TWMS J. App. and Eng. Math. V.15, N.1, 2025, pp. 242-255

AN INNOVATIVE RNA CRYPTOSYSTEM USING MOORE MACHINE

A. YASMIN[1], R. VENKATESAN[1*], §

Abstract. RNA Cryptography plays an exciting role in research, that has capability to provide a novel approach for the secure communication in the internet from terrible assailant. This paper presents the novel technique of RNA cryptosystem based on moore machine. The sender generates 512-bit secret key using the receiver credentials and used for encrypt the data. The randomly constructed moore machine provides the substitute RNA component during the data encryption. In this model, the RNA codons used for carrying the secure information and at the end, we discussed complexity, frequency and some of security attacks to prove that this novel scheme is efficient and secure cryptosystem.

Keywords: RNA Cryptography, RNA moore machine, Key generation, Encryption and Decryption.

AMS Subject Classification: 68Q45, 94A60

1. Introduction

Now-a-days communication is essential to run a human life. Currently most of the communications depend upon internet facilities than direct conversation. Therefore, it should be more secure to avoid the threats and attacks. Although internet has many cons, there are adverse effects in it. One of the techniques used to secure sensitive information on internet is performed by cryptography. The aim of cryptography is to transfer the secure data between legitimate persons without tampering and that cannot be access by illegal persons. In cryptography, CIA triad and its additional elements acts as a crucial role and it can be classified into two types symmetric (Private key cryptography) where the sender and receiver use same key for encryption and decryption process and asymmetric (Public key cryptography), where the sender and the receiver uses different key to generate the cipher text and plaintext. Recently, attack on traditional cryptographic technique is also possible by illegitimate persons. The new idea to protect the information using genetics of RNA/DNA called DNA/RNA Computing. The DNA computing was created by Leonard-Max Adleman in 1994 [1].

[1] Department of Mathematics, College of Engineering and Technology, SRM Institute of Science and Technology, Kattankulathur, Tamil Nadu - 603203, INDIA.
e-mail: ya5805@srmist.edu.in; ORCID: https://orcid.org/0009-0007-7599-212X.
e-mail: venkater1@srmist.edu.in; ORCID:https://orcid.org/0000-0002-8242-1444.
∗Corresponding author.

§ Manuscript received: April 28, 2022; accepted: April 26, 2023.
TWMS Journal of Applied and Engineering Mathematics, Vol.15, No.1;

In the field of research, Genetic (DNA/RNA) computing uses the molecules of DNA / RNA to perform the computational operations and the researchers are striving to build the new methods for managing and manipulating the molecules to generate the computational results.
Many of the researchers have done the genetic computing to achieve the efficient, unique, secure cryptographic algorithms and they concerned about the complexities, performance etc.[7, 8, 12, 13, 14, 16, 17, 18, 19]
Some of the literature articles are reviewed below.
Sally Safaa Nafea et.al [10] proposed a cipher algorithm using arithmetic operations and biological process by DNA-OTP sequence. They generated private key using biological process and used arithmetic for encryption process. The key size depends on user's input and translation processed to create the protein key that made cryptoanalysis more difficult. Jeevitha et.al [3] analysed the DNA based cryptography for transmitting the data then discussed DNA technology that contains biological process of electrophoresis and polymerase chain reaction. Rama et.al [4] conducted a study of DES (Data Encryption Standard) algorithm with cellular automata. DES has a standard encryption technique since 1976. The proposed scheme has random keys which are produced while the data admittance. However, the key length in DES is only 48 bits. Ayush et.al [11] established an data encryption technique involving Moore machine and the Fourier transform. In this model fourier transform is implemented in moore machine for encryption and inverse fourier transform used for decryption. Sony et.al [5] suggested the DNA cryptography on three stages of encryption using Moore machine. The three stages in this method includes secret key usage then self-generated moore machine and finally password. This method operates quite slowly. Pramod Pavithran et.al [15] proposed a novel cryptosystem based on DNA cryptography and finite automata. Initially, sender generates 256-bit key then encryption processed using randomized mealy machine generated by DNA codons. Herewith the DNA cryptosystem resists the security attacks. In [20] Pramod et.al generated the novel cryptosystem using finite state machine. This model tested the randomness of ciphertext and uses both mealy and moore machine
In this article, we utilize the RNA molecules to perform the novel cryptographic computing instead of DNA. As RNA has more stability, more efficient energy and easy to manipulate than DNA. Some of the potential drawbacks of the DNA molecules in cryptography includes limited encoding capacity due to its base pair limitations and double stranded nature, then the complex structure of DNA molecules makes difficulty in the cryptographic protocols and produces vulnerabilities, DNA has less computational efficiency in encoding and decoding complexity and also in analysis, manipulation complexity following that DNA nucleotides exhibits less dynamic behaviour and does not have wider functional capabilities in cellular automata cryptosystem. In the field of Cryptography, RNA computing is in the beginning stage and much more study and research is required to understand its multiple benefits like especially small size, high computational power, less energy consumption, resistance to changing landscape, high parallelism, bio-computability etc.,
The motive of our proposed model is to provide a high-level security to the confidential data as well as examining the complexities, security attacks, avalanche and frequency analysis.

