iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** X **Month of publication:** October 2017

DOI: http://doi.org/10.22214/ijraset.2017.10098

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 5 Issue X, October 2017- Available at www.ijraset.com

A Simple Approach to Protect Data with ASCII Values and Random Number

Maddila Suresh Kumar[1], Kakollu Vanitha[2]
[1,2] *Department of Computer Science, Gitam Institute of Science, GITAM University*

Abstract: ***Protecting data is very important. Different ways of protecting data are available. Data can be protected with the help of ASCII values. In this paper a simple method is proposed to encrypt the text. The proposed algorithm reverses the text first, generates a random number and combines with the ASCII values which can add more strength to the encryption process.***
Keywords: ***Data, reverse, protect, random, communication, ASCII.***

I. INTRODUCTION

In present days, communication has become a major part. Simultaneously data communication should be done safely. In the past days data protection was done with the help of code words. Generation of code words is done with the help of a key. If data is translated in such a way that it is not easily understood, it can be called as encryption. If the non understandable format is again translated to understandable way, it is called as decryption. Much of the strength lies with the key which is used to encrypt the data. The encrypted data can be decrypted only if the key is available. To have a good encryption the key should be tough enough to guess. Complexity of the key helps to have a good encryption.

Plain text can be encrypted with the help of a key. The key must not be revealed to other users. The key must be strong enough to guess it. Generally, a key can be guessed and information can be leaked. In order to guess a key, it takes a lot of time. With the evolution of fast computers with high computational speed, the keys are prone to be cracked. Keys can be generated or the process of encryption can be made more complex which take more time and resources. The main aim is to protect data in a simple way with less usage of computer resources.

II. RELATED WORK

Necessary steps to protect data were done and are also going on to find out new ways. Some encryption algorithm uses sixteen bit encryption process and some algorithms use a two stage authentication process. Some algorithms involve the usage of a random number to encrypt information. Every technique has its own advantages and also some disadvantages. Some algorithms need more time and some algorithms consume large space. Using ASCII (American Standard Code for Information Interchange) values and a random number, text encryption can be done. Some algorithms represent the text in binary format and make use of shift operations also. A combination of a random number along with ASCII values and reversing the given text can improve the algorithm efficiency and make the encryption process to be more effective. Most of the algorithms encrypts very efficiently but utilizes the computer resources. Additional hardware can also be used to increase the efficiency of encryption. Some algorithms use more random numbers for encryption. An algorithm which uses more mathematical computations uses more computer resources to encrypt the data. Matrix format can also be used which involves the usage of two dimensional arrays, but can increase the computational time to encrypt the data. Finally, whatever may be the method the objective is to protect data and help secure transmission.

III. PROPOSED TECHNIQUE

The proposed algorithm is a simple one but good results are expected with minimum utilization of resources. The proposed algorithm uses a single random number, next the text is reversed and the random number is added to the ASCII values of the plain text to give the cipher text. In order to decode the cipher text is taken as input and the value of the random number is subtracted to get the original text in reverse. The proposed

©IJRASET (UGC Approved Journal): All Rights are Reserved

algorithm is simple one but can be efficient because the random number is generated by the algorithm and while decryption the output will be still in reverse order only.

A. Algorithm for Encryption

1) Input plain text.
2) Generate a random number less than hundred.
3) Reverse the given text.
4) Add the character's ASCII values added with random number value.

B. Algorithm for Decryption

1) Input encrypted text.
2) Subtract random number value from each character's ASCII value.
3) Output the decrypted text (in reverse).

IV. OBSERVATIONS

When the random number generated is more than twenty five, the algorithm has a chance of giving better results. As the random number which is more than twenty five when added to ASCII value of a character produces special characters. Even the final output will be in reverse order which can misguide the one who is trying to steal the information.

V. RESULTS

TABLE I: Observed Results

PLAIN TEXT	ENCRYPTED TEXT
Where are you now?	"ËÃÂtÉÃÍt¹Æµt¹Æ¹¼«
Where are you now?	u-¥¤V«¥¯V›¨—V›¨›ž
Where are you now?	Ayqp"wq{"gtc"gtgjY
meeting is postponed	¿ÀÉÊËÏÎÊË{ÎÄ{ÂÉÄÏÀÀÈ
need your help	Ã¿¸»sÅÈÂÌs·¸¸Á
start immediately	ÑÄ½Ì¹Á¼½ÅÅÁxÌÊ¹ÌË
shall we meet	‘¸¸Š=,”=‰‰~…
coming tomorrow	¾¶¹¹¶´¶»g®µ°´¶ª

VI. CONCLUSIONS

There are many ways to protect data and protecting data is very important. The plain text is converted into a non readable format. To get the original information the key is needed. This proposed algorithm is designed to generate a random number, reverse the given text and add the number value to the ASCII values. Advantage is that the final output is generated in reverse order which may not be understood clearly. The disadvantage is that, if the random number generated is less than twenty five, it may not give good results. The proposed technique is simple one but can yield good results with low computer resources. To obtain better results, the algorithm can be further modified.

VII. ACKNOWLEDGMENT

We are very thankful for all the people who have shared their knowledge by various means. We will be very much thankful to all the reviewers for their valuable suggestions and ideas.

