Advances and Applications in Mathematical Sciences
Volume 21, Issue 1, November 2021, Pages 251-167

HYBRID DNA CRYPTOGRAPHY METHOD USING DIFFERENT KEY GENERATION TECHNIQUES

E. VIDHYA and R.RATHIPRIYA

Department of Computer Science
Ph.D. Research Scholar
Periyar University
Salem, Tamilnadu, India
E-mail: vidhya11tamilarasi@gmail.com
rathipriyar@gmail.com

Abstract

Nowadays, the large volumes of real-time data like structured and unstructured data are created by industries, hospitals, IT fields and so on. Day to day the data size is increased in the form of gigabyte or terabyte or pet a byte. All these big data contain confidential and sensitive information. They are communicated in an open-source network like an internet and stored in the cloud computing environment. The open-source network contains a lot of attackers and malicious users. They always attempt to access the confidential data without having the authorization of the right user. Sometimes they exchange the original data to fake data. So, the security of big data in open-source has become an important issue. DNA [Deoxyribonucleic acid] Cryptography is an advanced developed field for improving big data security which is developed based on the biological concept of DNA. In this paper, the data are encrypted with the hybridization of DNA Cryptography and the Insertion method. Here pseudo-random Number generator algorithm is hybrid with El-Gamal key generation to generate a key that enables the data to protect against many security attacks and share the key using a Shamir secret sharing. Finally, the experimental results as well as the security analysis show the better solution when compared to a well-known existing system.

1. Introduction

The large amounts of data are generated by industries in the field of social network, IT Industries, online-banking transactions and so on. The data sizes are increased day by day in the form of Megabyte or Gigabyte or

2020 Mathematics Subject Classification: 34Dxx, 93Dxx.
Keywords: DNA cryptography, Shamir secret sharing, El-Gamal cryptography, Pseudo-random Number generator, Insertion Method.
Received June 2, 2020; Accepted January 20, 2021

Terabyte or Petabyte. (E. Vidhya, Hybrid Key Generation for RSA and ECC, 2019) The data are in the form of text, image video and so on. The data are transmitted using the open-source network like an internet and the cloud computing network. All the data contains a sensitivity and confidentiality data. The attackers or the malicious users in the open-source network access all the data and transfer into another form, so the receiver cannot receive the original data. (E. Vidhya, 2016) Cryptography is a method of creating secret data. The main aim of cryptography is to create a secret data and communicate between source and destination. The malicious user and the attackers are not easily able to access the original data.

The cryptography algorithm contains two types

1. Symmetric cryptography algorithm.

2. Asymmetric cryptography algorithm.

In the symmetric cryptography algorithm, the secret key is communicated between the sender and the receiver. The encryption and decryption process are performed by the same secret key. In asymmetric cryptography algorithms, the two keys are created mathematically. The attackers are not easily able to get the key. The keys are not transmitted over the network. The keys are the public key and the private key. The public key is used to encrypt the data and the private key is used to decrypt the data. The two cryptography algorithms are not providing efficient security to data because the security model creates a cipher text with a combination of plaintext and the secret key. If the attackers are able to access the key, they can easily retrieve the plaintext. To overcome the problem, the (E. Vidhya, Two Level text Data Encryption using DNA Cryptography, 2018) DNA Cryptography technology is created. DNA Cryptography is proposed by Adleman and Risca (Ahlawat, 2015). It was created based on DNA Computing. In DNA computing, the data are transmitted into a biological form of nucleic acid, represented as a DNA Sequence [A, C, G, T]. The DNA sequence is combined with a key and forms a new DNA sequence. (E. Vidhya, 2020) The advantage is attackers are not easily able to access the plaintext because the plaintext is encoded with a biological form. It is very difficult to convert the DNA sequence to original data. So the researchers are mainly concentrating on the DNA cryptography to develop a new security to data. In DNA Cryptography,

the key is generated with the El-Gamal key generation. The prime number is generated by a user, not in a random format. To overcome this problem, the pseudo-random key is used. In the Pseudo random number generation, the keys are generated randomly. (Anushree Raj, 2017) The two keys are hybrid and generate a strong key. The Hybrid key is shared between the Sender and Receiver using an Shamir Secret sharing with an '*n*' number of shares. The attackers do not easily access the '*n*' number of keys.

