International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 11 (2018) pp. 9916-9923

Design and Implementation of Information Security using Neural Network Architecture

Kushal Karmakar[1], Soumik Kundu[2], Soumya Paul[3]

[1]*Student, Master of Computer Application,*

[2]*Student, Master of Computer Application,*

[3]*Associate Professor and Head Department of Computer Application,*

[1,2,3]*B.P. Poddar Institute of Management & Technology, Kolkata, West Bengal, 700052, India.*

Abstract

Internet is growing day by day with its uses. So it is needed to design and implement the new algorithms to make more secure communication every time. The main aim of this paper is to secure the data transmission using symmetric key cryptography with the help of neural network architecture supporting Multilayer Feed forward Network. Here a random key is generated based on the length of the plaintext and is applied to the message to convert it to the cipher text , which is further coded with the hidden layers of neural network to make the final cipher text more secured .In decryption process the cipher text is decrypted with the help of private key at receiver end and the original text is received.

Keywords: Cryptography, Neural Network Architecture, Network Security, Symmetric key

INTRODUCTION

NETWORK SECURITY

Network security consists of the provisions and policies to prevent and monitor unauthorized access, misuse, modification or denial of a computer network and network-accessible resource. Network Security involves the authorization of access to data in a network, which is controlled by the network administrator. Users are assigned a password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday's transactions and communications among business, government agencies and individual.

CRYPTOGRAPHY

Cryptography a word with Greek origin means "secret writing". Cryptography is a measure of providing security to the information from unauthorized access. The messages to be encrypted (plain text) are transformed by a function (key) and the output of the encryption process (cipher text) is then transmitted to the destination end. This messages then decrypted by the key to get back the original message.

SYMMETRIC KEY ENCIPHERMENT

Symmetric key encipherment uses a single key for both encryption and decryption. In symmetric key algorithm, two or more parties in source and destination end share the same secret key.

NEURAL NETWORK ARCHITECTURE: An Artificial Neural Network is a data processing system consisting of a large number of highly inters connected arterial neurons. The Neural Networks exhibit mapping capabilities and can process information in parallel, at high speed and in a distributed manner.

RELATED WORK

1 Proposed the concept of transferring the encrypted message by validating user identity by users image in database. The message is further validated by finger print and MD5 hash which enhances the security. [1]

2 Focused on cryptography and security in communicators, wireless and IP network security, as well as optical network security, quantum cryptography and quantum-key distribution processes specific to optical networks is discussed. [2]

3 Highlighted a software simulation version via MS. C#2013.NET of RSA cryptosystem, the simulation was tested for 32 bit encryption and decryption keys. It has been observed that the message should be limited to the range of the modules. The simulation results showed the comparable delay for encryption decryption process.[3]

4 Presented an enhanced security model by designing and implementing an encryption standard file encryption to track message along the transition path. It has been noted that the

proposed model was implemented by codifying a Timing Circuit Algorithm and Feedback Artificial Agent, which monitors the information on transition.[4]

5 Explained the importance of cryptography and highlighted several security issues of the communication channel using private key cryptography. It has been observed that the proposed method generated a reliable connection and increases confidentialities of messages. [5]

