

A NOVEL DNA ENCRYPTION SYSTEM USING CELLULAR AUTOMATA

G.Shanmugasundaram¹, P.Thiyagarajan², S.Pavithra¹

¹Department of Information Technology, Sri Manakula Vinayagar Engineering College, Madagadipet, Puducherry.

²Department of Computer Science and Engineering, Mahindra Ecole Centrale, College of Engineering, Hyderabad - 43.

ABSTRACT

DNA Cryptography is a new born cryptographic field emerged with the research of DNA Computing in which DNA is used as an Information carrier. Cellular automata is dynamic in nature so it provide dynamic behavior in the system which may increase the security in the system. DNA cryptography is provide a secure way to encrypt the text and automata changes the state of the system based on the present state, it will occur in discrete time. These qualities are most impressive in these technology which help us to provide a highly secured security system for the users. Most of the encryption techniques based on the cellular automata have limitations. To overcome this lacuna, we propose a novel DNA cryptography algorithm with cellular automata to achieve randomness, parallelism, uniformity, reversibility and stable. An algorithm implemented and its results obtained are depicts here, and a result analysis is done with other algorithms.

KEYWORDS

Cellular automata, DNA, Thymine, Uracil.

1. INTRODUCTION

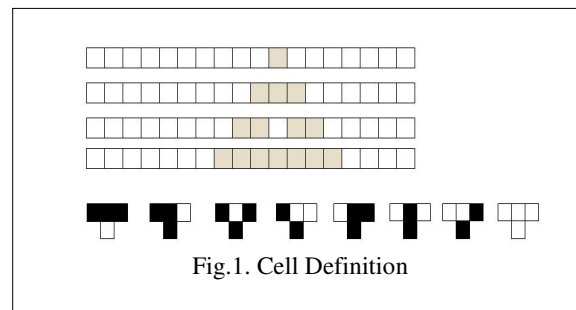
Nowadays, Internet has become parts and parts of human life and it has emerged closely with human such that it is elevated as one of the basic needs of human life. The facility of using the Internet in mobile phones has increased its use among common man. Many sectors of business such as bank, travel, shopping etc., make use of Internet to reach many people and flourish their business by introducing their application (apps). Though there are many advantages of Internet, it has adverse effect such as security. Sensitive information such as financial transactions, confidential government information, and medical records is transmitted through Internet. The protection of this sensitive information in the Internet is done by information security systems such as cryptography [1], steganography [2] [3] and combination of cryptography and steganography [4]. Security in Internet is provided by the information security systems. With the advancement in computational infrastructure and computer processing capacity, standard information security systems are no longer secure¹. As traditional cryptographic methods are based on mathematical and theoretical models, with the recent advancements in computational techniques, cryptographic methods are vulnerable to attacks. A novel technique for securing data was introduced using the biological structure of DNA called DNA Computing. It was invented by Leonard Max Adleman in the year 1994, for solving the complex problems such as directed Hamilton path problem, NP-complete problem and travelling salesman problem.

¹ <http://www.symantec.com/connect/blogs/2015-internet-security-threat-report-attackers-are-bigger-bolder-and-faster>

The DNA computing is also used in cryptography research. DNA is used in cryptography for storing and transmitting the information, as well as for computation. This paper, try to utilize the power of DNA to hide message [5]. The massive parallelism and extraordinary information density inherent in this molecule are exploited for cryptographic purposes. The current main difficulties of DNA cryptography are the absence of theoretical basis, the high tech lab requirements and computation limitations [6]. In this paper DNA cryptography is used along with cellular automata. A brief introduction of cellular automation is described in the below paragraph.

