Programming Encryption Algorithms with Steganography

Muharrem Tuncay GENÇOĞLU*

* Vocational School of Technical Sciences, Fırat University, Elazığ-Türkiye

(mtgencoglu23@gmail.com)

‡Corresponding Author Fırat University, Elazığ-Türkiye, Tel: +90 424 237 0000,

Fax: +90 424 212 2717,mt.gencoglu@firat.edu.tr

Received: 08.08.207 Accepted: 25.09.2017

Abstract- In this paper a different cryptographic method is introduced by using Power series transform, science of steganography. Here,we produce a new algorithm for cryptology,we use Expanded Laplace transformation of the exponential function for encrypting the plain text and we use codes of ASCII for support to the confidentiality of the chipertext. After, Chipertext have embedded by steganographic method in another plaintext to hide the existence of chipertext. We show corresponding inverse of Power Series transform for decryption. Then; Experimental results were obtained by writing a computer program for crypto machines.

Keywords Cryptology, Encryption, Decryption, Laplace Transform, Steganography, Programming for Encryption Algorithms.

1. Introduction

Confidential communication, with the technological progress has varied in terms of form and methods, have maintained continuous its importance. Because of the importance of confidentiality in applications, it is aimed to send protected information before third party's disposal, and studies have been started in this direction [2-5]. Network security problem has become very important in recent years. E-banking, e-commerce, e-government, e-mail, SMS services, security of ATMs and the existence of financial information has become indispensable in our lives. In these environments, the process, transfer, protection of information and security are of great importance. The Digital environment while providing data communication, from the sender to the recipient data unauthorized access, damage, prevent as there are many threats. These threats for the elimination of many encryption technique improved [2, 4-7]. Cryptography is the all of mathematical technical studies related to information security. Cryptology is cipher science and ensures security of information.

The main goal of cryptography is to allow two people to communicate through non-secure channels. Encryption is the process of blocking information to make it unreadable without special knowledge. These operations are expressed using an algorithm. In general this is called the symmetric algorithms. For encryption and decryption must be used the same secret key in the symmetric algorithms [5]. The inverse is also true. The security of this algorithms is associated with key [2]. The original information is known as plain text and cryptic text is encrypted format of this text. Encrypted text message contains all of the information in plain text message but it is not a readable format by a human or a computer without a suitable mechanism. The cipher is expressed by the parameters often called as the key by part of the external information. Encryption procedure is changed to vary of details of the algorithm operation based on the key. Without an appropriate key decryption is almost impossible. Advanced Encryption Standard (AES) method is the most used. Figure-1 also shows a symmetrical crypto system [2, 5-9]. Encryption converts data into an incomprehensible format makes it difficult to access the actual data but cannot ensure the confidentiality of communications. Steganography is come into question to hide a text as a complementary security solution at this point. Steganography as word meaning means hidden text or covered text. It is art of storing information which cannot be detected the presence [6]. The objective of the Steganography is hide the presence of a message and is create a channel to the implicit [8].

In this study; steganography and cryprography using together is intented to increase security for confidential data.Power series are used for cryptography. This process has been supported with 8 bit ASCII code and a high security application has been implemented for confidential data with

steganography combined. In the second section of the study;Respectively definations and some standard results are given for the proposed method.In the third section,flow diagrams are given together with recommended method and practice. In the fourth section,the evaluation of the results from the study are situated.

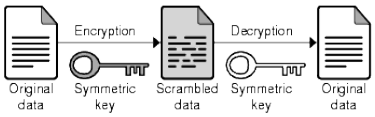

Fig. 1. Symmetrical crypto system.

2. Preliminaries

2.1. Defination

Let f(t) be defined for t>0. We say f is of exponential order if there exist numbers α, M>0 so that

$$|f(t)| \leq Me^{\propto t} \qquad (2.1)$$

If f(t) is exponential function then we have f(t)=∞ for t⟶∞[1].

2.2. Defination

Let f(t) be given for t≥0 and assume the function satisfy the property of α exponential order and t,s∈R. The Laplace transform of f(t) is defined by

$$F(s) = \int_0^\infty e^{-st} f(t)dt \quad . \qquad (2.2)[1].$$

Lets define a new transformation function by expanding the Laplace transformation using Definitions 1 and 2.

