**P-ISSN: 2656-1743 | E-ISSN: 2656-1735** **JURNAL RISET INFORMATIKA**
DOI: https://doi.org/10.34288/jri.v7i3.360 Vol. 7, No. 3. Juni 2025
**Accredited rank 4 (SINTA 4), excerpts from the decision of the DITJEN DIKTIRISTEK No. 230/E/KPT/2023**

# IMPLEMENTATION OF RSA ASYMMETRIC CRYPTOGRAPHY USING GPG AND KLEOPATRA FOR SCHOOL DATA SECURITY

**Ayu Pratiwi[-1], Muhlis Tahir[-2], Nawafilillah[-3], Ach. Almas Alvaradis[-4]**

[1]Pendidikan Informatika / Fakultas Keguruan dan Ilmu Pendidikan
Universitas Trunojoyo Madura
220631100052@student.trunojoyo.ac.id [1)], muhlis.tahir@trunojoyo.ac.id [2*)],
220631100057@student.trunojoyo.ac.id [3*)], 220631100056@student.trunojoyo.ac.id [4*)]

**Abstract**

Digital transformation drives the need for reliable data security systems to protect sensitive information from unauthorized access. This study aims to implement and analyze the use of the RSA cryptographic algorithm based on GPG (GNU Privacy Guard) software and the Kleopatra interface in securing school data. The research method employed is descriptive experimentation with a qualitative approach, conducted at SMK Al-Aziziyah Kwanyar in April 2025. The simulation includes RSA key pair generation, public key exchange, encryption and decryption of school digital data, and digital signature testing. The results indicate that the encryption process using the public key and decryption using the private key are effective and secure. The use of Kleopatra has proven to facilitate key management and cryptographic processes visually. This study emphasizes that the combination of RSA, GPG, and Kleopatra is a practical and efficient solution for data protection in educational environments and can serve as a reference for other institutions in implementing asymmetric cryptography-based digital data security.

Keywords: Cryptography, RSA, GPG, Data Security, Encryption.

***Abstrak***

*Transformasi digital mendorong kebutuhan akan sistem keamanan data yang andal untuk melindungi informasi sensitif dari akses tidak sah. Penelitian ini bertujuan untuk mengimplementasikan dan menganalisis penggunaan algoritma kriptografi RSA berbasis perangkat lunak GPG (GNU Privacy Guard) dan antarmuka Kleopatra dalam mengamankan data sekolah. Metode penelitian yang digunakan adalah eksperimen deskriptif dengan pendekatan kualitatif, dilakukan di SMK Al-Aziziyah Kwanyar pada April 2025. Simulasi mencakup pembuatan pasangan kunci RSA, pertukaran kunci publik, enkripsi dan dekripsi data digital sekolah, serta pengujian tanda tangan digital. Hasil menunjukkan bahwa proses enkripsi dengan kunci publik dan dekripsi dengan kunci privat berjalan efektif dan aman. Penggunaan Kleopatra terbukti memudahkan manajemen kunci dan proses kriptografi secara visual. Penelitian ini menegaskan bahwa kombinasi RSA, GPG, dan Kleopatra merupakan solusi praktis dan efisien untuk perlindungan data di lingkungan pendidikan, serta dapat dijadikan acuan bagi institusi lain dalam menerapkan keamanan data digital berbasis kriptografi asimetris.*

*Kata kunci: Kriptografi, RSA, GPG, Keamanan Data, Enkripsi.*

## INTRODUCTION

Digital transformation has fundamentally altered the way data is stored and managed, with most information now maintained in digital formats that are easily accessible anytime and anywhere. While this shift offers numerous advantages, it also introduces significant security challenges. Digital data is inherently vulnerable to various threats, including unauthorized access, data breaches, and cyberattacks. Malicious actors can exploit these vulnerabilities to commit cybercrimes, potentially leading to substantial harm for individuals, organizations, and institutions. This underscores the critical need for robust data security measures, such as encryption, access controls, and regular security audits, to protect sensitive information in the digital age (Mido, Iman, & Ujianto, 2022; Wahyudi, Hartama, Kirana, Sumarno, & Gunawan, 2022). Data security plays a crucial role in ensuring that sensitive information is accessible only to authorized individuals. This principle, known as confidentiality, is fundamental in protecting data from unauthorized access and potential breaches. Implementing robust security measures, such as encryption, access controls, and authentication protocols, helps maintain the

P-ISSN: 2656-1743 |E-ISSN: 2656-1735
DOI: https://doi.org/10.34288/jri.v7i3.360
Accredited rank 4 (SINTA 4), excerpts from the decision of the DITJEN DIKTIRISTEK No. 230/E/KPT/2023

confidentiality of information, thereby safeguarding privacy and maintaining trust in digital systems (Maulana & Simanjorang, 2021).

