Encryption and decryption algorithm

Engineering, Computer Security

Encryption and Decryption algorithm using ASCII values with substitution approach. First Author: M. Shruthi and Second Author: Gokaraju Rangaraju Institute of Engineering andTechnology, Bachupally, Nizampet, 500092www. griet. ac. in I.

Abstract

This paper shows the possibility of employing the characteristics of available algorithms with poly-alphabetic substitution techniques in a linear fashion, to produce ASCII values of the typed text and then putting in the translating, transposition techniques in order to get the encrypted text.

Before generating the cipher text, the algorithm will result in Message digest of the given text. This algorithm implements the model of symmetric Key cryptography. This algorithm can be implemented in any programming language such as C, C++, Java etc. In poly-alphabetic substitution the plain text's letters are encrypted differently corresponding to their position.

The name poly-alphabetic proposes that can be more than one key so we have used two keys combination instead of one, in order that it produces the cipher text. We can also use three or more keys to make the encoding process more complex. In this paper have generated ASCII Codes of the plain text and then we have reversed it say it as reverse ASCII Codes and then we have produced two random keys named K1 and K2.

Then these K1 and K2 Keys are alternatively applied on Reverse ASCII codes in order to produce encrypted text. On the other hand Decrypting algorithm is used to generate the plain text again. Our technique generates random

cipher text for the same plain text and this is the major asset of our technique.

II. Introduction

Related work: a. IntroductionNow-a-days need of security is essential to make data secure from the unauthorized user to access. Security is needed in many of the organizations like military, budgets of Government, it is also necessary to our general economy and many business applications also.

Business application involves the security among the data of the institute in which information about of the employees, manager workers and owner's profit is itself stored and similarly, application i. e, utilised by the user's according to their use also requires security. So security plays an indispensable role in our day to day life. Cryptography is one of the techniques for guarding data. Information Security is a set of thoughts for managing the processes, tools and policies necessary to prevent, detect, document and counter threats to digital and non-digital content.

The responsibilities of Information security include launching a set of business processes that will safeguard information assets regardless of how information is formatted or whether it is transit, is being processed or is at rest in storage. Important information or data cannot be sent across the internet without implementing any security mechanism, because this data can be seen by any intermediate person in order to change the message. So the command for Information Security across the networks is expeditiously increasing day-by-day.

Every business organisation has a burden to secure their data from being loss or theft. A message digest is a cryptographic hash function which includes a group of digits generated by a hash formula. Message digests are intended to secure the integrity of a piece of data or information to identify changes or alterations to any part of a message. Basic terms for securecommunicationare: Let us consider two parties that want to communicate secretly, A and B. If A wants to send something to B, some information, we call that information a plaintext.

After encrypting the plaintext a cipher text is produced. B knows the encryption method since he is the intended receiver and since he must use the same method together with his secret key to decrypt the cipher text and reveal the plaintext. b. Related Work: 1. Avinash Sharma and his team have proposed a technique for encryption and decryption.

In this paper they have explained about encryption and decryption techniques using ASCII values and substitution approach. (IJASCSE Vol 1, Issue 3, 2012)2. R. Venkateshwaran in his paper shows the possibility of utilizing the features of Genetic techniques with poly substitution methods in a linear way, to produce ASCII values of the given text and then employ transition, substitution with the features of Cryptography. (International Journal of Computer Applications (0975 – 8887) Volume 3 – No. 7, June 2010)3.

Sumith Chowdary and his team described about the algorithm in which randomly generated numbers are used with the help of modulus and

remainder by making program in any language i. e. c, c++ and java. (IJARCCE Vol. 2, Issue 8, August 2013)

III. Basic Mechanism for cryptography

P= Plain text C= Cipher text X= Some Plain text Y= Cipher text of plain text K= Any Random key E(K, X): Encryption of X using key D(K, Y): Decryption of Y using K C= E[K, P] P= D[E, C]

IV. History of Cryptography

The art of cryptography is considered to be born along with the art of writing. As civilizations period started, human beings got incorporated in tribes, groups, and kingdoms. This led to outgrowth of ideas such as power, battles, supremacy, and politics. These thoughts further furnished the natural need of people to communicate covertly with discriminative recipient which in turn assured the continuous evolution of cryptography as well. The roots of cryptography are found in Roman and Egyptian civilizations.

The word Cryptography has been derived from the Greek word kryptos (hidden) and graphing (writing). Cryptography is the technique with which a plain text can be converted to cipher text so that this cipher text is not understandable by anyone excluding the recipient. Cryptography, thescienceof encrypting and decrypting information can be traced back all the way to year 2000 BC in Egypt.

Here it was first used with the help of the standard hieroglyphics in order to communicate secretly. Julius Caesar(100-44 BC) used a simple substitution cipher which has been named after him today. During the first and the

second war the command for confidentiality increased rapidly all kinds of new cryptographic techniques developed.

V. Objective of the Algorithm

The core objective of the research is to safeguard information stealing in what so ever manner it may be, with the use of appropriate technology. To secure information spilling and to provide a high-level integrity and authenticity to data or information using MD5 and Cryptographic algorithm that is sent over the network.

Integrity: Ensures that a message is unchanged from the time it sent from the sender and till it is opened by the receiver. Authenticity: It verifies whether the identity of user in the system is a true or genuine user. To check the integration of message/information MAC is verified.

VI. Algorithm for Encryption

Decryption and MAC Generation: Algorithm encryption{Generate two random keys k1, K2. Take dataFind ASCII values for each character in the data. Reverse each ASCII value and store it. Add each key alternatively to each reversed ASCII value.//This is the encrypted data.}Algorithm decryption{Take the encrypted data and random numbers. Subtract the keys from the encrypted dataEach alternativelyReverse the obtained values.//

The reversed values will be ASCII codes of characters. Print the retrieved ASCII value's corresponding characters.}Algorithm MD5{Firstly append padded bitsThen append lengthInitialise MD BufferLater process message in 16-word blocks. Display the output.}Encryption Process: The above figure

(fig 1. 1) depicts the procedure of encryption. Let the text be HELLO WORLD. Firstly, generate 2 random keys named k1 and k2.

For example let us assumeK1 = 1123K2= 1452Then translate the each character of message into its corresponding ASCII Code and the we reverse these ASCII codes. (This is shown in table1. 1)Next, these keys k1, K2 are added alternatively to reverse ASCII numbers in order to generate cipher text.

Table 1. 1: Plain text ASCII number Reverse ASCII Number Cipher textH 72 27 1150E 101 101 1553L 108 801 2253L 108 801 1923O 111 111 1563 32 23 1146W 87 78 1530O 111 111 1234R 114 411 1863L 108 801 1923D 100 001 1453Decryption Process: This technique is exactly reverse technique to that of encryption. So in this process, subtract the keys from the obtained cipher text. That is first subtract k1 from first value of encrypted/cipher text and then subtract K2 from second value of cipher text, consecutively.

Repeat this step until you reach to the end of the message. Finally we will get the plain text which was sent by user. Following table will depict the process of decryption: Cipher text Reversed ASCII number ASCII code Plain text1150 27 72 H1553 101 101 E2253 801 108 L1923 801 108 L1563 111 111 O1146 23 32 1530 78 87 W1234 111 111 O1863 411 114 R1923 801 108 L1453 001 100 DVII.

MAC Generation: The MD5 hashing algorithm is a cryptographic technique that accepts a text of any length as input data and returns as output a constant-length digest parameter to be utilised for authenticating the true

message. From past years, there has been exaggerated interest in generating a MAC produced from a Cryptographic hash code, like SHA-1, MD5, etc. Here in this, we have used MD5 algorithm for resulting a 128 bit hash-value.

It is employed as a checksum to ascertain data integrity. Ex: 1. helloMD5 Hash of your string: 5D41402ABC4B2A76B9719D911017C5922. The attack is at 5 p. m. MD5 Hash of your string: 54759A4BE2031EA6CC8D56B10CD4A9AA

VIII. Snap shots of the algorithm implementation

Home page: After entering some text: Click on encrypt button: Click on Decrypt button: If the text-box is empty: And if clicked encrypt then it results to a message:

IX. Key words and Abbreviations

Cryptography: The process of encrypting and decrypting text for securing it.
Cryptanalysis: is the art of decoding or obtaining plain text from hidden messages over an insecure channel. It is also known as code cracking.
Encryption: The technique of converting plain text into some other format with the help of a key is known as Encryption.

Decryption: The technique of altering cipher text or encrypted text into plain (original) text is called as Decryption with the help of same key or other key.
Key: An amount of information used for encrypting and decrypting text.
Cipher text: The message written in secret code and is not understandable by anyone.

Plain text: The original message given by end-user. Encryption Algorithm: An Algorithm for encrypting given text. Decryption Algorithm: An Algorithm for decrypting the encrypted text. MD5 Algorithm: An Algorithm for finding 128 bit Message digest for the given text. Abbreviations used: MAC: Message Authentication CodeASCII: American Standard Code for Information Interchange. MD5: Message Digest v5

X. Future scope

This algorithm is formulated for the sake of security. There are many future scope of substitution approach employing ASCII value for Encryption & Decryption. Firstly it is certified that any intermediate person don't hack the data between the gap of plain text and cipher text. Secondly receiver receives the encrypted text as it's same as the senders send the plain text. Thirdly in the contemporary world, new technologies ameliorate day by day so we can exaggerate changes in this algorithm according to the requirement.

This work can be further improvised upon in the future in many different ways.

XI. Conclusion

There are many techniques such as RSA, IDEA, AES, DES, DIFFIE-HELLMAN algorithms and much more that can be utilized to modify a plain text into cipher text to transfer over the network so nobody else than an actual recipient can understand the message.

But Substitution and Transposition is the ground for every algorithm as each and every algorithm employs Transposition or Substitution or both of them.

In this view we have introduced a new technique that is titled as substitution using ASCII Codes. This new method for text encryption and decryption behaves randomly so grouping of the same cipher text and breaks it by just guessing it becomes more difficult.

This technique of combining cryptography and Message digest can lead to new area of research on securing data by other mechanisms. This technique of text encrypts and decrypt employing ASCII algorithm is definitely an impelling process when compared with other cryptographic systems. This algorithm is very meteoric, procure and trust worthy.

XII. References:

- 1. Stallings W. Cryptography and Network Security: Principles and Practice, 2/3e Prentice hall, 1999; 30-49. 2. Author: Vineet Sukhraliya, Sumit Chaudhary, Sangeeta Solanki, Title: Encryption and Decryption Algorithm using substitution array approach. IJARCCE Vol 2 Issue 8 August 2013. 3.
- Author: Avinash Sharma, Anurag Bhatnagar, Nikhar Tak, Anuradha Sharma, Jitendra Avasthi, Prerna Sharma Title: An Approach Of Substitution Method Based On ASCII Codes In Encryption Technique , IJASCSE Vol 1, Issue 3, 20124.
- Author: R. Venkateswaran Dr. V. Sundaram, Title: Text Encryption and Decryption with Poly Substitution Method and Combining the Features of Cryptography. IJCA Vol 3 – No. 7 June 2010. 5. https://en. wikipedia. org/wiki/Cryptography 6. https://en. wikipedia. org/wiki/MD5XII.