The main benefits of this article are given below

(1) Proposed a key of size 512-bit for extreme security.
(2) Novel method is introduced for encrypting and decrypting by RNA computing.
(3) Carried out an analysis for proving that this cryptosystem is efficient.

2. BACKGROUND WORK OF PROPOSED MODEL

2.1. **RNA Cryptography.** Ribonucleic Acid (RNA) is the composition of nucleotides and meant for balancing genomic material. The four nucleotides of RNA namely Adenine(A), Guanine(G), Cytosine(C) and Uracil(U). When using the RNA based cryptography, usually the encrypted text is in the form of RNA codons called RNA sequence otherwise the RNA codons converted into binary bit or specific code book, that is used in the process of encrypting the original text for enhancing data security. For example, to encrypt the plain text HI using RNA computing, we randomly convert the RNA codons into 2-bit binary values i.e., A=11, G=10, C=01 and U=00. The equivalent binary value of HI is 0100100001001001. Now, we transformed the binary value into RNA sequence CUGUCUGC using 2-bit binary values of RNA nucleotides.

2.2. **Moore Machine.** Finite Automata (FA) is divided into two types. FA with output and FA without output. The Moore machine is subject to FA with output and its output depends on states. The Moore machine "M" defined by using six tuples $M = (Q, \sum, \Delta, \delta, \lambda, I)$ where Q and $\sum$ are non-empty set of states and set of input characters respectively, $\delta : Q \times \sum \rightarrow Q$ is the transition function, Δ - set of output characters, $\lambda : Q \rightarrow \Delta$ is the output function and I be the initial state.

2.3. **The random dynamic RNA Moore machine.** The RNAMM (RNA moore machine) is build using 4 states, inputs and outputs. The RNAMM is defined by $M_R = (Q, \sum, \Delta, \delta, \lambda, I)$ where,
$Q = \{0, 1, 2, 3\}$
$\sum = \{A, C, G, U\}$
$\Delta = \{00, 01, 10, 11\}$
$I = 0$
$\delta, \lambda =$ ramdomly created.
In cryptography, Moore machine is used to swap the input characters by its output characters. In the existing cryptographic algorithms, the moore machine used to convert each input character by single output character. But in the proposed model, the new ideology is implemented while generating the moore machine, since we considered input be set of RNA nucleotides and ouput be set consisting of string of binary values. The proposed model converts each input (RNA base) into string of binary values in encryption process and in decryption, the conversion of binary string into RNA base by reverse process of moore machine is much complicated which is explained in Section 4.2 and this reverse process cannot be easily manipulated by attacker. The proposed RNAMM has ability to transform large RNA sequence into binary string with finite number of states, inputs and outputs. The randomly generated RNAMM has deterministic behaviour that ensures the reliability, integrity, security, compatibility in proposed model and assures the randomness in decrypted data. Therefore, this RNAMM plays a major role in proposed cryptosystem.

2.4. **Transition table and transition diagram.** The transition table is essentially a transition function which has two arguments (state character) and the return value (next state) in tabular format. In general, transition diagram is a digraph associated with graph vertices that corresponds to states of FA. Create the RNAMM diagram based on the randomly generated transition table (Table 1) and the output table (Table 2). The state values are $\{0, 1, 2, 3\}$ then the output values are $\{00, 10, 01, 11\}$ and the inputs are $\{A, G, U, C\}$.

TABLE 1. **Input to Next state**

STATE	**Input "A" Next State**	**Input "C" Next State**	**Input "G" Next State**	**Input "U" Next State**
→0	2	1	3	0
1	1	2	0	3
2	3	0	1	2
3	0	3	2	1

TABLE 2. **Input to Output**

STATE	**Input "A" Output**	**Input "C" Output**	**Input "G" Output**	**Input "U" Output**
→0	10	01	11	00
1	01	10	00	11
2	11	00	01	10
3	00	11	10	01

3. PROPOSED MODEL

The sender and receiver register their credentials in the server and requesting for key. The server individually sends the private and public keys to both persons. Then the receiver encrypts few of the attributes using the receiver private key and transmit to sender. Then sender decrypts the attributes using receiver public key and authenticate the receiver. The receiver requests the data and parameters. Subsequently the sender generates the 512-bit key and encrypts the secret data and with the required parameters and pass on to receiver.