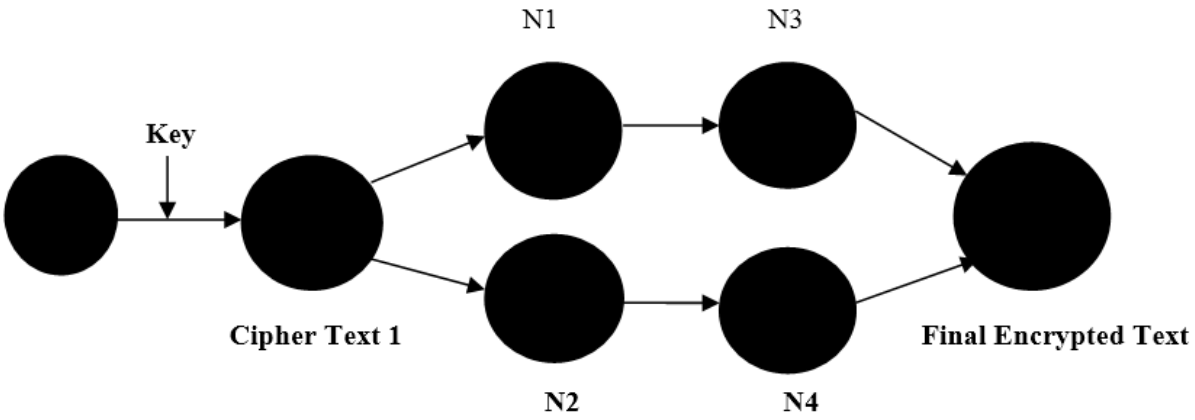


Figure 1. Encryption Flow Diagram

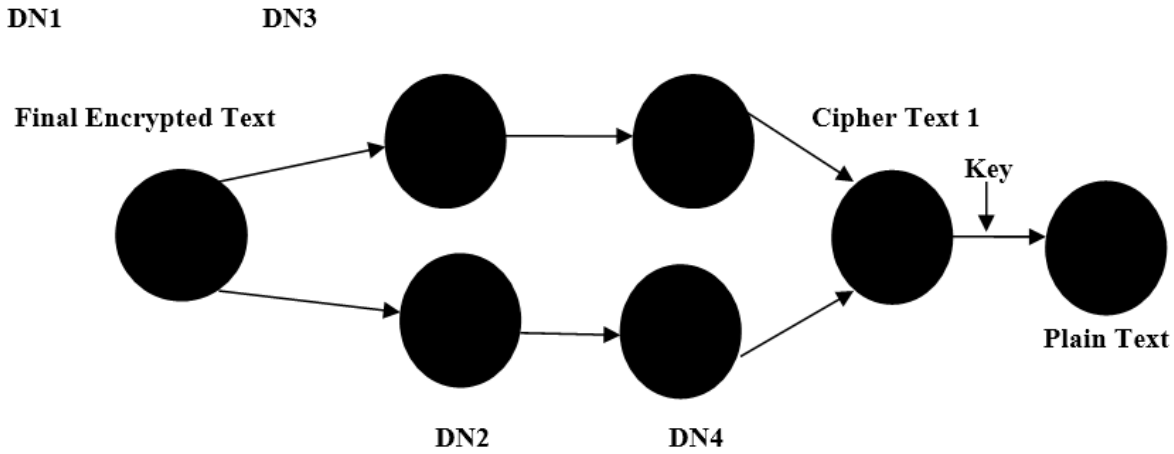


Figure 2. Decryption Flow Diagram

ALORITHMS

ALGORITHM FOR ENCRYPTION AND DECRYPTION

Input: A plain text is taken an input from user end.

Step 1. Call the algorithm for key generation. // Algorithm 4.2

Step 2. Call encryption algorithm E1. // Algorithm 4.3

Step 3. Cipher text is generated.

Step 4. Call decryption algorithm D1. // Algorithm 4.4

Step 5. Plain text is received at destination.

Step 6. Stop.

ALGORITHM FOR KEY GENERATION

Step 1. Start

Step 2. Calculate the length of the text

Step 3. XOR the length of the text with the positional value of each letter of the plain text according to the ASCII value.

Step 4. Write the corresponding ASCII value.

Step 5. Stop.

ALGORITHM FOR ENCRYPTION E1

Step 1. Start

Step 2. Apply the key with the plain text alternatively.

Step 3. Split the array in two halves, as node 1 and node 2 respectively.

Step 4. Take another array with the same length of cipher text 1 having the elements of prime numbers starting from 2. Then add the first half of the array of prime numbers with node 1 and subtract the rest from node 2. And generate Node3 and Node 4 respectively.

Step 5. Concat node 3 and node 4 into node 5 and convert array according to the ASCII value to get the final encrypted text.

Step 6. Stop.

ALGORITHM FOR DECRYPTION D1

Step 1. Start

Step 2. Covert the text according to the ASCII value first.

Step 3. Split the array in two halves, as D_Node 1 and D_Node 2 respectively.

Step 4. Subtract the first half of the prime numbers from D_Node1 and add the rest with D_Node 2. The results of the calculation give us D_Node3 and D_Node 4.

Step 5. Concat D_Node 3 and D_Node 4 into D_Node 5.

Step 6. Pick the alternate values from D_Node 5 and put them in different array and convert the values according to their ASCII value

Step 7. After conversion the key and the plain the first are retrieved in the first array and second array respectively. .

Step 8. Stop.

EXAMPLE ILLUSTRATION

Key Generation:

Choose a message"KUSHAL"

Write the ASCII value of each position of alphabets of Text.

K	U	S	H	A	L
75	85	83	72	65	76

Xor the length of the text with the value of each letter of the input text according to the ASCII value.

K	U	S	H	A	L
75	85	83	72	65	76
6	6	6	6	6	6
77	83	85	78	71	74
M	S	U	N	G	J

Encryption:

Key = "MSUNGJ"

Write the ASCII value of each position of alphabets of Key.