Cellular automation is a system made up of many discrete cells, each of which may be in one of a finite number of states [16]. A cell or automaton may change state only at fixed, regular intervals, and only in accordance with fixed rules [20] that depend on cells own values and the values of neighbors within certain proximity. The formal definition of Cellular Automation (CA) is one or two dimensional grid [10] of identical automata cells. Each cell processes information and proceeds in its action depending on its neighbors. Each cell (automaton) is defined by

- Set of States $S = \{S_1, S_2, S_3, S_4, \dots, S_N\}$
- Transition Rules T
- Therefore $A \sim (S, T, R)$ (R : neighboring automata)
- $T: (S_t, I_t) \rightarrow S_{t+1}$



The rest of the paper is organized as follows: Section 2 of this paper deals with related work in DNA cryptography. The proposed work and experiment methodology are discussed in section 3. Experiment results of the proposed work are presented in section 4. Section 5 concludes the paper.

2. LITERATURE SURVEY

This section describes some of the DNA computing and cellular automata methods reported in literature and it also describes the motivation to combine DNA computing and cellular automata.

According to Guangzhao Cui et al [8], DNA computing is a new computational paradigm by harnessing the potential massive parallelism, high density information of bio-molecules and low power consumption, which brings potential challenges and opportunities to traditional cryptography. Guangzhao Cui et al [8] in his paper discussed about DNA computing and its application in information security field and reviews the principle of DNA computing. It also elaborates about schemes with secret key searching and introduces the application of DNA computing in encryption, steganography and authentication [8].

S.Jeevidha et al [21] proposed an analysis on DNA based cryptography to transfer the data securely and also discusses DNA technology used in the cryptographic methods. DNA technology includes all biological process like polymerase chain reaction and electrophoresis.

H.Z.Hsu [7] in his method exploits the interesting properties of DNA sequence to encrypt data. The author presents three methods namely, the insertion method, the complementary pair method and the substitution method. In [8] the paper analyse some schemes with secret key searching and introduce the application of DNA computing in encryption, steganography and authentication. Anupriya et.al [9] in her paper proposed an algorithm which is based on reference sequence known only to sender and receiver. Since there are roughly 55 million publicly available DNA sequence it is virtually impossible to crack the sequence.

A Study of Data Encryption Standard (DES) Algorithm with Cellular Automata was proposed by Rama R et al [11]. DES algorithm was accepted as the standard encryption algorithm in 1976. Since then the development and usage of DES is widely recognized. The concept of Cellular Automata (CA) introduced by John von Neumann (1950s) is the first model which exhibited the capability of producing complex and random behavior.

Cellular Automata is a parallel processing machine and it involves context dependent behavior of all the value at time 't' [17]. The literature has witnessed the usage of Cellular Automata rules which are simple in nature for the operation of DES and Advanced Encryption Standard (AES) algorithms.

Cellular automata is applied in variety of fields such as smart devices to provide security [14], pattern classification [15], traffic modelling etc. Rama R et al [11] extend the usage of Cellular Automata (CA) for the key generation in DES. The proposed CA-based key generation methodology uses the elementary Cellular Automata rule 30 which possess more randomness. The initial seed involved is 15 bit multi-seed and presented the implemented DES with key generated using Cellular automata in Java. Due to cellular automata rule 30 randomness is highly provided in this method. The demerit of this method is the key size is minimal in this approach.

Pratibha Sharma et al [12] proposed Text Security Using 2D Cellular Automata Rules Encryption method which is the most common method for hiding text from unauthorized access. Encryption provides only one level of security during transmission over the channel. The main aim would be to provide 2 levels of security. First level comprises of hiding text to be sent behind some image using password and the second level comprises of encryption using 2D Cellular rules. If one level security is broken then the other level would provide security thereby ensuring more security to the transmitted message. Encryption would be done using 2 dimensional rules of Cellular Automata. Moore neighborhood model have been used as Cellular Automata model. In Moore neighborhood model 9 cells are considered at a time including the cell itself. The value of current cell (i.e. central cell) depends on its 8 neighbors. The merits of this method are: two level securities are provided in this method and the other is due to chip in automata machine which enhances the speed of encryption and decryption.