2.3. Defination

Transformation of f(t) for every t≥0 is defined as:

$$F(h) = T[f(t)] = \int_0^\infty \frac{1}{h} e^{\frac{-t}{h}} f(t)dt. \qquad (2.3)$$

(Extended Power Series Transformation) We present f(t)=T⁻¹[F(h)] to define the inverse transformation of f(t). Obtained extended power series transformation has the following standard results[3]

$$1.T\{t^n\} = \frac{n!}{s^{n+1}} \Rightarrow T^{-1}\left\{\frac{1}{s^{n+1}}\right\} = \frac{t^n}{n!}$$

$$2.T\{t^n e^{st}\} = \frac{n!.h^n}{(1-sh)^{n+1}} \Rightarrow \quad T^{-1}\{\frac{h^n}{(1-sh)^{n+1}}\} = \frac{t^n.e^{st}}{n!} \ (t\geq 0) \quad (2.4)$$

2.4. Defination

In order to keep the text information in the computer memory computer system assigns a numerical value to each letter or symbol. This process depends on the encoding system. By setting the numerical value of symbols, in order to represent non-numeric or alphabetic type of information on the computer the most commonly used as the coding system is used in ASCII coding system.

2.5. Defination

The process of hiding a data or message into another object is called steganography. The goal is to conceal the existence of the message [4].

3. Application

By combining methods of cryptography and steganography application stages of this hybrid model that increases data security and privacy are as follows;

3.1. Encryption

Assume that we want to send the message "FIRAT". Firstly we consider extended Taylor series with e^t:

$$f(x) = f(a) + \frac{f'(a)}{1!}(x-a) + \frac{f''(a)}{2!}(x-a)^2 + \cdots + \frac{f^n(a)}{n!}(x-a)^n + \cdots$$

$$= \sum_{n=0}^{\infty} \frac{f^n(a)}{n!}(x-a)^n. \quad (3.1)$$

Then, if we expand;

$$e^t = 1 + \frac{t}{1!} + \frac{t^2}{2!} + \frac{t^3}{3!} + \cdots = \sum_{n=0}^{\infty} \frac{t^n}{n!} \quad (3.2)$$

with t^3 , then we get:

$$t^3 e^t = t^3 + \frac{t^4}{1!} + \frac{t^5}{2!} + \frac{t^6}{3!} + \cdots = \sum_{n=0}^{\infty} \frac{t^{n+3}}{n!} \quad (3.3)$$

Therefore, we obtain:

$$f(t) = \sum_{n=0}^{\infty} K_n \frac{t^{n+3}}{n!}. \qquad (3.4)$$

If we enumarate letters of the alphabet from scratch "FIRAT" plain text be equal 6, 9, 19, 0, 22. If we write K_0=6,K_1=9,K_2=19,K_3=0,K_4=22 in to (3. 4), we get

$$f(t) = \sum_{n=0}^{\infty} K_n \frac{t^{n+3}}{n!}$$

$$= K_0 \frac{t^3}{0!} + K_1 \frac{t^4}{1!} + K_2 \frac{t^5}{2!} + K_3 \frac{t^6}{3!} + K_4 \frac{t^7}{4!} \quad (3.5)$$

If we apply extended power series transformation to both sides of (3. 5), we get

$$T[f(t)](h) = T[\sum_{n=0}^{\infty} K_n \frac{t^{n+3}}{n!}](h)$$

$$= T[K_0 \frac{t^3}{0!} + K_1 \frac{t^4}{1!} + K_2 \frac{t^5}{2!} + K_3 \frac{t^6}{3!} + K_4 \frac{t^7}{4!}](h)$$

$$= 6.3!\,h^3 + 9.4!\,h^4 + 19.5!\frac{h^5}{2!} + 0.6!\frac{h^6}{3!} + 22.7!\frac{h^7}{4!}$$

$\sum_{n=0}^{\infty} K_n(n+3)!\frac{h^{n+3}}{n!} = 36h^3 + 216h^4 + 1140\frac{h^5}{2!} + 0\frac{h^6}{3!} + 4620\frac{h^7}{4!}$. (3.6)

The provisions of 36, 216, 1140, 0, 4620 in the modes (28) are (K_n) 8, 20, 20, 0, 0. If we write chapters in mode operation instead of these numbers, we obtain the key (K_n') 1, 7, 40, 0, 165. "FIRAT" plain text converts "HSSAA" by (3. 3).

