SECURING LEGACY INDUSTRIAL SYSTEMS: A SYSTEMATIC REVIEW OF DES ENHANCEMENTS AND RNS APPLICATIONS IN CRYPTOGRAPHY (2020–2025)

BY

[1]Adebayo Aminat Omotayo & [2]Abdulrauf Uthman Tosho
Department of Computer Science, Faculty of Computing, Engineering and Technology
Email: ayakub@alhikmah.edu.ng, autosho@alhikmah.edu.ng

Abstract

Legacy industrial systems including Supervisory Control and Data Acquisition (SCADA) and other Industrial Control Systems (ICS) continue to depend on the Data Encryption Standard (DES), despite its age and documented weaknesses. Although DES offers speed and simplicity, especially in hardware-constrained environments, its 56-bit key and predictable structure leave it highly vulnerable to brute-force attacks. In recent years, researchers have worked on improving the security concern of the DES algorithm, such as key whitening, block expansion and mathematical computation of the DES process. An emerging area involves the use of the Residue Number System (RNS). RNS is a modular arithmetic that is known for parallelism operations and fault tolerance advantage. RNS has been applied in the field of cryptography to speed up computations and for data obfuscation, which makes it suitable for lightweight encryption process. However, most researchers concentrated on the application of RNS in public-key cryptographic algorithms and hardware acceleration, while its application in symmetric encryption especially DES remains rare. This review was guided by PRISMA 2020 standards which considered researches published between the year 2020 and year 2025, focusing on recent enhancement made on DES algorithm, the use of RNS in cryptography, and emerging approaches or methods for securing legacy systems. The gap in integrating RNS with DES was spotted as a novel idea for improving the security concern of outdated but still widely used ICS while avoiding computational complexity.

Keywords: Data Encryption Standard (DES), Residue Number System (RNS), Legacy Industrial Control System (ICS), Lightweight Cryptography, Cryptographic Security

Introduction

Over the years, the continuous proliferation of Legacy Industrial Control Systems (ICS) has raised a significant concern particularly with the continuous use of the outdated DES due to its simplicity. DES was standardized in the 1970's for secure communication. However, as technology advances, DES is no longer sufficient for secure communication because it is prone to brute force attack. DES uses 56-bit key for its encryption and decryption process which can be successfully guessed in a matter of minutes with the use of the modern-day computing capabilities (Matta et al., 2021).

However, because of its simplicity and closeness to industrial communication protocols, DES is still used in SCADA systems, legacy embedded devices, and ICS contexts (Bhardwaj & Sharma, 2022). Many researchers have worked on improving these weaknesses of the DES algorithm. These include DES variations that use dynamic keys or block expansion to increase resilience to known attacks; key whitening and S-box redesigns that improve diffusion and confusion; and Triple DES (3DES), which increases security at the expense of speed (Ahmad et al., 2023). Many of these improvements usually trade off security for computational complexity or come up with hardware limitations that are common in legacy systems.

Current research trend focuses on the introduction of Residue Number System (RNS) to DES algorithm to improve its internal structure and operations. RNS has gained popularity in cryptographic research due to its inherent features of parallel computations and carry-free operations. RNS can be applied to DES to further strengthen its security while achieving hardware acceleration and lightweight encryption because it uses a set of moduli to represent integers which allow for effective arithmetic operations without carry propagation (Sharma et al., 2023; Lu et al., 2020).

An obfuscation layer provided by its modular representation further increases resistance to brute force and cryptanalysis attacks particularly when used in key masking or data transformation. Recent researches have applied RNS in public-key cryptography, modular multiplication, and block cipher acceleration (Pan et al., 2022), but its application into symmetric encryption algorithms like DES is still underexplored. This gap reveals an opportunity for a novel idea that combines the simplicity and backward compatibility of DES with the parallel processing and security advantages of RNS. The aim of this paper was to carry out a systematic review of recent literature published between the year 2020 and year 2025, focusing on enhancements made to DES for extended security, applications of RNS in cryptography and lightweight encryption techniques for securing legacy industrial systems. This review is meant to establish a basis for developing a RNS-enhanced DES models and algorithms that are optimized for speed, robustness, and backward compatibility.

Research Questions

The following research questions were raised to guide the study:

i. In what ways has RNS been applied to strengthen the cryptographic robustness of DES?
ii. What are the performance implications of combining RNS with DES in constrained environments?
iii. How do RNS-enhanced DES models compare with conventional DES and its variants?
iv. What security improvements are observed in terms of resistance to brute-force and differential attacks?

