Volume 3, Issue 8, August 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A New Combinational Approach Using Different Encryption Technique

Miss Somalina Chowdhury
Assistant Professor in Computer Application Department
Guru Nanak Institute of Technology under WBUT (West Bengal, India)

Abstract*— Security is the most important part of information exchange and data storage in any network. Especially in today's world when education, business and all other transaction are spreading over internet technology. As security is concern there is always a high demand for efficient and effective encryption algorithm. There are many predefined algorithms like AES, DES, IDEA, RSA etc. Some of them have even achieved popularity. But as the levels of security increases the time, speed and complexity also increase thus, reduces their efficiency. Here I have proposed a new algorithm NCADET (New Combinational Approach using Different Encryption Technique) which will be much simple to implement and hard to crack as well as give proper security to the information transferred. This paper is an attempt to provide a new encryption algorithm which is efficient and simple.

Keywords*— Encryption, Decryption, Information Security, Sender, Receiver, Random hash function, XOR, Multithreading, Bit Shifting, Substitution, Session key.

I. INTRODUCTION

Nowadays when business and other transactions are being conducted over internet to a large extent, inadequate or improper security can cause loss or even can create destruction. So, Security is the main concern here. Security in terms of confidentiality, integrity, authentication, non-repudiation, access control and availability is measured. Cryptographic algorithms and protocol are very useful to keep a network system secure considering the above parameters. As we know Cryptography is an art and science of providing information by transferring it into an unreadable format which can be only read by the expected receiver having secret key to break the message. Many work under cryptography is already been done but till a vast era is yet to explore. There are many algorithms which are simple but not efficient. Others are efficient but very complex to understand and implement .So here proposed an algorithm namely, ***NCADET*** which is a complete trade off, that is multilevel yet simple and comparatively faster than other multilevel approach. ***NCADET*** will be applied on different blocks of plain text and executes in parallel manner through multithreading concept. The details of the algorithms are mentioned below.

II. PROPOSED ALGORITHM : *NCADET*

A. Fundamental characteristics of the NCADET algorithm

1. It is a key exchange Block cipher algorithm.
2. Each block of plain text size 16 bytes.
3. Two different key matrix generated by sender and Receiver must be send to each other with the help of two different channels secretly.
4. Size of key matrix generated by sender and Receiver are 16 bytes each and their value is randomly generated by sender & receiver respectively.
5. The size of actual key matrix use for cryptography is 16 bytes which is obtained from both sender and receiver.

B. *The steps of the NCADET Encryption algorithm*

1. The plaintext (P) is partitioned into static block of size 16 bytes (or 128 bits) each. This block is represented by a 4x4matix (P_i).In this technique blank spaces in p are ignored during partition.
2. The main two diagonal of P_i are swapped to get first temporary encrypted text T_1.
3. Now, treat every letter in T_1 as a number .The letters of alphabet A to Z are assigned with numerical value 1 to 26 respectively, irrespective of cases. Digits 1 to 9 are assigned with numerical value 27 to 35 respectively and zero assigned by *. The resultant second temporary encrypted text is T_2.
4. The values of 4x4 key matrix (K) are to be calculated with the help of both sender and receiver.
   a) The sender at first will generate a 4x4 random matrix K_{Sender} .
   b) The receiver at will also generate another 4x4 random matrix $K_{Receiver}$.
   c) $K=(K_{Sende}+K_{Receiver})\%26$
   The size of the key matrix (k) is equivalent to the block size of Pi (i.e. 16 bytes).
   K= [k1, k2,……, k16] K= Random (0, 25, 16)
5. Calculate the new coded key matrix k_{new} using the following formulae: $k_{new} = K \bmod 2$
6. Calculate the Transpose matrix of T_2 to get next temporary encrypted text which is denoted by T_3.
7. Add both the matrices k_{new} and T_3 to get T_4 .

