SETSCI Conference Indexing System,
Volume 2 (2018), 461-464

ISAS 2018
I^st International Symposium on Innovative Approaches in Scientific Studies
April 11-13, 2018, Kemer-Antalya, Turkey

Kablosuz Ağlarda Şifreleme Algoritmalarının Performans Analizi

Selçuk ÖKDEM[1], Mehmet KIRTAY[2*]

[1]*Bilgisayar Mühendisliği/MühendislikFakültesi, ErciyesÜniversitesi,Kayseri*
[2]*Meslek Yüksekokulu, NevsehirHacıBektaşVeliUniversitesi, Nevşehir*
[*]*Corresponding author: mehmet@nevsehir.edu.tr*
[+]*Speaker: mehmet@nevsehir.edu.tr*
Presentation/Paper Type: Oral / Full Paper

ÖZET

İnternette yaygın veri kullanımı ve kapasitesi her geçen gün hızla artmaktadır. Bu nedenle, bu verilerin aktarımı veya iletimi sırasında veri güvenliği önem arz etmektedir. Dolayısıyla, birçok 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 bildiride literatürden farklı olarak bu altı algoritmanın işlem süresi ve hafıza gereksinimi yönünden karşılaştırılmaları ve birbirlerine göre üstünlükleri veya dezavantajları konusunda çalışma yapılmıştır.

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

I.GİRİŞ

Günümüzde haberleşme ve iletişim için internet ortamı yoğun olarak kullanıldığından dolayı bilgi güvenliği önemli bir kavram haline gelmiştir. Dijital ortamda kullanılan verilerin üçüncü şahıslar tarafından ulaşılmaması için birçok yöntem kullanılmıştır. Bu yöntemlerden biriside şifreleme işlemidir. Şifreleme verinin belirli bir teknikle mesajın anlaşılamaz bir biçime dönüştürülmesi işlemidir. Verinin orijinal şekline açık metin, dönüştürülmüş haline şifreli metin denir [1].

Şifreleme işlemi için 2 yöntem kullanılmaktadır. Bunlar "Simetrik Şifreleme" ve "Asimetrik Şifreleme" olarak tanımlanmaktadır. Simetrik şifreleme aynı anahtar ile hem şifreleme hem de çözme işlemi yapılırken, asimetrik şifreleme de ise şifreleme işlemi için genel (Public) anahtar kullanılırken, çözme işlemi için özel (Private) anahtar kullanılmaktadır [2].

Bu çalışmanın diğer bölümlerinde daha önce yapılan çalışmalar incelenmiş, bu çalışmalarda kullanılan şifreleme algoritmaları hakkında kısa bilgi verilmiş ve yapılan çalışma anlatılmıştır. Sonraki bölümde ise çalışmanın sonuçları açıklanmıştır.

II. MATERYALLER VE YÖNTEM

A.Önceki Çalışmalar

H. Kodaz ve F. M. Botsalı simetrik ve asimetrik şifreleme algoritmalarının avantaj ve dezavantajları üzerinde durmuşlardır [3]. Bu çalışmada Simetrik şifreleme işleminde anahtarın karşı tarafa ulaştırmada güvenlik sorunu olarak ortaya koyarken Asimetrik şifrelemenin simetrik şifrelemeye göre daha uzun sürdüğünü ortaya koymuşlardır [3].

Aamer Nadeem ve M. Younus Javed simetrik şifreleme algoritmalarının dördü, yani DES, 3DES, AES (Rijndael) ve Blowfish algoritmalarının performansı, farklı içeriklerdeki ve farklı içeriklerdeki girdi dosyalarını şifrelemek suretiyle karşılaştırmışlardır [4]. Yaptıkları çalışmaya göre Blowfish'in, uygulama için seçilen algoritmalar arasında en iyi performans gösteren algoritma olduğu sonucuna varmışlarıdır [4].

S.B. Akben ve A. Subasi RSA (Rivest, Shamir, Adelman) ve Eliptik Eğri Şifreleme algoritmalarını performans açısından karşılaştırmışlardır [5]. Bu çalışmada RSA Eliptik Eğri Şifreleme algoritmasına göre daha yavaş ve güvensiz olduğunu belirtmişlerdir [5].