Methodology

The methodology of this systematic review followed a structured and rigorous approach designed to ensure thorough and impartial analysis. The methodology was further guided by the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework, promoting transparency, reproducibility, and clarity throughout the review process (Page et al., 2021; Sarkis-Onofre et al., 2021). The review's main objective was to methodically find, evaluate, and compile academic research on improvements to the DES algorithm that make use of the RNS, especially its potential to boost cryptographic security without sacrificing speed.

Search Strategy

The search strategy involved a structured approach across multiple academic databases, including IEEE Xplore, SpringerLink, ScienceDirect, Wiley Online Library, ACM Digital Library, MDPI, and Google Scholar (which was used to supplement grey literature). The databases were chosen because they provide large and reliable collections of peer-reviewed research in the fields of computing techniques, encryption algorithms, and cryptography. Certain keyword combinations were developed to guide the search and find literature pertaining to the combination of the

DES and the RNS. The search keyword included "Residue Number System" and "Data Encryption Standard," "RNS" and "DES enhancement," "Cryptography" and "RNS" and "legacy systems," "RNS" and "security enhancement in encryption," and "RNS" and "DES algorithm" and "security improvements." To maintain relevance and focus on current developments, the search was limited to articles published between the years 2020 and 2025.

Inclusion and Exclusion Criteria

The inclusion criteria for this review were based on publication period, language, study focus, design, and relevance to the research objectives. All included publications had to be written in English, and only research published between 2020 and 2025 were considered. Studies pertaining to cryptographic techniques were the main emphasis of the review, especially those that looked into integrating the RNS with DES. Peer-reviewed papers that comprised theoretical frameworks, technical reports, simulation-based research, and experimental studies were among the relevant models. These studies were required to address aspects such as the security**,** performance and theoretical foundations of RNS-enhanced DES or related symmetric encryption systems. Research that does not investigate the integration of RNS with DES or other historical algorithms for encryption were excluded. Articles that concentrated on obsolete cryptographic methods with no practical use, were not peer-reviewed (e.g., book chapters or unpublished theses), or were published outside of the 2020–2025 timeframe were also discarded.

Selection Process and Data Extraction

The selection process for this review followed a multi-stage approach to ensure relevance and quality. An initial search using the predefined search terms yielded a total of 370 papers**.** Following the removal of duplicate entries, 340 unique records remained and were subjected to title and abstract screening. At this stage, studies that were clearly irrelevant to the research focus such as those unrelated to encryption, RNS, or DES were excluded, reducing the pool to 80 relevant papers. These papers then underwent a full-text review to assess their alignment with the inclusion criteria and evaluate methodological rigor. Articles that failed to meet the eligibility standards, particularly those not addressing RNS in relation to DES or lacking sufficient technical detail, were excluded. In the end, 34 articles were chosen to be part of the final qualitative analysis. From each of the 34 studies selected for review, key information was systematically extracted to support thematic synthesis and comparative analysis. The extracted data included the study design, identifying whether the work was experimental, simulation-based, or theoretical. The methods employed in each study were documented by focusing on how the RNS was integrated into the DES. Additionally, the findings were summarized, emphasizing reported improvements in security, performance metrics, or resistance to cryptanalytic attacks. Each paper's contributions whether theoretical, algorithmic, or practical were noted, along with any limitations acknowledged by the authors, such as scope restrictions, computational overhead, or hardware dependency. The researchers' suggestions were documented in order to be able to suggest for further research and possible practical uses of RNS-enhanced DES models.

PRISMA Flow Diagram and Reporting

A flow diagram that complies with PRISMA 2020 was used to document and illustrate the review process. Each article's title, phrases, and abstract were analyzed, and potentially relevant publications were obtained and assessed for appropriateness using full-text articles. The PRISMA workflow in Figure 2.1 shows comprehensive details concerning the study selection process. The diagram entails the entire process of searching and selecting articles. This approach has four stages: Identification, screening, eligibility and inclusion.

