ISSN 2229-5518

Implementation of DNA algorithm for secure voice communication

Akanksha Agrawal, Akansha Bhopale, Jaya Sharma, Meer Shizan Ali, Divya Gautam

Abstract— secure voice communication is vulnerable nowadays. Received data on the other side becomes unfathomable and evasive ,as the algorithms involved in keeping data covert seems to be inefficient and data is prone to attacks. Hence the need for voice data protection is on the rise. DNA algorithm which has been described in this research includes the enigmatic way of ciphering the received converted voice commands that has been converted into text form. We propose a secure and computationally feasible encryption/decryption algorithm based on DNA components. This algorithm includes the four major DNA components which are serving the purpose of translating the received voice commands from the text form to an uncanny form, thus providing the secure voice communication by preventing eavesdropping and pilfering of data in a punctilious way. The main scope of this paper is to propose an algorithm to protect voice messages and making it secure using recent DNA algorithm.

Index Terms — DNA, DNA components, DNA Algorithm, Voice encryption

1 INTRODUCTION

DATA security is the main aspect of secure data transmission over network. Data Security is a challenging issue of data communication that touches many areas including secure communication channel, strong data encryption technique and trusted third party to maintain the database. The rapid development in information technology needs the secure transmission of confidential data which gets a great deal of attention. The information could be accessed by the unauthorized user for malicious purpose. Therefore, it is necessary to apply effective encryption/decryption methods to enhance data security.

When we talk about voice transmission, voice communication has threat of eavesdropping so in this paper we are proposing a secure way to convert detected voice into secure form, thus protecting it from eavesdropping. The speech detected will first gets converted into text format and then it will be encrypted using DNA algorithm. DNA encryption [5] is the forefront field of DNA computing. Different from traditional encryption methods, DNA (deoxyribonucleic acid) is a long molecule, with two strands rolled up in a double helix. This algorithm is implemented by using the natural DNA components (A – adenine, G – guanine, C – cytosine, T – thymine). Due to very high storage capacity of DNA, this field is becoming very talented. DNA algorithm is still in its development stage but offers so many possibilities.

The history of DNA computing is short, but full of amazing technological achievements. DNA computing was grounded in reality at the end of 1994, when Len Adleman a University of Southern California researcher, announced that he had solved a small instance of a computationally intractable problem using a small vial of DNA.

DNA computing and cryptography were introduced in 1990s. By representing information as sequences of bases in DNA molecules, Adleman showed how to use existing DNA-manipulation techniques to implement a simple, massively parallel random search [1], then in 1995 Lipton R J extended the adleman approach to solve another NP problem [2], Boneh D, Lipton R broke DES using molecular computations in 1995[3], then in 1996 Adleman L extended DNA computers to RNA used for breaking DES. After that C. T. Clelland, V. Risca, C. Bancroft cryptography has been shown to be one of the new applications of DNA computing in 1999[4], then in 2000 Gehani A, LaBean T H, Reif J Hused designed a discrete mathematics for designing a DNA cryptographic mechanism[5], P. L. Cox J find that the vast parallelism, exceptional energy efficiency and extraordinary information density are inherent in DNA molecules in 2001, Jie Chen proposed a novel design of DNA-based, molecular Cryptography design [6] Carbon nanotube-based message transformation, and DNA-based cryptosystem an proposed.

To demonstrate the performance, we present an interesting example to encode and decode images wing the proposed scheme in 2003 , Kartalopoulos S.V. initialized DNA cryptography in optics [7] in 2005 , Xing Wang, Qiang Zhang* use a new way to show how cryptography works with DNA computing, it can transmit message securely and effectively. The DNA has efficient parallel [8] molecular computation and huge storage which has been proved by the researchers by solving the issues such as expansive and time consuming problems.

