Comparison of Modern And DNA Cryptography

Saurabh Kumar[1], HPS Kang[2]
[1, 2] 1University Centre of Instrumentation and Microelectronics
Panjab University, Chandigarh, India

Abstract- *DNA is used as an information carrier and accounts for hereditary biological behavior. In this paper, confidential DNA data is transmitted to a receiver. In order to do so, firstly, digitize DNA into binary and then use a suitable unbreakable method to transmit the secret data. Hence, a cryptographic method called DNA cryptography and already existing method of modern cryptography are studied, implemented and results are obtained. Both these cryptographic method's results are compared and analyzed to find out the better approach. The comparison is done in the main aspects of key size, computational complexity and cryptographic strength. The analysis is made to find the ways these mentioned parameters are enhancing the respective cryptographic methods and the performance is evaluated.*

Keywords- DNA Cryptography; Modern Cryptography; DES Algorithm; One-Time Pad

I. INTRODUCTION

From the ancient days till present, the secret writing techniques are practiced to safeguard the data from the adversaries. Among these techniques, cryptography and steganography are the most common and widely used methods. Cryptography is the practise of protecting the contents of a message whereas steganography is used to conceal the contents of data from the hackers so that it does not attract the attention towards itself as an object of scrutiny. In the cryptographic process, certain parameters are to be considered i.e. the encryption and decryption process key generation, encrypted data form, method of retrieving the data back from the encrypted data.

The most secured and the presently practiced technique nowadays is the modern methods of cryptography. It involves more mathematical computations and there are two types of keys, the public and the private key. There is another newly emerging cryptographic technique in the field of cryptography called DNA cryptography. The main objective of this method is to encrypt the plain text and hide it in the original or duplicate DNA digital form. This method involves biological computations and the algorithm of DNA cryptography method to be executed. In this paper, the Triple DES algorithm from the modern methods and the DNA hybridization methods are implemented to transmit the confidential genetic DNA data.

II. THEORY

Cryptography is a scientific way of encrypting and decrypting the data so as to keep the data more secured. It is capable of keeping the secrecy of data while saving the information or passing it over the unsafe networks, like internet [1]. This is done to safeguard the data from the hackers and making it understandable only to the intended user (receiver). The flow diagram of cryptography is illustrated in Figure 2.1.

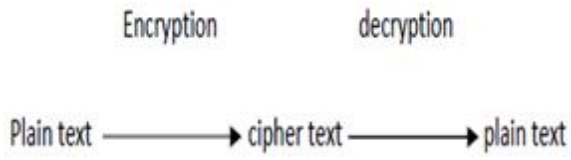

Figure 2.1- Flow Diagram of Cryptography

Plain text: The original data which is to be transmitted to the intended receiver is considered as the plain text.

Encryption: The method of acquiring the cipher text from the plain text is known as encryption.

Cipher text: The confused or the distorted data acquired as a result of the encryption process is known as the cipher text.

Decryption: Decryption is the converse (reverse process) of encryption. The original message or the plain text is acquired as a result of this process.

Thus, the confidentiality of the encrypted data acquired is entirely dependent on two main things: the cryptographic strength of the algorithm involved and the privacy of the key [2].

2.1 TYPES OF CRYPTOGRAPHIC FUNCTIONS:

The cryptographic functions are mainly classified into two types:

1) Secret key function

2) Public key function

2.1.1 Secret Key Cryptography

In secret key cryptography, the encryption is done by converting the message (plain text) into the unintelligible data (cipher text) by using a single key. The cipher text produced as a result of encryption is of the same length as the plain text. Decryption is the reverse process of acquiring the plain text by utilising the same key used in the encryption process. The process is represented in the form of flow diagram in the Figure 2.2.

Secret key cryptography can also be referred as the conventional cryptography or the symmetric cryptography [1]. The captain midnight code and mono alphabetic cipher are the best examples of this type of cryptography, though they are easy to break.