The brief note of novel RNA computing is given below:

We begin with generation of RNA Moore machine, key generation then the data encryption and decryption has been done, following that the theoretical analysis of frequency, security and complexity has explained, finally we concluded the proposed model. The workflow of the proposed scheme is shown in Figure 2

3.1. **Generation of RNA moore machine.**

As already mentioned in (section 2.4), the sender generated random transition and output table for designing the RNAMM.

Step:1 List out the number of states, inputs and outputs by Table 1 and 2. i.e., 0,1,2,3, A, C, G, U and 00,10,11,01.

Step:2 Start to design the transition diagram by introducing 4 nodes called 4 states 0,1,2,3 and point out the initial state 0 by right-arrow.

Step:3 Draw the directed loops and directed edges connecting each state.

Step:4 Label the inputs on edges and outputs on states that occur between the states.

Step:5 Complete the RNAMM diagram using Table 1 and 2 by following above (Step 4) until the last input and output.

This RNAMM given in Figure 1 can be encrypted and send to receiver by sender private key and receiver public key.

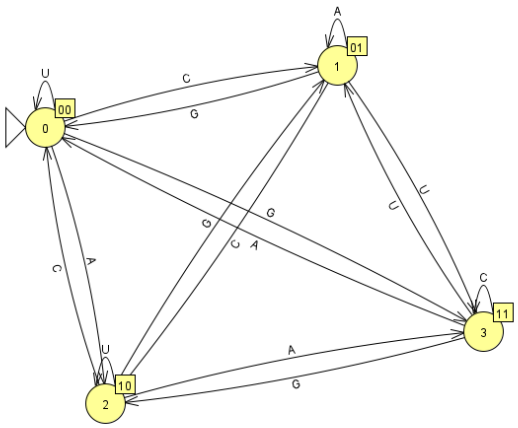

FIGURE 1. **RNA Moore Machine**

3.2. **Key generation.** The working procedure is as follows
Step:1 Initially the sender creates the string of minimum length 13 from the receiver's details i.e., Name, Phone number, email id, SSN, Passport id etc.,
Step:2 Convert the string into ASCII value
Step:3 Concatenate the ASCII value to get the new string
Step:4 Convert the new string into RNA sequence by using Code Book 1
Step:5 Transform the RNA sequence into its equivalent ASCII value
Step:6 Change the ASCII value to its binary value called binary string
Step:7 Consider the first 512-bit binary string by eliminating the extra terminal bits, which is the required 512-bit key

3.3. **Data encryption.** The sender considers the plaintext (PT) in capital letters. Then convert the plaintext into RNA sequence (i.e., RNA string R1) by replacing each character with its corresponding mapping of plaintext using randomly generated RNA Code Book 1 and 2. Pass the RNA string (R1) as input into the RNA Moore machine to get the output as new RNA string (R2). If R2 as n-bit then from the 512-bit key (K) take the first n-bit (K1). Perform the XOR operation between RNA string (R2) and the key(K1). If R2 is greater than 512-bit, then separate the R2 into blocks, perform the XOR and then concatenate it. Separate the entire string into 2-bits obtained from XOR operation. Now convert the each 2-bit into RNA Sequence (R3) by Code Book 3. R3 is the ciphertext. The sender transmits the ciphertext (R3) with all necessary parameters by encrypting receiver public key and then sender private key.

3.4. **Data decryption.** The receiver gets the encrypted data from sender and starts decrypting it. The receiver starts decrypting using sender public key then receiver private key so that the receiver retrieves the ciphertext and parameters. The receiver has to do the reverse process of encryption to get the plaintext. At the beginning, receiver has to degenerate the key by using his/her attributes as well as Moore machine by Table 1 and 2. Now the receiver converts the ciphertext(R3) into binary string by Code Book 3 following that the XOR operation is executed between the key(K1) and binary string to get the RNA string(R2). Execute the RNAMM transition function in reverse order to obtain R1 from R2. Eventually, receiver decrypted the plaintext, by taking corresponding character

of R1 from Code Book 1 and 2.

3.5. **Algorithm.** Encryption algorithm
Input: Plaintext(PT)
Output: Ciphertext(CT)

Step:1 Start
Step:2 Transform PT into RNA sequence (R1) by taking its corresponding characters
Step:3 Pass the R1 as input to RNAMM to get output as R2
Step:4 Perform the XOR between each R2 and key K1
Step:5 Convert the binary value into RNA string (R3) by Code Book 3
Step:6 End

3.6. **Algorithm.** Decryption algorithm
Input: Ciphertext(CT)
Output: Plaintext(PT)

Step:1 Start
Step:2 Decode RNAMM with parameters
Step:3 Convert R3 into binary value
Step:4 Execute XOR between binary string and key to get R2
Step:5 Apply Table 1 and 2 to find inputs(R1) of R2 where R2 is the output of R1
Step:6 Convert R1 into PT by Code Book 1 and 2
Step:7 End.

