Comparison of DNA Cryptography and Modern Cryptography using Cipher Text

Saurabh Kumar, H.P.S. Kang
University Centre of Instrumentation and Microelectronics
Panjab University, Chandigarh, India

Abstract

DNA is used as an information carrier and advanced biological technology tool. It carries style data between generations, and therefore accounts for hereditary biological behavior. DNA can be used for storing and transmitting the information in cryptography field. 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.

1. Introduction

From the ancient days till present, the secret writing techniques are practiced safeguarding the data from the adversaries. Among these techniques, cryptography and steganography are the most common and widely used methods. Cryptography does the role of encrypting the data whereas steganography is used to hide the data from the hackers. 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 [19] 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 is executed using bioinformatics toolbox in MATLAB.

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 (so first, digitizing of DNA is done), then, the results are compared and analyzed. It is done to find out in what aspects the security is improved in the DNA method compared to the other existing modern methods.

2. Theory

Cryptography is the science of encrypting and decrypting the data so as to keep the data more secured. It is capable of keeping the data in secret while saving the information or passing it over the unsafe networks, like internet [1]. This is done in order to safeguard the data from the hackers and make it understandable only to the intended receiver (see Figure 1).

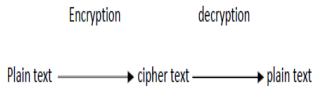

Figure 1. Flow Diagram of Cryptography

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

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

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

Decryption: Decryption is the reverse process of encryption. The original message or the plain text is obtained as a result of this process.

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

Copyright © 2018, Infonomics Society

2.1. Types of Cryptographic Functions

The cryptographic functions are classified mainly into two kinds as mentioned below:

- Secret key function
- 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 by using a single key. The unintelligible data produced as a result of encryption is of the same length as the plain text. Decryption is the reverse process of obtaining the plain text by using the same key used in the encryption process. The process is represented in the form of flow diagram in the Figure 2.

Secret key cryptography can also be referred as conventional cryptography or symmetric cryptography [18]. The captain midnight code and mono alphabetic cipher are the best examples of this type of cryptography, though they are easy to break.

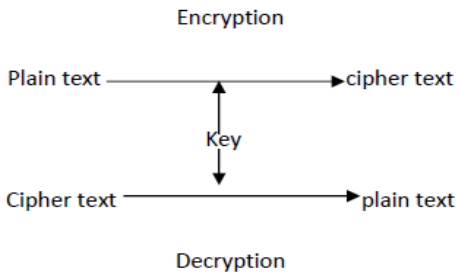

Figure 2. Flow diagrams for secret key cryptography

2.1.2. Public Key Cryptography. Public key cryptography is a recently found technique in 1975. It can be also referred as asymmetric cryptography. Unlike secret key cryptography, public key cryptography uses two keys. Instead, each individual has two keys: a private key which is to be kept much confidential and a public key that is possibly identifiable by everyone in the world.

At times a single letter is also used to represent the used keys. But unfortunately, both the words public and private start with p. Thus, the letter p will not work. So, in the aim of avoiding the confusion the letter e will be used to refer the public key, since public key [18] is used to encrypt a message. And the letter d will be used to refer the private key, since the private key is involved in decrypting a message. Encryption and decryption are inverse, mathematical, and opposite functions to each other. The flow diagram of the public key cryptography is illustrated below in the Figure 3.

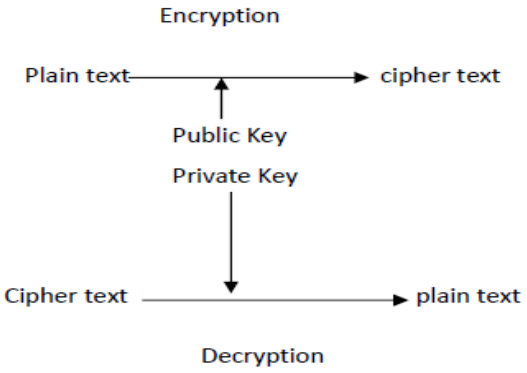

Figure 3. Flow diagram for public key cryptography

In addition, with public technology, 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. In addition, the public key signature differs from the secret key MAC (Message Authentication Code) [18]. It is because MAC verification needs the knowledge of the secret key used to generate it. And hence, a person who has the knowledge of verifying a MAC can also generate one and will be able to substitute many messages and the respective MAC.