8. Shift first three rows horizontally of T_4 matrix such that shift one byte from first row, shift two byte from second row, shift three byte from third row and fourth row remains untouched (All shifts done in clock wise direction). The resultant matrix is denoted by T_5.
9. Shift first three columns vertically of T_5 matrix such that shift one byte from first column, shift two byte from second column, shift three byte from third column and fourth column remains untouched (All shifts done in clock wise direction). The resultant matrix is denoted by T_6.
10. Apply XOR to original key matrix (K) and T_6 to get T_7.
11. Again, apply mod 2 on T_7 to get a new matrix (C_{test}) for the Receiver to check in initial level whether the encrypted matrix received by him is proper or not. This C_{test} matrix is useful during decryption.
12. Replace numeric values of T_7 by their corresponding letters and if 36 exist in T_7, it is replaced by the special character #. The ultimate cipher text is C_i.

C. *Explanation of NCADET point by point*

Plain text (p) = my name is somalina. I like to start my day with a cup of coffee every day.

First 16 bit plaintext (P_i) = my name is somalina

m	y	n	a
m	e	i	s
s	o	m	a
l	i	n	a

Plain text=P_i

a	y	n	m
m	i	e	s
s	m	o	a
a	i	n	l

Swap diagonals of P_i=T_1

1	25	14	13
13	9	5	19
19	13	15	1
1	9	14	12

Substitute T_1 to number=T_2

52	5	70	69
13	23	4	24
38	35	88	21
34	62	13	70

Random key of sender (K_{Sender})

51	10	11	70
59	36	9	10
45	35	38	23
39	54	11	32

Random key of receiver ($K_{Receiver}$)

25	15	3	9
20	7	13	8
5	18	22	17
21	12	24	24

K= (K_{Sender} + $K_{Receiver}$) % 26

1	1	1	1
0	1	1	0
1	0	0	1
1	0	0	0

Kmod2=k_{new}

1	13	19	1
25	9	13	9
14	5	15	14
13	19	1	12

Transpose $T_2=T_3$

2	14	20	2
25	10	14	9
15	5	15	15
14	9	1	12

$k_{new}+T_3=T_4$

14	20	2	2
14	9	25	10
15	15	5	15
14	19	1	12

After ShiftingT_4 horizontally=T_5

14	15	1	2
15	19	5	10
14	20	25	15
14	9	2	12

After Shifting T_5 vertically=T_6

23	0	2	11
27	20	8	2
11	6	15	30
27	5	26	20

K XOR $T_6=T_7$

1	0	0	1
1	0	0	0
1	0	1	0
1	1	0	0

T_7 mod 2=C_{test}

w	*	b	k
1	t	h	b
k	f	o	4
1	e	z	t

Substitute T_7 to letters =C_i

First 16 bit cipher Text (C_i) = w*bk1thbkfo41ezt

The cipher text block (C_i), the random key generated by sender (K_{Sender}) and the test matrix (C_{test}) are sends to the recipient. At the receiver side the below stated algorithm is executed which is just the reverse of the above stated algorithm in order to decrypt the cipher text into plain text.

D. The steps of the decryption algorithm for the proposed encryption algorithm (NCADET)

1. At first we have to generate the actual key matrix. The values of 4x4 key matrix (K) are to be calculated with the help of both sender and receiver key value which are available to the receiver. K= (K_{Sender} + $K_{Receiver}$) % 26
2. Receiver will get T_7 from the 16 bit cipher Text (C_i) by substituting letters with respected number same as encryption algorithm.
3. Now receiver will calculate C_{test} matrix by applying mod 2 on T_7 to get receiver's C_{test} and compare with sender's C_{test} matrix to check authenticity.
4. Calculate T_7 from K XOR T_7 to get T_6.

5. Shift first three columns vertically of T_6 matrix such that shift one byte from first column, shift two byte from second column, shift three byte from third column and fourth column remains untouched (All shifts done in anti-clock wise direction). The resultant matrix is denoted by T_5.
6. Shift first three rows horizontally of T_5 matrix such that shift one byte from first row, shift two byte from second row, shift three byte from third row and fourth row remains untouched (All shifts done in anti-clock wise direction). The resultant matrix is denoted by T_4.
7. Calculate the new coded key matrix k_{new} using the following formulae: $k_{new} = K \bmod 2$
8. Subtract both the matrices k_{new} from T_4 to get T_3.
9. Calculate the Transpose matrix of T_3 to get T_2.
10. Replace numeric values of T_7 by their corresponding letters to get T_1.
11. The main two diagonal of T_1 are swapped to get 16 bit plaintext (P_i)

E. Details and efficiency advantages of NCADET

The above stated algorithm multilevel yet simple, efficient and effective it satisfies all the parameters of security. In this algorithm the Key is used to encrypt and decrypt are generated with the help of both sender and receiver, stated in Fig. 2. The key K used is a *session key* i.e. for each session or each block a new key is used which is very difficult or almost unable to hack thus it satisfies *confidentiality* of a message. It also uses hash functions to support *integrity* and *authenticity*. And the key exchange mechanism enlightened the non-repudiation and availability property. *Access control* is also assured since without proper key of receivers and senders both this algorithms won't work.

