A New Cryptographic Model based on Residue Number System and Ribonucleic Acid Properties

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

Kolawole Bariu Logunleko
Dept. of Computer Science & Stas.
DS Adegbenro ICT Polytechnic,
Eruku-Itori, Ogun state, Nigeria

Kazeem Alagbe Gbolagade
Department of Computer Science,
Kwara State University, Malete,
Ilorin, Nigeria

ABSTRACT
The presence of information technology has drastically transformed ways of communication with one another. This development has tremendously increased the usage and ways of communication leaving behind the security consideration of what is being transmitted through a communication channel. Cryptography plays a vital role in securing information. Therefore, this research reveals a technical model on computation of the cryptography algorithms. The aim to be considered is the enhanced security of the encrypted data and thus fills the gap of security. Additionally, this newly concept integrate residue number system, Chinese reminder theorem and the properties of ribonucleic acid to generate a symmetric key by shuffling the key with the textual data, making the transformation of each character of the data better each time it is shuffled and thus, making the final output stronger to be broken. Subsequently, the developed concept secures the data more adequately than the existing one because of the designed pattern and confusion created during the process.

General Terms
Information Security, Encryption

Keywords
Residue Number System RNS, Chinese Remainder Theorem CRT, Deoxyribonucleic Acid DNA, Ribonucleic Acid RNA, RNA Binary Coded Scheme

1. INTRODUCTION
Nowadays, the entire globe is depending on internet and its application for their day to day activities. Security is necessary for an individual to maintain and manage the integrity of the data and information cross the internet [5]. [6][7] also emphasised that security and confidentiality is a crucial aspect of an information system. Here comes the requirement of securing information by ways of Cryptography. Cryptography is the most important automated tool for securing communication system. Additionally, in computer science, cryptographic algorithm consists set of complex mathematical formulas that indicates the rules of conversion of the plain text into cipher text and vice versa, combined with the secured key. However, algorithmic procedure for cryptography uses the same key or different keys. The major issue in designing an algorithmic procedure for encryption and decryption is to improve the secure level. Consequently, this paper aims to propose a new model for securing information using RNS Algorithm, CRT Algorithm and RNA Sequence. The cryptography scheme is designed by using the technologies of RNA synthesis, RNA digital coding and the theory of traditional cryptography. The scheme proposed in this paper has high confidential strength.

The rest of the paper is arranged as follows: section II provides a background of the existing literature and some related works were presented. Section III focuses on the methodology by presenting the algorithms. Section IV demonstrates the computation, analysis of the various experiments and the result of the study. Section V is conclusion, contribution to knowledge and future work.

2. LITERATURE REVIEW
Logunleko, et. al. (2020) [4] proposed a technical technique of the differential computation of the encryption algorithms. The research therefore fills the gap of security threat in EB64 pseudo code as compared with the newly proposed EHB64 pseudo code. In addition, this newly concept introduced generates a symmetric key by shuffling the original key with the textual data, thus making the transformation of each character of the data better each time it is shuffled. Thus the final output of the key-based pseudo code will be stronger than the pseudo code of EB64.

Kalsi et al. (2018) [8] discussed the concept of DNA deep learning cryptography to hide the ciphertext using deep learning and DNA cryptography techniques. They proposed method to generate keys using natural selection.

Aparna et al. (2017) [9] proposed an audio steganography method which is encrypted using a combination of DNA cryptography and AES encryption schemes. Piracy detection of movie files is one of the applications for which their work can be used.