Conversely, the verification of the signature requires the knowledge of the public key alone. And so a person (Alice) can generate a signature for a message which is unalterable by others. But others could only verify, identify and remember that the signature is of the corresponding person (Alice). Hence, it is known as signature because it shares the same property of the handwritten signature. In which the signature is identifiable or recognizable that it is of the authentic person (Alice) and unforgettable.

2.2. Biological Background

DNA (deoxyribonucleic acid) is hereditary in humans which stores the information as a code made of four chemical base: 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 and a phosphate molecule, which are arranged in two strands and form a spiral called a double helix, together are called 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 4 shows a section of the DNA sequence.

Copyright © 2018, Infonomics Society

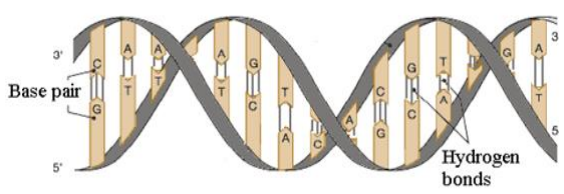

Figure 4. DNA structure

Proteins are 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’’ (see Figure 5).

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 5. Amino acids (Symbols and Codons)

Each codon is comprised from three nucleotides, where the codon corresponds to a single amino acid. 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. There is not another codon encoding methionine. There are three different codons indicating the end of protein synthesis. These are UAA, UAG and UGA. This is called the stop codons. During the production of proteins and enzymes, RNA copy sequences that corresponding to genes in DNA are extracted [4, 6, 9–11].

2.3. DES Algorithm

The DES algorithm is the Data Encryption Standard Algorithm [12] and it is a block cipher. The plain text message is divided into 64-bit blocks (see Figure 6). And each 64-bit block of the original message is initially permuted, and the bits are divided into right and left blocks. These left and right block bits are then undergone a Feistel function, F using the key K1 and an XOR operation and the output obtained from each of the blocks goes as an input to the next opposite blocks.

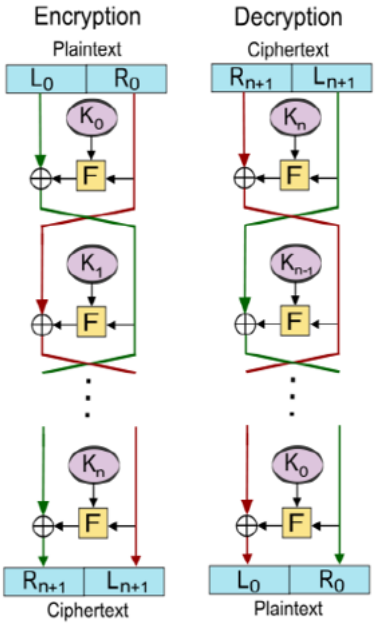

Figure 6. Illustration of DES Algorithm

2.4. 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. In this literature, the single stranded DNA sequences are represented as ssDNA and the double stranded or helical form of the DNA sequences are represented as dsDNA. A single unique ssDNA under specific situations can combine with other matching or complementary ssDNA to form the double stranded [17] DNA helix form dsDNA. The process of forming dsDNA is illustrated in the Figure 7. Since the ssDNA from distinct sources which are considered to be hybrids, join together to form

Copyright © 2018, Infonomics Society

molecules of double strands. This process is termed as hybridization.

