IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-8, Special Issue-1, Feb 2020 E-ISSN: 2347-2693

NTCETLS: A Novel Technique For Cryptography Ensuring Two Level Security

Sourav Ghosh[1*], Prithwijit Das[2], Ira Nath[3], Dharmpal Singh[4], Sudipta Sahana[5]

[1,2,3,4,5]Dept. of Computer Science, JIS College of Engineering, West Bengal, India

[*]*Corresponding Author: ghosh.sourav31@gmail.com, Tel.: +918910750906*

Available online at: www.ijcseonline.org

***Abstract*—** The method of hiding a message so that only the actual recipient receives it properly and securely is referred as encryption. Encryption can contribute a technique for hiding data from intruders. As huge amount of data is stored on computers or transmitted via computers are exposed to the attackers which is at a risk. With the quick evolution of digital information transmission in electronic way, data safety is essential in information storage and transmission. The confidentiality of data has a remarkable role in various fields like ethics, law and currently in Data Systems. With the progress of human intelligence, the art of cryptography has grown to be more complicated with the aim of make data more safe and secure. Different collections of Encryption systems are being utilized in the world of Data Systems by different institutes. A new algorithm has been proposed for the security purpose of the data to be hidden from any unauthorized access. The proposed algorithm takes a 4-digit user-defined key and also generates a key which will be used to decrypt the same. The new technique is able to handle any size data efficiently and effectively for cryptography. We have used two layers cryptography technique which is totally new as far of our knowledge. It can provide more security of data than existing works in linear time.

***Keywords*—** Cryptography, Security, Multi level Security

I. INTRODUCTION

Data is any information which is stored or transferred. Data is relevant or meaningful when the information stored in the data is transparent to the user. Cryptography gives authorized users access to the transparency of data. In cryptography, plaintext refers to the original message. A key is referred to as a password that is set by the user to perform cryptography. On applying the key on the plaintext an encrypted message is generated which is known as cypher text. An authorized user is one who has the correct key that is used to hide the transparency of data. Cryptography can be broadly classified as symmetric key and asymmetric key cryptography. Symmetric key cryptography is one where the key used to encrypt and decrypt is identical. Asymmetric key cryptography is one where the key used to encrypt and decrypt is unidentical. Cryptography is probabilistic and combinatorics study. It is obtained from the mathematical formulation of data. When the key is applied to the cypher text, we obtain a result. The originality of the data will depend on the application of the key. If the key applied is correct then the result will be correct if not then the receiver will land up obtaining a wrong result.

This paper proposes an algorithm which uses linear algebra to obtain encryption and decryption algorithm. ASCII value is used to perform all the mathematical operations on the data.

The paper consists of the following sections. Section II is representing the literature survey. The proposed work has been depicted in section III. In section IV, illustrative example has been presented. Section V is presenting the result and discussion of the proposed work. The complexity analysis has been depicted in section VI. The conclusion has been presented in section VII.

II. RELATED WORK

In 2015 [8], authors Rashmi Welekar and Deepti Chaudhary proposed a cryptographic technique based on Steganography and Visual Cryptography. Through this technique, the secret code is hidden in an image using the Steganography technique and requires a mechanical operation at the receiver's end without the involvement of a computer.

In 2017 A. Samir [7] explained a secured communication which can be built over Cloud network. In other words, it stated the way to protect the data by the method of encryption. In encryption, exchange of data is done with the help of an encryption algorithm, i.e., using the key in a twisted manner. The original message can be accessed only

by that user acquiring the same unique key. Thus, providing a tight security in providing security to data against the malicious attacks made from the intruder's side.

In 2017, S.S Roy, Kazi Md. Rokibul Alam, and Yasuhiko Morimoto [2] made a proposal for enciphering text messages with the help of time-varying delayed Hopfield neural network. On applying this network, a binary sequence is generated as an outcome that has to be passed further on to a permutation function. This is used for the generation of a key and regarded as the first level encryption. binary sequences are obtained after converting the plain text to its ASCII value. Here encryption is achieved by switching chaotic neural network maps. And a permutation function which is further dependent on the binary sequence generated from the above chaotic neural network. Moreover, an additional DNA cryptographic model is also used over the ciphertext obtained from the first level encryption with the purpose of robust the security of the proposed model.