2. Related Works

The below study focused on the DNA cryptography with Shamir Secret Sharing and with an OTP Generator.

2.1. DNA Cryptography with Shamir Secret Sharing

(Adhikari, 2006)This paper describes the DNA secret sharing is applied to a general access structure. (Chaudhuri, 2016) This paper describes, the Information is shared with a different percentage, and it gives storage information. It explains a multiple secret Image sharing scheme. The images are shared with an 'n' set of preliminary share matrices. (K. Shankar, 2018) This paper proposed new technology is an Index-based symmetric DNA encryption algorithm. The new algorithm is adopted with a Block cipher and Index of string.

2.2. DNA Cryptography

(Ahlawat, 2015) In this paper, the author says that a detailed description of the DNA cryptography. The DNA Cryptography techniques are applied to the cloud data and secure the data at a higher level. (E. Vidhya, Two Level text Data Encryption using DNA Cryptography, 2018) the author describes DNA cryptography. In the DNA cryptography, the binary numbers were created with two algorithms. The first algorithm is to transmit the binary numbers to a DNA sequence using public-key encryption. The second algorithm is to create a binary number with an XOR, One-time pad cryptography. (Wattar, 2015) The paper is to demonstrate the application of watermarks based on DNA sequence. To identify the unauthorized use of genetically modified organisms [GMOs]. This paper is to describe an DNA cryptography and the techniques are already used in this algorithm like an DNA digital encoding, polymerase Chain Reaction [PCR], DNA Synthesis,

electrophoresis etc., In this paper, the DNA cryptography algorithm created an DNA sequence with the DNA chip and biological technologies. The proposed algorithm results show the strong security when compared to the traditional encryption method. The author explained about an DNA cryptography and their methods. The result is given in a MATLAB bioinformatics toolbox. In this paper, the author says about a data hiding using an DNA cryptography and explain detailed about a technique.

The study, it was observed that DNA cryptography and Shamir Secret Sharing algorithm encryption techniques used very commonly. But in the proposed work, the DNA cryptography are hybrid with the Shamir secret sharing algorithm and Peudo-random Number Generator with El-Gamal Cryptosystem, which produce the strong encryption key. The proposed work is measured with the experimental results as well as the security analysis show the better solution when compare to an well-known existing system.

3. Methods and Materials

3.1. DNA Cryptography

DNA Cryptography is a new technology hiding (Alexander, 2017) a data using a biological structure of DNA Computing. It was developed by Leonard Max Adleman in the year 1994. In DNA Cryptography the Plaintext are transmitted to an DNA nucleotides which are [Adenine (A), Cytosine (C), Guanine (G) and Thymine (T)]. The DNA nucleotides are given in binary form of $\sum = \{A = 00, G = 01, C = 10, T = 11\}$.

3.2. El-Gamal Cryptosystem

El-Gamal Cryptosystem is an Asymmetric (Mikhail, 2014) (Meier, 2005) cryptography. This cryptosystem is based on the trouble of finding discrete logarithm in a cyclic group.

3.3. Pseudo Random Number Generator

Pseudo Random Number Generator (PRNG) is generating a number randomly with an mathematical formula.

3.4. Shamir Secret Sharing

Shamir's Secret Sharing is an algorithm in cryptography formed by Adi Shamir (Adhikari, 2006). It is a form of secret sharing, where a secret data is divided into 'n' number of parts, giving each member its own single part. To reconstruct the original data secret, a minimum number of parts is needed. In the threshold scheme this number is less than the total number of parts. Otherwise all members are needed to reconstruct the original secret data.