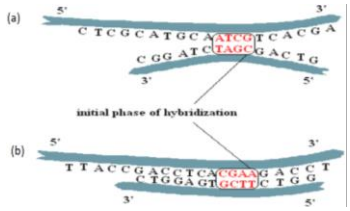

Figure 7. Hybridization process

2.4.1. 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 (see Figure 7).

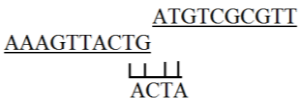

Figure 7. Binding process between two segments

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*. The distinct number of possible primers is 4^{20}, indicating the order of the brute force attack in this case.

3. Literature Review

Unlike using the conventional electronic means to encode data, Chen [13] proposed a novel design of DNA-based, Molecular Cryptography design in his paper. Due to the random nature of DNA, he made use of cryptography in principle unbreakable. Carbon nanotube-based message transformation and DNA based cryptosystem were proposed.

Kang and Ning [14] introduced a new cryptography method based on central dogma of molecular biology. Since this method simulates some critical processes in central dogma, it is a pseudo-DNA cryptography method. The theoretical analysis and experiments showed this method to be efficient in computation, storage and transmission; and it is very powerful against certain attacks. Thus, this method can be of many uses in cryptography, such as an enhancement insecurity and speed to the other cryptography methods. There are also extensions and variations to this method, which may have enhanced security, effectiveness, and applicability.

Ochani [15] proposed the solution to transmit a DNA image. Cryptography along with steganography are two popular methods available to impose security do DNA images. He used modified symmetric key {MSK} encryption with LSB steganography technique for security and performance concern of the existing.

Ahsan Omer and Muhammad Imran Farooq [16] presented the use of DNA computing in cryptography for secure communications. There are now several algorithms for DNA cryptography. The discussed algorithm uses One Time Pad encryption scheme. One time pad key is obtained using DNA bases. DNA lookup table has also been used for increasing the security of cipher text. The implementation is done on Matlab and is working as expected.

Monica Borda [17] 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 [18] 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.

From this paper [1] by Xiao et al., the knowledge of oligonucleotide sequencing using the Hamilton path model and segregation of the sequences with the sticker's method was understood. The Hamilton tracing method is proposed in DNA cryptography to trace out the primer sequences involved in limiting the length of the OTP key used in DNA security. And the primers are identified by solving the Hamilton weights and path involving the mathematical calculations. The paper says that the investigation problem of DNA cryptography still in existence and the progress is still in the beginning stage. Still then, the exclusive data storing capabilities in the DNA molecules, unique efficient energy and the wide analogous computations are the special merits in this field of cryptography.

4. The Software

MATLAB (*matrix laboratory*) is a multi-paradigm numerical computing environment and proprietary programming language developed by

Copyright © 2018, Infonomics Society

MathWorks [20]. 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. The various inbuilt functions listed in section 4.2 are used to form two new functions to digitize the DNA data into binary and vice versa – nucleotide2binary and binary2nucleotide.

4.1. 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. The various inbuilt functions in MATLAB [20] used

The 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.

ismember	Returns an array containing 1 (true when element of array A is found in array B) or 0 (false).
cell2mat	Convert cell array to numeric array
logical	Convert numeric values to logical
xor	Logical exclusive-OR (see Figure 8)
nt2aa	Convert nucleotide sequence to amino acid sequence
aa2nt	Convert amino acid sequence to nucleotide sequence
dna2rna	Convert DNA sequence to RNA sequence
rna2dna	Convert RNA sequence to DNA sequence
seqcomplement	Calculate complementary strand of nucleotide sequence

A	B	C
Zero	Zero	0
Zero	Nonzero	1
Nonzero	Zero	1
Nonzero	Nonzero	0

Figure 8. Truth table of "xor" in MATLAB

5. Proposed Methodology

5.1. 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 (see Figure 9).

