# ISMSIT2017

**1st International Symposium on Multidisciplinary Studies and Innovative Technologies Proceedings Book**

(November 2-4, 2017, Tokat, Turkey)

Symposium homepage: www.ismsitconf.org


# Arduino Kullanılarak Oluşturulan Kablosuz Sensör Ağında Şifreleme Algoritmalarının Karşılaştırılması


Cebrail Çiflikli[1], Kadir Aba[2*], Tahir Karakoç[3]

[1]*Kayseri Meslek Yüksekokulu, Erciyes Üniversitesi, Türkiye*

[2]*Meslek Yüksekokulu, Nevşehir Hacı Bektaş Veli Üniversitesi, Türkiye*

[3] *Meslek Yüksekokulu, Nevşehir Hacı Bektaş Veli Üniversitesi, Türkiye*

[*]*aba@nevsehir.edu.tr*



***Özet –*** Günümüzde birçok alanda kullanılan Kablosuz Algılayıcı Ağlar genellikle açık alan uygulamalarında kullanıldıkları için dışarıdan gelen farklı saldırılara karşı korumasız durumda olabilirler. Ağı saldırılara karşı korumak ve verilerin güvenliğini sağlamak, Kablosuz Algılayıcı Ağlar için her zaman önemli bir odak noktası olmuştur. İletişimi güvenli hale getirmek için, şifreleme algoritmaları ve veri şifreleme yöntemleri kullanılan yöntemlerden birisi olmuştur. Bu çalışmada da şifreleme algoritmalarından AES, RC5, TEA ve Shamir Sır Paylaşım algoritmalarının kablosuz ortamdaki performansları, şifreleme, şifre çözme, iletim süreleri, veri büyüklükleri ve harcadıkları enerji parametreleri temel alınarak karşılaştırılmıştır. Yapılan çalışma sonucunda 5 farklı alanda karşılaştırılan algoritmalardan AES algoritması toplamda 3 farklı parametrede en başarılı olurken, Shamir ve RC5 algoritmaları ise 2'şer farlı parametrede en başarılı algoritmalar olmuştur. Buna karşın tüm parametreler göz önüne alındığında TEA algoritmasının diğer algoritmalara göre en başarısız algoritma konumundadır. Elde edilen verilere göre TEA algoritması karşılaştırılan 4 algoritma arasında kablosuz sensör ağlarına uygun olmayan algoritma olmuştur.



*Keywords –* K*ablosuz sensör ağları, şifreleme algoritmaları, AES, TEA, RC5, Shamir Sır Paylaşım Algoritması*


## I. GİRİŞ

Günümüzde hayatın dijitalleşmesi ile birçok verimiz internete veya dijital ortama taşınmaya başlandı. Günlük yaşamı dijitalleştiren teknoloji sayesinde artık konuşmalarımızı ve yazışmalarımızı da elektronik ortamda gerçekleştirmeye başladık. Elektronik olarak iletilen veya saklanan verilerin istenmeyen kişiler tarafından ele geçirilmemesi için farklı çözümler arandı. Bunun sonucu olarak veri gizleme yöntemlerinin kullanımı yaygınlaştı. Şifreleme ve veri gizleme algoritmaları hassas veya önemli verilerin güvenliğini sağlamak için kullanılan algoritmalardır. Şifreleme algoritmaları, açık metin (plain text) üzerinde çeşitli işlemler ve değiştirmeler yaparak açık metni şifreli metne (chipher text) dönüştürür. Bilgi güvenliği için yaygın olarak kullanılan birçok şifreleme algoritması vardır. Şifreleme algoritmaları simetrik anahtar ve asimetrik anahtar şifreleme olmak üzere iki gruba ayrılırlar. [1]

Simetrik anahtar şifrelemesi, şifreleme ve şifre çözme işleminin aynı anahtar ile yapıldığı şifreleme işlemleridir. Geleneksel şifreleme olarak da bilinir. Asimetrik şifreleme, bir adet açık anahtar (public key) bir tane de özel anahtar (private key) olmak üzere farklı anahtarlar kullanılarak yapılan şifrelemedir. Açık anahtar şifreleme olarak ta bilinir [1].