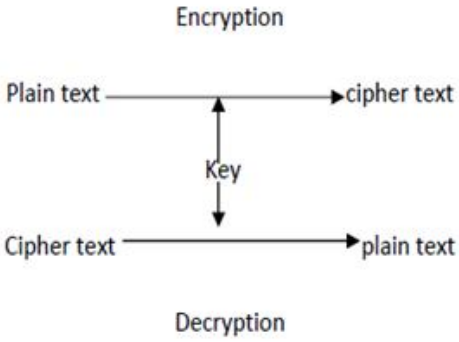

Figure 2.2 - Flow diagrams for secret key cryptography

2.1.2 Public Key Cryptography

Public key cryptography can be also referred as the asymmetric cryptography. Unlike secret key cryptography, public key cryptography utilises two keys. Instead of that each individual has two keys: a private key which is to be kept more confidential and a public key that is possibly recognizable by everyone in the world.

Encryption and decryption are inverse, mathematical and opposite functions to each other. The flow diagram of the public key cryptography [1] is illustrated below in the Figure 2.3. In addition with public technology, there is also the possibility of providing the digital signature on a message like a checksum.

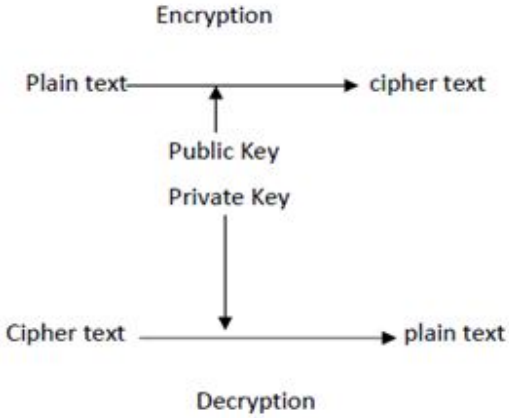

Figure 2.3 - Flow diagram for public key cryptography

2.2 BIOLOGICAL BACKGROUND

DNA (deoxyribonucleic acid) is hereditary in humans which stores the information as a code and is made of four chemical bases: A (adenine), C (cytosine), T (thymine) and G (guanine). DNA bases pair up with each other, A with T and C with G, to form units. Each base is also attached to a sugar molecule and a phosphate molecule, which is arranged in two strands to form a spiral called a double helix, together are called as a nucleotide. DNA is a molecule that carries most of the genetic information. Nucleotides are the building block of DNA. The nucleotide is chemical compound that consists of phosphate, sugar and bases cytosine (C), guanine (G), adenine (A), or thymine (T) [3–9]. Figure 2.4 shows a section of the DNA sequence.

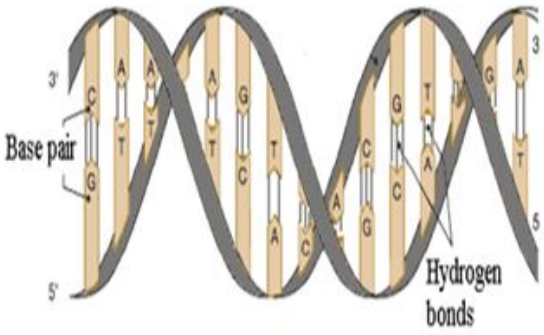

Figure 2.4 – DNA structure

Proteins are the large biomolecules consisting of one or more long chains of amino acid. Each amino acid in protein synthesis is encoded by three nucleotides. These trinucleotides in the DNA are called ‘‘Code’’ that are encoded amino acids. If they are in the RNA, they would be called ‘‘Codon.’’ Each codon is comprised from three nucleotides, where the codon corresponds to a single amino acid (refer Figure 2.5). Codes

are converted to the codons during mRNA synthesis in DNA. Code and codon are complementary. There are 64 types of codons in the RNA (U is Uracil instead of Thymine in case of RNA). All of 64 codons correspond to an amino acid [3–5]. One of these codons is AUG.

The AUG is start codon; this codon represents the amino acid methionine and there is not another such codon. There are three different codons indicating the end of the protein synthesis. These are UAA, UAG and UGA. These are called the stop codons [4, 6, 9–11].