Karimi and Haider (2017) [16] designed an encryption and decryption algorithm based upon biological operations which take place in DNA molecule. The DNA operations such as transcription, replication, annealing, marking and mutation are used. The algorithm generates a set of keys using the user's password as an input. The user generated password ensures random key generation. First the password is converted into binary, and then the bits taken pairwise are encoded to nucleotides as follows 00-Adenine, 01-Guanine, 11-Cytosine and 10-Thymine. If the length of the data is not divisible by 3 (codon length) or if length of data is less than 60, the data is extended by DNA replication. Next DNA annealing is done to get double stranded DNA. Next the DNA is converted to mRNA by replacing Thymine (T) with Uracil (U). Next mutation of mRNA is done. Both nonsense and missense mutation is performed on the DNA strand. Next the mRNA is split into subparts depending on occurrence of the stop codons UAG, UAA and UGA. This results in generation of subkeys. The number of subkeys generated is random as it depends on the number of stop codons in the mRNA. The subkeys are

converted into binary notation. Each subkey is grouped into 8-bit blocks. The 1st 8-bit block of input data is left shift 1 time and subkey1 is XOR with it. 2nd 8-bit block of input data is left shift 2 times and subkey2 is XOR with it. This is repeated for all the 8- bit blocks of input data to get final result. The encryption process is applied in reverse order to decrypt the message as it is a symmetric algorithm.

Saha and Haque (2017) [1] revealed an encryption algorithm based on DNA cryptography. They used a dynamic mapping for encoding to DNA bases. They also used operations such as Roll in encoding and data and key arrangement to improve its security.

Zhang (2017) [3] revealed a solution to the generation of random keys required by one time pad encryption scheme and secure transmission. They proposed the use of DNA molecule for generation and storage of the keys. They generated the keys from the DNA of the organism. This ensured its randomness. The secret key was then securely transported through a bacteria using recombinant DNA technology. The algorithm can be implemented in the biological DNA and bacteria with the current improvements in technology.

Karandeep (2016) [2] developed a layered algorithm combining DNA and RSA cryptographic techniques. The DNA encryption was done with respect to a reference DNA strand from a genetic database which acts as a secret key. The DNA strand was converted to decimal values based on the sequencing of reference strand. The scheme was developed for providing security in cloud infrastructure.

3. METHODLOGY

This study describes a cryptography modelling which is designed by using the technologies of DNA synthesis, DNA Binary Coded Scheme, and the theory of traditional cryptography as well combination of various efficient techniques such as RNS algorithm and CRT algorithm which formed a high level confidential strength model for cryptography.

3.1 Residue Number System

A Residue Number System is characterized by a moduli set$\{m_1\, m_2\, m_3\, \ldots\ldots\ldots m_l\}$, where the modulo, m_i,(i = 1, 2, …L), are pair wise relatively prime [15] [11][10]. Any integer X in the dynamic range,

$M = m_1\, m_2\, m_3\, \ldots\ldots\ldots m_l$ is represented by an L-tuple $(x_1\, x_2\, x_3\, \ldots\ldots\ldots x_{x-1} x_1)$ where, x_i is the residue of X in modulo m_i for i = 1, 2, ., L.

An integer X is represented by an L-tuple where, x_i is a nonnegative integer satisfying. Thus,

$X = m_i q_i + x_i$ and $0 \leq x_i < m_i$.

The residues can be represented as:

$$x = |X|_m \qquad (1.1)$$

3.2 Chinese Remainder Theorem

The statement of the Chinese Remainder Theorem (CRT) is as follows [10][11][13]:

Given a set of pair-wise relatively prime moduli $\{m_1, m_2, m_3, \ldots\ldots m_n\}$ and a residue representation $\{r_1, r_2, r_3, \ldots\ldots r_n\}$ in that system of some number X, i.e. $r_i = |X|_{m_i}$, that number and its residues are related by the equation:

$$|X|_M = \left|\sum_{i=1}^{n} r_i |M^{-1}{}_i|_{m_i} M_i\right|_M \qquad (1.2)$$

Where is the product of the m_i's, and $M_i = M/m_i$.

