DOI: http://dx.doi.org/10.26483/ijarcs.v16i2.7205

Volume 16, No. 2, March-April 2025

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

DEVELOPMENT OF THE RESIDUE NUMBER SYSTEM-BASESIXTY-FOUR (RNS-B64) ENCRYPTION ALGORITHM FOR SECURE DATA TRANSMISSION

Kolawole Bariu Logunleko
Department of Computer Science
D.S. Adegbenro ICT Polytechnic, Eruku-Itori, Ewekoro, Ogun state, Nigeria.

Ayisat Wuraola Asaju-Gbolagade
Department of Computer Science,
University of Ilorin, Ilorin Nigeria.

Abolore Muhamin Logunleko
Department of Computer Science, Gateway ICT Polytechnic, Saapade, Ogun State, Nigeria.

Akinbowale Nathaniel Babatunde
Kazeem Alagbe Gbolagade
Department of Computer Science, Kwara State University, Malete, Ilorin, Nigeria.

Abstract: Over the years, the Base64 cryptographic algorithm has been a crucial component of information security employed in various security protocols and applications including digital signature schemes, random number generation and Message Authentication Codes, to guarantee data integrity and authenticate the origin of data. However, research has identified security vulnerabilities in the algorithm due to its non-availability of key. The research aimed to develop a novel cryptosystem that uses Residue Number System (RNS) to enhance the Base64 (B64) algorithm's performance alongside with the efficiency of the algorithm. The developed cryptosystem employs the approach of a modern encryption algorithm with the adoption of length three moduli set to design an efficient forward conversion for the encryption algorithm and reverse conversion using Chinese Reminder Theorem (CRT) for decryption algorithm. The algorithmic process design was implemented using dart, flutter technology and android studio. The research examines various cryptographic algorithms while considering several evaluation metrics such as encryption time, decryption time, storage overhead and algorithm type. A secured cryptosystem called Residue Number System Base64 Algorithm (RNS-B64) was developed. In terms of encryption and decryption time performance, the result shows that the RNS-B64 cryptosystem has 0.0005 and 0.0002 respectively while the existing cryptosystem has 0.0037 and 0.0029 respectively on sixteen bytes textual data. The findings indicate that this research outperformed the previous work by enhancing the security level and reducing the encryption and decryption time thus increasing computational efficiency of the developed cryptosystem.

Keywords: Cryptosystem, Base64 Algorithm (B64), Residue Number System (RNS), Key, Moduli set.

INTRODUCTION

A variety of techniques had been used to protect data transfer across an insecure network, since a secure network cannot always be guaranteed. To guarantee data transfer security, a number of cryptographic approaches are available [1]. One such approach in the world of information security is Base64 transformation cryptography. Several serialization protocols, the web, logging applications, and human-readable database fields frequently employ Base64 algorithms being a popular method to encode binary data into a printable ASCII characters [2], [3]. Furthermore, Base64 algorithm is usually utilized to encode binary data [4] that needs to be stored and transferred through a communication channels so as to protect such data during transmission but due to its non-availability of key, the aforementioned algorithm is not adequately secure for both encryption and decryption of textual data. Research has shown this security flaws and vulnerabilities in most widely used Base64 transformation cryptography algorithm [5]. In cryptographic applications, the residue number system (RNS) is increasingly proposed to provide more internal parallelism. RNS uses a set of small co-prime moduli, called the base, to divide some arithmetic operations into independent and much smaller ones over the residues. This independence leads to faster operations without carry propagation between the moduli [6]. RNS helps to improve the security against some physical attacks [7]. In addition, RNS excels in a wide range of applications, including cryptography, digital signal processing, communications engineering, computer security, image processing, voice processing and transformation, where addition and multiplication are crucial arithmetic operations [8]. The introduction of RNS was due to its special properties often utilized for encryption and decryption purposes by applying forward and reverse conversion algorithm. This does not only enhance the existing base64 algorithm as the case may be, but also increases security and the efficiency of the algorithm. This research is significant because it solves security inadequacy in the existing Base64 algorithmic process as well as improving efficiency of the developed cryptosystem. [9] revealed that designing any algorithmic encryption and decryption process to raise the degree of security is the main problem. Therefore, in order to improve the security level and also, boost the performance of the base64 algorithm by minimizing a significant amount of encryption and decryption time, this study employs Residue Number System to address this research problem to form a novel symmetric-based cryptosystem named Residue Number System Base64 Algorithm (RNS-B64). The

developed algorithm improves the security by incorporating the key mechanism using residue number system (RNS) algorithm approach; this further creates more confusion, diffusion and transformation to the crypto algorithmic process thereby ensuring that the RNS-B64 is sufficiently safe to provide appropriate protection of both private and confidential communications. The RNS-B64 improves confusion performance of round transformation and hence, provides cryptographic privacy and authentication for data communication.

