iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** VI **Month of publication:** June 2018

DOI: http://doi.org/10.22214/ijraset.2018.6155

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue VI, June 2018- Available at www.ijraset.com

Implementation of Cipher text Generation Algorithm using ASCII Values

Charu Bathla[1],Kuldeep Kumar[2]
[1,2]*Assistant Professor*
[1]*Department of Computer Science Engg.Jan NayakChaudharyDeviLal Memorial College Of Engg.,Sirsa*
[2]*Department of Computer Science Applications, ChaudharyDeviLal University (CDLU),Sirsa*

Abstract: Network security is protection of the vulnerability of files and directories in a computer network from hackers, crackers and intruders etc.It is a major issue in Network Communication.Cryptography is a solution for the secure network communication.The purpose of this paper is to introduce and demonstrate a new algorithm for network security. The proposed algorithm is based on ASCII values of the input message which is to be encrypted. Firstly it fetches the ASCII values of the characters of the string and then computes the string length by counting the number of digits in ASCII values of each character. It performs some calculation on this string length and in such a way it generates the cipher key.
Keywords: ASCII, Cryptography, Network security, Ciphertext,String Length

I.INTRODUCTION

Cryptography or cryptology; from Greek meaning “hidden, secret”; and “writing”, or “study” respectively; is the practice and study of techniques for secure communication in the presence of third parties called adversaries. More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity, and authentication. Modern Cryptography intersects the disciplines of mathematics , computer science and electrical engineering. Applications of cryptography include ATM cards, computer passwords and electronic commerce.[1]

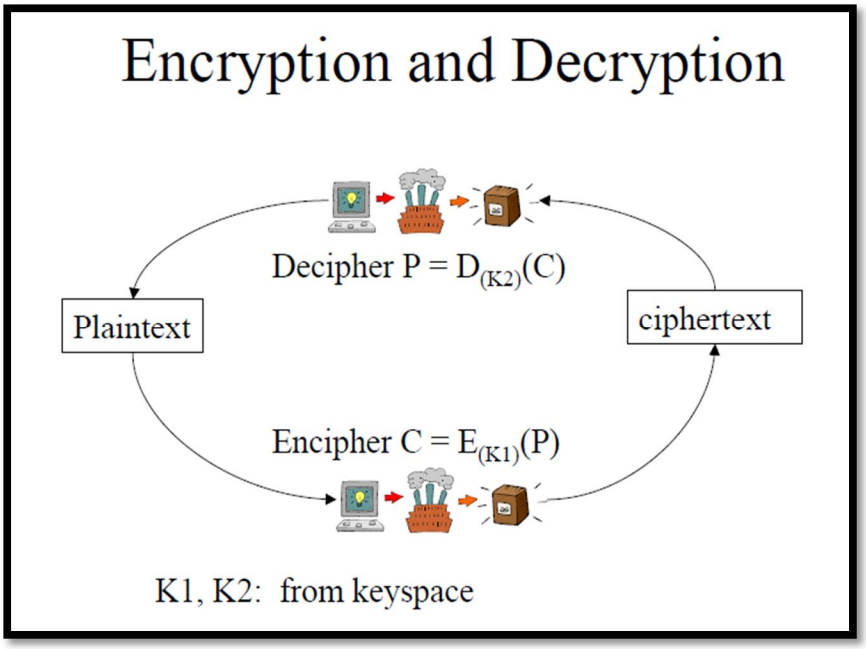


Fig. No. 1: Components of Cryptography

The original information to be hidden is called "plaintext". Plaintext is converted into ciphertext by means of an encryption engine whose operation is fixed and determinate (the encryption method), but which functions in practice in a way dependent on a piece of information (theencryption key) which has a major effect onthe output of the encryption process [2].

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue VI, June 2018- Available at www.ijraset.com

Encryption is the process of applying special mathematical algorithms and keys to transform digital data into cipher code before they are transmitted and decryption involves the application of mathematical algorithms and keys to get back the original data from cipher code. The encryption can be performed either using Symmetric key cryptography or by using Asymmetric key cryptography.