Çakıroğlu ve diğerleri [6] SEA algoritmasını AES ve RC6 algoritması ile karşılaştırmışlardır. Yaptıkları çalışmaya göre, SEA, her iki alternatif algoritmaya kıyasla daha az kod belleği boyutu gerektirir. Veri hafızasına gelince, SEA'nın AES'den daha az bellek boyutuna ihtiyacı vardır, ancak RC6 SEA'dan daha az bellek boyutu gerektirir. Ayrıca, SEA AES tarafından aşılmış olmasına rağmen, yürütme süresi ve

bant genişliği açısından RC6'ya göre daha iyi bir performansa sahip olduğunu ortaya koymuşlarıdır [6].

Luo ve diğerleri [7] yaptıkları çalışmada SEAL, RC4, RC5 Ve TEA algoritmaların şifreleme ve şifre çözme süreleri ve kapladıkları kod boyutlarını karşılaştırmaları sonucunda TEA algoritmasının kod yapısının kolay ve basit olmasına ile birlikte en az yer kapladığını ve en iyi performansı gösterdiğini ortaya koymuşlardır [7].

B. Şifreleme Algoritmaları

i. Tiny Encryption Algorithm (TEA)

Tiny Şifreleme Algoritması (TEA) ilk olarak 1994 yılında Roger Needham ve David Wheeler tarafından yayınlandı. TEA başlangıçta algoritmayı depolamak için gereken bellek açısından bakıldığında son derece küçük bir algoritma olarak tasarlanmıştır. Bu, temel işlemleri çok basit hale getirerek başarıldı. Temel işlemler çok basit olduğu için TEA da çok hızlı bir şifreleme algoritması olarak kabul edilir. Bu özellikler, TEA'nın, teknik özelliklerde belirtildiği gibi DES tarafından belirtilen tüm modlarda çalıştırılabildiği gibi, geçmişte zayıf donanım veya yazılım şifreleme uygulamaları için bir seçimdir [8].

ii.Tiny Encryption Algorithm (XTEA)

TEA, Wheeler ve arkadaşları tarafından XTEA'ya (Genişletilmiş TEA) genişletildi. (1997). Kelsey ve ark. Tarafından işaret edilen iki küçük zayıflığın düzeltilmesi önerilmiştir. (1997). TEA gibi, XTEA aritmetik ve mantıksal işlemleri kullanır [9].

iii.Advanced Encryption Standard (AES)

Gelişmiş Şifreleme Standardı (AES), ABD hükümeti tarafından kabul edilen bir şifreleme standardıdır. Standart, orijinal olarak Rijndael olarak yayınlanan daha büyük bir koleksiyondan kabul edilen üç blok şifreleri, AES 128, AES-192 ve AES-256 içerir. Her bir AES şifresinin, sırasıyla 128, 192 ve 256 bit anahtar boyutlarında 128 bit blok boyutu vardır. AES şifreleri kapsamlı bir şekilde analiz edilmiştir ve şu anda dünya çapında kullanılmaktadır [10].

iv.Data Encryption Standard (DES)

Veri Şifreleme Standardı (DES) 1976 yılında Amerika Birleşik Devletleri tarafından resmi FIPS standardı olarak seçilen ve daha sonra uluslararası alanda yaygın olarak kullanılmaya başlanan bir şifreleme yöntemidir [11].

Ulusal Standartlar Bürosu (NBS). Bu standardı, Veri Şifreleme Standardı'nı kullanmadan önce ya da çakışarak Federal bilgisayar sistemlerine uygulanabilen ve uygulanması gereken diğer bilgisayar güvenlik önlemleri ile birlikte ele almıştır [12].

v. RSA (R.Rivest, A.Shamir ve L.Adleman)

RSA R. Rivest, A. Shamir ve L. Adleman tarafından asimetrik şifreleme algoritması olarak geliştirildi. Çalışmalarında anahtar dağıtımının yanında şifreleme ve deşifreleme işlemlerini de gerçekleştirmişlerdir. RSA şifreleme sisteminde şifreli veriyi oluşturabilmek için bir açık anahtara ihtiyaç vardır. Şifreli veriyi alan kişinin de bilgiyi deşifre edebilmesi için gizli anahtarının olması gerekir [1].

