Kasu Journal of Computer Science Vol. 1 No. 2 [June, 2024], pp. 265-279
https://doi.org//10.47514/kjcs/2024.1.2.009

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

An Enhanced Message Encryption Approach Using Residue Number System

Kafayat Odunayo Tajudeen[1], Ahmed Oloduowo Ameen[2], Oladele Taye Aro[3], Akeem Femi Kadri[4], Ayisat Wuraola Asaju-Gbolagade[5]
[1, 3] Department of Computer Science, Al-Hikmah University, Ilorin, Kwara State, Nigeria
[2, 5] Department of Computer Science, University of Ilorin, Ilorin, Kwara State, Nigeria
[4]Department of Computer Science, Kwara State University, Malete
kotajudeen@alhikmah.edu.ng[1], aminamed@unilorin.edu.ng[2], taiwo774@gmail.com[3], akeem.kadri@kwasu.edu.ng[4], gbolagade.aaw@unilorin.edu.ng[5]

Abstract

Safe transmission of messages over the internet is ensured by data security. The data should be protected against unauthorized access and transmitted to the legal recipient safely and formally called cryptography. The well-known cryptography types are asymmetric and symmetric and different symmetric encryption algorithms such as Advanced Encryption Standard (AES), Data Encryption Standard (DES), Blowfish were proposed to protect the confidentiality of the transmitted and stored data. However, most of these symmetric techniques are vulnerable to brute-force attack because the cipher text remains unintelligible for the original data to be found. Consequently, this challenge prompted researchers to introduce Residue Number System for encryption. RNS helps to withstand the vulnerability of the encryption algorithms in brute-force attacks making transmitted and stored data more secure. Hence, this paper introduced encryption by using RNS to improve the security of transmitted data. Traditional moduli set set $\{m_1 = 2^n - 1, m_2 = 2^n \text{ and } m_3 = 2^n + 1\}$ *and Chinese Remainder Theorem (CRT) were used to encrypt and decrypt the data based on information exchange. Furthermore, this is done by representing each character in the plaintext data is assigned a unique number value and which is done by converting each character into its ASCII value and the ASCII value is then converted to Excess-3 value. Thus, anytime an attacker tries to access the data, the RNS algorithm will generate residues data, this helps to discourage an attacker from further threat. The result showed that the proposed system was able to resist brute-force attacks compared to others systems. Values of n for the moduli set were dynamic against encryption and decryption of data.*

Keywords: Plaintext Data, Data transmission, Moduli Set, Chinese Remainder Theorem, Residue Number System Encryption

1. Introduction

The prevalent usage of cryptography is a significant consequence of the information uprising. With the advent of electronic communications on computer networks, users need a method to ensure that conversations and transactions remain strictly confidential. It is believed that the art of writing and cryptography are complementary. Humans became arranged into tribes, societies, and kingdoms as civilizations developed. As a result, concepts like politics, dominance, power, and wars emerged (Kapoor, 2022). The aforementioned concepts additionally stimulated individuals' innate need to discreetly communicate with specific recipients, hence guaranteeing the ongoing advancement of cryptography. The roots of cryptography are found in Roman and Egyptian civilizations (Dewangan, 2020). Every society needs secure information. Therefore, cryptography was introduced to keep our information secure

Kasu Journal of Computer Science Vol. 1 No. 2 [June, 2024], pp. 265-279
https://doi.org//10.47514/kjcs/2024.1.2.009

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

(Elhoseny et al., 2020). Using cryptography, one can communicate securely when there are third parties present (Sarkar, 2021) Transforming legible and intelligible data into an unintelligible format is known as cryptography, and it is used to protect data (Mardon et al., 2021).

The term "cryptography" also precisely refers to the process of hiding the contents of messages; it is derived from the Greek words "Kryptos," which means concealed, and "graphikos," which means writing (Patil et al., 2021). The original text that must be hidden is known as plaintext; it can take any form, including characters, numbers, executable programs, images, and other types of data (Majeed, 2021). For instance, the text at the recipient after decryption or the message sent to the sender prior to encryption are examples of plaintext (Obaid, 2018). "Cypher text" describes the data that will be sent as a string of incoherent characters that only the recipient needs to understand (Kumar, 2018). This data will be sent precisely via the network; several methods are employed to convert plaintext into encrypted text (Abdullah, 2017).

Today, Cryptography is of one-way and two-way encryption techniques. The one-way symmetric key cryptography is also called secret key cryptography which uses the same key at the source and destination, while two-way asymmetric key cryptography is also called public key cryptography which uses different keys at the source and destination (Geetha et al., 2023). This act of cryptography has grown in importance in computing technologies for banking services, medical systems, transportation and other Internet of Things-based applications (Rana et al., 2022).

Researchers continue to build and improve cryptographic algorithms to stay ahead of evolving threats posed by hackers and other adversaries (Kaur & Ramkumar, 2022). Due to their increased computational requirements, asymmetric encryption methods like RSA and Diffie-Hellman operate almost a thousand times more slowly than symmetric methods (Sarumi, 2022). Typically, symmetric key algorithms are faster than those of the asymmetric algorithms (Bao & Xue, 2021). So, the better suitable method to encrypt the large text data is, to encrypt it with symmetric key encryption algorithms. Comparing symmetric encryption algorithms like DES, AES, Blowfish, and others to their asymmetric counterparts, RSA and ECC are more resistant to Brute-Force assaults, illegal access, and network hacking (Patil & Popat, 2022).