The above stated algorithm not only satisfies all the parameters of security but also no complex calculation still it is very secure because of random key selection process and key size is 128 bits which is hard to crack by intruders. It is executed with block wise parallel cryptographic model stated in Fig. 1 below.

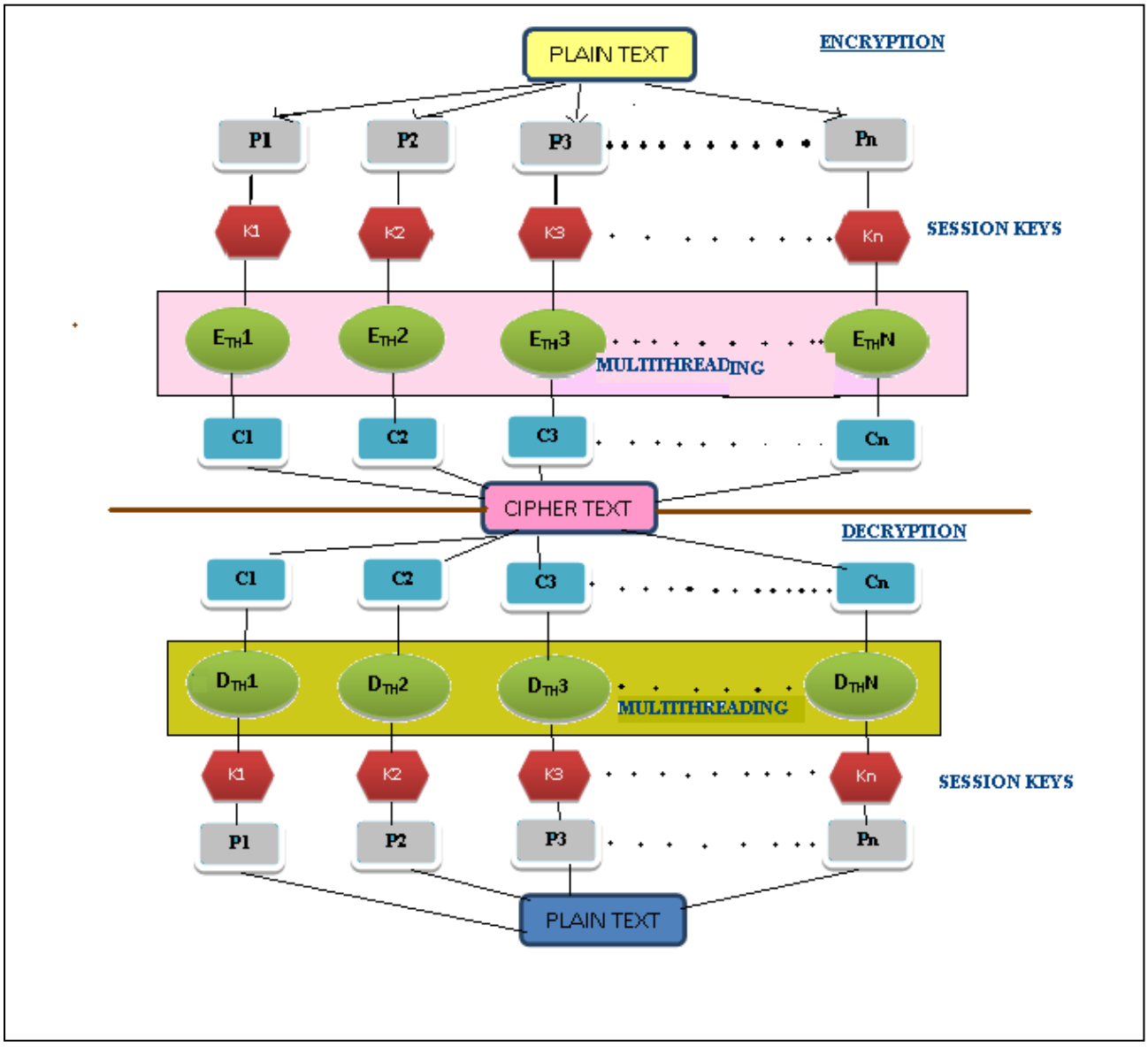

Fig. 1. Block wise parallel Encryption Decryption model of *NCADET*

There are many other advantage of these parallel system one of which the most striking feature is that it is platform independent design unlike most of the other existing systems. It is a combination of multilevel and multiple algorithms thus provide every levels of security that has been already stated before. In near future this also can apply to even media files. As the plain text is broken into blocks of 16 bytes and each of this bytes are subjected to the new sets of key and a new thread of *NCADET* algorithms thus supporting the session key concept as well as multithreading concept. This will use to implement pipeline or parallel execution in the system and also creates an modular approach towards the entire process. Multithreading also helps in speed up the process as thread takes less time to create, terminate, context switching as we know thread are the light weight processes that shares resources.

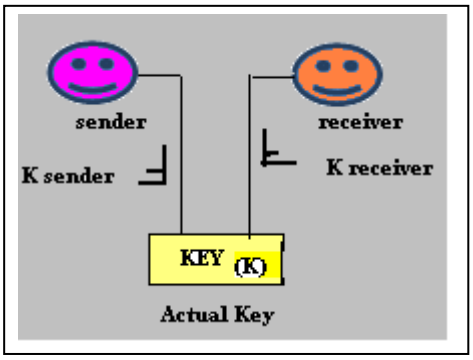

Fig. 2. Key generation for Encryption Decryption model of *NCADET with the help of both sender & receiver.*

III. Conclusion

There are many available algorithms in cryptography which are popular among masses but each have some benefits and some loop holes but here *NCADET* is proposed to create simple, efficient algorithms which has tries to remove almost all the loop holes. Here multilevel and multiple algorithm is combine to get a speedy, effective and efficient algorithm. In near future this algorithm will expected to be one of the most important and popular algorithm among people.