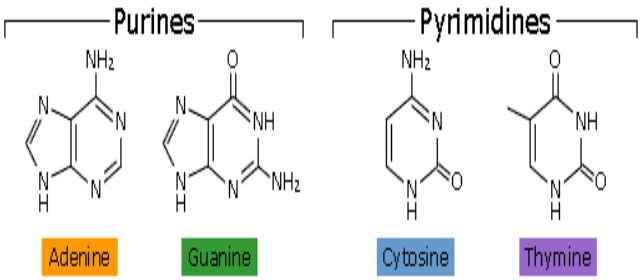
2 OVERVIEW OF DNA

DNA, or deoxyribonucleic acid, is the hereditary material in humans and almost all other organisms. Nearly every cell in a person's body has the same DNA. Most DNA is located in the cell nucleus (where it is called nuclear DNA), but a small

- *Akanksha Agrawal is currently pursuing Bachlors degree in Malwa Institute of Technology Indore. E-mail:akanksha.agrawalmit@gmail.com*
- *Akansha Bhopale is currently pursuing Bachlors degree in Malwa Institute of Technology Indore. E-mail:akanshabhopale15@gmail.com*
- *Jaya Sharma is currently pursuing Bachlors degree in Malwa Institute of Technology Indore. E-mail:jayasharma8@live.in*
- *Meer Shizan Ali,Assistant Professor MIT, Indore E-mail:mshizan@gmail.com*
- *Divya Gautam is Head of Department I.T. in Malwa Institute of Technology, Indore. E-mail: divyagautam06@gmail.com*

amount of DNA can also be found in the mitochondria (where it is called mitochondrial DNA or mtDNA).

The information in DNA is made up of four bases which combine to form chains. These bases include two purines (Adenine and Guanine) and two pyrimidines (Cytosine and Thymine).These are commonly referred to as A, G, C and T respectively. The structure of DNA purines and pyrimidines is shown in Figure 1 below-



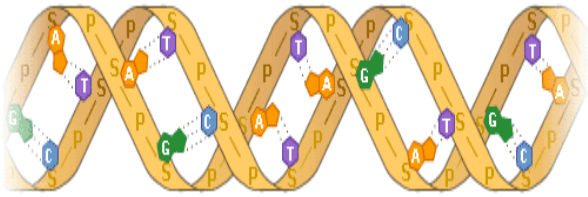


Figure 1. DNA Purines and Pyrimidines

A DNA molecule has double-stranded structure obtained by two single-stranded DNA chains, bonded together by hydrogen bonds: A = T double bond and C ≡G triple bond. An important property of DNA is that it can replicate, or make copies of itself. The basic DNA structure is shown in Figure 2 below-

Figure 2. Basic DNA structure

DNA bases pair up with each other, A with T and C with G, to form units called base pairs. Each base is also attached to a sugar molecule and a phosphate molecule. Together, a base, sugar, and phosphate are called a nucleotide. Nucleotides are arranged in two long strands that form a spiral called a double helix. The structure of the double helix is somewhat like a ladder, with the base pairs forming the ladder's rungs and the sugar and phosphate molecules forming the vertical sidepieces of the ladder.

What is really great about DNA is that it has a very autonomous self-replication mechanism in action. The replication process makes use of the two strands of DNA. Each of these strands acts as template and after going through a series of steps is converted into dual stranded DNA once again. This replication is very important because when the cell divides, the newly formed cell requires the same set of instructions for it to function and grow and the replicated DNA serves this purpose.

3. Mechanism Designed For DNA Algorithm

We have proposed a basic DNA algorithm structure. We have introduced strings by which we replaced a single character. Following table represents mapping of a character to a codon (string)-

S.No	Alphabet	codon	S.No.	Alphabet	codon
1	A	ATCG	27	a	CCAG
2	B	ATGC	28	b	CCGA
3	C	AGTC	29	c	CCAT
4	D	AGCT	30	d	CCTA
5	E	ACGT	31	e	GGAT
6	F	ACTG	32	f	GGTA
7	G	CATG	33	g	GGCT
8	H	CAGT	34	h	GGTC
9	I	CGAT	35	i	GGAC
10	J	CGTA	36	j	GGCA
11	K	CTAG	37	k	TTGA
12	L	CTGA	38	l	TTAG
13	M	TACG	39	m	TTCA
14	N	TAGC	40	n	TTAC
15	O	TCAG	41	o	TTCG
16	P	TCGA	42	p	TTGC
17	Q	TGAC	43	q	TTTT

