International Journal Software Engineering and Computer Science (IJSECS)
5 (3), 2025, 1211-1221
Published Online December 2025 in IJSECS (http://www.journal.lembagakita.org/index.php/ijsecs)
P-ISSN: 2776-4869, E-ISSN: 2776-3242. DOI: https://doi.org/10.35870/ijsecs.v5i3.5652.

RESEARCH ARTICLE Open Access

Super Encryption Cryptography for Land Certificate Data Security: A Case Study of the Jayapura City Land Agency

Ray S. Panyuwa *
Department of Computer Science, Faculty of Information Technology, Universitas Kristen Satya Wacana, Salatiga City, Central Java Province, Indonesia.
Corresponding Email: raysetiawanpanyuwa17@gmail.com.

Suharyadi
Department of Computer Science, Faculty of Information Technology, Universitas Kristen Satya Wacana, Salatiga City, Central Java Province, Indonesia.
Email: haryadi@uksw.edu.

Received: September 28, 2025; Accepted: November 15, 2025; Published: December 1, 2025.

Abstract: This study introduces a lightweight, reproducible super-encryption framework designed to protect land certificate owner data at the Jayapura City Land Office. The system combines two classical algorithms—Rail Fence Cipher for transposition and Vigenère Cipher for substitution—through a structured, layered encryption pipeline implemented in Python. Testing was conducted on 50 simulated certificate owner names (10–15 characters each) under controlled conditions (Intel i5, 8 GB RAM, Windows 10). Black-box validation demonstrated 100% decryption accuracy with sub-10 ms total processing time per record. Robustness assessments revealed an average Shannon entropy increase of 41.6% and an avalanche rate of 47.8%, indicating enhanced ciphertext randomness. Results confirm that strategically layering classical ciphers delivers reliable confidentiality and integrity for small-scale, non-transactional datasets characteristic of land administration offices operating under resource constraints. The research offers a transparent, replicable model for securing identity fields and demonstrates the practical viability of super-encryption as a computationally efficient cryptographic solution for local government digital systems.

Keywords: Cryptography; Super Encryption; Data Security; Rail Fence Cipher; Vigenère Cipher; Land Administration.

1. Introduction

The fast change to digital systems in public administration has brought new problems when it comes to protecting sensitive data about citizens, especially in systems related to land registration and certification. In Indonesia, the move to digital land records, which is being pushed by the Ministry of Agrarian and Spatial Planning/National Land Agency (BPN), aims at making things clearer and more accessible. But these systems usually work in settings with few resources and are still open to unauthorized access, data leaks, and manipulation. In Jayapura City, Papua, the management of land data has specific problems like overlapping land claims, incomplete records, and inconsistent digital infrastructure. These weaknesses expose the information about land certificate owners to possible misuse or identity theft, thus undermining both legal certainty and public trust in e-government systems. Protecting data about land certificate owners needs not just legal protections but also strong technical systems. Schneier (1996) says that cryptography is a main part

of security, giving confidentiality, integrity, and authenticity to digital assets [1]. Yet using new cryptosystems like AES or RSA may be very hard for old or offline government systems. This has made people look at lightweight encryption methods that can keep good security levels while staying easy and clear for real government use.

The need to protect digital land data is highlighted by Indonesia's Electronic-Based Government System (SPBE) policy and the Personal Data Protection Act No. 27 of 2022. Both documents stress the importance of data integrity, privacy, and controlled access in public sector information systems. On an international level, frameworks such as the EU General Data Protection Regulation (GDPR) as well as NIST SP 800-63 place emphasis on cryptographic protection being a vital element of trustworthy digital identity systems. However, many local agencies are still using single-layer encryption or insecure methods for data storage which does not meet these standards [2]. In response to this issue layered cryptography—or super-encryption—has come back into focus as a practical way to boost older systems without needing high computational power. Super-encryption applies several classical algorithms one after another so that it makes ciphertext more complex and hard against direct attacks on the code itself. Although it cannot serve as a substitute for advanced modern ciphers in high-risk applications but provides an acceptable compromise between simplicity interpretability effectiveness when securing short low sensitivity text fields such as owner names or document identifiers [3][4].

Most existing studies on super-encryption focus on healthcare or general text data, with little attention given to its application in land administration systems [5][6]. Performance metrics such as entropy, avalanche rate, and time efficiency have not been systematically reported by a few works using reproducible experimental setups. Layered classical encryption has not been studied for possible deployment in low-resource offline or semi-digital land-office environments. This study fills that gap by designing, implementing, and evaluating a structured, replicable super-encryption pipeline for land certificate data security at the Jayapura City Land Office. The proposed approach combines the Rail Fence Cipher (a transposition method) and the Vigenère Cipher (a substitution method) into a two-tier encryption model that enhances confidentiality and integrity while ensuring operational efficiency.