vi. RC5

RC5 1994'te Ron Rivest tarafından tasarlanan bir simetrik blok şifreleme algoritmasıdır. RC5'in yeni bir özelliği, veriye bağımlı rotasyonların ağır kullanımıdır. RC5 değişken bir kelime boyutuna, değişken bir sayıya ve değişken uzunlukta bir gizli anahtara sahiptir. Şifreleme ve şifre çözme algoritmaları son derece basittir [13].

C. Uygulama

Bu çalışmada şifreleme algoritmalarının aynı boyuttaki veriyi şifreleme süreleri, şifre çözme süreleri ve şifreli metinlerin hafızada kapladıkları boyutları açısından incelenmiştir. Bu amaçla TEA, XTEA, AES, DES, RSA ve RC5 algoritmalarının performans analizi yapılmıştır.

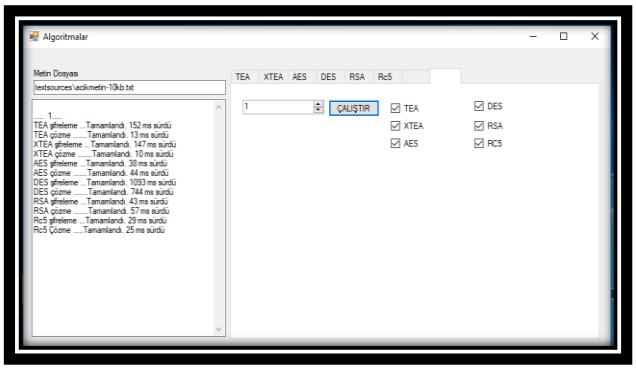
Bu çalışmada algoritmaların performans analizini gerçekleştirebilmek için kullanılan ortam;

- Visual Studio geliştirme ortamı
- C# kullanılarak algoritmalar yazılmıştır.
- İşlemci : İntel(R) Core(TM)2 Duo CPU T9400 2.53 GHz
- İşletim Sistemi : Windows 10
- Güvenli MOD ortamından test edilmiştir.

Bu çalışmada kullanılan dosya boyutları;

- 100 KB
- 200 KB
- 300 KB
- 400 KB
- 500 KB

Yapılan çalışmada mevcut 6 algoritmaların yazılımı kodlaması yapılıp her bir algoritmanın ayrı ayrı olarak açık metini şifreleme işlemi ve şifreli metnin açık metne dönüştürülme işlemleri gerçekleştirilmiştir. Yapılan simülasyon ortamı Resim1 de gösterilmiştir.

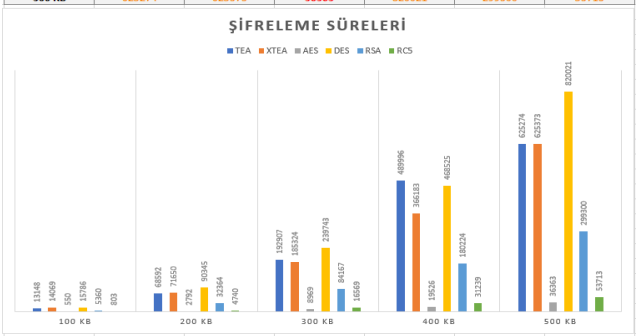


Resim 1. Yapılan Simülasyonun Görüntüsü

i. Şifreleme Performans Karşılaştırması;

Şifreleme işlemleri yapılırken açık metin algoritmaya gönderildiği anda sayaç başlatıldı ve şifreleme işlemi sona erdiği anda sayaç durdurulup şifreleme işlemi için geçen süre tespit edildi. TEA, XTEA, AES, DES, RSA ve RC5 algoritmaları 100 KB, 200 KB, 300 KB, 400 KB ve 500 KB açık metinleri şifreleme süreleri karşılaştırması Tablo1'de gösterilmiştir. Tablo1'de de görüleceği gibi en iyi şifreleme süresini AES algoritması gerçekleştirirken XTEA algoritması en uzun sürede şifreleme işlemini gerçekleştirmiştir.