3.3 RNA Binary Coded Scheme

As shown in table 1, Binary Coded Scheme transforms alphabets A, C, G and U of RNA Sequence into binary codes and vice versa

3.4 The Proposed Model

Encryption Algorithm for the Proposed Model

In symmetric cryptography, an encryption algorithm, or cipher, is a means of transforming plaintext into ciphertext under the control of a secret key. This process is called encryption or encipherment[12][14]. The proposed model used the concept of symmetric cryptography and thus, this is represented as:

$$c_i = rns(m_i) \oplus rns(k_i) \qquad (1.3)$$

where:

- m_0, m_1 ... are the plaintext bits,
- k_0, k_1 ... are the key bits,
- c_0, c_1 ... are the ciphertext bits.
- rns are the Residue Number Systems

Decryption Algorithm for the Proposed Model

Decryption is the same operation as encryption. This means

$$m_i = crt(c_i \oplus rns(k_i)) \qquad (1.4)$$

where:

- crt are the Chinese Reminders Theorem

3.5 Flow chart for the Proposed Model

The figure1 and figure2 represent the encryption and decryption flow chart for the proposed model respectively.

4. EVALUATIONS AND DISCUSSIONS

This section analysed the proposed model. The plaintext was encoded into ciphertext and then decoded into plaintext back.

The calculations:

Encryption Scheme Begins

Segment 1
Key:
Presume the key is "Abo". It has three characters. It follows in Table 2 the steps used to calculate the key generation.

Segment 2
Plaintext:
Presume the plaintext is "Space". It has five characters.
Index 1: S
ASCII: 83
Secret RNS = {34, 40, 9}
Binary: 00100010 00101000 00001001

Index 2: p
ASCII: 112
Secret RNS = {14, 26, 1}
Binary: 00001110 00011010 00000001

Index 3: a
ASCII: 97
Secret RNS = {48, 11, 23}
Binary: 00110000 00001011 00010111

Index 4: c
ASCII: 99
Secret RNS $= \{1, 13, 25\}$
Binary: 00000001 00001101 00011001

Index 5: e
ASCII: 101
Secret RNS $= \{3, 15, 27\}$
Binary: 0000011 00001111 00011011

Segment 3
Merging the plaintext binary and the key binary:

Binary:
$00100010 \oplus 00101001 = 00001011$
$00101000 \oplus 00101001 = 00000001$
$00001001 \oplus 00101001 = 00100000$
Binary:
$00001110 \oplus 00101001 = 00100111$
$00011010 \oplus 00101001 = 00110011$
$00000001 \oplus 00101001 = 00101000$
Binary:
$00110000 \oplus 00101001 = 00011001$
$00001011 \oplus 00101001 = 00100010$
$00010111 \oplus 00101001 = 00111110$
Binary:
$00000001 \oplus 00101001 = 00101000$
$00001101 \oplus 00101001 = 00100100$
$00011001 \oplus 00101001 = 00110000$
Binary:
$00000011 \oplus 00101001 = 00101010$
$00001111 \oplus 00101001 = 00100110$
$00011011 \oplus 00101001 = 00110010$

Segment 4
Concatenating the result binaries in segment 3, we have the following binary sequence:
000010110000000010010000000100111001100110010100000011001001000100011111100010100000100100001100000010101000100110011000110010

Segment 5
Splitting Segment 4 into two-bits binary. Thus, we have the following binary sequence, 00 00 10 11 00 00 00 01 00 10 00 00 00 10 01 11 00 11 00 11 00 10 10 00 00 01 10 01 00 10 00 10 00 11 11 10 00 10 10 00 00 10 01 00 00 11 00 00 00 10 10 10 00 10 01 10 00 11 00 10

Segment 6
Applying the Binary Coded Scheme, the following RNA sequences were obtained:
AAGUAAACAGAAAGCAAUAUAGGAACGCAGAGAUUGAGGAAGCAAUAA AGGGAGCGAUAG