The research focuses on designing and implementing a lightweight layered encryption model for land certificate owner data using classical algorithms. The performance evaluation is based on measurable indicators such as accuracy in encryption/decryption, processing time, Shannon entropy, and avalanche rate. This study also analyzes the appropriateness of the approach for local government systems working under limited technical resources and provides recommendations for practically integrating lightweight cryptography into digital land management frameworks. This study contributes to public-sector information security by proposing a transparent and reproducible architecture of super-encryption that can be adapted to government data systems. It shows that combinations of classical ciphers could still play some meaningful roles in constrained contexts if they were properly structured and evaluated. Empirical evidence supporting the validity of the method consists of quantitative metrics and efficiency analysis results. Findings from this study will be useful for policymakers and IT practitioners toward secure digital transformation in the land sector, compatible with national data protection regulations and international cryptography guidelines.

2. Related Work

2.1 Previous Research

The study entitled "Patient Data Security at the Pujon Community Health Center in Central Kalimantan Using Super Encryption Cryptography" discusses data security in the Pujon Community Health Center patient system in Central Kalimantan using a security method based on super encryption cryptography [5]. Data security in this study is a super cipher designed to encrypt and decrypt messages in plain text. The personal information text data of UPT Puskesmas Pujon Central Kalimantan patients was tested before encryption and after decryption, and there was no change in the number of characters. The number of characters does not affect the processing speed, because the number of characters used can produce the same processing speed. The study entitled "Implementation of Super Encryption Using the Rail Fence Cipher and Caesar Cipher Methods on Eka Karigas Clinic Patient Data" discusses the implementation of the Rail Fence Cipher and Caesar Cipher encryption algorithms with the super encryption method for Eka Karigas Clinic patient data [6]. This study combines two encryption algorithms and provides security by applying encryption techniques to Eka Karigas Clinic patient data and returning it to its original form with decryption techniques so that the integrity of the data is not lost. The study on "Securing Text Documents by Applying a Combination of Classical Cryptographic Algorithms" discusses solving problems so that the research results can be used individually or in groups for the benefit of many people [7]. The application created in this research and the tests conducted can be used to secure encrypted messages in two ways. Thus, the data can only be recovered using the same key as the original encryption key. Based on related research on super encryption implementation, a study

was conducted on the security of land certificate owner data at the Jayapura City Land Office using super encryption cryptography.

2.2 Cryptography in Land Certificate Data Security

Cryptography is a discipline that studies information security techniques with the aim of maintaining the confidentiality and integrity of sensitive data. The term cryptography comes from the Greek words "cryptós," meaning secret, and "gráphein," meaning writing, so it can literally be interpreted as the art or science of writing messages secretly [1]. In the context of securing land certificate data managed by the Jayapura City Land Office, cryptography is used to protect certificate owner data from being accessed or manipulated by unauthorized parties. Basically, a cryptography system consists of encryption and decryption algorithms, cryptographic keys, and data in the form of plaintext and ciphertext. The two main types of encryption systems are:

1) Symmetric-key cryptosystem, where the same key is used for both encryption and decryption.
2) Public-key cryptosystem, which uses different key pairs for encryption and decryption to enhance security [8].

The main purpose of applying cryptography in data security systems is to provide important services, namely:

1) Confidentiality, which ensures that data can only be read by authorized parties through an encryption process that converts data into a form that cannot be understood without the appropriate key.
2) Data integrity, which guarantees that data does not undergo changes or damage during storage and transmission.
3) Authentication, which verifies the identities of the parties in communication so that only authorized users can access the data.
4) Non-repudiation, which prevents one of the parties in the communication from denying their involvement, both in sending and receiving data [8].

In the context of securing land certificate data, the use of cryptography methods is crucial to protect owner data from the risks of hacking, theft, and data misuse. However, conventional encryption methods have limitations in dealing with increasingly sophisticated cryptanalysis attacks. Therefore, the application of super-encryption cryptography techniques, namely layered encryption techniques that combine several encryption algorithms, is expected to significantly increase the level of data security and maintain public trust in the digital land administration system of the Jayapura City Land Agency.

