Fırat Üniv. Müh. Bil. Dergisi
28(2), 217-220, 2016

Science and Eng. J of Fırat Univ.
28(2), 217-220, 2016

Kriptolojide İntegral Dönüşümünün Kullanımı

Muharrem Tuncay GENÇOĞLU
Teknik Bilimler M.Y.O., Fırat üniversitesi, Elazığ-TÜRKİYE
mt.gencoglu@firat.edu.tr

(Geliş/Received: 06.06.2016; Kabul/Accepted: 13.07.2016)

Özet

Bu çalışmada farklı bir kriptolojik yöntem genişletilmiş Laplace dönüşümü kullanılarak sunulmuştur. Burada, düz metin şifrelemelerinde üstel fonksiyonların genişletilmiş Laplace dönüşümünü kullandığımız, kriptoloji için yeni bir algoritma ortaya konulmuştur ve şifre çözümü için genişletilmiş Laplace dönüşümünün tersinin de uygun olabileceği gösterilmiştir.

Anahtar Kelimeler: Kriptoloji, Şifreleme, Deşifreleme, Laplace Dönüşümü.

Use of Integral Transform in Cryptology

Abstract

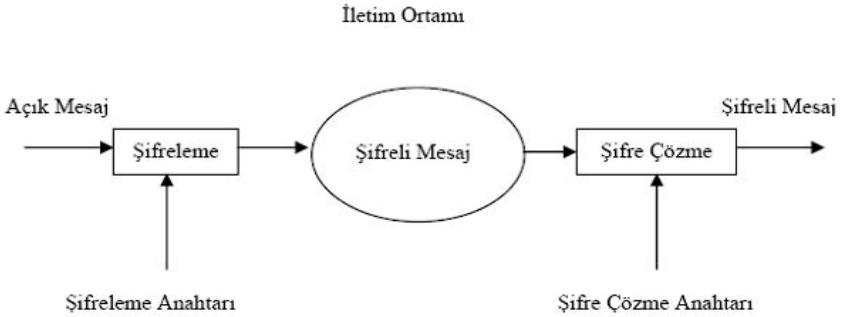
In this paper a different cryptographic method has introduced by using Expanded Laplace transform. Here,A new algorithm has been demonstrated for cryptology that we use expanded Laplace transformation of the exponential function for encryption the plain text and also inverse of expanded Laplace transform has been shown to be suitable for decryption.

Keywords: Cryptology, Encryption, Decryption, Laplace Transform.

1. Giriş

Günümüzde ağ güvenliği problemi çok önemli hale gelmiştir. e-bankacılık, e-ticaret, e-devlet, e-mail, SMS hizmetleri, ATM'lerin güvenliği, finansal bilgilerin varlığı hayatımızın vazgeçilmezi olmuştur.

Kriptolojinin temel amacı iki kişinin güvenli olmayan kanallar üzerinden iletişim kurmasına olanak tanımaktır. İletişim güvenliği günlük aktivitelerde elektronik iletişimin giderek artan kullanımının bir sonucu olarak önem kazanıyor. Kriptoloji güvenlik hizmeti sağlar ve bilgi güvenliğinin birçok alanında kullanılır. Şifreleme özel bilgi olmaksızın onu okunamaz yapmak için bilgi engelleme işlemidir. Bu işlemler bir algoritma ile ifade edilir. Genel olarak bu algoritmalara simetrik algoritmalar denir. Simetrik algoritmalarda, şifreleme anahtarının deşifreleme anahtarından üretilmesi mümkün ve oldukça kolaydır. Bunun tersi de doğrudur. Bu algoritmaların güvenliği anahtar ile bağlantılıdır [2]. Orijinal bilgi düz metin olarak bilinir ve şifreli metin bu metnin şifrelenmiş biçimidir. Şifreli metin mesajı düz metin mesajının tüm bilgilerini içerir fakat o deşifreye uygun bir mekanizma olmaksızın bir insan ya da bilgisayar tarafından okunabilir bir format değildir. Şifre genellikle anahtar olarak adlandırılan harici bilginin bir parçası tarafından parametrelerle ifade edilir. Şifreleme prosedürü algoritma işleminin detaylarının değiştiği anahtara dayalı olarak değişir. Uygun bir anahtar olmadan şifre çözme neredeyse imkânsızdır. Şekil-1 de simetrik bir kripto sistem görülmektedir [5,6].