Triple Stage DNA Cryptography Using Sequential Machine was proposed by Rupali Soni et al [13], to secure data there are some traditional cryptographic techniques such as substitution, transposition, and various algorithms such as RSA, DES, AES, IDEA etc. and protocols like SSL are used. This work in [13] represents a new approach to secure the data which is based on DNA logic, cryptographic scheme and automata theory. DNA Cryptography technique was proposed by L. M. Adleman in 1994 for solving Hamiltonian path problem and automata theory was firstly initiated in 20th century. In the proposed work [13] these two techniques are combined for creating powerful security algorithm. This algorithm is more reliable and powerful because of the use of secret key, auto generated Moore machine and use of password [13]. The merits of the method are security is provided in triple stage in this method and it is resist to many known attacks.

2.1. Merging of DNA Cryptography and Cellular Automata

DNA cryptography and cellular automata used in the cryptography field, but both are not combined to provide security. As both domains are yielding better solutions to the security issues, if these fields are combined, security provided by them will be enhanced. The proposed work in this paper combines both fields in an efficient way for developing highly secured system. As cellular automata are dynamic in nature it contributes for dynamic behavior in the system which increases the overall security. DNA cryptography provides a secure way to encrypt the data. These qualities are most impressive which motivates to provide a highly secured security system for the users. The ultimate aim of this proposed work is to provide high level security which may make the hackers less possible to crack the system.

3. PROPOSED SYSTEM

The objective of the work is to develop a prominent secure system that satisfies the needs of the user. The DNA cryptography and cellular automata will lead to provide effective cryptographic algorithms. Each field has their own characteristics to establish if they are combined to form a cryptosystem it will lead to achieve properties of both fields. This algorithm comprises the technique of both DNA cryptography and cellular automata and it is named as “A hybrid advanced encryption algorithm using DNA substitution combined with Elementary Cellular automata rule (ECA-51)” [18] [19].

3.1. Working of proposed system

Initially the plain text is taken from the user either in file or direct input. The input file is initially convert the data in the file to DNA sequence until the end of file. Then convert the DNA sequence into binary file and divide the binary sequences into parts and perform xor operation on the binary parts with the help of key on the n parts after xor operation. Convert the resultant value of xor operation i.e binary sequence into DNA sequence and send to automata machine. Here with the help of automata machine the DNA sequence is convert into DNA code words which is in the form of text and number and in unrecognized form. Thus along with the result output embedded the key value and its generation used as cipher text to the receiver. The algorithm flow is shown in the architecture diagram shown in fig 2.

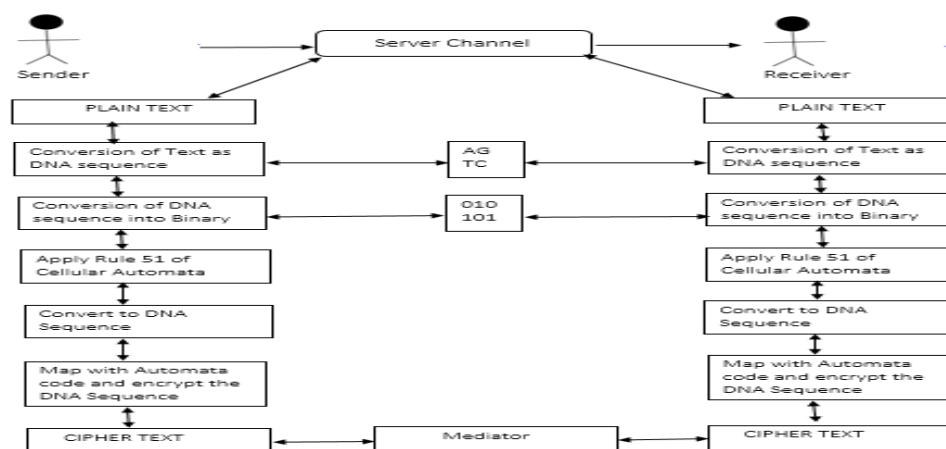


Fig.2. Pictorial illustration of DNA based Cellular Automata System

3.2. Proposed Algorithm

The proposed algorithm is detailed below in the form of pseudocode.