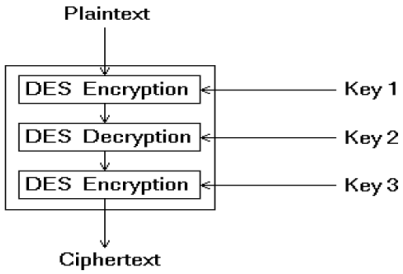

Figure 9. Triple DES block diagram

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 (see Figure 10):

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

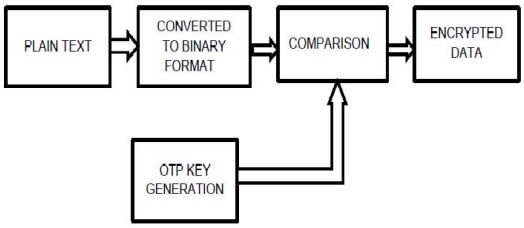

Figure 10. Block Diagram for Encryption Process

5.1. Algorithm for Encryption

Step-1: The plain text (i.e. A, T, G and C) is converted into binary code using function nucleotide2binary in MATLAB. 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 ASCII code of size (perform 8-bit division of bytes) depending upon the size of obtained step 1 binary is generated.

Copyright © 2018, Infonomics Society

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.

5.2. Algorithm for Decryption

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 (see Figure 11).

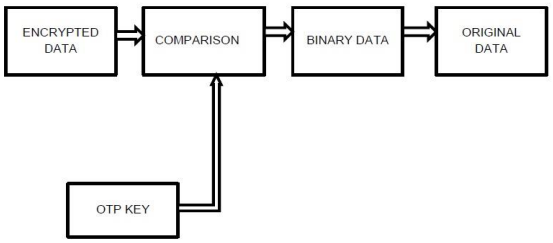

Figure 11. Block Diagram for Decryption Process

Step-5: Binary code of decrypted message is converted into DNA base equivalent by using function binary2nucleotide. And finally, the result in form of A, T, G, C is obtained by the receiver.

5.3. DNA Hybridization

In the DNA hybridization technique [17], 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.

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 [21] of species 'Clostridium botulinum' (Locus or Accession No. YP_009069373) is represented as follows –

```
ATGATTAACATAATAGAAGATAAAAGCATTCTGAT
CAATAAAGCCAATGATTGCGAACCAAGCGCGAAAT
CATTCTAAAGGACGATTTCTCTAAGAAGAGAAAAC
AGTATTATAATATGTTAAATTAAAGGAAGACTGCA
AGTCTATTTTTGTAAAGGGCGAGTACGTGATCGAA
ATATCGACGATTCTAATTATATTAAATACATCTGG
ATCAACGGAGACTCCGTAGAAAAGCTATTAAATCA
AAAGAACGATCAGTACCGTCTCCTTATAGATAATA
TCCTTGGGAATAAGCTT
```

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

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.

6. Results and Discussion

6.1. 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 (see Figure 12).

Private Key K → 148 216 211

Copyright © 2018, Infonomics Society

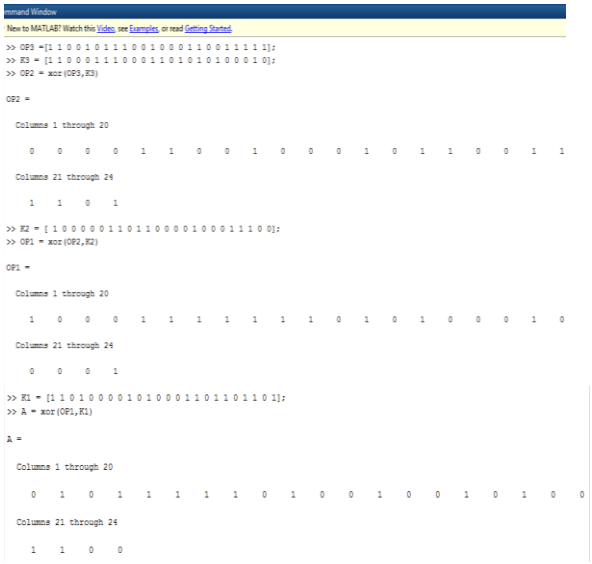

Figure 12. Application of 'xor' in MATLAB command window (Decryption process using Secret Key Cryptography method)