In 2006 Nadeem, H [6] has been conducted a study on different secret key algorithms with the purpose to identify which algorithm can be provided the best performance to encrypt and decrypt data. Four most common algorithms such as Blowfish, AES, DES and 3DES were conducted upon for evaluation. The respective algorithm contents and sizes of encrypting input files were changed and two different platforms were used to test them, i.e., P-II 266 MHz and P-4 2.4 GHz. According to the test results, the best performance is provided by the Blowfish algorithm has the ability to provide in compare to the other secret key algorithms.

In 2015, Nilesh Chaubey, Sanket A. Ubhad, and Prof. Shyam P. Dubey [3] proposed a special technique in which information is supposed to be sent as a collection of three keys over the network. Usually, every hacker tries to get access to the key used during the process of encryption. While enciphering the information, the authors preferred using a combination of word range and matrix multiplication. In 2015, A. Pandya etc [11] explain a unique methodology which uses both - encryption as well as data compression techniques. Firstly, the actual data size is reduced by implementing the data compression techniques and then the output gets encrypted with the purpose of raising its security. Hence, the technique proposed in this paper is very useful in reducing the data size, raising data transfer rate as well as providing more security during communication. In their proposed system, based on entropy encoding technique the encoded string is created from the input string composed of symbols and characters.

III. METHODOLOGY

In this paper, we have proposed an algorithm which takes in a message of any length along with a 4-digit key whose range is 0000 to 9999. After taking in the inputs, the message is encrypted. The cypher text generated is of the same length as that of the original text. Another encrypted message of the same length is also generated. In this algorithm, we treat this as another key that will be used during decryption of the message.

A. Encryption Process:

i. The user enters the message of length **n** to be encrypted.
ii. The user enters the key in the range 0000 – 9999. This value is denoted by '**K** [4]'.
iii. The message is treated as a string. It is converted into an array of characters. (**C** [0,1…, n]).
iv. Every character of the string is converted to its corresponding ASCII value. (**A** [0,1…, n]). i∈ [0, n).
v. For every C[i], the square root of the perfect square number closest to the ASCII value A[i] is calculated. (Q [0,1…, n]).
vi. For every C[i], the difference between corresponding A[i] and the square of Q[i] is calculated. (P [0,1…, n]).
vii. Similarly, the sum of Q[i] and P[i] is calculated. (R [0,1…, n]). It is then treated as the 1st part of the encrypted message.
viii. For every Q[i], the sum of Q[i] and the square of K[j] is calculated where j resets to 0 when j exceeds 3. (T [0,1…, n]). This array is regarded as the 2nd part of the encrypted message.

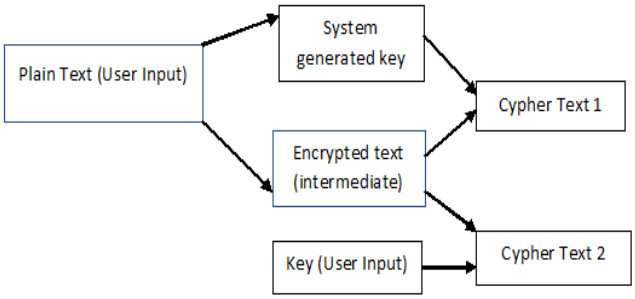
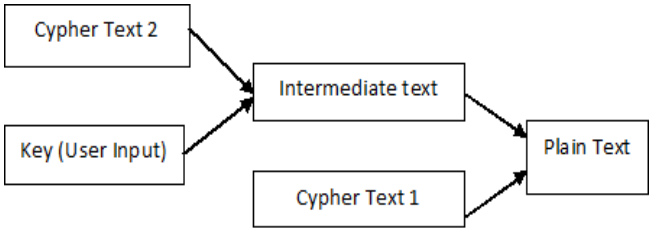