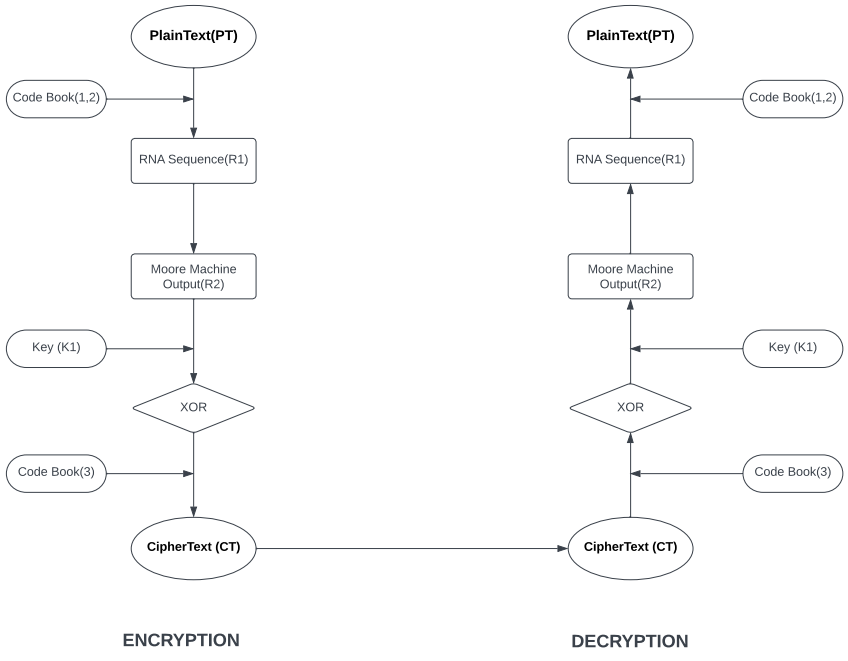

FIGURE 2. **Workflow of Proposed Scheme**

TABLE 3. **Random Conversion of RNA Codons into Alphabets.**

CODE BOOK 1

RNA CODONS	**ALPHABETS and NUMBERS**	**RNA CODONS**	**ALPHABETS and NUMBERS**
UUU	**A**	CUU	**N**
UCU	**B**	CCU	**O**
UAU	**C**	CAU	**P**
UGU	**D**	CUC	**Q**
UCC	**E**	CCA	**R**
UAC	**F**	CAC	**S**
UGC	**G**	CGC	**T**
UUA	**H**	CUA	**U**
UCA	**I**	AUG	**V**
UAA	**J**	CAA	**W**
UGA	**K**	CGA	**X**
UUG	**L**	ACU	**Y**
UGG	**M**	CAG	**Z**
CUG	**1**	GCG	**6**
AUC	**2**	UAG	**7**
GUG	**3**	CGU	**8**
CCG	**4**	GAU	**9**
UCG	**5**	UUC	**0**

TABLE 4. **Random Conversion of RNA Codons into Special Characters..**

CODE BOOK 2

RNA CODONS	**SPECIAL CHARACTERS**	**RNA CODONS**	**SPECIAL CHARACTERS**
CGG	**:**	AGG	**&**
AUU	**;**	GCC	**(**
AAU	**<**	GGU	**)**
AGU	**>**	GUU	**SPACE**
ACA	**=**	GUC	*****
AAC	**?**	GCA	**+**
AGC	**{**	GAC	**,**
AUA	**}**	GGC	**_**
ACG	**[**	GUA	**.**
ACC	**]**	GAA	**/**
AAA	**!**	GGA	**@**
AGA	**'**	GAG	**~**
CCC	**#**	GGG	**|**
GCU	**$**	AAG	**%**

Table 5. **Conversion of RNA Nucleotides from 2-bit binary value**

CODE BOOK 3

RNA NUCLEOTIDES	2-bit BINARY VALUE
A	11
C	10
G	01
U	00

4. ILLUSTRATION OF PROPOSED SCHEME

The Sample implementation of proposed scheme is described in this section.

4.1. **Key Generation.** The messenger/sender performs succeeding steps for key generation

a) The sender has the receiver's details i.e., name: abcdef, phone number:9871010101, email id:g@yahoo.com, SSN:456012123, passport id:BUZ73U90, from this details sender creates a string of length 13

abc987g@456BU

b) String converted into ASCII value

[97, 98, 99, 57, 56, 55, 103, 64, 52, 53, 54, 66, 85]

c) The new string is formed by concatenating b)