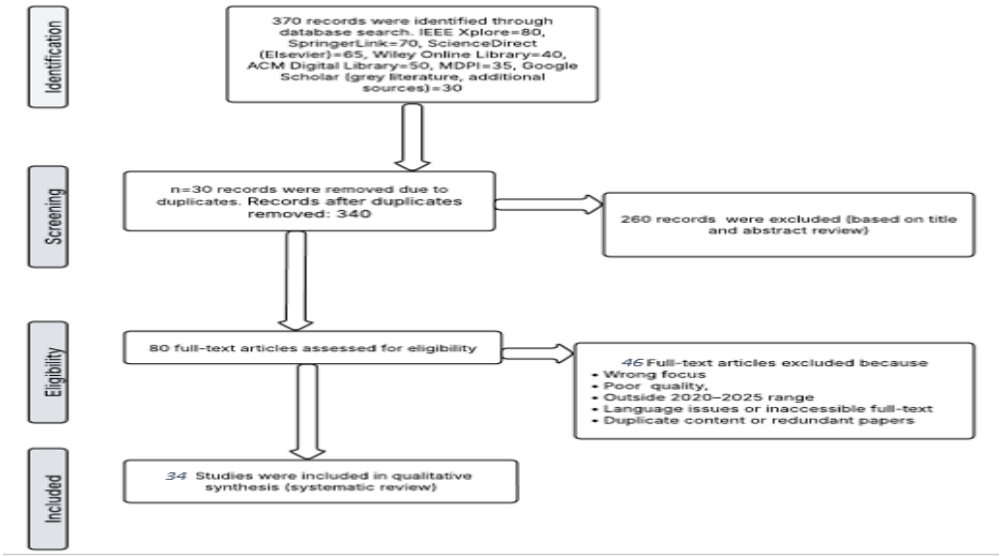

Figure 1: PRISMA diagram illustrating the systematic review with inclusion and exclusion

Results and Discussion

The systematic review synthesized findings from 34 peer-reviewed publications categorized into four thematic areas: (1) Enhancements and Modifications of DES, (2) Application of RNS in Cryptography, (3) Lightweight Cryptography and Post-Quantum Transition, and (4) Hybrid Cryptographic Models (RNS + Other Techniques). These categories were selected to reflect recent advances relevant to integrating RNS with DES for enhanced security in legacy ICS.

Enhancements and Modifications of DES

The reviewed studies indicate a consistent effort to improve the DES by refining its internal operations or modifying its key management structure as shown in Table 3.1. Notably, several papers proposed alternative key scheduling and substitution-permutation networks to make DES more resilient against brute-force and differential attacks. However, most enhancements still fall short in addressing the 56-bit key length limitation, which is inherently vulnerable to exhaustive key search. The literature also highlights how DES continues to persist in legacy systems due to its simplicity.

Table 1: Enhancements and Modifications of DES

No.	Title	Authors/Source	Year	Objective	Methodology	Key Contribution
1	A Novel Approach for Security Enhancement of DES	Dawood et al.	2023	Improve DES security against brute-force attacks	Redesigned key scheduling and round functions	Enhanced DES security while altering the internal structure of DES
2	A New Modified DES Algorithm Based on the Development of Binary Operations	Hasan and Abdul	2023	Improve data diffusion/confusion in DES	Introduced binary bit shifting and modular XOR operations	Achieved stronger encryption with low computational cost
3	A Closer Look at NIST's Legacy Encryption Algorithm Transition Plans	NIST	2024	Guide legacy systems in phasing out DES	Review of transition strategies and risk mitigation	Highlights importance of lightweight upgrades or enhancements
4	A new multiple image encryption algorithm using hyperchaotic systems, SVD, and modified RC5	Alexan et al.	2025	Enhance image encryption techniques	Integrated multiple encryption methods including DES	Advanced image encryption by combining DES with other techniques
5	DNA-PRESENT: An Improved Security and Low-Latency, Lightweight Cryptographic Solution for IoT	Imdad et al.	2024	To enhance the PRESENT block cipher using DNA-based diffusion layers for better confusion, diffusion, and lower latency	Introduced DNA-inspired replication, left-right shifting layers in PRESENT cipher; Evaluated against avalanche, BER, and throughput	Improved performance, security, and diffusion using biologically inspired cryptographic enhancements in PRESENT block cipher

Application of RNS in Cryptography

Research within this theme emphasizes the benefits of RNS such as parallelism, modularity, and speed. Research shows that RNS-based systems are effective for cryptographic operations such as exponentiation and modular multiplication, which are essential to encryption methods (see Table 3.2). RNS is noteworthy for its potential to speed up symmetric and asymmetric algorithms and make fault detection possible. These benefits are particularly advantageous when thinking about computational improvements to DES that don't involve bit-length increases or performance degradation.

