Düzce Üniversitesi
Bilim ve Teknoloji Dergisi

Araştırma Makalesi

Yayın Şifreleme Şemaları Üzerinde Bir Karşılaştırma: Bir Yeni Yayın Şifreleme Şeması

Hüseyin BODUR [a,*], Resul KARA [b]

[a] *Bilgisayar Mühendisliği Bölümü, Mühendislik Fakültesi, Düzce Üniversitesi, Düzce, TÜRKİYE*
[b] *Bilgisayar Mühendisliği Bölümü, Mühendislik Fakültesi, Düzce Üniversitesi, Düzce, TÜRKİYE*
** Sorumlu yazarın e-posta adresi: huseyinbodur@duzce.edu.tr*

ÖZET

Bir yayın haberleşme yönteminde bir kaynaktan çoklu kullanıcılara mesaj iletimi için genellikle içerisinde şifreleme yöntemlerinin kullanıldığı şemalardan yararlanılır. Bu şema yapıları anahtar sunucu işlemleri açısından merkezi ve de-merkezi olmak üzere ikiye ayrılır. Bu çalışmada günümüzde yaygın olarak kullanılan iki merkezi yöntem olan Mantıksal Anahtar Hiyerarşisi (MAH) ve Tek Yönlü Fonksiyon Ağacı (TFA) şemalarına değinilmiştir. Yayın haberleşme için bir şema önerilmiş ve kullanıcı ekleme/çıkarma işlemlerinde anahtar iletim sayıları-boyutları ve kullanıcılarda bulunan anahtar sayıları-boyutları açılarından mevcut şemalar ile karşılaştırılmıştır.

Anahtar Kelimeler: *Yayın Haberleşme, Mantıksal Anahtar Hiyerarşisi, Tek Yönlü Fonksiyon Ağacı.*

A Comparison on Broadcast Encryption Schemes: A New Broadcast Encryption Scheme

ABSTRACT

In a broadcast communication method,the schemes in which encryption methods are used are often used to transmit messages from a source to multiple users. These schemes are divided into central and de-central in terms of key server operations. In this work, two central methods which are widely used nowadays are mentioned: Logical Key Hierarchy (LKH) and One Way Function Tree (OFT) schemes. A scheme for broadcast communication is proposed and compared with the existing schemes in terms of numbers-sizes of key transmissions in user joining/removing and numbers-sizes of keys in the user.

Keywords: *Broadcast Communication, Logical Key Hierarchy, One Way Function Tree*

Geliş: 07/01/2019, Düzeltme: 23/01/2019, Kabul: 25/01/2019