Available online at www.elixirpublishers.com (Elixir International Journal)

Computer Engineering

Elixir Comp. Engg. 109 (2017) 48071-48073

ISSN: 2229-712X

Cryptographic algorithm based on Mathematical Substitution

P K Kumaresan
Professor, Computer Science and Engineering, VMVK Engineering College, Vinayaka Missions University, Salem- 636308, Tamil Nadu.

ARTICLE INFO

Article history:
Received: 29 July 2017;
Received in revised form:
16 August 2017;
Accepted: 24 August 2017;

Keywords
Cryptography,
Encryption,
Decryption,
Key,
Cipher Text,
Plain Text,
Execution Time.

ABSTRACT
This paper presents an efficient cryptographic algorithm based on the mathematical functions that determine the important properties of the numbers. The conversion of characters to numbers makes this algorithm more secure. The other features of this algorithm include the lesser time that it takes to execute the encryption and the decryption. Also, the dynamic nature of the key makes this algorithm invulnerable to attacks.

1. Introduction

Cryptography is a technique that hides the data and thus provides information security. The algorithm discussed in this paper provides faster execution time as the process of encryption and decryption are done in small amount of time.

This paper discusses the mathematical operations that can be performed on the numbers to get the encrypted text and then the original message can be decrypted from that encrypted text by using the converse of the mathematical property.

Section 2 explains the process of encryption and decryption of the text with the use of mathematical property like division. Section 3 describes an implementation of the technique with the help of an example. Section 4 comprises of an analytical discussion and results of the technique used in this paper. Lastly, section 5 gives the conclusive discussion on the same.

2. The scheme

This paper discusses some properties that can be applied on the data. The most important numeric property used in this paper is:-

"The cube of any positive integer is either of the form 9m, 9m+1, or 9m+8 where m is a positive integer."

Using this property along with other operations, the numerical data is encrypted to the cipher text and decrypted back to the original message. Section 2.1 describes the encryption algorithm and section 2.2 describes the decryption algorithm.

2.1Encryption

The steps to encrypt the data are given below which convert the plain text into cipher text:

Step 1 Represent each text message by a string variable, say "text'. Then, represent each character in the message text with a number, according to the two key arrays to be sent. This representation of characters into numbers is shown in section 2.3.

Step 2 Each character is thus converted into numerical data form and these numerical values of the message text are stored in a single dimensional array, *a[ ]*.

Step 3 The array a[ ] is modified by replacing each element by the sum of the element itself and the previous element in the array sequence as a[2]=a[2]+a[1]; a[3]=a[3]+a[2] and so on.

Step 4 Now each of the elements of the array a[ ] is cubed.

Step 5 Next, divide each of the elements of the array a[ ] by 9 and get a corresponding quotient array and a remainder array (remainder will be either 0,1 or 8).

Step 6 For each element in the array a[ ], we send both the quotient and the remainder as two different elements to the receiver.

Thus, the plain text is sent as cipher text in the form of numbers as quotients and remainders in the form of two different arrays.

The fundamental idea used in this algorithm is as follows:

"The cube of any positive integer is either of the form 9m, 9m+1, or 9m+8 where m is a positive integer," the converse of which is used to decrypt the message. Also, the key should be sent to the receiver in order to decrypt the message.

2.2 Decryption

The steps used for decryption to convert the cipher text to plain text are as follows:-

Step 1 On receiving the quotient array and the remainder array, for each value, the receiver multiplies the factor by 9 and adds the remainder to the value

Tele:
E-mail address: pkkumaresan@hotmail.com

Step 2 These values are stored in the array, say a[ ].
Step 3 Then, take the cube root of these values and store in array a[ ].
Step 4 The array is then modified by subtracting the previous element from the actual element and the value hence obtained is again stored in array a[ ]. Like a[2]=a[2]-a[1]; a[3]=a[3]-a[2] and so on.
Step 5 Next, the values are converted back to their text form using the two key arrays sent that is the key.
Thus, the text message can be decrypted from the cipher text.

