RESEARCH ARTICLE OPEN ACCESS

ASCII Value Based Encryption System (AVB)

A.Vijayan[1], T.Gobinath[2],M.Saravanakarthikeyan[3]
[1]*(Department Of Information Technology, Chettinad College Of Engineering & Technology,Karur,)*
[2,3] *(Assistant Professor Department Of Information Technology, Chettinad College Of Engineering & Technology,Karur)*

ABSTRACT
Encryption and decryption are considered to be the guard for data in this technological world. To provide some kind of security, this paper proposes a new algorithm called AVB algorithm which is used to enhance the security of the data. This algorithm mainly focuses on ASCII value of data. ASCII value of the character is encrypted using normal mathematical calculation for number of time on a particular character and converted to numerical value. Then the cipher text is decrypted to get the original plain text. This algorithm is efficient in two ways it difficult for the intruders to predict the data as each character follows different form of encryption based on the key. And also it is simple, fast, and cost efficient while compared to ASCII value based text encryption system by Udepal Singh and Upasna Garg

I. INTRODUCTION

In technological world everything is easy both attack and prevention. Every technology in this High-fi world has vulnerability.Attacks from the vulnerability can be minimized by drum card "cryptography". In cryptography Lots of methods have been proposed by various cryptographers to minimize the attack of intruder's. *Cryptography* is the science of using maths to encrypt and decrypt data. Cryptography enables you to store secure information or to be transmitted across vulnerable network (like the Internet) so that it cannot be read by anyone except the intended recipient .While cryptography is the science of securing data, *cryptanalysis* is the science of applying and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck.Level of security depends upon the algorithm that has been used to produce cipher text, number of round doesn't matter where the logic of algorithm matter's. In order to fulfil the requirements, many encryption schemes have been proposed and analysed as possible solution systems.

In this paper, a new cryptographic algorithm is proposed, which follows a different method using the ASCII value. This new method provides security to data in a lower cost.

II. RELATED WORK

Udepal Singh, Upasna Gargencrypted the data on the basis of Unicode values, in which the security of data is increased [1].JGitanjali, Dr.N.Jeyanthi, C.Ranichandra, M.Pounambal proposed a newAlgorithm for encryption Technique, UPMM algorithm, which is applied on ASCII value of data. ASCII values are encrypted using a key involving Palindrome numbers and unique alphanumeric id, which is also converted into ASCII value to provide authentication over the network [2].Dr.M.MohamedSathik, A. KalaiSelvi, proposed data encryption anddecryption process using secret sharing scheme, which is based on generating the random polynomial and evaluates the mean value of the polynomial's coefficients. The mean value is added with the ASCII value of the plain text to get the cipher text [3].Prasant Sharma, Amit Kumar Gupta analyzed the speed of RSA public key cryptosystem to reduce the time taken for finding factor for a large number [4].SubhranilSom, DipanjanMitra, JhilomHaldarproposed an algorithm in which A Key is created from the input. Generating different randomized Matrices forms the Key. The value of the generated is manipulated with the individual ASCII values of the plain text. After completion of this process all the different resultant ASCII values will be further converted into their corresponding binary values [5].Dhavelvegad Husain Ullah khan NimishGhosh proposed an algorithm in which length of the key is calculated by adding any two random characters at starting and ending of a text and Ascii value of each character is calculated and shift operation is performed. They also tried encrypting file in the same manner[6].SatyajeetR.Shinge and Rahul Patil Proposed an algorithm in which uses Ascii value of the plain text to encrypt it, this system randomly generates a key for user having equal to length of the plain text. The randomly generated key is converted to another key which is used for

decryption purpose[7].m.lavanyaR.vijaysai proposed an idea which is based on Ascii value and random number generator to achieve data security and prevent unauthorized person from meddling secret data [8].AnupamKumarBairagi proposed an algorithm in which every character can be represented as an ASCII value which is either even or odd .depending upon this evenness or oddness, the character is encrypted differently [9].

III. LITERATURE SURVEY

Cryptography is the art of writing or solving codes. The main objective of cryptography is to provide security to the data in this vulnerable world. Cryptography mainly focuses upon encryption and decryption. Cryptography concentrates on confidentiality, integrity, authentication, access control.
Encryption
Decryption

Encryption:

Encryption is the concept of altering or modifying the original data (plain text) into some meaningless or sometime meaningful data but which is not same as compared to the plain text. Encryption uses some logic to convert plain text to cipher text. The logic can be done in two ways with or without key.
Symmetric key
Asymmetric key

Symmetric key:

It is one of the method in encryption this type of encryption uses same key on both sender and receiver side to encrypt and decrypt data. The length of the key and type of data which we use as a key is strength of algorithm as well as security of data.

