Cryptanalysis of Application of Laplace Transform for Cryptography

Muharrem Tuncay GENÇOĞLU[*]

Vocational School of Technical Sciences, Firat University, Elazig, Turkey

Abstract. Although Laplace Transform is a good application field in the design of cryptosystems, many cryptographic algorithm proposals become unsatisfactory for secure communication. In this cryptanalysis study, one of the significant disadvantages of the proposed algorithm is performed with only statistical test of security analysis. In this study, Explaining what should be considered when performing security analysis of Laplace Transform based encryption systems and using basic mathematical rules, password has broken without knowing secret key. Under the skin; This study is a refutation for the article titled Application of Laplace Transform for Cryptography written by Hiwerakar[3].

Keywords: Laplace Transform; Cryptography; Cryptanalysis; A general attack scenario.

[*] Corresponding author: mtgencoglu23@gmail.com

1 Introduction

Several encryption algorithms were designed by using the dynamics which were presented by Laplace Transform system for cryptographic applications [1-5]. However, security analyses of the proposed algorithms in several designs were shown by using experimental results and statistical tests [6-10]. The resistance of algorithm to brute force attack was correlated to the number of parameters which are only used in key production. Eventually, the weakness of these Laplace Transform based cryptosystem designs is shown by using simple.

The fundamental difficulty of designing a cryptosystem is to express with a mathematical model for structures used in encryption architecture then to prove that these structures are cryptographically secure. Indeed, approaching problem with a cryptanalyst point of view while designing encryption scheme will disappear several possible problems which may exist in further stages. Same situation is valid for Laplace Transform based cryptology, as well. A Laplace Transform based text encryption algorithm was proposed in [3]. Security analyses of the proposed algorithm were done only by using statistical tests and experimental results. In this study, cryptanalysis of the proposed algorithm was performed. Firstly; a general attack scenario was given for cryptanalysis, secondly; how to obtain plaintext from cipher text was shown using this scenario without knowing key parameter. In the last section, obtained results were discussed and some general proposals were presented.

2 Description of the encryption algorithm

Fundamental of the proposed encryption algorithm depends on encryption of the letters with substitution method produced with the help of a Laplace transform. Encryption process is carried out by using of Taylor series. Since the proposed algorithm is a symmetrical encryption algorithm, in the beginning a secret key in between sender and receiver is determined. The encryption algorithm steps are as follows:

Step 1. Before starting encryption process, sender and receiver agree on a key.

Step 2. Laplace Transform which will be used in the algorithm is determined. Hyperbolic functions were used in the proposed encryption algorithm. Standard expansion of Hyperbolic functions were given in Eq. (1). Plaintext is determined by using Eq. (2).

$$\sinh rt = rt + \frac{r^3t^3}{3!} + \frac{r^5t^5}{5!} + \frac{r^7t^7}{7!} + \cdots + \frac{r^{2i+1}t^{2i+1}}{(2i+1)!} + \cdots + \cdots = \sum_{i=0}^{\infty} \frac{(rt)^{2i+1}}{(2i+1)!} \qquad (1)$$

Where $r \in N$ is a constant,

$$t^2 \sinh 2t = 2t^3 + \frac{2^3t^5}{3!} + \frac{2^5t^7}{5!} + \frac{2^7t^9}{7!} + \cdots + \frac{2^{2i+1}t^{2i+3}}{(2i+1)!} + \cdots + \cdots = \sum_{i=0}^{\infty} \frac{2^{2i+1}t^{2i+3}}{(2i+1)!} \qquad (2)$$

It allocated 0 to A and 1 to B then Z was 25.

Step 3. Given plaintext "FLOWER" was equivalent to

5 11 14 22 4 17.

