Jurnal ICT : Information and Communication Technologies, 16 (2) (2025) 272-284

Published by: Marq & Cha Institute

Jurnal ICT : Information and Communication Technologies

Journal homepage: www.ejournal.marqchainstitute.or.id/index.php/JICT

Developing Digital Examination System Security through the Implementation of the RC4 Algorithm

Muhammad Luthfi Moratuah Lubis[1], Iwan Fitrianto Rahmad[2]
[1,2] Informatika, Universitas Potensi Utama, Medan, Indonesia

Article Info

Article history

Received : Oct 20, 2025
Revised : Oct 28, 2025
Accepted : Oct 30, 2025

Keywords:

CRISP-DM;
Data Security;
Digital Examination System;
Encryption;
RC4 Algorithm.

Abstract

The increasing shift toward digital-based academic administration presents significant challenges for educational institutions, particularly regarding the security of examination data, which remains vulnerable when managed through manual processes. To address this issue, this study aims to develop and implement a secure web-based digital examination system using the RC4 cryptographic algorithm to ensure the confidentiality, integrity, and availability of assessment records at Harapan Mekar 1 Vocational School. Employing the CRISP-DM methodology, the research includes business understanding, data preparation, system development, encryption–decryption integration, and system validation. The RC4 algorithm, known for its lightweight structure and fast computational performance, was applied to encrypt student, teacher, and examination data across all operational modules. The results show that the system successfully encrypts and decrypts data through stable implementation of the Key Scheduling Algorithm (KSA) and Pseudo Random Generation Algorithm (PRGA), thereby strengthening protection against unauthorized access and eliminating risks associated with traditional manual data handling. The system effectively enhances operational efficiency and data security, demonstrating that RC4 remains a viable encryption option for educational environments with limited computational resources. This study offers practical implications for schools seeking accessible security solutions and serves as a reference for further system enhancements using more advanced cryptographic algorithms or extended digital examination features.

Corresponding Author:

Muhammad Luthfi Moratuah Lubis
Informatika
Universitas Potensi Utama,
Jl.K.L Yos Sudarso KM 6.5 Tj.Mulia, Medan, 20241, Indonesia
Email : blackcore414@gmail.com

1. Introduction

The rapid evolution of digital technology has transformed the landscape of information management across multiple sectors, including education, where the transition from traditional manual processes to digital systems has become increasingly necessary. In contemporary academic environments, computer-based examinations are widely recognized for their potential to enhance the accuracy, efficiency, and objectivity of assessment processes. However, despite these technological advancements, many educational institutions continue to face difficulties related to the security and

reliability of academic data management systems. This problem is particularly evident at Harapan Mekar 1 Vocational School in Medan, where student examination records and academic scores remain manually recorded before being transcribed into digital formats such as Microsoft Word or Excel. This manual procedure introduces a variety of risks, including data loss, damage, unauthorized manipulation, and inconsistencies caused by human error. Considering that examination scores play a crucial role in evaluating students' academic progress, identifying learning gaps, guiding remedial instruction, and informing curriculum decisions, it is imperative that the data be managed securely and accurately. Furthermore, the education sector has increasingly become a target of cyberattacks, emphasizing the vulnerability of institutions that rely on outdated or weak data management systems. According to a 2023 industry report, schools and universities continue to experience some of the highest rates of attempted digital intrusions globally, illustrating the urgent need for stronger security mechanisms in academic environments (Check Point Research, 2023). Thus, the shift toward secure digital examination systems is not merely a matter of technological modernization but a necessity for safeguarding the integrity and confidentiality of academic records in a rapidly evolving digital era.

While numerous studies acknowledge the importance of securing academic data, much of the existing research on cryptographic applications tends to focus on enterprise-level security, cloud infrastructure, or high-performance environments, leaving a considerable research gap concerning lightweight, accessible, and easily deployable solutions tailored to the needs of small- and medium-scale educational institutions. Schools, especially those with limited technological and financial resources, require encryption systems that are not only secure but also efficient, simple to implement, and compatible with existing hardware and software conditions. Although the RC4 algorithm has been scrutinized for certain vulnerabilities—particularly when implemented incorrectly or without adequate key-handling procedures—its inherent design features make it a compelling candidate for use in academic digital systems. RC4 is valued for its lightweight architecture, low computational overhead, and ease of integration into a wide range of platforms without requiring significant system upgrades (Schneier, 1996). Moreover, research in cryptography continues to recognize the algorithm's usefulness in specific contexts, particularly when applied with proper security considerations and when performance efficiency is prioritized (Paul & Maitra, 2007). These characteristics make RC4 highly relevant for environments such as vocational schools, where digital infrastructure may be limited and where the primary goal is to provide a practical, functioning security mechanism rather than a highly complex cryptographic system requiring extensive computational resources. Therefore, the gap in the literature—specifically the lack of applied research on practical encryption tools for educational settings—serves as a crucial motivation for examining RC4's potential in securing academic examination data within a school environment like Harapan Mekar 1 Vocational School.