RNS is an integer system that divides numbers into smaller components so that one is independent of the other, therefore speeding up arithmetic operations (Oke et al., 2021). Remainder arithmetic units, a binary to residue converter, and a residue to binary converter are the three essential components of an RNS architecture (NavaeiLavasani et al., 2020). For reverse conversion, the Chinese Remainder Theorem (CRT) and Mixed Radix Conversion (MRC) are the two most popular methods (Kuchukov et al., 2023). Therefore, an RNS approach that completely alters the message's uniqueness is needed to prevent attackers from knowing about the encrypted contents and to make deciphering the message difficult.

2. Related Works

Cryptography is the collection of secure information and communication techniques employing mathematical concepts and algorithms used to disguise the content of messages. The technique of cryptography involves the process of hiding or coding information so that only the person a message was intended for can read it. The art of cryptography has been used to code messages for thousands of years and continues to be used in bank cards, computer passwords, and ecommerce. The method of cryptography also entails data encryption that makes it possible to send confidential data in a way that only the recipient with the cipher key can decipher (Dixit, 2018). The process of transforming encrypted content back into legible, readable text is known as data decryption. This phrase could be used to describe a process that uses the appropriate keys to unencrypt the data. (Chaudhari, 2017). Figure 1 shows the diagrammatic representation the process cryptography

Kasu Journal of Computer Science Vol. 1 No. 2 [June, 2024], pp. 265-279
https://doi.org//10.47514/kjcs/2024.1.2.009

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

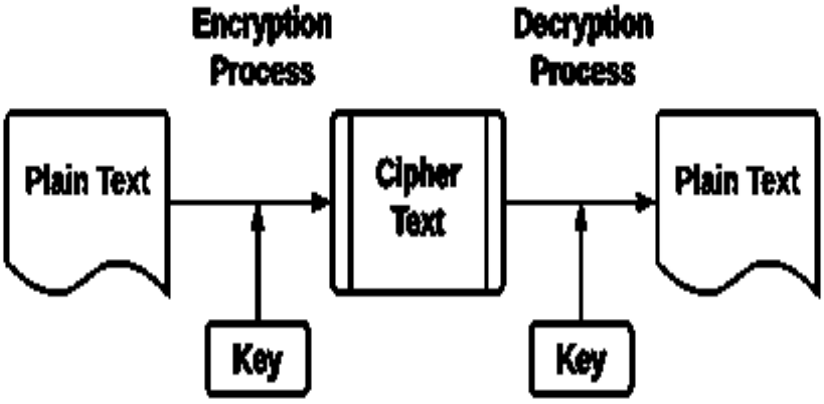

Figure 1: Process of cryptography (Abella, 2022)

2.1.1 Concept of Cryptography

There are two branches cryptography symmetric cryptography and public key (asymmetric) cryptography. the key used for encryption and decryption are identical in symmetric cryptography.

2.1.1 Symmetric key Cryptography

In symmetric key cryptography, sometimes referred to as private-key cryptography, a secret key is either shared by the sender and the recipient of the communication, or it can be held by a single individual. When sending confidential messages between two parties via private key cryptography, a copy of the secret key must be kept by both the sender and the recipient (Sharma, 2017). The challenge with secret keys is transferring them via the internet without letting them get into the wrong hands. The message can be decrypted by anybody with the secret key (Martin, 2020). (Martin, 2020). Examples AES, Blowfish, Twofish, DES, 3DES, RC2, RC4 and so on. Figure 1 shows the concept of cryptography.

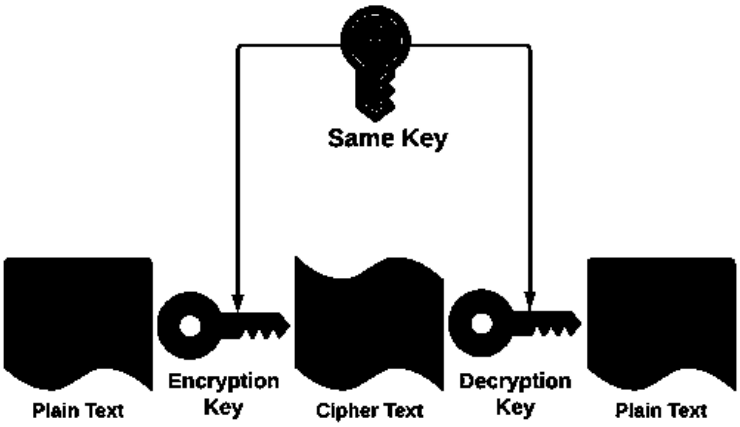

Figure 2: Symmetric Encryption (Tushar et al., 2021)

2.1.2 Asymmetric Key Cryptography

Asymmetric key cryptography is when two unique keys are utilized for encryption and decoding process, it is called public key cryptography. Public key is applied for encryption process and private key is used for

Kasu Journal of Computer Science Vol. 1 No. 2 [June, 2024], pp. 265-279
https://doi.org//10.47514/kjcs/2024.1.2.009

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

unscrambling process. It is also called asymmetric cryptography. For example, RSA and Elliptic Curve. Examples are RSA, ECC etc. However, asymmetric encryption has a speed disadvantage over symmetric encryption (Yassein et al., 2018). The message's content must be encrypted and decrypted using much more computing resources (Aljawarneh, 2017).