4. Proposed Scheme

4.1 Proposed Workflow Diagram

Figure 1 shows DNA cryptography (AI-Harbi, 2020) with Shamir secret sharing encryption process (Adhikari, 2006). The proposed work contains four phases. 1. DNA Sequence, 2. Key generation, 3. Encryption Process, 4. Decryption process. The first phases are a DNA sequence creation. The plaintext is converted to an ASCII value. The ASCII values are converted to binary values. The binary values are converted to DNA Sequence [A-00, C-01, G-10, T-11]. The second phase is a key generation, The key values are generated by a Pseudo Random Number Generator with random and El-Gamal Key Generation. The two keys are hybrid and generate new hybrid key. The Hybrid key values are converted to an Hybrid key Binary values. The hybrid keys are read by an Shamir secret sharing. The Hybrid keys are split with 'n' number of shares and with an 't' threshold. The third phase is an encryption, the binary values and the Hybrid key binary values are combined using an insertion method and create a new binary number. The new binary numbers are converted to a New DNA sequence. The New DNA sequence is read by a Complementary-Pair rule [A-T, T-A, C-G, G-C] and creates an Fake DNA sequence. The Fake DNA sequence is sent to a receiver by a sender. Figure 2 shows the fourth phases of the decryption process, the decryption is a reverse process of encryption. The Fake DNA sequence are read by an complementary-Pair rule and converted to an New DNA Sequence. The New DNA sequence are read by an insertion decryption. The Hybrid key values are removed and create a binary value. The binary values are converted to an ASCII values. The ASCII values are converted to a Plaintext. The plaintext is return by a receiver.

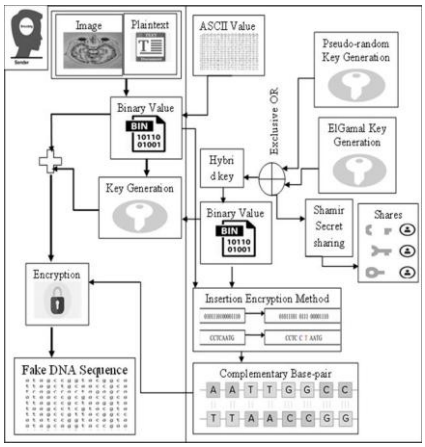

Figure 1. Proposed Workflow Diagram for Encryption process.

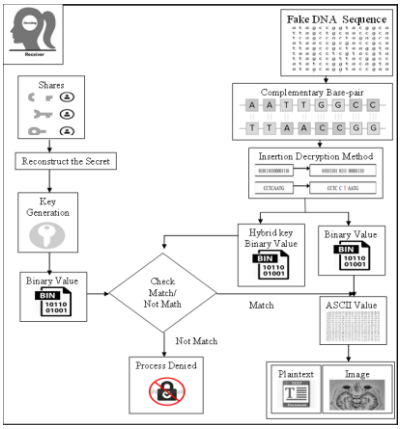

Figure 2. Proposed Workflow Diagram for Decryption process.

4.2. Proposed Work Algorithm

Phases I: Transform Plaintext to Binary form

Pseudo code-binary form (): {Initialization: PT<-Plaintext, bn<-binary number.

Process:

1. Read PT.
2. Split: st <- split (PT).
3. Convert: as <- ASCII(st)

4. Convert: bn <- (as)2.

5. Return bn. }

Phases II: Key Generation:

Pseudo code-Key Generation (): { Pseudo-random key generator ():

{Initialization: p<-values [1< = n]. where n-natural numbers

Process:

1. Generate random values p1: random(p)

2. rp = p.

3. return rp }

El-Gamal key generation():

{ Initialization: prime numbers <- p, primitive element<- q

Process:

1. Large prime p.

2. primitive element q.

3. Possibly random integer d where $2 \leq d \leq p-2$

4. compute key $k : k = q^d (\text{mod } p)$

5. return k. }

Hybrid Key Generation():

{ Initialization: Hybrid key<- hk.

Process:

1. Exclusive OR() {

1. compute hybrid key hk : $hk = rp + k$

2. return hk

3. Convert: bk <- (hk)2

4. return bk. } }

Secret Sharing():

{ **Process:**

1. Pass the hybrid binary key [bk] to the secret split.

2. Secret Split method is split the hybrid binary key with polynomial $f(x)$.

$$f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 +, \ldots, + a_{t-1}x^{t-1} (\text{mod } p)$$

Where p = prime number [select based on level of security need for the secret].

a_0 = Constant term for the secret 's'. t = threshold value $[1 <= t <= n]$.