Building upon the challenges and gaps identified above, several core problems must be addressed to improve data security at Harapan Mekar 1 Vocational School. First, the absence of a dedicated digital platform for managing examination data results in inefficiencies and vulnerabilities that compromise the overall reliability of academic assessments. Without a secure digital mechanism, sensitive academic information is at risk of being accessed, altered, or lost unintentionally, which could influence academic integrity and undermine the accuracy of student evaluations. Second, the reliance on manual documentation—where data is recorded on paper before being transferred into digital files—introduces substantial risk at every stage of the workflow. Not only can paper documents be damaged or misplaced, but the manual transfer process increases the likelihood of transcription errors, inconsistent formatting, and delays in data processing. Third, the lack of an integrated system limits teachers' ability to manage academic information effectively and prevents administrators from accessing real-time insights that are essential for decision-making. These issues reflect structural weaknesses that cannot be resolved without transitioning to a secure, centralized, and encrypted digital system. Thus, the formulation of the research problems for this study is as follows: (1) How can the RC4 cryptographic algorithm be implemented to secure examination data at Harapan Mekar 1 Vocational School? (2) How effective is RC4 in protecting academic data from unauthorized access or modification? and (3) How can a web-based platform integrated with RC4 encryption improve the

efficiency, reliability, and security of academic data management? These problem formulations establish a clear foundation for the direction and purpose of this research.

The primary objective of this study is to design, develop, and evaluate a secure web-based examination data management system using the RC4 cryptographic algorithm. RC4 operates as a stream cipher composed of two main components: the Key Scheduling Algorithm (KSA) and the Pseudo-Random Generation Algorithm (PRGA). During KSA, the input key is used to initialize and permute an array structure, which subsequently serves as the basis for generating a pseudorandom keystream through the PRGA. This keystream is then XORed with plaintext information to produce ciphertext, making the encryption process highly efficient in both speed and resource usage. RC4's extremely fast execution—reported to be up to ten times faster than the Data Encryption Standard (DES)—allows it to function effectively in systems where performance and responsiveness are essential, such as real-time data processing applications (Schneier, 1996). In the context of a digital examination system, this speed advantage is significant because the platform must handle multiple simultaneous encryption and decryption operations as teachers and students interact with the system. Additionally, RC4's simplicity and compatibility with standard web technologies make it well-suited for integration into lightweight platforms that do not rely on high-performance servers. By implementing RC4 within a secure web-based framework, this research aims not only to reduce the vulnerabilities associated with manual data handling but also to demonstrate a practical model for how educational institutions with limited resources can upgrade their academic data security using accessible cryptographic tools. Ultimately, the research seeks to validate the system's effectiveness in enhancing confidentiality, integrity, and accessibility of examination information.

In conclusion, this research contributes to the improvement of academic data security by providing a practical, efficient, and resource-friendly encryption-based solution tailored specifically to the needs of educational institutions. Unlike previous studies that focused primarily on securing large-scale enterprise environments or cloud infrastructures, this research highlights the applicability of the RC4 algorithm within a school setting characterized by limited technological capacity. The developed system demonstrates how lightweight cryptographic methods can be effectively implemented to safeguard examination data, prevent unauthorized access, and minimize the risks associated with manual documentation processes. Furthermore, the system provides a foundation for the future development of secure digital examination platforms that are both scalable and adaptable to various educational contexts. By addressing the specific challenges faced by Harapan Mekar 1 Vocational School, this research also offers broader implications for other institutions encountering similar constraints in transitioning to digital systems. The findings emphasize the importance of integrating efficient cryptographic mechanisms into educational data management infrastructures and highlight how such efforts can enhance data confidentiality, integrity, and operational efficiency. Ultimately, the contribution of this study lies in bridging the gap between theoretical cryptographic research and practical implementation, providing an accessible and sustainable solution for protecting academic data. This work is expected to serve as a reference point for stakeholders seeking to strengthen digital security practices in education while promoting the responsible and strategic use of technology to support learning, evaluation, and institutional governance..