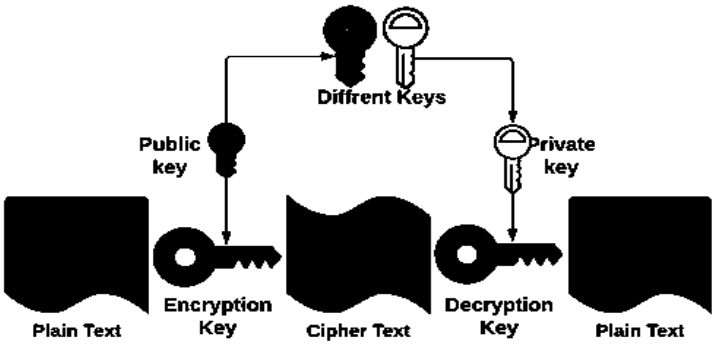

Figure 3: Asymmetric Encryption (Tushar et al., 2021)

Parekh et al (2024) provides robust resistance against attacks by combining the Affine Cipher, RSA, and XOR algorithms with randomly generated keys. The algorithm divides the movie into digestible chunks first, and then uses the Affine Cipher technique to randomly produce a unique key for each chunk. Next, to ensure a safe transfer to the receiver, the keys are encrypted using the RSA technique. Using a random number generator, a new key is created for each unique video clip in order to boost security. To provide an additional layer of security, the proposed approach also encrypts the video data using the XOR algorithm. The XOR method prevents the encrypted video data from being viewed without a matching key. experimental results of this study show that the proposed strategy provides robust security against multiple types of assaults, such as statistical, brute-force, and differential attacks. By encrypting and decrypting video data nearly instantaneously, the technique further demonstrates its exceptional efficiency. In just 174.25 and 136.38 nanoseconds, respectively, can a pixel be encrypted and decrypted. A number of applications, including online video streaming, video conferencing, and video surveillance, can benefit from the use of the proposed algorithm since it provides a dependable, efficient, and secure solution for video encryption.

Sawant et al (2024) demonstrates the development of a safe image encryption technique using symmetric data encryption in Python. The algorithm's main computations include Mix Columns, a Key Dependent Ex-Or operation involving the matrix's upper and lower triangular parts, Shift Rows, and a Customized Sub Bytes transformation that creates confusion and diffusion. The algorithm's integrity, confidentiality, and authenticity are demonstrated by the results of several analyses that were done on it.

Kuppuswamy and Sivakumar (2024) In their study, proposes a hybrid cryptosystem that utilizes the benefit of both symmetric key and asymmetric cryptographic methods. For encryption and decryption of any data, a secure key is required. Satisfying security requirements is one of the most significant goals for cryptography system security designers. In this research article, the proposed scheme has been designed for securing transactions by using the well-known public key RSA algorithm and symmetric key algorithm, which is based on simple integer numbers. Experimental results show that the new hybrid method improves both the interacting performance and the security service for desired data communication transactions. Several points can be concluded from the experimental results. Based on the results, security, and

Kasu Journal of Computer Science Vol. 1 No. 2 [June, 2024], pp. 265-279
https://doi.org//10.47514/kjcs/2024.1.2.009

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

performance analysis with various metrics has been concluded that the proposed method consumes a reasonable amount of encryption and decryption time with better security than alternative methods.

Madamiovich (2024) states that data encryption has emerged as a crucial approach to ensuring data security and confidentiality in cloud settings. Some common data encryption algorithms used in advancing cloud storage data security and confidentiality are symmetrical and asymmetrical data encryption technologies. Cloud storage has evolved how individuals and organizations store their data. As a modern technological development, cloud storage creates trustworthy storage, management, and retrieval of data.

Zhang and Cao (2022) presents an enhanced AES algorithm-based secure encryption technique for data related to online transactions. To achieve transaction processing, several private chains are created when the e-commerce transaction method is examined. Each business in the database generates the AES encryption algorithm key using its unique certificate. The affine S-box of the AES encryption technique is transformed using affine transformation, and data encryption and decryption are accomplished using a pseudo-random number key stream. For e-commerce transaction data, a secure encryption method has been developed and finished. The outcomes of the experiment demonstrate that this strategy has some practical value and can reduce the time needed for data encryption.

Sanap and More (2021) provides an outline of the encryption methods that can be used to improve data security. The security aspects and design processes of the most popular symmetric encryption algorithms, such as DES, 3DES, and AES, are analysed in this study. Additionally, entropy, floating frequency, and histogram comparison and analysis of various encryption processes are carried out.

Kumar and Karthigaikumar (2020) gives an effective and novel key-dependent AES technique is introduced to secure data stored digitally in any remote place or transmitted over the internet. The avalanche effect provided by this proposed work is stricter and better than that of the original AES algorithm. Once 1000 pairs of samples with various secret keys have been tested, the suggested algorithm's results are achieved. Results indicate that, in 58% of cases, the new algorithm that is proposed outperforms the current technique in terms of avalanche impact.

Salih et al (2020) suggests a technique to improve AES security that is built upon two approaches. The first technique builds on a prior work titled a Novel Approach for Enhancing Security of Advance Encryption Standard using Private XOR Table and 3D chaotic regarding to Software quality Factor. Instead of using the fixed XOR operation utilized in AES rounds, the current study creates a dual dynamic XOR table using 3D chaotic map. The dual dynamic XOR table consists of two bits for odd rounds and one bit for even rounds. The second method is the dynamic MixColumns transformation, which uses a 3D chaotic map to create a dynamic, private maximum distance separable (MDS) matrix in place of the MixColumns transformation's fixed and public MDS matrix. Secret keys are generated via a 3D chaotic map. These upgrades improve the security of AES, especially its ability to fend off attacks. The suggested method's security is examined using the histogram, entropy, correlation coefficient, and Diehard and NIST tests. The suggested and unique algorithms are implemented using C++. For the security analysis, MATLAB and LINX are employed. The suggested approach outperforms the original AES, according to the results.