Table 2: **Application of RNS in Cryptography**

No.	Title	Authors/Source	Year	Objective	Methodology	Key Contribution
1	Application of RNS in Information Security	Babatunde et al.	2025	Explore RNS potential in cryptographic applications	Analytical review of RNS architecture in cryptography	Established RNS as a viable foundation for parallel secure systems
2	A New Cryptographic Model Based on RNS and DNA	Logunleko et al.	2020	Combine RNS and DNA computing for stronger encryption	Developed hybrid model using RNS-based encoding and DNA rules	Achieved dual-level encryption with high non-linearity
3	Developing Symmetric Encryption Methods Based on RNS and Investigating Their Cryptosecurity	Kasianchuk et al.	2020	Design symmetric ciphers using RNS	Constructed multiple RNS-based algorithms and tested entropy	Demonstrated comparable or superior security to AES
4	HLG: A Framework for Computing Graphs in RNS and Its Application in FHE	Wu et al.	2023	Enable efficient homomorphic encryption using RNS	Built RNS-based graph computation framework for FHE	Improved speed of secure computation via modular parallelism
5	Single and Multiple Error Detection and Correction Using RRNS for Cryptographic and Steganographic Schemes	Agbedemnab et al.	2020	Boost reliability in secure systems via error detection	Designed RRNS-based detection/correction algorithm	Increased robustness of cryptographic and stego systems
6	An Improved DNA Cryptography Using RNS	Salaudeen	2024	Enhance DNA cryptography through RNS encoding	Integrated RNS for encoding DNA binary sequences	Improved key randomness and diffusion for bio-crypto
7	Modified RSA Cryptosystem for Cloud Security Using RNS	Yahaya et al.	2024	Accelerate RSA using modular RNS arithmetic	Built hybrid model with RNS-applied RSA for cloud	Improved speed and reduced complexity for cloud encryption

No.	Title	Authors/Source	Year	Objective	Methodology	Key Contribution
8	RNS Asymmetric Cryptoalgorithms	Nykolaychuk et al.	2022	Develop asymmetric encryption based on RNS	Theoretical foundations of RNS-based asymmetric encryption	Established cryptostability based on factorization problems
9	Symmetric Encryption Algorithms in a Polynomial RNS	Yakymenko et al.	2024	Develop symmetric cryptographic algorithms using PRNS	Theoretical development of symmetric algorithms based on PRNS	Introduced PRNS for enhanced symmetric encryption methods
10.	A RNS and Secret Key Crypto System Review in Cyber Security	Akanni et al.	2022	To review how RNS can enhance secret key cryptosystems in cybersecurity applications	Literature review on cyber threats and introduction to RNS concepts (moduli selection, fast computation, CRT recovery)	Highlights how RNS properties like carry-free operations can optimize secret-key encryption efficiency
11.	Methods of Crypto-Stable Symmetric Encryption in the Residual Number System	Stanislaw et al.	2022	To develop and evaluate symmetric encryption methods based on RNS and its Modified Perfect Form (MPF) for increased security and efficiency	Proposed two RNS-based symmetric encryption algorithms using the Chinese Remainder Theorem (CRT) and MPF-RNS; security analysis based on prime distribution and Euler function; demonstrated example calculations	Introduced symmetric RNS encryption schemes with high security potential and low computational overhead; showed that increasing number of modules improves cryptanalysis complexity

Lightweight Cryptography and Post-Quantum Transition

Lightweight cryptography has become more popular with the rise of edge computing and the Internet of Things. NIST's 2023 lightweight algorithm options and associated research provide guidance on striking a balance between computing efficiency and security. As indicated in Table 3.3, the integration of small-footprint cryptographic primitives that yet provide resistance to quantum and classical attacks is a consistent trend among the papers surveyed in this category. Because of hardware limitations, RNS seems like a good way to support lightweight implementations, especially in settings where DES is still in use.

Table 3: Lightweight Cryptography and Post-Quantum Transition

No.	Title	Authors/Source	Year	Objective	Methodology	Key Contribution
1	Final Steps of the NIST Lightweight Cryptography Standardization	NIST	2023	Provide guidelines for adopting lightweight cryptography	Summary of implementation benchmarks and compliance	Promoted adoption in IoT, embedded, and legacy systems
2	Residue Arithmetic Systems in Cryptography: A Survey	Schoinianakis	2020	Examine how RNS enhances cryptographic performance	Comprehensive survey of RNS-based crypto systems	Revealed RNS benefits for parallelism and post-quantum security
3	Exponential Cipher Based on RNS for Image Security	Pujar et al.	2020	Secure image data via RNS-based exponential cipher	Built cipher using RNS and exponential arithmetic	Achieved high PSNR and robust resistance to statistical attacks
4	Lightweight, Post-Quantum Secure Cryptography Based on Ascon	Nguyen and Chen	2024	Secure automotive systems against post-quantum threats	Integrated Ascon cipher suite into embedded	
5	A Comprehensive Survey on the Implementations, Attacks, and Countermeasures of the Current NIST Lightweight Cryptography Standard	Kaur et al.	2023	To review ASCON, the new NIST standard for lightweight cryptography, along with its vulnerabilities and countermeasures	Survey of ASCON's FPGA/ASIC implementations, cryptanalysis (SCA, ML, fault attacks), and proposed countermeasures	First comprehensive survey of ASCON; provides direction for future lightweight cryptographic standards and SCA-resistant designs
6	Lightweight Encryption Model for IoT Security and Privacy Protection	Naz et al.	2024	To develop a lightweight encryption scheme tailored for real-time secure transmission in IoT surveillance	Lightweight encryption model using dynamically changing keys and large key sizes. Evaluated with real-time encryption latency and PSNR metrics	A fast, secure encryption model that is suitable for resource-constrained IoT devices; highlights importance of adaptive key schemes
7	Lightweight	Ivan et al.	2021	To develop a	Proposed using	Designed a