If we convert "HSSAA" encrypted text to 8-bit characters in the ASCII code we obtain 72,83,83,65,65. If these codes are written in binary system we get the keys $(1001000)_2$, $(1010001)_2$, $(1010001)_2$, $(1000001)_2$, $(1000001)_2$. ASCII 8 bit keys are in the text as follows: A provision giving the binary number system in the space between each word of the text namely if the number between two words 1 then we get $(1)_2$ and we define 2 with $(0)_2$. in the Table 1.

Table 1. Embedded Text

Kriptoloji,_haberleşen__iki__veya_daha__fazla__ tarafın__bilgi_alışverişini__emniyetli_olarak__yapmasını__ sağlayan_ve_gizli_ya__da_özel__bilgiyi__istenmeyen_ kişilerin_anlamayacağı_hale__getirerek__korumayı__ esas__alan,__temeli_matematiksel_yöntemlere__dayalı__ uygulamaların__ve__tekniklerin__bir_bütünüdür.	Cryptology is a set of practices and techniques based on the basis of mathematical methods providing safety of the exchange of information communicating two or more the parties and bringing protection to make people to not understand unsolicited confidential or proprietary information.

Sender also send this text clearly with (1, 7, 40, 0, 165) secret key.

Hence theorem can be following

Theorem

The given plain text in terms of (K_n) ,under Laplace transform of $K_n\frac{t^{n+3}}{n!}(h)$, can be converted to cipher text,

$(K_n') = (K_n) - 28q_n$ (n=0, 1, 2,…) (3.7)

Where a key

$q_n = \frac{K_n - K_n'}{28}$ (n=0,1,2,…) (3.8)

3.2. Decryption

The recipient receives a text message and by reading the spaces between words with software that will get the data buried create the necessary numerical equivalents. If these numbers are divided into 8-bits groups then ASCII provision of the data buried has been obtained. We can see the hidden data buried “HSSAA” in the Table 2.

Table 2. Embedded text and solution

Kriptoloji,_haberleşen__iki__veya_daha__fazla__ tarafın__bilgi_alışverişini__emniyetli_olarak__yapmasını__ sağlayan_ve_gizli_ya__da_özel__bilgiyi__istenmeyen_ kişilerin_anlamayacağı_hale__getirerek__korumayı__ esas__alan,__temeli_matematiksel_yöntemlere__dayalı__ uygulamaların__ve__tekniklerin__bir_bütünüdür.					
Text Bits	100 1000	101 0001	101 0001	100 0001	100 0001

Secret Data	72	83	83	65	65
Cipher Message	H	S	S	A	A

If we write H,S,S,A,A→8,20,20,0,0 and secret key values (1,7,40,0,0,165) into

$A_n = \frac{K_n - K'_n}{28}$

$\mathbf{36} = 28x1 + 8$

$\mathbf{216} = 28x7 + 20$

$\mathbf{1140} = 28x40 + 20$

$\mathbf{0} = 28x0 + 0$

$\mathbf{4620} = 28x165 + 0$ are obtained.

If we apply these values 36,216,1140,0,4620 to the

$$\sum_{n=0}^{\infty} K_n (n+3)! \frac{h^{n+3}}{n!}$$

then, we get

$\sum_{n=0}^{\infty} K_n (n+3)! \frac{h^{n+3}}{n!} = 36h^3 + 216h^4 + 1140\frac{h^5}{2!} + 0\frac{h^6}{3!} + 4620\frac{h^7}{4!}$

$= 6.3!\,h^3 + 9.4!\,h^4 + 19.5!\frac{h^5}{2!} + 0.6!\frac{h^6}{3!} + 22.7!\frac{h^7}{4!}$.