M	S	U	N	G	J
77	83	85	78	71	74

Plain text and Key are arranged alternatively to generate the Cipher text.

K	M	U	S	S	U	H	N	A	G	L	J

Split the array in two halves which generates node 1 and node 2 respectively.

Node 1:

K	M	U	S	S	U

75	77	85	83	83	85

Node 2:

H	N	A	G	L	J

72	78	65	71	76	74

Take another array with the same length of cipher text having the elements of prime numbers starting from 2.

0	1	2	3	4	5	6	7	8	9	10	11
2	3	5	7	11	13	17	19	23	29	31	37

Add the first half of the array of prime numbers with node 1

Node 3:

77	80	90	90	94	98

Subtract the rest from node 2.

Node 4:

55	59	42	42	45	37

Concentration of node 3 and node 4 generates node 5.

Node 5:

77	**80**	**90**	**90**	**94**	**98**	**55**	**59**	**42**	**42**	**45**	**37**

M	**P**	**Z**	**Z**	**^**	**b**	**7**	**;**	*****	*****	**-**	**%**

The final encrypted text is obtained as :

"MPZZ^b7;-%"**

Decryption:

77	**80**	**90**	**90**	**94**	**98**	**55**	**59**	**42**	**42**	**45**	**37**

M	**P**	**Z**	**Z**	**^**	**b**	**7**	**;**	*****	*****	**-**	**%**

Split the array in two halves, as D_Node 1 and D_Node 2 respectively.

D_Node 1:

77	**80**	**90**	**90**	**94**	**98**

D_Node 2:

55	**59**	**42**	**42**	**45**	**37**

Subtract the first half of the prime numbers from D_Node1

D_Node 3:

75	**77**	**85**	**83**	**83**	**85**

Add the rest with D_Node 2.

D_Node 4:

72	**78**	**65**	**71**	**76**	**74**

Concatenation of D_Node 3 and D_Node 4 generates D_Node 5.

D_Node 5:

75	**77**	**85**	**83**	**83**	**85**	**72**	**78**	**65**	**71**	**76**	**74**

Values in the node 5 are converted corresponding ASCII values

Plain Text:

75	**85**	**83**	**72**	**65**	**76**

K	**U**	**S**	**H**	**A**	**L**

Key:

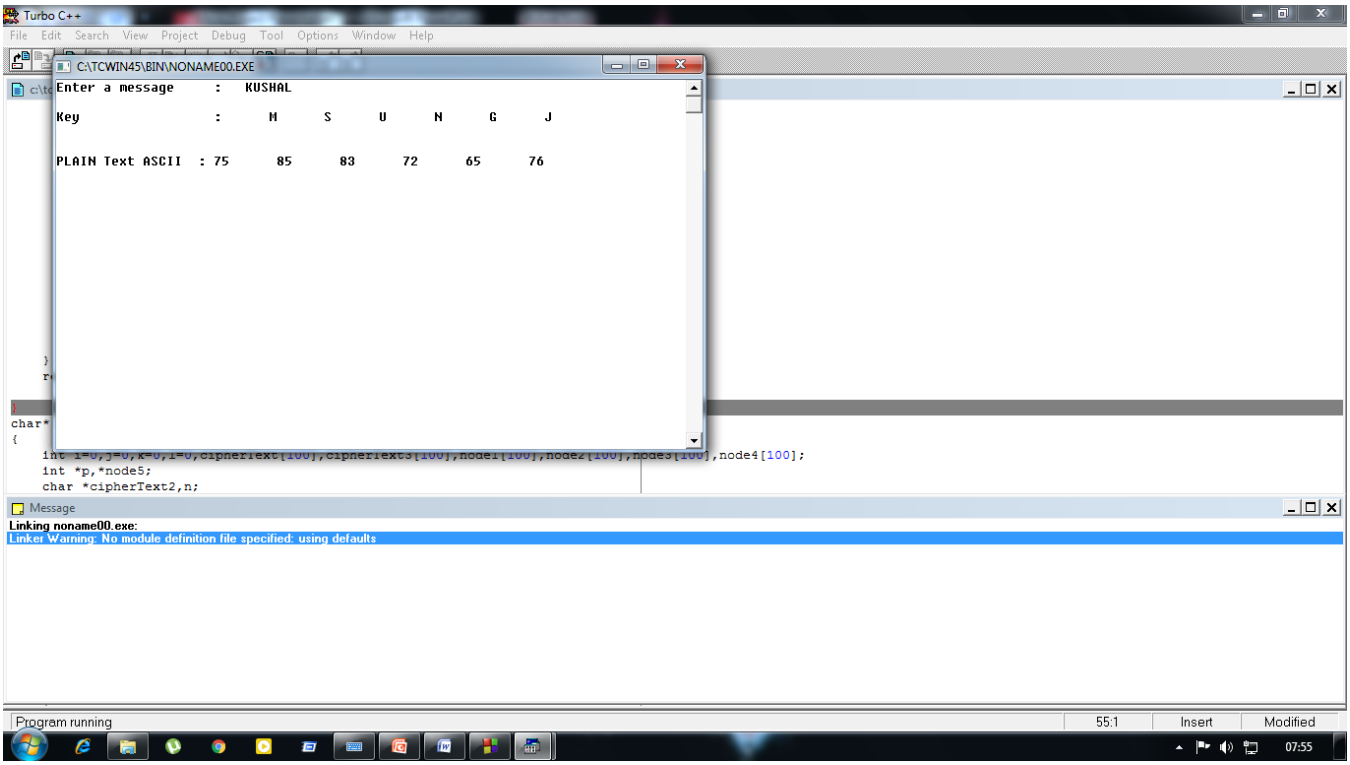
77	**83**	**85**	**78**	**71**	**74**

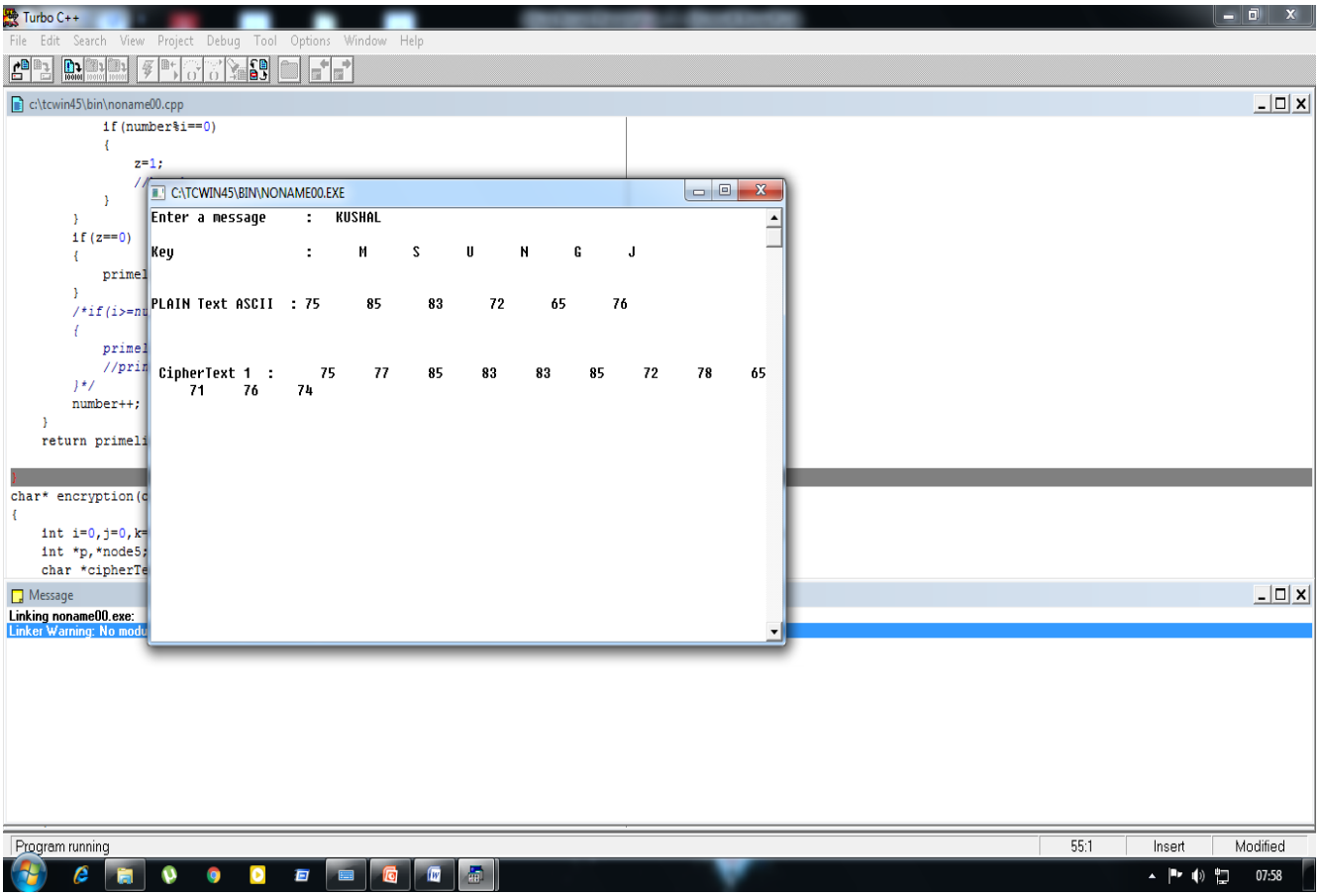