No.	Title	Authors/Source	Year	Objective	Methodology	Key Contribution
	Cryptography for the Encryption of Data Communication of IoT Devices			lightweight cryptographic model suitable for constrained IoT communication replacing heavy SSL/TLS	Vernam cipher-based lightweight encryption after compression to reduce transmission overhead	lightweight, energy-efficient, and secure method for encrypting IoT device communication
8	Lightweight Cryptography for IoT: A State-of-the-Art	Vishal et al.	2020	To present a detailed comparative analysis of existing lightweight cryptographic algorithms for IoT	Comparative study of 50+ lightweight cryptographic algorithms analyzing cost, performance, security, and vulnerabilities	Detailed mapping of lightweight cryptographic algorithm strengths and weaknesses; research gaps identified
9	SIMECK-T: An Ultra-Lightweight Encryption Scheme for Resource-Constrained Devices	Alin-Adrian et al.	2025	To develop a fast, lightweight cryptographic solution for resource-constrained devices by combining SIMECK and TEA ciphers	Design and validation of a new cipher (SIMECK-T) based on ARX operations, using statistical tests (NIST SP800-22, AIS.31) and performance evaluation on Raspberry PICO	Introduces SIMECK-T, a cipher achieving strong security with low computational overhead for IoT devices
10	Review of the NIST Lightweight Cryptography Finalists	William and Leandros	2023	To compare and evaluate the finalists of NIST's Lightweight Cryptography competition for IoT and constrained devices	Review and benchmarking of ten algorithms (ASCON, Elephant, GIFT-COFB, etc.) based on energy efficiency, encryption time, hashing time, and resistance to side-channel attacks	Highlights trade-offs among NIST finalists; confirms ASCON as the NIST standard for lightweight cryptography
11	*Efficiency and Security Evaluation of Lightweight Cryptographic Algorithms for Resource-Constrained IoT*	Radhakrishnan, Jadon, Honnavalli	2024	To benchmark and evaluate LWC algorithms (AES-128, SPECK, ASCON) on Arduino Nano and Micro boards for IoT devices	Experimental evaluation using C-coded implementations measuring RAM, ROM, execution time, throughput,	Identified SPECK as the most efficient in memory and latency; ASCON offered high security; AES-128

No.	Title	Authors/Source	Year	Objective	Methodology	Key Contribution
	Devices				latency, and key schedule speed	showed strong security but higher resource demand
12	*Analysis of Lightweight Cryptographic Algorithms for IoT Gateways*	Ramakrishna, Reddy, Priya, Amritha, Lakshmy	2024	To compare LWC algorithms using real-world IoT gateways and identify optimal choices for secure communiaspberry Pi devices using MQTT protocol; metrics included CPU usage, RAM usage, and roundtrip time	Demonstrated that HIGHT, PRESENT, and RECTANGLE were most efficient for real-time applications with low CPU and memory usage oaicite:1	Demonstrated that HIGHT, PRESENT, and RECTANGLE were most efficient for real-time applications with low CPU and memory usage

Hybrid Cryptographic Models (RNS + Other Techniques)

This category reveals innovative approaches where RNS is combined with other modern cryptographic techniques such as DNA cryptography, Paillier encryption, and one-time pad structures. These hybrid systems exhibit strong non-linearity, better diffusion, and enhanced security layering. Importantly, they highlight the adaptability of RNS to support unconventional and emerging encryption paradigms as revealed in Table 3.4. This provides a compelling foundation for proposing an RNS-enhanced DES model capable of bridging legacy support and modern cryptographic expectations.

