© A Publication of the Centre for Research and Development (CERAD), The Federal University of Technology, Akure, Nigeria (www.jost.futa.edu.ng)

JOST 2021

Enhanced Cryptographic System Using Caesar Cipher and Deoxyribonucleic Acid (DNA) Sequences

Akintola A. Ganiyat[1], Aro T. Oladele[2], Daniel A. Olorunleke[1] and Salihu S. Aderonke[1]

[1]*Department of Computer Science, University of Ilorin, Ilorin, Nigeria*

[2]*Department of Mathematical and Computing Sciences, Kola Daisi University, Ibadan, Nigeria*

Corresponding Author: Aro, T.O.: taiwo774@gmail.com

ABSTRACT: Information security encompasses the protection of digital privacy strategies which are used to stop illegal access to information, records and computing devices. This paper applied an algorithm based on Caesar Cipher and DNA Sequences. In the proposed system, a method of generating DNA Sequences with keys to secure data with encryption and decryption methods were implemented. The algorithm utilized large hidden keys values during the encryption process for shifting in the Caesar Cipher algorithm and DNA sequencing applied the uniqueness of DNA characteristics. The system achieved effective level security for data compared to existing algorithms as the Cryptanalysis of the Caesar Cipher decrypted texts with Chi-Squared values around 150. The enhanced Caesar Cipher with DNA Sequences decrypted texts with Chi-Squared values far above 150 which showed that the system is less vulnerable to hackers and unauthorized access.

Keywords: Cipher, Cryptography, Deoxyribonucleic acid, Sequences

JoST. 2021. 11(1): 1-12

Accepted for Publication, March 16, 2020

INTRODUCTION

Information security provides confidentiality, data integrity, authentication and non-repudiation services (Karimi, 2017; Das, Sarma, & Deka, 2019). The sensitive information protection against unauthorized access or fraudulent changes has been of prime concern throughout the countries (Najaftorkaman & Kazazi, 2015). There are many techniques used to transforming information (text in plain format) into an unreadable format (text in cypher format) (Al-mahdi, Shahin, Fouad, & Alkhaldi, 2018). Cryptography is one of such techniques which information is hidden by a secret key with a specific algorithm (Bhanot & Hans, 2015). Cryptography can be traced since its existence use by the Egyptians some 4000 years ago (Mavanai, Pal, Pandey & Nadar, 2019), to the twentieth century, where it had performed a very significant function in the outcomes of the world war one and two. Consider scenarios in the past by which a sender who sent a message through courier would want to make sure that if the carrier of the message were cut off, the interceptors could not read the message.

With the enormous data being shared on the electronic networks, there is need to develop more effective technique of encryption to protect highly secretive information, such as credit card numbers and communications (Ruhan, Malarvizhi & Patel, 2016). The cryptography protects users by allowing functionality for the encryption of data and authentication of several users (Kumari, 2017). Cryptography in data security offers three essence areas that protect data from attempt break-ins, theft or any unauthorized use of stored data and possible fraudulent activity. Cryptography protects these extremely important areas, authentication, integrity, and confidentiality (Xiang, Tao., Wong & Liao, 2007). The Caesar cipher also referred to as shift cipher, (Caesar's cipher or Caesar shift), which employs a replacement approach to derive the text that is encrypted (Sailakshimi, & Sasikala, 2015). It is one of the earliest known

cryptographic systems which was first used by Julius Caeser 50 BC (Lin & Tong, 2018).

The disadvantage of Caesar cipher is that it can be broken easily, even in cipher-text situation only. Several techniques have been discovered to crack text in cipher from the application of frequency analysis and pattern words. One of the methods is using brute force to pair the distribution of the letters of frequency. This is possible because they are only limited numbers of possible shifts; 26 in English (Jain, Dedhia & Patil, 2015). Also, the techniques of DNA sequence can be used to enhance the Caesar Cipher algorithm for stronger encryption and make it more difficult to decrypt. Caesar cipher is the simplest method of cryptography that could be quite easily decoded by a hacker because of its simplicity and size of encryption (Purnama & Rohayani, 2015). However, Caeser Cipher can be enhanced with DNA sequences to further strengthen data or information security.

The nucleotides are specific molecules which create DNA. The only four nucleotides that are being in use are Adenine (A), Thymidine (T), Guanine (G), and Cytosine (C) (Soni, Soni, Sandeep & Mathariya, 2012). Strand of a DNA is considerably comparable to exceedingly lengthy sentence that employs only four letters. DNA has two strands like a zipper and the nucleotides. The two-strand is the key to how DNA can replicate itself. It could certainly occur because one strand is a complement to another strand. A continuously pair up with T and G constantly pair up with C. For the reason, it is called base pairs. The work by (Dubey, Saxena & Gond, 2015) gave an idea in understanding the ideologies and some methods of the new innovative steganography and cryptography through DNA. From studies, most approaches based on Caeser Cipher are either single shift or double shifts (Enas, Imran, & Farah, 2014), but the problem of easy decryption still lingers. Enhanced approaches are needed to better secure data by doing multiple shifting and transformation of Cipher text using another Cryptographic mechanism (Balogun, Sadiku & Mojeed, 2017).