II.RELATED WORK

Udepal Singh and UpasnaGarg have proposed an algorithm for encryption and decryption which is based on Symmetric Key generation. This algorithm uses ASCII values for key generation and it generates 4-character key. Thesystem can be improved by using variable length key. System can be made to encrypt the data on basis of Unicode values [1]Khamg A.I. and Ramli A.R.have implemented cryptography technique for E-mails. The problem of time execution and the authentication between sender and receiver are considered in this study. New Technique is based on both Symmetric Key and Asymmetric Key. It is a powerful tool in protecting the e-mail privacy. This algorithm can be developed for encryption of image files [2].Ruchika Gupta and Pallavi Sharma have developed an algorithm for cryptography. It provides GUI which helps the students and users to try various inputs and see how the plain text is converted into encrypted text.This algorithm runs as a desktop application.In the future, it can be developed as a server-based application [3].AryaSuraj has implemented Two Layers Based Uniform Encryption Decryption Algorithm (TLBUED). Two layers based encryption decryption Techniqueexecutes encryption process in two steps. These steps further divided in two layers. First layer take Input message and convert character by character as per symbol table. The second layer is used for uniformity purpose for the encryption of messages and uses first level conversion as input and provides the special character according to input which makes the encrypted message uniform. [9]

III.RESEARCH METHODOLOGY

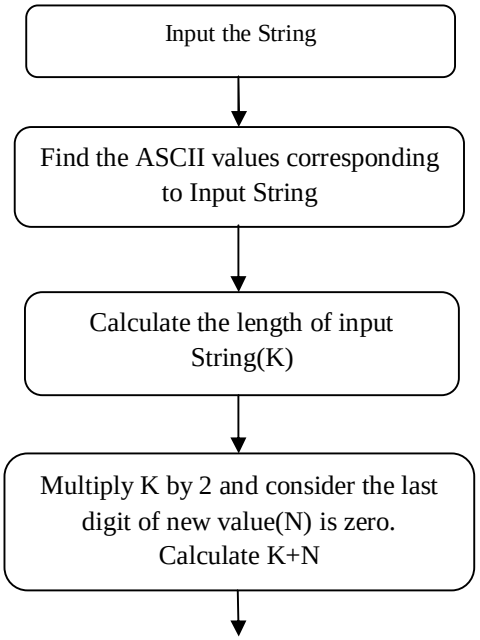
A. Experimental Setup

This algorithm is implemented in PHP language. It is a general purpose language but it is mainly designed for web development. It is a server side scripting language.It is easy to understand.It is a cross platform language.