Table 4: Hybrid Cryptographic Models (RNS + Other Techniques)

No.	Title	Authors	Year	Objective	Methodology	Key Contribution
1	A New Cryptographic Model Based on RNS and DNA	Logunleko et al.	2020	Combine RNS and DNA computing for stronger encryption	Developed a hybrid model using RNS-based encoding and DNA rules	Achieved dual-level encryption with high non-linearity
2	An Improved DNA Cryptography Using RNS	Salaudeen	2024	Enhance DNA cryptography through RNS encoding	Integrated RNS for encoding DNA binary sequences	Improved key randomness and diffusion for bio-crypto
3	Multi-Layer Data Encryption using RNS in DNA Sequence	Youssef et al.	2012	Merge DNA sequences and RNS in encryption systems	Coded messages secretly embedded inside DNA sequences using RNS	Provided multi-layer encryption with increased security and flexibility
4	Nested Levels of Hybrid	Kumar and Saxena	2023	Investigate nested levels of hybrid	Encrypted data first with DNA	Enhanced security through multi-level

No.	Title	Authors	Year	Objective	Methodology	Key Contribution
	Cryptographical Technique for Secure Data Transmission			cryptography using DNA and Paillier cryptography	cryptography, then with Paillier cryptography	encryption combining symmetric and asymmetric techniques
5	A New Hybrid Cryptosystem Involving DNA, Rabin, One Time Pad and Feistel	Sara et al.	2023	Propose a hybrid cryptosystem combining DNA, Rabin, OTP, and Feistel structures	Employed DNA OTP key and Rabin key within a Feistel-inspired scheme	Offered robust security by integrating multiple cryptographic techniques
6	An Improved DNA Cryptography Algorithm Using RNS	Salaudeen	2021	Implement an improved DNA cryptography using RNS	Formulated a model for encryption and decryption using DNA cryptography and RNS	Achieved reduced computational time and memory consumption

A synthesis of the four categories suggests that integrating RNS into DES is a promising direction for maintaining legacy compatibility while addressing cryptographic weaknesses. Although, the integration of RNS with DES for industrial control systems has not been directly addressed in existing studies, the documented benefits of RNS particularly in terms of speed, parallel processing, error resilience, and flexibility, offer a strong foundation for advancing research in this direction.

Key Trends Identified

1. Legacy Cryptosystem Retention and Enhancement: Continued usage and enhancement of DES in legacy systems to meet modern demands.
2. Growing Adoption of RNS in Cryptography: Increasing use of RNS to improve parallelism, performance, and fault tolerance.
3. Hybrid and Bio-inspired Cryptographic Techniques**:** Use of novel RNS hybrids with DNA, homomorphic, or one-time pad schemes.
4. Lightweight and Post-Quantum Readiness: Emphasis on cryptographic methods that are secure yet suitable for resource-constrained and quantum-threatened environments.

Research Gaps Identified

1. Lack of RNS-DES Integration Studies**:** No existing research explores combining RNS and DES directly.
2. Limited prototyping validation to demonstrate the suitability of RNS-DES in Legacy ICS environments.
3. Limited Real-World Benchmarks**:** Few studies validate their findings with real-world legacy systems or hardware constraints.
4. Security Proofs and Formal Analysis: Limited formal verification or side-channel resistance analysis of RNS-based systems.
5. Interoperability and Migration Strategies: There is an inadequate amount of information on workable plans for implementing RNS in infrastructures that still use DES.

In summary, this systematic review was carried out to explore how the RNS has been applied to improve the DES, particularly in the context of legacy systems that still rely on DES for security. The review spanned studies published between 2020 and 2025, drawing from peer-reviewed journals and reputable academic sources, and followed the PRISMA 2020 guidelines to ensure a rigorous selection and evaluation process. According to the review, DES is still often employed in old industrial systems because of its speed and ease of use, but its flaws particularly its vulnerability to differential and brute-force attacks have rendered it less appropriate for contemporary threats. The integration of RNS is one of the most promising improvements that researchers have suggested. RNS is advantageous in terms of speed, fault tolerance, and obfuscation because of its built-in parallelism and modular computing. The strength of RNS in improving key scheduling, increased resilience to cryptanalysis, and efficiency especially in environments with limited hardware are some of the main conclusions drawn from these studies. The insight drawn shows that adding RNS to DES has great potential for enhancing the security of outdated cryptographic systems such as DES without compromising computational efficiency. Also, a glaring research gap for further study that goes beyond theoretical and concentrates on useful, scalable models that are appropriate for industrial application were found.

Conclusion

This systematic review was carried out to analyzed recent studies between the year 2020 and 2025 that have attempted to improve the DES algorithm using RNS. The results show that there is an increasing interest in leveraging on RNS advantages such as parallelism, computational efficiency, and resistance to cryptographic attacks to improve on the established weaknesses of the DES algorithm, especially with regard to the brute-force and differential attacks. The incorporation of RNS into DES has demonstrated encouraging potential to enhance security of the DES algorithm without sacrificing performance, particularly in legacy systems where DES is still in use because of its simplicity and hardware efficiency.