In addition, RNS-B64 also improves the computational efficiency because of RNS characteristic nature, such as high processing speed, reduced power and complexity, thereby improving algorithm's encryption and decryption times. The developed cryptosystem will not only solve the problem of a non-secured transmitting channel such as SMS communication system and email system, but also make the system more efficient than other contemporary symmetric-key algorithms.

The developed cryptosystem makes the cipher text file larger by increasing confusion and making it harder for hackers to access it. As a result, the developed cryptosystem can be used to provide end-to-end key-based encryption for SMS and email, therefore addressing security flaws in data transmission caused by cryptographic assaults such as known plaintext attacks, brute force attacks etc. Users can communicate critical information over SMS and email using the developed cryptosystem which guards against intruders intercepting the transmission. Also, the developed RNS-B64 cryptosystem can be utilized as an alternative to SMS and email application systems due to its reduced computational cost and ability to send text across a network with limited bandwidth. Consequently, the study is applicable to domains where communications can be transmitted across networks i.e., where SMS, email and so on, are used to ensure that the confidentiality and integrity of the message are maintained throughout. The rest of the paper is structured as follows: Section II includes relevant papers of the related works. Section III covers the methodology, while Section IV and V present the results and conclusion respectively.

REVIEW OF RELATED WORKS

According to [10], security is the process of guarding against physical damage or theft of digital data while maintaining its confidentiality and accessibility, yet as technology advances swiftly, cybercrime rates increase as well, both in frequency and complexity. However, the degree of security offered by a cryptographic scheme depends to a larger extent on the type and length of the keys utilized, the levels of encryption to create chaos, the throughput rate of the algorithms as well as the ability of such encryption algorithms to encrypt smaller messages, [11]. Similarly, [12] also revealed that the security of a system should depend on the secrecy of the key and not of algorithms.

[1] did research on development of RSA encryption algorithm for secure data transmission. The authors combined a pair of even integers in the private key and public key, as compared to previous method, to enhance the factorization and complexity of variables, thus increasing data security through this modification of the RSA encryption technique. The study raises the degree of data security by using even numbers in the RSA encryption algorithm to produce better efficiency and dependability. Hence, the maximum data security via the network is guaranteed by this novel approach.

[5] applied Base64 algorithm to image files so as to ensure security of data from unauthourized users. The researcher revealed that Base64 was often used for simple encryption purposes such as hiding non-sensitive information and authentication processes. However, he further pointed out that Base64 algorithm was not designed for strong encryption security simply because of its security inadequacy mechanism. Therefore, the algorithms' security needs to be improved so as to make the algorithm stronger for a symmetric based cryptography.

[10] did research on a residue number system-based data hiding using steganography and cryptography. The research employed a steganography technique in which a secret message is embedded into a regular picture file, concealing its presence from the prowler. The RSA algorithm is employed in conjunction with steganography to increase the resilience of the system and prevent exposure of the contents of the covered file. RSA's public and private exponents are typically quite big in practice, which slows down the decryption process. The Chinese Remainder Theorem, which focuses on modulus computation, was used to expedite the decryption process. Consequently, the study suggested a quicker RSA-CRT technique for data decryption.

[7] developed a multi-level data encryption standard using residue number system for data security. Residue Number System (RNS) was introduced to enhance the security of the DES algorithm, as the study shows the tremendous efforts made by researchers to reduce its computational complexity and improve its security, DES remains vulnerable to brute force attacks. In order to address the security flaw in the DES algorithm, the DES-RNS model was created. Based on the study, the DES-RNS model performed better than the DES model, according to the results. Potential avenues for further research might involve enlarging the key size in this model. Building a fault-tolerant architecture that permits the addition of redundant data might be a further topic of study in the future work.

[13] revealed that data security applications using base64 algorithm could secure text data sent and received by users on communication networks using social media and communication media on mobile devices. According to the research, the system's ability to convert plaintext into ciphertext and vice versa using the base64 algorithm allowed the system to secure users' text data. However, there is need to improve the key mechanism, the encryption and decryption timing of algorithm to further strengthen the cryptosystem.

[14] presented the design methods of information encryption and decryption using Residue Number System (RNS). Three moduli sets $\{2^n - 1,\ 2^n, 2^n + 1\}$ were chosen for the study, and an efficient forward conversion was designed for the chosen moduli set with 4n + 2 and 8n as delay and area, respectively, for the information encryption and reverse conversion were designed for the same moduli set with 4n + 3 and 8n + 3 as area and delay, respectively. The suggested scheme offers better security and computational efficiency than the state of the art.

[15] explained the modern ways of employing RNS parallelism for key generation in asymmetric cryptosystems. He further

revealed that the creation of novel encryption methods of RNS and the research of their resistance to crypto analysis is now an incredibly relevant issue.