Amino Acid	3 Letter Abbreviation	IUPAC Notation	Translating Codons
Alanine	Ala	A	GCT, GCC, GCA, GCG
Arginine	Arg	R	CGT, CGC, CGA, CGG, AGA, AGG
Asparagine	Asn	N	AAT, AAC
Aspartic acid	Asp	D	GAT, GAC
Cysteine	Cys	C	TGT, TGC
Glutamine	Gln	Q	CAA, CAG
Glutamic acid	Glu	E	GAA, GAG
Glycine	Gly	G	GGT, GGC, GGA, GGG
Histidine	His	H	CAT, CAC
Isolucine	Ile	I	ATT, ATC, ATA
Methionine	Met	M	ATG
Leucine	Leu	L	TTA, TTG, CTT, CTC, CTA, CTG
Lysine	Lys	K	AAA, AAG
Phenylalanine	Phe	F	TTT, TTC
Proline	Pro	P	CCT, CCC, CCA, CCG
Serine	Ser	S	TCT, TCC, TCA, TCG, AGT, AGC
Threonine	Thr	T	ACT, ACC, ACA, ACG
Tryptophan	Trp	W	TGG
Tyrosine	Tyr	Y	TAT, TAC
Valine	Val	V	GTT, GTC, GTA, GTG
STOP	Stop	*	TAA, TGA, TAG

Figure 2.5 – List of Amino acids & their translating codons

III. LITERATURE REVIEW

The research objective is to compare the modern method algorithm and the DNA method algorithm by comparing the various parameters such as key size, mathematical expressions involved in the algorithm, cryptographic strength, computational complexity, memory, cost, data length, existing period and to find out the best algorithm among the two methods – Modern Cryptography and DNA Cryptography.

Ahsan Omer and Muhammad Imran Farooq [13] presented the use of DNA computing in cryptography for secure communications. The discussed algorithm utilised One Time Pad encryption scheme. One time pad key was acquired using DNA bases. DNA lookup table was also used for increasing the security of cipher text. The implementation was done on Matlab.

Monica Borda [14] presented the principles of bio molecular computation (BMC) and several algorithms for DNA (deoxyribonucleic acid) steganography and cryptography: One Time-Pad (OTP), DNA XOR OTP and DNA chromosomes indexing. It represents a synthesis of her work in the field, sustained by former referred publications. Experimental results obtained using Matlab Bioinformatics Toolbox and conclusions were made at the end of work.

Gehani [15] described the beginning study of the DNA oriented data confidentiality and its utilization. The DNA security was explained briefly in two main ways. One method based on the one-time-pads of DNA and the other way, based on the steganography method of DNA. The one-time-pad concept was used in XOR approach and the substitution approach of DNA. Their values are strong and indestructible. From this paper it was well understood, the DNA OTP key producing methods of binding the sequences is done using a special enzymatic protein called ligase.

IV. PROPOSED METHODOLOGY

4.1 THE SOFTWARE

MATLAB (matrix laboratory) is a multi-paradigm numerical computing environment and proprietary programming language developed by MathWorks [17]. MATLAB allows matrix manipulations, plotting of functions and data, implementation of algorithms, creation of user interfaces, and interfacing with programs written in other languages, including C, C++, C#, Java, Fortran and Python.

Although MATLAB is intended primarily for numerical computing, an additional package Simulink, adds graphical multi-domain simulation and model-based design for dynamic and embedded systems.

The various inbuilt functions present in MATLAB are used to form two new functions to digitize the DNA data into binary and vice versa –

1. nucleotide2binary
2. binary2nucleotide

4.1.1 Conversion of Binary data to DNA data format and vice versa

When the data is found to be ‘A’ in the DNA form, it is converted to the binary form ‘00’.

When the data is found to be ‘G’ in the DNA form, it is converted to the binary form ‘01’.

When the data is found to be ‘C’ in the DNA form, it is converted to the binary form ‘10’.

When the data is found to be 'T' in the DNA form, it is converted to the binary form '11'.

4.2 Triple DES Algorithm

The Triple DES Algorithm is used to implement the data security in binary representation of DNA sequence using three randomly generated keys K1, K2 and K3.

Triple DES algorithm utilizes the normal DES algorithm three times (refer Figure 4.1) to obtain the cipher text from the plain text and to get back the original message from the encrypted message using the three keys K1, K2 and K3.