97989957565510364525354668 5

d) Pass c) into Code Book 1 to get RNA sequence

GAUUAGGAUCGUGAUGAUUCGUAGUCGGCGUCGUCGCUGUUCGU
GGCGCCGUCGAUCUCGGUGUCGCCGGCGGCGCGUUCG

e) Transform d) to its ASCII value

[71, 65, 85, 85, 65, 71, 71, 65, 85, 67, 71, 85, 71, 65, 85, 71, 65, 85, 85, 67, 71, 85, 65, 71, 85, 67, 71, 71, 67, 71, 85, 67, 71, 85, 67, 71, 67, 85, 71, 85, 85, 67, 71, 85, 71, 71, 67, 71, 67, 67, 71, 85, 67, 71, 65, 85, 67, 85, 67, 71, 71, 85, 71, 85, 67, 71, 67, 67, 71, 71, 67, 71, 71, 67, 71, 67, 71, 85, 85, 67, 71]

f) Convert e) to its binary value

1000111100000110101011010101100000110001111000111100000110101011000 0
1110001111010101100011110000011010101100011110000011010101101010 1100
0011100011110101011000001100011110101011000001110001111000111100 00111
0001111010101100001110001111010101100001110001111000011101010110 0011
1101010110101011000011100011110101011000111100011110000111000111 1000
0111000011100011110101011000011100011110000011010101100001110101 0110
0001110001111000111101010110001111010101100001110001111000011100 0011
1000111100011110000111000111100011110000111000111100001110001111 0101
0110101011000011100 0111

The string length of f) has 567-bit

h) Take the first 512-bit by eliminating remaining terminal values

1000111100000110101011010101100000110001111000111100000110101011000 0
1110001111010101100011110000011010101100011110000011010101101010 1100
0011100011110101011000001100011110101011000001110001111000111100 00111
0001111010101100001110001111010101100001110001111000011101010110 0011
1101010110101011000011100011110101011000111100011110000111000111 1000

01110000111000111101010110000111000111100000110101011000011101010110000111000111100011110101011000011110101011000011100011110000111000011100001111000111000011110001111
the above 512- bit binary is the required 512-bit key for encryption and decryption of this proposed algorithm

4.2. **Data Encryption.** The sender encrypts the confidential data in this process.
a) The sender has to encrypt the Plain Text (PT).
PT= "HI WORLD"
b) Pass a) to Code Book 1 and 2 to get corresponding mapping of RNA sequence R1.
R1= UUAUCAGUUCAACCUCCAUUGUGU
c) Convert R1 into binary string by using Moore machine, consider R1 as input to Moore machine whose output will be binary string called new RNA string (R2)
R2= 00000010100010011101101100011010000101110100001101
d) Separate K1 from K, where K1 be first n-bit from 512-bit key, where n is length of R2.
K1= 10001111000001101010110101011000001100011110001111
e) To obtain XOR value, XOR operation is performed between R2 and K1
XOR= 10001101100011110111011001000100010011010100000010
f) Each 2-bit of XOR is replaced by RNA codons(R3)
R3= CUAGCUAAGAGCGUUCUCGCCCUUC
Therefore, "R3" is the Ciphertext.

4.3. **Data Decryption.** The receiver has to perform reverse process of encryption to regenerate the plaintext
a) The sender has Ciphertext(CT)
CT=CUAGCUAAGAGCGUUCUCGCCCUUC=R3
b) By using the Binary value given in Code Book 3 of R3, receiver gets the XOR value
XOR= 10001101100011110111011001000100010011010100000010
c) Execution of XOR operation between Key K1 and b)
R2= 00000010100010011101101100011010000101110100001101
d) Now R2 is the input to Moore Machine to get new RNA Sequence R1. The receiver performs the invert process to execute the Moore Machine using Table 1 and 2. The sample idea of execution is given below
1. Each 2-bit of R2 is transformed into RNA sequence except initial 2-bit. Because in Moore Machine, the output string contains initial state output. Here the Moore machine start state is 0 and the output of state 0 is 00, to refer the initial state output first 2-bit presented in R2.
2. Consider the next two-bit i.e., 00. The start state is 0. In Table 2 for State 0, the output 00 is presented in input column U. So, "00" is replaced by "U". Therefore, the first character of R1=U.
3. To find the next state, use transition table Table 1. Here, for state 0 and input U the next state will be 0
4. The 3rd 2-bit value is 00. In output table Table 2 for state 0 and the value 00 is presented in column, and its input is "U". Again "00" is replaced by "U" $\rightarrow$ R1= UU.
5. In state table Table 1 for state 0 and input U the next state is again 0. The following 2-bit in R2 is "10". In Output table Table 2 for state 0, 10 is presented in column input as "A". Now "10" is replaced by "A" $\rightarrow$R1= UUA.
6. In transition table Table 1 for state 0 and the input A, the state 0 changes to state 2. Process the above process till the last bit of the RNA String R2.
i.e., **R1= UUAUCAGUUCAACCUCCAUUGUGU**

e) Eventually, PT is decrypted from R1 using Code Book 1 and 2
PT= "HI WORLD"
The output of the illustration of proposed algorithms implemented in Python is shown in Figure 3