[16] carried out research on Base64 Character Encoding and Decoding Modeling. The study applies the Base64 algorithm to encrypt and decrypt textual data. The study revealed that the Base64 algorithm's low security strength prevents it from being utilized for symmetric encryption as frequently as the other cryptographic algorithms. Consequently, the model's security characteristics needed to be enhanced by using a key to improve the algorithm.

[17] developed an improved elliptic curve cryptography (ECC) model for text encryption. The model aims to improve the security of ECC by enhancing its base linear equation. The model uses elliptic curve arithmetic and a 256-bit key size for double encryption. Simulations were conducted using Java programming language on Net Beans IDE. The improved ECC outperformed existing systems in encryption and decryption times, but with higher encryption times.

[18] proposed Padding Key Encryption (PKE) algorithm to encrypt data by generating a secret key in an unreadable format, and decrypting it using a private key in a readable format. This method offers high security for confidential data or files.

[19] suggested a simple message cryptography method that divides a message into blocks with fixed sizes, using a secret color image to generate an array as a private key. The method calculates the number of rotation digits for each block, applying block rotation left operation. The method was evaluated using parameters like Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Correlation Coefficient (CC), and throughput, and compared to standard methods like Data Encryption Standard (DES), Triple-DES (3DES), Advanced Encryption Standard (AES), and Blow Fish (BF).

[20] introduced a chaotic 2D encryption method for text, utilizing two levels of transformation and bit-plane slicing to enhance security. The method uses p, q values and iterations from user input and SHA-256 hash operation. Testing results show improved encryption performance and perfect decryption, with Bit Error Rate (BER) and Crossover Error Rate (CER) values of 0.

[21] proposes a Key-based Enhancement of the DES (KE-DES) technique for text security. The study involves merging Odd/Even bit transformations and replacing the right-side expansion with a Key-Distribution function. The random key and data create adequate security, making the KEDES model more efficient for text encryption.

[22] developed a novel symmetric cryptography technique, based on Caesar cipher. The study transforms original text into secret using a hash code, providing a symmetric key to the receiver for decryption.

METHODOLOGY

Residue Number System-Base64 Algorithm (RNS-B64)

Residue Number System-Base64 Algorithm (RNS-B64) is a new cryptography algorithm developed for encryption and decryption of a sensitive data in order to maintain integrity, confidentiality and absolute privacy using a symmetric key. The algorithm's security features are enhanced by XORing the key into the existing Base64 algorithmic process. The technique uses the residue number system to improve base64 algorithm by adopting the contemporary encryption algorithms pattern. The improved technique uses a secret key, the same key is utilized for both encryption and decryption, respectively to develop an efficient forward conversion for the encryption algorithms. The Chinese Reminder Theorem (CRT) is used to develop a reverse conversion for the length three moduli set, which is used for decryption algorithms. The design carried out will not only increase the security level of the algorithmic process but also reducing the encryption and decryption time of the newly proposed algorithms thus increasing computational efficiency of the developed algorithms.

Residue Number System

The basis of a residue number system (RNS) is an N-tuple of integers $\{y_j\}_{j=1}^{K}$, each of which is referred to as a modulus. In the RNS representation $\{r_j\}_{j=1}^{K}$, given any base, are numbers defined by a set of N equations

$$p = q_j y_j + r_j \quad (1)$$

where j = 1, 2, ……..,K and q_j is an integer so chosen that $0 \leq r_j < y_j$. it is clear that q_j is an integer value of the quotient p/y_j which is denoted by $[p/y_j]$.

The quantity r_j is the least positive integer remainder of the division of p by y_j and is denoted as $p \ mod \ y_j$, i.e., $|p|_{y_i}$ [23], [24]. Equation (1) above can be re-written as;

$$p = y_j[p/y_j] + |p|_{y_{j_i}} \quad (2)$$

Chinese Remainder Theorem

RNS conversion to binary or decimal is done using this theorem. Considering the residue representation $\{r_1, r_2, \dots, r_{n\}}$ of p, the CRT allows one to ascertain $|p|_y$, if the gcd of any two moduli is 1. Such moduli are called pairwise relatively prime. [14], [23], [24].

The CRT is given by

$$|p|_y = |\sum_{e=1}^{K} \hat{y}_e |\frac{r_e}{\overline{y_e}}|_{ye}|_y \quad (3)$$

where $\hat{y}_e = \frac{Y}{y_e}$, $Y = \prod_{e=1}^{K} y_e$ and $\gcd(y_e, y_f) = 1 \ for \ e \neq f$.

The developed (RNS-B64) Model

The developed cryptosystem can be categorized into encryption and decryption model.

