Fırat Üniv. Müh. Bil. Dergisi
29(2), 37-40, 2017

Science and Eng. J of Fırat Univ.
29(2), 37-40, 2017

Laplace Dönüşümü Kullanarak Kriptografinin Yeni Bir Metodunun Kriptoanalizi

M.Tuncay Gençoğlu
Fırat Üniversitesi, Teknik Bilimler MYO, 23119 Elazığ, Türkiye
e:mail mt.gencoglu@firat.edu.tr

(Geliş/Received: 02.01.2017; Kabul/Accepted: 10.05.2017)

Özet

Laplace dönüşüm kripto sistemlerin tasarımında iyi bir uygulama alanı olmasına rağmen, birçok şifreleme algoritması gibi güvenli iletişim için yetersizdir. Kriptografinin yeni bir metodunun kriptoanalizinin yapıldığı bu çalışmada, önerilen şifreleme algoritmasının güvenlik analizinin sadece istatistiksel testlerle gerçekleştirilmesi önemli bir dezavantajdır. Bu kriptoanaliz çalışmasında; Laplace dönüşüm tabanlı şifreleme sistemlerinin güvenlik analizi yapılırken dikkat edilmesi gereken noktalar açıklanmış ve temel matematik kuralları kullanılarak, gizli anahtar bilinmeden, şifre kırılmıştır.

Anahtar Kelimeler: Laplace dönüşümü, Kriptografi, Kriptoanaliz.

Cryptanalysis of a New Method of Cryptography Using Laplace Transform

Abstract

Although Laplace Transform is a good application area in the design of cryptosystems, many cryptographic algorithms are inadequate for secure communication. In this cryptoanalysis study, it is a significant disadvantage that the security analysis of the proposed encryption algorithm is carried out only by statistical tests. In this cryptoanalysis study, when performing security analysis of laplace transformation based encryption systems explaining the need to pay attention to what and using basic mathematical rules, without knowing the secret key, the password was broken.

Keywords: Laplace transform, Cryptography, Cryptanalysis.

1. Giriş

Laplace dönüşüm sistemi çeşitli şifreleme algoritmalarında kullanılmıştır [1-5]. Ayrıca önerilen algoritmalar için güvenlik analizi istatistiksel testler kullanılarak gösterilmiştir [6,7]. Algoritmanın herhangi bir saldırıya karşı direnci yalnızca anahtar üretiminde kullanılan parametrelerin sayısıyla ilgilidir. Bir kripto sistemi tasarlamanın zorluğu, şifreleme mimarisinde kullanılan yapıları matematiksel bir modelle hesaplamak ve daha sonra bu yapıların şifreleme açısından güvenli olduğunu kanıtlamaktır. Aslında bir şifreleme planı kriptoanalist bir bakış açısı ile tasarlanırsa bir sonraki adımlarda ortaya çıkabilecek muhtemel problemlerin bazıları giderilebilecektir. Aynı durum Laplace dönüşüm tabanlı şifreleme için de geçerlidir.

Laplace dönüşüm tabanlı bir metin şifreleme algoritması önerilmiştir [2]. Önerilen algoritmanın güvenlik analizleri sadece istatistiksel testler kullanılarak yapılmıştır. Bu çalışmada Laplace dönüşüm tabanlı kriptosistem tasarımlarının zayıf yönleri modüler aritmetiğin kuralları kullanılarak gösterilmiş ve buradan hareketle önerilen algoritmanın kriptoanalizi yapılmıştır. Önce, kriptoanaliz için genel bir bakış açısı verilmiş, daha sonra anahtar bilinmeden şifreli metinden düz metnin nasıl elde edileceği gösterilmiştir. Son olarak yapılan kriptoanalizin sonuçları verilerek yazarın iddiası çürütülmüştür.

2. Şifreleme Algoritması

Önerilen şifreleme algoritmasının esası; Laplace dönüşümü yardımıyla üretilen yerine koyma metodu ile harflerin şifrelenmesine bağlıdır. Şifreleme işlemi Taylor serisi genişlemesi kullanılarak gerçekleştirilir. Önerilen algoritma simetrik bir şifreleme algoritması olduğundan, başlangıçta gönderici ile alıcı

arasında bir gizli anahtar belirlenmiştir. Şifreleme algoritması adımları aşağıdaki gibidir:

1.Basamak: Şifreleme süreci başlamadan önce, gönderici ve alıcı bir anahtar üzerinde mutabakat sağlarlar.

2.Basamak: Algoritmada kullanılacak Laplace dönüşümü belirlenir. Önerilen şifreleme algoritmasında Taylor serisi kullanılmıştır. (1) nolu denklemde Taylor serisinin genişlemesi verilmiştir. (2) nolu denklem kullanılarak açık metin belirlenmiştir.

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

Burada $r \in N$ bir sabit olup

$$te^{rt} = t + \frac{rt^2}{1!} + \frac{r^2t^3}{2!} + \frac{r^3t^4}{3!} + \cdots + \frac{r^nt^{n+1}}{n!} + \cdots + \cdots = \sum_{n=0}^{\infty} \frac{(rt)^{n+1}}{n!} \quad (2)$$

A'dan itibaren Z'ye kadar harfler 0'dan 25'e kadar sayılarla yer değiştirilmiştir.