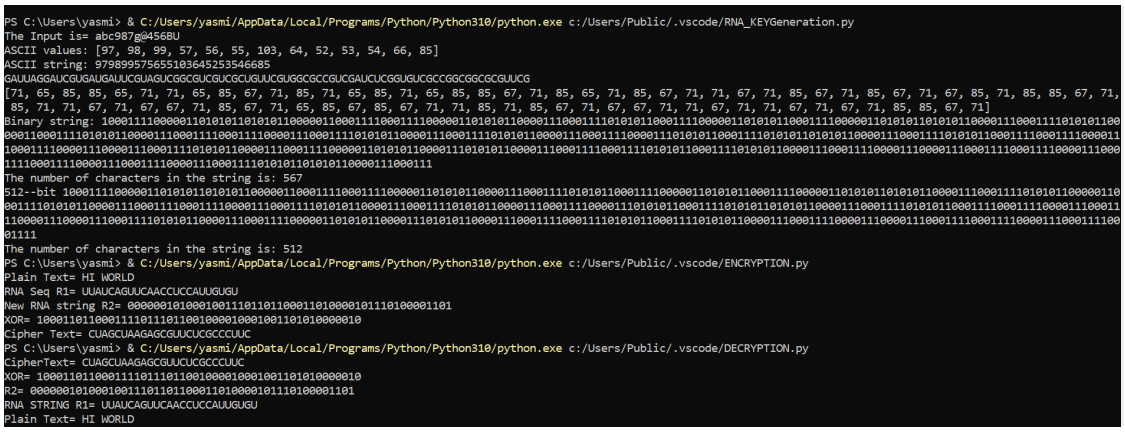

FIGURE 3. **Output of Proposed Scheme Illustration in Python.**

5. COMPLEXITY ANALYSIS

The Complexity analysis usually determines the run time and space requirements of an algorithm. It also provides a way to compare and evaluate different algorithms that helps to predict the most suitable algorithm by depending upon relationship between execution time and input size. Here, we are analysing the time complexity of the proposed algorithms such as key generation, encryption and decryption with few of the existing algorithms given in Table 6. The overall time complexity of the proposed model is $O(n)$, where $O(n)$ refers that the execution time of the algorithms increases linearly with an input size, whereas in the existing models the time complexity of some of the algorithms will be $O(n^2)$, it indicates that there is a quadratic relation between input size and execution time in existing models. Therefore, the time complexity of the proposed model is comparatively minimized than prior models.

TABLE 6. **Comparitive analysis of time complexity of Proposed method**

ALGORITHM	**Pramanik**[2]	**Kaundal, Paul**[9, 6]	**Proposed Model**
Key Generation	$O(n)$	$O(n^2)$	$O(n)$
Encryption	$O(n^2)$	$O(n)$	$O(n)$
Decryption	$O(n^2)$	$O(n)$	$O(n)$

6. FREQUENCY ANALYSIS

In this part, we stated the frequency analysis of the proposed scheme. The frequency analysis is a most important part of Cryptoanalysis. Here the attacker determines the frequency of each character given in the ciphertext and then compare this frequency distribution with expected frequency distribution for the language of the PT.
The analysis of proposed model frequency is executed using 4 set of data (PT) and the results are taken according to number of occurrences of RNA codons (A, C, G, U) in CT.

The 4 set of datas (PT) are 50 A's, 50 C's, 50 G's AND 50 U's. The frequency analysis is given in the Table 7 and the frequency distribution is given in Figure 4. The Figure 4 indicates that the CT significantly contains all the four RNA codons for each set of data but each data (PT) be the 50 times of single character. Therefore, this proposed model withstands this frequency analysis

TABLE 7. **Result of Frequency Analysis** (in CT)

Data Set	Plaintext	A	C	G	U
1	**50 A's**	42	36	33	40
2	**50 C's**	45	31	36	39
3	**50 G's**	35	35	36	45
4	**50 U's**	39	31	40	41

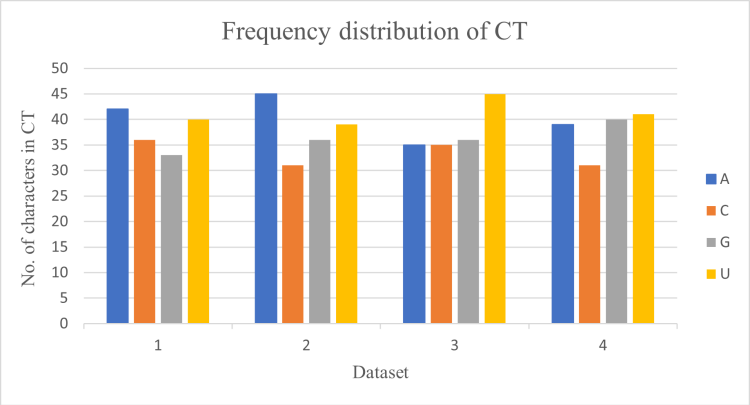

FIGURE 4. **Frequency Distribution chart of RNA codons in CT**

7. AVALANCHE EFFECT

The Avalanche Effect is an important property of cryptographic algorithm because it makes significantly difficult task for an attacker to decrypt the CT or to recover the key. A slight change in the input (PT) character or the single bit change in the secret key leads to significant change in output (CT).