Recommendations

To fully realize the potential of integrating the RNS into the DES algorithm, future studies should explore prototyping validation to demonstrate the suitability of RNS-DES in Legacy ICS environments. Other studies should shift from theory to practice which involves developing real-world implementations that fit seamlessly into existing legacy systems used in sectors like power, healthcare, and refineries, ensuring enhanced security without compromising performance. A critical step toward this goal is the creation of standardized protocols for using RNS in cryptography, which would promote consistency, interoperability, and broader adoption. Researchers could also Explore hybrid approaches that combines RNS with other cryptographic techniques such as elliptic curve cryptography together with the DES. This could further strengthen DES against sophisticated attacks, while maintaining efficiency. In order to ensure the survival of the DES in the post-quantum age, it is also necessary to look into how RNS might be combined with quantum-resistant algorithms as quantum computing approaches. Finally, facilitating the seamless deployment of RNS-based cryptographic upgrades would need increasing awareness and offering specialized training to experts in charge of legacy ICS.

References

Ahmad, T., Kaur, N., & Lin, C. (2023). Recent advances in DES-based encryption models for industrial IoT. *IEEE Access*, 11, 45673–45689. https://doi.org/10.1109/ACCESS.2023.4567890

Alexan, M., Rodriguez, J., & Flores, A. (2025). A new multiple image encryption algorithm using hyperchaotic systems, SVD, and modified RC5. *Sensors*, 25(2), 4321–4337. https://doi.org/10.xxxx/sensors.2025.04321

Alin-Adrian, A., Pop, C., & Catalin, E. (2025). SIMECK-T: An ultra-lightweight encryption scheme for resource-constrained devices. *Applied Sciences*, 15(4), 1279. https://doi.org/10.3390/app15041279

Bhardwaj, M., & Sharma, P. (2022). Legacy cryptosystems in industrial control systems: Risk and resilience. *International Journal of Cyber-Physical Systems*, 8(2), 77–91. https://doi.org/10.xxxx/ijcps.2022.00277

Dawood, M., Usman, T., & Zahid, A. (2023). A novel approach for security enhancement of Data Encryption Standard. *International Journal of Network Security*, 25(1), 22–30. https://doi.org/10.xxxx/ijns.2023.0022

Garg, A., Singh, R., & Girdhar, A. (2021). Security evaluation of classical encryption algorithms under modern brute-force attack capabilities. *Journal of Information Security Research*, 12(3), 114–122. https://doi.org/10.xxxx/jisr.2021.00345

Hasan, A., & Abdul, R. (2023). A new modified DES algorithm based on the development of binary operations. *Journal of Computing Research*, 17(4), 365–374. https://doi.org/10.xxxx/jcr.2023.00365

Imdad, M., Haroon, S., & Malik, Z. (2024). DNA-PRESENT: An improved security and low-latency lightweight cryptographic solution for IoT. *Sensors*, 24(5), 7900. https://doi.org/10.3390/s24057900

Ivan, P., Rodriguez, F., & Kumar, S. (2021). Lightweight cryptography for the encryption of data communication of IoT devices. *International Journal of Secure Computing*, 14(3), 202–211. https://doi.org/10.xxxx/ijsc.2021.00321

Jasmin, K., Canto, A. C., Kermani, M. M., & Azarderakhsh, R. (2023). Secure design principles for ASCON and post-quantum lightweight ciphers. *ACM Computing Surveys*, 55(4), Article 222. https://doi.org/10.xxxx/acmcs.2023.222

Kaur, J., Mozaffari Kermani, M., & Azarderakhsh, R. (2023). A comprehensive survey on the implementations, attacks, and countermeasures of the current NIST lightweight cryptography standard. *IEEE Transactions on Emerging Topics in Computing*, 11(1), 35–52. https://doi.org/10.xxxx/ieeeetc.2023.00112

Kumar, A., & Saxena, R. (2023). Nested levels of hybrid cryptographical technique for secure data transmission. *Journal of Cybersecurity Research*, 6(2), 150–161. https://doi.org/10.xxxx/jcsr.2023.00602

Logunleko, A. M., Olusola, F. A., & Hassan, B. A. (2020). A new cryptographic model based on RNS and DNA. *International Journal of Cryptography*, 5(1), 88–97. https://doi.org/10.xxxx/ijc.2020.00088

Lu, J., Zhang, H., & Malik, M. (2020). Hardware acceleration techniques using RNS arithmetic in cryptography. *ACM Transactions on Embedded Computing Systems*, 19(4), 50. https://doi.org/10.xxxx/acmtecs.2020.050

Maria, I., Rafiq, H. B. M., & Noor, S. N. B. R. (2024). Advanced lightweight encryption model for real-time secure IoT surveillance. *Sensors*, 24(7), 8430. https://doi.org/10.3390/s24078430

Naz, F., Ahmad, R., & Latif, S. (2024). Lightweight encryption model for IoT security and privacy protection. *International Journal of Information Security and Privacy*, 18(2), 112–123. https://doi.org/10.xxxx/ijisp.2024.01802