One of the fundamental techniques employed to ensure data confidentiality and integrity is cryptography. Cryptography involves securing messages by transforming readable information into an unreadable format using various algorithms, so that only authorized parties can access and understand the content. This process ensures that sensitive information remains protected from unauthorized access and tampering, thereby maintaining its confidentiality and integrity. Cryptographic methods are essential in safeguarding digital communications and data in today's interconnected world (Solihin & Krisna, 2022). Cryptography is the practice of securing information and communications by converting data into a coded format that only authorized individuals can decipher. This process involves transforming readable data (plaintext) into an unreadable format (ciphertext) using encryption algorithms, and then converting it back to readable form through decryption. Cryptography ensures that sensitive information remains confidential and maintains its integrity during transmission over both public and private networks (Irawan & Rachmawanto, 2021). Cryptographic algorithms are categorized into two main types: symmetric key algorithms and asymmetric key algorithms. (Simangunsong & Syahrizal, 2024). This algorithm employs a single key for both encryption and decryption processes, hence it is often referred to as a single-key algorithm (Alrido, Nugroho, & Perangin-Angin, 2021). Asymmetric cryptographic algorithms utilize a pair of distinct keys for the encryption and decryption processes. Encryption is performed using a public key, which is openly accessible, while decryption requires a private key that remains confidential and is known only to authorized parties. Due to the public availability of the encryption key, this method is also referred to as public-key cryptography (Putra, Raihana, Mondong, & Kardian, 2023). Asymmetric cryptography offers a significant advantage by employing a pair of keys public and private to ensure that transmitted data can only be accessed by the intended recipient possessing the corresponding private key. This mechanism guarantees data security during transmission and restricts access solely to authorized parties. By keeping the private key confidential and openly sharing the public key, asymmetric encryption facilitates secure communication without the risks associated with key distribution in symmetric systems. This approach is foundational to secure digital interactions, including email encryption, digital signatures, and secure web browsing (Arif & Nurokhman, 2023).

One of the most widely used asymmetric cryptographic methods to date is the RSA (Rivest Shamir Adleman) algorithm, which falls under the category of public key algorithms (Siregar, Nugroho, & Sigalingging, 2023). RSA is an asymmetric cryptographic algorithm known for its high level of security, primarily due to the significant difficulty involved in factoring large composite numbers (Annisa, Seta, & Falih, 2022). The RSA algorithm is an asymmetric cryptographic method that employs two distinct keys: a public key for encryption and a private key for decryption (Putri & Juliasari, 2022; Tarigan, Fitri Boy, & Mariami, 2021).

To implement RSA in real-world applications, tools are needed to facilitate practical data encryption and decryption. GPG (GNU Privacy Guard) is one such software that enables users to implement the RSA algorithm effectively. GnuPG is a free and comprehensive tool that implements the OpenPGP standard as defined by RFC4880 (also known as PGP) (Alhidaifi, Asghar, & Ansari, 2024). GPG is an open-source software that enables the secure encryption and signing of data or communications. It uses RSA public keys for encryption and private keys for decryption.

Kleopatra is a graphical interface designed to simplify the management of GPG keys. With Kleopatra, users can easily create, import, and export RSA keys. It also allows users to encrypt and decrypt files directly. Additionally, Kleopatra can be used to sign and verify digital signatures, which serve as a form of non-repudiation, ensuring that the sender cannot deny having sent a document once it is declared valid (Suharya & Widia, 2020). All of this is made possible through RSA implemented by GPG with the Kleopatra interface. By combining RSA, GPG, and Kleopatra, schools or institutions can easily implement asymmetric cryptography to secure sensitive data, such as student records or other important information, thereby preserving the confidentiality and integrity of valuable.