Input: F [file of any type], A [Automata for Plain text to AGTC data generation], $c1$ [code book1], $c2$ [code book2], $c3$ [code book3], $c4$ [code book4]
Output: File F with the AGTC coded DNA sequence

Algorithm : Encryption

Step 1: The File F is converted into DNA sequence:
 $F \rightarrow F[DNA(U)]$; // AGTC sequence file.

Step 2: In the File $F[DNA]$ convert the Uracil into Thymine acid
 $F[DNA(U)] \rightarrow F[DNA(T)]$;

Step 3: The DNA sequence is converted into binary sequence, The DNA output file of
 $F[DNA(T)] \rightarrow Binary[F[DNA(T)]]$; // Binary file

Step 4: Split the Binary Sequence into equivalent parts:
 $Binary[F[DNA(T)]] \rightarrow \{Binary[F1[DNA(T)]],$
 $\rightarrow Binary[F2[DNA(T)]],$
 $\rightarrow Binary[F3[DNA(T)]],$
 $\rightarrow Binary[F4[DNA(T)]]\}$

Step 5: Perform XOR operation with help of keys $K1, K2, K3, K4$ for all Binary Sequences $F1, F2, F3, F4$. // key generated and used.
 $X1 = (Binary[F1[DNA(T)]] (XOR) K1$
 $X2 = (Binary[F2[DNA(T)]] (XOR) K2$
 $X3 = (Binary[F3[DNA(T)]] (XOR) K3$
 $X4 = (Binary[F4[DNA(T)]] (XOR) K4$

Step 6: Combine the all output of the binary sequence into a single sequence.
 $X = X1 + X2 + X3 + X4$;

Step 7: Apply the rule 51 for the resultant binary sequence X .
 Now the state of x in time t is $X(t)$.
 RULE 51 $(00110011) \rightarrow s(t+1) = NOT(s_currentCell(t))$
 Next State of $X(t)$ is $X(t+1)$.
 $X(t+1) = Rule\ 51(X(t))$;

After applying rule, resultant will be binary sequence. // Initial state t is transformed into $t+1$ next state.

Step 8: Convert the Binary sequence into DNA sequence

$X(t+1) \rightarrow X[\text{DNA}(t+1)];$

$S = X[\text{DNA}(t+1)]$

Step 9: In the Sequence S convert the Thymine(T) into Uracil(U) acid.

$S \rightarrow S(T);$

Step 10: Send the $S(T) \rightarrow$ Automata Machine $A[S(T)];$ // DNA code word is generated

Step 11: Repeat the above steps until reach the end of the file;

Step 12: The Encrypted Data is the output of the automata machine

$A[S(T)] \rightarrow$ Encrypted Sequence;

Step 13: Append the Key in the output file at the end

Encrypted File[F] \rightarrow Encrypted Sequence + key;

This output file Contains the DNA code sequence.

End Algorithm

3.3.Implementation of Algorithm

The algorithm is implemented in three stages, initially the plain text which is taken as input from the user is converted into DNA sequence by the codebook1 and codebook 2 given below in table 1 and table 2 respectively.

This code book 1 and 2 converts the plain text into DNA Sequence for performing the step 1 operation of the algorithm.

Code Book 2

Then convert DNA sequence contains uracil into thymine component, the now converted DNA sequence is converted into binary sequence by based on the codebook 3 given below.

By using the codebook 3 the DNA sequence is converted into binary sequence, for performing step 4,5and 6. Where it converts into binary sequence and perform xor operation with key.

Code Book 3

Apply rule 51 of cellular automata [20] for the binary sequence, and convert the binary sequence into DNA code word using the table 3 and Send the AGTC data to Automata machine and with the help of the code book 4 and automata machine convert the DNA sequence into DNA code word.