3. The shares are created with an 'n' random value $[Sh_1, Sh_2, \ldots, Sh_{t-1}]$.

$\text{shares}_i(s) = (x_i, f(x_i))$ Where $x_i \neq 0\}$

Phases III Encryption Process:

Pseudo code-Encryption ():

{ Initialization: { n<- Natural Numbers.

Process:

Insertion method (): {

1. Read bn.
2. Split: ib = (bn% k) [1>= k<=n].
3. Split: sbk= (bk%k). [1>= k<=n].
4. Insert Encryption: fb = Insert(ib, sbk).
5. Convert: fda = DNA Code(fb).
6. Return fda.}

Complementary-pair ():

{ Initialization: Cp <- [A-T, T-A, C-G, G-C].

Process:

1. Read fda.
2. Convert: nda = cp(fda).
3. Return nda. }}

Phases IV Decryption Process:

Pseudo code-Decryption ():

{ Initialization: Cp <- [A-T, T-A, C-G, G-C], n<- Natural Numbers,

Process:

1. The shares are reconstructed with a threshold 't' out of 'n' number of shares $[sh_1, sh_2, \ldots, sh_{t-1}]$.

$(x_0 f(x_{i0}))$, $(x_1 f(x_{i1}))$, $(x_2, f(x_{i2}))$, …, $(x_{t-1}, f(x_{it-2}))$

Where $f(x) = \sum_{t=0}^{t-1} f(x_i) * l_i(x)$, $l_i(x) = \prod_{j=0, j\neq 1}^{t-1} \frac{x - x_j}{x_i - x_j}$,

$l_i(x)$ has the value 1 at $x_i 0$ at every other x_j

2. Polynomial $f(x)$ is reconstructed. $f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \ldots + a_{t-1} x^{t-1}$

3. return rbk.

4. Complementary-Pair: fda = cp(nda).

5. Convert : fb = (fda, DNA Code).

6. Insertion decryption: bn1 = split(fb%k) [1>= k<=n]

7. Check:.

if (bk != rbk): Process stopped.

Else Process Continued.

8. Remove: bn= remove(bn1, hk). [remove hk of split binary Numbers]

9. Convert: as= ASCII(bn)

10. Convert: PT= chr(as).

11. Return plaintext PT}

5. Result and Discussion

1. Experimental setup:

The data are run using an HPC. HPC means High Performance computing High Performance Computing most commonly refers to the perform of aggregating computing power in a method that deliver much advanced performance than individual can obtain out of a characteristic desktop computer or workplace in classify to solve large problems in science, engineering, or business.

2. Shannon Entropy: H(X)

Shannon entropy defined as the amount of Information in a variable, that variable has been providing the basic theory around the notation of Information. It can set in terms of the probabilistic model. (Entropy (information theory)), (Wang). It means that the modules which have many possible rearrangements, then the system has high entropy, and the system has very few rearrangements, and then the system has low entropy. The Shannon entropy equation (1) is used to calculate approximately the average lowest amount of bit necessary to predetermine a string of symbols, based on the frequency of the symbols.

$$H(X) = -\sum_{i=1}^{n} P(x_i) \log_b P(x_i) \tag{1}$$

Where H = Shannon Entropy, x_i = fraction of population composed of a single species i, log = natural log (2 or 10 or ent), n = how many species encountered, Σ = summation of species 1 to n.

Maximum Possible Information: H_{MAX}

$$H_{Max} = \log_2 M \tag{2}$$

Where M = Number of Message

Percentage of maximum possible information: AVG

$$AVG = \left[\frac{H(X)}{H_{MAX}}\right] * 100. \tag{3}$$

Table 1. Entropy values for text files.