Recognizing coefficients that

$$G_0 = 5, G_1 = 11, G_2 = 14, G_3 = 22, \qquad G_4 = 4, G_5 = 17,$$

$$G_n = 0 \quad for \ \ n \geq 5.$$

Writing these numbers as a coefficients of $t^2 \sinh 2t$, and assuming $f(t) = G\, t^2 \sinh 2t$, He get

$$f(t) = t^2[G_0\,.\,2t + G_1 \frac{2^3t^3}{3!} + G_2 \frac{2^5t^5}{5!} + G_3 \frac{2^7t^7}{7!} + G_4 \frac{2^9t^9}{9!} + G_5 \frac{2^{11}t^{11}}{11!}]$$

$$=\sum_{i=0}^{\infty}\frac{2^{2i+1}t^{2i+3}}{(2i+1)!}G_i \qquad (3)$$

$$=5\frac{2t^3}{1!}+11\frac{2^3t^5}{3!}+14\frac{2^5t^7}{5!}+22\frac{2^7t^9}{7!}+4\frac{2^9t^{11}}{9!}+17\frac{2^{11}t^{13}}{11!}\ .$$

Step 4. Taking Laplace transform on both sides he have

$$L\{f(t)\}=L\{\,Gte^{2t}\}=5\frac{2t^3}{1!}.\frac{3!}{s^4}+11\frac{2^3t^5}{3!}.\frac{5!}{s^6}+14\frac{2^5t^7}{5!}.\frac{7!}{s^8}+22\frac{2^7t^9}{7!}.\frac{9!}{s^{10}}+4\frac{2^9t^{11}}{9!}.\frac{11!}{s^{12}}+17\frac{2^{11}t^{13}}{11!}.\frac{13}{s^{14}}$$

$$\frac{60}{s^4}+\frac{1760}{s^6}+\frac{18816}{s^8}+\frac{202752}{s^{10}}+\frac{225280}{s^{12}}$$

$$+\frac{5431296}{s^{14}} \qquad (4)$$

Adding 5 to the resultant values

60 1760 18816 202752 225280 5431296 to mod 26,

65=1 mod 26,1765=23 mod 26,

18821=23 mod 26, 202757=9 mod 26, 225285= 21 mod 26,5431301=5 mod 26.

Step 5. Sender sends the values, 2 67 723 7798 8664 208896 as a key.

$$G_0{}'=13,\qquad G_1{}'=23,\qquad G_2{}'=23,\qquad G_3{}'=9,\qquad G_4{}'=21,\qquad G_5{}'=5,\quad G_n{}'=0\quad(n\geq 6)$$

The given plain text was converted to cipher text

13 23 23 9 21 5.

The message “FLOWER” was converted to “NXXJVF”.

3 A general attack scenario for Laplace transform based encryption schemes

Below, a general attack scenario which a cryptanalyst can use while analyzing any Laplace transform based encryption schemes was briefly summarized.

Case 1. The structures used in encryption scheme must be expressed with a mathematical model. It must be investigated if the model can be expressed with simpler equations or cannot and, if exist, algebraic dependencies must be revealed.

Case 2. Encryption system must be shown to be resistant to known attacks. According to Taylor series expansion(Laplace Transform) and modular arithmetic of principle; it should be assumed that the attacker knows everything except secret key in encryption scheme and what kind of things can be obtained with specifically chosen plain text/cipher text pairs about encryption scheme should be investigated.

Case 3. Since the security of encryption algorithm is dependent on chosen key space, the specifications which can be done on key space must be investigated. Key design algorithm must be expressed mathematically; the existence of poor keys caused by design must be investigated.

Case 4. Topological properties of Laplace Transform systems used in encryption architecture should be investigated in detail. It must not be forgotten that the required confusion and diffusion properties which cryptographic systems need to be secure are provided by Laplace Transform used in encryption scheme.

Case 5. The problems which can occur because of divide rules when Laplace Transform systems and mode are carried out on digital computers must be investigated. Although very strong structures are used, special attacks to the design must be investigated by taking into account that the tiniest opening can affect entire system.

4 Cryptanalysis

In this section, how a cryptanalysis is carried out by applying the attack scenario given in previous section onto the proposed Laplace Transform based text encryption algorithm [3] step by step was demonstrated. Encryption architecture was expressed with a simple mathematical model as shown in Eq. (5). Ih the proposed algorithm, it was stated that a relationship between numbers correspond to ciphertext and modular arithmetic exists. . It is not necessary to know the secret key since cihpher is solved according to modular arithmetic principle. The existence of dependencies in between numbers correspond to ciphertext and modular arithmetic is one of the drawbacks in algorithm.

$$L\left\{\sum_{i=0}^{\infty}\frac{2^{2i+1}t^{2i+3}}{(2i+1)!}G_i\right\}=\sum_{i=0}^{\infty}\frac{2^{2i+1}.(2i+3)!}{(2i+1)!.s^{2i+4}}G_i \tag{5}$$

Encrypted text is converted to numbers with the method used by the author;

“NXXJVF”→ 13 23 23 9 21 5.