Şekil 1. Simetrik kripto sistem

2. Ön Hazırlık

Tanım 2.1.

Bir f fonksiyonu tüm t>0 için tanımlı,α bir sabit ve M pozitif bir tamsayı olmak üzere f fonksiyonu $e^{-\propto t}|f(t)| \leq M$ şeklinde yazılabiliyorsa bu f fonksiyonuna üstel mertebeli fonksiyon denir ve buradan

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

yazılabilir. f(t) üstel fonksiyon ise t→∞ için f(t)=∞ olur [1].

Tanım 2.2.

t≥0 ve t,s∈R olmak üzere f(t) üstel fonksiyonu için

$$F(s) = \int_0^\infty e^{-st} f(t)dt \tag{2.2}$$

ise F fonksiyonuna f fonksiyonunun Laplace dönüşümü denir [1]. Tanım 2.1 ve Tanım 2.2 den hareketle f(t) fonksiyonu için Laplace dönüşümünü genişleterek yeni bir dönüşüm fonksiyonunu şu şekilde tanımlayalım;

Tanım 2.3.

Tüm t≥0 reel sayıları için f(t)' nin bir dönüşümü

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

şeklinde tanımlanır.(Genişletilmiş Laplace dönüşümü) f(t)=T⁻¹[F(h)] ile de f(t)' nin ters dönüşümü gösterilir. Elde edilen Genişletilmiş Laplace dönüşümü aşağıdaki standart sonuçlara sahiptir; [3,4]

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

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

3. Uygulama

3.1. Şifreleme

"FIRAT" mesajını göndermek istediğimizi farz edelim;

Öncelikle e^tile genişletilen Taylor serisini göz önüne alalım. Taylor serisi;

$$f(x) = f(a) + \frac{f'(a)}{1!}(x-a) + \frac{f''(a)}{2!}(x-a)^2 + \cdots + \frac{f^n(a)}{n!}(x-a)^n + \cdots = \sum_{n=0}^{\infty} \frac{f^n(a)}{n!}(x-a)^n \tag{3.1}$$

dir. Buradan;

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

serisini t^3 ile genişletirsek

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

olur. Buradan da;

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

elde edilir. Alfabenin harfleri sıfırdan başlanarak numaralandırılırsa "FIRAT" düz metni

6,9,19,0,22 sayılarına eşit olur. K_0=6,K_1=9,K_2=19,K_3=0,K_4=22 değerleri (3.4)'de yerine yazılırsa

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

elde edilir. (3.5)'in her iki tarafına genişletilmiş Laplace dönüşümü uygulanırsa;

$$T[f(t)](h) = T\left[\sum_{n=0}^{\infty} K_n \frac{t^{n+3}}{n!}\right](h) =$$
$$T[K_0 \frac{t^3}{0!} + K_1 \frac{t^4}{1!} + K_2 \frac{t^5}{2!} + K_3 \frac{t^6}{3!} + K_4 \frac{t^7}{4!}](h)$$
$$= 6.3!\, h^3 + 9.4!\, h^4 + 19.5! \frac{h^5}{2!} + 0.6! \frac{h^6}{3!} + 22.7! \frac{h^7}{4!}$$

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

elde edilir. 36,216,1140,0,4620 sayılarının mod(28) deki karşılıkları (K_n) 8,20,20,0,0 dır. Bu sayıların yerine mod işlemindeki bölümler yazılırsa; (K_n') 1,7,40,0,165 anahtarlarını elde ederiz. (3.3) de verilen atamalar kullanılarak "FIRAT" düz metni "HSSAA" olur. Gönderici açık bir şekilde bu mesajı, mesaj ile birlikte; (1,7,40,0,165) gizli anahtarı ve genişletilmiş Laplace dönüşümünü de gönderir. ($8h^3$+$20h^4$+$20h^5$+$0.h^6$+$0h^7$)

3.2. Deşifreleme

Alıcı şifreli mesajı alır. H,S,S,A,A→8,20,20,0,0 ve gizli anahtar değerlerini (1,7,40,0,0,165)

$A_n = \frac{K_n - K_n'}{28}$ ifadesinde yerine yazar.