This paper came up with an improved approach of information security for cryptographic system using the combination of Caesar cipher and deoxyribonucleic acid sequences

RELATED WORK

Dixit, Trivedi, Gupta, Yadav and Singh, (2019) presented a metamorphic cryptography Deoxyribonucleic Acid (DNA) based cryptography to achieve cryptographic strength. Plaintext message which contained sensitive information was converted into its corresponding ASCII values. The ASCII values obtained then changed into corresponding binary values. Also, the study applied a binary index compression technique to reduce data up to 50% which improved payload capacity. The output of the steps was converted into sequences of DNA nucleotides. Concept of steganography is implemented with the help of LSB algorithm. The proposed metamorphic algorithm is secure as it utilizes the concept of DNA, have higher payload capacity as it uses binary index compression technique and simple to implement as the LSB algorithm is used for hiding purposes.

Al-Mahdi, Shahin, Fouad and Alkhaldi, (2018) used asymmetric DNA binary cryptography algorithm to encrypt and decrypt plaintext information. The study introduced a mathematical algorithm to generate a strong secret key from the DNA of different multiple living creatures. The encryption process was implemented using another 16 keys which randomly produced from the secret key. The efficiency and confidence of the proposed algorithm were evaluated based on encryption and decryption time, avalanche effect and the resistance of the secret key against the attack.

Fernandez, Juan, Adrian, Silva and Terren (2018) designed a DNA binary cryptography that was symmetric, which performed encryption and decryption on the information in plain text. The significance of the study was of two folds: First, an algorithm in mathematical form was introduced to produce more secured secret key employing the DNA of diverse many living creatures. At phase two, the encryption process was implemented with another 16 keys which were generated randomly from the secret

key. The effectiveness of the developed system was evaluated in terms of the time of encryption or decryption, avalanche effect and the resistance of the secret key against the attack.

Balogun et al. (2017) developed a new enhanced model of Caesar cipher for improved security using multiple encryption techniques, whereby an already-encrypted message was encrypted one or more times using the same or different algorithm. The new model worked by wrapping a plaintext message in three crypto wrappers and each encryption/decryption phase used a different shift key from the other. The model supports both uppercase and lowercase characters. However, the model did not encrypt/decrypt numbers, special characters, whitespace, and file types such as word document, binary, or pdf files, but only text files. Most importantly, the new enhanced model can provide improved security of message by encrypting a plaintext message three times; in this way, brute-forcing or an exhaustive key search will be difficult to perform; thus, making cryptanalysis almost a mirage.

Ruhan Malarvizhi and Patel (2016) proposed a novel system based on cryptography of DNA, which enhanced the data security aspects being transferred across a network. The study introduced a Feistel inspired structure and adding complex operations to it. One Time Pad was applied for key production, which provided distinct key each time by application of a random function. It made the system difficult and also to prevent the attackers to achieve any brute force attacks. The results showed that the integrity and confidentiality of the data were maintained and the Feistel inspired structure for DNA cryptography using a one-time pad for the generation of a key to produce an efficient encryption rate.

Jain, Dedhia and Patil (2015) improved Caesar algorithm to conquer some of the drawbacks and downsides of Caesar cipher. For replacement, a randomized method was used, which was combined with double columnar transposition method to maximize the strength. Cryptanalysis was performed on the algorithm being modified, it was challenging to break using frequency analysis. Heuristically, it is not an easy task to crack the algorithm by brute force technique since the attacker needs to attempt a complete of key length raised to 256 diverse key combinations. The algorithm provided security which was limited by using an encryption algorithm and symmetric key approach instead of an asymmetric key.

Sailakshimi and Sasikala (2015) develop a procedure to improve Caesar cipher with the generation of random number method for key generation methods. The authors include classical cipher with modern cipher properties; encryption which was achieved by applying columnar transposition with arbitrary random order column selection. The proposed approach was a mixed method of classical and modern cipher properties. The procedure gave an enhanced Security with high throughput and occupied minimum memory space.

Omolara, Oludare and Abdulahi, (2014) proposed a hybridized technique by the combination of Caesar cipher and Vigenere cipher to amplify the diffusion and confusion characteristics of cipher text, the study used methods from current ciphers such as xoring key to the first letter of plain text, xoring first letter of the plain text to second letter and so on. The limitation of the research work was that it used less key values for shifting in Caesar Cipher algorithm.

Imran and Abdulkareem, (2014) presented an enhanced method for Caesar cipher which uses modulo 26 with a fixed key and scrambles its characters for difficult cryptanalysis purpose. Also, the key formulation is based on various methods such as the address of the message, the length of the first word, and the number of words in the first line.

Goyal and Kinger (2013) performed changes to old Caesar cipher where the key size was kept fixed as one, it was difficult to break by using cryptanalysis. While the substitution was checked by the index of the alphabet, if the index was even then the key is increased value by one, else if the index was odd then the key-value was decreased by one. The weakness of the method was that it used less key values for shifting in the Caesar Cipher algorithm.

From the review of related literatures, the limitation of the studies stated is the use of low

key values for shifting in their respective algorithms with major emphasis on the Caesar Cipher Algorithm, which this study has attempted to resolve by a Cryptography of the existing Caesar Cipher algorithm with DNA sequences which is largely a new concept that will further strengthen data security when compared with the related works reviewed.