Decryption Scheme Begins

Segment 1
Repeat the key generating process in encryption process above

Segment 2
Replacing
"AAGUAAACAGAAAGCAAUAUAGGAACGCAGAGAUUGAGGAAGCAAUAA AGGGAGCGAUAG" by corresponding Binary Coded Scheme, we have the following binary sequence, 00 00 10 11 00 00 00 01 00 10 00 00 00 10 01 11 00 11 00 11 00 10 10 00 00 01 10 01 00 10 00 10 00 11 11 10 00 10 10 00 00 10 01 00 00 11 00 00 00 10 10 10 00 10 01 10 00 11 00 10

Segment 3
Concatenating the result binaries in segment 2, we have the following binary sequence:
000010110000000010010000000100111001100110010100000011001001000100011111100010100000100100001100000010101000100110011000110010

Segment 4
Splitting the binary in segment 3 into eight-bit, we have the following binary sequence:
00001011 00000001 00100000 00100111 00110011
00101000 00011001 00100010 00111110 00101000
00100100 00110000 00101010 00100110 00110010

Segment 5
Merging the ciphertext binary and the key binary:

Binary:
$00001011 \oplus 00101001 = 00100010$
$00000001 \oplus 00101001 = 00101000$
$00100000 \oplus 00101001 = 00001001$

Binary:
$00100111 \oplus 00101001 = 00001110$
$00110011 \oplus 00101001 = 00011010$
$00101000 \oplus 00101001 = 00000001$

Binary:
$00011001 \oplus 00101001 = 00110000$
$00100010 \oplus 00101001 = 00001011$
$00111110 \oplus 00101001 = 00010111$
Binary:
$00101000 \oplus 00101001 = 00000001$
$00100100 \oplus 00101001 = 00001101$
$00110000 \oplus 00101001 = 00011001$
Binary:
$00101010 \oplus 00101001 = 00000011$
$00100110 \oplus 00101001 = 00001111$
$00110010 \oplus 00101001 = 00011011$

Segment 6
Binary: 00100010 00101000 00001001
CRT(Secret RNS) $= \{34, 40, 9\}$
ASCII: 83
Index 1: S

Binary: 00001110 00011010 00000001
CRT(Secret RNS) $= \{14, 26, 1\}$
ASCII: 112
Index 2: p

Binary: 00110000 00001011 00010111
CRT(Secret RNS) $= \{48, 11, 23\}$
ASCII: 97
Index 3: a

Binary: 00000001 00001101 00011001
CRT(Secret RNS) $= \{1,13, 25\}$
ASCII: 99
Index 4: c

Binary: 0000011 00001111 00011011

$\text{CRT}(\text{Secret RNS}) = \{3, 15, 27\}$

ASCII: 101

Index 5: e

Finally, the plaintext 'Space' is formed.

The amount of the plaintext is five characters. The total bit is 8 x 15 bits = 120 bits. The 120-bits are divided into 15 parts of 8-bits characters. The 120-bits are divided into 2-bits characters to form the cipher text of sixty characters.

5. FIGURES/CAPTIONS

Table1: Binary Coded Scheme

Alphabet	Binary Representation
A	**00**
C	**01**
G	**10**
U	**11**

Table2: Analysis of the Key Calculation

Index	**1**	**2**	**3**
Char	**A**	**b**	**o**
Decimal	**65**	**98**	**111**
Weight	**1**	**1**	**1**
Key Function	**195**	**294**	**666**
xor	**895**		
Secret RNS	**{13, 35, 7}**		
xor	**13 ⊕ 35 ⊕ 7 = 41**		
Binary	**00101001**		