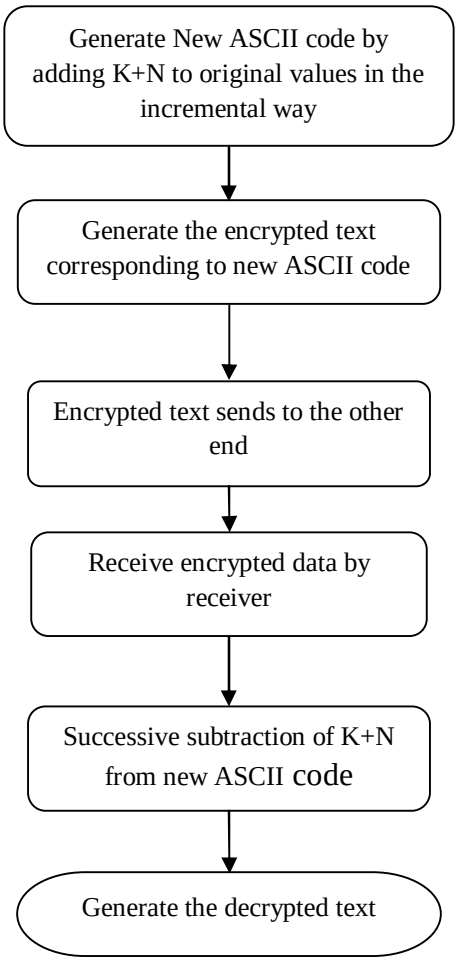
B. Procedure of Algorithms

I have implemented two techniques which are based on ASCII values of the input string.These techniques generate random key when the message is inputted. These techniques firstly find the ASCII values of letters and blank spaces in the input message. After that it will compute the string length by counting the number of digits in the ASCII values of input string. Then it will perform some computations on it and in this way, it generates the encrypted text.There is difference between the numeric operations (which are performed on String length) of these two techniques.

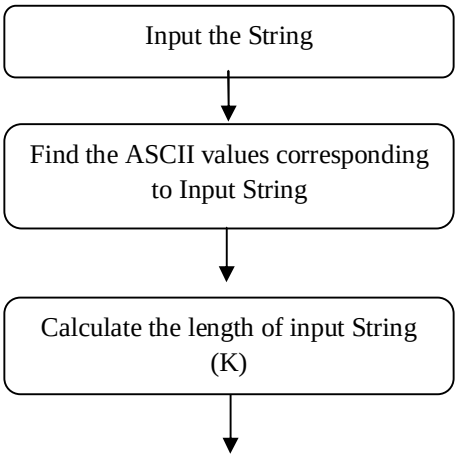
Flowchart for Technique-1: Encryption Process

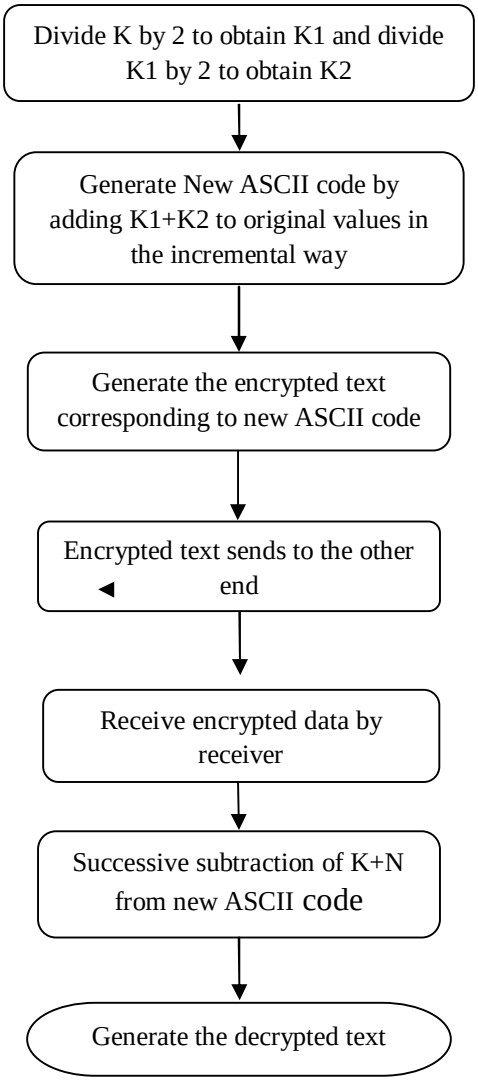


ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue VI, June 2018- Available at www.ijraset.com



Flowchart for Technique 2: Encryption process





IV.EXPERIMENTAL RESULTS

The experiments are carried out by giving various inputs of different sizes. ASCII values of input string are fetched and then perform the encryption. This algorithm is implemented in PHP language. Wamp server and windows OS complete the execution environment.