Asymmetric key:It is one of the method in encryption this type of encryption uses different key on both sender and receiver side to encrypt and decrypt data. In this method public and private key is used in which if public key is used for encryption then private key is used for decryption and vice versa.

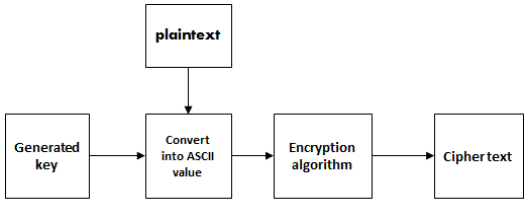
Decryption:

Decryption is the reverse process of encryption, in which the cipher text is converted to plain text using same method followed in encryption.

IV. PROPOSED METHOD

[1] Encryption phase

In this algorithm the information to be encrypted is fetched. The fetched data is stored in an array of characters, the characters are converted into their corresponding ASCII values. Square root for the ASCII values are found for "N" times where N is derived from Key string. The key which is used to encrypt the information is encrypted. Key string is stored in an array after taking ASCII value for all the characters in the key string. Square root for ASCII value of the key string is taken for "N"times. Finally an array consist of floating point numbers is the cipher text. This encryption phase continues until all the characters are encrypted. Then cipher text is sent to the receiver end



.

(II)Pseudo codefor Encryption:
The pseudo code for encryption phase is as follows

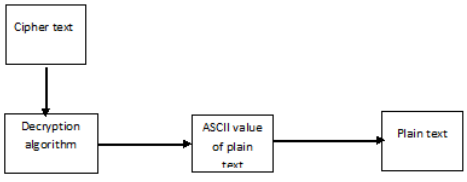
Begin:

1. Fetch the string to be encrypted
2. Calculate the ASCII value for all the characters in the string
3. Calculate the ASCII value for all the characters in the Key string
   a) for int i = 0 ; i <N; i++
   b) Calculate the square root for all the ASCII values of the key string for 'N" times
   c) End Loop
   d) for int i = 0 ; i <N; i++
   e) Calculate the square root for all the ASCII values for the data for 'N" times
   f) End Loop
4. Store floating point in an array which is the cipher text

End

[2] Decryption phase

Decryption is the vice-versa of encryption in which the cipher text is converted back to plain text (original text).it uses the same methodology followed in encryption. Decryption is critical phase since authentication is must and also we have to make sure that there is no changes in the data while transmission. There are several methods followed to meet the above mentioned criteria. Decryption in this proposed algorithm is as follows,fetch the cipher text which is in the form of floating point numbers both the encrypted data and key and square the cipher text for "N" times if only the key string matches. As a result of squaring a whole number is formed which is the ASCII value of the character. The ASCII value is converted into corresponding character based on the ASCII values, which is the original data or plain text. The algorithm for decryption is shown below.
Pseudo codefor Decryption:



The pseudo code for Decryption phase is as follows

Begin:

1. Fetch the string to be decrypted
2. Calculate the length of the Key string and length be 'N'
   a. for int i = 0; i <N; i++
   b. Calculate the square value for all the Floating point values of the key string for 'N' times
   c. Find the corresponding character based on the ASCII value
   d. End Loop
   e. for int i = 0; i <N; i++
   f. Calculate the square value for all the Floating point values for the data for 'N' times
   g. Find the corresponding character based on the ASCII value
   h. End Loop
3. Display it to the user.

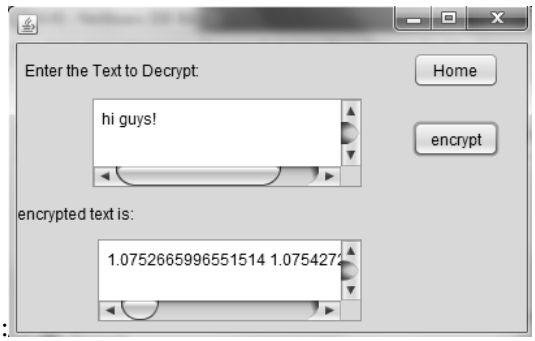
End.

V. RESULT

The proposed algorithm is implemented as a project for encrypting and decrypting both files and data. The result of encryption and decryption is as follows.

[a] Encryption of text message:

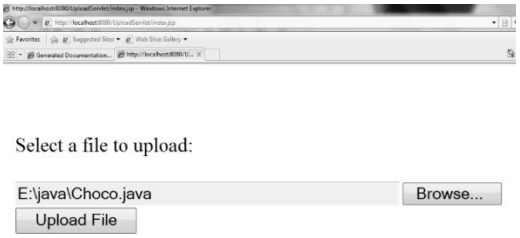
There are several algorithms available to provide security to the data. In this we are demonstrating the proposed algorithm in practical aspect. The snapshot shown below is the output of this algorithm. The procedure to perform encryption is as follows. To encrypt the text message input the message/data in the Text Box and then click encrypt button to perform encryption and the result is displayed in the resultant text box.