The Avalanche Effect of the proposed model is analysed by changing single character in 4 set of data given in Section 6. Changes in RNA codons of the output (CT in %) for single character change in input (PT) is given in the Table 8. If initial character in the PT is changed then we get at most 99.9% change in CT and the minimal change is 75.8% when we randomly change the single character in PT. Table 8 proves that the proposed model thwarts the avalanche effect. The graphical representation of avalanche effect of our proposed model is given in Figure 5.

TABLE 8. **Results of Avalanche Effect**

Plaintext	Changes in CT(in %)
1 B + 49 A's	80.79%
1 D + 49 C's	83.2%
1 H + 49 G's	75.8%
1 V + 49 U's	99.9%

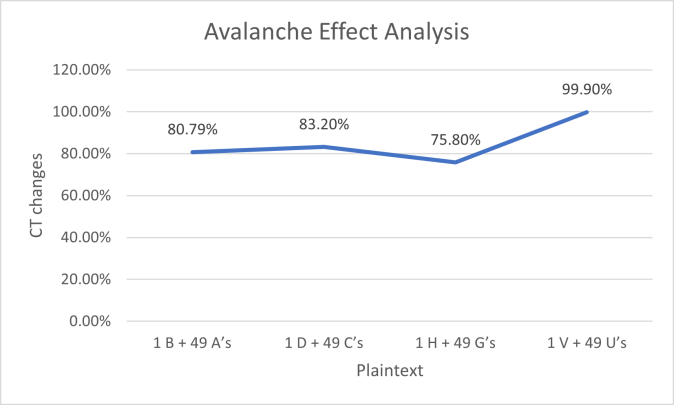

FIGURE 5. **Graphical representation of Avalanche Effect**

8. SECURITY ANALYSIS

In this section, some of the familiar attacks can be restricted by the proposed scheme

8.1. **Brute-Force Attack.** In this attack, the assailant tries to figure out all the possibilities of encryption secret key. But in this proposed model, the key size is 512-bit of binary string, which is much more challenging task. As the attacker has to try 2^{512} possibilities, it's not computationally possible. Therefore, our model is resistant to this attack.

8.2. **Ciphertext Only Attack.** In this Cryptographic attack, the assailant de-cipher the encrypted message but unaware of encryption method. The attacker may deduce the original PT by using the repeating sequences of CT. However, in proposed scheme the encrypted similar character CT make the distinct PT character. Thus, this scheme resilient to ciphertext only attack.

8.3. **Known Plaintext Attack.** In a Known Plaintext Attack, the assailant is able to deduce encryption key or encryption algorithm. The intruder has access to PT and associated CT. In our method, XOR operation is performed between RNA string and Key. RNA string is brought from randomly generated Moore Machine. Besides the same character in the PT produces different CT characters. Hence, proposed scheme withstands to known plaintext attack.

8.4. **Phishing Attack.** The goal of this attack aims to trick the legitimate user into clicking the link or opening the attachment so that the malware installs to their device to create a fake login page, where the attacker asks the legitimate user to enter the personal details. This attack can be hard to detect and frequently succeeds. But in proposed model both sender and receiver exchange the required data in encrypted form by their private and public keys and the keys are generated by server. In addition, none of the personal details is directly requested from receiver. Receiver itself encrypt his/her information by using key and send to sender for authentication. This thwarts the phishing attack.

8.5. **Man-in-Middle Attack.** During this Attack, the attacker perform masquerade, replay, modify, denial-of-service. These are types of active attack. Here the attacker goal is to modify the data stream or creating false stream. In the proposed method, the receiver attributes are encrypted before transmitting to sender. The CT with parameters (Tables and Codebooks) are also encrypted using private and public keys. The private keys are

kept confidentially and not known to anyone excluding the deliberate person. If the assailant tries to interrupt too, she/he cannot retrieve anything. Thus, our model resistant this man-in-middle attack.