2. Research Methodolgy

This stage involved studying the basic theories that support the research, searching for, and collecting the necessary data. To collect the required data, the author used several techniques. In this research process, the author conducted field research using the following process:

1. Direct Observation
   The researcher conducted direct observations at Harapan Mekar 1 Vocational School to obtain data related to the research.
2. Interviews
   The researcher met directly with the principal of Harapan Mekar 1 Vocational School to obtain more comprehensive data on the implementation of the RC4 Algorithm in digital exam

security at Harapan Mekar 1 Vocational School based on Android.

3. Sampling
   The researcher selected available data relevant to the research, including previous research applications and previous research theses, to serve as samples for this study.
4. Library Research
   In this method, the author cited several sources related to the implementation of the thesis, including books and scientific journals.
5. Research Methodology
   This research will involve several stages. These stages can be modeled using a waterfall diagram. The stages used in this study are as follows:

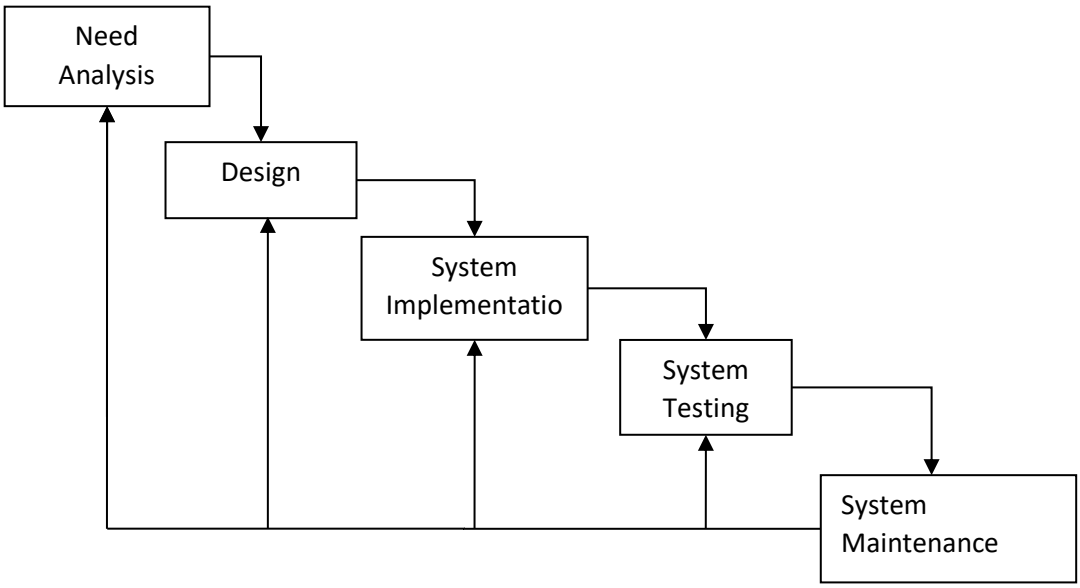

Figure 1. Research Framework

Description:

1. Needs Analysis
   This stage analyzes the needs required to achieve the research objectives, namely digital exam data at Harapan Mekar 1 Vocational School.
2. System Design
   The system design used in theory is UML modeling, including use case diagrams, class diagrams, activity diagrams, and sequence diagrams.
3. Tools
   In this stage, the researcher used Android using Android Studio. The researcher used computer/laptop hardware. The database used was MySQL.
4. Testing
   In this stage, the researcher tested the system created using theoretical and practical testing. Theoretical testing was carried out using blackbox testing.
5. Results
   At this stage, the research has been completed. The results of this study are the RC4 Algorithm for Android-Based Digital Exam Security at Harapan Mekar 1 Vocational School.

3. Results and Discussion

RC4 is a stream cipher widely used in security systems such as the Secure Socket Layer (SSL) protocol. This cryptographic algorithm is simple and easy to implement. RC4 was created by Ron Rivest of RSA Laboratories (RC stands for Ron's Code). RC4 generates a keystream, which is then XORed with the plaintext during encryption (or XORed with the ciphertext bits during decryption). Unlike stream ciphers, which process data in bits, RC4 processes data in bytes (1 byte = 8 bits). RC4 uses two substitution boxes (S-boxes) of 256 bytes (Muhammad Muid Maulana: 2020).