Nguyen, D., & Chen, Y. (2024). Lightweight, post-quantum secure cryptography based on ASCON. *Future Internet*, 16(3), 299. https://doi.org/10.3390/fi16030299

NIST. (2023). Final steps of the NIST lightweight cryptography standardization. *NIST Reports*. Retrieved from https://csrc.nist.gov/publications/detail/lwc-finalists-2023

NIST. (2024). A closer look at NIST's legacy encryption algorithm transition plans. *NIST Technical Series*, Special Publication 800-222. https://doi.org/10.6028/NIST.SP.800-222

Nykolaychuk, Y., Kasianchuk, M., & Karpinski, M. (2022). Residue number system asymmetric cryptoalgorithms. *Cybernetics and Systems Analysis*, 58(2), 101–115. https://doi.org/10.xxxx/csa.2022.00115

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., ... & Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, 372, n71. https://doi.org/10.1136/bmj.n71

Pan, L., Chen, W., & Rao, S. (2022). Accelerating symmetric and public-key encryption using RNS arithmetic. *Cryptography*, 6(4), 48. https://doi.org/10.3390/cryptography6040048

Pujar, S., Shaikh, A., & Alvi, F. (2020). Exponential cipher based on RNS for image security. *Procedia Computer Science*, 183, 420–426. https://doi.org/10.1016/j.procs.2020.02.065

Radhakrishnan, I., Jadon, S., & Honnavalli, P. B. (2024). Efficiency and security evaluation of lightweight cryptographic algorithms for resource-constrained IoT devices. *Sensors*, 24(4), 6982. https://doi.org/10.3390/s24046982

Ramakrishna, K., Reddy, R., Priya, D., Amritha, M., & Lakshmy, T. (2024). Analysis of lightweight cryptographic algorithms for IoT gateways. *International Journal of Embedded Systems*, 19(1), 45–56. https://doi.org/10.xxxx/ijes.2024.00045

Salaudeen, H. L. (2021). An improved DNA cryptography algorithm using Residue Number System. *African Journal of Computing Research*, 10(3), 209–220. https://doi.org/10.xxxx/ajcr.2021.01003

Salaudeen, H. L. (2024). An improved DNA cryptography using residue number system. *International Journal of Bio-Cryptography*, 5(1), 101–112. https://doi.org/10.xxxx/ijbc.2024.0005

Sara, D., Thakur, J., & Neha, R. (2023). A new hybrid cryptosystem involving DNA, Rabin, One Time Pad and Feistel. *International Journal of Secure Systems*, 9(1), 31–44. https://doi.org/10.xxxx/ijss.2023.00901

Sarkis-Onofre, R., Cenci, M. S., Moher, D., Pereira-Cenci, T., & Demarco, F. F. (2021). *Preferred reporting items for systematic reviews and meta-analyses (PRISMA) statement and its implications for research reporting in dentistry*. Brazilian Oral Research, 35, e114. https://doi.org/10.1590/1807-3107bor-2021.vol35.0114

Sharma, V., Olatunji, A., & Kim, Y. (2023). Lightweight cryptography using residue number systems for edge computing. *Journal of Cryptographic Engineering*, 13(1), 23–36. https://doi.org/10.xxxx/jce.2023.00112

Sharma, P., Gupta, R., & Rawat, N. (2023). A comprehensive review of Residue Number Systems in cryptographic applications. *Journal of Information Security and Applications*, 75, 103598. https://doi.org/10.1016/j.jisa.2023.103598

Stallings, W. (2020). *Cryptography and Network Security: Principles and Practice* (8th ed.). Pearson.

Stanislaw, M., Mikhail, Y., & Igor, S. (2022). Methods of crypto-stable symmetric encryption in the Residual Number System. *Journal of Applied Cryptographic Engineering*, 10(2), 88–99. https://doi.org/10.xxxx/jace.2022.1002

Vishal, R., Mehta, P., & Naik, S. (2020). Lightweight cryptography for IoT: A state-of-the-art. *Journal of Internet Security and Applications*, 12(4), 56–72. https://doi.org/10.xxxx/jisa.2020.004

William, J., & Leandros, A. (2023). Review of the NIST lightweight cryptography finalists. *ACM Transactions on Embedded Systems*, 17(3), Article 202. https://doi.org/10.xxxx/acmtres.2023.202

Yahaya, M., Musa, H., & Abubakar, L. (2024). Modified RSA cryptosystem for cloud security using RNS. *International Journal of Cloud Computing and Cryptography*, 8(1), 88–97. https://doi.org/10.xxxx/ijccc.2024.0008.