Encryption Model

This is a method of transforming plaintext to cipher-text with the use of mathematical notations. The developed system used the concept of the symmetric cryptography model and thus, the encryption model is represented in equation (4) as:

$$c_t = b64(rns(m_i) \oplus rns(k_i)) \quad (4)$$

where:
m_i - plaintext bits
k_i - key bits
c_t - cipher text
rns - residue number system
b64 - the forward encoding system for base64 Algorithm

Decryption Model

This is a method of transforming cipher-text to plaintext with the use of mathematical notations. The decryption model is represented in equation (5) as:

$$m_i = crt(c_t \oplus rns(k_i)) \quad (5)$$

where:
rns - residue number system
C_t - cipher text
m_i - plaintext bits
crt - Chinese Reminders Theorem (CRT)

Diagram of Data Flow for the RNS-B64 Cryptosystem

There are two phases in the data flow diagram for the RNS-B64 Cryptosystem implementation. Figure 1 illustrates the encryption process, and Figure 2 shows the data flow diagram for decryption process. In figure 1, the processes are explained as follows:

1. Convert the key to decimal using ASCII
2. Apply weight function to decimal number (y = (x * character count)/weight)
3. XOR all key decimal
4. Compute residue using secrete moduli set
5. XOR residues together
6. Convert result to 8-bit binary
7. Lookup characters in the ASCII table
8. Compute the remainders of each decimal using the supplied modulo
9. Convert each of the decimal remainders to 8-bit binary
10. XOR each 8-bit binary of message with 8-bit binary of key
11. Merge all 8-bit binary
12. Split into groups of 6 bits each
13. Convert each group using base64 lookup table

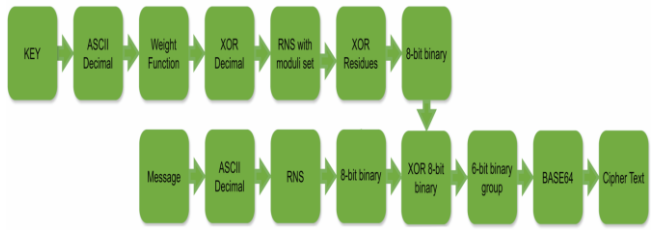

Figure 1: RNS-B64 Encryption Data Flow Diagram

Similarly, the figure 2 processes are also explained as follows:
1. Repeat the key process mechanism
2. Replace each character with its equivalent 6-bit binary from base64 lookup table
3. Merge all 6-bit binary
4. Split merge into groups each of 8-bit
5. XOR 8-bit binary of key with each 8-bit binary of ciphertext
6. Convert result to decimal
7. Compute the original number with CRT using n consecutive decimal numbers and the supplied modulo; where n is the number of modulo provided.
8. Lookup each computed decimal from ASCII table

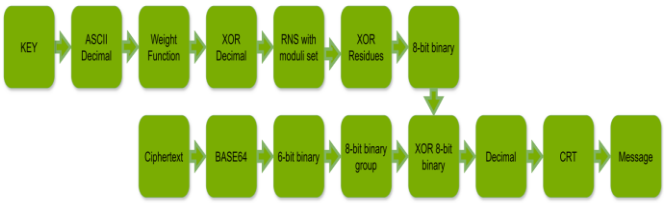

Figure 2: RNS-B64 Decryption Data Flow Diagram

The algorithmic process design is implemented using flutter technology and android studio respectively. The choice of programming language used is dart. The RNS-B64 cryptosystem encrypts and decrypts both intelligible and non-intelligible messages accordingly as shown in Figure 3, Figure 4a and Figure 4b respectively.

RESULTS AND DISCUSSIONS

Experiment Result Analysis

The experiment was carried out on a string plaintext that contains the message "Names" with secret key k = "Kola" and a secret modulus set. The cryptographic strength and performance evaluation of the developed cryptosystem were investigated. The cryptosystem was subjected to the dissimilar assessments as shown in [13], [25], [26]. The time taken for encryption and decryption, and storage overhead were computed for a plaintext with a varying number of words as shown Figure 4a, Figure 4b and Table 1 respectively.

Figure 3: RNS-B64 Based Cryptosystem Application

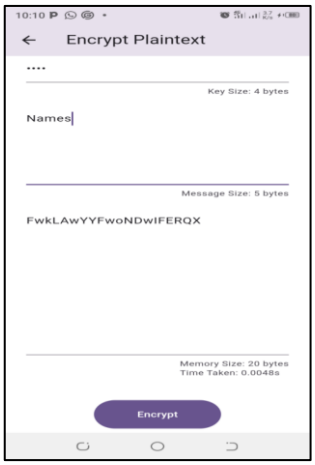

Figure 4(a): RNS-B64 Application Encryption Page Display

Figure 4(b): RNS-B64 Application Decryption Page Display

This section allows user to encrypt messages by supplying key and the message and then press "encrypt" button as shown in Figure 4a Encryption page.

RNS-B64 Application Decryption Page Display

In this section, users can decrypt the produced cipher text by providing the symmetric key. The cipher text produced in Figure 4(a), was supplied into the message box of the application decryption page and then press "decrypt" button as shown in Figure 4(b) Application Decryption Page to finally produce the initial original intelligible message.

