

Kablosuz Ağlarda Şifreleme Algoritmalarının Performans Analizi

Selçuk ÖKDEM¹, Mehmet KIRTAY^{2*}

¹Bilgisayar Mühendisliği / Mühendislik Fakültesi, Erciyes Üniversitesi , Kayseri

²Meslek Yüksekokulu, Nevşehir Hacı Bektaş Veli Üniversitesi, Nevşehir

*(mehmet@nevsehir.edu.tr) Email

ÖZET

İnternette yaygın veri kullanımı ve kapasitesi her geçen gün hızla artmaktadır. Bu nedenle bu verilerin aktarımı veya iletimi sırasında veri güvenliği önem arz etmekle birlikte bir çok veri şifreleme algoritmaları kullanılmaktadır. Literatürde en yaygın kullanılan algoritma çeşitleri TEA, XTEA, AES, DES, RSA, RC5 algoritmalarıdır. Literatürde bu şifreleme algoritmalarının performans analizi ile ilgili bir çok çalışma bulunmasına rağmen bunların altısının birbiri ile kıyaslanması hakkında çalışma bulunmamaktadır. Bu çalışmada literatürden farklı olarak bu altı algoritma gerçekleşme süresi ve dosya boyutu bakımından karşılaştırılarak birbirlerine göre üstünlükleri veya dezavantajları incelenmiştir.

Anahtar Kelimeler: Şifreleme Algoritmaları, TEA, XTEA, AES, DES, RSA, RC5 , veri güvenliği, performans analizi

Performance Analysis of Encryption Algorithms in Wireless Networks

Selçuk Ökdem¹ , Mehmet Kırtay^{2*}

¹Computer Engineering Department / Engineering Faculty, Erciyes University, Kayseri

² Vocational School, Nevşehir Hacı Bektaş Veli University, Nevşehir

*(mehmet@nevsehir.edu.tr) Email

Abstract

The widespread usage and capacity of the internet is rapidly increasing day by day. For this reason, data security is important during transmission or transmission of these data. To provide this security, many data encryption algorithms are used. The most widely used algorithm types in the literature are TEA, XTEA, AES, DES, RSA, Rc5 algorithms. Although there are many studies about the performance analysis of these encryption algorithms in the literature, there is no study about the comparison of the six of them. In this study, the six algorithms were compared in terms of actualization time and file size, and their advantages or disadvantages were examined.

Keywords: encryption algorithms, TEA, XTEA, AES, DES, RSA, RC5 ,data security, performance analysis.

ISAS 2018

International Symposium on Innovative Approaches in Scientific Studies