Table 1: Code Book 1 - Plain text to DNA Sequence

SLNo	Plain Text	DNA Sequence	SLNo	Plain Text	DNA Sequence
1	A	UUU	14	N	GUC
2	B	UUC	15	O	GUA
3	C	UUA	16	P	GUG
4	D	UUG	17	Q	UCU
5	E	CUU	18	R	UCC
6	F	CUC	19	S	UCA
7	G	CUA	20	T	UCG
8	H	CUG	21	U	CCU
9	I	AUU	22	V	CCC
10	J	AUC	23	W	CCA
11	K	AUA	24	X	CCG
12	L	AUG	25	Y	ACU
13	M	GUU	26	Z	ACC

Table 2: Code Book 2 - Numbers and Special Characters to DNA Sequence

SLNo	Number & Symbols	DNA Sequence	SLNo	Number & Symbols	DNA Sequence
1	1	ACA	21	{	GAA
2	2	ACG	22	}	GAG
3	3	GCU	23	[UGU
4	4	GCC	24]	UGC
5	5	GCA	25	\	UGA
6	6	GCG	26		UGG
7	7	UAU	27	“	CGU
8	8	UAC	28	’	CGC
9	9	UAA	29	:	CGA
10	0	UAG	30	;	CGG
11	!	CAU	31	?	AGU
12	@	CAC	32	/	AGC
13	#	CAA	33	>	AGA
14	\$	CAG	34	.	AGG
15	%	AAU	35	<	GGU
16	^	AAC	36	,	GGC
17	&	AAA	37	_	GGA
18	*	AAG	38	-	GGG
19	(GAU	39	+	UU1
20)	GAC	40	=	CC1

Table 3: Code Book 3 - DNA Sequence to Binary Sequence

SLNo	Digital Code word	DNA Code word
1	00	A
2	01	G
3	10	T
4	11	C

Table 4: Code Book 4 - DNA code word

SLNo	DNA Code	Automata Code	SLNo	DNA Code	Automata Code
1	UUU	F1	34	UAC	Y2
2	UUC	F2	35	UAA	B1
3	UUA	L1	36	UAG	B2
4	UUG	L2	37	CAU	H1
5	CUU	L3	38	CAC	H2
6	CUC	L4	39	CAA	Q1
7	CUA	L5	40	CAG	Q2
8	CUG	L6	41	AAU	N1
9	AUU	I1	42	AAC	N2
10	AUC	I2	43	AAA	K1
11	AUA	I3	44	AAG	K2
12	AUG	M1	45	GAU	D1
13	GUU	V1	46	GAC	D2
14	GUC	V2	47	GAA	E1
15	GUA	V3	48	GAG	E2
16	GUG	V4	49	UGU	C1
17	UCU	S1	50	UGC	C2
18	UCC	S2	51	UGA	B1
19	UCA	S3	52	UGG	W1
20	UCG	S4	53	CGU	R1
21	CCU	P1	54	CGC	R2
22	CCC	P2	55	CGA	R3
23	CCA	P3	56	CGG	R4
24	CCG	P4	57	AGU	S5
25	ACU	T1	58	AGC	S6
26	ACC	T2	59	AGA	R5
27	ACA	T3	60	AGG	R6
8	ACG	T4	61	GGU	G1
29	GCU	A1	62	GGC	G2
30	GCC	A2	63	GGA	G3
31	GCA	A3	64	GGG	G4
32	GCG	A4	65	UU1	X1
33	UAU	Y1	66	CC1	X2

Finally append the key with the DNA code word and send to receiver i.e. encrypted text data or file.

4. RESULTS AND DISCUSSION

The proposed algorithm is implemented using Java and MySql as back end. The sample screen shot of the implementation is shown in Fig.3. The database is created and the encrypted and decrypted values are stored. The following are the computational parameters which have been considered for evaluation for the proposed algorithm,

- Encryption and decryption time consumed by the data (bits)
- Space utilization (MB)
- Throughput

Table 5: Comparing the data based on the encryption time and storage

Types of Algorithm	Computation time (s) of data (bits)						Average time (ms)	Throughput (ms)	Storage (MB)
	8	16	32	64	128	256			
RSA	50	52	54	56	58	60	55	9.163	82.26
AES	48	49	50	50	53	56	51	9.881	82.15
DES	49	49	51	51	52	55	51.16	9.853	82.35
Proposed Method	50	50	51	51	52	53	50.26	10.02	82.03