Fig 1: Block Diagram for Encryption process

B. Decryption Process:

i. 2nd part of the encrypted message, i.e., T [] is fetched first.
ii. For every T[i], the difference between T[i] and the square of K[j] is calculated where j resets to 0 when j exceeds 3. (D [0,1…, n]).
iii. Now 1st part of the encrypted message, i.e., R [] is fetched.
iv. For every R[i], the difference between R[i] and D[i] is calculated. (F [0,1…, n]).
v. For every F[i], the sum of D[i] and square of F[i] is calculated. (B [0,1…, n]).

vi. A character array (S [0,1…, n]) is generated such B[i] is the ASCII value of character S[i].
vii. The characters of S [] is then concatenated together and treated as a string.
viii. This string is the original message, restored after decryption.



Decryption Block Diagram
Fig 2: Block Diagram for Decryption process

IV. ILLUSTRATIVE EXAMPLE

Table-1: Encryption process for cipher text 1

Column 1	Column 2	Column 3	Column 4	Column 5
C	67	8	3	11
e	101	10	1	11
n	110	10	10	20
t	116	10	16	26
r	114	10	14	24
e	101	10	1	11

A. Encryption:
i. Let the message be: Centre. The second column in Table-1 shows the ASCII values for the given message.
ii. Now we break the ASCII value into 2 different parts. As square root of 67 is 8.18535277 we consider 8 to be one part and the other to be 67-82 i.e. 67-64=3.
iii. Step 2. Is followed for each and every character
iv. We Sum up the values of the 3rd and 4th column row-wise in Table-1. The resulting values are shown in the 5th column in Table-1.
v. The corresponding characters of the values in the 5th column in Table-1 are now stored into the database.
vi. Now we consider the values of the fourth column.
vii. The user is asked to provide a key of size 4. The range of the key starts from 0000 to 9999.
viii. For the above example, the key value is 4326.
ix. The values of the key are repeated as illustrated in Table-2.
x. Now we use the formula a2+b to obtain the 8th column in Table-2 where 'a' represents the value of the 7th column and 'b' represents the value in the 6th column of Table-2. These values are now stored in a memory device which resides with the user.

Table-2: Encryption process for cipher text 2

Column 6	Column 7	Column 8
3	4	19
1	3	10
10	2	14
16	6	52
14	4	30
1	3	10

Table-3: Decryption process for cipher text 2

Column 1	Column 2	Column 3
19	4	3
10	3	1
14	2	10
52	6	16

B. Decryption:
i. To decrypt the encrypted data, we now require the memory device along with the 4-digit pin that was provided at the time of encryption.
ii. The user is asked to provide a key of size 4. The range of the key starts from 0000 to 9999.
iii. For the above example, the key value is 4326.
iv. The values in the memory device are fetched and the characters are converted to their corresponding ASCII value. The values are shown in column 1 of Table-3.
v. The values of the key are repeated as illustrated in Table-3.
vi. Now we use the formula c - a2 to obtain the 3rd column in Table-3 where 'a' represents the value of the second column and 'c' represents the value in the first column of Table-3.
vii. The encrypted text is fetched from the database. The characters are converted to their corresponding ASCII value which is shown in column 4 of Table- 4.
viii. The values obtained in column 3 Table-3 is shown in column 5 Table-4.
ix. The values of column 5 are subtracted from values of column 4 in Table-4 to obtain column 6.
x. Now we use the formula a2+b where 'a' represents the value of column 6 and 'b' represents the value of column 5 in Table-4.
xi. The values that are obtained from step 10 are converted to the corresponding character. This results in column 7 which was the original message. e.g. 82+3=67, 67 is the ASCII value of 'C'.