Furthermore, the developed cryptosystem experimented upon with the samples of plaintext messages with bytes sizes variation for both the key and plaintext to determine the performance and efficiency of the developed system. The time taken for encryption and decryption, and storage overhead was computed with a varying number of words as shown in Table 1.

RNS-B64 Application Encryption Page Display

Table 1: Encryption Time, Decryption Time and Storage Overhead for different cases using RNS-B64 Based Cryptosystem

S/N	Number of Words (Plaintext)	Number of Bytes (Plaintext)	Plaintext (Bits)	Encryption Time(s)	Ciphertext (Bytes)	Decryption Time(s)
1	1	5	40	0.0005	20	0.0007
2	6	36	288	0.0012	144	0.0023
3	21	300	2400	0.0046	1216	0.0057
4	100	640	5120	0.0127	2624	0.0071
5	204	1033	8264	0.0232	4188	0.0109
6	612	4162	33296	0.1836	16864	0.0414
7	816	5544	44352	0.3250	22464	0.0554
8	1224	8322	66576	0.6943	33720	0.0829
9	3264	10240	81920	1.0787	41984	0.1036
10	6528	20480	163840	3.7052	83968	0.2073

The time required for encryption and decryption of different plaintext sizes by the developed cryptosystem is analyzed in figures 5 and 6 respectively. The RNS-B64 based cryptosystem's encryption and decryption times were found to grow with the size of the plaintext. Also, the decryption time of the developed cryptosystem is much shorter compare to encryption time as a result of storage overhead.

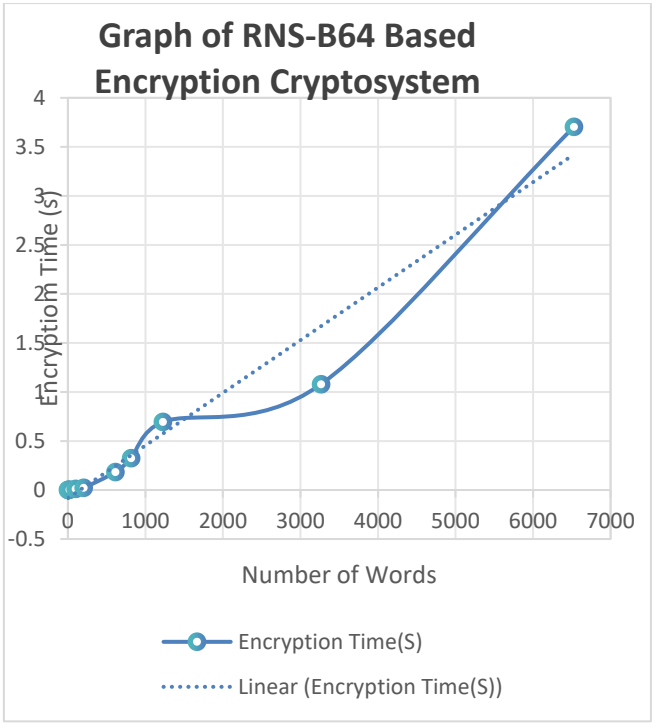

Figure 5: Graph of Number of words against Encryption time for RNS-B64

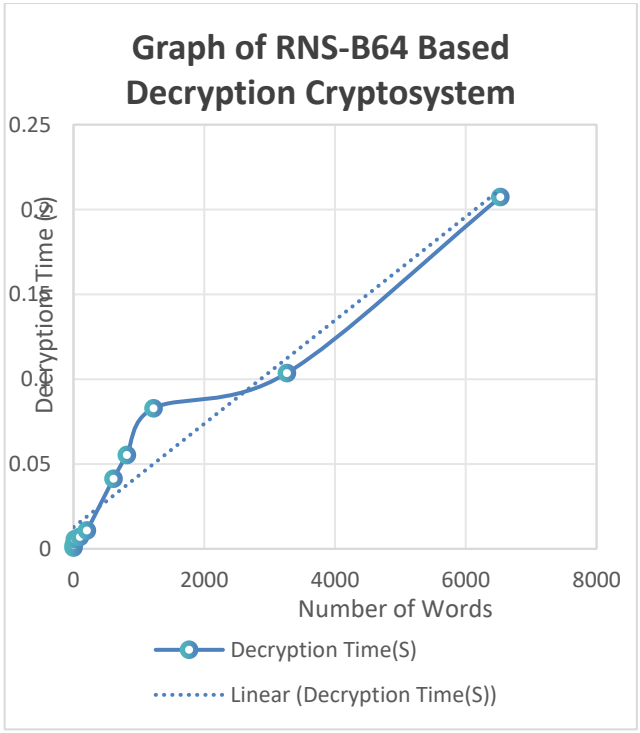

Figure 6: Graph of Number of words against Decryption time for RNS-B64

Discussion of Results on Comparison of the Developed RNS-B64 Based Cryptosystem with Existing Work

A comparison of the newly developed cryptosystem with the previous works is presented in Tables 2 and 3 respectively. It was demonstrated that, in terms of encryption and decryption execution times, the new cryptosystem (RNS-B64) outperforms the existing ones. Furthermore, the storage overhead of the developed cryptosystem is higher because RNS adds permutation and confusion to the developed cryptosystem, thus increasing the ciphertext and strengthening more the security mechanism of the cryptosystem.