If we apply inverse Extended Power Series Transformation to both sides of the (3.7), then we get

$T^{-1}\left[\sum_{n=0}^{\infty} K_n (n+3)! \frac{h^{n+3}}{n!}\right] = T^{-1}[6.3!\,h^3 + 9.4!\,h^4 + 19.5!\frac{h^5}{2!} + 0.6!\frac{h^6}{3!} + 22.7!\frac{h^7}{4!}\ ]$

$\sum_{n=0}^{\infty} K_n \frac{t^{n+3}}{n!} = 6.t^3 + 9.t^4 + 19.\frac{t^5}{2!} + 0.\frac{t^6}{3!} + 22.\frac{t^7}{4!}$.

If we convert the $K_n$coefficients we will get the first plain text 6,9,19,0,22→F,I,R,A,T.

Hence theorem can be following

Theorem

The given cipher text in terms of (K'_n),with a given key q_n, can be converted top lain text (K_n) under the inverse Laplace transform of

$T^{-1}\left[\sum_{n=0}^{\infty} K_n (n+3)! \frac{h^{n+3}}{n!}\right] = \sum_{n=0}^{\infty} K_n \frac{t^{n+3}}{n!}$,

Where

$K_n = 28q_n + K'_n$ (n=0,1,2,…).

Operations performed in this section is shown in Figure 2 and Figure 3.