Table-4: Decryption process for cipher text 1

Column 4	Column 5	Column 6	Column 7
11	3	8	C
11	1	10	e
20	10	10	n
26	16	10	t
24	14	10	r
11	1	10	e

V. RESULTS AND DISCUSSION

We have implemented our heuristic with Dev-C++ using 32-bit operating system and 2 GB RAM. The length of the generated cipher text is the same with the size of the plain text. After performing the decryption algorithm over the cipher text, the original message is generated. Here the output screenshot is presented to ensure the working of our theory for encryption and decryption both.

ENCRYPTION:
We have taken the message "Cryptography" as the plain text with the key value as 4326. The entire encryption process has been depicted in figure 3 and figure 4. The figure 3 is showing the output that we have received for generating cipher text 1 during the encryption process.
The figure 4 is showing the output that we have received for generating cipher text 2 during the encryption process.

DECRYPTION:
The whole decryption process has been presented in figure 5 and figure 6. The figure 5 is showing the steps of decryption for decrypting the cipher text 2.

C	67	8	3	11
r	114	10	14	24
y	121	11	0	11
p	112	10	12	22
t	116	10	16	26
o	111	10	11	21
g	103	10	3	13
r	114	10	14	24
a	97	9	16	25
p	112	10	12	22
h	104	10	4	14
y	121	11	0	11

Fig 3: Encryption process to generate cipher text 1

The figure 6 is showing the decryption process of cipher text 1 and output generated by figure 5 to create the original plain text.

3	4	19
14	3	23
0	2	4
12	6	48
16	4	32
11	3	20
3	2	7
14	6	50
16	4	32
12	3	21
4	2	8
0	6	36

Fig 4: Encryption process to generate cipher text 2

In the last column of the last image, we can see that the decrypted text is the same as the encrypted text.

The figure 7 is showing the decryption of the cipher text if the entered key is wrong.

VI. COMPLEXITY ANALYSIS

This program is working in linear time. In the above algorithm, we see that while encrypting the message three loops are used. Among these three loops, one loop has n/4 number of iterations and the other two loops have n number of iterations (where n is the string length). So, from this, we say that the time complexity to be O (n). The same thing also happens in the case of decryption algorithm and so the complexity is O (n).

19	4	3
23	3	14
4	2	0
48	6	12
32	4	16
20	3	11
7	2	3
50	6	14
32	4	16
21	3	12
8	2	4
36	6	0

Fig 5: Decryption process for cipher text 2

11	3	8	C
24	14	10	r
11	0	11	y
22	12	10	p
26	16	10	t
21	11	10	o
13	3	10	g
24	14	10	r
25	16	9	a
22	12	10	p
14	4	10	h
11	0	11	y

Fig 6: Decryption process for cipher text 1 and output generated by figure 5 to create the original plain text

11	-6	17	
24	-13	37	L
11	-60	71	u
22	12	10	p
26	7	19	p
21	-16	37	I
13	-57	70	Ù
24	14	10	r
25	7	18	K
22	-15	37	J
14	-56	70	ý
11	0	11	y

Fig 7: Decryption of cipher text with wrong Key

VII. CONCLUSION AND FUTURE SCOPE

This paper presents a novel technique with two-layered information security. Nowadays internet and network usage are increasing rapidly thus making it more necessary or rather a liability to ensure the safe transmission of data over various networks using various services. To safeguard the utilization of network and information various procedures have been undertaken. The main objective of the two-layered cryptography technique is that if one-layer security is hacked by the hackers, the hackers will not be able to hack the whole data as another layer security is untouched by the attackers. In this way, the security is being enhanced more in our heuristic than other existing procedures present in this field in linear time only. Our future work is looking forward to implementing a hardware-based application using this novel technique to set up a more secure environment for storage and transmission of data.

REFERENCES

[1] Diaa, S., E, Hatem M. A. K., & Mohiy M. H. (2010, May) Evaluating the Performance of Symmetric Encryption Algorithms. International Journal of Network Security, Vol.10, No.3, (pp.213-219).

[2] Sudipta Singha Roy, Kazi Md. Rokibul Alam, Md. Asaf- Uddowla, Shaikh Akib Shahriyar, and Yasuhiko Morimoto (2017). "A novel encryption model for text messages using delayed chaotic neural network and DNA cryptography".