ACKNOWLEDGMENT

A special thanks to all those people who have encouraged me and guided me though out my journey.

REFERENCES

[1] W.Stallings,*Cryptography and Network Security: Principles and Practrices*, Prentice Hall, 1999.
[2] Sunita Bhati & Prof. S.K.Sharma,*Block Wise Parallel Encryption though Multithreading concept*, Research Paper Published in Aishwarya Research Communication Journal(ISSN : 09753613) Vol. 3, August 2011,pp.100-106.
[3] Himansu Gupta,*Multiphase Encryption Technique*, An Article, Amity University U.P.,March 2011.
[4] Sairam Natarajan #1,*A Novel Approach for data security Enhancement Using MultiLevel Encryption Scheme*,Research Paper,IJCSIT, Vol.2(1),2011, 469-473.
[5] Sunita Bhati, Anita Bhati,S.K. Sharma,*A New Approach towards Encryption Algorithm: BREA*, Research Paper Published in WCECS 2012,October 24-26,2012,San Francisco, USA.
[6] Yogesh Kumar,Rajiv Munjal,Harsh Shrma,*Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and counter measures*,IJCSMS,Vol.11,Issue 03,oct 2011.
[7] Vishwa Gupta, Gajendra Singh, Ravindra Gupta,*Advance Cryptography Algorithm for improving data Security*,IJARCSSE,vol. 2, Issue 1,January 2012.
[8] Atul Kahate,*Cryptography and Network Security*,*2nd Ed*.,Tata Megraw hill,2009.
[9] A.ath,S.Das,A.chakrabarti, *Data Hiding and Retrival*, Proceedings of IEEE International conference on Computer Intelligence and computer Network held at Bhopal from 26-28 Nov,2010.

AUTHOR BIOGRAPHY

Obtained her MCA degree in 2011 from Department of Computer Application in Guru Nanak Institute of Technology, Sodepur affiliated under West Bengal University of Technology. At presently working as Assistant Professor in the same institution. Area of working interest is Network Security, Cryptography and Wireless Sensor Network.