The encryption time is nothing but the time taken by the data to be encrypted and then to be stored in the database similarly the decryption time is the time taken to obtain the plain text from

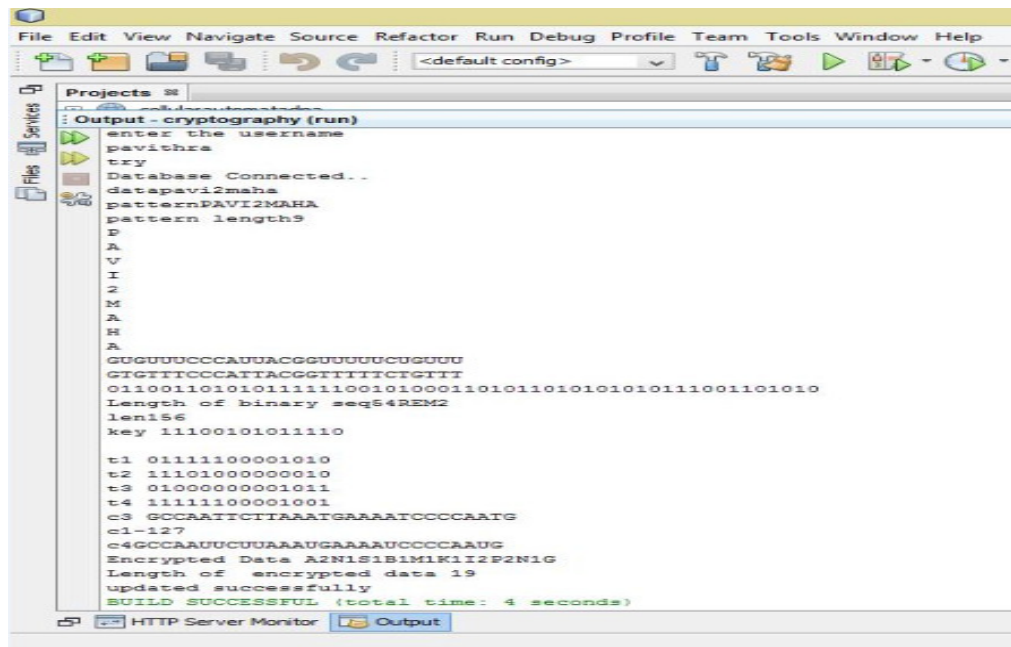
the cipher text. The standard algorithms which are taken for the comparison are RSA, AES and DES algorithms. The parameters which are taken for comparison are average encryption and decryption time, throughput and storage. The comparison of the well-known algorithms with the proposed algorithm is given in table 5. As the storage size shows slight deviation on considering the bits individually, so the values of the database was assigned as zero initially and after aggregating all the set of the bits the final value was observed. To calculate the computation time of data different block size in bits are taken into account, they are 8,16,32,64,128 and 256 bits. The throughput can be obtained by dividing the average time with the total size of the data bit and it is expressed by the formulae:

$$\eta = \frac{\sum_{i=0}^n D_n}{T}$$

Where, η is throughput, D is data and T is the average time consumed by the data.

Encryption

The Plain text given by the user is encrypted using this algorithm effectively by applying all the steps discussed in the algorithm and rule 51 is also applied to generate the encrypted data.



```

enter the username
pavithra
try
Database Connected...
datapavi2maha
patternDAVI2MAHA
pattern length9
D
A
V
I
2
M
A
H
A
GUGUUUCCCAUUACGGUUUUUCUGUUU
GTGTITCCCATACGGTTTTCTGTIT
0110011010101111110010100011010110101010111001101010
Length of binary seq54REM2
len156
key 11100101011110

t1 01111100001010
t2 11101000000010
t3 01000000001011
t4 11111100001001
c3 GCCAATTCTTAAATGAAAATCCCAATG
c1-127
c4GCCAAUUCUAAAUGAAAAUCCCCAAUG
Encrypted Data A2N1S1B1M1K1I2P2N1G
Length of encrypted data 19
updated successfully
BUILD SUCCESSFUL (total time: 4 seconds)

```

Fig.3. Encryption output

Result Analysis

The result based on the throughput obtained for the different algorithms during the encryption process is shown in fig 4. It denotes that the DNA based Cellular Automata cryptographic algorithm is having better performance than the other cryptographic algorithm.