Awan et al (2020) presents a framework with important characteristics including owner data privacy and improved security. By using a double round key feature, Encryption is accelerated by 1000 blocks per second compared to the original 128 AES approach by utilizing a double round key feature. On the other hand, the conventional method uses a single round key that executes 800 blocks every second. The proposed algorithm minimizes power consumption, enhances load balancing, and manages network resources more effectively. The proposed architecture includes the deployment of AES with 16, 32, 64, and 128 plain text

Kasu Journal of Computer Science Vol. 1 No. 2 [June, 2024], pp. 265-279
https://doi.org//10.47514/kjcs/2024.1.2.009

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

bytes. The simulation results' visual representation demonstrates how well the approach works to achieve particular quality standards. Based on the findings, the recommended framework lowers energy usage by 14.43%, delays by 15.67%, and network utilization by 11.53%. As a result, the suggested framework improves security, decreases resource usage, and shortens deployment times for computational cloud services.

Lavanya and Karpagam (2020) focuses on aims to decrease the risks by increasing the difficulty of cryptanalysis by minute modifications to the shift row transformation and key expansion unit of the AES algorithm. The recommended small-scale discrepancies in the word column of the key expansion unit and the linear layer of the cipher unit generate confusion during encryption. The modified method is found to have higher diffusion and confusion features in terms of balance, Strict Avalanche Criterion, and bit independence criterion. The AES variations are further assessed using the NIST-800-22 statistical test package for random number generators. Additionally, this study proposes an obfuscation control unit that allows the three AES variants to be selected on-demand, resulting in a modifiable encryption pattern for a plaintext-key pair.

Assaf and Hashim (2020) Suggests the use of the Avalanche Effect to assess the performance of the Advanced Encryption Standard (AES) in Cipher Block Chaining (CBC) mode, with an emphasis on security. This research introduces a novel, enhanced method for boosting AES-CBC security. Prior to encryption rounds, in CBC mode, the Unix time serves as the source for the Initialization Vector (IV). The outcomes demonstrated that the method produces distinct ciphertext on each run. Stated otherwise, the likelihood of deciphering the encryption key is much reduced when distinct ciphertext output is used. Additionally, the outcomes are checked to see if they meet the security requirements and investigated utilizing the Avalanche Effect. The obtained outcomes demonstrated that, by stopping the encryption key update for each new ciphertext, the encryption technique is able to preserve the avalanche effect requirement and give extra strength to the encryption process.

Zodpe and Sapkal (2020) introduce a novel method that makes use of the PN Sequence Generator to produce the modified S-box values and initial key needed for encryption or decryption (better key creation). By comparison with the original AES method, the proposed modifications to the AES algorithm demonstrate a notable enhancement in the encryption quality. A 60% avalanche effect and enhanced key generation make the conventional AES algorithm impervious to attacks when combined with the newly suggested unique modified S-box approach. Throughput is significantly increased when the suggested design is synthesized on different Field Programmable Gate Array (FPGA) devices when compared to the current designs. The Spartan6 FPGA device is used to implement the suggested design.

Arman et al (2020) provides significant improvements over Advanced Encryption Standard, emphasizing the Symmetric Key Cryptosystem and AES algorithm for security and simplicity of use. Various metrics, including data block size, run-time, compile time, encryption/decryption speed, and so on, were used to compare the performance. This experiment was primarily designed to use a real-world application to test the newly improved AES's superior efficacy over the original AES. There were three new procedures implemented: the removal of the Mix-Column process, the right shift key approach, and a new key implementation process. The proposed approach can be applied to other versions as well; calculations based on the AES-128-bit version are reported in this study. Achieving quick execution times and low memory consumption while maintaining robust security was the aim. Our approach produced improved net execution time and 88% throughput, as the data shows. Compared to the conventional AES, this has a significant increase in efficiency.

Marqas and Ihsan (2020) computes the execution time consumed for asymmetric encrypting algorithm (RSA) and symmetric encrypting algorithm (AES) cryptography algorithm in encryption and decryption for message of various words length. The experimental result shows that AES has better execution time

Kasu Journal of Computer Science Vol. 1 No. 2 [June, 2024], pp. 265-279
https://doi.org//10.47514/kjcs/2024.1.2.009

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

than RSA in encryption and decryption. The paper also shows that AES has three different key sizes (128,192,256) whereas RSA has only two different key size (1024,4096) in other way the AES is more flexible than RSA and in addition the features of AES show better performance and faster than RSA. Over all the result shows that symmetric algorithms (AES) are better than an asymmetric algorithm (RSA).

Conclusively, it was observed that most of all the literatures reviewed has recorded an avalanche effect of no more than 60% and also therefore, this proposed study will perform more better in security strength.

3. Methodology

3.1 Character Representation and Forward Encryption

The first phase of proposed method involves the representation of each of the letter to ASCII decimal values using a created character as shown in Table 1. The designed table ensure that only lower-case characters such as alphabets are used.