M	**S**	**U**	**N**	**G**	**J**

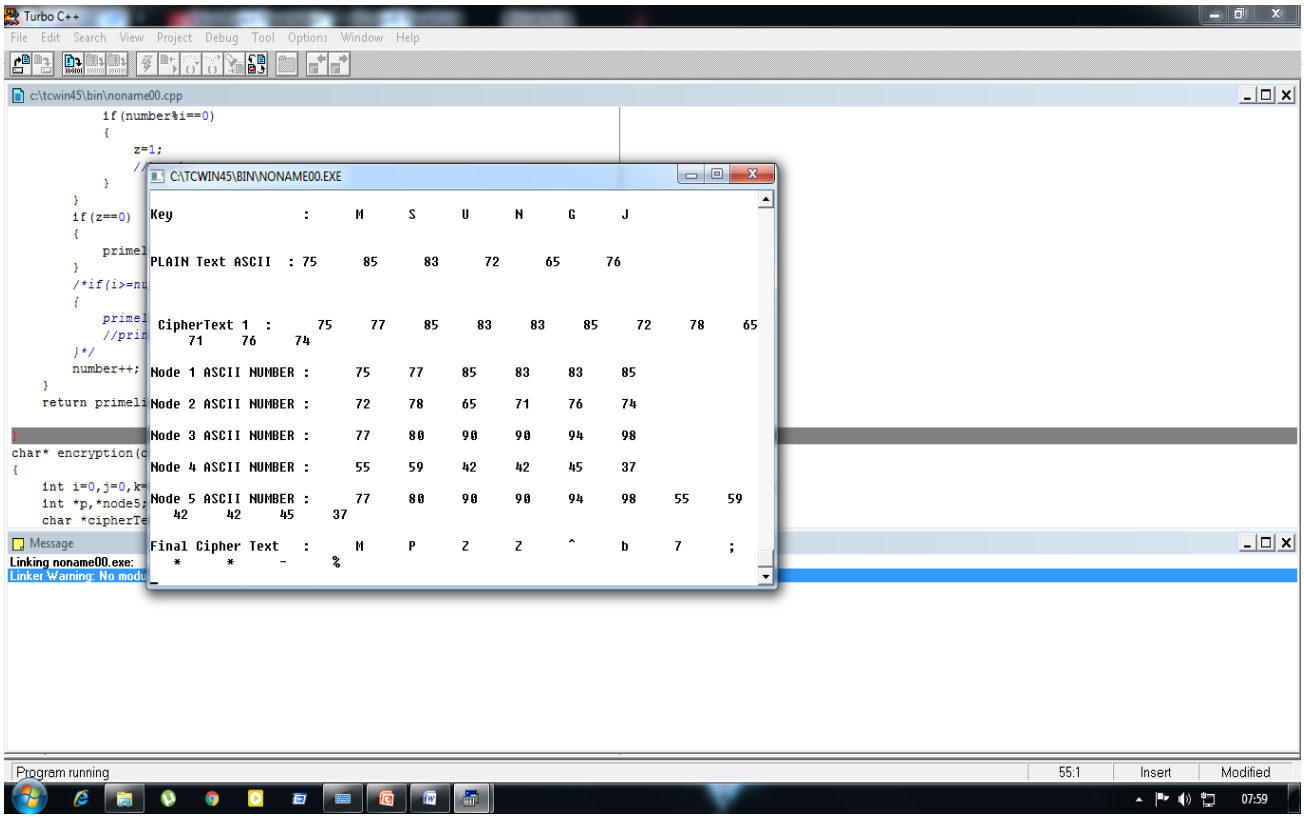
Finally plain text and key are obtained as:

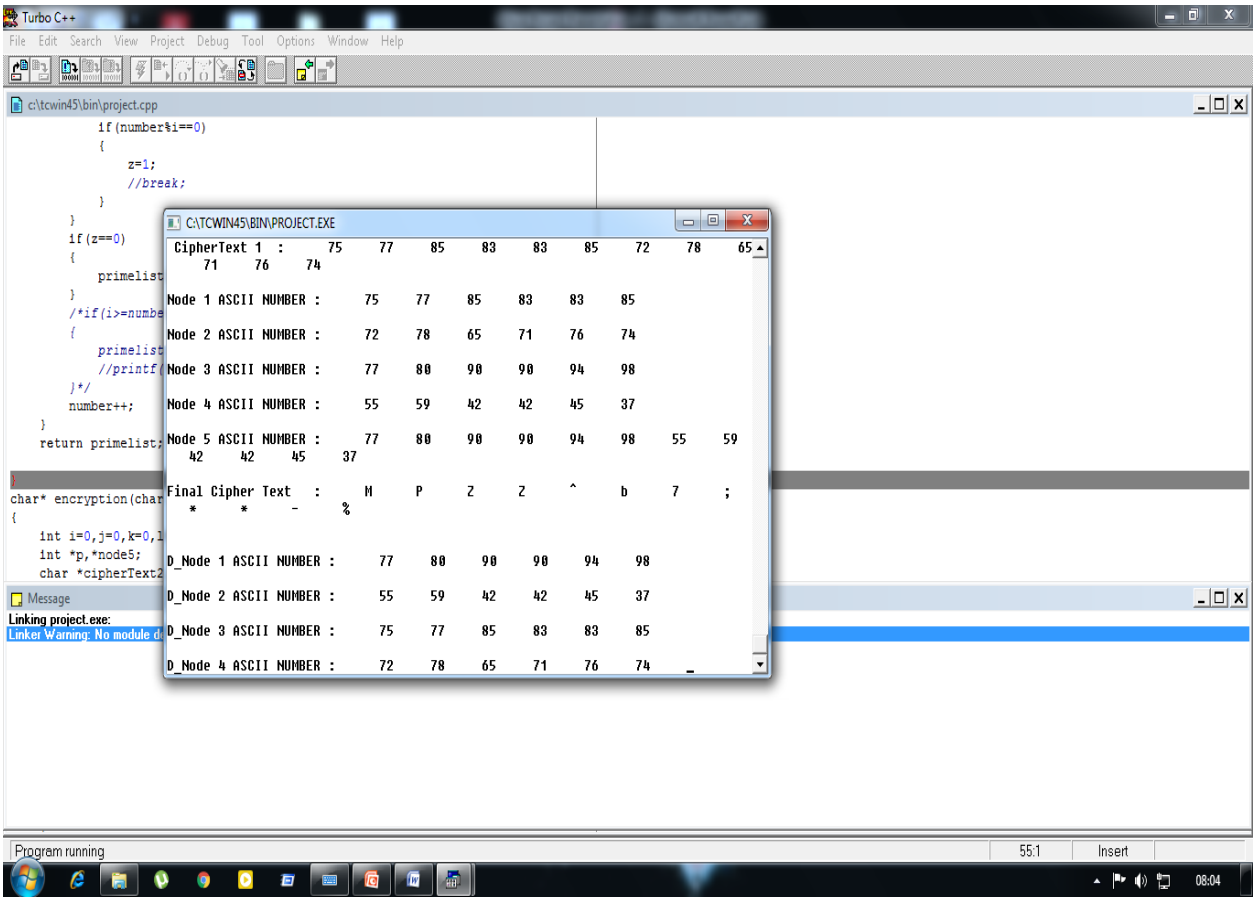
KUSHAL MSUNGJ respectively.