3.Basamak: Verilen "PROFESSOR" açık metni 15 17 14 5 4 18 18 14 17 sayılarına eşitlenmiştir.

Bu sabitler

$$G_0 = 15, G_1 = 17, G_2 = 14, G_3 = 5,$$

$$G_4 = 4, G_5 = 18, G_6 = 18, G_7 = 14,$$

$G_8 = 17,\ G_n = 0\ \ (n \geq 9)$ şeklinde te^{rt} 'nin katsayıları olarak yazılmış;

$f(t) = Gte^{2t}$ de yerine yazılarak

$$f(t) = t\left[G_0 . 1 + G_1 . \frac{2t}{1!} + G_2 \frac{2^2t^2}{2!} + G_3 \frac{2^3t^3}{3!} + G_4 \frac{2^4t^4}{4!} + G_5 \frac{2^5t^5}{5!} + G_6 \frac{2^6t^6}{6!} + G_7 \frac{2^7t^7}{7!} + G_8 \frac{2^8t^8}{8!}\right]$$

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

$$= 15.t + 17.\frac{2t^2}{1!} + 14\frac{2^2t^3}{2!} + 5\frac{2^3t^4}{3!} + 4\frac{2^4t^5}{4!} + 18\frac{2^5t^6}{5!} + 18\frac{2^6t^7}{6!} + 14\frac{2^7t^8}{7!} + 17\frac{2^8t^9}{8!}$$

elde edilmiştir.

4.Basamak: Her iki tarafın Laplace dönüşümü alınarak

$$L\{f(t)\} = L\{Gte^{2t}\}$$

$$= L\left\{t\left[G_0 . 1 + G_1 . \frac{2t}{1!} + G_2 \frac{2^2t^2}{2!} + G_3 \frac{2^3t^3}{3!} + G_4 \frac{2^4t^4}{4!} + G_5 \frac{2^5t^5}{5!} + G_6 \frac{2^6t^6}{6!} + G_7 \frac{2^7t^7}{7!} + G_8 \frac{2^8t^8}{8!}\right]\right\}$$

$$\frac{15}{s^2} + \frac{68}{s^3} + \frac{168}{s^4} + \frac{160}{s^5} + \frac{320}{s^6} + \frac{3456}{s^7} + \frac{8064}{s^8} + \frac{14336}{s^9} + \frac{39168}{s^{10}} \quad (4)$$

elde edilir.

Elde edilen 15 68 168 160 320 3456 8064 14336 39168 katsayıları düzenlenerek mod 26 daki karşılıkları alınır.

15=15 mod26,68=16 mod26,168=12 mod26, 160=4 mod26, 320=8 mod 26,

3456=24 mod26, 8064=4 mod 26,

14336=10 mod26,39168=12 mod 26.

5.Basamak: Gönderici mod işlemindeki bölümleri, 0 2 6 6 12 132 310 351 1506, anahtar olarak gönderir.

$$G_0' = 15, \quad G_1' = 16, \quad G_2' = 12, \quad G_3' = 4, \quad G_4' = 8, \quad G_5' = 24, \quad G_6' = 4, \quad G_7' = 10, \quad G_8' = 12, \quad G_n' = 0 \quad (n \geq 9)$$

Verilen açık metin 15 16 12 4 8 24 4 10 12 şifreli metnine dönüştürülür. Böylece

"PROFESSOR" mesajı "PQMEIYEKM" şekline dönüştürülmüştür.

3. Kriptoanaliz İçin Genel Bir Bakış

1.Durum: Şifreleme planında kullanılan yapılar matematiksel bir modelle belirtilmelidir. Modelin daha basit denklemler tarafından ifade edilmesi için araştırılması gerekiyorsa ya da mümkün değilse, cebirsel bağımlılıklar açıklanmalıdır.

2.Durum: Şifreleme sisteminin bilinen saldırılara dayanıklı olduğu gösterilmelidir. Taylor serisinin genişlemesi ve modüler aritmetiğin esasları uyarınca; metin şifrelenir ve şifresi çözülür.

3.Durum: Şifreleme algoritmasının güvenliği, seçilen anahtar alanına bağlıdır. Anahtar tasarım algoritması matematiksel olarak ifade edilmelidir. Tasarımdan kaynaklanan zayıf anahtarların varlığı araştırılmalıdır.

4.Durum: Şifreleme mimarisinde kullanılan Laplace dönüşümünün özellikleri ayrıntılı bir şekilde incelenmelidir. Unutulmamalıdır ki, şifreleme sistemlerinin karışıklık ve yayılma özelliklerinin, şifreleme planında kullanılan Laplace'de güvenli bir şekilde sağlanması gerekir.

5.Durum: Laplace Dönüşümü ve modları gerçekleştirilirken bölme kuralları nedeniyle ortaya çıkabilecek sorunlar araştırılmalıdır. Çok kuvvetli yapılar kullanılsa da, en küçük açıklığın tüm sistemi etkileyebileceği düşünülerek tasarıma yönelik özel saldırılar araştırılmalıdır.