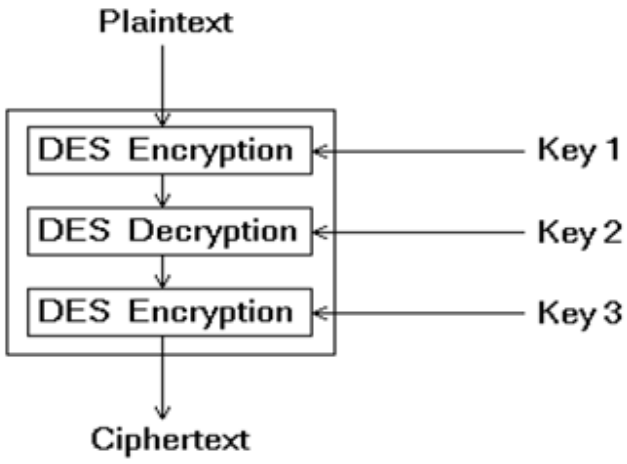

Figure 4.1 - Triple DES block diagram

Confidential DNA data or plain text to be transferred 'GGTTGACGGATA'.

One Time Pad (OTP) - The essential Security of the OTP (One Time Pad) is entirely because of the randomness of the key. The one-time pad is that the solely cryptosystem that exhibits what's mentioned as good secure.

Key K1 → 208 163 109
Key K2 → 131 97 28
Key K3 → 199 26 162

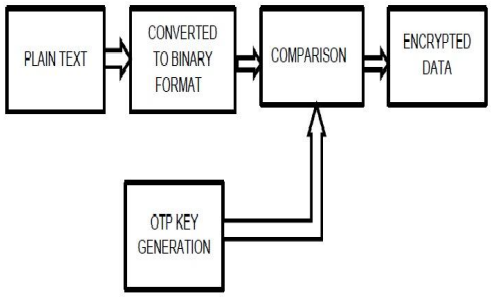

Figure 4.2 – Block Diagram for Encryption Process

4.2.1 Algorithm for Encryption

(refer Figure 4.2)

Step-1: The plain text (i.e. A, T, G and C) is converted into binary code using function nucleotide2binary in MATLAB (refer figure 5.4). Also, convert the binary code into ASCII code (perform 8 bit division of bytes). The plain text is the data to be transferred to the receiver.
Step-2: Generate three random OTP keys with ASCII code of size (perform 8 bit division of bytes) depending upon the size of obtained step 1 binary is generated.
Step-3: ASCII code of OTP Keys K1, K2 and K3 is converted into binary code (number conversion is applied).
Step-4: Now xor is done of key K1 and binary obtained in step 1.
Step-5: The result obtained in step 4 is xor with key K2, and later, xor with key K3 is obtained.
Step-6: The result finally obtained after K3 in binary form is converted to ASCII code. This code is known as encrypted message or data

4.2.2 Algorithm for Decryption (refer Figure 4.3)

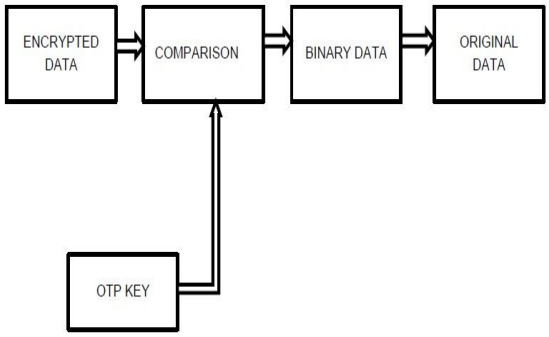

Figure 4.3 - Block Diagram for Decryption Process

Step-1: The ASCII code of encrypted data is converted to binary code (using 8 bit division of bytes).

Step-2: Now, the binary obtained in step 1 is xor with key K3, and the result obtained is xor with key K2 and later, result is xor with K1 (for the case of secret key cryptographic method).
Step-3: For the case of public key cryptographic method, a different key K is xor with the binary code of encrypted data to obtain the result.
Step-4: The results obtained in step 2 and 3 (as both results will be same) is called decrypted message.
Step-5: Binary code of decrypted message is converted into DNA base equivalent by using function binary2nucleotide (refer figure 5.2). And, finally the result in form of A, T, G, C is obtained by the receiver.

4.3 DNA HYBRIDIZATION

The unnatural strands DNA are obtained or formed through the chemical process using a DNA synthesizer machine. The strands or sequences of DNA obtained have 50 to 100 nucleotides in extent. These strands are termed as oligonucleotides. A single unique ssDNA under specific situations can combine with other matching or complementary ssDNA to form the double stranded [14] DNA helix form dsDNA. The process of forming dsDNA is illustrated in the figure 4.4. Since the ssDNA from distinct sources which are considered to be hybrids, join together to form molecules of double strands. This process is termed as hybridization.