METHODOLOGY

In this study cipher text from Caesar cipher was used as an input in bioinformatics algorithm Decryption and encryption bio-informatics techniques were based on properties of DNA such as replication, translation and transcription. A DNA was applied to generate a new key scheme. The encrypted text characters were scrambled in such a way that if an attempt is made to decrypt the cipher text it would be difficult or impossible to achieve. The block diagram of the enhanced Caeser cipher with DNA sequence system is shown in Figure 1.

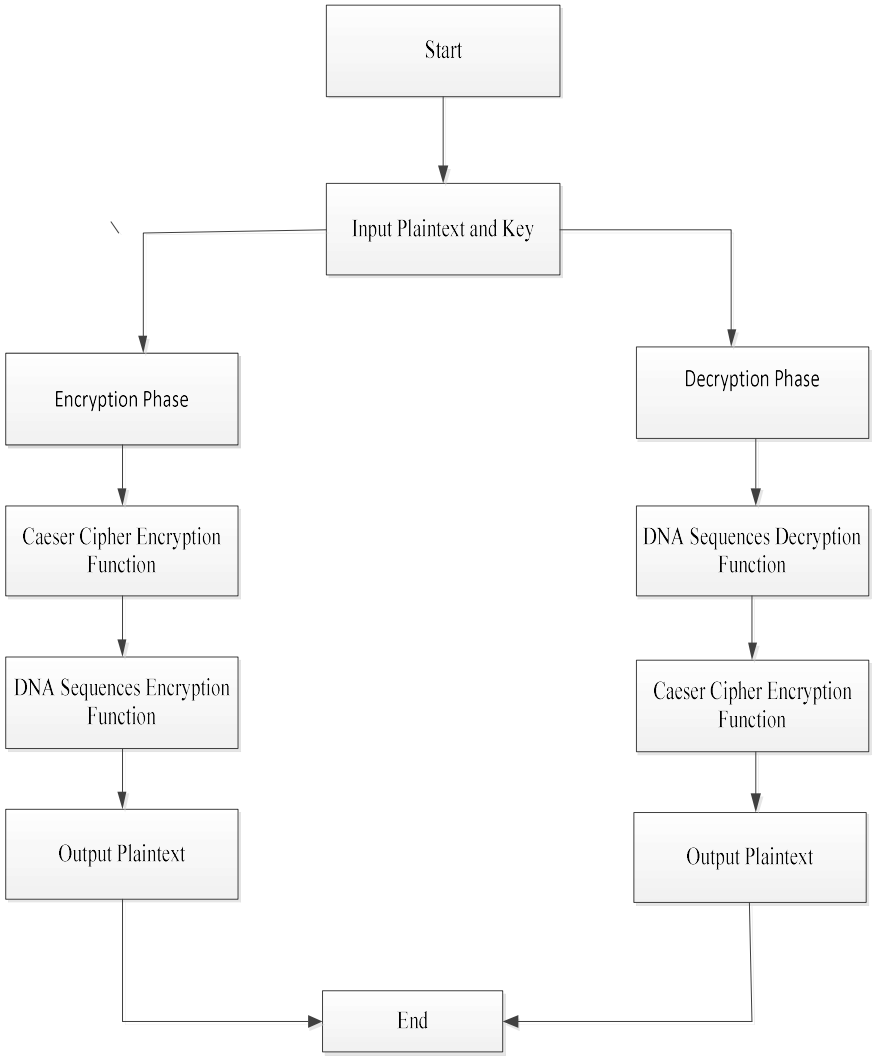

Figure 1: Enhanced Caser Cipher with DNA Sequence

Enhanced Caeser Cipher System Approach

The enhanced Caeser cipher developed entails different stepwise algorithms, this is described in the following subsections:

Caesar Cipher Encryption Algorithm

Step 1: Input the plaintext
Step 2: Input the integer value for the key
Step 3: Change the alphabet into the number that goes with its order in the alphabet initial from 0, and label this numeral X (A=0, B1, C=2, …., Y=24, Z=25)
Step 4: If key >0 then shift forward by key value
Step 5: Calculate: Y = (X + Key) mod 26
Step 6: If key<0 then shift backward by key value
Step 7: Calculate: Y = (X + (-key)) mod 26
Step 8: Print outs the calculation Y

Bioinformatics Encryption Algorithm

Step 1: Convert input data into binary
Step 2: Binary data into A, T, G AND C letters
Step 3: Key-value from server
Step 4: Apply complementary rules step 2 and 3
Step 5: Apply XOR operation between the output from step 4
Step 6: Convert output from step 5 into the DNA sequence
Step 7: Convert DNA sequence into ASCII Values
Step 8: Convert into Binary format (cipher data)

Caesar Cipher Decryption Algorithms

Step 1: Take the cipher text
Step 2: Take the key for integer value
Step 3: Change the num into the alphabet that goes with its order in the alphabet initial from 0, and label this numeral X (0=A, 1B, 2=C, …., 24=Y, 25=Z)
Step 4: If key <0 then shift forward by key value
Step 5: Calculate: Q = (-X + Key) mod 26
Step 6: If key<0 then shift backward by key value
Step 7: Calculate: Q = (-X + key) mod 26
Step 8: Printouts the calculation Q

Bioinformatics Algorithm

Step 1: Convert cipher data (binary format) into ASCII value of DNA sequence
Step2: Convert DNA sequence (output) from step 1 into Binary sequence
Step 3: Convert binary into a DNA sequence
Step 4: Key-value from server
Step 5: Apply a complementary rule for step 3 and 4
Step 6: XOR operation between step 3 and step 4 after step 5
Step 7: original binary format after step 6

In the binary format, 0 complement is 1 and 1 complement is 0. Hence 00 and 11 are a complement to each. 01 and 10 also complement. Here A is 00, T is 11, G is 01, C is 10 and ASCII value of G is 71, C is 67, A is 65, T is 84.