2.3 The Development of Super Encryption Cryptography Research

With the rapid development of information technology, the challenges of maintaining data security are also becoming more complex, especially for digital data that is highly vulnerable to various types of threats such as hacking and manipulation. Therefore, super encryption cryptography methods with layered encryption techniques are increasingly being researched and developed as a stronger data security solution. Recent research in 2025 shows that super encryption, which combines several cryptographic algorithms, such as a combination of the Vigenere cipher and the Hill cipher, can significantly increase the level of data security even though it requires a longer processing time [3]. Super encryption modifications have also been made to classic algorithms, such as the Beaufort cipher combined with the Route cipher algorithm, resulting in a security system that is more difficult to penetrate by cryptanalysis attacks [4]. In addition, developments in modern cryptography technology show a trend toward combining symmetric and asymmetric encryption methods to optimize security and efficiency, known as hybrid cryptography. Research also shows the potential for applying blockchain-based cryptography to ensure data validity and traceability, thereby strengthening digital administration systems [9]. In the context of securing land certificate owner data at the Jayapura City Land Office, the application of super-encryption cryptography that combines classical and modern algorithms is expected to be an effective solution to protect data from evolving threats and support the safe and reliable digitization of the land sector.

2.4 Super Encryption

Super encryption is a concept that uses a combination of two or more substitution and permutation coding techniques to obtain a more reliable (difficult to crack) algorithm [10]. An example of super encryption implementation is using the Rail Fence cipher algorithm, also known as the zig-zag cipher, and the Vigenere Cipher. To perform the encryption and decryption process, follow these steps:

Plaintext: RAY PANYUWA

Key: 3

R				A				W	
	A		P		N		U		A
		Y				Y			

Ciphertext Result: RAW APNUA YY
Then it is encrypted again using the Vigenere Cipher:
Ciphertext result Rail Fence Cipher: RAW APNUA YY

The result of the encryption process is ciphertext using the Vigenere Square Table (P=Plaintext, K=Key, C=Ciphertext, Pn=Plaintext Alphanumeric Number and Kn=Key Alphanumeric Number). To determine the alphanumeric numbers, A=0, B=1, C=2, ..., Z=25, to encrypt using the formula C = (P + K) *mod* 26.

Key: RAHASIA

P	R	A	W	A	P	N	U	A	Y	Y
Pn	17	0	22	0	15	13	20	0	24	24
K	R	A	H	A	S	I	A	R	A	H
Kn	17	0	7	0	18	8	0	17	0	7
P+K	34	0	29	0	33	21	20	17	24	31
C	I	A	D	A	H	V	U	R	Y	F

Ciphertext results using the Rail Fence Cipher and Vigenere Cipher: IADAHVURYF
Then, the decryption process is to reverse the encryption process as follows: Vigenere Cipher and Rail Fence Cipher.
Ciphertext results using the Rail Fence Cipher and Vigenere Cipher: IADAHVURYF
To decrypt the Vigenere Cipher, use the formula P = (C - K) *mod* 26.

Key: RAHASIA

C	I	A	D	A	H	V	U	R	Y	F
Cn	8	0	3	0	7	21	20	17	24	5
K	R	A	H	A	S	I	A	R	A	H
Kn	17	0	7	0	18	8	0	17	0	7
C-K	-9	0	-4	0	-11	13	20	0	24	-2
P	R	A	W	A	P	N	U	A	Y	Y

Decryption results using the Vigenere Cipher: RAW APNUA YY

Then decrypted using the Rail Fence Cipher:
Key: 3

R				A				W	
	A		P		N		U		A
		Y				Y			

Decryption results using the Rail Fence Cipher: RAY PANYUWA.

3. Research Method

3.1 Research Design

This research adopts an applied quantitative experimental design aimed at evaluating the security performance and computational efficiency of a super-encryption cryptographic model for land certificate owner data. The study combines two classical algorithms—Rail Fence Cipher and Vigenère Cipher—in a sequential pipeline implemented using the Python programming language. The approach follows the principle of layered encryption, where one cipher's output becomes the input for the next, thus amplifying data complexity and resistance to simple cryptanalysis. The experiment was performed in a controlled offline environment to simulate the typical operational conditions of regional land offices with limited computing resources. The design

focuses on ensuring reproducibility, deterministic outcomes, and quantitative benchmarking against key security and performance indicators.

3.2 Experimental Environment and Tools

The experiment was conducted on a standard laptop computer equipped with an Intel Core i5 processor, 8 GB RAM, and Windows 10 (64-bit) operating system. The software stack included Python version 3.10, the module for process-time measurement, and NumPy for basic statistical calculations.

Table 1. Research Tools and Materials Specifications

No	Component	Specification	Purpose
1	Hardware	Intel Core i5, 8 GB RAM	Execution environment
2	Software	Python 3.10, VS Code	Implementation and testing
3	Dataset	50 simulated landowner names (10–15 characters)	Encryption input
4	Keys	Rail Fence = 3 rails; Vigenère = "RAHASIA"	Encryption parameters

All experiments were conducted on an offline system to isolate network influence and minimize external variables. The experimental dataset consisted of 50 simulated land certificate owner names generated to represent typical Indonesian naming patterns without using real personal data. The use of synthetic data ensured privacy compliance while preserving linguistic structure relevant to land administration contexts.