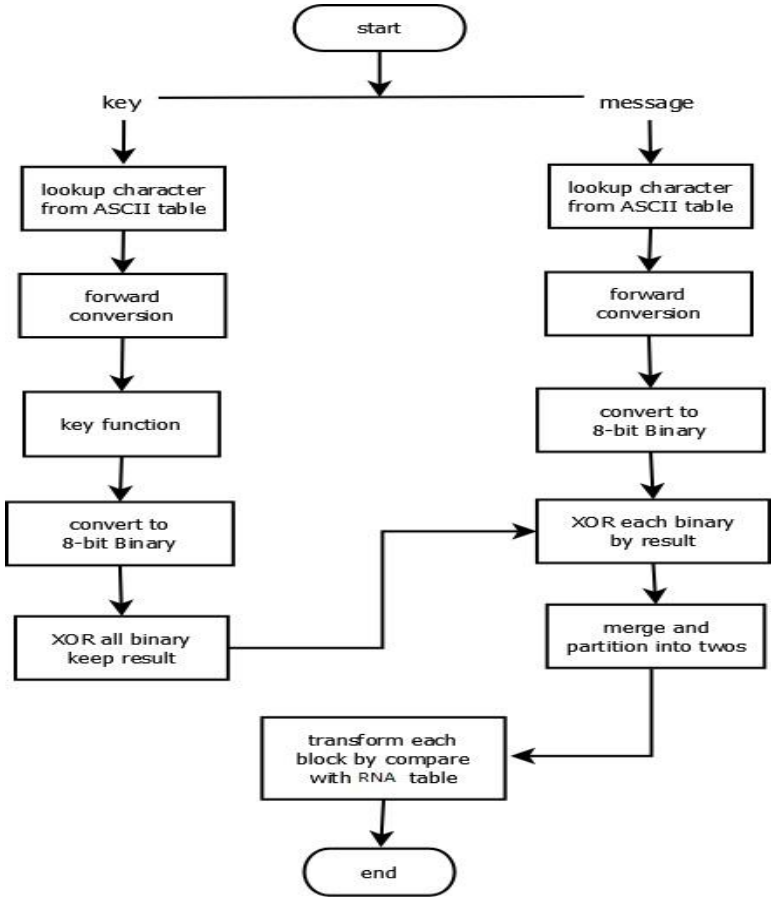

Figure 1: Encoding Flowchart

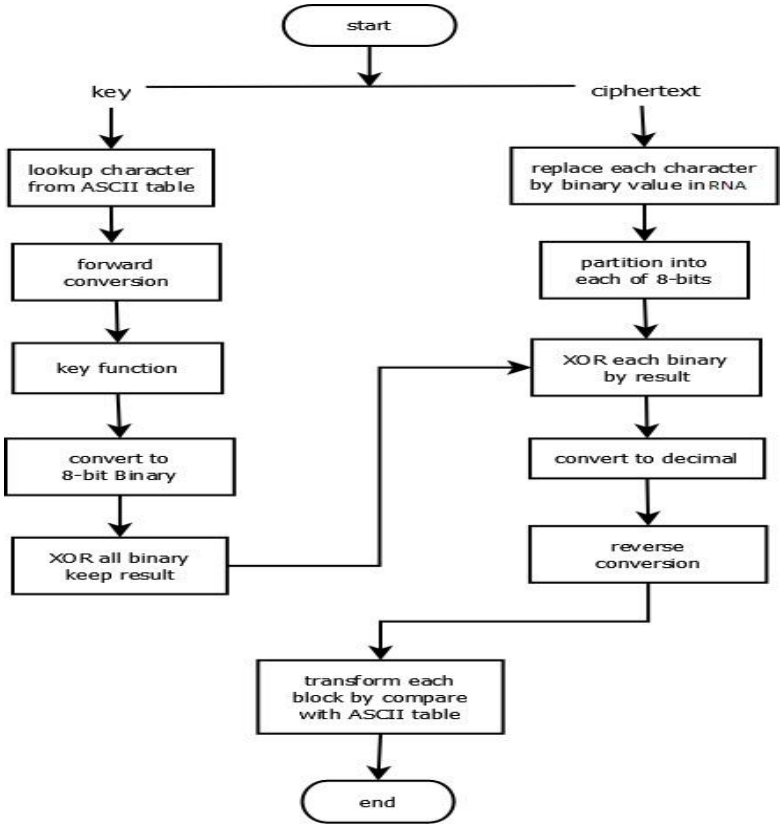

Figure 2: Decoding Flowchart

6. CONCLUSION

The research was successfully performed. The calculation above concludes that RNS-RNA Based Algorithm is good at information security system for encryption and decryption. Residue Number System is merged with the RNA sequence, which added more permutations and combinations that provides more security, flexibility with less complexity. RNS have special properties which can be utilized for encryption and decryption purposes by applying forward conversion and backward conversion techniques.