Bu çalışmanın diğer bölümlerinde yapılan önceki çalışmalara yer verilmiş, şifreleme algoritmaları ve kablosuz sensör ağları hakkında kısa bilgi verilmiş ve yapılan uygulama anlatılmıştır. Sonraki bölümde ise çalışmanın sonuçları açıklanmıştır.

## II. MATERYALLER VE YÖNTEM

### *A. Önceki Çalışmalar*

Mahajan ve diğ. [2] çalışmalarında ağda iletişim yaparken verilerin güvenliğini sağlamak için kriptografiye odaklanmışlardır. Bu çalışmada [2] AES, DES ve RSA algoritmaları uygulanmış ve bu tekniklerin şifreleme ve şifre çözme anındaki zamanlarının analizlerine dayanan performans karşılaştırması yapmışlardır. 153, 196, 312 ve 868 KB'lık veri paketlerinde yapılan çalışmada şifreleme zamanlarına bakıldığında AES algoritmasının en hızlı, RSA algoritmasının ise en yavaş algoritma olduğu görülmüştür. Aynı paket boyutlarındaki şifre çözme işlemlerinde ise 153KB lık paket hariç tüm paketlerde DES algoritması en hızlı olurken 153KB'lık pakette AES algoritması en hızlı çözen algoritma olmuştur. Tüm paketlerde ise RSA'nın en yavaş algoritma olduğu görülmüştür [2].

Luo ve diğ. [3] algoritmaların şifreleme ve şifre çözme süreleri ve kapladıkları kod boyutları üzerine yaptıkları çalışma, TEA algoritmasının hem en az yer kaplayan hem de en basit algoritma olduğunu göstermektedir. Ayrıca [3]'te TEA algoritmasının diğer algoritmalara göre en hızlı algoritma olduğu ortaya çıkmıştır.

Kaps ve diğ. [4] AES ve SHA-1 algoritmalarının enerji gereksinimleri üzerine yaptıkları çalışmada SHA-1 algoritmasının AES'e göre %10 daha fazla enerji tükettiğini göstermişlerdir.

Alesia [5], 3DES ile AES algoritmalarının güvenlik ve performansları üzerine çalışmalar gerçekleştirmiştir. Güvenlik söz konusu olduğunda AES'in pratik kullanımda kırılamaz olduğunu ve daha hızlı olduğunu söylemiştir.

Sasi ve diğ. [6] DES ve Blowfish algoritmalarını kullanarak yaptıkları çalışmada, algoritmaların çalışma süreleri ve tükettikleri pil kapasitesi üzerine incelemede bulunmuşlardır. Çalışmada [6], Blowfish algoritması daha kısa sürede işlemi yerine getirirken, tam pil kapasitesinin %85'i korunmuştur. Buna karşılık DES algoritmasında pilin %65 seviyesinde olduğunu belirtmişlerdir.

Mushtaque [7], çeşitli simetrik anahtar şifreleme algoritmalarının farklı parametrelere dayalı tam analizlerini sunmuştur. DES ve AES aynı bellek gereksinimine ihtiyaç duymasına karşın AES'in performansı DES'ten çok daha iyi çıkmıştır.

Ramesh ve diğ [8] bilgi güvenliği için şifreleme algoritmalarının performans analizlerini yapmışlardır. DES, AES ve Blowfish algoritmalarının çalışma süresi ve uygulama ve işlem için gerekli bellek parametreleri üzerine araştırma yapmışlardır. Ve Blowfish algoritmasının en iyi performans gösteren algoritma olduğu açıklamışlardır.

Zhang ve diğ. [9], yaptıkları çalışmada Kablosuz Algılayıcı Ağlardaki güvenli iletişimin enerji verimliliğine odaklanmışlardır. Ve sonuç olarak kablosuz algılayıcı ağlarda verileri şifrelemede akış şifreleme yerine blok şifreleme kullanmayı önermişlerdir.