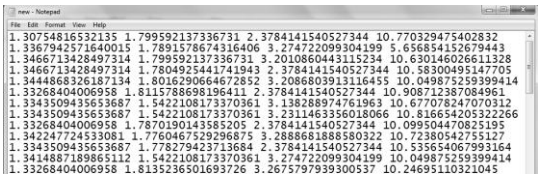


:

[a] Encryption of file:

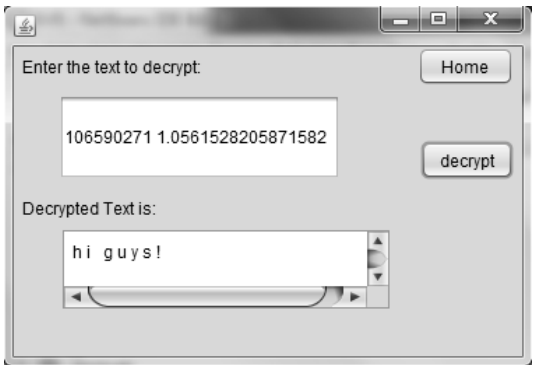
The proposed method is also implemented for encrypting the files. Since file sharing and uploading is most common means of communication between two parties now a days. It is used to provide security to files while uploading and sharing via internet. The procedure to perform this is, the user browses the file to be encrypted and fetch the original file. The file is encrypted on clicking the encrypt button and the encrypted file is saved in a location and address is displayed to the user.





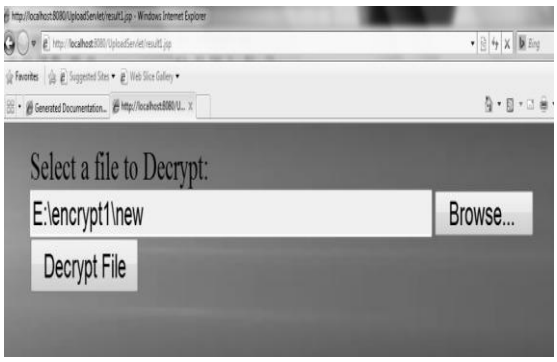
[a] Decryption of text message:

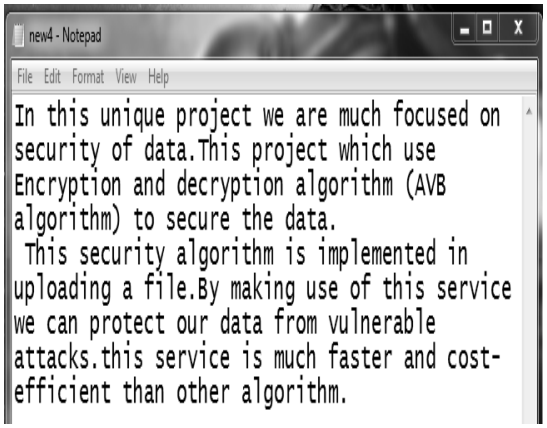
As mentioned earlier decryption is the reverse process of encryption. Demonstration of decryption is as follows, to decrypt the text message, just click in decrypt button and the cipher text in text box is converted to plain text (original text).



[b] Decryption of file:

Procedure to decrypt the file is, user browses the file to be decrypted and fetch the encrypted file. The file is decrypted on clicking the decrypt button and the decrypted file is saved in a location and address is displayed to the user.





VI. CONCLUSION

In this paper we proposed an algorithm to encrypt and decrypt data using ASCII value further no additional data is added so it is difficult to find out the original data also in this algorithm the data is encrypted after going through the several rounds. It is difficult to predict since key string also encrypted.

VII. FUTURE WORKS

With the proposal of this paper as a base we are working on to implement this algorithm on all file formats in future also we will implement this algorithm in asymmetric key based encryption, decryption system.

REFERENCES

Journal papers:

[1]. Udepal Singh, Upasna Garg ; An ASCII value based text data encryption System in International Journal of Scientific and Research Publications, Volume 3, Issue 11, November 2013 1 ISSN 2250-3153.

[2]. SubhranilSom, DipanjanMitra,JhilomHaldar; Session Key Based Manipulated Iteration Encryption Technique (SKBMIET),2008 International Conference on Advanced Computer Theory and Engineering.

[3]. Satyajeet R. Shinge, Rahul Patil, An encryption algorithm Based on ASCII value of data, international journal of computer science and information technologies,vol 5(6),2014,7232-7234

[4]. DhavalVegad Husain Ullah Khan, character based encryption and decryption using modulo arithmetic,international; journal of science technology&engineering|volume 1|issue 10|april 2015