Cryptanalysis of the Caesar Cipher and Enhanced Caeser Cipher with DNA Sequences

The Cryptanalysis process for this study used Chi-Squared formula to locate algorithm vulnerabilities and break them into cryptography systems. The Caesar Cipher and enhanced Caesar cipher with DNA sequence are cracked with different unique keys so that all of them can be tested and scored to measure closeness to the English words or texts by using Chi-Squared.

Chi-Squared Statistic

It is a measure of the differential degree of two categorical distributions as presented in Equation (1)

$$x^2 = \sum \frac{(O-E)^2}{E} \quad (1)$$

x^2 = Chi Squared obtained
Σ = Sum of observed and expected score
O = Observed score
E = Expected score

Replication and Transcription Processes

The summary of DNA Sequences Structure detailing its Replication and Transcription processes is shown in Table 1.

Table 1: Replication and Transcription Processes

Complementary Bases	
Replication	*Transcription*
DNA -> DNA	DNA -> RNA
A -> T	A -> U
T -> A	T -> A
C -> G	C -> G
G -> C	G -> C

A = Adenine, C = Cytosine, G = Guanine, T = Thymine, U = Uracil

RESULTS AND DISCUSSION

Developed Enhanced Caser Cipher System Interface

The interface of the enhanced system is shown in Figure 2, where the plain text and key are entered for the Caesar Cipher Encryption

Result of Cryptographic System for decrypting the enhanced Ceasar Cipher Encryption

Figure 3 shows the Cryptographic System Decryption of the results obtained.

Result of Cryptographic for decrypting the enhanced Ceasar Cipher Encryption

The Cryptographic System for decrypting the enhanced Ceasar Cipher Encryption is shown in Figure 4.

Evaluation of the Developed and Existing Algorithms

The enhanced Caesar cipher with DNA Sequence algorithm was evaluated and compared as shown in Tables 2, 3 and 4. The relevant analysis is presented for each of the examined algorithms, the analysis was obtained by practically decrypting ciphertext with different keys to identify decrypted cipher texts that are similar to English words or statements. From the Cryptanalysis of the Caesar Cipher with only decrypted texts shown in Table 3, it can be deduced from the low Chi-Squared values obtained (around 150) that using only Caesar for securing data/information is an effort in futility as it can be easily hacked or accessed by unauthorized users.