Several previous studies have explored the implementation of cryptographic algorithms for data security in the education sector. Research by (Hulu, 2024; Maulana & Simanjorang, 2021) a study conducted at SMA Swasta Jaya Krama Beringin underscores the importance of securing students' personal data using the RC4 algorithm. This method integrates the Key Scheduling Algorithm (KSA) to generate a pseudo-random key stream and applies the XOR operation for encryption and decryption,

thereby maintaining the confidentiality of student information. Conversely, research at MTs Daarul Falah by (Sugiarto & Purwanto, 2022) implemented the RSA algorithm within a Java-based desktop application to encrypt critical files, including teacher data, exam questions, and student scores. The findings demonstrated RSA's effectiveness in safeguarding documents against unauthorized access. Additionally, research has explored the use of hybrid cryptosystems that combine symmetric and asymmetric encryption methods to enhance data security. For example, integrating algorithms like IDEA (International Data Encryption Algorithm) with RSA has been studied to improve the protection of sensitive information, such as students' SNMPTN enrollment data. These hybrid approaches leverage the speed of symmetric encryption and the secure key distribution of asymmetric encryption, providing layered protection against unauthorized access (Nizatsary, Seta, & Wahyono, 2022). Another study reviewed the effectiveness of RSA and Blowfish in securing confidential messages. While each algorithm produced different encryption results, both ensured the confidentiality of the message content (Rahayu, Ardana, Pramudhita, Syafitri, & Sirega, 2024). Another study explored the combination of the Caesar Cipher and RSA algorithms to secure student grade data. The results indicated that this dual-encryption approach effectively transformed plaintext into ciphertext that is difficult to decipher without the appropriate decryption processes (Aulia Putri, Hesti, & Aryanti, 2020). Although various algorithmic approaches have been researched, the use of user interfaces such as Kleopatra in the context of file encryption in educational environments remains underexplored, despite the potential of these tools to offer practical and cost-effective solutions for securing digital data.

Based on the explanation above, the purpose of this study is to apply the RSA algorithm using GPG and Kleopatra to secure school data. This study will explore how the encryption and decryption processes using RSA can be carried out effectively, as well as assess the ease of use of GPG and Kleopatra software in the context of securing digital data used in educational institutions. With this research, it is hoped that schools or other institutions can better understand the benefits of applying asymmetric cryptography to improve the security of the data they manage.

## RESEARCH METHODS

### Types of research

This study utilizes a descriptive experimental method within a qualitative framework. The researcher performs a comprehensive simulation of RSA implementation using GPG (GNU Privacy Guard) software along with the Kleopatra interface. The aim is to outline the steps and processes of encrypting and decrypting data with RSA while assessing the convenience and effectiveness of this cryptographic technique in a school setting.

### Timeline and Location

This study was conducted in April 2025 at SMK Al-Aziziyah Kwanyar, utilizing Windows 10 and Windows 11 operating systems, along with the Gpg4win software suite and the Kleopatra interface.

### Research Subjects

The subjects of this study are digital school data, including student records, grade files, and other documents, which will be simulated for encryption and decryption processes. Additionally, the simulation involves two roles: the Administrative Staff (TU) as the data sender and the Teacher as the data recipient.

### Procedure

The research was conducted through the following steps:

1. Download and install the Gpg4win software package, which includes GnuPG and Kleopatra.
2. Generate an RSA key pair (3072-bit) using the Kleopatra interface.
3. Export the public key and distribute it to the second party.
4. Use the public key to encrypt school data.
5. Use the private key to decrypt the data.
6. Test digital signatures and verify files.
7. Attempt to breach the encrypted data.
8. Document the results of each step with screenshots and process explanations.

### Data, Instruments, and Data Collection Techniques

The data utilized in this study comprises simulated school files in .pdf format. The instruments employed include:

1. Two laptops operating on Windows 10 and Windows 11.
2. Gpg4win software suite (encompassing GPG and Kleopatra).
3. School data files.

Data collection was conducted through documentation of the process via screenshots and narrative notes.