Table 1: Lowercase letters represented in ASCII decimal values

Lower-case letters	ASCII Decimal values	Excess-3 Decimal Values	Lower-case letters	ASCII Decimal values	Excess-3 Decimal Values
a	97	100	o	111	114
b	98	101	p	112	115
c	99	102	q	113	116
d	100	103	r	114	117
e	101	104	s	115	118
f	102	105	t	116	119
g	103	106	u	117	120
h	104	107	v	118	121
i	105	108	w	119	122
j	106	109	x	120	123
k	107	110	y	121	124
l	108	111	z	122	125
m	109	112			
n	110	113			

Moduli set of set $\{m_1 = 2^n - 1, m_2 = 2^n \; and \; m_3 = 2^n + 1\}$ is used for the forward encryption for every letter in the message. To compute the moduli, n in the moduli set is given a numerical value. Three residue numbers should be produced for every letter in the excess-3 values representation using the moduli set. From the generated residue numbers, a matrix is created, containing the cipher-text, with a row for each letter in the original message.

3.2 RNS Encryption Approach

3.2.1 RNS Forward Decryption Stages

Kasu Journal of Computer Science Vol. 1 No. 2 [June, 2024], pp. 265-279
https://doi.org//10.47514/kjcs/2024.1.2.009
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

The RNS forward encryption is achieved using

$x = mi\ [x\ mi/] + |x|m$ (1)

When the integer to be transposed is x, and m is the modulus.

3.2.2 The RNS Backward Decryption Stages

The Chinese Remainder Theorem will be used to convert the residues produced during the encryption procedure backward during the decryption phase. The RNS to decimal conversion is accomplished using this theorem. Given the residue representation $\{r1, r2, \ldots, rn\}$ of c, the CRT makes it possible to determine $|c|m$, provided the gcd of any pair of moduli is 1. Pairwise relative primes are moduli of this type

The CRT is given by:

$|x| = |\sum_{j=1}^{N} \hat{m}j\ |\frac{rj}{\hat{m}j}|mj|m$ (2)

where

$\hat{m}j = \frac{M}{mj}$, $M = \prod_{j=1}^{N} mj$ (3)

and

$\gcd(m_j, m_k) = 1 for\ j \neq k$ (4)

$X = |x_1|m_1|\hat{m}j|m_1 + |x_2|m_2|\hat{m}_2|m_2 + |x_3|m_3|\hat{m}_3|m_3$ (5)

3.3 Algorithm of Message M Encryption

ALGORITHM 1: Message M Encryption Algorithm

Step 1: Start
Step 2: Input the message of specified size
Step 3: Represents each character in ASCII Decimal values
Step 4: The ASCII Decimal values are converted to Excess-3 Decimal values
Step 5: Choose moduli set to be used
Step 6: When computing your moduli, set the value for n.
Step 7: Afterwards, the RNS forward encryption is used to transform the produced Excess-3 values into residues.

Step 8: Stop

3.4 Algorithm for Cipher C Decryption

Kasu Journal of Computer Science Vol. 1 No. 2 [June, 2024], pp. 265-279
https://doi.org//10.47514/kjcs/2024.1.2.009

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

ALGORITHM 2: Ciphertext C Decryption Algorithm

Step 1: Start

Step 2: One row at a time, read each residue.

Step 3: Apply the Chinese Remainder Theorem to the residues to do a reverse conversion and use the moduli set set $\{m_1 = 2^n - 1, m_2 = 2^n \; and \; m_3 = 2^n + 1\}$ to generate the corresponding Excess-3 values.

Step 4: To retrieve the ASCII values in turn, subtract the extra decimal value of three from the Excess-3 numbers that were generated.

Step 5: The built-in character function in MATLAB is then used to decrypt the ASCII values and retrieve the original plain message M.

Step 6: Stop

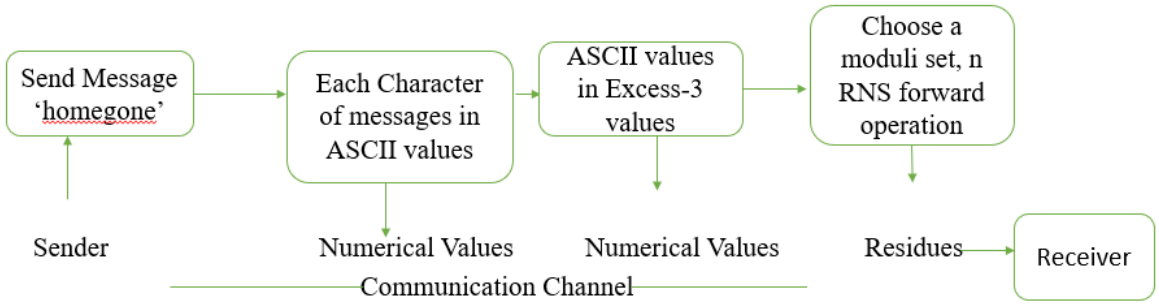

Figure 4: Framework for the proposed Model

The framework shows: the steps involved in the system development, and how RNS encryption is being used to encrypt plaintext message to improve its security. Keyboard characters was used as the dataset, and different message was generated for the evaluation, among these is 'homegone' which was used as the message sent from the sender to the receiver.

Figure 4 showed how the plaintext was first substituted to ASCII decimal number at the beginning of the encryption process, this was done using standard character to decimal conversion table as shown in table 1, after which the substituted data was encoded by an increase of value three, then the encoded message was further encrypt with RNS to generate the residues. The residue generated was sent through a communication channel to the receiver. At the receiver side, residue was decrypted using Chinese remainder theorem to decode the residues and finally converted to the original message. This enables the system to secure text data.