A. Technique-1

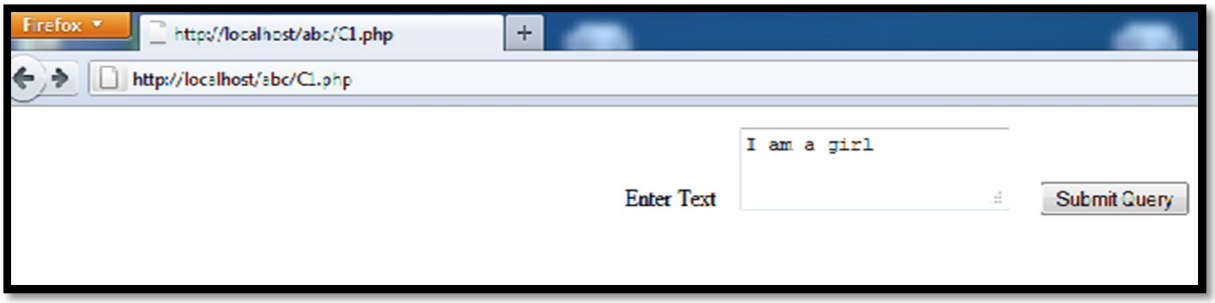


Fig. No. 2: Plain Text as Input

Fig 2 and 3 shows the complete process of Encryption to generate the cipher text as described in earlier sections.