P-ISSN: 2656-1743 |E-ISSN: 2656-1735
DOI: https://doi.org/10.34288/jri.v7i3.360
Accredited rank 4 (SINTA 4), excerpts from the decision of the DITJEN DIKTIRISTEK No. 230/E/KPT/2023

### Data Analysis Techniques

The collected data were analyzed using a descriptive qualitative approach, focusing on detailing each process based on the outputs displayed in Kleopatra and the file system. The analysis encompassed evaluating the effectiveness of the encryption process, the authenticity of digital signatures, and assessing the usability of the GPG software and Kleopatra interface in the context of securing school data.

## RESULTS AND DISCUSSION

### Installation of GPG and Kleopatra

The installation process of GPG and Kleopatra was carried out on the Windows operating systems of both the teacher's and administrative staff's laptops. Kleopatra serves as the graphical user interface for GPG, facilitating key management and cryptographic operations for users.

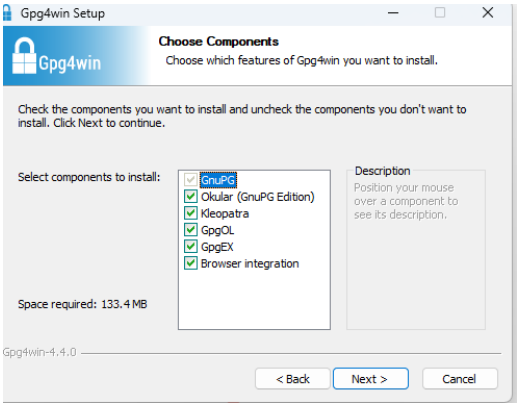


Figure 1. Installation of GPG and Kleopatra Applications

This installation process serves as the foundational step prior to generating and utilizing RSA keys. Upon completion of the installation, the applications are ready for key creation and encryption management.

### RSA Key Pair Generation

The RSA key pairs for both the administrative staff and the teacher were generated using the Kleopatra interface on their respective laptops. During this process, users provided their personal information, such as name and email address. Subsequently, a passphrase was set to enhance security, which is required when transferring the private key to another device. This measure ensures that only trusted individuals possess the private key.

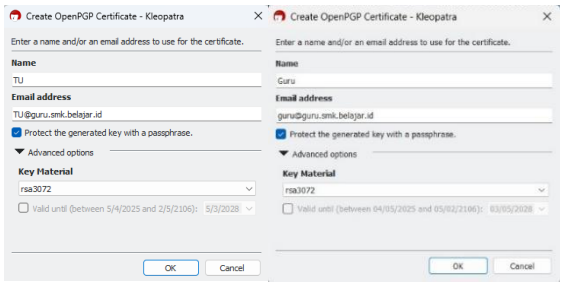


Figure 2. RSA Key Pair Generation for Administrative Staff and Teacher Using Kleopatra

An RSA key pair consists of a public key and a private key. The public key is used for encrypting data, while the private key is used for decrypting it. Kleopatra facilitates the export and import of keys, allowing secure sharing between parties. Among the available key materials in Kleopatra, the RSA 3072-bit option was selected due to its high compatibility and stability, making it suitable for securing school data.

### Public Key Exchange

The teacher's public key was exported and transferred to the administrative staff via flash drive or email. Upon receipt, the administrative staff utilized Kleopatra to import the key.

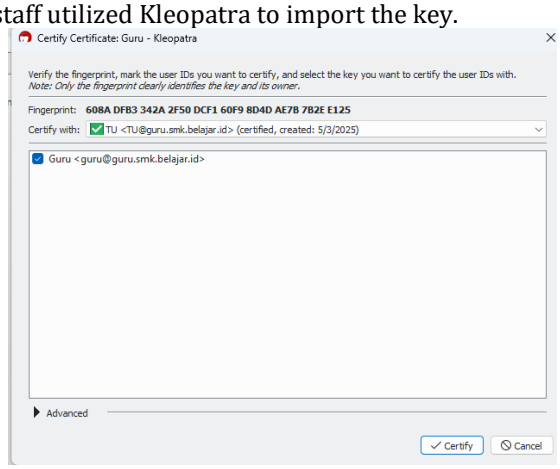


Figure 3. Importing the Teacher's Public Key into the Administrative Staff's Kleopatra

The public key received from the teacher was imported into the administrative staff's Kleopatra interface. Following the import, the administrative staff entered their passphrase to enable the use of the teacher's public key and to certify its authenticity.