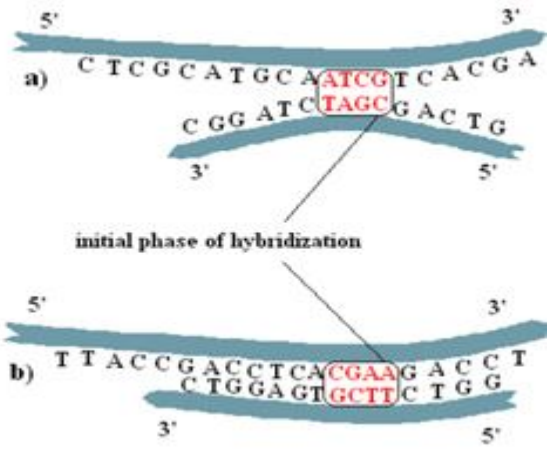

Figure 4.4 - Hybridization process

4.3.1 DNA OTP Generation in two main ways

Assembling randomly long sequences from short oligonucleotide sequences. The ssDNA segments can be bound together using a special protein (ligase) and a short complementary strand as template as shown in Figure 4.5.

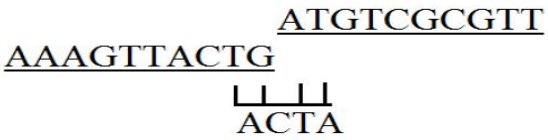

Figure 4.5 – Binding process between two segments

Using the chromosome DNA sequence which is very large (thousands, millions bases), or segments of chromosomes. The delimitation of a DNA segment in a long sequence can be done using short length (20 bp) primers.

4.3.2 Algorithm for Encryption & Decryption

In the DNA hybridization technique [14], the original message which is the plain text is converted into the binary form of the data. The key used is an OTP key generated randomly. The length of the key is 12 times longer than the plain text. Then for each '1' bit in the binary data, the key is compared with the binary digit and the encrypted message is produced. And if the binary digit is found to be '0', no operation is performed. The encrypted message is in the form of DNA. The decryption process is performed in reverse to obtain the original data.

Confidential DNA data or plain text to be transferred 'GGTTGACGGATA'.

Primers:

Primers are the short DNA sequences. In DNA cryptography, two primers are used. The two primers are used as a header and footer in picking the DNA data from the public database (NCBI) which is used as an OTP key. The primers will be shared between the users to identify the exact OTP key from the entire message obtained. So, the OTP key in the database sequence starts where the header primer ends and the OTP key ends where the footer primer starts.
From the OTP key given below, the following DNA sequences are the primers.

Primer 1: ATAGAAGATAAA
Primer 2: GGGAATAAGCTT

The randomly generated OTP key using MATLAB bioinformatics toolbox [18] of species 'Clostridium botulinum' (Locus or Accesion No. YP_009069373) is represented as follows –

ATGATTAACATAATAGAAGATAAAAGCATTCTGATC
AATAAAGCCAATGATTGCGAACCAAGCGCGAAATCA
TTCTAAAGGACGATTTCTCTAAGAAGAGAAAACAGT

ATTATAATATGTTAAATTAAAGGAAGACTGCAAGTC
TATTTTTGTAAAGGGCGAGTACGTGATCGAAATATCG
ACGATTCTAATTATATTAAATACATCTGGATCAACGG
AGACTCCGTAGAAAAGCTATTAAATCAAAAGAACGA
TCAGTACCGTCTCCTTATAGATAATATCCTTGGGAAT
AAGCTT

The above key is a randomly generated single stranded DNA strand (ssDNA) with the length of about 300 bases.

Actually, based on the size of the plain text, the OTP key is generated depending on it. The key is made 12 times huger than the binary form of the data. It is because; 1 bit of the binary information is encoded into nucleotides with length 12. So accordingly, depending on the size of the data, a group of ssDNA sequences will be obtained. Therefore, the key is lengthier that the original data. Thus high security is confirmed.