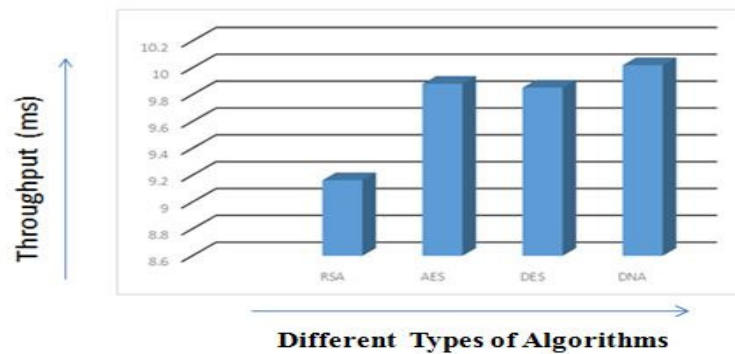


Fig.4. Comparison of algorithm based on throughput for encryption

Fig 5 illustrates the result based on the based on the throughput obtained for the different algorithms during the decryption process. It denotes that the DNA based Cellular Automata cryptographic algorithm is having better performance than the other cryptographic algorithm.

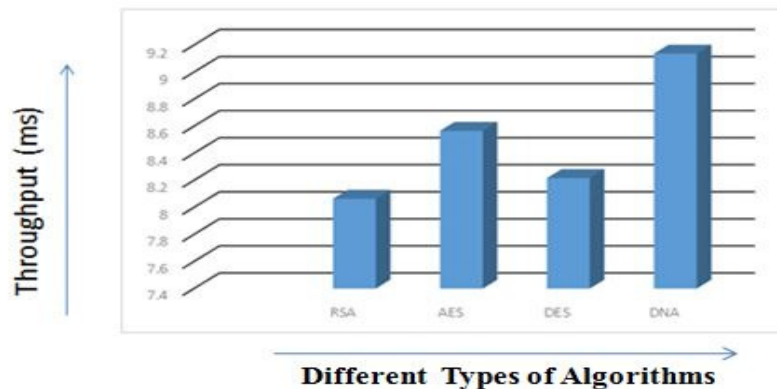


Fig.5. Comparison of algorithm based on throughput for decryption

From these results, it is easy to observe that the existing cryptographic algorithms still have a disadvantage in the encryption process over the DNA cryptographic algorithms in terms time consumption and serially in throughput. On the other hand, it is easy to observe that existing cryptographic algorithm have a disadvantage in the decryption process over other algorithm in terms of time consumption and storage. So based on the observed results it is found that the DNA based Cellular Automata algorithm has good performance when compared with AES, DES and RSA.

5. CONCLUSION

This paper explores the DNA cryptography along with the finite state machine. In the proposed algorithm data is secured at 4 levels, using : XOR, conversion in DNA, DNA is converted into binary based sequence, and it is subjected to rule 51 of cellular automata. Binary sequence is again converted into DNA Sequence. By using this algorithm and mechanism the generated cipher text is quite difficult to crack. The proposed algorithm is powerful in terms of security

features. The proposed algorithm is compared with other standard cryptographic algorithms against various parameters. The proposed algorithm can be further customized such that it can secure cloud database and other vulnerable system. As for now, the proposed algorithm can be used only for the text encryption it can also be extended to image encryption.