### Encrypting School Files Using a Public Key

In this phase, a simulated school data file was encrypted using the teacher's public key, which

had been previously imported by the administrative staff.

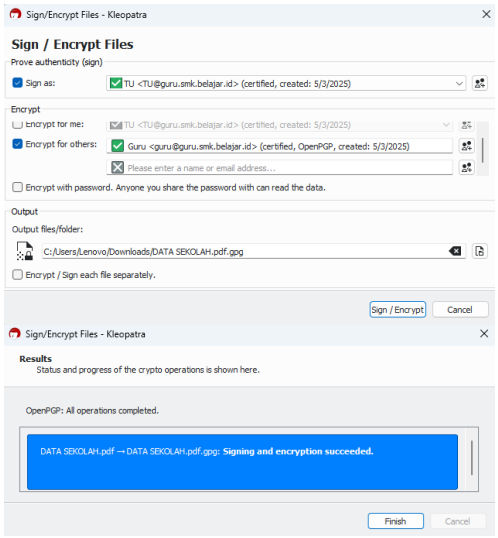


Figure 4. ncrypting School Data File Using the Teacher's Public Key

During the file encryption process using Kleopatra, several important settings were configured to ensure data security and authenticity. The "Prove authenticity (sign)" option was selected under the "Sign as" section to add a digital signature, which serves to verify the sender's identity and confirm that the file has not been altered, thereby ensuring its authenticity and integrity. The "Encrypt for me" option was checked to allow the sender to decrypt the encrypted file later if necessary, ensuring that the sender retains access to the encrypted content. Additionally, the "Encrypt for others" option was selected, and the recipient's public key (in this case, the teacher's) was chosen to ensure that only the designated recipient can decrypt and access the file's contents. The result of this encryption process was a file with a .gpg extension, indicating that it is encrypted and cannot be opened without the corresponding private key. This process exemplifies the application of the confidentiality principle in cryptography. Furthermore, by including a digital signature, the process also upholds the principles of authenticity and data integrity.

**Decrypting Files Using a Private Key**

In this phase, the encrypted file created by the administrative staff (TU) was transferred to the teacher via email or flash drive for decryption using the teacher's private key.

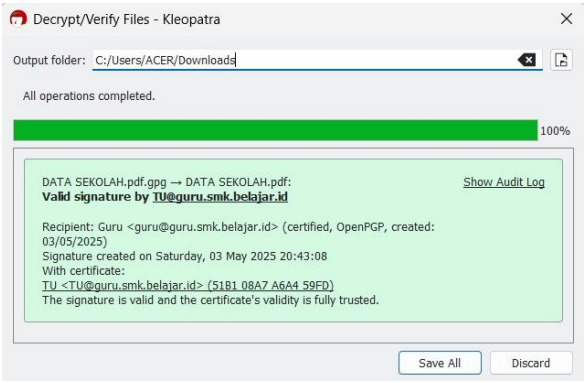


Figure 5. File Decryption Process Using a Private Key

Upon successful decryption, Kleopatra displays the message "Valid signature," indicating that the file was signed with a trusted key and has been restored to its original form. If the message "The data could not be verified" appears, it suggests that the digital signature cannot be verified due to the absence of the sender's public key. Additionally, the error "Decryption not possible: No secret key" signifies that decryption has failed because the corresponding private key is unavailable. This process underscores that only the rightful owner of the private key can access the encrypted data, thereby ensuring the security and confidentiality of the information.

**Simulating an Attack: Corrupted Data During Transmission**

In this simulation, an encrypted file created by the administrative staff (TU) was intentionally altered using a text editor by deleting several characters within the file. This modification aimed to simulate a data corruption scenario during transmission. Subsequently, the teacher attempted to decrypt the tampered file using their private key.