4. Kriptoanaliz

Bu bölümde, bir önceki bölümde verilen kriptoanalist bakış kullanılarak Laplace tabanlı metin şifreleme algoritmasının [2] kriptoanalizinin nasıl yapılacağı gösterilmiştir. Burada, şifreleme algoritması denklem (5) de gösterildiği gibi basit bir matematiksel model ile ifade edilmiştir. Önerilen algoritmada, rakamların kodlanmış bir metne ve modüler aritmetiğe karşılık geldiği belirtilmektedir. Şifre, modüler aritmetik kurallarına göre çözüldüğünden, gizli anahtarı bilmeye gerek yoktur. Sayılar arasındaki bağımlılıkların varlığı şifreleme bağlamına karşılık gelir ve modüler aritmetiğin dezavantajlarından biridir.

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

Şifreli metin bu yöntem ile aşağıdaki gibi dönüştürülür;

"PQMEIYEKM"→ 15 16 12 4 8 24 4 10 12

Daha sonra

$$G_0.\frac{1!}{0!s^2}+G_1.\frac{2^1.2!}{1!.s^3}+G_2.\frac{2^2.3!}{2!.s^4}+G_3.\frac{2^3.4!}{3!.s^5}+ G_4.\frac{2^6.5!}{4!.s^6}+G_5.\frac{2^7.6!}{5!.s^7}+G_6.\frac{2^8.7!}{6!.s^8}+G_7.\frac{2^9.8!}{7!.s^9}+ G_8\frac{2^{10}.9!}{8!.s^{10}}. \qquad (6)$$

Mod işlemi gereği G_n ler 25'den büyük olamazlar. Buradan hareketle;

$$G_0.1=26.K_0+15\Rightarrow G_0=\frac{26.K_0+15}{1}$$
$$\Rightarrow\begin{cases} K_0=\mathbf{0}\ için\ G_0=\mathbf{15}\end{cases}$$

$$G_1.4=26.K_1+16\Rightarrow G_1=\frac{26.K_1+16}{4}$$
$$\Rightarrow\begin{cases} K_1=\mathbf{2}\ için\ G_1=\mathbf{17}\end{cases}$$

$$G_2.12=26.K_2+12\Rightarrow G_2=\frac{26.K_2+12}{12}$$
$$\Rightarrow\begin{cases} K_2=\mathbf{6}\ için\ G_2=\mathbf{14}\end{cases}$$

$$G_3.32=26.K_3+4\Rightarrow G_3=\frac{26.K_3+4}{32}$$
$$\Rightarrow\begin{cases} K_{3,0}=22\ için\ G_{3,0}=18\\ K_{3,1}=\mathbf{6}\ için\ G_{3,0}=\mathbf{5}\end{cases}$$

$$G_4.80 = 26.K_4 + 8 \Rightarrow G_4 = \frac{26.K_4 + 8}{80}$$
$$\Rightarrow \begin{cases} K_4 = \mathbf{12}\ için\ G_4 = \mathbf{4} \end{cases}$$

$$G_5.192 = 26.K_5 + 24 \Rightarrow G_5 = \frac{26.K_5 + 24}{192}$$
$$\Rightarrow \{\ K_5 = \mathbf{132}\ için\ G_5 = \mathbf{18}$$

$$G_6.448 = 26.K_6 + 4 \Rightarrow G_6 = \frac{26.K_6 + 4}{448}$$
$$\Rightarrow \begin{cases} K_6 = \mathbf{310}\ için\ G_6 = \mathbf{18} \end{cases}$$

$$G_7.1024 = 26.K_7 + 10 \Rightarrow G_7 = \frac{26.K_7 + 10}{1024}$$
$$\Rightarrow \begin{cases} K_7 = \mathbf{551}\ için\ G_7 = \mathbf{14} \end{cases}$$

$$G_8.2304 = 26.K_8 + 12 \Rightarrow G_8 = \frac{26.K_8 + 12}{2304}$$
$$\Rightarrow\ K_8 = \mathbf{1506}\ için\ G_8 = \mathbf{17}$$

değerleri bulunur ve

15 17 14 5 4 18 18 14 17 → "PROFESSOR" açık metnine ulaşılır.

5. Sonuç

Hiwarekar tarafından simetrik bir şifreleme algoritması önerilmiştir [2]. Önerilen algoritmada, gönderen ile alıcı arasındaki şifreli metin, modüler aritmetik kullanılarak çözülmüştür. Yani, anahtarı bilmeden, şifreli algoritma yalnızca şifreli metni görerek, basit bölünebilme ve modül teorisi ile bir bilgisayar olmadan kırılmıştır. Bu ise yazarın kırılması imkânsız bir algoritma ürettiği iddiasını çürütmektedir.

6. Kaynaklar

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. (2013). A new method of cryptography using Laplace transform of Hyperbolic functions, International Journal of Mathematical Archive, 4/2 : 208-213.

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.