For further research, we shall investigate some mathematical properties of our approach, and also, try to insert an image as a secret data to be hidden inside the RNA sequence and see the effect on the security aspects.

6. REFERENCES

[1] Saha, R. and Haque, R. (2017). A novel Rolling based DNA Cryptography. *Journal of Bioinformatics and Genomics*, Vol.1,No.3, pp.1-6.

[2] Karandeep, K. (2016). A Double Layer Encryption Algorithm based on DNA and RSA for Security on Cloud. *International Research Journal of Engineering and Technology*, Vol.03, No.03, pp.1742-1745.

[3] Zhang, Y. (2017). DNA based random key generation and management for OTP encryption. *BioSystems*, Vol.159, pp.51– 63.

[4] Logunleko, A.M. and Gbolagade, K.A. (2020). A Differential Computational Encryption Modeling Technique on Textual Data. International Journal of Scientific Research in Computer Science and Engineering. Vol.8, Issue.1, pp.81-86, E-ISSN: 2320-7639.

[5] Isnar, S., and Andysah, P.U.S. (2016). Base64 Character Encoding and Decoding Modeling. *International Journal of Recent Trends in Engineering & Research (IJRTER)*, Volume 02, Issue 12, ISSN: 2455-1457.

[6] Poonkuzhali dan, S.M., and Therasa, M. (2015). Data Hiding Using Visual Cryptography for Secure Transmission. *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 4, no. 4, pp. 440-441.

[7] Siahaan, A.P.U. (2016). A Three-Layer Visual Hash Function Using Adler-32. *International Journal of Computer Science and Software Engineering*, vol. 5, no. 7, pp. 142-147.

[8] Kalsi, S., Harleen, K. and Victor, C. (2018). DNA Cryptography and Deep Learning using Genetic Algorithm with New algorithm for Key Generation. *Journal of medical systems*, Vol. 42, No.1, pp.17.

[9] Aparna, A., Akshay, C.B. Juvin, V, and Kodakara, S. C. E. T. (2017). Video Piracy Detection Based on Audio Steganography, AES and DNA Cryptography. *International Journal of Engineering Science*, Vol. 7, No.3, pp. 5487-5489.

[10] Aremu, I.A., Gbolagade, K.A., (2017). An overview of Residue Number System. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)* Volume 6, Issue 10, ISSN: 2278 – 1323 1618.

[11] Sharoun, A.O, (2013). Residue Number System (RNS). *Poznan University of Technology Academic Journals, Zawia University, Libya.* pp 265-270.

[12] Solanki, V. Vankani, P. Pukle dan S. Iyer, (2016). Multimedia Encryption Using Visual Cryptography. *International Journal of Recent Trends in Engineering & Research*, vol. 2, no. 9, pp. 261-264.

[13] Anton, H and Rorres, C. (2011). Elementary Linear Algebra, John Wiley & Sons.

[14] Bhanot, R and Hans, R (2015). A Review and Comparative Analysis of Various Encryption Algorithms. *International Journal of Security and Its Applications*, vol. 9, no. 4, pp. 289-306.

[15] Youssef, M.I, Emam, A.E and Abd Elghany, M, (2012). Multi-Layer Data Encryption using Residue Number System in DNA Sequence, *International Journal of Computer Applications* (0975 – 8887) Volume 45– No.10.

[16] Karimi, M and Haider, W. (2017).Cryptography using DNA Nucleotides. *International Journal of Computer Applications*, vol. 168, no.7.