REFERENCES

1. Ferguson, N., Schnier, B. and KonhoT, "Cryptography Engineering: Design principles and Practical applications", 2010
2. Thiagarajan P, Aghila G, Prasanna Venkatesan V, "Dynamic Pattern Based Image Steganography", Journal of Computing , Volume 3, Issue 2 February 2011, pp.1-9, ISSN 2151-9617
3. Thiagarajan P, Natarajan V, Aghila G, Prasanna Venkatesan V, Anitha R, "Pattern based 3D Image Steganography", Springer 3D Research Journal, Vol. 04, no.1, March 2013, pp.1-8, ISSN: 2092-6731
4. Thiagarajan P, Aghila G, Prasanna Venkatesan V, "Stepping up Internet Banking Security using Dynamic Pattern Based Image Steganography", Springer (LNCS) in Communications in Computer and Information Science Series(CCIS) , June 2011, ISSN: 1865:0929
5. U.Noorul Hussain, T.Chithralekha, "Review of DNA cryptology", CiiT International Journal of Networking and Communication Engineering, vol 3, No 13, October 2011, pg No 843-849.
6. Grasha Jacob, A. Murugan, "DNA based Cryptography: An Overview and Analysis", ISSN: 2222-4254, Int. J. Emerg. Sci., 3(1), 36-42, March 2013.
7. H. Z. Hsu and R. C. T. Lee, "DNA Based Encryption Methods", The 23rd workshop on combinatorial mathematics and computation theory.
8. Guangzhao Cui, Cuiling Li, Haobin Li, Xiaoguang Li "DNA Computing and Its Application to Information Security Field", 2009 fifth international conference on natural computation.
9. Anupriya Aggarwal, Praveen Kanth, "Secure Data Transmission Using DNA Encryption", Computer Engineering and Intelligent Systems, Vol.5, No.7, 2014.
10. Sambhu Prasad Panda, Madhusmita Sahu, Umesh Prasad Rout, Surendra Kumar Nanda "Encryption and Decryption algorithm using two dimensional cellular automata rules in Cryptography", International Journal of Communication Network & Security, Volume-1, Issue-1, 2011.
11. Rama R, BalaSuyambu J, Andrew Arokiaaraj, Shanmugam Saravanan, "A Study of DES Algorithm with cellular automata", International Journal of Innovative Management, Information & Production ISME International ©2011 ISSN 2185-5439 Volume 3, Number 1, March 2012 PP.10-16
12. Pratibha Sharma, Niranjana Lal, Manoj Diwakar "Text Security using 2D Cellular Automata Rules", Conference on Advances in Communication and Control Systems 2013 (CAC2S 2013).
13. Rupali Soni*, Gopal Prajapati, Arif Khan, Deepak Kulhare, "Triple Stage DNA Cryptography Using Sequential Machine", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 8, August 2013 ISSN: 2277 128X.
14. M.Venugopal, Dr. E.G.Rajan, Dr. Sharma, "Security measures for Smart Devices through Cryptography Using Cellular Automaton", M.Venugopal et al, (IICSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (1) , 2013, 129 – 133.
15. Pradipta Maji and Chandrama Shaw, Niloy Ganguly, Biplab K. Sikdar and P. Pal Chaudhuri, "Theory and Application of Cellular Automata For Pattern Classification", Fundamenta Informaticae 58 (2003) 321–354 IOS Press.
16. Stephen Wolfram, "Random sequence generation by cellular automata". Advances in Applied Mathematics, 7:123,169, 1986.
17. Cellular automaton - Wikipedia, the free encyclopedia url:http://en.wikipedia.org/wiki/Cellular_automaton retrieved on July 15, 2015
18. Cellular Automata rules lexicon - User DLLs - url:http://psoup.math.wisc.edu/mcell/rullex_life.html retrieved on Aug 26, 2015.
19. Cellular Automaton -- from Wolfram MathWorld url:<http://mathworld.wolfram.com/UniversalCellularAutomaton.html> retrieved on Aug 31, 2015.
20. Cellular Automata The 256 Rules (Stanford Encyclopedia of Philosophy)- url:<http://www.roguobasin.com/index.php> retrieved on September 16, 2013.
21. S.Jeevidha et.al , "Analysis on DNA based Cryptography to Secure Data Transmission", International Journal of Computer Applications (0975 – 8887), Vol 29– No.8, September 2011.