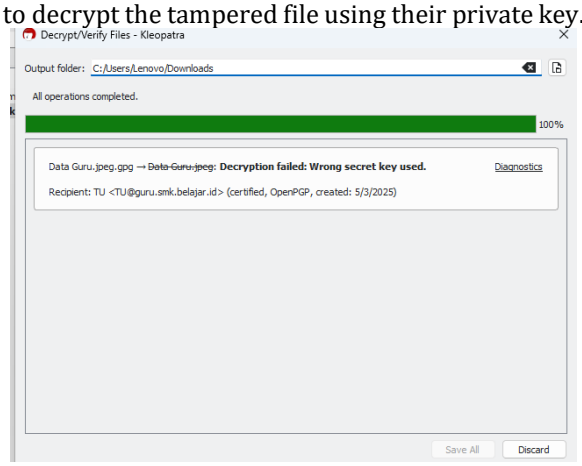


Figure 6. Decryption Result of a Corrupted File

Upon attempting decryption, Kleopatra displayed the message: "Decryption failed: Wrong secret key used." This error indicates that the decryption process failed due to the file's integrity being compromised. The corrupted file could not be decrypted, demonstrating that any unauthorized alterations render the data unreadable. This outcome underscores the robustness of the encryption system in maintaining data confidentiality and integrity, even in the face of potential attacks or data corruption during transmission.

**Data Evaluation of Results and Data Security**

Based on the entire process outlined above, the implementation of RSA encryption using GPG and Kleopatra has proven effective in maintaining data confidentiality, ensuring file integrity, and verifying the authenticity of the sender. This simulation demonstrates that this method is suitable for securing school data, such as student records, grades, and other important documents.

## CONCLUSIONS AND SUGGESTIONS

**Conclusions**

This study demonstrates that the implementation of RSA encryption via GPG and Kleopatra effectively secures data transmission between school administrative units. The encryption and decryption processes confirm that only parties possessing the corresponding key pairs can access confidential information. Furthermore, simulations involving data corruption scenarios reveal that this method preserves data integrity and authenticity. These findings indicate that GPG and Kleopatra are reliable tools for safeguarding important school documents, such as student records and grades.

**Suggestions**

Future researchers may explore the integration of GPG into automated school information systems to broaden its application. It is also recommended that educational institutions provide training for educators and staff on the use of cryptographic tools. Additionally, adopting digital signatures as a standard for verifying official school documents could enhance trust and security in administrative communications.

## REFERENCES

Siregar, S. J., Nugroho, N. B., & Sigalingging, H. (2023). Implementasi Algoritma Kriptografi RSA (Rivest Shamir Adleman) Dalam Pengamanan Data Gaji Karyawan Di Kantor BSPJI. *Agustus*, *22*, 528–538. Retrieved from https://ojs.trigunadharma.ac.id/index.php/jis/index

Alhidaifi, S. M., Asghar, M. R., & Ansari, I. S. (2024). A Survey on Cyber Resilience: Key Strategies, Research Challenges, and Future Directions. *ACM Computing Surveys*, *56*(8), 1–48. doi:10.1145/3649218

Alrido, M., Nugroho, N. B., & Perangin-Angin, M. I. (2021). Implementasi Algoritma Rivest Shamir Adleman (RSA) Untuk Keamanan Data Nilai Siswa Pada SMK Multi Karya Medan. *Jurnal CyberTech*, *4*(3). Retrieved from https://ojs.trigunadharma.ac.id/

Annisa, S., Seta, H. B., & Falih, N. (2022). Model Pengamanan Berkas Menggunakan Kriptografi Asimetris RSA Dan Algoritma Kompresi PPM Pada File Curriculum Vitae (CV), (2).

Arif, Z., & Nurokhman, A. (2023). Analisis Perbandingan Algoritma Kriptografi Simetris Dan Asimetris Dalam Meningkatkan Keamanan Sistem Informasi Comparative Analysis of Symmetric and Asymmetric Cryptographic Algorithms in Improving Information System Security. *JTSI*, *4*(2), 394–405.