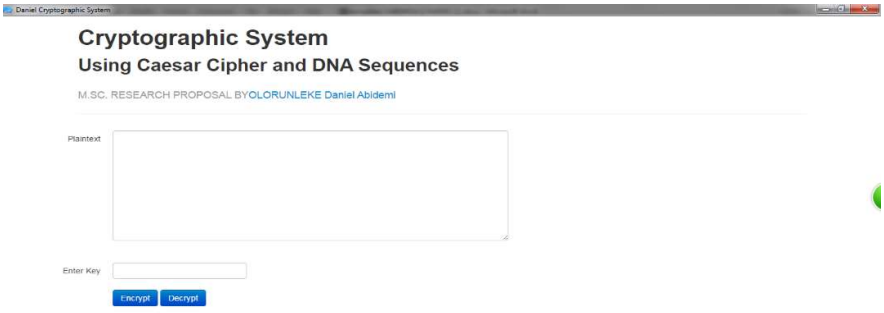

Figure 2: Cryptographic System Interface

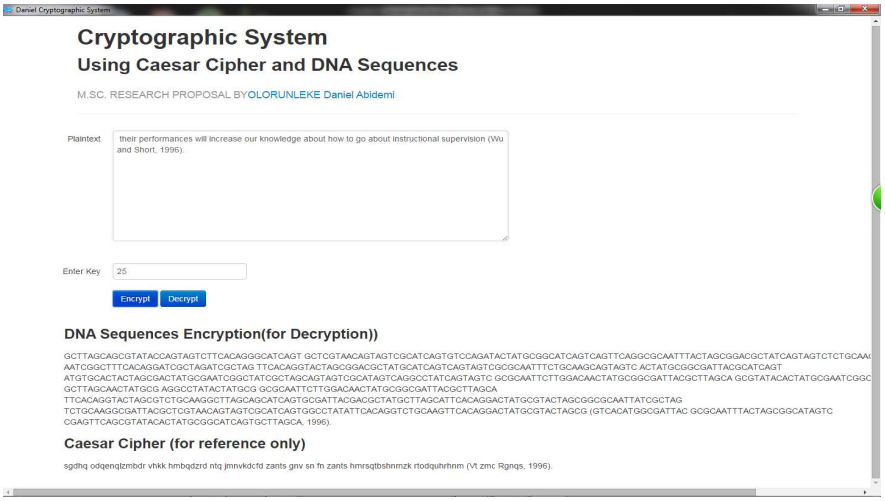

Figure 3: Interface for Cryptographic System Decryption

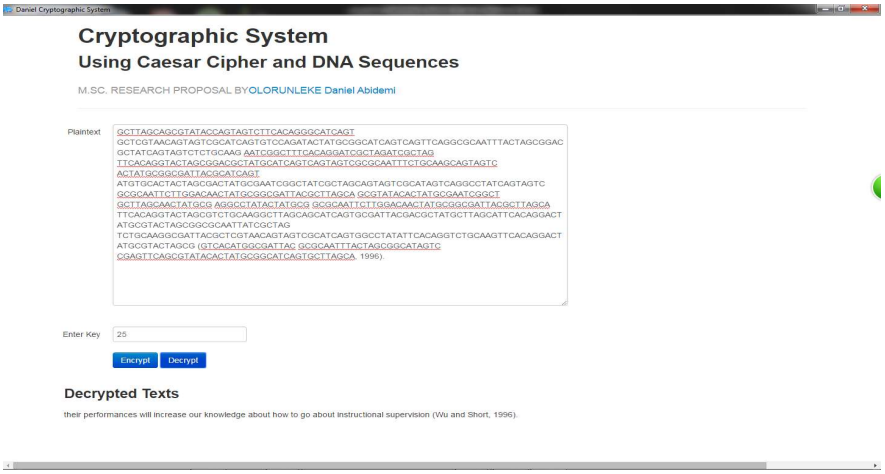

Figure 4: Interface for Cryptographic for decrypting the enhanced Ceasar Cipher Encryption

Table 2: Relative Frequency of the First Letter of an English word

A=11.682%	B=4.434%	C=5.238%	D=3.174%
E=2.799%	F=4.027%	G=1.642%	H=4.200%
I=7.294%	J=0.511%	K=0.456%	L=2.415%
M=3.826%	N=2.284%	O=7.631%	P=4.319%
Q=0.222%	R=2.826%	S=6.686%	T=15.978%
U=1.183%	V=0.824%	W= 5.497%	X=0.045%
Y=0.763%	Z=0.045%		

Table 3: Cryptanalysis of the Caesar Cipher Only Decrypted Texts

Shift Key	Decrypted text	Chi-Sq Score
1	Oiftfmmttfbtifmmtczuiftfbtipsg	157.7825066
2	Ujgugnnuugcujgnnudavjgugcujqtg	534.7156469
3	Vkhvhoovvhdvkhoovebwkhvhdvkruh	299.7012102
4	Wliwippwwiewlippwfcxliwiewlsvi	154.5055963
5	Xmjxjqqxxjfxmjqqxgdymjxjfxmtwj	3048.475405
6	Ynkykrryykgynkrryheznkykgynuxk	385.6916792
7	Zolzlsszzlhzolsszifaolzlhzovyl	3083.352285
8	Apmamttaamiapmttajgbpmamiapwzm	174.4662539
9	Bqnbnuubbnjbqnuubkhcqnbnjbqxan	807.6407678
10	Crocovvccokcrovvclidrocokcrybo	155.1607209
11	Dspdpwwddpldspwwdmjespdpldszcp	211.8585288
12	Etqeqxxeeqmetqxxenkftqeqmetadq	1994.630884
13	Furfryyffrnfuryyfolgurfrnfuber	146.7403296
14	Gvsgszzggsogvszzgpmhvsgsogvcfs	925.8819525
15	Hwthtaahhtphwtaahqniwthtphwdgt	95.84617614
16	Ixuiubbiiuqixubbirojxuiuqixehu	608.3853772
17	Jyvjvccjjvrjyvccjspkyvjvrjyfiv	1615.940903
18	Kzwkwddkkwskzwddktqlzwkwskzgjw	1151.241238
19	Laxlxeellxtlaxeelurmaxlxtlahkx	807.6407678
20	Mbymyffmmyumbyffmvsnbymyumbily	211.7118721
21	Ncznzggnnzvnczggnwtocznzvncjmz	2419.975554
22	Odaoahhooawodahhoxupdaoawodkna	75.3495711
23	Pebpbiippbxpebiipyvqebpbxpelob	330.575228
24	Qfcqcjjqqcyqfcjjqzwrfcqcyqfmpc	2601.039571
25	Rgdrdkkrrdzrgdkkraxsgdrdzrgnqd	387.1881587
26	Shesellsseashellsbytheseashore	45.49886857

Table 4: Cryptanalysis of the Enhanced Caesar Cipher with DNA Sequence Only decrypted texts

Shift Key	Decrypted text	Chi-Sq Score
1	ATACCGTGCAGGATTCAGGCCTATGCGATTACA GGCCTATTACTAGCGTACTAGCGGCGATTACGC GATTACAGGCCTATGACGCTATGCGATTACCAG GATTCAGGCCTATTACTAGCGTACTAGCGGCGA TTACGCATAGTCGCGCAATTGGCCTATACAGGA TTCAGGCCTATGCGATTACAGGCCTATGACGCT ATGCGATTACCAGGATTCATACGGTCGCTTAGC AAGGCCTAT	1391.424048
2	ATCCTGAGATGTGCACGCGTATACGGCCTATAG CGTATACACTATGCGACTATGCGGGCCTATAGG CCTATAGCGTATACGCATAGTCGGCCTATAATG TGCACGCGTATACACTATGCGACTATGCGGGCC TATACAGTAGTCCTTGGACAAATCGGCTATGTG CACGCGTATACGGCCTATAGCGTATACGCATAG TCGGCCTATAATGTGCACGCATCAGTGCGATTA CGCGTATAC	1391.424048