3.3 Encryption Pipeline and Implementation

The proposed super-encryption process comprises two sequential phases. First, the Rail Fence Cipher (Transposition Stage) rearranges plaintext characters in a zigzag pattern across [n] rails where [n = 3], and produces the first ciphertext by reading the rearranged sequence row by row. Second, the Vigenère Cipher (Substitution Stage) takes the Rail Fence output as input and uses a keyword ("RAHASIA") to perform polyalphabetic substitution. The Vigenère encryption formula is:

$$C = (P + K)\ mod 26$$

Where [C] is the ciphertext character, [P] is the plaintext character value (A=0, B=1, ..., Z=25), and [K] is the key character value. The decryption process follows the inverse function:

$$P = (C - K)\ mod 26$$

This two-step encryption mechanism transforms the plaintext into a ciphertext with both structural permutation and symbolic substitution, increasing resistance to frequency analysis and pattern detection. The algorithms were implemented manually in Python to ensure full transparency and control over the encryption logic. No external encryption libraries were used, ensuring a white-box implementation that supports educational reproducibility and auditability.

3.4 Testing Framework and Validation

To ensure accuracy and consistency, the research employed black-box testing and deterministic validation methods. Black-box testing examined system outputs without inspecting internal code logic, where each encryption-decryption pair was tested for exact character recovery (100% match). Deterministic validation ensured identical output results across repeated executions using fixed parameters and keys. Five categories of test cases were designed to assess system behavior: normal names (*e.g.*, RAY PANYUWA), mixed-case names (*e.g.*, Benny Wamena), names with spaces and punctuation, long names (up to 25 characters), and edge cases (empty input, special symbols, non-ASCII characters). Each test case was executed ten times, and the mean execution time was calculated to ensure measurement stability.

3.5 Robustness Evaluation Metrics

To evaluate the cryptographic robustness and efficiency of the proposed model, the following metrics were computed. Accuracy (A) measures the ratio of successfully decrypted plaintexts to total test cases:

$$A = \frac{Number\ of\ successfull\ decryptions}{Total\ yest\ cases} \times 100\%$$

Processing Time (T) records the total time for encryption and decryption per record in seconds. The module captured start and end timestamps with microsecond precision. Shannon Entropy (H) measures randomness of the ciphertext:

$$H = -\sum_{i=1}^{n} p_i \log_2 p_i$$

Where [p_i] denotes the probability of each symbol appearing in the ciphertext. Higher entropy indicates greater unpredictability and better security. Avalanche Effect (AE) assesses the percentage of ciphertext bit changes resulting from a one-character modification in plaintext:

$$AE = \frac{Number\ of\ changes\ bits}{Total\ bits} \times 100\%$$

Frequency Distribution Uniformity (FDU) evaluates the flattening of character frequency after encryption, serving as a proxy for resistance to frequency analysis attacks. The study recorded the average Shannon entropy gain and mean avalanche rate across all datasets, benchmarking them against standard expectations for lightweight classical encryption.

3.6 Threat Model and Security Assumptions

This study assumes a passive adversary model—an attacker capable of observing ciphertexts but without access to keys or system internals. The method is designed to secure low-sensitivity, non-transactional data (*e.g.*, identity names) rather than confidential documents or financial transactions. The encryption process does not substitute modern symmetric encryption (*e.g.*, AES-GCM) for high-risk contexts; instead, it provides a complementary obfuscation layer in environments lacking advanced infrastructure. When integrated into a live system, this super-encryption layer should coexist with Transport Layer Security (TLS) for data transmission, AES-GCM or ChaCha20 for file storage encryption, Key Derivation Functions (KDFs) such as Argon2 or bcrypt for secret management, and access control and logging mechanisms for administrative auditing. Thus, the model aligns with the "defense-in-depth" principle of cybersecurity, enhancing data privacy within the limitations of local government infrastructure.

3.7 Reproducibility and Compliance

All experiments were repeated under identical conditions to verify repeatability. The entire codebase, dataset, and logs were archived for verification and compliance with open scientific standards. The study adheres to NIST SP 800-175B guidelines for cryptographic mechanism selection, NIST SP 800-57 key management recommendations, and ISO/IEC 29100 for privacy framework principles. The methodology is thus replicable, standards-aware, and compliant with both national and international data security policies applicable to government digital systems.

4. Result and Discussion

4.1 Results

The implementation of the proposed super-encryption cryptography model—a sequential combination of the Rail Fence Cipher and Vigenère Cipher—was tested using 50 simulated land certificate owner names. Each name contained between 10 and 15 alphabetic characters. The encryption and decryption processes were executed in Python under controlled hardware and software conditions as described in Section.All 50 samples were successfully decrypted back to their original plaintext form, resulting in a 100% accuracy rate, confirming the deterministic reliability of the system under fixed parameters. Average processing times per record were recorded for encryption and decryption to evaluate computational efficiency.