Aulia Putri, N., Hesti, E., & Aryanti, A. (2020). Pengamanan Data Nilai Mahasiswa Menggunakan Algoritma Caesar Chiper dan RSA Berbasis Web. *Jurnal Rekayasa SIstem Komputer (RESISTOR)*, *3*(1), 61–70. Retrieved from https://s.id/jurnalresistor

Putra, N. B. N., Raihana, F. A., Mondong, W. M. A., & Kardian, A. R. (2023). Analisis Enkripsi Kriptografi Asimetris Algoritma RSA Berbasis Pemrograman Batch pada Media Flashdisk. *Jurnal Risat Sistem Informasi Dan Teknik Informasi (JURASIK)*, *8*(1), 142–154. Retrieved from https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

Hulu, S. (2024). Implementasi Algoritma Kriptografi Simetris Dalam Pengamanan Data Absensi Guru Dan Pegawai Pada Website Sekolah SMK Dharma Caraka Teluk Dalam Menggunakan RC4 Chiper. *KETIK : Jurnal Informatika*, *1*(04), 01–07. doi:10.70404/ketik.v1i04.58

Irawan, C., & Rachmawanto, E. H. (2021). Keamanan Data Menggunakan Gabungan Kriptografi AES dan RSA. *Proceeding SENIDU 2021*, 567–573.

Maulana, R., & Simanjorang, R. M. (2021). Implementasi Kriptografi Untuk Pengamanan Data Pribadi Siswa SMA Swasta Jaya Krama

Beringin Dengan Algoritma RC4. *Jurnal Nasional Komputasi Dan Teknologi Informasi*, *4*(6).

Mido, A. R., Iman, E., & Ujianto, H. (2022). Analisis Pengaruh Citra Terhadap Kombinasi Kriptografi RSA DAN Steganorafi LSB, *9*(2), 279–286. doi:10.25126/jtiik.202294852

Nizatsary, R. N., Seta, H. B., & Wahyono, B. T. (2022). Penerapan Keamanan Data Siswa Menggunakan International Data Encryption Algorithm (IDEA) dan Rivest Shamir Adleman (RSA), (2).

Putri, I. G. A. Y. A., & Juliasari, N. (2022). Implementasi Kriptografi File Ujian Siswa dengan Metode RSA Berbasis Website di SMAN 84 Jakarta. *Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)*, 130.

Rahayu, A., Ardana, A. P., Pramudhita, C., Syafitri, D., & Sirega, R. Z. (2024). Perbandingan Algoritma RSA dengan Algoritma Blowfish Pada Perancangan Aplikasi Keamanan Data. *Jurnal Ilmu Komputer Dan Sistem Informasi (JIKOMSI*, *7*(1), 203–207.

Simangunsong, S., & Syahrizal, M. (2024). Modifikasi Pembangkit Kunci Algoritma Berufort Cipher Berdasarkan Pembangkit Kunci CSPRING Berbasis RSA. *Jurnal Ilmu Komputer, Teknologi Dan Informasi*, *2*(2), 39–47. Retrieved from https://journal.grahamitra.id/index.php/jurikti

Solihin, M. Z., & Krisna, A. M. (2022). Implementasi Kriptografi Menggunakan Metode Algoritma RSA Pada Aplikasi Pengamanan Data Berbasis Java Desktop Untuk UD TIRTA SOEPER TELOER. *Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI) Jakarta-Indonesia*, 351–359.

Sugiarto, M., & Purwanto. (2022). Implementasi Algoritma RSA untuk Perancangan Aplikasi Berbasis Java Desktop pada MTs Daarul Falah. *Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI) Jakarta-Indonesia*, 344–350.

Suharya, Y., & Widia, H. (2020). Implementasi Digital Signature Menggunakan Algoritma Kriftografi RSA untuk Pengamanan Data di SMK Wirakarya 1 Ciparay. *Jurnal Informatika - COMPUTING*, *7*(1), 20–28.

Tarigan, Y., Fitri Boy, A., & Mariami, I. (2021). Aplikasi Smart School Dengan Pengamanan Data Menggunakan Metode RSA (Rivest Shamir Adleman) Pada PKBM Hanuba Medan. *Jurnal CyberTech*, *4*(2), 1–7. Retrieved from https://ojs.trigunadharma.ac.id/

Wahyudi, W., Hartama, D., Kirana, I. O., Sumarno, S., & Gunawan, I. (2022). Implementasi Algoritma Kriptografi Rivest Shamir Adlemen untuk Mengamankan Data Ijazah pada SMK Swasta Prama Artha Kab. Simalungun. *Jurnal Ilmu Komputer Dan Informatika*, *2*(1), 57–66. doi:10.54082/jiki.19