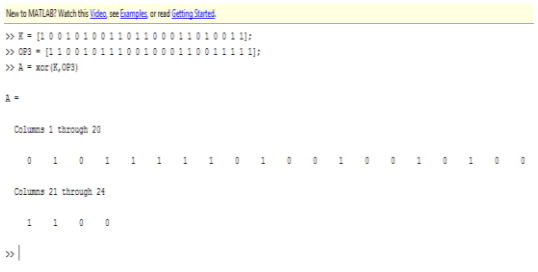

Figure 13. Application of 'xor' in MATLAB command window (Decryption process using Public Key Cryptography method)

The decrypted message (A) – 95 73 76

6.2. Discussion of Results

The Encryption and Decryption using "XOR approach" and Triple DES Algorithm used above can be of two types:

- Secret Key Type Cryptography
- Public Key Type Cryptography

Triple DES Algorithm uses 3 keys K1, K2 and K3 applied sequentially for Encryption along with "XOR approach" to transmit data to the receiver end. Then for the case of Secret Key Cryptography while Decryption, all the 3 keys are used in opposite way as that of Encryption i.e. K3, K2 and then K1 sequentially to retrieve the data back using XOR (see Figure 13).

For the case of Public key Cryptography while Decryption, 3 keys are not required to be applied either only one key called "Private Key" is applied to retrieve data back using XOR (see Figure 13). Clearly Public Key Cryptography is a fast method of retrieving encrypted data whereas Secret key cryptography 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. In addition, the public key signature differs from the secret key MAC (Message Authentication Code). It is because MAC verification needs the knowledge of the secret key used to generate it. And hence, a person who has the knowledge of verifying a MAC can also generate one and will be able to substitute many messages and the respective MAC. Conversely, the verification of the signature requires the knowledge of the public key alone.

6.3. 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 (see Figure 14).

The binary digits are compared with the DNA data in reverse order and the message is encrypted. The generated binary data: 0101111101001001010 01100. The randomly [21] 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 14. Encryption Process

Thus, the encrypted message for the whole binary data can be formed as follows [17]:

```
CTATTATAGGAA, TTGCTAGTCATG,
AATTTAGTTTTC, CATCTTTTCGAT,
TTGCCTCTGAGG, ATGTAGACCTAG,
TAGCTGCTAAGA, AGATAAAAACAT,
```