Alanazi ve diğ. [10] üç şifreleme algoritmasının (DES, 3DES ve AES) karşılaştırmalı analizini yapmışlardır. Karşılaştırmada, anahtar uzunluğu, şifre türü, blok boyutu, güvenlik gibi dokuz farklı parametreyi hesaplamışlardır. Ve çalışma sonunda AES algoritmasının DES ve 3DES den daha iyi olduğu ortaya çıkmıştır.

Mandal ve diğ. [11], çalışmalarında yaygın olarak kullanılan iki simetrik şifreleme algoritması olan DES ve AES algoritmalarını hafıza gereksinimi ve gerçekleşme süresi gibi parametreleri kullanarak karşılaştırmışlardır. Ve AES algoritmasının daha kullanılabilir bir algoritma olduğunu söylemişlerdir.

### *B. Şifreleme Algoritmaları*

#### *i. TEA (Tiny Encryption Algorithm)*

TEA minimum hafıza alanı ve maksimum hız hedeflenerek oluşturulmuş bir şifreleme algoritmasıdır. Karışık cebirsel işlemleri kullanan ve Feistel türü bir şifreleme yapan bir algoritmadır [12]. Gömülü sistemlerdeki yüksek performansı, gerçekleme kolaylığı, hızlı olması, düşük enerji tüketimine imkan vermesi, düşük masraflı olması ve güvenli olması hafif (lightweight) olması özelliği ile TEA gömülü sistem tasarımlarına oldukça uygundur [13].

#### *ii. RC5 Algoritması*

Modern şifreleme algoritmaları sınıfında yer alan RC5 algoritması, birçok donanım ile çalışabilmesi ve tüm mikroişlemcilerde yer alan ilkel matematiksel işlemleri kullanıyor olmasından dolayı kendisine avantajlar sağlamaktadır. 16, 32 ve 64 bit kelime uzunlukları ile çalışabilen RC5, değişken boyutlu anahtar uzunluğu ve döngü sayısı sayesinde de kırılması zor şifreleme üretilmesine de imkân tanımaktadır. [14]

#### *iii. Shamir Sır Paylaşım Algoritması*

Adi Shamir tarafından 1979 yılında yapılan çalışma, sır paylaşımı konusunda yapılan ilk çalışma olmuştur [15]. Sır paylaşım algoritmalarının genel yapısı, bir sırrın birden çok kişi tarafından saklanmasıdır. Shamir Sır Paylaşım algoritması polinom tabanlı olup rastgele seçilmiş parametreler üzerine kurulmuştur. n ve t parametreleri sırası ile pay sayısını ve kaç adet pay bir araya gelirse sır değerinin yeniden elde edilebileceğini ifade eden parametrelerdir.

### *C. Kablosuz Sensör Ağları*

Kablosuz Algılayıcı Ağlar güvenlik, afetlere müdahale, savaş gözetimi, üretim otomasyonu, sağlık ve çevre koruma gibi alanlarda gerçekleştirilen uygulamalarda sıklıkla kullanılmaktadır. Bahsedilen uygulamaların tamamı hem güvenli hem de güvenilir veri iletimi gerektirmektedir. KAA'lar (WSN) genellikle ad-hoc ağlardır ve sınırlı güç, hafıza ve bant genişliğine sahiptirler.

Kablosuz algılayıcı ağlar çok sayıda algılayıcı düğümlerin bir araya gelmesi ile oluşur. Her bir algılayıcı düğüm etraftan topladığı bilgiyi bir sonraki düğüme veya baz istasyonuna iletir. Baz istasyonuna iletilen veriler merkez tarafından alınarak değerlendirme ve analizlere tabi tutulurlar. Algılama, işleme, iletişim ve güç ünitelerinden oluşan algılayıcı düğüm ve bunların birleşmesi ile oluşmuş bir kablosuz algılayıcı ağ yapısı şekil 1'de [16] verilmiştir.