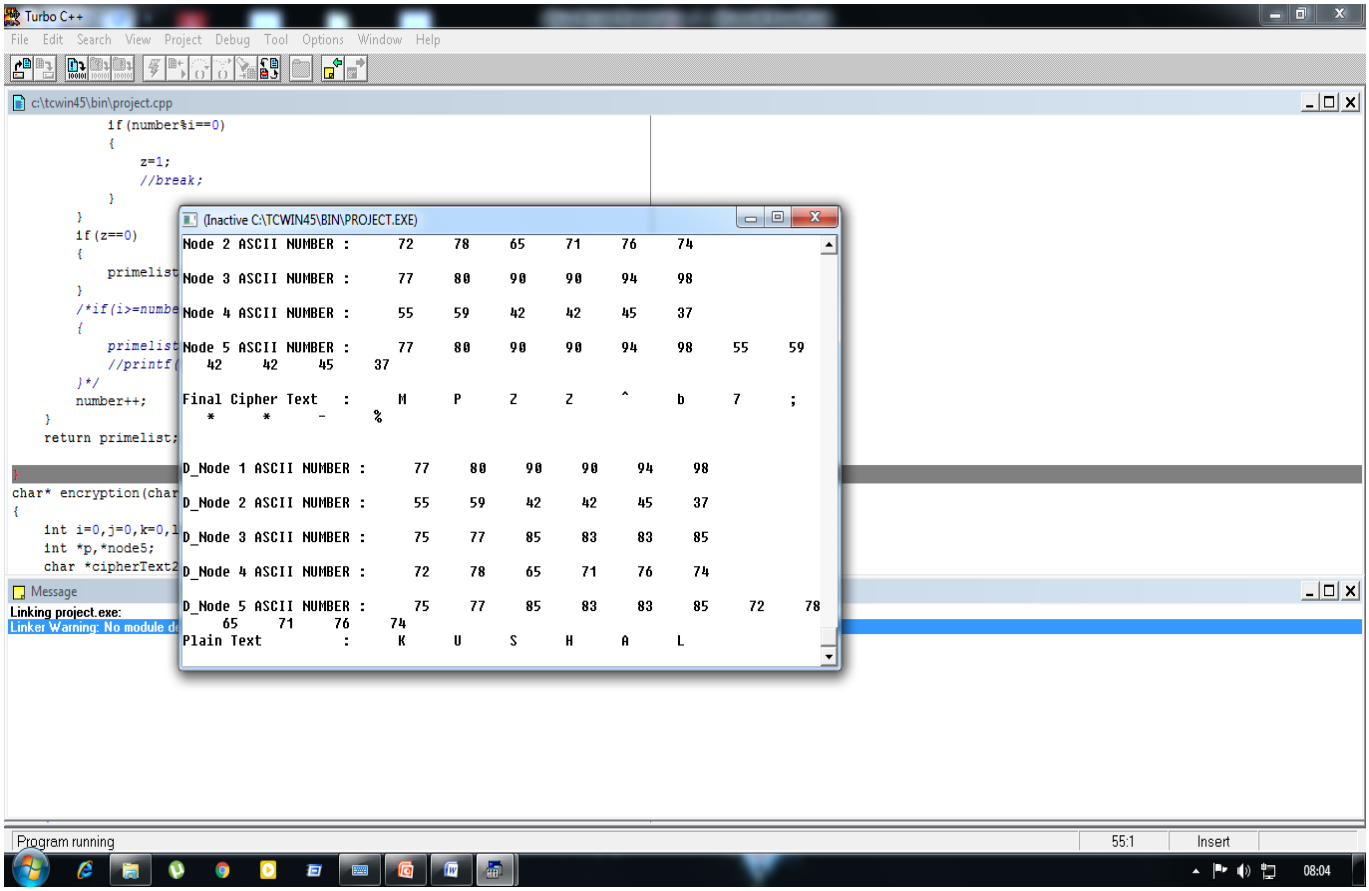
SAMPLE OUTPUT






Turbo C++
File Edit Search View Project Debug Tool Options Window Help
c:\tcwin45\bin\noname00.cpp
C:\TCWIN45\BIN\NONAME00.EXE
Key : M S U N G J
PLAIN Text ASCII : 75 85 83 72 65 76
CipherText 1 : 75 77 85 83 83 85 72 78 65
71 76 74
Node 1 ASCII NUMBER : 75 77 85 83 83 85
Node 2 ASCII NUMBER : 72 78 65 71 76 74
Node 3 ASCII NUMBER : 77 80 90 90 94 98
Node 4 ASCII NUMBER : 55 59 42 42 45 37
Node 5 ASCII NUMBER : 77 80 90 90 94 98 55 59
42 42 45 37
Final Cipher Text : M P Z Z ^ b 7 ;
* * - %
Message
Linking noname00.exe:
Program running
55:1
Insert
Modified
07:59