SURVIVING ALGORITHM													HYBRIDIZATION KEY GENERATION			
ALGORITHM	ElGamal Cryptosystem				DNA Cryptography				DNA Elagamal Cryptosystem				DNA Psudorandom Elagamal Cryptosystem			
PLAINTEXT [MB]	PT	CT			PT	CT			PT	CT			PT	CT		
	H(X) [bits/message]	H_{MAX}	H(X) [bits/message]	AVG %	H(X) [bits/message]	H_{MAX}	H(X) [bits/message]	AVG %	H(X) [bits/message]	H_{MAX}	H(X) [bits/message]	AVG %	H(X) [bits/message]	H_{MAX}	H(X) [bits/message]	AVG %
20	4.237	6.169	6.169	97	4.237	5.357	2.805	52	4.237	6.169	6.890	97	4.237	5.392	3.119	57
53.6	4.617	6.169	6.418	97	4.617	5.754	3.207	56	4.617	6.169	6.472	97	4.617	6.442	3.308	51
312	3.319	6.169	6.951	97	3.319	3.700	2.578	71	3.319	6.169	6.924	97	3.319	3.700	2.659	71
318	3.352	6.169	6.949	97	3.352	3.700	2.605	72	3.352	6.169	6.935	97	3.352	3.700	2.676	72
321	3.362	6.169	6.990	97	3.362	3.700	2.681	72	3.362	6.169	6.932	97	3.362	3.584	2.579	72

PT: Plaintext, CT: Cipher text. H(X): Shannon Entropy. HMA: Maximum Possible Information, AVG: Percentage of maximum possible information.

3. Key Entropy:

Key Entropy is to measure the Strength of the Key.

$$\text{Key Entropy} = \frac{\text{Log (Phrases)}}{\text{Log(b)}} \tag{4}$$

Where Phrases: encryption key, b: base (2 or 10 or ent)

Table 2. key Entropy.

SURVING ALGORITHM				HYBRIDIZATION KEY GENERATION	
El agamal Key Generation		Pseudo-Random Number Generator		El-Gamal-Pseudo-Random Generator	
Key size [bits]	Key entropy [bits]	Key Size [bits]	Key entropy [bits]	Key Size [bits]	Key entropy [bits]
7.74	13.71	8.43	251.01	8.48	254.01
7.03	21.03	8.19	252.16	8.03	253.28
6.84	15.37	8.60	252.80	9.43	254.53
8.23	26.38	8.51	254.67	8.71	255.17
8.98	20.24	7.23	250.60	8.98	252.28

4. Password Entropy

Password entropy is a amount of how changeable a password

$$E = Log_2(R^L) \tag{5}$$

Where R = pool of unique characters, L = number of characters in password,

E = Password Entropy R^L = Number of Possible password.

Table 3. Password Entropy.

SURVIVING ALGORITHM				HYBRIDIZATION KEY GENERATION		
		El agamal Key Generation	Pseudo-Random Number Generator	El-Gamal-Pseudo-Random Number Generator		
L	R	E[bits/character]	E[bits/character]	HL	HR	HE[bits/character]
1	95	6.598	13.139	4	95	26.279
2	95	13.139	19.709	6	95	19.709
3	95	19.709	26.279	8	95	52.558
4	95	26.279	32.849	10	95	65.698
5	95	32.849	39.419	12	95	78.838
6	95	39.419	45.988	14	95	91.977
12	95	78.831	52.558	16	95	105.117
17	95	111.687	59.128	18	95	118.257
18	95	118.258	65.698	20	95	131.397
76	95	499.304	72.268	22	95	144.536
77	95	505.878	78.838	24	95	157.676

R = pool of unique characters, L = number of characters in password, E = Password Entropy.

5. Avalanche Effect

In cryptography a property called diffusion reflects cryptographic strength of an algorithm. A small change in the key or the plaintext should

cause a strong change in the cipher text. Calculate how the cipher is strong. Avalanche effect value must greater than 50. If it is lower than 50 then it is not best one.

$$\text{Avalanche effect} = \left[\frac{\text{Number of chaged bit in cipher text}}{\text{Number of bits in cipher text}}\right] * 100. \quad (6)$$

Table 4. Avalanche Effect.

Algorithm	SURVIVING ALGORITHM								HYBRIDIZATION KEY GENERATION			
	El-gamal key generation				Pseudo-random number				El-Gamal-Pseudo random Key generation			
Keys size [bits]	1	2	3	4	1	2	3	4	1	2	3	4
Plaintext												
1	50	52	50	49	44	57	40	48	53	52	51	52
2	50	53	51	48	57	54	54	46	43	51	50	57
3	52	51	50	50	47	55	45	46	40	54	51	57
4	51	51	51	52	51	54	56	49	63	44	48	44
5	53	53	51	51	50	50	53	49	46	53	43	50
Average	51	52	51	50	50	54	51	48	49	51	49	52
Overall Average[%]	50				50				50			

6. Hamming Distance:

The Hamming distance between two equal-length strings of symbols is the number of positions at which the corresponding symbols are different

Table 5. Hamming Distance of text file.