2.3 Key Formulation

The key used in this algorithm is based on the assignment of the numeric codes to the alphabets taken. The text message is taken and its duplicate elements are removed and are stored in an array (in alphabetical order) say **reducedmessage[ ].** Now a corresponding numeric array called **reference2message[ ]** is created which is going to contain consecutive integers which refer to the characters in **reducedmessage[ ].** For example if the text to be encrypted is "My name is Aakanksha", the reducedmessage[] will be :-
reducedmessage[]=[<blank space> A a e h i k M m n s y]
The reference2message[ ] array will be:
reference2message[ ]=[1 2 3 4 5 6 7 8 9 10 11 12]
Each element in the numeric array refernce2message[] references the characters stored in the string array reducedmessage[]. So, these are the two key arrays sent.

3. Implementation

This section discusses the implementation of the technique with the help of examples. This section will clearly indicate the technique describing it with the help of an example. Section 3.1 describes the encryption process and section 3.2 discusses the decryption process using an example.

3.1 Process for Encryption

The technique discussed in this paper is discussed further with the help of examples. For instance, consider a text message which is stored as text="My name is Aakanksha".
Converting the text message into numerical values using the key, we have:-
a= [8 12 1 10 3 9 4 1 6 11 1 2 2 7 3 10 7 11 5 3]
After modification of the array by replacement, we get:-
a[ ]=[8 20 13 11 13 12 13 5 7 17 12 3 4 9 10 13 17 18 16 8]
Now, cubing the array a[], we get:-
a[ ]=[512 8000 2197 1331 2197 1728 2197 125 343 4913 1728 27 64 729 1000 2197 4913 5832 4096 512]
Dividing each of the elements of array a[] by 9 to get the factor and the remainder:-
a[ ]=[56.8 888.8 244.1 147.8 244.1 192.0 244.1 13.8 38.1 545.8 192.0 2.3 7.1 81.0 111.1 244.1 545.8 648.0 455.1 56.8]
The quotient array and the remainder array are as follows:-
Q[ ]=[56 888 244 147 244 192 244 13 38 545 192 2 7 81 111 244 545 648 455 56]
R[ ]= [8 8 1 8 1 0 1 8 1 8 0 3 1 0 1 1 8 0 1 8]

3.2 Process for Decryption-

The decryption process is implemented as follow on the aforesaid example:-
On receiving the quotient array and factor array which are as follows:-
Q[ ]=[56 888 244 147 244 192 244 13 38 545 192 2 7 81 111 244 545 648 455 56]
R[ ]= [8 8 1 8 1 0 1 8 1 8 0 3 1 0 1 1 8 0 1 8]
Combining the two matrices, the resultant matrix a[ ] becomes:-
a[ ]=[56.8 888.8 244.1 147.8 244.1 192.0 244.1 13.8 38.1 545.8 192.0 2.3 7.1 81.0 111.1 244.1 545.8 648.0 455.1 56.8]
The receiver multiplies the first number of each element by 9 and adds the remainder to it (the second number)
Thus, the matrix becomes:-
a[ ]= [512 8000 2197 1331 2197 1728 2197 125 343 4913 1728 27 64 729 1000 2197 4913 5832 4096 512]
Now taking the cube root of the array a[ ] we have:-
a[ ]=[8 20 13 11 13 12 13 5 7 17 12 3 4 9 10 13 17 18 16 8]
Next, the array is modified as:-
a[ ]=[8 12 1 10 3 9 4 1 6 11 1 2 2 7 3 10 7 11 5 3]
From here the numerical data is easily converted into text message which is: "My name is Aakanksha".

4. Results and Analysis

This algorithm is very efficient in terms of time taken to execute the process. The time taken is very less and the use of mathematical properties makes the algorithm secure. However, the disadvantage of this method is that as the amount of characters increases, the data of encrypted message to be sent to the intended receiver also increases linearly as a text message with 2 characters requires only 2 data values to be sent. But as we go on increasing the number of characters in the text to 7, the amount of encrypted data increases linearly. A table below illustrates the same. This can also be shown with the help of a graph. The various texts on which analysis is done are:-

Table 4.1. Encrypted Message for Varying Text Length.