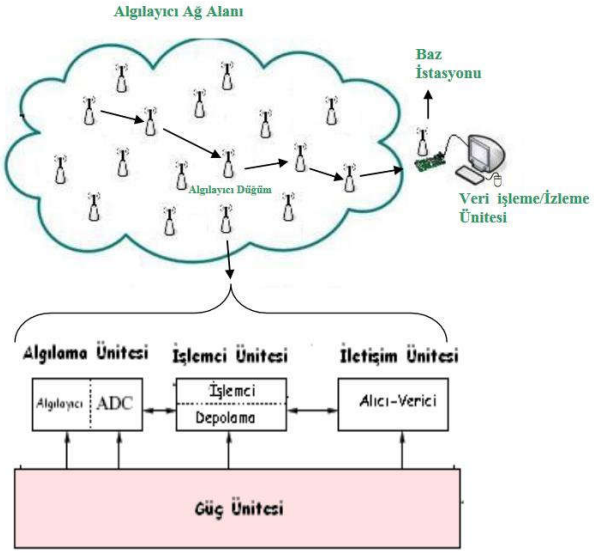


Fig. 1 Örnek bir kablosuz sensör ağı

### *D. Uygulama*

Bu çalışmada 4 şifreleme algoritmasının kablosuz algılayıcı ağlar üzerindeki performansları karşılaştırılmıştır. Bu amaçla AES, TEA, RC5 ve Shamir Sır Paylaşım algoritmaları, şifreleme ve şifre çözme süreleri, şifreleme işlemi sonrası oluşan veri büyüklükleri, iletim süreleri ve harcadıkları enerji bakımından incelenmiştir.

Algoritmaları karşılaştırabilmek için kablosuz alıcı ve vericiden oluşan bir kablosuz ağ ortamı hazırlanmıştır. Hazırlanan kablosuz ortam, veri gönderebilmek için bir adet verici modül ve gelen sinyalleri yakalayabilmek için bir adet de alıcı modülden meydana gelmektedir. Sensörlerden alınan verilerin iletimini temsilen 1, 2, 4, 8, 32 ve 64 KB'lık örnek veriler oluşturulmuştur. Ve tüm testler bu örnek veriler üzerinde gerçekleştirilmiştir.

Oluşturulan kablosuz ortam şekil 2'de de gösterildiği gibi aşağıdaki bileşenlerden meydana gelmektedir.

- 2 adet Arduino Mega 2560 kart
- 2 adet xBee modül
- 2 adet xBee Explorer kart
- Bazı elektronik bileşenler

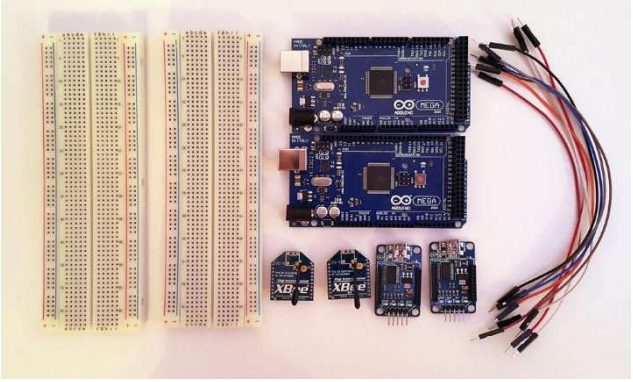

Fig. 2 Kablosuz iletişim ortamını kurmak için kullanılan malzemeler

xBee modüllerinin alıcı veya verici uç olarak çalışabilmeleri için öncelikle buna göre ayarlanmaları gerekmektedir. xBee modülleri bilgisayara bağlanır ve XCTU programı kullanılarak bir tanesi alıcı bir tanesi de gönderici modül olarak ayarlanır. XCTU kullanılarak xBee modüllerinin CH, ID ve CE parametreleri alıcı ve verici olacak şekilde değiştirilmiştir. Şekil 3'de verileri toplayan ve veri gönderen modüller gösterilmiştir. Şekil 4'te ise oluşturulan kablosuz ortam yer almaktadır.