ŞİFRELEME	TEA	XTEA	AES	DES	RSA	RC5
100 KB	13148	14069	550	15786	5360	803
200 KB	68592	71650	2792	90345	32364	4740
300 KB	192907	185324	8969	239743	84167	16569
400 KB	489996	366183	19526	468525	180224	31239
500 KB	625274	625373	36363	820021	299300	53713

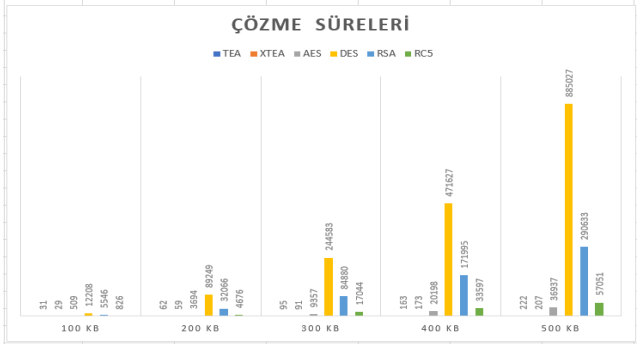


Tablo1. Şifreleme Süreleri

i. Çözme Performans Karşılaştırması;

Algoritmaların çözme süreleri karşılaştırılırken oluşturmuş oldukları şifreli metin algoritmalara gönderilip açık metin elde edilmesi için geçen süre tespit edilmiştir. Şifre çözme işlemleri Tablo2'de görüldüğü gibi TEA ve XTEA en iyi performansı göstermişlerdir. Buna karşın DES algoritması en uzun sürede şifreli metin çözme işlemini gerçekleştirmiştir.

ÇÖZME	TEA	XTEA	AES	DES	RSA	RC5
100 KB	31	29	509	12208	5546	826
200 KB	62	59	3694	89249	32066	4676
300 KB	95	91	9357	244583	84880	17044
400 KB	163	173	20198	471627	171995	33597
500 KB	222	207	36937	885027	290633	57051

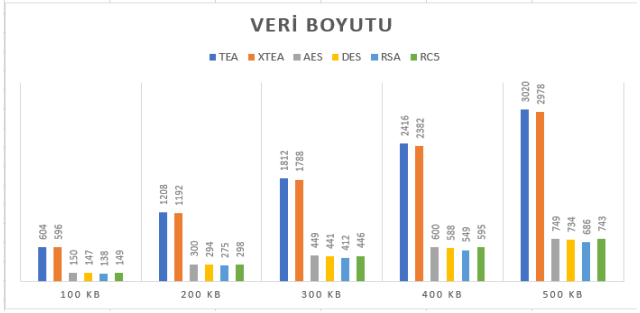


Tablo2. Şifre Çözme Süreleri

iii. Şifreli Metin Boyutları Karşılaştırması;

Şifreleme işlemi gerçekleştirilirken aynı boyuttaki aynı veriler algoritmalara gönderilmiştir. Bunun sonucunda oluşan şifreli metinlerin boyutları farklılık göstermiştir. Şifreli metinlerin boyutları Tablo3'te gösterilmiştir. Tablo3'te görüleceği gibi en az şifreli metin boyutu RSA algoritması gerçekleştirirken TEA algoritması en büyük veri boyutu olarak gerçekleştirmiştir. Veri boyutları incelendiğinde TEA ve XTEA açık metnin yaklaşık 6 katı veri boyutuna ulaşırken, AES, DES, RSA ve RC5 açık metnin yaklaşık 1,5 katı veri boyutuna ulaşmıştır.

VERİ BOYUTU	100 KB	200 KB	300 KB	400 KB	500 KB
TEA	604	1208	1812	2416	3020
XTEA	596	1192	1788	2382	2978
AES	150	300	449	600	749
DES	147	294	441	588	734
RSA	138	275	412	549	686
RC5	149	298	446	595	743



Tablo3. ŞifreliVeri Boyutları

III. BULGULAR

Bu çalışmada, kablosuz ağlarda kullanılan şifreleme algoritmalarının açık metni şifreleme süreleri, şifreli metni çözme süreleri ve şifreli metin boyutları incelenmiştir. Yapılan çalışmada algoritmaların açık metni şifreleme süreleri ve şifreli metni çözme süreleri farklılıklar göstermiştir. Veri boyutlarına baktığımızda şifreli metinlerin boyutları da farklılık göstermektedir.