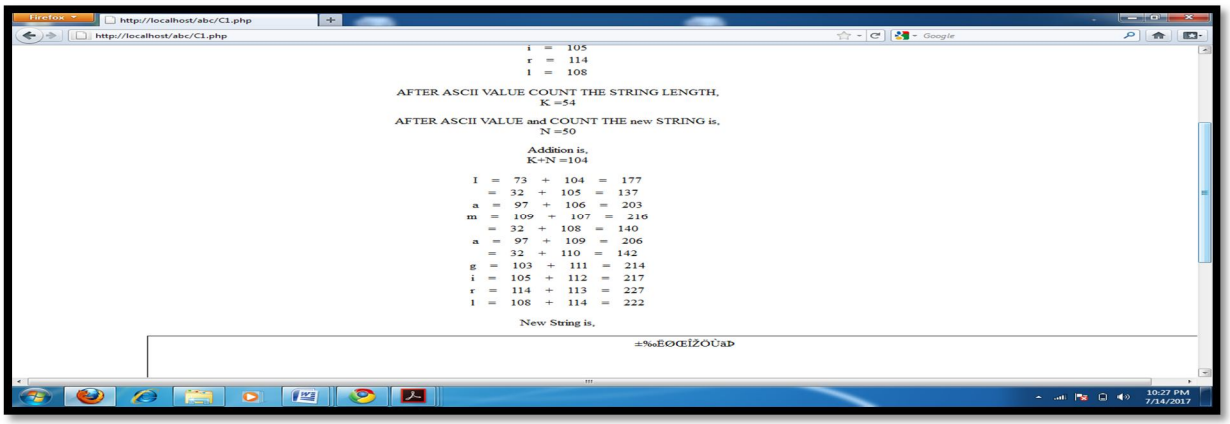


Fig. No. 3: Encryption process

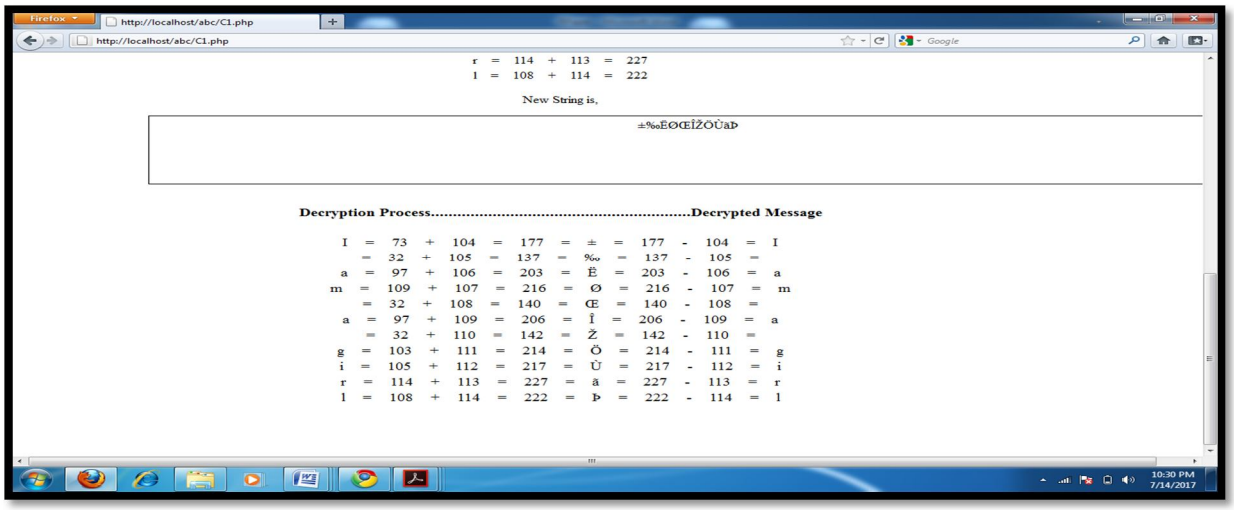


Fig. No. 4: Decryption process

B. Technique-2

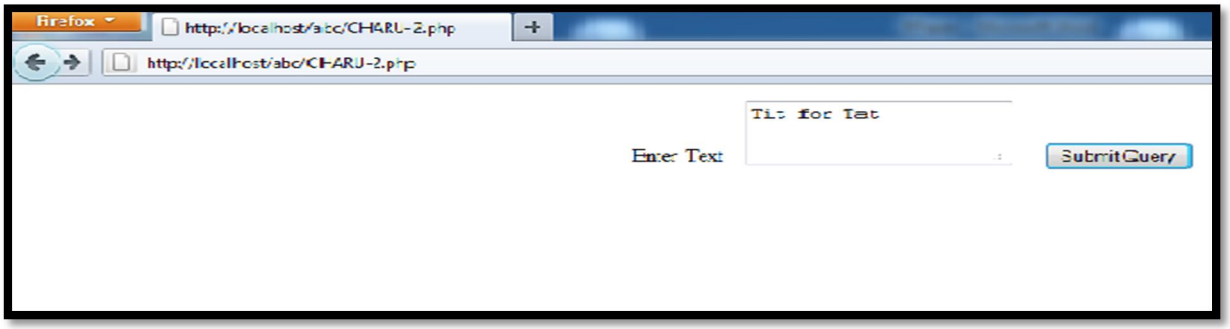


Fig. No. 5: Plain text as input

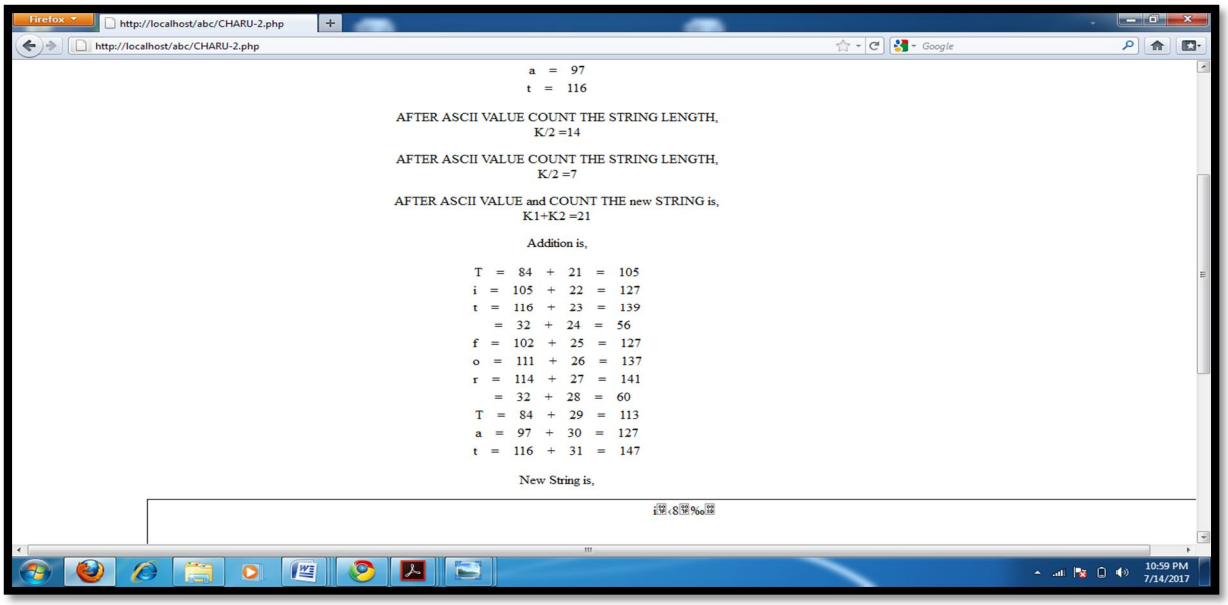


Fig. No. 6: Encrypted Text

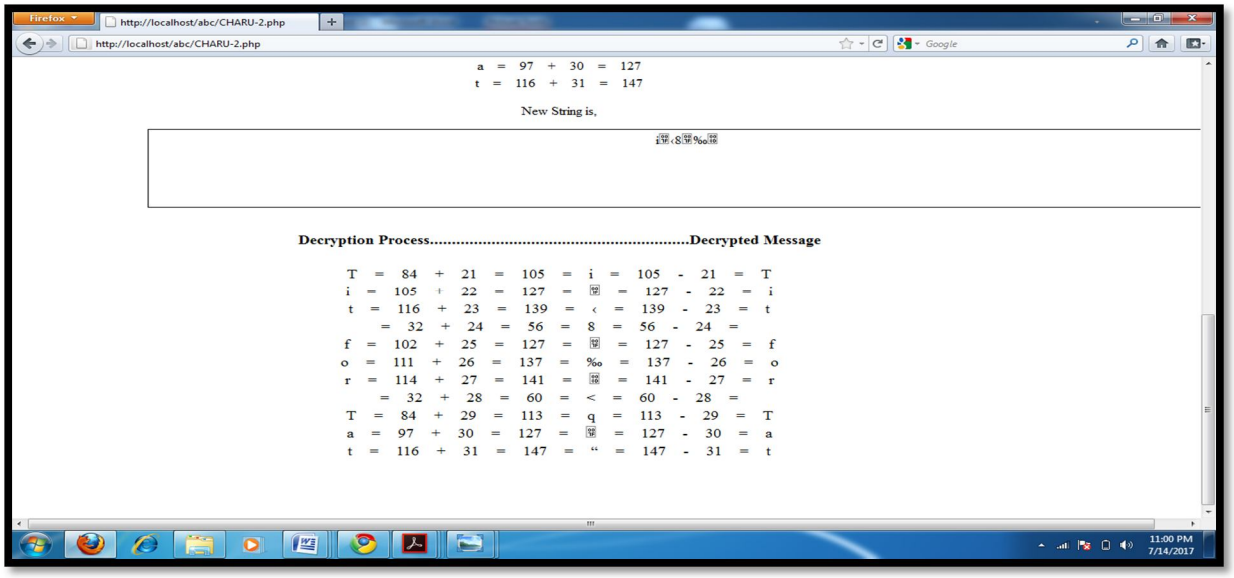


Fig.7: Decrypted Text

V.CONCLUSION