Turbo C++
File Edit Search View Project Debug Tool Options Window Help
c:\tcwin45\bin\project.cpp
C:\TCWIN45\BIN\PROJECT.EXE
CipherText 1 : 75 77 85 83 83 85 72 78 65
71 76 74
Node 1 ASCII NUMBER : 75 77 85 83 83 85
Node 2 ASCII NUMBER : 72 78 65 71 76 74
Node 3 ASCII NUMBER : 77 80 90 90 94 98
Node 4 ASCII NUMBER : 55 59 42 42 45 37
Node 5 ASCII NUMBER : 77 80 90 90 94 98 55 59
42 42 45 37
Final Cipher Text : M P Z Z ^ b 7 ;
* * - %
D_Node 1 ASCII NUMBER : 77 80 90 90 94 98
D_Node 2 ASCII NUMBER : 55 59 42 42 45 37
D_Node 3 ASCII NUMBER : 75 77 85 83 83 85
D_Node 4 ASCII NUMBER : 72 78 65 71 76 74
Message
Linking project.exe:
Program running
55:1
Insert
08:04



CONCLUSION

In conclusion, the confidentiality of a message that is to be transferred by network is maintained. The proposed algorithm has been designed and implemented using symmetric key cryptography with neural network architecture, which ensures information security with private key in communication channel. A Multilayer Feed Forward Network has been implemented which supports message transfer in end to end manner.

REFERENCES

[1] Khushbu Soni , Shashi Sharma , Nagendra Kumar Sutilya, 2017 "Encrypted Image Message sending using Triple DES with Finger Print and MD5", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 6, Issue 9.

[2] Subhrajit Mondal, Tania Khatun Mollah, Arindam Samanta, Soumya Paul , 2016 "A Survey on Network Security Using Genetic Algorithm ", International Journal of Innovative Research in Science, Engineering and Technology(A High Impact Factor, Monthly Peer Reviewed Journal)Vol. 5, Issue 1.

[3] Hasan Al-Qadeeb, Qasem Abu Al-Haija and Noor A. Jebril, 2017 "Software Simulation of Variable Size Message Encryption Based RSA CryptoAlgorithm Using Ms. C#. NET", International Journal of Cyber-Security and Digital Forensics (IJCSDF) 6(1): 35-43 35 The Society of Digital Information and Wireless Communications (SDIWC), ISSN: 2305-0012

[4] A.O. Isah, J.K Alhassan, S.S Olanrewaju, Enesi Femi Aminu, 2017 "Enhancing AES with Time-Bound and Feedback Artificial Agent Algorithms for Security and Tracking of Multimedia Data on Transition", International Journal of Cyber-Security and Digital Forensics (IJCSDF) 6(4): 162-178 162 The Society of Digital Information and Wireless Communications (SDIWC), ISSN: 2305-0012.

[5] NehaTyagi, Ashish Agarwal, Anurag Katiyar, Shubham Garg, Shudhanshu Yadav, 2017 "Methods for Protection of Key in Private Key Cryptography", International Journal of Innovative Research in Computer Science & Technology (IJIRCST), Volume-5, Issue-2.

[6] K.Thamodaran , 2015 "Optimized Data Encryption System Based on GA", SSRG International Journal of Computer Science and Engineering (SSRG-IJCSE) – volume 2 issue 9.

[7] L.M.R.J Lobo, Suhas B. Chavan, 2012 "Use of Genetic Algorithm in Network Security"

International Journal of Computer Applications (0975 – 8887) Volume 53– No.8, September.

[8] Swarnendu Mukherjee, Debashis Ganguly and Somnath Naskar, 2009 "A New Generation Cryptographic Technique", International Journal of Computer Theory and Engineering, Volume. 1, No. 3.

[9] Sameer Hasan Al-Bakri, M. L. Mat Kiah, A. A. Zaidan, B. B. Zaidan and Gazi Mahabubul Alam, 2011 "Securing peer-to-peer mobile communications using public key cryptography: New security strategy", International Journal of the Physical Sciences Volume. 6, No.4, pp. 930-938.

[10] Challa Narasimham, Jayaram Pradhan, 2008 "Evaluation of Performance Characteristics of Cryptosystem Using Text Files", Journal of Theoretical and Applied Information Technology.

[11] Mina Mishra & V. H. Mankar, 2011 "Review on Chaotic Sequences Based Cryptography and Cryptanalysis", International Journal of Electronics Engineering, Volume.3, No.2, pp. 189– 194.

[12] Somalina Chowdhury, Sisir Kumar Das, Annapurna Das , 2015" Application of Genetic Algorithm in Communication Network Security", International Journal of Innovative Research in Computer and Communication Engineering(An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 1.

[13] Soumya Paul , Sudipto Bhattacharyya 2015 "Implementation of Network Security Using Neural Network Architecture" IJCSMC, Vol. 4, Issue. 6

[14] Ashvini Jangam, Prof. Nilesh Sable," 2018 Data Security Scheme: Share and Audit Our Data into Cloud using Encryption", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 7, Issue 3.