Copyright © 2018, Infonomics Society

```
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 0101111101 00100101001100 → 95 73 76.

6.4. Comparison and 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 (see Table 1).

In the DNA hybridization method [19], 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.

Table 1. Comparison of DNA and Modern Cryptography

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	Many 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 expected to last longer

7. 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 [19]. 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

Copyright © 2018, Infonomics Society

high security when came into existence as the Triple DES algorithm offers high security at present.

8. 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.

Abbreviations:

A : Adenine
G : Guanine
C : Cytosine
T : Thymine
U : Uracil
RNA : Ribo Nucleic Acid
DNA : Deoxy Ribonucleic Acid
OTP : One – Time Pad
DES : Data Encryption Standard

9. References

[1] Xiao, G., Lu, M., Qin, L. et al., (2006). New field of cryptography: DNA cryptography. Chinese Science Bulletin, China. 51, 1413–1420. https://doi.org/10.1007/s11434-006-2012-5.

[2] Adleman, L.M., (1994). Molecular computation of solutions to combinatorial problems. Science, Vol. 266, Issue 5187, pp. 1021-1024. DOI:10.1126/science.7973651. https://science.sciencemag.org/content/266/5187/1021.abstract (Access date: 1 November 2018).

[3] Fickett, J.W., Tung, C.S., (1992). Assessment of protein coding measures, Nucleic Acids Research, Volume 20, Issue 24, 25 December, Pages 6441–6450, https://doi.org/10.1093/nar/20.24.6441.

[4] Koonin, E. V., and Novozhilov, A. S., (2009). Origin and evolution of the genetic code: the universal enigma. IUBMB life, 61(2), 99–111.https://doi.org/10.1002/iub.146.

[5] CourseHero, Cryptography. http://www.coursehero.com, (Access date: 2 January 2018).

[6] Tuqan, J., and Rushdi, A., (2008). A DSP Approach for Finding the Codon Bias in DNA Sequences. IEEE Journal of Selected Topics in Signal Processing, 2, 343-356.

[7] Kwan, H. K., and Arniker, S. B., (2009). Numerical representation of DNA sequences, IEEE International Conference on Electro/Information Technology, Windsor, ON, Canada, 2009, pp. 307-310, doi:10.1109/EIT.2009.5189632.

[8] Grandhi, D.G., and Chakka, V.K. (2007). 2-Simplex mapping for identifying the protein coding regions in DNA. TENCON 2007. IEEE Region 10 Conference, 1-3.

[9] Cristea, P. D., (2002). Genetic signal representation and analysis, Proc. SPIE 4623, Functional Monitoring and Drug-Tissue Interaction, https://doi.org/10.1117/12.491244.

[10] Akhtar, M., Epps, J., and Ambikairajah, E., (2007). On DNA Numerical Representations for Period-3 Based Exon Prediction, IEEE International Workshop on Genomic Signal Processing and Statistics, Tuusula, Finland, 2007, pp. 1-4, doi: 10.1109/GENSIPS.2007.4365821.

[11] Holden, T., Subramaniam, R, Sullivan, R., Cheung, E., Schneider, C., Tremberger Jr., G., Flamholz, A., Lieberman, D. H. and Cheung, T. D., (2007). ATCG nucleotide fluctuation of Deinococcus radiodurans radiation genes, Proc. SPIE 6694, Instruments, Methods, and Missions for Astrobiology X, 669417; https://doi.org/10.1117/12.732283

[12] Wikipedia, Data Encryption Standard, http://en.wikipedia.org/wiki/DES. (Access date: 14 February, 2018).

[13] Chen, J., (2003). "A DNA-based, biomolecular cryptography design," Proceedings of the 2003 International Symposium on Circuits and Systems. ISCAS '03., Bangkok, Thailand, 2003, pp. III-III, doi: 10.1109/ISCAS.2003.1205146.

[14] Ning, K., (2009). A Pseudo DNA Cryptography Method.https://arxiv.org/abs/0903.2693. (Access dat e: 25 June, 2018).

[15] Ochani, A., Jadhav, D., Gulwani, R., (2016). "DNA image encryption using Modified Symmetric Key (MSK)," 2016 International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India, pp. 1-4, doi:10.1109/INVENTIVE.2016.7823276.

[16] Omer, A., Farooq, M.I., (2015). DNA Cryptography Algorithms and Applications. https://docplayer.net/49007186-Dna-cryptography-algorithms-and-applications.html. (Access date: 2 May, 2018).

[17] Borda, M., Hodorogea, O.T.T., (2009). Secret Writing by DNA Hybridization.

[18] Gehani A., LaBean T., Reif J., (2003). DNA-based Cryptography. In: Jonoska N., Păun G., Rozenberg G. (eds) Aspects of Molecular Computing. Lecture Notes in Computer Science, vol 2950. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-24635-0_12.

Copyright © 2018, Infonomics Society

[19] Thiruthuvadoss, A.P., (2013). Comparison and Performance Evaluation of Modern Cryptography and DNA Cryptography.

[20] Mathworks, (2018). MATLAB for Artificial Intelligen ce www.mathworks.com, (Access date: 3 April, 2019).

[21] National Center for Biotechnology Information Search database (NCBI), www.ncbi.nlm.nih.gov. (Access date: 12 June 2018).

Copyright © 2018, Infonomics Society