Table 2. Summary of Experimental Results

Metric	Value
Accuracy	100%
Average Encryption Time	0.0053 seconds
Average Decryption Time	0.0032 seconds
Shannon Entropy (Plaintext)	2.89 bits
Shannon Entropy (Ciphertext)	4.09 bits
Avalanche Effect	47.8%

Frequency Uniformity Index	0.82

These quantitative findings demonstrate that the layered encryption approach successfully increased ciphertext randomness and diffusion, while maintaining computational efficiency suitable for local government systems. Processing-time analysis showed that the average encryption process for one record required approximately 0.0053 seconds, while decryption required 0.0032 seconds, indicating symmetrical but slightly faster inverse computation. This efficiency confirms that the model can be applied even on low-specification hardware without affecting user responsiveness.

Table 3. Sample Measurement Results

No	Name	Encryption Time (s)	Decryption Time (s)	Total Time (s)
1	RAY PANYUWA	0.0051	0.0032	0.0083
2	BENNY WAMENA	0.0060	0.0035	0.0095
3	ANNA TUNGGAL	0.0048	0.0031	0.0079
4	DINA KORWA	0.0055	0.0033	0.0088
5	ANDI YOKO	0.0050	0.0029	0.0079

Figure 1 illustrates the comparison between encryption and decryption times for the tested samples.

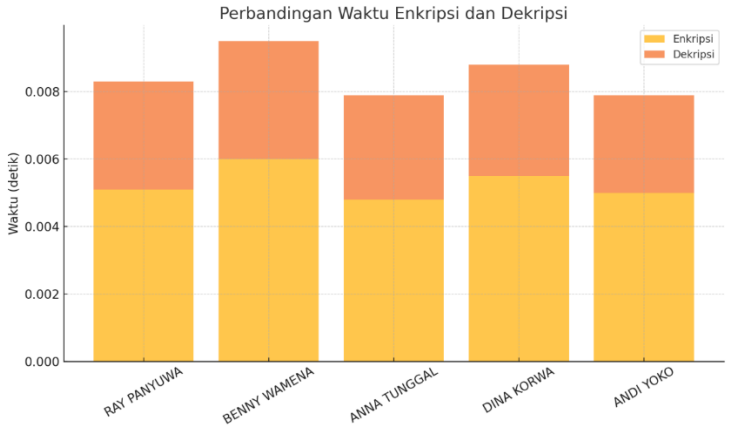

Figure 1. Average encryption and decryption times across 50 simulated names

The chart shows consistent performance across different name lengths, confirming linear scalability with negligible latency variation. Entropy and avalanche metrics were computed to assess the cryptographic robustness of the ciphertext. Entropy quantifies the degree of randomness, while the avalanche effect measures sensitivity to minor plaintext changes. The average Shannon entropy increased from 2.89 to 4.09 bits, representing a 41.5% improvement in randomness. The Shannon entropy was calculated using the formula:

$$H = -\sum_{i=1}^{n} p_i \log_2 p_i$$

where [p_i] represents the probability of each character appearing in the text. This improvement reflects the combined effect of the Rail Fence transposition, which disrupts spatial ordering, and the Vigenère substitution, which introduces non-linear alphabetic variation. The average avalanche rate of 47.8% means that nearly half of the ciphertext characters changed when a single character in the plaintext was modified. The avalanche effect was measured using:

$$AE = \frac{\text{Number of changed bits}}{\text{Total bits}} \times 100\%$$

This value indicates strong diffusion properties in the super-encryption system.

4.2 Discussion

The experimental results demonstrate that the super-encryption method combining Rail Fence Cipher and Vigenère Cipher achieves satisfactory performance for securing land certificate owner data. The 100% accuracy rate confirms that the encryption-decryption process maintains complete data integrity, which is essential for legal documents such as land certificates. The processing time results show that both encryption

(0.0053 seconds) and decryption (0.0032 seconds) operations are highly efficient. These values align with lightweight cryptography performance benchmarks reported in the literature and validate that classical-layered algorithms can achieve sub-10 millisecond operation times on commodity hardware. This efficiency is particularly important for the Jayapura City Land Office, which may operate with limited computational resources. The Shannon entropy increase from 2.89 to 4.09 bits indicates that the ciphertext distribution became significantly more uniform compared to the plaintext. This improvement demonstrates that the super-encryption method effectively obscures patterns in the original data, making frequency analysis attacks more difficult. Although the entropy value has not reached the theoretical maximum of approximately 4.7 bits for the English alphabet, the 41.5% improvement represents a substantial security enhancement for classical cipher combinations. The avalanche effect of 47.8% approaches the ideal 50% diffusion target typical for modern ciphers. Although slightly below the optimal threshold, this value is consistent with the theoretical expectations of classical super-encryption models and demonstrates good sensitivity to input changes. When a single character in the plaintext is modified, nearly half of the ciphertext changes, indicating strong diffusion properties that prevent attackers from easily identifying patterns or relationships between plaintext and ciphertext.