Table 2: Comparison Based on Number of Bytes, Algorithm type, Encryption and Decryption Time.

Authors and Year	No of Bytes	Algorithm Type	Encryption Time(s)	Decryption Time(s)
[13]	16	Secret-key	0.0037	0.0029
RNS-B64 Based System	16	Secret-key	0.0005	0.0002

Table 3: Evaluation Based on Level of Security, Storage Overhead, Algorithm type, Encryption and Decryption Time.

Authors	Level of Security	Storage Overhead	Algorithm Type	Encryption Time	Decryption Time
[13]	Single-layer	High	Symmetric	Fast	Fast
RNS-B64 Based System	Single-layer	Higher	Symmetric	Faster	Faster

The cryptosystem was subjected to the dissimilar assessments which include encryption time, decryption time and storage overhead. The developed cryptosystem experimented upon with the samples of plaintext messages with bytes sizes variation for both the key and plaintext to determine the performance and efficiency of the developed system. A comparison of the newly developed cryptosystem with the previous works was presented. This demonstrated that the developed cryptosystem (RNS-B64) outperforms the existing ones based on the encryption and decryption execution times. Furthermore, the storage overhead of the developed cryptosystem is higher because RNS adds permutation and confusion to the developed cryptosystem, thus increasing the ciphertext and strengthening more the security mechanism of the cryptosystem.

CONCLUSION

This study uncovered some base64 algorithm research efforts as well as some constraints, thus providing a basis for improving the algorithm in terms of its security and efficiency. This leads to the development of the RNS-B64 cryptosystem, which addresses the Base64 security flaw and reduces the

encryption and decryption time. The study therefore increases the system's overall performance and efficiency thereby bridging the research gap. The analysis of the research revealed that the complexity of cryptanalysis rises as the parameters that were provided increase. In addition, the study conducted several different experiments using different sizes of plaintexts as shown in Table 1, to analyse and evaluate the performance of the developed system with the previous work as shown in table 2 and table 3 respectively. The results obtained show that RNS-B64 outperformed the previous work in terms of encryption and decryption time. For further research, comparism of our approach with other cryptographic algorithms techniques and attempt to conceal a secret image within the RNS-B64 scheme to observe the impact on security will be looked into.