V. RESULS & DISCUSSION

5.1 Triple DES Algorithm

The **encrypted message (OP3) -** 203 145 159

Key K1, K2 and K3 are **Public Keys** whereas **Key K** is the **Secret Key.**

Private Key K □ 148 216 211

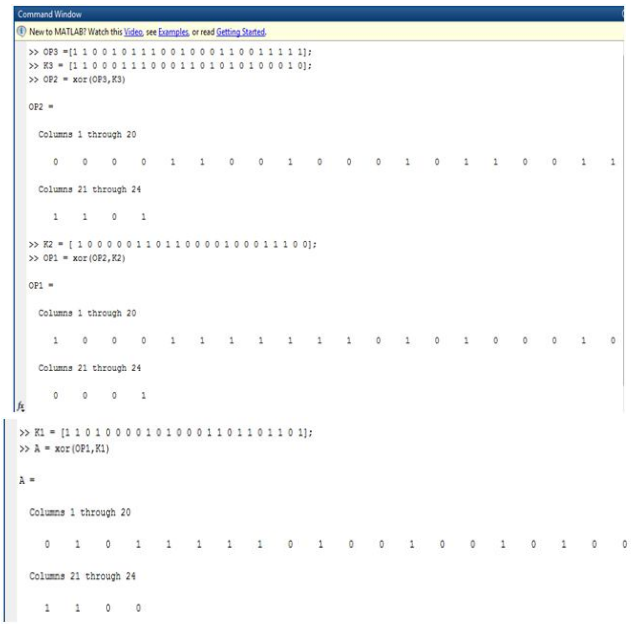

Figure 5.1 - Application of 'xor' in MATLAB command window (Decryption process using Secret Key Cryptography method)

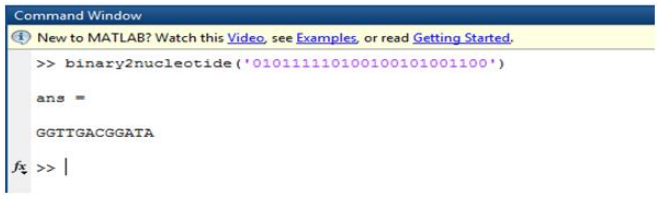

Figure 5.2– Application of 'binary2nucleotide' command in MATLAB command window (Decryption process)

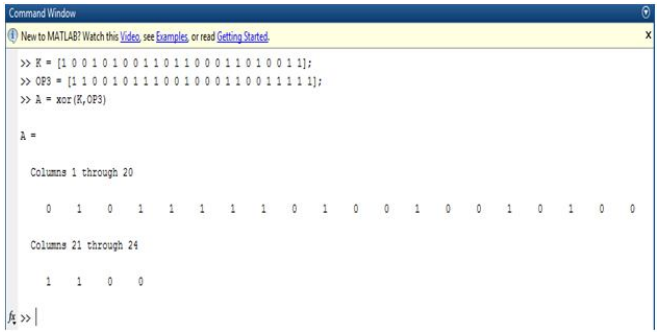

Figure 5.3 - Application of 'xor' in MATLAB command window (Decryption process using Public Key

Cryptography method) The **decrypted message (A) –** 95 73 76

The decrypted plain text is (refer figure 5.2) **'GGTTGACGGATA'.**

So, clearly Public Key Cryptography (Figure 5.2) is a fast method of retrieving encrypted data whereas Secret key cryptography (refer Figure 5.1) ensures high level of security as well as confidentiality as it is difficult to break. But, one of the drawbacks of the secret key method is that it can cause confusion.

Also for public key method, there is also the possibility of generating the digital signature on a message like a checksum. The checksum can be generated by anyone whereas; the digital signature can be generated only when the private key is known.

5.2 DNA Hybridization

During the encryption process, the operation is performed only for the binary '1' in the data.

If the binary bit is found to be '0' no operation is functioned.

The binary digits are compared with the DNA data in reverse order and the message is encrypted.
The generated binary data (refer figure 5.4): 010111110100100101001100

The randomly [18] generated OTP key:

ATGATTAACATA, ATAGAAGATAAA,
AGCATTCTGATC, AATAAAGCCAAT,
GATTGCGAACCC, AAGCGCGAAATC,
ATTCTAAAGGAC, GATTTCTCTAAG,
AAGAGAAAACAG, TATTATAATATT,
GTTAAATTAAAG, GAAGACTGCAAG,
TCTATTTTTGTA, AAGGGCGAGTAC,
GTGATCGAAATT, ATCGACGATTCT,
AATTATATTAAA, TACATCTGGATC,
AACGGAGACTCC, GTAGAAAAGCTA,
TTAAATCAAAAG, AACGATCAGTAC,
CGTCTCCTTATA, GATAATATCCTT,
GGGAATAAGCTT.