Figure 4 shows how the message was encrypted with RNS Encryption. Each character of the original message M was exchanged with ASCII decimal values, the ASCII decimal values was encoded with additional increased of three and the encoded data were encrypted using Residue Number System. RNS forward converter was used with 2- and 3-digit numbers to generate the key. Below is the procedure;

i. Given the moduli set set $\{m_1 = 2^n - 1, m_2 = 2^n \; and \; m_3 = 2^n + 1\}$, take n=2. Consider X representing the character 'h' of a message to be encrypted, ASCII character representation h = X = 104

Kasu Journal of Computer Science Vol. 1 No. 2 [June, 2024], pp. 265-279
https://doi.org//10.47514/kjcs/2024.1.2.009

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

and Excess-3 representation of X = 104 + 3 = 107. Then the conversion process is as follows; If X = 107, and n = 2 to encrypt X by RNS, for moduli set $\{m_1 = 2^n - 1, m_2 = 2^n \; and \; m_3 = 2^n + 1\}$, we have, the moduli ($m_3 = 2^2 - 1, m_2 = 2^2 \; and \; m_1 = 2^2 + 1$) = (4 - 1, 4, 4+1) = (3, 4, 5). The dynamic range M of moduli (3, 4, 5) = 3 * 4 * 5 = 60.

To get the residue, we have 107 = 01101011 = (8 bits) X is partitioned into 3 blocks; we partition X = 107 into 3-bits block.

Therefore; $r_1 = |107|_3 = 2$

$r_2 = |107|_4 = 3$

$r_3 = |107|_5 = 2$

This implies that |107| 9, 8,7 = {8, 3, 2}. This is the ciphertext that the recipient got, r1, r2 and r3 represent the residues of decimal 'h'. M is the dynamic range which is the multiplication of all the moduli in the moduli m_j.

which is

$\hat{m}j = \frac{M}{mj}$, $M = \prod_{j=1}^{N} mj = 3 * 4 * 5 = 60$

While $| \hat{m}1 |_{m1}$ is the multiplicative inverse of m_j with respect to moduli

$| \hat{m}_1|_{m1} = | \frac{60}{3} |_3 = | 20^{-1}|_3 = 2$ then $| \frac{1}{\hat{m}1} | = 2$

$| \hat{m}_2|_{m2} = | \frac{60}{4}|_4 = | 15^{-1}|_4 = 3 \quad | \frac{1}{\hat{m}2} | = 3$

$| \hat{m}_3|_{m3} = | \frac{60}{5} |_5 = | 12^{-1}|_5 = 3 | \frac{1}{\hat{m}3} | = 3$

$X = |x_1|m_1|\hat{m}j|m_1 + |x_2|m_2|\hat{m}_2|m_2 + |x_3|m_3|\hat{m}_3|m_3$

= ((20 * 2 * 2) + (15 * 3 * 3) + (12 * 3 * 2))

$= |80 + 135 + 72|_{60}$

$= | 287|_{60}$

= 47

Verifying the residue values through the following:

47 mod 3 = 2

47 mod 4 = 3

47 mod 5 = 2

So, the decimal number x for residue (2, 3 ,2) for moduli set $\{2^n - 1, \; 2^n, \; 2^n + 1\}$ and moduli {3, 4, 5} when n = 2, is 47. The decimal was then converted back to character to get the original message.

4. Results and discussion

Kasu Journal of Computer Science Vol. 1 No. 2 [June, 2024], pp. 265-279
https://doi.org//10.47514/kjcs/2024.1.2.009

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

The study shows the result of the message encryption as shown in Figure 5 which indicate how the message is being encrypted and what the receiver will first see before decrypting the message. Figure 4 illustrates how the original data "homegone" was converted to ASCII code, each ASCII has been encoded with Excess-3 conversion and then the encoded decimal number is encrypted with Residue Number System using forward conversion method based on moduli set $2^n - 1,\ 2^n,\ 2^n + 1\}$ and value of 'n' to generate the residue (ciphertext). With this, the system was able to encrypt the text message. The residue which is the ciphertext is sent to the recipient. Figure 4 shows several messages that have been delivered to the recipient's, the message delivered as a residue which needs to be decrypted by the recipient to get the original information. In order to decrypt the residues, the receiver needs to know the steps involved in decrypting the message, the numerical representation for the text data as RNS can only operate on numbers, the algorithms used, the moduli set used and also the value of n. The Chinese remainder theorem was used as the reverse conversion algorithm to generate the decimal. Then finally the code generated from RNS is converted to text using the MATLAB inbuilt function. The technique ensures an enhanced message security to access the secure message. The result of the decryption from the receiver side is also shown in Figure 5.

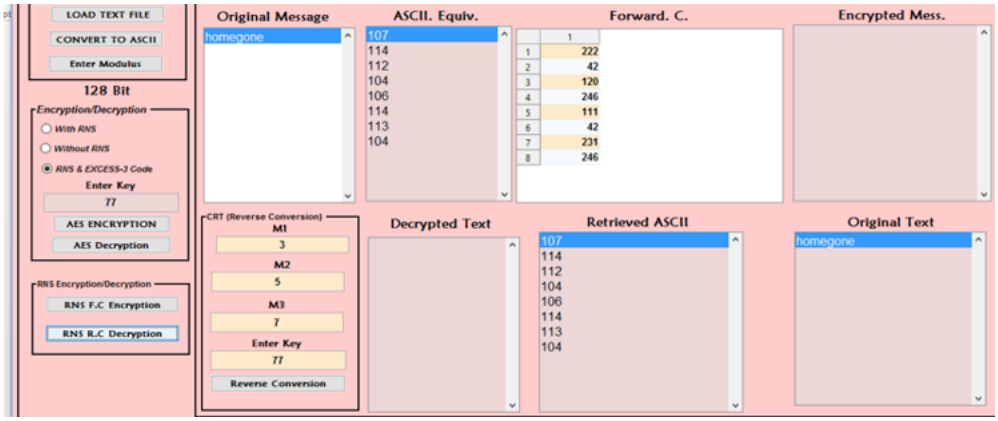

Figure 5: Graphical User Interface of RNS Message Encryption

Table 1. Comparison of conventional symmetric encryption with proposed technique.