Shift Key	Decrypted text	Chi-Sq Score
3	GTCACATGATCGCTAGTTCACAGGAATCGGCTT TCACAGGGCTCGTAAGCTCGTAAAATCGGCTAA TCGGCTTTCACAGGCAGTAGTCAATCGGCTATC GCTAGTTCACAGGGCTCGTAAGCTCGTAAAATC GGCTGTCCAGATGACGCTATCACGTGATATCGC TAGTTCACAGGAATCGGCTTTCACAGGCAGTAG TCAATCGGCTATCGCTAGTCTGCAAGGGCCTAT ATTCACAGG	1391.424048
4	TGCGACTACAGTTCAGCAGGATTCCACGTGATC AGGATTCATACGGTCATACGGTCCACGTGATCA CGTGATCAGGATTCGTCCAGATCACGTGATCAG TTCAGCAGGATTCATACGGTCATACGGTCCACG TGATAGGCCTATGCATAGTCTACAGTCGCAGTT CAGCAGGATTCCACGTGATCAGGATTCGTCCAG ATCACGTGATCAGTTCAGGCTTAGCAAATCGGC TCAGGATTC	1391.424048
5	GTACGTACTACTAGCGATGTGCACTACAGTCGA TGTGCACGCATCAGTGCATCAGTTACAGTCGTA CAGTCGATGTGCACAGGCCTATTACAGTCGTAC TAGCGATGTGCACGCATCAGTGCATCAGTTACA GTCGGCGTATACCAGTAGTCTGCCAATGTACTA GCGATGTGCACTACAGTCGATGTGCACAGGCCT ATTACAGTCGTACTAGCGGCGATTACCACGTGA TATGTGCAC	1391.424048
6	TCAGACGTACTATGCGATCGCTAGTGCCAATGA TCGCTAGTCTGCAAGTCTGCAAGTGCCAATGTG CCAATGATCGCTAGGCGTATACTGCCAATGACT ATGCGATCGCTAGTCTGCAAGTCTGCAAGTGCC AATGTTCACAGGGTCCAGATGCGCAATTACTAT GCGATCGCTAGTGCCAATGATCGCTAGGCGTAT ACTGCCAATGACTATGCGGGCCTATATACAGTC GATCGCTAG	1391.424048
7	TACGAGTCGCTCGTAACAGTTCAGGCGCAATTC AGTTCAGGCTTAGCAGCTTAGCAGCGCAATTGC GCAATTCAGTTCAGTTCACAGGGCGCAATTGCT CGTAACAGTTCAGGCTTAGCAGCTTAGCAGCGC AATTCAGGATTCAGGCCTATCTTGGACAGCTCG TAACAGTTCAGGCGCAATTCAGTTCAGTTCACA GGGCGCAATTGCTCGTAAAATCGGCTTGCCAAT GCAGTTCAG	1391.424048
8	TCCAAGTGATACGGTCTACTAGCGCTTGGACAT ACTAGCGGCGATTACGCGATTACCTTGGACACT TGGACATACTAGCGCAGGATTCCTTGGACAATA CGGTCTACTAGCGGCGATTACGCGATTACCTTG GACAATGTGCACGCGTATACGACGCTATATACG GTCTACTAGCGCTTGGACATACTAGCGCAGGAT TCCTTGGACAATACGGTCCACGTGATGCGCAAT TTACTAGCG	1391.424048

Shift Key	Decrypted text	Chi-Sq Score
9	GCGAATTCGCATCAGTACTATGCGGACGCTATA CTATGCGGGCCTATAGGCCTATAGACGCTATGA CGCTATACTATGCGATGTGCACGACGCTATGCA TCAGTACTATGCGGGCCTATAGGCCTATAGACG CTATATCGCTAGTTCACAGGGCATAGTCGCATC AGTACTATGCGGACGCTATACTATGCGATGTGC ACGACGCTATGCATCAGTTACAGTCGCTTGGAC AACTATGCG	1391.424048
11	GAACTTGCGCTTAGCAATACGGTCCAGTAGTCA TACGGTCCACGTGATCACGTGATCAGTAGTCCA GTAGTCATACGGTCCAGTTCAGCAGTAGTCGCT TAGCAATACGGTCCACGTGATCACGTGATCAGT AGTCTACTAGCGATGTGCACGTCCAGATGCTTA GCAATACGGTCCAGTAGTCATACGGTCCAGTTC AGCAGTAGTCGCTTAGCAGCGCAATTGCATAGT CATACGGTC	1391.424048
12	AGTTGACCGCGATTACGCATCAGTGTCCAGATG CATCAGTTACAGTCGTACAGTCGGTCCAGATGT CCAGATGCATCAGTTACTAGCGGTCCAGATGCG ATTACGCATCAGTTACAGTCGTACAGTCGGTCC AGATACTATGCGATCGCTAGAGGCCTATGCGAT TACGCATCAGTGTCCAGATGCATCAGTTACTAG CGGTCCAGATGCGATTACCTTGGACACAGTAGT CGCATCAGT	1391.424048
13	GACTGCATGGCCTATATCTGCAAGAGGCCTATT CTGCAAGTGCCAATGTGCCAATGAGGCCTATAG GCCTATTCTGCAAGACTATGCGAGGCCTATGGC CTATATCTGCAAGTGCCAATGTGCCAATGAGGC CTATGCTCGTAACAGTTCAGGCGTATACGGCCT ATATCTGCAAGAGGCCTATTCTGCAAGACTATG CGAGGCCTATGGCCTATAGACGCTATGTCCAGA TTCTGCAAG	1391.424048
14	TTCCAGGAAATCGGCTGCTTAGCAGCGTATACG CTTAGCAGCGCAATTGCGCAATTGCGTATACGC GTATACGCTTAGCAGCTCGTAAGCGTATACAAT CGGCTGCTTAGCAGCGCAATTGCGCAATTGCGT ATACATACGGTCTACTAGCGTTCACAGGAATCG GCTGCTTAGCAGCGTATACGCTTAGCAGCTCGT AAGCGTATACAATCGGCTGCATAGTCAGGCCTA TGCTTAGCA	1391.424048
15	TAGGCTACCACGTGATGCGATTACTTCACAGGG CGATTACCTTGGACACTTGGACATTCACAGGTT CACAGGGCGATTACATACGGTCTTCACAGGCAC GTGATGCGATTACCTTGGACACTTGGACATTCA CAGGGCATCAGTACTATGCGCAGGATTCCACGT GATGCGATTACTTCACAGGGCGATTACATACGG TCTTCACAGGCACGTGATCAGTAGTCGCGTATA CGCGATTAC	1391.424048