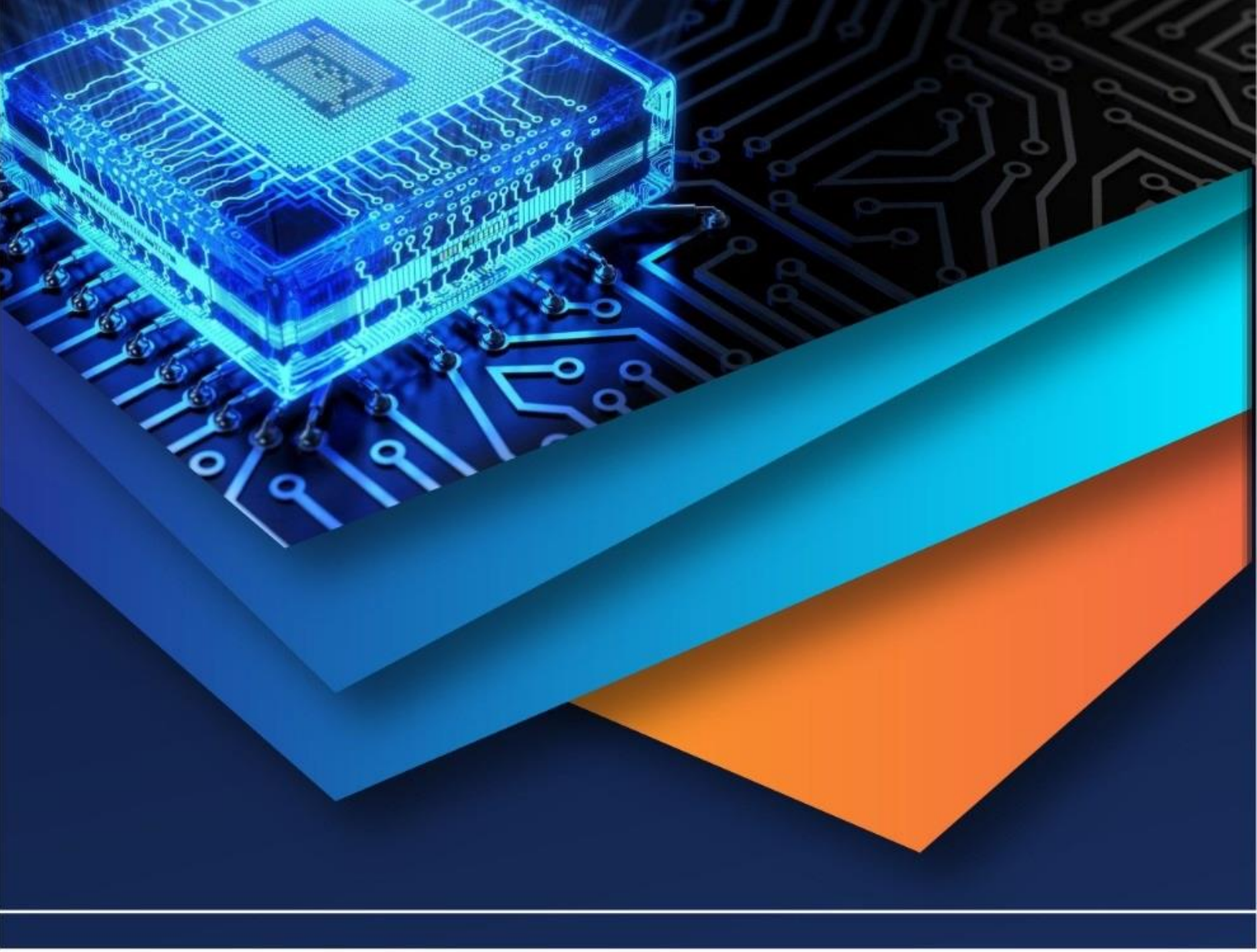
Mostly security models are based on one technique then it is very easy for the intruder to break that technique as by concentration on one method. Its loop holes can be easily found by the intruders so more than one technique must be used for encryption and decryption purpose. The current study has two encryption decryption techniques which are based on ASCII values. Secondly, Key generation of these methods is also unpredictable as keys values depends on the string length and string length vary from one plain text to other. So these are the secure encryption techniques. Both techniques ASCII Based Encryption Decryption Technique-1 and ASCII Based Encryption Decryption Technique-II have different key generation methods which are unique and robust.

