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].