©IJRASET (UGC Approved Journal): All Rights are Reserved

REFERENCES

[1] M. Suresh Kumar, G. Babu Rao, Data Protection Using Random Number in Association with ASCII Values, International Research Journal of Engineering and Technology, Volume 03, Issue 06, June 2016.

[2] Udepa Singh, Upasana Garg, An ASCII value based text data encryption System, International Journal of Scientific and Research Publications, Volume 3, Issue 11, November 2013.

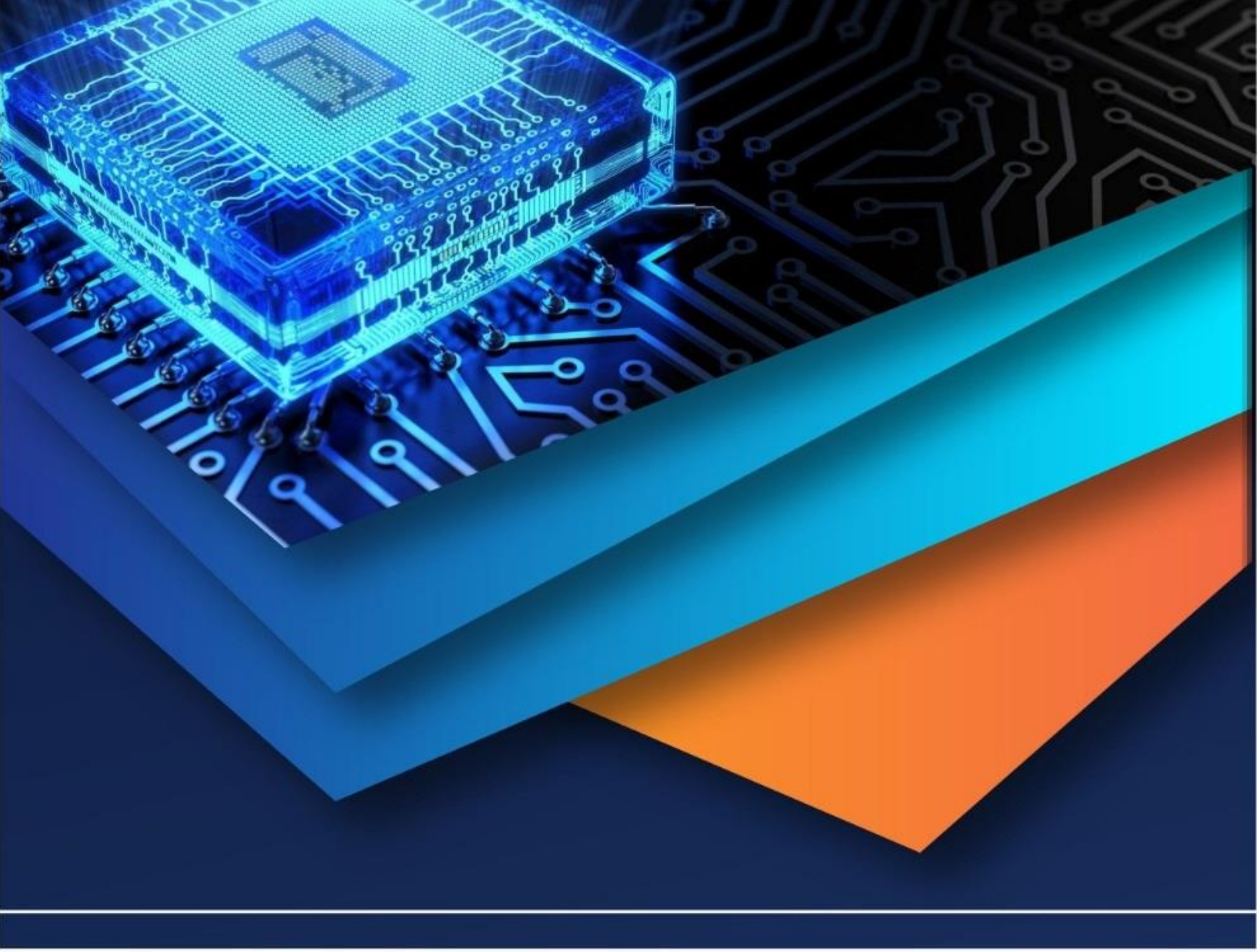
[3] Mina Mishra, V. H. Mankar, Text Encryption Algorithms based on Pseudo Random Number Generator, International Journal of Computer Applications, Volume 111 – No 2, February 2015.

[4] M. lavanya, R. Vijay Sai, A. Festina, J. Eshwari, T. Manopriya and V. Vaithiyanathan, An Encryption Algorithm Functioning on ASCII Values and Random Number Generation, Indian Journal of Science and Technology, Vol 8(35), December 2015.

[5] P. Pavan Kumar, J. Madan Kumar, M. Neelima, A new method for generating key for cryptography using Deterministic random number generator, International Journal of Engineering Trends and Technology (IJETT), Volume 4 Issue 9, September 2013.

[6] William Stallings, Cryptography and Network Security: Principles and Practices, Third Edition.

©IJRASET (UGC Approved Journal): All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)