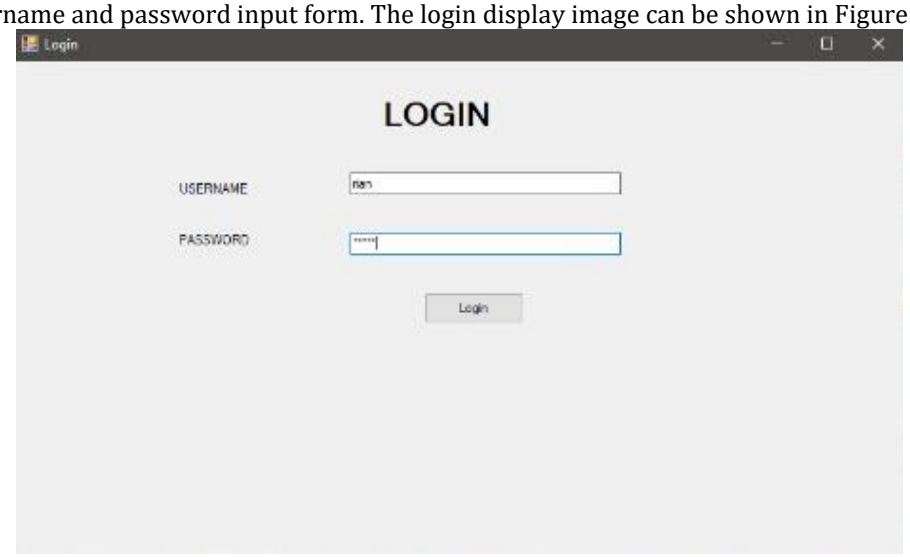

Fig 2. Login Menu Display

2) Main Form Display

The main form is the overall cryptography program interface, where to use this cryptography application can be through the main form interface. In the main form there are several menus, namely, the file menu and the program menu. For more details, the main form can be seen in Figure 3 below.

Fig 3. Main Form Display

3) Display of Encryption Data Form

This encryption form functions to change the contents of file data in the form of chipretext, save the encryption results (chipertext), and exit the encryption data form. The following display of the encryption data form can be seen in Figure 4 below:

Fig 4. Display of Encryption Data Form

4) Display of Decryption Data Form

This decryption form functions to upload data that will be secured. The following display of the decryption data form can be seen in Figure 5 below:

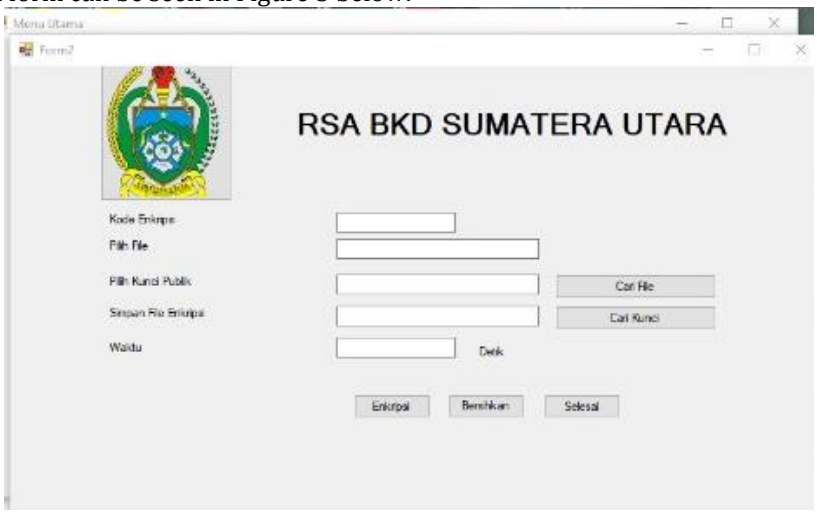

Fig 5. Display of Decryption Data Form

a. Display of Encryption Result

The Security Application for Personnel Data Distribution at the North Sumatra Personnel Office by Utilizing the RSA Asymmetric Cryptography Algorithm has the following appearance:

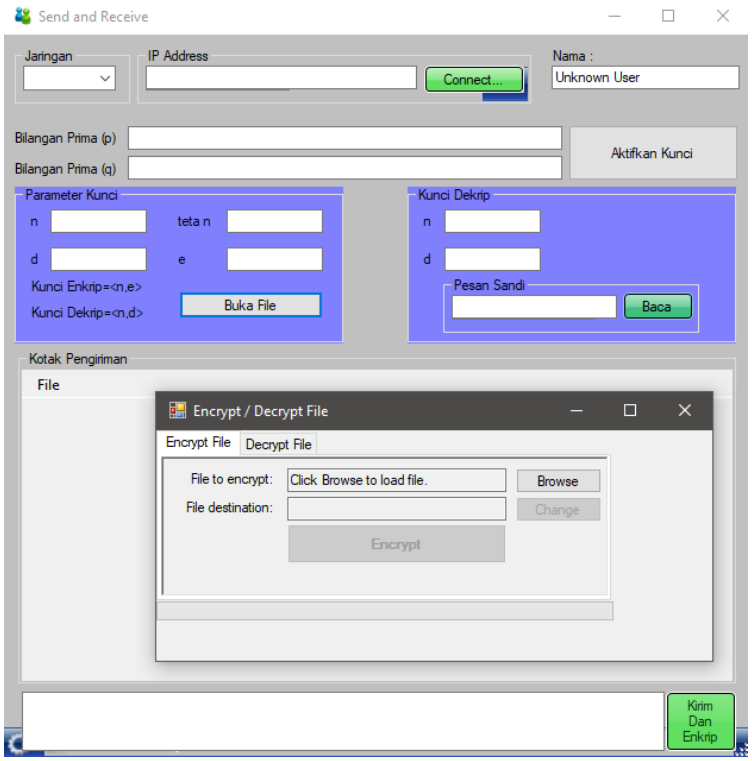

Fig 6. Display of Encryption Form

b. Decrypted Result Display

The Security Application for Personnel Data Distribution at the North Sumatra Personnel Office by Utilizing the RSA Asymmetric Cryptography Algorithm has the following appearance:

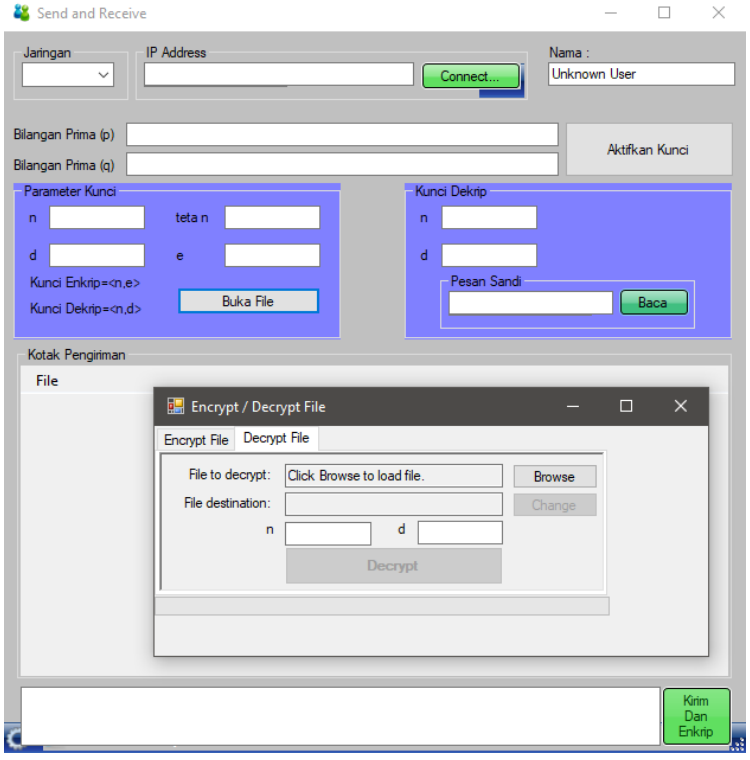

Fig 7. Decrip Form Display

B. Discussion

The discussion of hardware and software in making the application for securing the distribution of staffing data at the North Sumatra Staffing Agency by utilizing the RSA Asymmetric Cryptography Algorithm is described as follows:

1) Laptop hardware with the following specifications:
   a) Minimum Core 2 duo processor.
   b) Minimum 4 Gb RAM.
   c) Minimum 80 Gb hard drive.
2) Sofware with the following spesifications:
   a) OS Windows.
   b) Visual Studio 2019.
   c) Microsoft Word.

C. Advantages and Disadvantages of the System

Every system has advantages and disadvantages, the following are the advantages and disadvantages of the system that has been created.

1) Advantages of the System

   The advantages of the system that has been made include:

a) The application that has been created can keep the contents of the text in the sales capital database secret
b) The application that has been created uses two methods so as to strengthen the confidentiality of text data.
c) The application can store the results of data encryption and decryption into the SQL Server database.

2) Disadvantages of the System

   The disadvantages of the system that has been made include:

a) The application that has been created does not use one method.
b) The application that has been created cannot read data per database.
c) The application that has been created does not have instructions for use.

4. CONCLUSION

Based on the results of the review and trials that have been carried out, it can be concluded that the application has been built and can manipulate Personnel data at the Personnel Agency of North Sumatra Province with the RSA algorithm application encoding system. The system built has been able to encrypt and decrypt data so that it can protect personnel data at the North Sumatra Provincial Personnel Agency using the RSA method. The system built has a very simple appearance and is easy to use by users.

REFERENCES

[1] Azhari, M., Mulyana, D. I., Perwitosari, F. J., & Ali, F. (2022). Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES). Jurnal Pendidikan Sains Dan Komputer, 2(01), 163–171. https://doi.org/10.47709/jpsk.v2i01.1390

[2] Cristy, N., & Riandari, F. (2021). Implementasi Metode Advanced Encryption Standard (AES 128 Bit) untuk Mengamankan Data Keuangan. JIKOMSI [Jurnal Ilmu Komputer Dan Sistem Informasi], 4(2),75–85. https://ejournal.sisfokomtek.org/index.php/jikom/article/view/181%0A

[3] Ferdy Riza (2018) Analisa Frekuensi Hasil Enkripsi Pada Algoritma Kriptografi Blowfish Terhadap Keamanan Informasi

[4] Fitriyani A, Handayani R, & Widanengsih E. (2020). Sistem Pendukung Keputusan Pemilihan Jurusan Pada SMK YMIK Joglo Jakarta Barat Menggunakan Metode Simple Additive Weigting (SAW). Jtksi, 03(01), 11–19.

[5] Janis, J. W., Mamahit, D. J., Sugiarso, B. A., Rumagit, A. M., Elektro, T., Sam, U., & Manado, R. (2020). Rancang Bangun Aplikasi Online Sistem Pemesanan Jasa Tukang Bangunan Berbasis Lokasi. Jurnal Teknik Informatika, 15(1), 1–12. https://doi.org/10.35793/jti.15.1.2020.29023

[6] Kaban, R., Yunita, W., & Faradillah, Y. (2019). Aplikasi Pemesanan Tiket Bus Berbasis Android (Study Kasus : Pt . Als Terminal Pasar X Tanjung Beringin). Jurnal Manajemen ..., 32(1).

[7] Lubis, R. S., Tulus, & Nababan, E. B. (2022). Pengamanan File Teks Menggunakan Algoritma RSA – LUC dan Algoritma Zig- Zag dalam Hybrid Crypto Sistem. InfoTekJar : Jurnal Nasional Informatika Dan Teknologi Jaringan, 6(2), 185–189.

[8] Marpaung, R., & Informasi, T. (2022). PENYIMPANAN DATA PRIBADI DENGAN METODE. 2(11), 1–14.
[9] Muharromin, M., Informatika, J. T., & Darma, U. B. (n.d.). Analisis Performance Web Application Firewall ModSecurity dan Shadow Daemon Dalam Keamanan Web Server Apache. 393–402.
[10] Nugroho, A. P., & Suseno, H. B. (2020). Keamanan Data Transaksi Nasabah Pada Aplikasi Bank Sampah Berbasis Web Menggunakan Algoritma AES. "QUERY: Jurnal Sistem Informasi Keamanan Data Transaksi Nasabah Pada Aplikasi Bank Sampah Berbasis Web Menggunakan Algoritma AES.," 04(April), 9–17. http://jurnal.uinsu.ac.id/index.php/query/article/view/8007/3720
[11] Perbawa, K. A. (2022). Application of Linear Congruential Generator (LCG) Algorithm in Android Based Mathematics Education Game Penerapan Algoritma Linear Congruential Generator (LCG) dalam Game Edukasi Matematika Berbasis Android. Jurnal Komputer, Informasi Dan Teknologi, 2(1), 47–56.
[12] Prayudha, J., _ S., & _ I. (2019). Implementasi Keamanan Data Gaji Karyawan Pada PT. Capella Medan Menggunakan Metode Advanced Encryption Standard (AES). Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika Dan Komputer), 18(2), 119. https://doi.org/10.53513/jis.v18i2.150
[13] Ruing, M. O. I., & Ujianto, E. I. H. (2020). Penerapan Kombinasi Algoritma Kriptografi (Caesar, Vigenere, Zig-Zag) Dan Metode Steganografi Lsb Untuk Mengamankan Pesan Ke Dalam Citra Digital. 1–8. http://eprints.uty.ac.id/4888/
[14] Setiaji, A. (2020). RANCANG BANGUN APLIKASI PEMESANAN DESAIN JERSEY BERBASIS ANDROID DENGAN MENGGUNAKAN TEKNOLOGI FIREBASE (Studi Kasus : Konfeksi Minister). Jurnal Sistem Informasi Dan Sains Teknologi, 2(2). https://doi.org/10.31326/sistek.v2i2.664
[15] Sitepu, D. A., Nurhayati, & Khair, H. (2022). Implementasi Pengamanan Data Koperasi Menggunakan Algoritma Advanced Encryption Standard (AES). CITISEE 2016 Proceedings, 6(1), 37–40. https://citisee.amikompurwokerto.ac.id/assets/proceedings/paper/8__Amikom_Purwokerto_Implementasi_Pengamanan_Data_Koperasi_Menggunakan_Algoritma_Advanced_Encryption_Standard_(Aes).pdf
[16] Suparman, B. (2022). Aplikasi Pengamanan Data Menggunakan Kriptografi Dengan Metode Wake dan Algoritma Des Bebasis Java Desktop. OKTAL: Jurnal Ilmu Komputer Dan Sains, 1(07), 808–817. https://journal.mediapublikasi.id/index.php/oktal/article/view/777%0Ahttps://journal.mediapublikasi.id/index.php/oktal/article/download/777/304
[17] Waruwu, E. V., Nugroho, N. B., & Sonata, F. (2022). Penerapan Digital Signature Menggunakan Metode RSA Untuk Verifikasi Surat Keterangan Keaslian Ijazah SMA Swasta Bina Artha. Jurnal Cyber Tech, 1(1).
[18] Sandy, C. L. M., Fadlisyah, F., & Rizal, R. A. (2023). Sistem Informasi E-Voting Berbasis Web Menggunakan Metode RSA dan Base64. Jurnal CoSciTech (Computer Science and Information Technology), 4(1), 200-206.