REFERENCES

1. A. Guru and Ambhaikar, 'Development of "RSA" Encryption Algorithm for Secure Data Transmission', *Res. J. Comput. Inf. Technol. Sci.*, vol. 8, no. 1, pp. 9–12, 2020.
2. P. Chatzigiannis and K. Chalkias, 'Base64 Malleability in Practice', pp. 1–8, 2018.
3. K. B. Logunleko, O. D. Adeniji, and A. M. Logunleko, 'A Comparative Study of Symmetric Cryptography Mechanism on DES, AES and EB64 for Information Security', vol. Vol.8, no. Issue.1, pp. 45–51, 2020.
4. N. Taliasih and I. Afrianto, 'Implementation of RC4 and Base64 combination algorithm to secure client database of pt infokes.', 2020.
5. F. Baso, 'Analysis and Utilization of the Base64 Algorithm for Image Encryption and Decryption Security in Web-Based Images', *J. Secur. Comput. Inf. Embed. Netw. Intell. Syst.*, pp. 52–57, Dec. 2023, doi: 10.61220/scientist.v1i2.20233.
6. L. Djath, K. Bigou, and A. Tisserand, 'Hierarchical Approach in RNS Base Extension for Asymmetric Cryptography', in *2019 IEEE 26th Symposium on Computer Arithmetic (ARITH)*, Kyoto, Japan: IEEE, Jun. 2019, pp. 46–53. doi: 10.1109/ARITH.2019.00016.
7. A. Adebayo, A. AdeniyI, J. Ajao, R. Isiaka, kazeem Gbolagade, and S. Abdulsalam, 'Development of a Multi-Level Data Encryption Standard with Residue Number System for Data Security', in *Faculty of Communication and Information Sciences, University of Ilorin, Ilorin, Nigeria*, ILORIN: Faculty of Communication and Information Sciences, University of Ilorin, Ilorin, Nigeria(ICT4NDS2024), May 2024, pp. 15–34.
8. N. Singh, 'An overview of Residue Number System', *Natl. Semin. Devices Circuits Commun. Organ. Dep. ECE BIT Mesra*, p. Ranchi-835215, 2008.
9. K. Thiagarajan, P. Balasubramanian, J. Nagaraj, and J. Padmashree, 'Encryption and decryption algorithm using algebraic matrix approach', *J. Phys. Conf. Ser.*, vol. 1000, p. 012148, Apr. 2018, doi: 10.1088/1742-6596/1000/1/012148.
10. K. A. Gbolagade, J. Eseyin, and G. Akanni, 'A Residue Number System and Secret Key Crypto System Review in Cyber Security', vol. 7, no. 10, 2022.
11. D. R. Stinson, Maura. B. Paterson, and M. P. Paterson, *Cryptography : Theory and Practice*. in Forth Edition. CRC Press Taylor & Francis Group LLC, 6000 Broken Sound Parkway NW, Suite 300, Boca Raton London New York, FL 33487-2742, 2019. [Online]. Available: https://taylorandfrancis.com/
12. W. N. Baraka, S. Antao, and S. L. Loserian, 'Enhanced Security Model For Mobile Banking Systems In Tanzania', *Int. J. Technol. Enhanc. Emerg. Eng. Res.*, vol. 1, no. 4, pp. 4–19, 2013.
13. M. I. Rifki, M. E. Raditya, and A. H. Hasugian, 'Text Data Security Application Using a Mobile-Based Base64 Algorithm', vol. volume 15, no. 2, pp. 224–235, 2023, doi: Doi. 10.54209/jurnalkomputer.v15i02.146.
14. I. A. Aremu and K. A. Gbolagade, 'Information encoding and decoding using Residue Number System for {22n -1, 22n, 22n+1} moduli sets', *Int. J. Adv. Res. Comput. Eng. Technol. IJARCET*, vol. 6, no. 8, pp. 1260–1267, 2017.
15. L. Sousa, S. Antao, and P. Martins, 'Combining Residue Arithmetic to Design Efficient Cryptographic Circuits and Systems', *IEEE Circuits Syst. Mag.*, vol. 16, no. 4, pp. 6–32, 2016, doi: 10.1109/MCAS.2016.2614714.
16. I. Sumartono, A. P. U. Siahaan, and Arpan, 'Base64 Character Encoding and Decoding Modeling', *Int. J. Recent Trends Eng. Res. IJRTER*, vol. 02, no. 12, pp. 63–68, 2016, [Online]. Available: https://www.researchgate.net/publication/311715821
17. A. O. David and O. Sulaimon, 'Text Encryption with Improved Elliptic Curve Cryptography', *J. Adv. Math. Comput. Sci.*, pp. 32–41, Feb. 2023, doi: 10.9734/jamcs/2023/v38i31749.
18. A. Mittal and F. Sidney, 'Secure Data Communication Using Padding Key Encryption Cryptography Algorithm', in *2023 IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS)*, Raichur, India: IEEE, Feb. 2023, pp. 1–5. doi: 10.1109/ICICACS57338.2023.10099570.
19. M. Abu-Faraj, A. Al-Hyari, K. Aldebei, Z. A. Alqadi, and B. Al-Ahmad, 'Rotation Left Digits to Enhance the Security Level of Message Blocks Cryptography', *IEEE Access*, vol. 10, pp. 69388–69397, 2022, doi: 10.1109/ACCESS.2022.3187317.
20. D. R. Ignatius Moses Setiadi, E. Hari Rachmawanto, R. Zulfiningrum, and M. K. Sarker, 'Text Encryption using Transform Dimension, Bit Plane Slicing, and Chaos System', in *2022 International Seminar on Application for Technology of Information and Communication (iSemantic)*, Semarang, Indonesia: IEEE, Sep. 2022, pp. 51–55. doi: 10.1109/iSemantic55962.2022.9920413.
21. O. Reyad, H. M. Mansour, M. Heshmat, and E. A. Zanaty, 'Key-Based Enhancement of Data Encryption Standard For Text Security', in *2021 National Computing Colleges Conference (NCCC)*, Taif, Saudi Arabia: IEEE, Mar. 2021, pp. 1–6. doi: 10.1109/NCCC49330.2021.9428818.

\22. S. Kumar, M. S. Gaur, P. Sagar Sharma, and D. Munjal, 'A Novel Approach of Symmetric Key Cryptography', in *2021 2nd International Conference on Intelligent Engineering and Management (ICIEM)*, London, United Kingdom: IEEE, Apr. 2021, pp. 593–598. doi: 10.1109/ICIEM51511.2021.9445343.