$\mathbf{36} = 28x1 + 8$
$\mathbf{216} = 28x7 + 20$
$\mathbf{1140} = 28x40 + 20$
$\mathbf{0} = 28x0 + 0$
$\mathbf{4620} = 28x165 + 0$

Böylece 36, 216, 1140, 0, 4620 değerleri

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

denklemine uygulanırsa;

$$\sum_{n=0}^{\infty} K_n (n+3)! \frac{h^{n+3}}{n!} = 36h^3 + 216h^4 + 1140\frac{h^5}{2!} + 0\frac{h^6}{3!} + 4620\frac{h^7}{4!}$$
$$= 6.3!\, h^3 + 9.4!\, h^4 + 19.5!\frac{h^5}{2!} + 0.6!\frac{h^6}{3!} + 22.7!\frac{h^7}{4!} \quad (3.7)$$

elde edilir. (3.7)'nin her iki tarafına ters genişletilmiş Laplace dönüşümü uygulanırsa;

$$T^{-1}\left[\sum_{n=0}^{\infty} K_n (n+3)! \frac{h^{n+3}}{n!}\right] =$$
$$T^{-1}[6.3!\, h^3 + 9.4!\, h^4 + 19.5!\frac{h^5}{2!} + 0.6!\frac{h^6}{3!} + 22.7!\frac{h^7}{4!}\ ]$$
$$\sum_{n=0}^{\infty} K_n \frac{t^{n+3}}{n!} = 6.t^3 + 9.t^4 + 19.\frac{t^5}{2!} + 0.\frac{t^6}{3!} + 22.\frac{t^7}{4!}$$

elde edilir. Burada ki K_n katsayıları dönüştürülürse 6, 9, 19, 0, 22→F,I,R,A,T ilk düz metin elde edilir.

4. Sonuçlar

K_n terimlerinde verilen mesajın şifrelenmesi için $f(t) = Kt^3e^t$ ifadesini dikkate alarak Genişletilmiş Laplace dönüşümünü kullanıp verilen K_n mesajını K_n' ne dönüştürebiliriz. Burada $K_n' = K_n\,(mod28)$ olduğundan anahtar

$A_n = \frac{K_n - K_n'}{28}$ $(n = 0,1,2,\dots)$ dir.

K_n' terimlerinde alınan mesajın deşifrelenmesi için $\frac{Kt^3}{n!}$ ifadesini dikkate alarak Genişletilmiş Laplace dönüşümünü kullanıp verilen K_n'mesajını K_n ne dönüştürebiliriz. Burada $K_n = 28.A_n + K_n'$ $(n = 0,1,2,\dots)$ dir.

Bu çalışmada genişletilmiş Laplace dönüşümü kullanılarak yeni bir kriptolojik uygulama ortaya konuldu. Gizli anahtar(K_n'); mod(28) de 28 ile bölündüğü zaman K_n'nin bölümleridir. Herhangi bir saldırı ile gizli anahtarı bulmak çok zordur. Daha sonra üretilen bu anahtarı genişletilmiş Laplace dönüşümü ve modüler aritmetik tabanlı algoritmanın şifreleme ve deşifrelemesi için kullandık ve algoritmanın en yüksek seviye de güvenlik sağladığını gördük.

5. Kaynaklar

1. Aydın, M., Gökmen, G., Kuryel, B., Gündüz, G. (1990). Diferansiyel Denklemler ve Uygulamaları, Barış Yayınları, İzmir, 429s.

2. Koç, Ç.K., (2009). Cryptographic Engineering. Springer, New York, 517s.

3. Belgacem, F.B.M., Karaballi ,A.A., Kalla, L.S. (2003). Analytical Investigations of the Sumudu Transform and Applications to Integral Productions Equations. Mathematical Problems in Engineering, **3:** 103-118.

4. Bodkhe, D.S., Panchal, S.K., (2015). Use of Sumudu Transform in Cryptography. Bulletin of the Marathwada Mathematical society, **16(2):** 1-6.

5. Martin, K.M. (2012). Everyday Cryptography Fundemental Principles and Applications. Oxford University Press. New York, 553s.

6. Delfs, H., Knebl, H. (2015). Introduction to Cryptography Principles and Applications. Springer, Berlin, 529s.