*i. Şifreleme Süreleri:* AES, TEA, RC5 ve Shamir Sır Paylaşım algoritmalarının 1, 2, 4, 8, 16, 32 ve 64 KB boyutundaki veriler kullanılarak yapılan şifreleme testleri sonucunda elde edilen şifreleme süreleri tablo 1'de verilmiştir. Elde edilen süreler değerlendirildiğinde 4 algoritma içerisinde en hızlısının Shamir Sır Paylaşım algoritması olduğu tespit edilmiştir. Buna karşılık TEA algoritması şifreleme süreleri açısından en yavaş algoritma olmuştur. Şifreleme testleri sonucunda elde edilen sürelerin grafiksel gösterimi şekil 5'te verilmiştir.

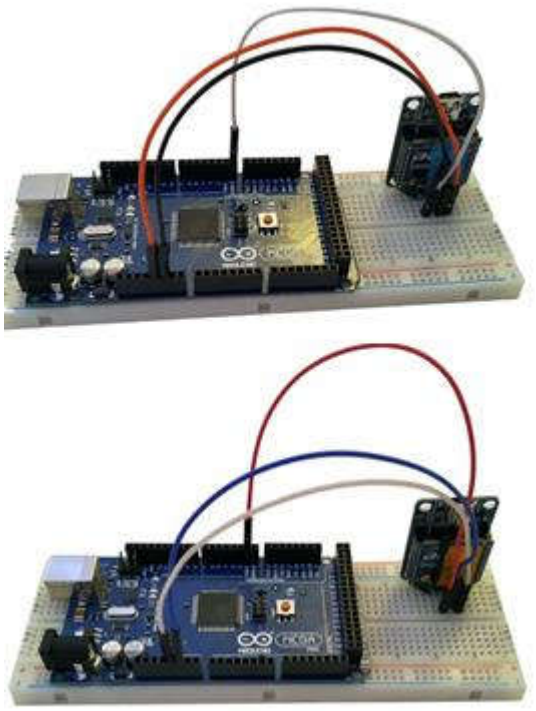

Fig. 3 Gönderici ve alıcı modüller

Fig. 4 Kablosuz ortam

Tablo 1. Şifreleme Süreleri

| | 1KB | 2KB | 4KB | 8KB | 16KB | 32KB | 64KB |
|---|---|---|---|---|---|---|---|
| AES | 166 | 333 | 664 | 1328 | 2655 | 5310 | 10620 |
| TEA | 698 | 1397 | 2792 | 5586 | 11171 | 22340 | 44680 |
| RC5 | 212 | 425 | 851 | 1702 | 3404 | 6808 | 13615 |
| Shamir | 5 | 10 | 19 | 38 | 75 | 149 | 299 |

*ii. Oluşan Şifreli Veri Büyüklükleri:* Şifreleme işlemleri farklı algoritmalar kullanılarak aynı veriler üzerinde gerçekleştirilmiştir. Şifreleme işleminden sonra, şifresiz veri ile şifreli verinin büyüklükleri arasında farklılıklar olduğu gözlemlenmiştir. AES ve RC5 algoritmalarında şifresiz metin ile şifreli metnin kapladığı boyutlar eşitken, Shamir algoritması 3 kat daha büyük, TEA algoritması ise 4 kat daha büyük şifreli metin üretmiştir. 128 byte'lık şifresiz verinin şifrelendikten sonra kapladığı alan tablo 2'de verilmiştir