[3] Stallings, W. (2006). Cryptography and network security: principles and practices. Pearson Education India.

[4] Deshpande, H. S., Karande, K. J., & Mulani, A. O. (2014, April). Efficient implementation of AES algorithm on FPGA. In Communications and Signal Processing (ICCSP), 2014 IEEE International Conference on (pp. 1895-1899).

[5] Sanket A. Ubhad, Prof. Nilesh Chaubey, Prof. Shyam P. Dubey (2015). "Advanced ASCII Based Cryptography Using Matrix Operation, Palindrome Range, Unique id".

[6] Nadeem, H (2006). "A performance comparison of data encryption algorithms", IEEE Information and Communication Technologies, (pp. 84-89).

[7] Samir A. El-Seoud and Hosam F. El-Sofany (2017). "Studying Security of Data in Cloud Computing through

[8] Rashmi Welekar and Deepti Chaudhary (2015). "Secure Authentication Using Visual Cryptography".

[9] Padate, R., & Patel, A. (2014). Encryption and decryption of text using AES algorithm. International Journal of Emerging Technology and Advanced Engineering, 4(5), 54-9.

[10] Kretzschmar, U. (2009). AES128–AC Implementation for Encryption and Decryption. TI-White Paper.

[11] Abhishek Pandya & Bobby Jasuja. (April 2015). Crypto-Compression System: An Integrated Approach using Stream Cipher Cryptography and Entropy Encoding

Authors Profile

Sourav Ghosh is pursuing B.Tech-CSE from JIS College of Engineering, Kalyani, W.B India. He has completed his 10th and 12thboard exams from Birla High School, Kolkata, W.B., India under C.B.S.E in the year 2015 and 2017 respectively. He finds interest in software development, network security. He has successfully filled an Indian Patent for his innovative projects.

Prithwijit Das is currently pursuing his B,Tech Degree in the field of Computer Science and Engineering from JIS College of Engineering, Kalyani, Nadia. He is an active member of the Computer Society of India (CSI) Student Chapter, JIS College of Engineering. He did a training on Embedded System and Robotics in the year 2018-19. He has interest in Internet of Things and Android Development.

Ira Nath has received her M.Tech degree in Software Engineering from the Maulana Abul Kalam Azad University of Technology, West Bengal, India (MAKAUT) in 2008 formerly West Bengal University of Technology (WBUT), India. She is currently pursuing her Ph.D in Computer Science & Technology at Indian Institute of Engineering Science and Technology (IIEST), Shibpur, India formerly Bengal Engineering and Science University (BESU)**,** Shibpur, India.. She is currently an assistant professor in the department of Computer Science & Engineering, JIS College of Engineering, Kalyani, Nadia. Her research interests include WDM optical Networks, Mobile Adhoc Network and network security. She is a life time member of CSI.

Mr Dharmpal Singh received his Bachelor of Computer Science and Engineering and Master of Computer Science and Engineering from West Bengal University of Technology. He has done his Ph.D in year 2015. He has about 12 years of experience in teaching

and research. At present, he is with JIS College of Engineering, Kalyani, and West Bengal, India as an Associate Professor and Head of the department. He has published 32 papers in referred journal and conferences index by Scopus, DBLP and Google Scholar and editorial team and senior member of many reputed journal index by SCI, Scopus, DBLP and Google Scholar. He has organized seven national levels Seminar/Workshop, published two patents and has applied for the AICTE Research Project (MRP) in year of 2019.

Sudipta Sahana is an assistant professor of a renowned engineering college of West Bengal. For more than 8 years, he has worked in this region. He has passed his M.Tech degree in Software Engineering and B.Tech Degree in Information Technology from West Bengal University of Technology with a great CGPA/DGPA on 2010 and 2012 respectively. He is recently working in Ph.D. in the domain of "Cloud Computing". He is a member of the Computer Science Teachers Association (CSTA), Computer Society of India (CSI) and also a member of International Association of Computer Science and Information Technology (IACSIT).