SURVIVING ALGORITHM					HYBRIDIZATION KEY GENERATION			
Algorithm	El-Gamal Cryptosystem		DNA Cryptosystem		DNA El-Gamal Cryptosystem		DNA Psudorandom	
Plaintext [MB]	H [P an C]	H [P and C]	H [P and C]	H [P and C]	H [P and C]	H [P and C]	H [P and C]	H [P and C]
20	19409	0	18119	0	19418	0	18119	0
53.6	53420	0	49141	0	53368	0	49137	0
312	308112	0	308232	0	308003	0	306612	0
318	313646	0	314316	0	313687	0	317422	0
321	316501	0	320302	0	316602	0	317680	0

7. Security Analysis

Security Analysis is an analysis about the security strength of encryption and decryption algorithm. The result of the analysis is the encryption algorithm gives the better solution

8. Key Sensitivity Analysis

Key sensitivity Analysis is to measure the key strength. If the plaintext is stable and the small changes to the key it gives an lot of changes in the cipher text. Table 4 shows the analysis of the key sensitivity.

9. Plaintext Analysis

Plaintext Analysis is to measure the Plaintext strength. If the key is stable and the small changes in the plaintext. It shows an lot of difference in the cipher text. Table 4 shows the analysis of the plaintext analysis.

10. Key Space Analysis

Key Space Analysis is analysis how much of key size is used. The measurements are given in the table 2 and 3.

11. Brute Force Attack

Table 6. Brute Force Attack for Password.

Password Length	Password to encrypt data	Possible Combinations
4	5432	81450625
6	Pass34	735091890625
7	AwDs238	69833729609375
8	Am13bn81	6634204312890625
9	$SS39901b	630249409724609375
10	123456vy29	59873693923837890625

12. Throughput

Throughput is to calculate the units of Information a system can progression in a given time.

$$\text{Throughput} = \frac{\sum(\text{inputfile})}{\sum(\text{execution time})}. \tag{7}$$

Table 7. Throughput value for text file.

Phases	DNA Cryptography	DNA with El-gamal Cryptography	DNA with El-gamal Cryptography and Pseudo random Number generator
DNA Sequence	1.2874	1.4770	1.9354
Key Generation	0.16402	0.24994	0.44062
Encryption	0.56502	0.584388	1.05077
Decryption	0.156345	0.16538	0.2969

Conclusion

The goal line of this paper was to recover the security level to information by using DNA cryptography with the Shamir Secret sharing algorithm and the Pseudorandom number generator. The proposed work is to encrypt the information with a DNA sequence and the key is generated using a Pseudo random Number generator and El-Gamal Cryptosystem. The Insertion method and the complementary method is to generated a fake DNA sequence so the unofficial person cannot reach the information. Finally, the experimental results as well as the security analysis show the better solution when compare to a well-known existing system.

Acknowledgment

The authors would like to acknowledge and thank URF (University Research Fellowship) for supporting this work in the Department of Computer Science, Periyar University, Salem, Tamil Nadu, India.

Reference

[1] M. S. Abdul-Hassan, A Modification of El-Gamal Cryptosystem using Statistical Methods European Journal of Scientific Research (2015), 20-25.

[2] A. Adhikari, DNA Secret Sharing IEEE Congress on Evolutionary Computation Vancouver, BC, Canada: IEEE. (2006), 1407-1411.

[3] M. A. Ahlawat, A survey of DNA Based Cryptography International Journal of Scientific Engineering and research 3(4) (2015), 132-134.

[4] P. Akkasaligar, Selective medical image encryption using DNA cryptography Information Security journal: A global perspective 29(2) (2020), 91-101.

[5] G. Alexander, DNA Based cryptography and steganography. Global Research and Development Journal for engineering 2(6) (2017, May), 249-253.