Techniques for Conventional Symmetric Encryption	**Technique for RNS Encryption**
The keys sizes are constant in length	The moduli set can be dynamic
It's very easy to crack	It is not easy to crack
It's not secured enough	It's very secured
Mathematical operation is linear giving room to attacks	Involves some complex mathematical operations

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

Problems of key sharing	Has no problem of key distribution

5. Conclusion

Due to the security weakness of most of the existing data security techniques to brute-force attack, the study proposed an enhanced message Encryption with Residue Number System for securing transmitted data through an unsecure channel. The proposed technique provides an improved security to encrypted message by making it difficult because it requires a lot of effort for an attacker in determining the numerical computations involved, the algorithms used, moduli set, value of n and character representation that was used in the process of encryption and decryption. In the future, several aspects of this work can be explored, such as broaden by evaluating the performance of the system in terms of avalanche effect, execution time. Also, the future study can be widened into image security, video encryption and audio protection. Other character representations and applying of lower-case letters can also be considered as a future work.

Reference

Abdullah, A. M. (2017). Advanced encryption standard (AES) algorithm to encrypt and decrypt data. *Cryptography and Network Security*, *16*(1), 11.

Abella, F. A. (2022). IMPLEMENTATION OF CRYPTOGRAPHY USING AES-128 ALGORITHM. *Jurnal Ilmu Komputer (JIKOMP)*, *1*(1).

Abikoye, O. C., Haruna, A. D., Abubakar, A., Akande, N. O., & Asani, E. O. (2019). Modified advanced encryption standard algorithm for information security. *Symmetry*, *11*(12), 1484.

Akanni Gabriel, A., & Gbolagade, K. A. A Residue Number System and Secret Key Crypto System Review in Cyber Security.

Aljawarneh, S., Yassein, M. B., & Talafha, W. A. A. (2017). A resource-efficient encryption algorithm for multimedia big data. *Multimedia Tools and Applications*, *76*, 22703-22724.

Arman, S., Rehnuma, T., & Rahman, M. (2020). Design and implementation of a modified AES cryptography with fast key generation technique. In *2020 IEEE International Women in Engineering (WIE) Conference on Electrical and Computer Engineering (WIECON-ECE)* (pp. 191-195). IEEE.

Assafli, H. T., & Hashim, I. A. (2020). Security enhancement of AES-CBC and its performance evaluation using the Avalanche effect. In *2020 3rd International Conference on Engineering Technology and its Applications (IICETA)* (pp. 7-11). IEEE.

Awan, I. A., Shiraz, M., Hashmi, M. U., Shaheen, Q., Akhtar, R., & Ditta, A. (2020). Secure framework enhancing AES algorithm in cloud computing. *Security and communication networks*, *2020*, 1-16.

Bao, Z., & Xue, R. (2021). Survey on deep learning applications in digital image security. *Optical Engineering*, *60*(12), 120901-120901.

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

Chaudhari, S., Pahade, M., Bhat, S., Sawant, T., & Jadhav, C. (2017). A survey on methods of cryptography and data encryption. *Methods Cryptogr. Data Encrypt.*, *3*, 440-43.

Dash, S., Mondal, J., & Swain, D. (2023). A survey on symmetric text encryption techniques. In *AIP Conference Proceedings* (Vol. 2981, No. 1). AIP Publishing.

Dewangan, P. (2020). A review paper on network security and cryptography. *International Journal of Science and Research (IJSR)*, *9*(1).

Dixit, P., Gupta, A. K., Trivedi, M. C., & Yadav, V. K. (2018). Traditional and hybrid encryption techniques: a survey. In *Networking Communication and Data Knowledge Engineering: Volume 2* (pp. 239-248). Springer Singapore.

Elhoseny, M., Shankar, K., Lakshmanaprabu, S. K., Maseleno, A., & Arunkumar, N. (2020). Hybrid optimization with cryptography encryption for medical image security in Internet of Things. *Neural computing and applications*, *32*, 10979-10993.

Farooq, H. (2017). A Review on cloud computing security using authentication techniques. *International Journal of Advanced Research in Computer Science*, *8*(2).

Geetha, V., Singh, P., Patil, N. S., & Reddy, S. S. S. (2023). *Introduction To Cryptography And Network Security*. AG PUBLISHING HOUSE (AGPH Books).

Gudimetla, S. R. (2024). Data Encryption in Cloud Storage. *International Research Journal of Modernization in Engineering Technology and Science*, *6*, 2582-5208.

Kapoor, A. (2022). AES, DES, and RSA: A Comprehensive Study on Data Security Mechanisms. *Available at SSRN 4267943*.

Kaur, J., & Ramkumar, K. R. (2022). The recent trends in cyber security: A review. *Journal of King Saud University-Computer and Information Sciences*, *34*(8), 5766-5781.