[19] Putra, A. C., Simanjuntak, M., & Nurhayati, N. (2022). PENERAPAN ALGORITMA RIVEST SHAMIR ADLEMAN (RSA) UNTUK MENGAMANKAN DATABASE PROGRAM KELUARGA HARAPAN (PKH). JTIK (Jurnal Teknik Informatika Kaputama), 5(1), 76-84.
[20] Ardiansyah, A. F. (2023). Pemanfaatan Digital Signature pada Sertifikat Digital Berbasis Blockchain. Authentication Authorization Accounting Pendidikan Teknologi Informasi dan Teknologi Informasi, 1(2), 103-107.
[21] Muis, M. D., Sukarno, P., & Wardana, A. A. (2022). Analisis Dan Implementasi Sistem Pendeteksi Ijazah Dan Transkrip Palsu Dengan Menggunakan Ipfs Dan Smart Contract Blockchain. eProceedings of Engineering, 8(5).
[22] Azhari, M., Mulyana, D. I., Perwitosari, F. J., & Ali, F. (2022). Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES). Jurnal Pendidikan Sains Dan Komputer, 2(01), 163–171. https://doi.org/10.47709/jpsk.v2i01.1390
[23] Cristy, N., & Riandari, F. (2021). Implementasi Metode Advanced Encryption Standard (AES 128 Bit) untuk Mengamankan Data Keuangan. JIKOMSI [Jurnal Ilmu Komputer Dan Sistem Informasi], 4(2),75–85. https://ejournal.sisfokomtek.org/index.php/jikom/article/view/181%0A
[24] Ferdy Riza (2018) Analisa Frekuensi Hasil Enkripsi Pada Algoritma Kriptografi Blowfish Terhadap Keamanan Informasi
[25] Fitriyani A, Handayani R, & Widanengsih E. (2020). Sistem Pendukung Keputusan Pemilihan Jurusan Pada SMK YMIK Joglo Jakarta Barat Menggunakan Metode Simple Additive Weigting (SAW). Jtksi, 03(01), 11–19.
[26] Janis, J. W., Mamahit, D. J., Sugiarso, B. A., Rumagit, A. M., Elektro, T., Sam, U., & Manado, R. (2020). Rancang Bangun Aplikasi Online Sistem Pemesanan Jasa Tukang Bangunan Berbasis Lokasi. Jurnal Teknik Informatika, 15(1), 1–12. https://doi.org/10.35793/jti.15.1.2020.29023
[27] Kaban, R., Yunita, W., & Faradillah, Y. (2019). Aplikasi Pemesanan Tiket Bus Berbasis Android (Study Kasus : Pt . Als Terminal Pasar X Tanjung Beringin). Jurnal Manajemen …, 32(1).
[28] Lubis, R. S., Tulus, & Nababan, E. B. (2022). Pengamanan File Teks Menggunakan Algoritma RSA – LUC dan Algoritma Zig- Zag dalam Hybrid Crypto Sistem. InfoTekJar : Jurnal Nasional Informatika Dan Teknologi Jaringan, 6(2), 185–189.
[29] Marpaung, R., & Informasi, T. (2022). PENYIMPANAN DATA PRIBADI DENGAN METODE. 2(11), 1–14.
[30] Muharromin, M., Informatika, J. T., & Darma, U. B. (n.d.). Analisis Performance Web Application Firewall ModSecurity dan Shadow Daemon Dalam Keamanan Web Server Apache. 393–402.
[31] Nugroho, A. P., & Suseno, H. B. (2020). Keamanan Data Transaksi Nasabah Pada Aplikasi Bank Sampah Berbasis Web Menggunakan Algoritma AES. "QUERY: Jurnal Sistem Informasi Keamanan Data Transaksi