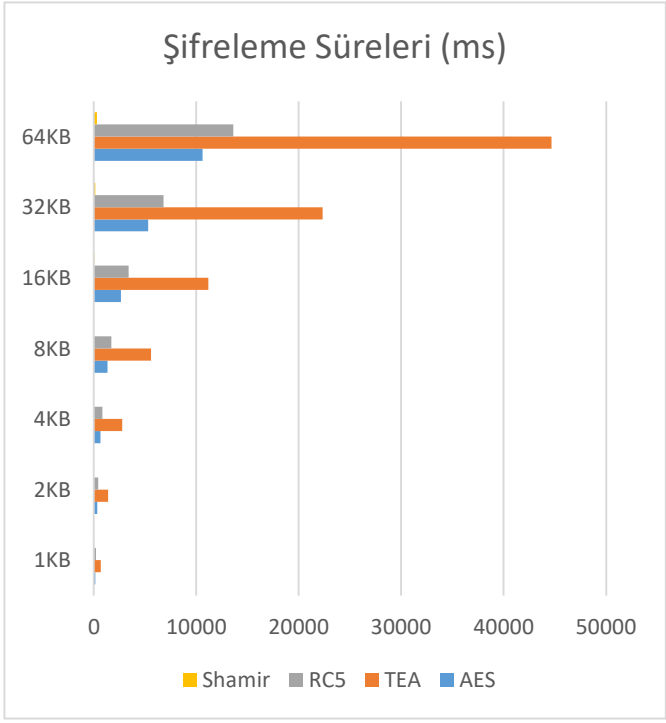


Fig. 5 Algoritmaların şifreleme sürelerinin grafiksel gösterimleri

*iii. Şifre Çözme Süreleri:* Örnek veriler şifrelenip kablosuz olarak iletilir ve alıcı modül tarafından alınır. Alınan şifreli metin üzerinde şifre çözme işlemleri uygulanmıştır. AES, TEA, RC5 ve Shamir Sır Paylaşım algoritmalarının 1, 2, 4, 8, 16, 32 ve 64 KB'lık verileri şifreledikten sonra yeniden bu şifreli metinleri çözmeleri için geçen süreler hesaplanmıştır.

Tablo 2. Şifresiz ve şifreli veri boyutları

| | Veri Boyutu | Şifrelenmiş Veri Boyutu |
|---|---|---|
| AES | 128 byte | 128 byte |
| TEA | 128 byte | 512 byte |
| RC5 | 128 byte | 128 byte |
| Shamir | 128 byte | 384 byte |

Şifreli metinlerin veri büyüklükleri, AES ve RC5'e göre TEA algoritmasında 4 kat, Shamir Sır Paylaşım algoritmasında 3 kat fazladır. Çözme süreleri hesaplanırken bu veri boyutları dikkate alınmıştır. Şifrelemede olduğu gibi, şifreleri çözme işleminde de Shamir Sır Paylaşım algoritması en kısa sürede tamamlanan algoritma olmuştur. Benzer şekilde TEA algoritması da en uzun sürede çözen algoritmadır. Shamir Sır Paylaşım algoritmasının çözmesi gereken veri boyutu diğer algoritmalara göre fazla olmasına rağmen en kısa sürede çözen algoritmadır. Şifre çözme süreleri tablo 3'te verilmiştir. Hesaplanan sürelerin grafiksel gösterimleri ise şekil 6'te yer almaktadır.

Tablo 3. Şifre çözme süreleri

| | 1KB | 2KB | 4KB | 8KB | 16KB | 32KB | 64KB |
|---|---|---|---|---|---|---|---|
| AES | 219 | 438 | 876 | 1753 | 3505 | 7009 | 14018 |
| TEA | 637 | 1274 | 2547 | 5092 | 10185 | 20369 | 40739 |
| RC5 | 230 | 462 | 924 | 1847 | 3695 | 7389 | 14779 |
| Shamir | 56 | 111 | 222 | 443 | 887 | 1772 | 3545 |