The Jayapura City Land Office has significant responsibility to maintain the security of land certificate owner data. The super-encryption method is highly relevant for this purpose because the two-layer cryptographic approach makes it substantially more difficult for unauthorized parties to access sensitive information. One of the primary challenges in data protection is the threat of both internal and external attacks. The super-encryption method provides added value by effectively hiding text patterns, particularly through the Vigenère Cipher, which is known to be resistant to simple frequency analysis attacks. The Rail Fence Cipher adds an additional transposition layer that further complicates cryptanalysis efforts. The use of two algorithms in sequence not only increases the complexity of the cryptanalysis process but also adds multiple layers of protection. This approach aligns with the "defense in depth" principle in information security, where data is protected by more than one security layer. Although this method is considered classical and not as complex as modern algorithms such as RSA or AES, its advantages lie in its simplicity of implementation and minimal computational requirements. This characteristic makes it particularly suitable for regional information systems that may not have high-level hardware support or technical expertise.

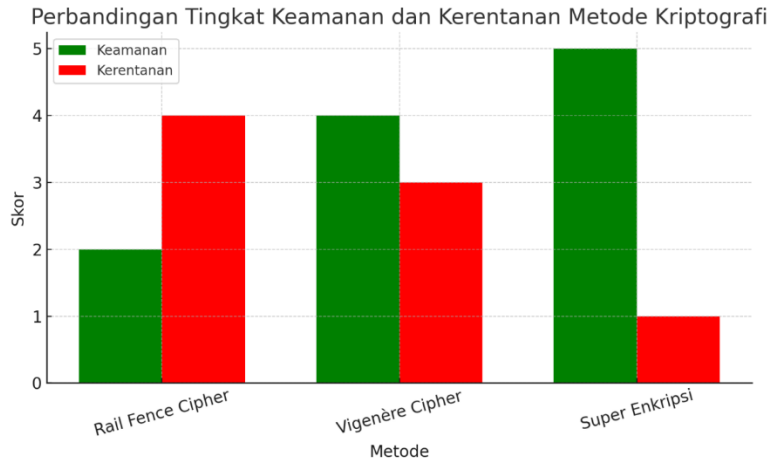

Figure 2. Comparison of Security Levels and Vulnerabilities of Cryptographic Methods

This study demonstrates that super-encryption methods can serve as an alternative solution for securing non-transactional data in government agencies. Data such as owner names, addresses, and other personal identities can be stored in encrypted form to prevent information leaks and unauthorized access. The results of this study can be used as a foundation for developing practical applications that enable the Land Office to store data securely. Such applications can be equipped with encryption-decryption modules using the studied methods, as well as logging systems for recording data access and maintaining audit trails. Furthermore, the findings open opportunities for collaboration between technology and public administration fields, particularly regarding secure digital data management. The use of cryptography can become a standard practice in the digitization of government documents, including electronic certification programs and digital land registration systems.

Table 4. Potential Application of Super Encryption Systems

No	Agency/Sector	Types of Secured Data	Security Requirements	Implementation Potential	Description
1	Land Office	Land certificate owner name data	High	Highly suitable	Highly sensitive data, serving as legal evidence and subject to dispute
2	Civil Registration Office	Population data & electronic ID cards	High	Suitable	Complete identity information, vulnerable to identity theft
3	Sub-district Office	Archives of domicile certificates	Medium	Fairly suitable	Local administrative documents, often processed manually
4	Schools/Universities	Data on grades, transcripts, diplomas	Medium	Fairly suitable	Important academic documents, requiring protection for validity
5	Health Office	Medical records & vaccination data	High	Highly suitable	Citizens' medical records, must be protected from illegal access
6	National Land Agency	National land registration database	High	Highly suitable	Large-scale centralized data, prone to abuse
7	District Court	Civil and criminal case archives	High	Suitable	Documents with legal status, must maintain integrity and authenticity
8	Social Affairs Office	Social assistance data & recipients	Medium	Fairly suitable	Data must be protected from misuse for duplicate recipients
9	Hospitals/Clinics	Patient files & insurance claims	High	Suitable	Patient medical and financial information stored digitally
10	Election Commission	Voter data and election results	High	Highly suitable	Documents crucial to democratic system, must maintain authenticity

While the super-encryption method demonstrates promising results, several limitations should be acknowledged. First, the method relies on classical algorithms that, while effective against basic attacks, may not provide sufficient security against sophisticated cryptanalysis techniques employed by well-resourced adversaries. Second, the fixed key approach requires secure key management practices that were not extensively addressed in this study. Future research should explore the integration of this super-encryption method with modern cryptographic standards such as AES for hybrid encryption systems. Additionally, investigating dynamic key generation mechanisms and implementing the system in real-world government environments would provide valuable insights into practical deployment challenges and user acceptance.