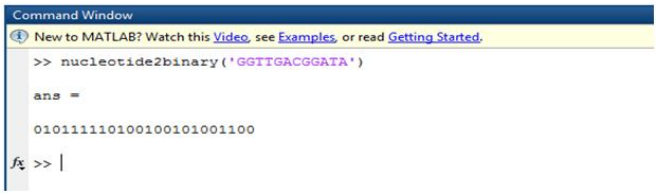

Figure 5.4 – Application of 'nucleotide2binary' command in MATLAB command window (Encryption process)

Figure 5.5 – Encryption process explained

Thus the **encrypted message** (refer Figure 5.3) for the whole binary data can be formed as follows [14] -

CTATTATAGGAA, TTGCTAGTCATG,
AATTTAGTTTTC, CATCTTTTCGAT, TTGCCTCTGAGG,
ATGTAGACCTAG, TAGCTGCTAAGA,
AGATAAAAACAT,
ATAATATTATAA, CTAAAGAGATTC,
CTAACGCTTGGG, TTATTTCGGTTA.

It is known that during the encryption process, the comparison was done from the reverse. So, in the decryption process, the first 12 bits of the encrypted message is compared with the last 12 bits of the OTP key, if they are found to be complementary then a binary '1' is formed. If the complementary matches are not found, it is simply replaced with a zero, '0'.

Thus, the process continues in this manner and the decrypted message is obtained as
010111110100100101001100 □ 95 73 76

The decrypted plain text is (refer figure 5.2) **'GGTTGACGGATA'.**

5.3 Comparison & analysis

The Triple DES algorithm uses three keys. In this method the DES block cipher algorithm is utilized three times to each different block of the input data to obtain the encrypted text. And then the DES block cipher decryption algorithm is applied to the obtained cipher text three times using the same three keys and the original message is obtained. The key size is increased in Triple DES more than that of the DES which makes the algorithm more secured.

In the DNA hybridization method [16], the original message which is referred as plain text is converted in the form of binary. This binary form of data is then compared with the randomly generated OTP key in the DNA form and the encrypted message is obtained. This obtained encrypted message is also in the form of DNA. The decryption message is carried out in reverse using the encrypted data and the OTP key and the original message is retrieved. The comparison between the DNA and Modern Cryptography is presented in tabular form on the basis of various parameters listed in Table 5.1.

Table 5.1- Comparison of DNA cryptography and Modern Cryptography [16]

PARAMETERS	DNA CRYPTOGRAPHY (DNA Hybridisation)	MODERN CRYPTOGRAPHY (Triple DES)
Key size	Large key size depending on the input	Smaller key size when compared to DNA cryptography
Mathematical expressions	Mathematical expressions are totally absent	A lot of mathematical expressions are used
Cryptographic strength	High strength based on the type, size and the randomness of the key	High strength based on the complexity and difficulty of the rounds of operations involved
Computational complexity	High complexity based on the comparison, shifting and the scanning process	High complexity because of the Feistel cipher operation involved in it
Memory	Requires more memory space for storing the lengthy key and performing the operations involving it	Less memory space required compared to the DNA cryptosystems
Cost	High	Less cost than the DNA cryptosystems
Data Length	The data security can be offered for an expansive length of the data	Confidentiality cannot be offered equally to the size of the data as in DNA methods in the same duration as the DNA method takes
Existing period	Believed to withstand any duration of time but yet to be practiced	Still in practice and expectedto last longer

VI. CONCLUSION

Thus, the DNA cryptosystems containing the DNA hybridization technique and the Triple DES approach (Modern cryptosystems) are studied, explained, implemented and the corresponding results are taken from MATLAB. The analysis of all the security parameters related to each method is done and compared and thus, the performance is evaluated.