Shift Key	Decrypted text	Chi-Sq Score
16	ATCGGTCATACAGTCGGGCCTATACAGGATTCG GCCTATAGACGCTATGACGCTATCAGGATTCCA GGATTCGGCCTATAGCATCAGTCAGGATTCTAC AGTCGGGCCTATAGACGCTATGACGCTATCAGG ATTCTCTGCAAGGCTCGTAAATGTGCACTACAG TCGGGCCTATACAGGATTCGGCCTATAGCATCA GTCAGGATTCTACAGTCGGTCCAGATTTCACAG GGGCCTATA	1391.424048
17	CTGATACGTGCCAATGAATCGGCTATGTGCACA ATCGGCTGCATAGTCGCATAGTCATGTGCACAT GTGCACAATCGGCTTCTGCAAGATGTGCACTGC CAATGAATCGGCTGCATAGTCGCATAGTCATGT GCACGCTTAGCAATACGGTCATCGCTAGTGCCA ATGAATCGGCTATGTGCACAATCGGCTTCTGCA AGATGTGCACTGCCAATGAGGCCTATCAGGATT CAATCGGCT	1391.424048
18	GCCGTAATGCGCAATTCACGTGATATCGCTAGC ACGTGATCAGTAGTCCAGTAGTCATCGCTAGAT CGCTAGCACGTGATGCTTAGCAATCGCTAGGCG CAATTCACGTGATCAGTAGTCCAGTAGTCATCG CTAGGCGATTACGCATCAGTCAGTTCAGGCGCA ATTCACGTGATATCGCTAGCACGTGATGCTTAG CAATCGCTAGGCGCAATTGCGTATACATGTGCA CCACGTGAT	1391.424048
19	ATCCGGTACTTGGACATACAGTCGCAGTTCAGT ACAGTCGGTCCAGATGTCCAGATCAGTTCAGCA GTTCAGTACAGTCGGCGATTACCAGTTCAGCTT GGACATACAGTCGGTCCAGATGTCCAGATCAGT TCAGGGCCTATATCTGCAAGTACTAGCGCTTGG ACATACAGTCGCAGTTCAGTACAGTCGGCGATT ACCAGTTCAGCTTGGACATTCACAGGATCGCTA GTACAGTCG	1391.424048
20	GTGACATCGACGCTATTGCCAATGTACTAGCGT GCCAATGAGGCCTATAGGCCTATTACTAGCGTA CTAGCGTGCCAATGGGCCTATATACTAGCGGAC GCTATTGCCAATGAGGCCTATAGGCCTATTACT AGCGAATCGGCTGCTTAGCAACTATGCGGACGC TATTGCCAATGTACTAGCGTGCCAATGGGCCTA TATACTAGCGGACGCTATCAGGATTCCAGTTCA GTGCCAATG	1391.424048

Expected Count = FREQ / 100 × LEN

A Chi-Squared value that is above 150 does not and will likely not be similar to or appear to be similar to an English statement or word.

Results from Table 3 confirm the different Chi-Squared value for Caesar Cipher decrypted texts and it was observed that "Shesellsseashellsbytheseashore, X 2 = 45.49886857" that has the least chi-squared value using a shift of 26. Reading from the decrypted text for a shift of 26 it can be observed that it is an English statement. Hence cipher can be hacked and decoded easily.

Results from Table 4 confirm a different Chi-Squared value which is 1391.424048 for all enhanced Caesar cipher with DNA sequence

decrypted texts while using different shift. Since the value is far above 150, It strongly indicate that the decrypted texts does not and will likely not be similar to English statements, clearly showing its non-vulnerability for hackers and unauthorized access.

CONCLUSION

In this paper, an enhanced Caesar Cipher Cryptographic system was developed. It was achieved by using Deoxyribonucleic Acid (DNA) sequencing techniques in the generation of keys for shifting the cipher texts obtained from the Caesar Cipher encryption. The characters obtained in the DNA sequencing technique were scrambled by using only four letters A, T, C and G which represents the nucleotides which make up a DNA molecule. The results showed enhancement of information and Data security with respect to data Integrity, Authentication and Confidentiality which is presently limited to the encryption/decryption of text files only.