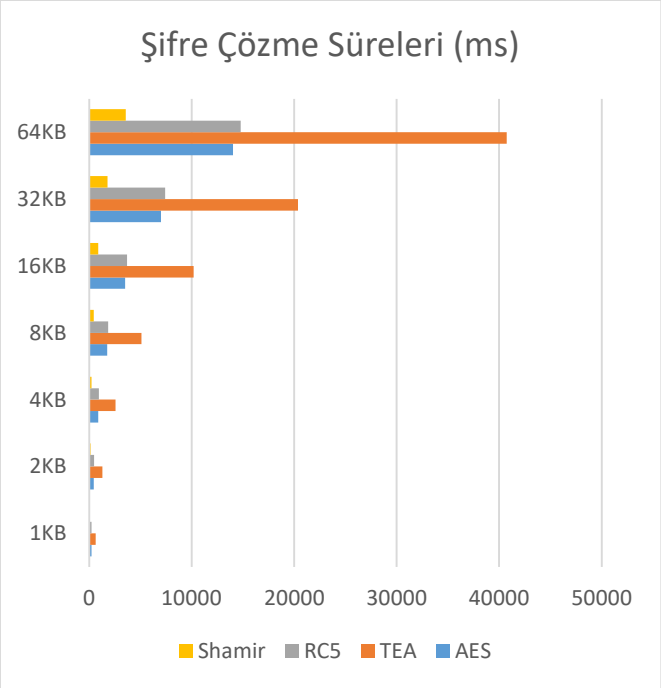


Fig. 6 Algoritmaların şifre çözme sürelerinin grafiksel gösterimleri

*iv. İletim Süreleri:* Şifrelenen metinler gönderici modülden alıcı modüle iletilmektedir. Bunun için de xBee kullanılmıştır. Gönderilen veriler metin bazlı veriler olduğu için her bir algoritma için ortak bir gönderim alt yapısı oluşturulmuş ve yine farklı veri büyüklüklerinde gönderim süreleri test edilmiştir. Verilerin gönderimi byte'lar seviyesinde yapılmıştır ve her 128 byte'lık veriden sonra 330ms bekleme süresi eklenmiştir. Bekleme süresi ekleyerek gönderilen verilerin karşı taraftan doğru bir şekilde alınması amaçlanmıştır.

Gönderim süreleri doğrudan algoritmalara bağlı değildir. Bu nedenle sadece veri boyutları ve verileri gönderirken harcanan süreler hesaplanmıştır.

Tablo 4. Farklı boyutlardaki verilerin iletim süreleri

| Veri Boyutu (KB) | İletim Süresi (ms) |
|---|---|
| 1 | 2833 |
| 2 | 5998 |
| 4 | 12326 |
| 8 | 24984 |
| 16 | 50299 |
| 24 | 75652 |
| 32 | 100930 |

*v. Harcanan Enerji:* Şifreleme, iletim ve şifre çözme işlemleri sırasında çekilen akım değerleri ölçülmüş ve algoritmalardan hangisinin daha fazla hangisinin daha az güç harcadığı tespit edilmiştir. Boş durumda bekleyen Arduino kartlar 0.07A akım çekerken bunlara xBee bağlandığı zaman çekilen akım değerleri 0.014A'ya çıkmıştır. 3 işlem (şifreleme, iletme, şifre çözme) sonrasında en uzun sürede işlem yapan algoritma en çok güç harcayan, en kısa sürede işlem yapan algoritma ise en az güç harcayan algoritma olmuştur.

Aşağıdaki tabloda (tablo 5) 8KB'lık örnek veri için hesaplanan şifreleme, iletme ve şifre çözme süreleri ve bu sürelerin toplamı verilmiştir. Hesaplanan sürelerin grafiksel gösterimleri şekil 7'de gösterilmektedir.

Tablo 5. Algoritmaların şifreleme, iletme ve şifre çözme işlemleri için harcadıkları toplam süreler

| | Şifreleme Süresi (ms) | İletim Süresi (ms) | Çözme Süresi (ms) | Toplam Süre (ms) |
|---|---|---|---|---|
| AES | 1328 | 24984 | 1753 | 28065 |
| TEA | 5586 | 100930 | 5092 | 111608 |
| RC5 | 1702 | 24984 | 1847 | 28533 |
| Shamir | 38 | 75652 | 443 | 76133 |