Text	No of Characters	KEY	Quotient array	Remai-nderArray
is	2	[i=1 s=2]	[0 1]	[1 0]
bat	3	[a=1 b=2 t=3]	[0 1 13]	[1 0 8]
that	4	[a=1 h=2 t=3]	[0 1 13 7]	[1 0 8 1]
eight	5	[e=1 g=2 h=3 i=4 t=5]	[0 1 13 38 81]	[1 0 8 1 0]
edition	7	[d=1 e=2 i=3 n=4 o=5 t=6]	[0 1 13 38 38 56 147]	[1 0 8 1 1 8 8]

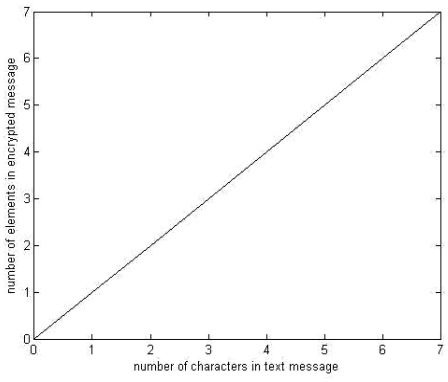

Figure 4.1. **Plot of Encrypted Message vs Varying Text Length.**

The table 4.2 below shows a relation between the numbers of characters in the text to be encrypted with the encryption time of the text. Execution time is equal to the sum of the encryption time and the decryption time of the text message implemented in the same program.

Table 4.2. The Encryption Time for Varying Text Length.

Number of Characters	Encryption Time
20	0.056423
31	0.085062
52	0.093160
72	0.101460
97	0.120941
127	0.144572
152	0.177882
177	0.212534
210	0.264692
232	0.307033

The figure 4.2 gives a plot of the data of the table 4.2.

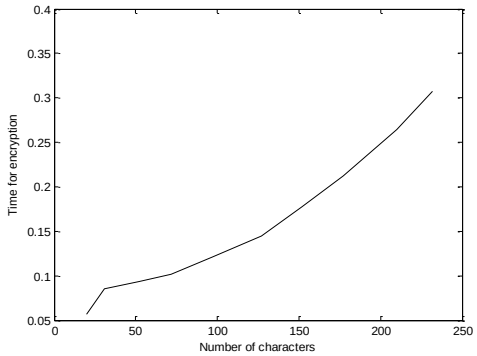

Figure 4.2. Graphical Representation of the Relationship between Time for Encryption and Text Length.

5. Conclusion

This algorithm hides the data as the data is modified and then numerical operations are applied on it. This algorithm has wide use and applications because of its less time in execution. Also being concise and secure, it can tolerate the targeted attacks and thus has a great scope ahead. The key is dynamic and hence adds to the advantages of this algorithm. This algorithm will find wide variety of applications in cryptography.

6. References

[1]. Pranam Paul, Saurabh Dutta, "A Private- Key Storage-Efficient Ciphering Protocol for Information Communication Technology", National Seminar on Research Issues in Technical Education (RITE), March 08-09, 2006, National Institute of Technical Teachers' Training and Research, Kolkata, India.

[2]. William Stallings, Cryptography and Network security: Principles and practice (Second Edition), Pearson Education Asia, Sixth Indian Reprint 2002.

[3]. Atul Kahate (Manager, i-flex solution limited, Pune, India), Cryptography and Network security, Tata McGraw-Hill Publishing Company Limited.

[4]. Mark Nelson, Jean-Loup Gailly, The Data Compression Book, BPB Publication.

[5]. Saurabh Dutta, "An Approach Towards Development of Efficient Encryption Technique", A thesis submitted to the university of North Bengal for the Degree of Ph.D., 2004.

[6]. Pranam Paul, Saurabh Dutta, A. K. Bhattacherjee, "An Approach to ensure Security through Bit-level Encryption with Possible Lossless Compression", International Journal of Computer Science and Network Security, Vol. 8 No. 2, pp 291-299.

[7]. Pranam Paul, Saurabh Dutta, "An Enhancement of Information Security Using Substitution of Bits Through Prime Detection in Blocks", Proceedings of National Conference on Recent Trends in Information Systems (ReTIS-06), July 14-15, 2006, Organized by IEEE Gold Affinity Group, IEEE Calcutta Section, Computer Science & Engineering Department, CMATER & SRUVM Project-Jadavpur University and Computer Jagat

[8]. Mandal J. K., Mal S., Dutta S., A 256 Bit Recursive Pair Parity Encoder for Encryption, accepted for publication in AMSE Journal, France, 2003.