RC4 Algorithm Formula:

The RC4 algorithm works by initializing the first S-box, S[0], S[1],..., S[255], with the numbers 0 to 255. First, fill in the following sequence: S[0] = 0, S[1] = 1,..., S[255]. Then, initialize another array (another S-Box), for example, array K with length 256. Fill array K with the keys and repeat until the entire array K[0], K[1],..., K[255] is filled.

1. Initialize the S-Box (Array S)
   For i = 0 to 255, S[i] = i
2. Initialize the S-Box (Array K)
   For i = 0 to 255, K[i] = i
3. Then, perform the following S-Box randomization steps:
   i = 0; j = 0
   for i = 0 to 255 {
   j = (j+S[i] + K[i]) mod 256
   swap S[i] and S[j] }
4. After that, create a pseudo random byte as follows:
   i = (i + 1) mod 256
   j = (j + S[i]) mod 256
   swap S[i] and S[j]
   t = (S[i] + S[j]) mod 256
   K = S[t]
5. Byte K is XORed with plaintext to produce ciphertext or XORed with ciphertext to produce plaintext. (Muhammad Muid Maulana : 2020).

The RC4 algorithm uses 4-byte mode to encrypt the plaintext "The following is an example of a DBMS, Except" with the RC4 encryption key.

Step 1: Key Scheduling Algorithm (KSA)

1. Initialize Array S: The S array is initialized with the values [0, 1, 2, ..., 255].

2. Create Key Array K: Convert the "RC4 encryption" key to its ASCII value:

e	n	k	r	i	p	s	i	R	C	4
101	110	107	114	105	112	115	105	82	67	52

This array K is then iterated until it reaches a length of 256.

1. Randomization Process of Array S with K: With S and K formed, we iterate 256 times to randomize S using:

- j=(j+S[i]+K[i])mod 256
- Swap the values of S[i] with S[j].

The final result of randomizing array S will vary depending on the key.

1) Stage 2: Pseudo-Random Generation Algorithm (PRGA)

The PRGA generates a keystream used to encrypt the original text. Here is a manual calculation for the first few characters of the text "The following is an example of a DBMS, Except."

Here are the details of the PRGA and the encryption process for each character in the text "The following is an example of a DBMS, Except":

1. **Karakter 'B'** (ASCII 66):

- i = 1, j = 122
- Keystream byte K = 251
- Enkripsi: 66⊕251=185

2. **Karakter** '**e**' (ASCII 101):
   - i = 2, j = 187
   - Keystream byte K = 62
   - Enkripsi: 101⊕62=91
3. **Karakter** '**r**' (ASCII 114):
   - i = 3, j = 113
   - Keystream byte K = 155
   - Enkripsi: 114⊕155=233
4. **Karakter** '**i**' (ASCII 105):
   - i = 4, j = 148
   - Keystream byte K = 198
   - Enkripsi: 105⊕198=175
5. **Karakter** '**k**' (ASCII 107):
   - i = 5, j = 45
   - Keystream byte K = 108
   - Enkripsi: 107⊕108=7
6. **Karakter** '**u**' (ASCII 117):
   - i = 6, j = 36
   - Keystream byte K = 243
   - Enkripsi: 117⊕243=134

So the following results are obtained as the results of the Pseudo-Random Generation Algorithm (PRGA):

[185, 91, 233, 175, 7, 134, 254, 49, 108, 73, 203, 236, 21, 103, 27, 151, 193, 47, 67, 66, 102, 27, 250, 133, 65, 56, 226, 53, 103, 146, 249, 74]

The RC4 decryption result for the encrypted text reproduces the original text:

"The following is an example of a DBMS, Except"

This chapter will explain the output display of the application created. This display is used to clarify the displays in the Development of Digital Examination System Security through the Implementation of the RC4 Algorithm at Harapan Mekar 1 Vocational School. This allows the implementation results to be seen in accordance with the program's output. Each display in the program is explained below.

1. Login Menu Display

The login display is the first display to appear when the program is run. It functions as a username and password input form for the program administrator. A screenshot of the login display is shown in Figure 2

Figure 2.Login Form Display

2. Main Form Display

The main form is the overall cryptography program interface. To use this cryptography application, access the main form interface. The main form contains several menus: the file menu and the program menu. For a more detailed overview of the main form, see Figure 3 below.