Kuchukov, V., Telpukhov, D., Babenko, M., Mkrtchan, I., Stempkovsky, A., Kucherov, N., ... & Grigoryan, M. (2022). Performance Analysis of Hardware Implementations of Reverse Conversion from the Residue Number System. *Applied Sciences*, *12*(23), 12355.

Kumar, K., Ghosh, S., & Sahana, S. (2018). SECRET KEY BASED STRING REVERSE ENABLING USER LEVEL ENCRYPTION TECHNIQUE FOR DATA SECURITY. *International Journal of Advanced Research in Computer Science*, *9*(2).

Kuppuswamy, P., Al Khalidi, S. Q., & Sivakumar, N. R. (2024). Incorporating RSA with a New Symmetric-Key Encryption Algorithm to Produce a Hybrid Encryption System. *International Journal of Computer Science & Network Security*, *24*(1), 196-204.

Lavanya, R., & Karpagam, M. (2020). Enhancing the security of AES through small scale confusion operations for data communication. *Microprocessors and Microsystems*, *75*, 103041.

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

Lu, Y., Zhang, W., & Cao, L. (2022, October). Data Security Encryption Method Based on Improved AES Algorithm. In *2022 Global Reliability and Prognostics and Health Management (PHM-Yantai)* (pp. 1-6). IEEE.

Madamiovich, K. S. (2024). DATA PROTECTION AND ENCRYPTION METHODS. *Научный Фокус*, *2*(13), 135-139.

Majeed, M. A., Sulaiman, R., Shukur, Z., & Hasan, M. K. (2021). A review on text steganography techniques. *Mathematics*, *9*(21), 2829.

Manoj Kumar, T., & Karthigaikumar, P. (2020). A novel method of improvement in advanced encryption standard algorithm with dynamic shift rows, sub byte and mixcolumn operations for the secure communication. *International Journal of Information Technology*, *12*, 825-830.

Marqas, R. B., Almufti, S. M., & Ihsan, R. R. (2020). Comparing Symmetric and Asymmetric cryptography in message encryption and decryption by using AES and RSA algorithms. *Xi'an Jianzhu Keji Daxue Xuebao/Journal of Xi'an University of Architecture & Technology*, *12*(3), 3110-3116.

Martin, K. (2020). *Cryptography: The key to digital security, how it works, and why it matters*. WW Norton & Company.

NavaeiLavasani, P., Adeli, S., Taheri, M., Moaiyeri, M. H., & Navi, K. (2020). Fast and energy-efficient FPGA realization of RNS reverse converter for the ternary 3-moduli set {3 n–2, 3 n–1, 3 n}. *SN Applied Sciences*, *2*, 1-12.

Obaid, T. A., Khami, A. P. D. M. J., & Shehab, L. G. (2018). A classical approach for hiding encryption key in the same encrypted text document. *Journal of Kufa for Mathematics and Computer*, *5*(1), 25-38.

Oke, A. A., Nathaniel, B. A., Bukola, B. F., & Ayopo, O. A. (2021). RESIDUE NUMBER SYSTEM BASED APPLICATIONS: A LITERATURE REVIEW. *Annals. Computer Science Series*, *19*(1).

Parekh, A., Antani, M., Suvarna, K., Mangrulkar, R., & Narvekar, M. (2024). Multilayer symmetric and asymmetric technique for audiovisual cryptography. *Multimedia Tools and Applications*, *83*(11), 31465-31503.

Patil, B. P., Kharade, K. G., Kharade, S. K., & Kamat, R. K. (2021). Significant Study of Data Encryption and Steganography. *Recent Advances in Mathematical Research and Computer Science Vol. 1*, 79-91.

Patil, L. K., & Popat, K. A. (2022). Comparative Analysis of Several Approaches of Encoding Audio Files. In *International Conference on Advancements in Smart Computing and Information Security* (pp. 128-143). Cham: Springer Nature Switzerland.

Rana, A., Chakraborty, C., Sharma, S., Dhawan, S., Pani, S. K., & Ashraf, I. (2022). Internet of medical things-based secure and energy-efficient framework for health care. *Big Data*, *10*(1), 18-33.

Salih, A.I., Alabaichi, A.M., & Tuama, A.Y. (2020). Enhancing advance encryption standard security based on dual dynamic XOR table and MixColumns transformation. *Indonesian Journal of Electrical Engineering and Computer Science*.

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

Sanap, S. D., & More, V. (2021). Analysis of encryption techniques for secure communication. In *2021 International Conference on Emerging Smart Computing and Informatics (ESCI)* (pp. 290-294). IEEE.

Sarkar, A., Chatterjee, S. R., & Chakraborty, M. (2021). Role of cryptography in network security. *The" Essence" of Network Security: An End-to-End Panorama*, 103-143.

Sarumi, J. A. (2022). A review of encryption methods for secure data communication. In *Proceedings of the 30th iSTEAMS Multidisciplinary & Inter-tertiary Research Conference* (pp. 63-82).

Sawant, V., Solkar, A., & Mangrulkar, R. (2024). Modified symmetric image encryption approach based on mixed column and substitution box. *Journal of Applied Security Research*, *19*(2), 196-229.

Sharma, S. (2017). Cryptography: An art of writing a secret code. *International Journal of Computer Science & Technology*, *8491*(1).

Wenceslao Jr, F. V. (2018). Enhancing the performance of the advanced encryption standard (AES) algorithm using multiple substitution boxes. *International Journal of Communication Networks and Information Security*, *10*(3), 496.

Zodpe, H., & Sapkal, A. (2020). An efficient AES implementation using FPGA with enhanced