ISSN No:-2456-2165

A Secure Substitution Technique for Text Encryption and Decryption Based on ASCII Value

Manoj Kumar
Assistant Professor, Department of Computer Science and Engineering
Ajay Kumar Garg Engineering College Ghaziabad

Abstract:- Internet play a vital role for sharing information online but this mode is dangerous for data hacking and cracking by the unauthorized person. Information security is an important requirement of today world due to increasing use of internet. The privacy of information can be achieved through cryptography by applying the encryption process on the plain text being transmitted over network. Encryption is the process of converting the original text into cipher text so that only intended receiver of the message can read it.

In this paper we proposed a new ASCII code based substitution technique for text encryption which is more secure than Caesar Cipher substitution technique and proposed technique is implemented in java. In the proposed technique we used the ASCII value of the character and the position of the alphabet for encrypting the plain text.

Keywords:- *Cryptography, Substitution, Encryption, Decryption, ASCII Value.*

I. INTRODUCTION

Cryptography, from the Greek word 'kryptos' (hidden) and 'graphein' (to write), is the art and science of making communication unintelligible to all except the intended recipients [1].

Basic terminology used in cryptography is as follows.

A. Plain Text

Plain text is the original message sent by the sender to the intended receiver and work as input for the encryption algorithm.

B. Cipher Text

Cipher Text is the scrambled message produced as the output of the encryption algorithm.

C. Encryption

Encryption is the method of converting the plain text into cipher text using some substitution or transformation on the plain text.

D. Decryption

Decryption is a process performed at intended receiver side for obtaining the original message by decrypting the cipher text.

E. Secret key

The secret key is some critical information shared between sender and receiver of the message and play the main role in encrypting the plain text and decrypting the cipher text.

F. Simple Model for Cryptosystem

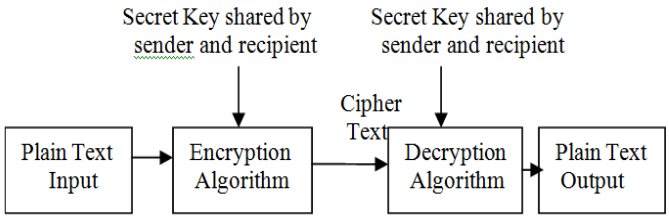

Fig 1: Simplified model of conventional Encryption

There are two basic types of encryption.

- *Symmetric Encryption:*

Symmetric encryption is a process of converting the plain text into cipher text where a secret key is used to encrypt and decrypt the plain message and this secret key is known to both sender and recipient of the message.

- *Asymmetric Encryption:*

In this type of encryption a pair of key is needed for encryption and decryption. These Key are the private and public key .Sender and receiver both has their private key and corresponding public key. Public key of each user known to other. Asymmetric Encryption is slower than symmetric encryption but it is more secure.

G. Secure Communication

In secure data communication the security of the message being transmitted over the network is maintained by ensuring the following properties.

- Confidentiality of message which ensure that message is secure from unauthorized person it means private information remains private.

- Integrity of message which ensure that message should not be altered or modified illegally.

- Authentication in communication which ensure the identity of valid sender and receiver of the message.

- Authorization of communication which ensure that a certain party attempting to perform a function has relevant permission to do so.

- Non repudiation in communication ensure against a party denying a data or a communication that was initiated by them [2].

II. LITERATURE REVIEW

Ciphers make textual communication a mystery to anyone who might unduly intercept it. Hence, a cipher is a method used to encode characters to hide their values [5]. Cipher is employed in design of cryptosystem. A cryptosystem is a system, method, or process that is used to provide encryption and decryption.

In the old days of cryptography two basic methods are used for the information security purpose. These two main Classical techniques are cipher types such as transposition ciphers, which rearrange the order of letters in a message (e.g., 'world' becomes 'owrdl' in a trivially simple). Second one is substitution ciphers, which systematically replace letters or groups of letters with other letters or groups of letters (e.g., 'fly at once' becomes 'gmz bu podf' by replacing each letter with the one following it in the Latin alphabet)[3].

A. Substitution Technique

A substitution cipher is a method of encryption in which the letters in the plaintext are replaced with other letter, symbol or number or mixture of these according to a system so that the receiver can decrypt the cipher text by performing an inverse substitution.

There are a number of different types of substitution cipher available like Caesar Cipher, Mono-alphabetic Cipher, Homophonic Substitution Cipher, Polygram Substitution Cipher, Polyalphabetic Substitution Cipher, Playfair Cipher and Hill Cipher.

B. Transposition Technique

In cryptography transposition cipher is a method of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system, so that the cipher text constitutes a permutation of the plaintext. That is, the order ofthe units is changed. Mathematically a objective function is used on the characters' positions to encrypt and an inverse function to decrypt.

There are a number of different types of Transposition cipher available like Rail Fence Cipher, Simple Columnar Transposition, Vernam Cipher, Double transposition, Myszkowski Transposition, Disrupted Transposition [3].

Since in this paper we proposed a substitution technique which is motivated by Caesar Cipher and is more secure than Caesar Cipher substitution. So we explained the Caesar Cipher in this section.

C. Caesar Cipher

One of the simplest examples of a substitution cipher is the Caesar cipher [6]. It is said to have been used by Julius Caesar to communicate with his army. Caesar is considered to be one of the first persons to have ever employed encryption for the sake of securing messages. Caesar decided that shifting each letter three places down the alphabet in the message would be his standard algorithm, and so he informed all of his generals of his decision, and was then able to send them secured messages [7].

Caesar Cipher is one of the simplest type of substitution method. In this method letters of plain text are replaced by letters three places further down the alphabet. But in general, this shift may be of any places [4]. Using the Caesar Cipher, the message “RETURN TO ROME” is encrypted as “UHWXUAWR URPH”. So attacker is not able to read the message if he intercepts the message. If in case it is known that a given cipher text is Caesar Cipher, then brute force cryptanalysis is easily performed: Try all the 25 keys.

There are some weak points of the Caesar Cipher substitution technique. Some of them are as follows.

- Caesar Cipher is not suitable for the plain text which contains special symbols or mixture of letters and number.

- Only 25 keys are to try.

- The language of the plaintext is known and easily recognizable. So it is not so much secure.

ISSN No:-2456-2165

III. PROPOSED SUBSTITUTION TECHNIQUE

In the proposed substitution technique we used the ASCII value of the character and position of the alphabet (as shown in the Table I) to encrypt the plain text and we also used the reverse operation to make the algorithm more secure.

Table I. ALPHABET AND THEIR POSITION

Alphabet	Position	Alphabet	Position	Alphabet	Position
a	00 or 0	j	09 or 9	s	18
b	01 or 1	k	10	t	19
c	02 or 2	l	11	u	20
d	03 or 3	m	12	v	21
e	04 or 4	n	13	w	22
f	05 or 5	o	14	x	23
g	06 or 6	p	15	y	24
h	07 or 7	q	16	z	25
i	08 or 8	r	17		

A. Algorithm for Encryption.

Following steps are used in the proposed algorithm to convert the plain text into cipher text.

Step1. To make the process secure at first perform the reverse operation on the plain text.

For each character of the plain text perform the following -

Step2. Replace each character of the plain text by it's ASCII value and represent the ASCII value in three digit.

Step3. For ASCII value of each character first two digits from right side represent the position of alphabet from 00 to 25 and third digit represent the position of alphabet from 0 to 9 as shown in table.

Step4. Substitute these position by the alphabet which occur at that position.

Step5. After performing the above steps we get the cipher text in lower case where each character of the plain text is encrypted by two alphabet.

B. Algorithm for Decryption

Following steps are used to obtained the plain text from the cipher text.

Step 1: At the receiver side in the cipher text for each two consecutive alphabet from right side first alphabet is replaced by its position from 00 to 25 and second alphabet is replaced by it's position from 0 to 9.

Step 2: After performing the step 1 each two consecutive alphabet of cipher text are represented in three digit numerical value. This three digit value is corresponds to ASCII value of a specific character. Substitute this ASCII value by corresponding character.

Step 3: Apply the reverse operation on the text obtained in the step2.

Step 4: After performing the step 3 receiver get the plain text sent by the intended sender.

C. Advantages of the Proposed Algorithm

Some of the advantages of the proposed substitution technique are here.

- Proposed algorithm is more secure than Caesar Cipher.
- Proposed algorithm can be apply to plain text which contains any type of character.
- Proposed algorithm take less computing time.

IV. EXAMPLE

Consider the following plain text p&M? to be transmit over the network from sender to receiver.

A. Encryption Process

Following steps are performed on the given plain text to convert it into cipher text.

Step1. Plain Text is p&M? which is input for encryption algorithm.

Step2. Perform the reverse operation on the plain text as shown in TableII.

ISSN No:-2456-2165

Table II. TABLE FOR RESULT OF STEP2

Plain Text	p	&	M	?
Text After applying reverse operation on plain text	?	M	&	p

Step3. Substitute the ASCII value for each character in three digit representation as shown in Table III.

Table III. TABLE FOR RESULT OF STEP3

Plain Text	p	&	M	?
Text After reverse operation	?	M	&	p
ASCII Value	063	077	046	112

Step4. For each ASCII Value substitute the alphabet according to Table 1 at the position indicated by first two digit and third digit in that ASCII value as shown in Table IV.

Table IV: TABLE FOR THE RESULT OF STEP4

Plain Text	p	&	M	?
Text after reverse operation	?	M	&	p
ASCII Value	063	077	046	112
Substitution by alphabet at corresponding position.	gd	hh	eg	lc

Step5. After step 4 cipher text for the Plain text p&M? is gdhheglc

B. Decryption Process

At the receiver side receiver take the cipher text as input and following steps are performed.

Step1. Substitute by the position corresponding alphabet in the cipher text. For each two consecutive alphabets first alphabet is substitute by position range from 00 to 25 and second alphabet is substituted by position range from 0 to 9.In this way we got the ASCII Value in three digit representation as shown in Table V.

Table V. TABLE FOR THE RESULT OF STEP1

Cipher text	gd	hh	eg	lc
For each two consecutive alphabets Substitution by position of first and second alphabet.	063	077	046	112

Step2. Substitute character corresponds to the three digit ASCII Value as shown in Table VI.

Table VI. TABLE FOR RESULT OF STEP2

Cipher text	gd	hh	eg	lc
For each two consecutive alphabets Substitution by position of first and second alphabet.	063	077	046	112
Substitution by the character of ASCII Value	?	M	&	p

Step3. Perform the reverse operation on the text obtained in step2 of decryption process.

Table VII. TABLE FOR RESULT OF STEP3

Cipher text	gd	hh	eg	lc
For each two consecutive alphabet Substitution by position of first and second alphabet	063	077	046	112
Substitution by the character of ASCII Value	?	M	&	p
Reverse Operation	p	&	M	?

Step4. For the Cipher text gdhheglc receiver obtained p&M? as plain text.

V. CONCLUSION AND FUTURE WORK

The algorithm proposed in this paper has been successfully verified with the help of an example. The proposed algorithm is fast, secure and reliable. The proposed algorithm for text encryption and decryption using ASCII value and position of alphabet is effective than Caesar Cipher. The proposed algorithm also satisfied its main feature that this algorithm can be used to convert the plain text which include any kind of character, symbol or mixture of both, algorithm support conversion for range ASCII value 32 to 255, because ASCII Value 0 to 31 are specified for control codes. The proposed algorithm can also be used further in other application for text based information security.

REFERENCES

[1]. Luciano D. and Prichett G., "Cryptology: From Caeser Ciphers to Public-Key Cryptosystem", The College Mathematics Journal, vol 18, no 1, pp. 2 -17, 1987.
[2]. http://www.netsec.org.sa/cryptography.html
[3]. Atul Kahate, Cryptography and Network Security, Second Edition, the McGraw-Hill Companies.
[4]. http://en.wikipedia.org/wiki/Transposition_cipher.
[5]. Dulaney E., *CompTIA Security+ Study Guide, Fourth Edition*, Wiley Publishing Inc., Indianapolis, Indiana, 2009.
[6]. Sinkov A., *Elementary Cryptoanalysis – A mathematical Approach*, Mathematical Association of America, 1966.
[7]. http://www.cs.trincoll.edu /~crypto/historical/caesar.html