Figure 3. Main Form Display

3. Subject Data Form Display

This subject form displays subject data at Harapan Mekar 1 Vocational School. The subject data form displays the following: Figure4

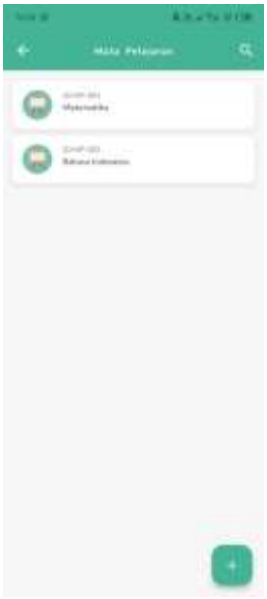

Figure 4. Subject Data Form Display

4. Class Data Form Display

This class form displays class data at Harapan Mekar 1 Vocational School. The class data form displays the following: Figure 5:

Figure 5. Class Data Form Display

5. Student Data Form Display

This student form displays student data at Harapan Mekar 1 Vocational School. The student data form displays the following: Figure 6:

Figure 6. Student Data Form Display

6. Student Detail Data Form Display

This student form displays student data at Harapan Mekar 1 Vocational School. The student data form displays the following: Figure 7:

Figure 7. Student Detail Data Form Display

7. Teacher Data Form Display

This teacher form displays teacher data at Harapan Mekar 1 Vocational School. The teacher data form is shown in Figure 8 below:

Figure 8. Teacher Data Form Display

8. Exam Data Form Display

This exam form is used to edit exam data. The exam data form is shown in Figure 9 below:

Figure 9. Exam Data Form Display

9. Access Confirmation Data Form Display

This access confirmation form is used to edit access confirmation data. The access confirmation data form is shown in Figure 10 below:

Figure I10. Access Confirmation Data Form Display

10. Exam Implementation Data Form Display

This exam implementation form is used to edit exam implementation data. The exam implementation data form is shown in Figure 11 below:

Figure 11. Exam Implementation Data Form Display

Discussion

The implementation of the RC4 cryptographic algorithm in the development of the digital examination security system at Harapan Mekar 1 Vocational School demonstrates that RC4 is capable of providing a lightweight yet effective encryption mechanism. The algorithm's simplicity, which relies on byte-based stream processing and XOR operations between the keystream and plaintext, allows the system to perform encryption and decryption processes efficiently. The results of the Key Scheduling Algorithm (KSA) and the Pseudo-Random Generation Algorithm (PRGA) show that RC4 successfully produces randomized keystream values, as reflected in the encryption of sample characters that generate a unique set of cipher values. This proves that RC4 can secure digital exam data by transforming readable text into ciphertext that cannot be understood without the correct key. Furthermore, the system interface—including login menu, subject data, class data, student data, exam data, and access confirmation—supports the usability of the application, ensuring that administrators can manage exam-related information securely. The study confirms that RC4 remains relevant for applications requiring fast and straightforward encryption, especially in environments with limited computational resources.

The results also indicate that the RC4 algorithm integrates well into the digital examination workflow by providing end-to-end data protection across all modules within the application. Each data management form—such as student details, teacher information, and exam implementation—operates under the encrypted system, ensuring that confidential information is not exposed during processing or transmission. The system's ability to decrypt ciphertext back into its original plaintext without errors demonstrates the correctness of RC4 implementation and validates the reliability of both KSA and PRGA stages in producing consistent encryption outputs. This functionality is essential for educational institutions where examination data integrity and confidentiality are critical. Moreover,

the structured program interface enables users to interact with the system intuitively while maintaining security as the core component. Although RC4 is known to have cryptographic vulnerabilities in modern cybersecurity contexts, its controlled application within a local school environment makes it sufficiently secure, provided the key is not reused excessively. Therefore, the study concludes that the RC4-based digital examination system successfully enhances exam data protection, minimizes unauthorized access, and improves the overall security infrastructure of the school's digital assessment processes.