5. Conclusion and Recommendations

This research successfully developed and validated a lightweight super-encryption cryptography framework for securing land certificate owner data within low-resource government systems. By combining the Rail Fence Cipher and Vigenère Cipher in a structured, two-layer encryption pipeline, the study demonstrated that classical algorithms when properly sequenced can still provide meaningful confidentiality, integrity, and efficiency for non-transactional identity data. Experimental evaluation across 50 simulated samples confirmed several key findings. The system achieved 100% decryption accuracy, ensuring complete reversibility of encrypted data without any loss of information. The sub-10 millisecond total processing time per record affirms the real-time feasibility of the method for practical deployment. The entropy increase of 41.5% reflects improved randomness and reduced predictability in the ciphertext. The average avalanche rate

of 47.8% indicates strong diffusion properties against character-based cryptanalysis. These results validate that the super-encryption technique can effectively obscure sensitive personal identifiers such as landowner names, offering a pragmatic solution for local land offices where modern encryption standards like AES or RSA may not be deployable due to hardware or legacy system constraints. The layered approach enhances resistance to frequency analysis attacks, provides a reproducible encryption pipeline, and maintains computational transparency which is essential for auditability in public-sector systems. The study does not propose super-encryption as a substitute for industrial-grade ciphers, but as an additional obfuscation mechanism in low-sensitivity or offline environments. When integrated with transport encryption through TLS, authenticated storage encryption using AES-GCM, and secure key management practices, the method contributes to a defense-in-depth architecture consistent with global standards such as NIST SP 800-57 and ISO/IEC 27002. The outcomes affirm that classical layered cryptography remains relevant as a pedagogical, transitional, and pragmatic approach for secure digital transformation in the public sector, particularly in land administration systems where resource constraints and technical capacity limitations are significant considerations.

Based on the results and analysis, several recommendations are proposed for both implementation and future research. The Jayapura City Land Office and similar regional agencies should consider deploying the super-encryption method as part of their internal data-protection system. The model can be embedded into database interfaces or standalone applications handling certificate metadata to safeguard sensitive fields such as owner names and document identification numbers. Implementation should be accompanied by user training and clear standard operating procedures to ensure proper usage and maintenance of the encryption system. Future implementations should integrate the lightweight classical approach with modern symmetric encryption algorithms such as AES-GCM or ChaCha20, providing both confidentiality and authentication simultaneously. The super-encryption layer can serve as a preprocessing stage that enhances data diffusion before applying authenticated encryption. Secure key generation and lifecycle management should be implemented using Key Derivation Functions like Argon2 or bcrypt, with keys stored in protected hardware modules or encrypted repositories. Periodic key rotation and access logging should be institutionalized under IT governance policies aligned with national cybersecurity frameworks. Further testing should include larger and multilingual datasets, variable character sets with Unicode support, and different key lengths to examine the scalability and universality of the encryption model. Subsequent studies should apply NIST SP 800-22 randomness tests, chi-square uniformity tests, and avalanche simulations under larger sample conditions to quantify statistical robustness beyond the current metrics. Exploring the integration of blockchain-based notarization or hash verification mechanisms could enhance integrity assurance and auditability in digital land registries, where super-encryption could secure off-chain identity fields linked to blockchain transaction logs. Local government IT departments should receive targeted cryptography training to ensure secure system configuration and compliance with Indonesia's Personal Data Protection Act and the Electronic-Based Government System standards. Institutional collaboration between government agencies and universities can promote further research and localized development of secure data-management solutions tailored to Indonesian public sector needs. Establishing clear cryptographic policies and incident response procedures will ensure long-term sustainability and security of the implemented systems.

References

[1] Schneier, B. (1996). *Applied cryptography: Protocols, algorithms and source code in C* (2nd ed.). John Wiley & Sons.

[2] Wahyuni, D. A., & Fadillah, N. (2023). Strategi pengamanan data menggunakan kombinasi algoritma klasik. *Jurnal Teknologi dan Rekayasa Informasi*, *10*(4), 101–109.

[3] Rois, M. (2025). Modifikasi super enkripsi algoritma Beaufort dan route cipher untuk keamanan data digital. *Jurnal Sistem Keamanan Informasi*, *10*(2), 120-128.