23. I. A. Aremu and K. A. Gbolagade, 'An overview of Residue Number System', *Int. J. Adv. Res. Comput. Eng. Technol. IJARCET*, vol. 6, no. 10, 2017.
24. A. O. Sharoun, 'RESIDUE NUMBER SYSTEM (RNS)', pp. 265–270, 2013.
25. H. A.-J. Al-Asady, H. F. Fakhruldeen, and Y. Mudhafar, 'An image encryption method based on logistical chaotic maps to encrypt communication data', *Kufa J. Eng.*, vol. Vol. 15, no. No. 4, pp. 55–64, 2024, doi: https://doi.org/10.30572/2018/KJE/150405.
26. P. S. Uha, V. M. Akula, A. Sola, C. Shivani, R. R. Gajula, and M. Savaram, 'Digital Image Encryption Using Various Cryptographic Algorithms', *Int. J. Adv. Eng. Manag. IJAEM*, vol. 5, no. 11, pp. 229–241, 2023.

AUTHORS BIOGRAPHY

LOGUNLEKO, Kolawole Bariu is a Lecturer at the Computer Science Department, D.S. Adegbenro ICT Polytechnic Eruku-Itori, Ewekoro, Ogun State Nigeria. He bagged his B.Sc (Hons) Degree in

Mathematical Sciences (Computer Science Option) with Second Class Upper Division at the Federal University of Agriculture, Abeokuta, Ogun State, Nigeria and his Master Degree in Computer Science at the prestigious Premier University, University of Ibadan, Oyo State, Nigeria. At present, he is a PhD student at the Department of Computer Science, Kwara State University, Malete, Ilorin, Nigeria. Besides, he is an active member of the Computer Professionals (Registration Council of Nigeria), Nigeria Computer Society, Academia in Information Technology Professionals among many others. His research interest includes Cryptography, Information Security, Computer Arithmetic and Parallel Computing. Logunleko, K.B attended both Local and International conferences and has several Conferences and Journals publications.

LOGUNLEKO Abolore Muhamin, PhD bagged BSc Mathematical Sciences (Computer Science) from the University of Agriculture, Abeokuta, Ogun State, Nigeria in the year 2007. He bagged Master of Science Computer Science from premier university, University of Ibadan, Nigeria in the year 2012 and Doctor of Philosophy Computer Science (Information Security) at Kwara State University Malete, Ilorin, Nigeria in the year 2022. At the moment, he is a lecturer at Gateway Polytechnic, Saapade, Ogun State, Nigeria. He authored and co-authored many publications both in international and national journals. His research interest includes Cybersecurity, Information Security, Cryptography, Computer Arithmetic, Parallel Computing, Software Development and Database System. He belongs to many professional bodies such as the British Computer Society, Computer Professional Regulation Council of Nigeria, Nigeria Computer Society, Information Technology Security System Professional, Academia in Information Technology Professionals, Nigeria Information Tech. Professional in Civil & Public Service etc.

Dr (Mrs) ASAJU-GBOLAGADE, Ayisat Wuraola is a Senior Lecturer in the Department of Computer Science, Faculty of Communication and Information Sciences, University of Ilorin, Ilorin, Nigeria with about nine years of university teaching, research, and administrative experiences. She served as a Students Level Adviser, Faculty Representative to Junior Staff Appointment and Promotion Committee, her area of research interest cut across Data Science, Machine Learning, Artificial Intelligence and Residue Number systems. She has to her credit over twenty publications in reputable outlets like Elsevier, Springer, among others covering journals, edited conference proceedings and chapters in books. She was part of the team that won 2020 ETF Institutional research grant and 2021 National TETFUND grant.

BABATUNDE, Akinbowale Nathaniel received B.Sc, M.Sc and Ph.D. degrees from the Computer Science Department, University of Ilorin. He joined Kwara State University, Malete as a Lecturer in the Department of Computer Science, in 2013. He has authored and co-authored several publications from both international and national journals. He is a member of Computer Professionals of Nigeria, Institute of Electrical and Electronics Engineers (IEEE) and of the Internet Society. His research interest includes information security, computer arithmetic and natural language processing.

Prof. GBOLAGADE Kazeem Alagbe received his PhD in Computer Science from the Delft University of Technology in the Netherlands, his M.Sc and BSc in Computer Science from the University of Ibadan and Ilorin, respectively, in Nigeria. He began his lecturing career at the Olabisi Onabanjo University, Ago-Iwoye, Ogun State Nigeria in January 2002 and rose through the ranks to be appointed a professor of Computer Science in March, 2014 at the prestigious Kwara State University, Malete, Kwara State, Nigeria. Professor Gbolagade has supervised twenty-eight PhD Students to completion and a number of Students at MSc and undergraduate levels. He is the author of more than 150 scholarly works published in prestigious peer-reviewed journals and conferences. In June 2018, he was given the inaugural Post Professorial Achievement Award. He is a FELLOW of the prestigious Chartered Institute for Entrepreneurship and Community Development (FPAI) as well as of the Nigeria Computer Society (FNCS). Among many other professional associations, Professor Gbolagade is an active member of the Computer Professionals (Registration Council of Nigeria)-CPN.