REFERENCES

Al-Mahdi, H., R.Shahin, O., Fouad, Y. and Alkhaldi, K. (2018). Design and analysis of DNA Binary Cryptography Algorithm for Plaintext. *International Journal of Engineering and Technology*, *10*(3), 699–706. https://doi.org/10.21817/ijet/2018/ v10i3/ 181003055

Al-mahdi, H., Shahin, O. R., Fouad, Y. and Alkhaldi, K. (2018). Design and analysis of DNA Binary Cryptography Algorithm for Plaintext. *International Journal of Engineering and Technology*, *10*(3), 699–706. https://doi.org/10.21817/ijet/2018/ v10i3/ 181003055

Balogun, A., Sadiku, P. and Mojeed, H. (2017). Multiple Ceaser Cipher Encryption Algorithm. *ABACUS*, *44*(2), 250–258.

Bhanot, R. and Hans, R. (2015). A Review and Comparative Analysis of Various Encryption Algorithms. *International Journal Secuirty*, *9*(4), 289–306.

Das, A., Sarma, S. K. and Deka, S. (2019). Data Security with DNA Cryptography. *Proceeding of the World Congress on Engineering*, 1–6.

Dixit, P., Trivedi, M. C., Gupta, A. K., Yadav, V. K. and Singh, V. K. (2019). Video steganography using concept of DNA sequence and index compression technique. *International Journal of Engineering and Advanced Technology*, *8*(5), 408–417.

Dubey, R., Saxena, A. and Gond, S. (2015). An Innovative Data Security Techniques Using Cryptography and Steganographic Techniques. *International Journal of Computer Science and Technologies*, *6*(3), 2175–2182.

Enas, Imran, I. and Farah. (2014). Enhancement Caesar Cipher for Better Security. *IOSR Journal of Computer Engineering*, *16*(3), 1–5.

Fernandez, S. A., Juan, A. A., Adrian, J. de A., Silva, D. G. e. and Terren, D. R. (2018). Metaheuristics in Telecommunication Systems: Network Design, Routing, and Allocation Problems. *IEEE Systems Journal*, 1–10. https://doi.org/10.1109/JSYST.2017. 2788053

Goyal, K. and Kinger, S. (2013). Modified Caesar Cipher for Better Security Enhancement. *International Journal of Computer Applications*, *73*(3), 26–31.

Imran, I. E. and Abdulkareem, F. A. (2014). Enhancement Caesar Cipher for Better Security. *IOSR Journal of Computer Engineering*, *16*(3), 1–5.

Jain, A., Dedhia, R. and Patil, A. (2015). Enhancing the Security of Caesar Cipher Substitution Method using a Randomized Approach for more Secure Communication. *International Journal of Computer Applications*, *129*(13), 6–11.

Karimi, M. (2017). *Cryptography using DNA Nucleotides*. *168*(7), 16–18.

Kumari, S. (2017). A research Paper on Cryptography Encryption and Compression Techniques. *International Journal of Engineering and Computer*

Science, *6*(4), 20915–20919 .https://doi.org/10.18535/ijecs/v6i4.20

Lin, A. and Tong, Z. (2018). Implementation Cryptography Data Encryption Standard (DES) and Triple Data Encryption Standard (3DES) Method in Communication System Based Near Field Communication (NFC) Implementation Cryptography Data Encryption Standard (DES) and Triple Data En. *Journal of Physics*, *954*.

Mavanai, S., Pal, A., Pandey, R., Prof, A. and Nadar, D. (2019). Message Transmission Using DNA Crypto-System. *International Journal of Computer Science and Mobile Computing*, *8*(4), 108–114.

Najaftorkaman, M. and Kazazi, N. S. (2015). A Method to Encrypt Information with DNA-Based Cryptography. *International Journal of Cyber-Security and Digital Forensic*, *4*(3), 417–426.

Omolara, O. E., Oludare, I. A. and Abdulahi, S. E. (2014). Developing a Modified Hybrid Caesar Cipher and Vigenere Cipher for Secure Data Communication Omolara Computer Engineering and Intelligent Systems. *Computer Engineering and Intelligent System*, *5*(5), 34–46.

Purnama, B. and Rohayani, H. (2015). A New Modified Caesar Cipher Cryptography Method With Legible Ciphertext From A Message To Be Encrypted. *Procedia - Procedia Computer Science*, *59*(Iccsci), 195–204. https://doi.org/10.1016/j.procs.2015.07.552

Ruhan, A., Malarvizhi, S. and Patel, K. (2016). Information Coding and its Retrieval Using DNA Cryptography. *Journal of Engineering Science and Technology Review*, *9*(3), 86–92.

Sailakshimi, S. and Sasikala, G. (2015). Caesar Cipher with Complement Approach. *International Journal of Advanced Research in Computer and Software Engineering*, *5*(5), 398–400.

Soni, E. R., Soni, E. V., Sandeep, E. and Mathariya, K. (2012). Innovative field of cryptography : DNA cryptography. *Computer Science & Information Technology*, 161–179.

Xiang, Tao., Wong, K. and Liao, X. (2007). Selective image encryption using a spatiotemporal chaotic system. *Chaos*, *17*. https://doi.org/10.1063/1.2728112