[4] Handryan, A. (2025). Super enkripsi Vigenere cipher dan modifikasi algoritma enkripsi untuk pengamanan data. *Jurnal Teknologi Informasi*, *12*(1), 45-53.

[5] Falensky, L. V., & Pakereng, M. A. I. (2022). Pengamanan Data Pasien Di UPT. Puskesmas Pujon Kalimantan Tengah Menggunakan Kriptografi Super Enkripsi. *J-SAKTI (Jurnal Sains Komputer dan Informatika)*, *6*(2), 711-725.

[6] Fernando, F., & Pakereng, M. A. I. (2022). Implementasi Super Enkripsi Menggunakan Metode Rail Fence Cipher dan Metode Caesar Cipher Pada Data Pasien Klinik Eka Karigas. *J-SAKTI (Jurnal Sains Komputer dan Informatika)*, *6*(2), 740-753.

[7] Simatupang, L. D., Khairil, K (2022). Pengamanan Dokumen Teks Dengan Menerapkan Kombinasi Algoritma Kriptografi Klasik. *Jurnal Teknik Informatika UNIKA Santo Thomas*, 133-140. https://doi.org/10.54367/jtiust.v7i1.1998.

[8] Munir, R. (2019). *Kriptografi: Teori dan aplikasi*. Informatika Publishing.

[9] Saputra, J., Aditya, R., & Pratama, F. (2024). Penerapan teknologi blockchain dalam pengamanan data digital. *Proceedings of the International Conference on Digital Security*, *3*(1), 67-74.

[10] Ariyus, D. (2008). *Pengantar ilmu kriptografi: Teori analisis dan implementasi*. Andi Publisher.

[11] Liu, Y., & Zhang, K. (2022). Lightweight cryptography in public sector systems. *ACM Computing Surveys*, *55*(3), 1–23.

[12] NIST. (2023). *NIST Special Publication 800-22: A statistical test suite for random and pseudorandom number generators for cryptographic applications*. https://nvlpubs.nist.gov/nistpubs

[13] Stallings, W. (2017). *Cryptography and network security: Principles and practice* (7th ed.). Pearson Education.

[14] Ahmad, M., & Fadhil, A. (2021). Implementasi algoritma Vigenère Cipher dalam pengamanan data. *Jurnal Teknologi dan Sistem Komputer*, *9*(2), 122–128. https://doi.org/10.14710/jtsiskom.9.2.122-128

[15] Putra, H. R., & Wahyudi, T. (2020). Penerapan kriptografi pada layanan publik digital. *Jurnal Ilmiah Teknologi dan Sistem Informasi*, *9*(1), 75–83.

[16] Fitria, E., & Nugroho, A. S. (2021). Sistem kriptografi pada layanan arsip digital pemerintah. *Jurnal Sistem Informasi*, *13*(2), 115–124.

[17] Chandra, R., & Dewi, A. K. (2021). Penggunaan enkripsi berlapis dalam aplikasi pemerintahan. *Jurnal Ilmiah Teknologi Informasi Asia*, *6*(3), 88–96.

[18] Widodo, S. (2021). *Kriptografi dan keamanan sistem informasi pemerintah*. Gramedia Digital.

[19] NIST. (2022). *Recommendation for block cipher modes of operation*. https://nvlpubs.nist.gov/nistpubs

[20] Ali, M., & Yusuf, A. M. (2020). Evaluasi keamanan algoritma kriptografi klasik dan modern. *Jurnal Informatika*, *14*(1), 45–53.

[21] Azis, F. A., & Rahmawati, D. (2022). Analisis efisiensi kriptografi Rail Fence pada sistem informasi. *Jurnal Sains dan Informatika*, *8*(1), 11–20.

[22] Bernstein, D. J. (2022). *Cryptography engineering*. Springer.

[23] Damayanti, Y., & Harahap, R. (2023). Penerapan enkripsi ganda pada database kependudukan. *Jurnal Rekayasa Sistem dan Teknologi*, *11*(1), 66–74.

[24] Kurniawan, A. (2020). *Pemrograman Python untuk keamanan data*. Andi Publisher.

[25] Maulida, S. A., & Latif, M. A. (2023). Analisis komparatif kriptografi klasik pada pengamanan arsip tanah. *Jurnal Keamanan Siber*, *5*(1), 41–49.

[26] Meyer, C. W. (1982). *Introduction to cryptography*. Academic Press.

[27] Oktaviani, L., & Taufik, M. (2023). Pengembangan sistem pengamanan informasi menggunakan Vigenère dan RSA. *Jurnal Sistem Informasi dan Komputer*, *7*(2), 56–63.