VI.FUTURE SCOPE

New invented techniques cannot be traced out by the intruder easily as it ‘key generation is random which cannot be determined earlier by the intruders thus blend of many techniques for same text encryption is a good approach. These algorithms can be further improved by considering some important parameters like execution time, complexity etc.

REFERENCES

[1] Singh Udepal and GargUpasna (2013).An ASCII value based text data encryption system. International Journal of Scientific and Research Publications, Volume 3, Issue 11, ISSN 2250-3153
[2] Khamg A.I. and Ramli A.R. (2009) Implementation and Evaluation of New Cryptography Algorithm for E-mail Applications. International Journal of The Computer, the Internet and Management Vol. 17.No.1 pp 34-4
[3] Gupta Ruchika and SharmaPallaviStand-Alone Java Application for Cryptographic Algorithms.International Journal of Advanced Research in Computer Science and Software Engineering.Volume 3, Issue 5, May 2013,ISSN: 2277 128
[4] Soni, Ranu.,Johar, Arun., and Soni,Vishakha(2013). An Encryption and Decryption Algorithm for Image Based on DNA. 2013 International Conference on Communication Systems and Network Technologies
[5] G L, Prakash, Prateek, Manish.,Inder Singh(2014). Data Encryption and Decryption Algorithms using Key Rotations for Data Security in Cloud System, International Conference on Signal Propagation and Computer Technology (ICSPCT). 978-1-4799-3140-8/14/$31.00 ©2014 IEE
[6] Chatterjee, Ayantika and Sengupta,Indranil (2015). Translating Algorithms to handle Fully Homomorphic Encrypted Data on the Cloud. DOI 10.1109/TCC.2015.2481416, IEEE
[7] Teodorescu, R.M., Lita,I., Cioc,I.B., Visan D.A(2015).Virtual Instrumentation Application For Symmetrical and Asymmetrical Text Encryption/Decryption Studying. ECAI 2015 - International Conference – 7th Edition Electronics, Computers and Artificial Intelligence. Bucharest, ROMÂNIA 978-1-4673-6647-2/15/$31.00 ©2015 IEE
[8] Trivedi, Sneha .V., andHasamnis M. A(2015) Development of Platform Using NIOS II SoftCore Processor for Image Encryption and Decryption Using AES Algorithm; IEEE ICCSP 2015 conference
[9] AryaSuraj [2017].”Implementation of ASCII Based Information Hiding Technique to Perform the Secure communication Between Sender and Receiver”; International journal of science technology and management; Volume 6, Issue 1, January 2017 ISSN: 2394-1537(O); ISSN: 2394-1529(P) Research Paper Available online at: ;www.ijstm.com; impact factor 2.87
[10] ShuklaAlok Kumar and Kapoor, V (2014). Data Encryption and Decryption using Modified RSA Cryptography Based on Multiple Public Keys and ‘n’ Prime Number. International Journal Of Engineering Sciences & Research Technology; ISSN: 2277-9655 Scientific Journal Impact Factor: 3.449 (ISRA).Signal Processing and Communication Systems (lSPACS 2010) 978-1-4244-7371-7110/$26.00 ©201O IEEE
[11] Singh Saraswati and Kumar Vinay, VermaNilmani (2014). A Survey Report on Video Encryption and Decryption Techniques. International Journal of Computer Science and Mobile Computing, Vol.3 Issue.12, pg. 270-274.
[12] Senhaji Youssef and MedromiHicham et.al. (2015). Network Security: Hybrid IDPS ,Foundation of Computer Science FCS, International Journal of Applied Information Systems (IJAIS), Volume 9 p.5 ISSN : 2249-086
[13] Devi,L. and shantharajah ,S.P(2015). Survey on authentication and security Maintenance in wireless sensor networks. International Journal of Computer Science and Mobile Computing, Vol.4 Issue.5, pg. 53-70,ISSN 2320–088X



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY