AN APPROACH OF HYBRID TRANSPOSITION METHOD BASED ON ASCII VALUE IN CRYPTOGRAPHY

[1]VISHAL THAKOR, [2]PAPRI GHOSH, [3]PRAVIN BHATHAWALA

[1]Assistant Professor, Auro University, Gujarat, India
[2]Research Scholar, Pacific University, Rajasthan, India
[3]UGC Visiting Professor, HNG University, Gujarat, India
E-mail: [1]vishalthakor@yahoo.co.in, [2]papri_g@rediffmail.com,[3]pcb1010@yahoo.com

Abstract – Every day millions of people interact electronically through different computer applications such as e-mail, e-commerce websites, ATM machines, or different mobile device applications and uses Internet either directly or indirectly to transfer the data over the networks. With perpetual growth of Internet usage, the demand for data security while transferring and storing the data has increased. This has further led to increase the importance of cryptography and its various technics for security reasons.

In this paper, a hybrid cryptography method is proposed which uses both substitution and transposition technics to secure the plain text. The proposed method first applies substitution with the help of three different keys followed by transposition using forth key consist of matrix size on equivalent ASCII values of plaintext. The forte of the method is its all four keys. Within the same manner decryption will be done at receiver's facet but in reverse way of encryption.

Keywords - Cryptography, Encryption, Decryption, Cryptanalysis, Symmetric key, Asymmetric key, Hybrid, Transposition

I. HISTORY OF CRYPTOGRAPHY

From ancient time, Human being had two natural needs: I) communication and sharing of information II) maintaining confidentiality of what they communicate[1]. These two fundamental needs gave birth to the art of coding the messages in such a way that only the targeted people could have access to the information and if message have been stolen by an unauthorized person, he/she could not extract any information. i.e., "Cryptography is the art and science of protecting information from undesirable individuals by converting it into a form non-recognizable by its attackers while stored and transmitted".[2]The word "Cryptography" comes from Greek word "Kryptos" which means hidden writing[3].

II. INTRODUCTION

Cryptography consists of two processes. 1) Encryption: is a process of converting plain text into unreadable text usually called cipher. 2) Decryption: is a process of converting cipher text back into original plaintext In other words, it is the science of using mathematics to encrypt and decrypt information.

Cryptography in today's digital world offers three core areas that protect your data from an unauthorized access of your data and fraud. They are Confidentiality, Integrity, and Availability[4].

Confidentiality: It assures that private or confidential information is not made available or disclosed to unauthorized individuals.

Integrity: It assures that information and programs are changed only in a specified and authorized manner.

Availability: It assures that systems work on time and service is not denied to authorize users.

Cryptographic systems are characterized along three independent dimensions as follows [4]:

1) The type of operations used for transforming plaintext to cipher text.

- All encryption algorithms are based on two general principles: Substitution, in which each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element, and Transposition, in which elements in the plaintext are rearranged.
- The fundamental requirement is that no information be lost (i.e., that all operations are reversible).

2) The number of keys used.

- If both sender and receiver use the same key, the system is referred to as symmetric, single-key, secret-key, or conventional encryption.
- If the sender and receiver use different keys, the system is referred to as asymmetric, two-key, or public-key encryption.

3) The way in which the plaintext is processed.

- A block cipher processes the input one block of elements at a time, producing an output block for each input block.
- A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along.

III. PROPOSED TECHNIQUE

There are many different basic methods for cryptography such as caesar cipher, monoalphabetic, polyalphabetic, playfair, rail fence, column transpose which us either substitution or transposition technics to convert the plain text into cipher. Our proposed

method is based on these fundamental methods and combines both the technics, substitution and transposition, which is named as Hybrid Transposition technic. The traditional substitution method adds or subtracts some digits depending on the key from the original text character and generates the cipher accordingly[4]. Similarly, the classical transposition method comprise of a matrix and a key to interchange the columns. In order to add more security to the cipher, either the same key or another key can be applied for further interchange of columns which is called double transposition[5]. The proposed method first applies substitution with the help of three different keys followed by transposition using forth key consist of matrix size on equivalent ASCII values of plaintext. The forte of the method is its all four keys. Same process can be followed in reverse way to get the original text from the cipher text.

Encryption:

The idea behind this technic is to develop an algorithm with higher security which is difficult to break because of its keys strength. It uses four different keys to encrypt the text and same keys will be used by the receiver to get the original text.

The process starts by reading the number of characters in provided plaintext. Once the characters are read and counted, a matrix size is decided to form a square matrix to accommodate the plaintext. Before storing characters into the matrix, each character is converted to its equivalent ASCII value and then placed row wise into the matrix. To understand these steps, consider the following example:

Plaintext: Hello Singapore

Number of characters N (including space): 15

Matrix size (MxM): 4x4, where M * M or (M^2) ≥ N (i.e. 16 > 15)

Equivalent ASCII: 72 101 108 108 111 32 83 105 110 103 97 112 111 114 101

Matrix:

72	101	108	108
111	32	83	105
110	103	97	112
111	114	101	

Figure (1(a))

72	101	108	108
111	32	83	105
110	103	97	112
111	114	101	**42**

Figure (1(b))

Once the matrix is formed and filled with ASCII values, check for the empty cells. These cells also need to be filled with some value(s). For convince, we append ASCII value of '*' (i.e., value 42) to the matrix as shown in figure 1(b).

The fully filled matrix is then divided into three parts, diagonal elements, upper triangle elements, and lower triangle elements. In our case, they will be (72, 32, 97, 42), (101, 108, 108, 83, 105, 112), and (111, 110, 103, 111, 114, 101) respectively.

First three keys key1, key2, and key3 are used for substitution purpose to get a new matrix. The maximum length of these keys is two digits (0-99). The key1 is added to the diagonal elements, key2 is added to the upper triangle elements, and key3 is added to the lower triangle elements. For example key1 = 10, key2 = 20 and key3 = 40, then new matrix will be as follows:

82 (72+10)	121 (101+20)	128 (108+20)	128 (108+20)
151 (111+40)	42 (32+10)	103 (83+20)	125 (105+20)
150 (110+40)	143 (103+40)	107 (97+10)	132 (112+20)
151 (111+40)	154 (114+40)	141 (101+40)	52 (42+10)

Figure (2)

Let's call this new matrix as "mid-matrix".

The last key, key4 will be used to apply transposition on mid-matrix to achieve the final matrix. The length of the key4 depends on the length of the plaintext and is derived from the diagonal size of the matrix (or matrix size (MxM)). Here, the diagonal size is 4 (the matrix size (4x4)), the length of the key4 will be four. For example, let's take key4 = 2031, where each digits in this key need to be less than its length, i.e no digit is greater than 3 as we start with zero. Also, digits in this key can't be repeated.

The columns of the mid-matrix will be swapped according to the digits in the key4 and stored in another matrix called final-matrix. That is, in our example, column 2 from mid-matrix will be placed at first column in the final-matrix, and then column 0 from mid-matrix will be placed at second column in the final-matrix, column 3 from mid-matrix will be placed at third column in the final-matrix, and finally, column 1 from mid-matrix will be placed at last column in the final-matrix.

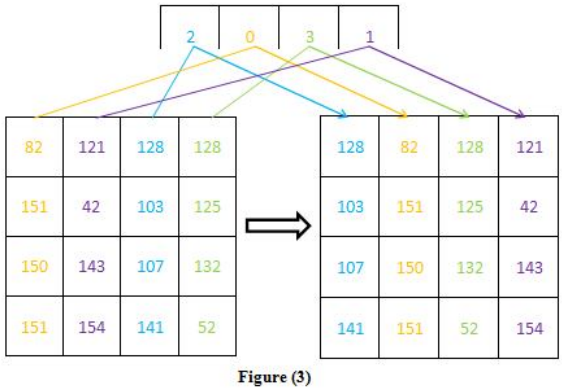

Figure (3)

Now, read the final-matrix row wise to get the cipher text. This will get following result in taken example.

128	82	128	121
103	151	125	42
107	150	132	143
141	151	52	154

Figure (4)

Read outcomes:
"128, 82, 128, 121, 103, 151, 125, 42, 107, 150, 132, 143, 141, 151, 52, 154"
Finally, each ASCII value from the read outcomes will be converted to its equivalent character by comparing it with the ASCII table.
So, the cipher text generated here will be "R y g } * k K ". Here, only printable characters from 32 to 127 (ASCII value) will be displayed and rest will be white spaces in the cipher.
This cipher can be stored into the database along with a unique identity number (at least 5 digits long) to add more security to the cipher.

Encryption Algorithm

STEP 1: Read the plain text.
STEP 2: Count the number of characters (N) in the plain text including white spaces.
STEP 3: Convert the plain text into equivalent ASCII code, character by character.
STEP 4: Create a square matrix (M) such that it can accommodate ASCII value of all N characters row wise from left to right and then fill remaining cells with 42 (ASCII of '*').
STEP 5: Read the elements of the matrix into three parts, diagonal, upper triangle and lower triangle.
STEP 6: Apply three different keys k1, k2 and k3 on diagonal, upper triangle and lower triangle parts respectively for encryption (i.e. add these keys on respective parts)
STEP 7: Arrange the matrix column by column according to the key k4 and then read the matrix row wise.
STEP 8: Convert the ASCII values into characters to obtain the cipher text.

Decryption:

The process of decrypting cipher into original text is exactly in the reverse order of its encryption process. The only difference here is user has to apply unique identity number first to prove himself/herself as an authentic person for further implementation of the keys. The things to be taken care are sharing the unique identity number, first three keys (maximum two digits), and fourth key (size depends on the length of plaintext). Furthermore, the decrypted message will carry the '*' for the number of empty spaces in the matrix which appended at the time of creation of matrix during encryption.

1. ANALYSIS

Here in the proposed algorithm, only numbers are considered to form the keys. We have three different (can be same) keys, k1, k2 and k3 of two digits in length and key k4 whose size depends on the size of matrix created from the plain text.

Key	Number of possible digits	Length of the key	Possible Combinations
k1	10	2	$(10)^2$
k2	10	2	$(10)^2$
k3	10	2	$(10)^2$
k4	M=5	M=5	$(M)^M = (5)^5$

Table 6.1 Possible combinations of keys

Here, M denotes the size of the transpose matrix.
So the possible combinations of the all the keys K1, K2, K3 and K4 of the proposed algorithm will be $[(10)^6 \times (5)^5] = 3.125 \times 10^9$ possible combinations. With 3.125×10^9 possible combinations of keys the proposed algorithm will be difficult to cryptanalyze. If an attacker check any of these possible key combinations every second it would take roughly one billion times the lifetime of the universe to check all of the keys and find the correct one.

2. 3. 4. CONCLUSION

The proposed hybrid transposition technique is based on symmetric key cryptography which has the speed and computational efficiency and can handle large volume of data encryption. Also, the technique uses stream cipher which works on few bits at a time and therefore has low memory requirement. In addition, four different keys applied on different parts of message are generated independently of the message stream. This presents high degree of confusion to an attacker during cryptanalysis. Moreover, size of key k4 depends on the size of the message.

REFERENCES

[1] Z. A. A.-F. a. H. J. B.B. Zaidan, "On the Differences between Hiding Information and Cryptography Techniques: An Overview.," Journal of Applied Sciences, vol. 10, no. 15, p. 7, June 2010.
[2] Sharma, A. Bhatnagar, N. Tak, A. Sharma, J. Avasthi and P. S. , "An approach of substitution method based on ASCII codes in encryption technique," IJASCSE, vol. volume 1 Issue 3, 2012.
[3] William Stallings, in CRYPTOGRAPHY AND NETWORK SECURITY, PRINCIPLES AND PRACTICE, NY, Prentice Hall, 2011, p. 900.
[4] M. Stamp, in INFORMATION SECURITY-PRINCIPLESANDPRACTICE, NewJersey, United States of America, JohnWiley & Sons, Inc., 2006, p. 413.

[5] R. Babu, G. Abraham and K. Borasia, "A review on securing distributed systems using symmetric key cryptography," International journal of advances in science and technology, vol. volume 4 issue 4, 2012.
[6] H. Disina, "Robust caesar cipher against frequency cryptanalysis using bi directional shifting," UniversityTun Hussein Onn, Malaysia, 2014.
[7] D. k. Gupta, S. k. Srivastava and V. Singh, "New concept of symmetric encryption algorithm-A hybrid approach of caesar cipher and columnar transposition in multistages," Journal of global research in computer science, pp. 60-66, 2012.
[8] Kahate, Cryptography and network Security, McGraw Hill Education (india) private limited, 2013.
[9] Q. A. Kester, "A hybrid cryptosystem based on Vigenere cipher and columnar transposition cipher," International journal of advanced technology and engineering research, pp. 141-147, 2013.
[10] S. R. Shinge and R. Patil, "An encryption algorithm based on ASCII value of data," International journal of computer science and information technologies, pp. 7232-7234, 2014.
[11] S. A. Ubhad, N. Chaubey and S. P. Dubey, "Advanced ASCII based cryptography using matrix operation , palindromee range, unique id," International journal of computer science and mobile computing, pp. 66-71, 2015.
[12] D. Das, S. J. Sharma and U. A. Lanjewar, "The Art of Cryptology: From Ancient Number System to Strange Number System," International Journal of Application or Innovation in Engineering and Management, vol. Volume 2, no. Issue 4, p. 11, April 2013.
[13] "www.tutorialspoint.com," Tutorials point, [Online]. Available: www.tutorialspoint.com/cryptography/origin_of_cryptography.htm. [Accessed 29 June 2017].

★★★