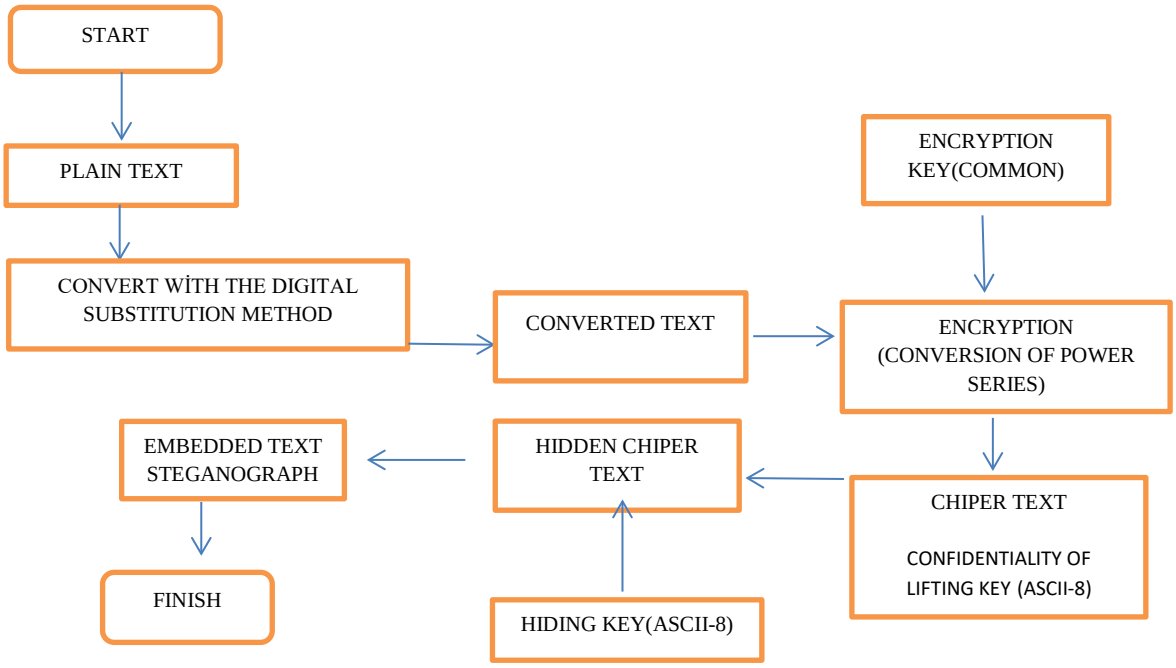

Fig. 2. Flow Diagram of Encryption System

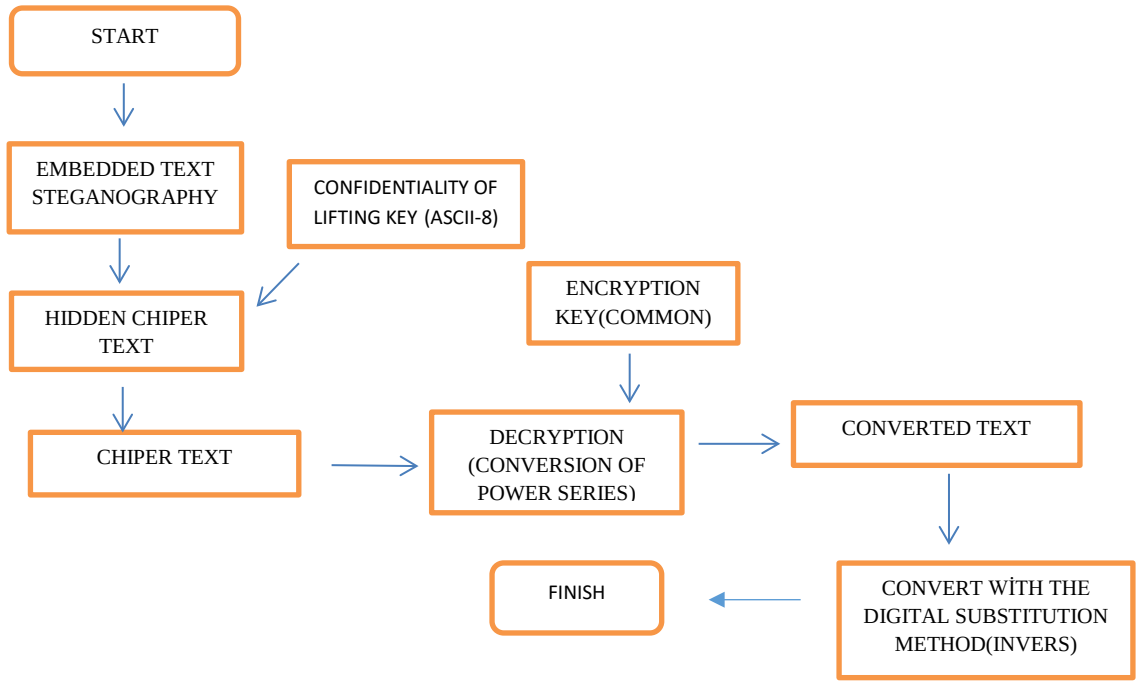

Fig. 3. Flow Diagram of Decryption System

4. Application of Programming Algorithms

The applications of the program written using the C # programming language are shown in Figure 4 and Figure 5.