9. Conclusions

A novel RNA cryptosystem is presented in this paper for the secure exchange of data between sender and receiver. This novel cryptosystem is secured by different levels, initially 512-bit secret key generated for extreme protection, then randomly generated Moore machine and RNA Codebooks (1,2 and 3) for enhancing the model, following that the XOR operation and then encrypted message (CT) consists of combinations of RNA nucleotides. Hence, this RNA cryptosystem is secure and efficient. In the last sections we discussed the complexity analysis, security attacks, frequency and avalanche effect of this proposed model. In future, we wish to implement this proposed scheme mathematically and extending this for image encryption.

Acknowledgement. The authors would like to thank the anonymous referees for their valuable suggestions.

References

[1] Adleman, L. M., (1994), Molecular Computation of Solutions to Combinatorial problems, Science, 266(5187), pp. 1021-1024.
[2] Pramanik, S., and Setua, S. K., (2004), DNA Cryptography, 7^{th} IEEE International Conference on Electrical and Computer Engineering, pp. 551-554.
[3] Jeevidha, S., Basha, M. S., and Dhavachelvan, P., (2011), Analysis on DNA based Cryptography to Secure Data Transmission, International Journal of Computer Applications, 29(8), pp. 16-20.
[4] Rama, R., Suyambu, J. B., Andrew, A., and Shanmugam, S., (2012), A study of DES algorithm with the Cellular Automata, International Journal of Innovation Management, 3(1), pp. 10-16.
[5] Sony, R., Prajapati, G., Khan, A., and Kulhare, D., (2013), Triple stage DNA Cryptography using sequential machine, International Journal Of Advanced Research in Computer Science, 3(8).
[6] Kaundal, A. K., and Verma, A. K., (2015), Extending feistel structure to DNA cryptography, Journal of Discrete Mathematical Sciences and Cryptography, 18(4), pp. 349-362.
[7] Shanmugasundaram, G., Thiyagarajan, P., and Pavithra, S., (2015), A Novel DNA Encryption system Using Cellular Automata, International Journal of Security, Privacy and Trust Management, 4(3), pp. 39-49.
[8] Rahman, N. H., Balamurugan, C., and Mariappan, R., (2015), A Novel DNA Computing Based Encryption and Decryption Algorithm, International Conference on Information and Communication Technologies, 46, pp. 463-475.
[9] Paul, S., Anwar, T., and Kumar, A., (2016), An innovative DNA Cryptography technique for Secure Data Transmission, International Journal of Bioinformatics Research and Applications, 12(3), pp. 238-262.
[10] Nafea, S. S., and Ibrahem, M. K., (2018), Cryptographic Algorithm based on DNA and RNA Properties, International Journal of Advanced Research in Computer Engineering and Technology, 7(11), pp. 804-811.
[11] Mittal, A., and Gupta, R., (2019), An Encryption method involving Fourier transform and Moore machine, International journal of scientific and technology research, 8(11), pp. 3997-3998.
[12] Vikram, A., Kalaivani, S., and Gopinath, G., (2019), A Novel Encryption Algorithm based on DNA Cryptography, International Conference on Communication and Electronics Systems, pp. 1004-1009.
[13] Adithya, B., and Santhi, G., (2021), DNA Computing Using Cryptographic and Steganographic Strategies, Data Integrity and Quality, 6, pp. 1-19.
[14] Omar fitian, R., (2021), Text encryption Based on DNA Cryptography, RNA, and Amino Acid, MCAIT, pp. 167-173.
[15] Pavithran, P., Mathew, S., Namasudra, S., and Lorenz, P., (2021), A novel Cryptosystem based on DNA cryptography and randomly generated mealy machine, Computer and Security, 104, pp. 1-15.

[16] Kabra, A., Gangwal, K., Kinage, A., and Agarwal, K., (2022), A Review paper on Cryptography using Automata Theory.
[17] Pavithran, P., Mathew, S., Namasudra, S., and Srivastava, G., (2022), A novel cryptosystem based on DNA cryptography, hyperchaotic systems and randomly generated Moore machine for cyber physical systems, Computer communications, 188(3).
[18] Dubey, H., Barik, R., (2022), Emerging DNA Cryptography based Encryption Schemes, International Journal of Information and Computer Security, 1(1).
[19] Hassan, A., (2022), Proposed Approach for Key Generation Based on RNA, Journal of the College of Basic Education, 21(87), pp. 101-113.
[20] Pavithran, P., Mathew, S., Namasudra, S., and Ashish, S., (2023), Enhancing randomness of the ciphertext generated by DNA-based cryptosystem and finite state machine, Cluster computing, 26, pp. 1035-1051.

A. Yasmin graduated from the Department of Mathematics in 2019 and received master's degree in Mathematics from SRM Institute of Science and Technology in 2021. Currently she pursuring her Ph.D degree in the same institution. Her current area of research includes Automata theory and Cryptography.

R. Venkatesan working as an assistant professor in the Department of Mathematics, SRM Institute of Science and Technology, India. His current area of research includes Formal languages and Automata theory, Algebraic automata theory and Cryptography.