S.No.	Neumerics& special charcters	codon	S.No.	Special characters	codon
1	1	CCCA	23	+	CGCG
2	2	CCCG	24	=	AATT
3	3	CCTT	25	{	AAAC
4	4	CCGG	26	}	AAAG
5	5	CCAA	27	[	AAGT
6	6	TTCC	28	]	AACT
7	7	TTAA	29	|	AAAT
8	8	TTGG	30	\	AATG
9	9	AAGG	31	;	CACA
10	0	AACC	32	:	TCTC
11	!	GGAA	33	“	TGTG
12	@	GGTT	34	‘	TATA
13	#	GAGA	35	<	TAAA
14	**$**	GTGT	36	>	CAAA
15	%	GCGC	37	,	ATTT
16	^	AATC	38	.	CTTT
17	&	ACAC	39	?	GAAA
18	*	AGAG	40	/	GTTT
19	(	ATAT	41	_	CCTG
20	)	CTCT	42	space	AGGG
21	-	AACC	43	~	GGAA
22	`	CCGT			

18	R	TGCA	44	r	GGGG
19	S	GTCA	45	s	AAAA
20	T	GTAC	46	t	CCCC
21	U	GATC	47	u	TTTA
22	V	GACT	48	v	TTTG
23	W	GCTA	49	w	TTTC
24	X	GCAT	50	x	GGGA
25	Y	AACG	51	y	GGGT
26	Z	AAGC	52	z	GGGC

Table 1. Mapping of character to a codon (string)

Following table represents mapping of all special characters and numeric values with codon (string)-

Table 2. Mapping of all special characters and numeric values with codon (string)

4. Working Of Voice Encryption System-

Figure 3 illustrates how the system is working or the sequence in which action gets performed.

Both computer and speakers are provided with power supply.

- Firstly, user gives voice input via microphone to computer.
- Secondly, voice input gets converted to text if user wants to type any message then he/she can type.
- Thirdly, user will have to enter encryption key.
- Fourthly, that text gets encrypted and gets saved.
- Fifthly that saved encrypted text opens up as a message.
- Sixthly, user will have to enter decryption key.
- Seventhly, message decrypted and user can again listen to his message via speakers.

.

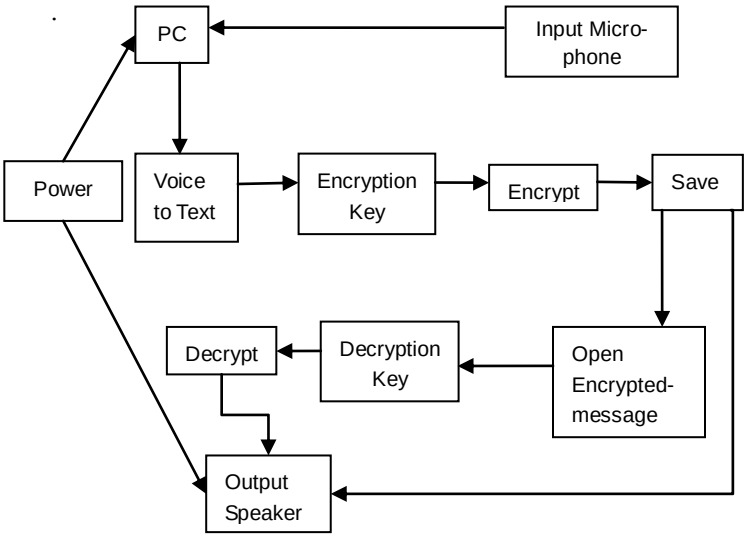


Figure 3. System Architecture activities

In this system we are using symmetric key or private key for encryption.Reason for using symmetric key is that it's Encryprtion and decryprion time is less than asymmetric key. As we know that an asymmetric scheme that uses a pair of keys for encryption: a public key, which encrypts data, and a corresponding private, or secret key for decryption.But symmetric key has following advantages over asymmetric key-

- Faster and easier to implement

- Lower overhead on system resources

Figure 4 shows symmetric key encryption by using DNA algorithm-

Figure 4. Symmetric Key Encryption

4. CONCLUSIONS-

Man has always needed some form of cryptography in order to conceal and protect information. This paper has main aim to facilitate the understanding of principles and some techniques of the new born field of DNA cryptography. All kinds of cryptography have their own advantages and disadvantages and can be treated as the complement of each other in future security applications. In this paper, proposed DNA algorithm is encrypting or hiding a data in terms of DNA sequences. All the experimental analyses show that the proposed encryption algorithm-

1. Encrypted message is associated with an ID number and at the time of decryption receiver must know that id and the correct Decryption key.
2. For the encryption of each character (upper/lower), special symbol and numbers there is corresponding DNA Sequences.