The OTP method which is known to be perfectly secure, used in the DNA method and Triple DES enables the high confidentiality of the data due to its randomness. The randomness of the operations involved in the encryption and decryption process along with the huge size of the key also adds up to the main purpose of providing high security in the cryptography. From the results and the analysis, the computation time taken by the DNA cryptosystems is very less. Besides, the capability of enabling the security for a large amount of data is possible in DNA systems, which is comparatively higher than the Triple DES algorithm.

Thus, it can be concluded that along with the practice of Triple DES methods, the DNA methods of cryptography can also be included in practice. So with the practical implementations of the DNA cryptosystem, the enhanced ways of attaining the security for an expansive message with less computation time can be possibly be attained and added in the field of cryptography as a new method. Thus, the DNA algorithm is also expected to provide high security when came into existence as the Triple DES algorithm offers high security at present.

VII. ACKNOWLEDGEMENT

Foremost, I would like to express my sincere gratitude to my professor and guide Er. H.P.S Kang, Associate Professor in University Centre of Instrumentation and Microelectronics at Panjab University for his support, motivation, patience, enthusiasm and guidance. His advice was inevitable and with his help I was able to work on my own interested field.

I would like to express my heartfelt gratitude to all my teachers of University Centre of Instrumentation and Microelectronics. I would also like to thank all my lovely friends and classmates who have been there for me always. Last but not least my lovely parents who have been my pillar of strength and support throughout my life. I dedicate this entire life to the Almighty who has guided me, protected me and blessed me abundantly.

Conflicts of Interest: The author declares no conflict of interest.

REFERENCES

[1] L. M. Q. L. &. L. X. Xiao Guozhen, "New Field of Cryptography: DNA cryptography," in *Chinese Science Bulletin*, vol. 51, pp. 1139–1144, China, 2006

[2] L.M.Adleman, "Molecular computation of solution to combinatorial problems," Science in JSTOR, vol. 266, pp. 1021–1025, 1994.

[3] JW Ficket, CS Tung “Assessment of protein coding measures” Nucleic Acid Research, pp 6441-6448, NCBI,1992.

[4] EV Koonin, AS Novozhilov “Origin and evolution of the genetic code: the universal enigma”, IUBMB Life, 2009.

[5] Course Hero: http://www.coursehero.com

[6] J Tugan, A Rushdi (2008) A DSP based approach for finding the codon bias in DNA sequences. IEEE J Signal Process 2: 343–356.

[7] HK Kwan, SB Arniker (2009) “Numerical representation of DNA sequences”. In: IEEE international conference on electro/information technology, EIT ‘09, Windsor, pp 307–310

[8] DG Grandhi, Vijaykumar C (2007) “Simplex mapping for identifying the protein coding regions in DNA”. TENCON-2007, Taiwan.

[9] PD Cristea (2002) “Genetic signal representation and analysis”. In: SPIE information conference biomedical optics, pp 77–84.
[10] M Akhtar, J Epps, E Ambikairajah (2007) “On DNA numerical representations for period-3 based exon prediction”. IEEE workshop on genomic signal processing and statistics (GENSIPS), pp 1–4.
[11] T Holden, R Subramaniam, R Sullivan, Cheng E, Sneider C, G Tremberger, JA Flamholz, DH Leiberman, TD (Cheung 2007) “ATCG nucleotide fluctuation of deinococcusradiodurans radiation genes”. In: Proceedings of society of photo-optical instrumentation engineers (SPIE), pp 1598–1609
[12] Wikipedia : http://en.wikipedia.org/wiki/DES
[13] Ahsan Omer and Muhammad Imran Farooq “DNA Cryptography Algorithms and Applications”, Research gate, pp 1-17, 2015.
[14] O. T. T. H. M. E. Borda, "Secret Writing by DNA Hybridization",IEEE conferences 2010.
[15] Ashish Gehani, Thomas H. LaBean and John H. Reif “DNA-based Cryptography” 5th Annual DIMACS Meeting on DNA Based Computers(DNA 5), MIT, Cambridge, MA, June 1999.
[16] “Comparison and performance evaluation of cryptographies”, Angeline Thiruthuvadoss,KTH publications, pp 9-60, 2013.
[17] Wikipedia : http://en.wikipedia.org/wiki/MATLAB
[18] National Center for Biotechnology Information : www.ncbi.nlm.nih.gov.