Yapılan çalışma sonucunda toplam şifreleme ve çözme sürelerinde en iyi performası AES algoritması göstermiştir. Bu karşın XTEA algoritması en uzun süren algoritma olmuştur. Şifreli metinlerin boyutlarına bakıldığında en iyi sonucu RSA algoritması gerçekleştirmiştir.

IV. TARTIŞMA VE SONUÇ

Algoritmaların şifreleme sürelerinde en başarılı algoritma AES algoritmasıdır. TEA ve XTEA algoritmaları şifre çözme işlemini en hızlı gerçekleştirmelerine rağmen şifreleme süreleri uzun olduğundan AES algoritmasında daha uzun süre harcamışlardır. En uzun süren algoritma ise DES algoritması olmuştur. Bu 6 algoritmanın şifreleme işlemi ve şifre çözme işlemi toplam süreleri dikkate alındığında en iyi performansı AES algoritması gösterirken en kötü performansı DES algoritması göstermiştir. Şifreli veri boyutları incelendiğinde RSA'nın şifreli metni en az yer kaplarken, TEA algoritmasının şifreli metni en çok yer kapladığı görülmüştür.

KAYNAKÇA

[1] T. Yerlikaya, E. Buluş& N. Buluş. *"Asimetrik Şifreleme Algoritmalarinda Anahtar Değişim Sistemleri"*.[2006] Akademik Bilişim 2006 (Ab2006), 9-11 Şubat 2006, Denizli.

[2] C. Çiflikli, K.Aba, T.Karakoç *"Arduino Kullanılarak Oluşturulan Kablosuz Sensör Ağında Şifreleme Algoritmalarının Karşılaştırılması "* November 2-4, 2017, Tokat, Turkey

[3] Kodaz H., & BOTSALI, F. M. (2010). "Simetrik Ve Asimetrik Şifreleme Algoritmalarinin Karşılaştırılması". Selçuk-Teknik Dergisi", 9(1), 10-23.

[4] Nadeem, A., &Javed, M. Y. (2005, August). A performance comparison of data encryption algorithms. In Information and communication technologies, 2005. ICICT 2005. First international conference on (pp. 84-89). IEEE.

[5] Akben, S. B., &Subaşı, A. (2005). "RSA ve eliptik eğri algoritmasının performans karşılaştırması". KSÜ Fen ve Mühendislik Dergisi, 8(1), 35-40.

[6] Çakıroglu, M., Cüneyt, B., Ahmet, T. Ö., &Özdemir, Ç. (2010). Performance evaluation of scalable encryption algorithm for wireless sensor Networks. Sci. Res. Essays, 5(9), 856-861.

[7] X. Luo, K. Zheng, Y. Pan, Z. Wu "Encryption algorithms comparisons for wireless networked sensors", in 2004 IEEE International Conference On Systems, Man and Cybernetics, 2004, pp. 1142-1146.

[8] Grabowski, J., &Keurian, J. (2010). Tiny Encryption Algorithm. Internet: http//people. rit. edujwg6168crypto TEA_Grabowski_Keurian. pdf.

[9] Andem, V. R. (2003). A cryptanalysis of the tiny encryption algorithm (Doctoral dissertation, University of Alabama).

[10] Miller, F. P., Vandome, A. F., &McBrewster, J. (2009). Advanced encryption standard.

[11] Standard, D. E. (1999). Data encryption standard. Federal Information Processing Standards Publication.

[12] Davis, R. (1978). The data encryption standard in perspective. IEEE Communications Society Magazine, 16(6), 5-9.

[13] Rivest, R. L. (1994, December). The RC5 encryption algorithm. In International Workshop on Fast Software Encryption (pp. 86-96). Springer, Berlin, Heidelberg.