Despite its auspicious debut in 1994, it seems that DNA computing is destined to be remembered as a novel idea that was too difficult to implement practically. DNA cryptography is the future of the information security. Its complexity and randomness provides a great uncertainty which makes encoding of data in DNA format better than other mechanism of cryptography. The field of DNA computing is still in its infancy and the applications for this technology are still not fully understood. The research of DNA cryptography is still at the be-ginning, and there are many problems to be solved. But the vast parallelism, exceptional energy efficiency and extraordinary information density inherent in DNA molecules endow DNA cryptography special advantages over other kinds of cryptography.

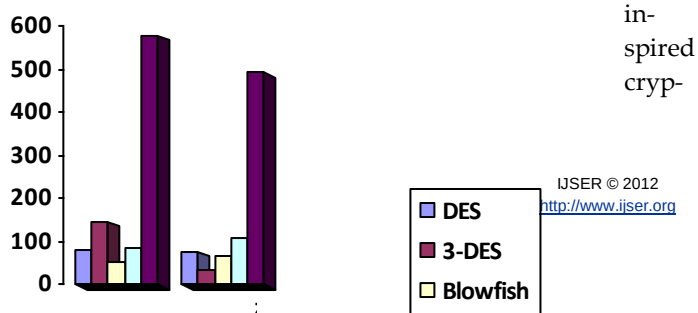


Figure 5. Encryption/Decryption time for DNA and classical ciphers

As seen in Figure 5, the DNA Algorithm requires a longer time for encryption and decryption, comparatively to the other ciphers [10]. Similarly the algorithm which we are using also have much greater encryption and decryption time than other classical ciphers, but it provides better security than others.The advantage is that DNA has a huge storing capacity, but on the other hand practically using the implementations requires a lot of time[9].

5. REFERENCES-

[1] Leonard M. Adleman "Molecular Computation of solution to combinatorial problems" Science, New Series, Vol. 266, No. 5187. pp. 1021-1024 Nov. 11, 1994

[2] R. J. Lipton," Using DNA to Solve NP-Complete problems," Science, vol. 268, pp. 542 545, 1995

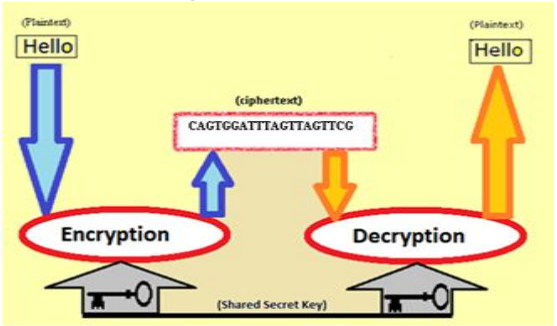
[3] D. Boneh, "Breaking DES using Molecular computer", American Mathematical Society, pp 37-65, 1995

[4]Taylor Clelland, "Hiding messages in DNA Microdots". Nature Magazine vol.399, June 1999

[5] A. Gehani, T. LaBean, and J. Reif, "DNA-Based Cryptography", Lecture Notes in Computer Science, Springer. 2004

[6] J Chen "A DNA-based, Bimolecular Cryptography Design"ISCAS'03.Proceedings2003

[7] Kartalopoupoulos, S.V.;," DNA-inspired cryp-



tographic method in optical communications, authentication and data mimicking ",Military Communications Conference, 2005. MILCOM 2005. IEEE

[8] G. Z. Cui, "New Direction of Data Storage: DNA Molecular Storage Technology," Computer Engineering and Applications, vol. 42, pp. 29–32, 2006.

[9] O. Tornea and M. E. Borda, DNA Cryptographic Algorithms, International Conference on Ad- vancements of Medicine and Health Care Through Technology, IFMBE Proceedings 26 (2009).

[10] Er. Ranu Soni, Er.Vishaka Soni, Er.Sandeep kumar "Innovative field of cryptography: DNA cryptography" Computer Science and Information technology CSCP 2012

[11] S. Jeevidha, Dr.M.S.Saleem Basha, Dr.P.Dhavachelvan "Analysis on DNA based Cryptography to Secure Data Transmission" Dept. of CSE Pondicherry University Volume 29– No.8, September 2011

[12]Amrita Vishwa Vidyapeetham " An Uncompressed Image Encryption Algorithm Based on DNA Sequences"Department of Computer Science & Engineering, CS & IT 02, pp. 258–270, 2011