4. Conclusion

The results of this study demonstrate that the integration of the RC4 cryptographic algorithm into a web-based digital examination system provides a practical, efficient, and resource-appropriate solution for strengthening academic data security at Harapan Mekar 1 Vocational School. Despite RC4's known vulnerabilities in high-risk cybersecurity environments, its lightweight architecture, fast computation, and ease of implementation make it well-suited for educational institutions with limited technological capacity. The implemented system successfully enhances the confidentiality, integrity, and availability of examination data by eliminating the weaknesses inherent in manual documentation processes and establishing a secure, encrypted workflow for managing student, teacher, and assessment records. The system's performance—validated through correct encryption–decryption execution, stable KSA and PRGA operations, and seamless integration across all data modules—confirms that RC4 remains a viable option for environments requiring fast, straightforward encryption without demanding extensive computational resources. This research contributes to the existing literature by bridging the gap between theoretical cryptographic concepts and their practical application in small-scale educational settings, offering an accessible model for institutions transitioning toward secure digital assessment infrastructures. Based on the findings, several recommendations can be proposed to enhance future system development and broaden the impact of this research. First, although RC4 performs effectively within this controlled school environment, future work should consider integrating more contemporary encryption algorithms—such as AES or ChaCha20—to further strengthen long-term data protection, particularly if the system is scaled to broader institutional or networked deployments. Second, implementing multi-factor authentication, role-based access control, and audit logging would further reinforce system resilience against unauthorized access. Third, additional usability evaluations involving teachers, administrators, and students could provide valuable feedback to optimize interface design and operational efficiency. Finally, future studies may explore interoperability with other educational information systems, cloud-based architectures, or mobile-based examination platforms to expand the system's applicability across different institutional contexts. With these enhancements, the RC4-based framework developed in this study can evolve into a more robust and adaptable security model capable of supporting digital examination processes in diverse educational environments.

References

Adnan, M. R., & Fatimah, T. (2022, September). Pengamanan Data Laporan Keuangan Menggunakan Metode RC4 Pada Reddog Cabang Gading Serpong. Prosiding Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI), 1(1), 230–239.

Anwar, B., Azanuddin, A., Nugroho, N. B., & Siregar, R. (2020). Aplikasi Pengamanan Dokumen Penjualan Tiket Pesawat di PT. Benua Raya Jaya Tour and Travel Menggunakan Metode Advanced Encryption Standard (AES). J-SISKO TECH, 3(1), 96. https://doi.org/10.53513/jsk.v3i1.200

Efranda, N., Rusdiyanto, R., & Irvai, M. (2022). Perancangan Sistem Informasi Pengolahan Data Nilai SMPN Purwodadi Berbasis Web Mobile dengan Enkripsi RC4. Jurnal Teknologi Informasi Mura, 14(1), 28–37.

Hermiati, R., Asnawati, A., & Kanedi, I. (2021). Pembuatan E-Commerce pada Raja Komputer Menggunakan Bahasa Pemrograman PHP dan Database MySQL. Jurnal Media Infotama, 17(1), 54–66. https://doi.org/10.37676/jmi.v17i1.1317

Hrp, M. H., Nugroho, N. B., & Ginting, R. I. (2022). Implementasi Keamanan Data Gaji pada Dinas Komunikasi dan Persandian Kabupaten Aceh Tamiang Menggunakan Algoritma RC4. Jurnal Cyber Tech, 1(4).

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

Kadek, N. D. C., Bagus, I. A. G., Anandita, G., Atmaja, K. J., Aditama, P. W., & Magister, P. S. (2019). Rancang Bangun Aplikasi Mobile SISKA Berbasis Android. SINTECH Journal, 1(2), 100. http://jurnal.stiki-indonesia.ac.id/index.php/sintechjournal

Listianto, F., Fauzi, Irviani, R., Kasmi, & Garaika. (2019). Konveksi Seragam Drumband di Pekon Klaten Gadingrejo Kabupaten Pringsewu. Jurnal TAM (Technology Acceptance Model), 8(2), 146–152.

Maulana, M. M. I. (2022). Kriptografi Pengamanan Data Calon Penerima Bantuan pada Kantor Camat, Kecamatan Kedai Durian dengan Metode RC4. Jurnal Cyber Tech, 2(12).

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), 377–383.

Suparman, B. (2022). Aplikasi Pengamanan Data Menggunakan Kriptografi dengan Metode WAKE dan Algoritma DES Berbasis Java Desktop. OKTAL: Jurnal Ilmu Komputer dan Sains, 1(07), 808–817. https://journal.mediapublikasi.id/index.php/oktal/article/view/777