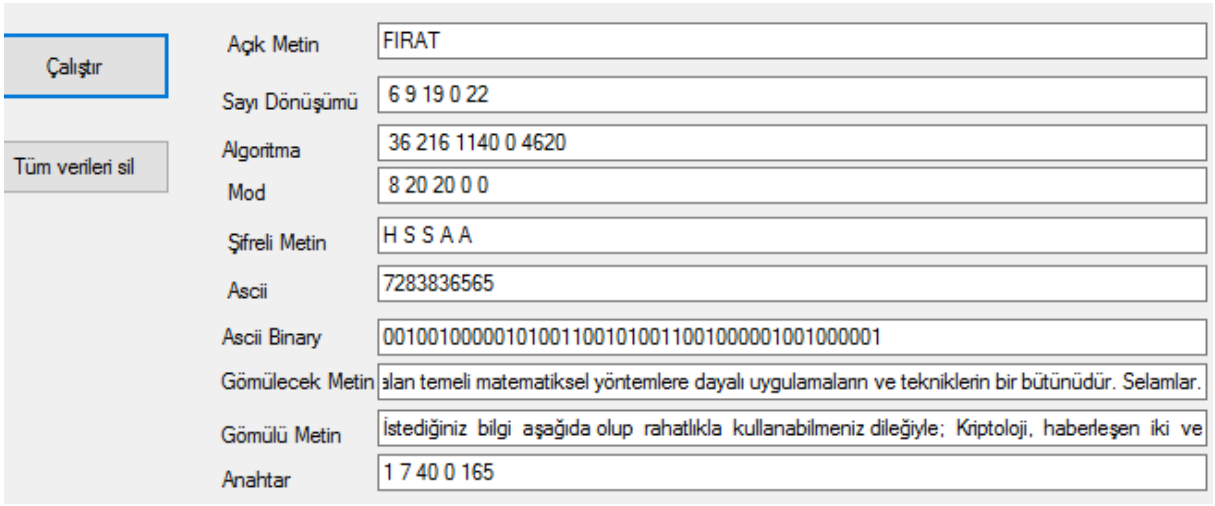

Fig. 4. Encryption

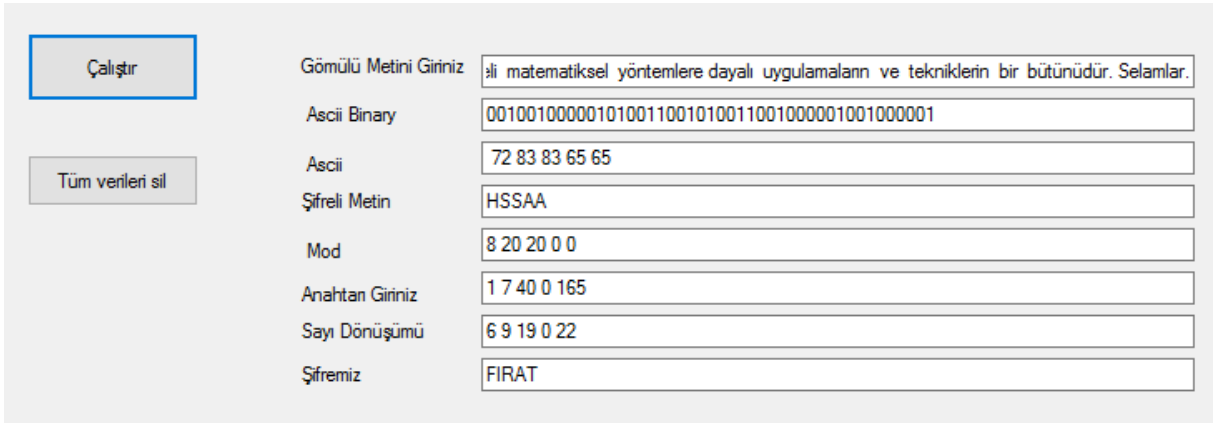

Fig.5. Decryption

5. Conclusion

By using a conversion which we called the power series conversion algorithm has been created.The keys generated using this algorithm is similar to the method known as substitution method in literatüre.But this method has been obtained by the method emerged as a result of digitization.In order to provide greater security developed a hybrid model using steganography and explained the details of it.Through this proposed hybrid model user has hidden this message with keys instead of (K_n') coefficient of q_n coefficient obtained by taking and has hidden existence of this message with ASCII code.Then,using another a password is hidden encrypted text into a text.In this way, higher safety feature is provided to data using steganography approach. Finally; written program will be used in crypto machine.

References

[1] M. Aydın, G. Gökmen, B. Kuryel, G. Gündüz, Diferansiyel Denklemler ve Uygulamaları, Barış Yayınları, 1990, pp. 332-349.

[2] Ç. K. Koç, Cryptographic Engineering ,Springer, 2009, pp. 125-128.

[3] M.T. Gençoğlu.,Use of Integral Transform in Cryptology.Science and Eng. J of Fırat Univ., Vol. 28, No. 2, pp. 217-220,2016.

[4] K.M. Martin.,Everyday Cryptography Fundemental Principles and Applications,Oxford University Press, 2012, pp. 741-744.

[5] H. Delfs, H. Knebl, Introduction to Cryptography Principles and Applications,Springer, 2007, pp. 169-175.

[6] Y. Yalman, İ. Ertürk. Kişisel Bilgi Güvenliğinin Sağlanmasında Steganografi Bilminin Kullanımı.ÜNAK Bilgi Çağında Varoluş:"Fırsatlar Ve Tehditler" Sempozyumu, pp. 215, 01-02 Ekim 2009.

[7] C. Paar, J. Pelzl,J, Understanding Cryptography,Springer, 2010,pp. 78-83.

[8] S. Usha, G. A. Sathish Kumal, K. Boopathybagan, A Secure Triple Level Encryption Method Using Cryptography and Steganography, International Conference on Computer Science and Network Technology, IEEE, pp. 565-578, 24-26 Dec.2011.

[9] N.F. Johnson, S. Jajodia, Exploring steganography: Seeing the unseen, Computer, Vol. 31, No 2, pp. 26-34,1998.