[6] Anushree Raj, DNA Cryptography algorithm using Genetic algorithm. International Journal of Latest trends in Engineering and technology (2017), 34-39.

[7] R. R. E. Vidhya, Key Generation for DNA Cryptography Using Genetic Operators and Diffie-Hellman Key Exchange Algorithm. International Journal of Mathematics and Computer Science 15(4), 1109-1115.

[8] E. Vidhya, Two Level text Data Encryption using DNA Cryptography. International Journal of Computational Intelligence and Informatics 8(3) (2018), 106-118.

[9] E. Vidhya, Hybrid Key Generation for RSA and ECC, International Conference on Communication and Electronics Systems (ICCES), (2019).

[10] E. R. Vidhya, A Study on Unstructured Data Security Issues, International Journal of Innovations and Advancement in Computer Science (2016), 61-65.

[11] Entropy (information theory) (n.d.).

[12] K. Gyu-Chol, (n.d.), A study on the fast El-Gamal encryption.

[13] G. Hamed, Comparative study for various DNA based Steganography techniques with the essential conclusions about the future research. Conference: 2016 11th International conference on computer Engineering and system (ICCES) (2016).

[14] E. M. Hossain, A DNA cryptographic techniques based on Dynamic DNA sequence Table 19th International conference on computer and information technology (2016), 270-275.

[15] M. B. Jornea, DNA secret writing techniques 8th International conference on communications (2010), 451-456.

[16] K. Shankar and I. R. Multi, Secret Image Sharing Scheme based on DNA Cryptography with XOR, International Journal of Pure and Applied Mathematics 118(7) (2018), 393-398.

[17] R. Kumar, Image Encryption using a combination of HAAR and DNA algorithm International journal of advanced trends in computer science and engineering 3(5) (2014), 82-87.

[18] M. E. Borda, O. A, DNA Cryptographic Algorithm IFMBE Proceeding (2009), 223-226.

[19] G. Madhvi Popli, DNA Cryptography: A novel approach for data security using Flower Pollination Algorithm. International Conference on sustainable computing in science, technology, (2019).

[20] H. A. Mahdi, Design and analysis of DNA Binary cryptography algorithm for plaintext, International Journal of engineering and technology 10(3) (2018), 699-706.

[21] A. V. Meier, The El-Gamal Cryptosystem, (2005).

[22] M. Mikhail, Extension and Application of El-Gamal Encryption Scheme, IEEE., (2014).

[23] D. I. Nassr, Secure Hash Algorithm-2 formed on DNA. Journal of the egyptian mathematical society (2019), 1-20.

[24] P, K. K., A Novel text encryption algorithm using DNA ASCII Table with a sprial Approach. International Journal of Recent Scientific Research 9(1) (2018), 23588-23595.

[25] G. P. Panday, Implementation of DNA cryptography in cloud computing and using huffman algorithm, soccer *t* programming and new approach to secure cloud data, SSRN, (2020).

[26] M. Popli, DNA Cryptography: A Novel approach for data security using genetic algorithm International journal of advance research in computer science and management studies (2018), 1-10.

[27] S. K. Pujari, A hybridized model for image encryption through genetic algorithm and DNA sequence 6th International conference on smart computing and communications (2017), 7-8.

[28] R. Rathipriya, E. Comparative Study of Hybrid RSA-ECC and Hybrid DNA-Insertion for Large Dataset, International Journal of Grid and Distributed Computing 13(1) (2020), 2286-2303.

[29] R. Rathipriya, E. A., Comparative Study of Hybrid RSA-ECC and Hybrid DNA-Insertion for Large Dataset. International Journal of Grid and Distributed Computing 13(1) (2020), 2286-2303.

[30] N. H. Rahman, A Novel DNA Computing Bassed Encryption and decryption Algoriithm. International Conference on information and communication Technology (ICICT) (2015), 463-475.

[31] D. O. Vadaviya, Secure encryption techniques using DNA computation. International Journal of Modern trends in engineering and research (2015), 176-182.

[32] Wang (n.d.), Information and Entropy.

[33] A. H. Wattar, Review of DNA and pseudo DNA cryptography International Journal of computer science and engineering 4(4) (2015), 65-76.