Nasabah Pada Aplikasi Bank Sampah Berbasis Web Menggunakan Algoritma AES.," 04(April), 9–17. http://jurnal.uinsu.ac.id/index.php/query/article/view/8007/3720
[32] Perbawa, K. A. (2022). Application of Linear Congruential Generator (LCG) Algorithm in Android Based Mathematics Education Game Penerapan Algoritma Linear Congruential Generator (LCG) dalam Game Edukasi Matematika Berbasis Android. Jurnal Komputer, Informasi Dan Teknologi, 2(1), 47–56.
[33] Prayudha, J., _ S., & _ I. (2019). Implementasi Keamanan Data Gaji Karyawan Pada PT. Capella Medan Menggunakan Metode Advanced Encryption Standard (AES). Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika Dan Komputer), 18(2), 119. https://doi.org/10.53513/jis.v18i2.150
[34] Ruing, M. O. I., & Ujianto, E. I. H. (2020). Penerapan Kombinasi Algoritma Kriptografi (Caesar, Vigenere, Zig-Zag) Dan Metode Steganografi Lsb Untuk Mengamankan Pesan Ke Dalam Citra Digital. 1–8. http://eprints.uty.ac.id/4888/
[35] Setiaji, A. (2020). RANCANG BANGUN APLIKASI PEMESANAN DESAIN JERSEY BERBASIS ANDROID DENGAN MENGGUNAKAN TEKNOLOGI FIREBASE (Studi Kasus : Konfeksi Minister). Jurnal Sistem Informasi Dan Sains Teknologi, 2(2). https://doi.org/10.31326/sistek.v2i2.664
[36] Sitepu, D. A., Nurhayati, & Khair, H. (2022). Implementasi Pengamanan Data Koperasi Menggunakan Algoritma Advanced Encryption Standard (AES). CITISEE 2016 Proceedings, 6(1), 37–40. https://citisee.amikompurwokerto.ac.id/assets/proceedings/paper/8__Amikom_Purwokerto_Implementasi_Pengamanan_Data_Koperasi_Menggunakan_Algoritma_Advanced_Encryption_Standard_(Aes).pdf
[37] Suparman, B. (2022). Aplikasi Pengamanan Data Menggunakan Kriptografi Dengan Metode Wake dan Algoritma Des Bebasis Java Desktop. OKTAL: Jurnal Ilmu Komputer Dan Sains, 1(07), 808–817. https://journal.mediapublikasi.id/index.php/oktal/article/view/777%0Ahttps://journal.mediapublikasi.id/index.php/oktal/article/download/777/304
[38] Waruwu, E. V., Nugroho, N. B., & Sonata, F. (2022). Penerapan Digital Signature Menggunakan Metode RSA Untuk Verifikasi Surat Keterangan Keaslian Ijazah SMA Swasta Bina Artha. Jurnal Cyber Tech, 1(1).
[39] Sandy, C. L. M., Fadlisyah, F., & Rizal, R. A. (2023). Sistem Informasi E-Voting Berbasis Web Menggunakan Metode RSA dan Base64. Jurnal CoSciTech (Computer Science and Information Technology), 4(1), 200-206.
[40] Putra, A. C., Simanjuntak, M., & Nurhayati, N. (2022). PENERAPAN ALGORITMA RIVEST SHAMIR ADLEMAN (RSA) UNTUK MENGAMANKAN DATABASE PROGRAM KELUARGA HARAPAN (PKH). JTIK (Jurnal Teknik Informatika Kaputama), 5(1), 76-84.
[41] Ardiansyah, A. F. (2023). Pemanfaatan Digital Signature pada Sertifikat Digital Berbasis Blockchain. Authentication Authorization Accounting Pendidikan Teknologi Informasi dan Teknologi Informasi, 1(2), 103-107.
[42] Muis, M. D., Sukarno, P., & Wardana, A. A. (2022). Analisis Dan Implementasi Sistem Pendeteksi Ijazah Dan Transkrip Palsu Dengan Menggunakan Ipfs Dan Smart Contract Blockchain. eProceedings of Engineering, 8(5).
[43] Lubis, R. S., Tulus, T., & Nababan, E. B. (2022). Pengamanan File Teks Menggunakan Algoritma RSA–LUC dan Algoritma Zig-Zag dalam Hybrid Crypto Sistem. InfoTekJar: Jurnal Nasional Informatika dan Teknologi Jaringan, 6(2), 186-189.
[44] Listiani, I., Nasution, M. S., Sari, W. I., & Nasution, A. B. (2022). PERANCANGAN KEAMANAN DATA PASIEN DI KLINIK KECANTIKAN RATU BEAUTY STUDIO MENGGUNAKAN METODE KRIPTOGRAFI RSA. Jurnal Informatika Teknologi dan Sains (Jinteks), 4(4), 437-443.
[45] Fauzan, D. A., & Fathurrozi, A. (2023). Perancangan Aplikasi Pengamanan Data Menggunakan Algoritma RSA (Rivest Shamir Adleman) dan AES (Advanced Encryption Standard) Berbasis Web. Journal of Informatic and Information Security, 4(1), 91-104.
[46] Sumiah, A., & Hakim, R. R. (2020). IMPLEMENTASI METODE LINEAR CONGRUENTIAL GENERATOR PADA GAME PUZZLE BERBASIS ANDROID. JEJARING: Jurnal Teknologi dan Manajemen Informatika, 5(1), 1-10.
[47] Abi Perbawa, K., & Diana, D. (2022). Application of Linear Congruential Generator (LCG) Algorithm in Android Based Mathematics Education Game. Jurnal Komputer, Informasi dan Teknologi (JKOMITEK), 2(1), 47-56.
[48] Putra, B. J. M., Fuâ, A., & Yuniarti, D. A. F. (2022). Analisa dan Rancangan Sistem Informasi Pariwisata Pacitan dengan UML dan ERD. Information System For Educators And Professionals: Journal of Information System, 7(1), 63-72.
[49] Andikos, A. (2019). Perancangan aplikasi multimedia interaktif sebagai media pembelajaran pengenalan hewan pada tk islam bakti 113 koto salak. Jurnal Sakinah, 1(1), 34-49.