These numbers were obtained in Eq. (5). Then,We get

$$G_0.\frac{2.3!}{1!.s^4}+G_1.\frac{2^3.5!}{3!.s^6}+G_2.\frac{2^5.7!}{5!.s^8}+G_3.\frac{2^7.9!}{7!.s^{10}}+G_4.\frac{2^9.11!}{9!.s^{12}}+G_5.\frac{2^{11}.13!}{11!.s^{14}}. \tag{6}$$

Since $G_i \leq 25$ and numbers have used equivalents in mode 26 we get

$$G_0.12+5=26.K_0+13 \Rightarrow G_0=\frac{26.K_0+8}{12} \Rightarrow \left\{\begin{array}{l} G_{0,1}=\mathbf{5}\ for\ K_0=\mathbf{2} \\ G_{0,2}=18\ for\ K_0=8 \end{array}\right.$$

$$G_1.160+5=26.K_1+23 \Rightarrow G_1=\frac{26.K_1+18}{160} \Rightarrow \left\{\begin{array}{l} G_{1,1}=\mathbf{11}\ for\ K_1=\mathbf{67} \\ G_{1,2}=24\ for\ K_1=147 \end{array}\right.$$

$$G_2.1344+5=26.K_2+23 \Rightarrow$$

$$G_2 = \frac{26.K_2 + 18}{1344} \Rightarrow \left\{ \quad K_2 = \mathbf{723}\ i\c{c}in\ G_2 = \mathbf{14} \right.$$

$$G_3.9216 + 5 = 26.K_3 + 9 \Rightarrow G_3 = \frac{26.K_3 + 4}{9216} \Rightarrow \left\{ G_3 = \mathbf{22}\ for\ \ K_3 = \mathbf{7798} \right.$$

$$G_4.56320 + 5 = 26.K_4 + 21 \Rightarrow G_4 = \frac{26.K_4 + 16}{56320} \Rightarrow \left\{ \begin{array}{l} G_4 = \mathbf{4}\ \ for\ \ K_4 = \mathbf{8664} \\ G_4 = 17\ for\ \ K_4 = 36824 \end{array} \right.$$

$$G_5.319488 + 5 = 26.K_5 + 5 \Rightarrow G_5 = \frac{26.K_5}{319488} \Rightarrow \left\{ \begin{array}{l} G_5 = \mathbf{17}\ for\ K_5 = \mathbf{208896} \\ \end{array} \right.$$

5 11 14 22 4 17 → “FLOWER”.

5 Conclusion

A symmetrical encryption algorithm was proposed by Hiwarekar[3]. In the proposed algorithm, by using modular arithmetic the secret key detected between sender and receiver and cipher text solved. Namely; proposed encryption algorithm without knowing the key is broken only by seeing encrypted text.Therefore, claimed by author “It is very difficult for an eyedroper to trace the key by any attack.” is dasabled also the password is broken without a computer with simple divisibility and module theory.

References

1. Bodkhe D.S, Panchal S.K. (2015). Use of Sumudu Transform in Cryptography, Bulletin of the Marathwada Mathematical society, **16/2:** 1-6.
2. Hiwarekar A.P. (2012). A new method of cryptography using Laplace transform, International Journal of Mathematical Archive, **3/3 :** 1193-1197.
3. Hiwarekar A.P. (2015). Application of Laplace Transform for Cryptography, International Journal of Engineering & Science, **5/4 :** 129-135.
4. Lakshmi G.N, Kumar B.R, Sekhar A.C. (2011). A cryptographic scheme of Laplace transforms, International Journal of Mathematical Archive, **2/12:** 2515-2519.
5. Gençoğlu M.T. (2016). Use of Integral Transform in Cryptology, Science and Eng.J of Fırat Univ., **28/2:** 217-220.
6. Ge X, Liu F, Lu B, Yang C. (2010). Improvement of Rhouma's attacks on Gao algorithm, Physics Letters A, **374:** 1362-1367.
7. Sakallı M. T, Aslan B. (2014). On the algebraic construction of cryptographically good 32 × 32 binary linear transformations, Journal of Computational and Applied Mathematics, **259 :** 485–494.