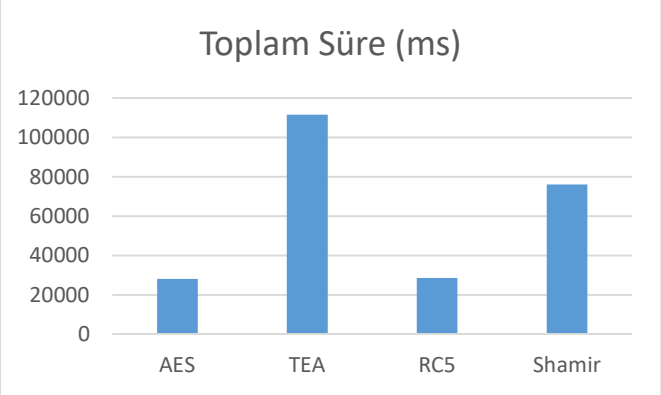


Fig. 7 Toplam sürelerin grafiksel gösterimleri

## III. BULGULAR

Bu çalışmada, veri güvenliği için kullanılan şifreleme algoritmalarının performansları karşılaştırılmıştır. AES, RC5, TEA ve Shamir Sır Paylaşım algoritmalarının şifreleme süreleri, şifre çözme süreleri, veri büyüklükleri, iletim süreleri ve harcadıkları enerji hesaplanmıştır. Sonuçların tutarlı olması için eş değer ortam ve veriler hazırlanmıştır.

Yapılan testler sonucunda kullanılan algoritmaların şifreleme ve şifre çözme süreleri birbirlerinden farklı çıkmıştır. Bununla beraber şifreleme işleminden sonra ortaya çıkan şifreli metin boyutları da farklıdır. Art arda gerçekleştirilen şifreleme, iletme ve çözme sürelerinin toplamı değerlendirildiğinde en hızlı çalışan algoritmanın AES algoritması olduğu görülmüştür. AES algoritmasını sırası ile RC5, Shamir Sır Paylaşım ve TEA algoritmaları takip etmiştir.

xBee modülü çalışırken çekilen akım sabit olduğu için en kısa sürede işlemi tamamlayan algoritma en az enerji harcayan algoritma (AES) olurken, en uzun sürede işlemini tamamlayan algoritma ise en çok enerji harcayan algoritma (TEA) olmuştur.

## IV. TARTIŞMA

Şifreleme ve şifre çözme adımlarında en başarılı algoritma Shamir Sır Paylaşım algoritmasıdır. Bu çalışmada Shamir algoritması için pay değeri 4, sır değerini yeniden oluşturabilmek için 3 eşik değeri referans alınarak yapılmıştır. Pay ve eşik değerlerini artırmak güvenliği artıracaktır fakat harcanan enerji ve işlem süreleri üzerinde olumsuz etki yapacaktır. Çalışma ile ilgili yapılan önceki çalışmalarda da olduğu gibi AES algoritması en başarılı algoritma olmuştur.

## V. SONUÇ

Toplam süre ve harcanan enerjiye göre AES algoritmasının 4 algoritma arasında ki en uygun algoritma ve TEA algoritmasının ise seçilen algoritmalar arasındaki en verimsiz algoritma olduğu belirlenmiştir. Buna karşın TEA algoritması, diğer algoritmalarla karşılaştırıldığında kod karmaşıklığı açısından en sade algoritma durumdadır.

## REFERENCES

[1] G. Singh, Supriya, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security", International Journal of Computer Applications, vol. 67, no. 19, pp.33-38, April, 2013.

[2] P. Mahajan, A. Sachdeva, "A Study of Encryption Algorithms AES, DES and RSA for Security", Global Journal Of Computer Science And Technology Network, Web & Security, vol. 13, no. 15, pp. 15-22, 2013.

[3] 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.

[4] J.P. Kaps, "Energy comparison of AES and SHA-1 for ubiquitous computing", EUC Workshops, vol. 4097, pp. 372-381, 2006.

[5] N. Aleisa, "A Comparison of the 3DES and AES Encryption Standards", International Journal of Security and its Applications, vol. 9, no. 7, pp. 241-246, July, 2015.

[6] S. B. Sasi, N. Sivanandam "A Survey on Cryptography using Optimization algorithms in WSNs", Indian Journal of Science and Technology, vol. 8, no. 3, pp. 216-221, February, 2015.

[7] A. Mushtaque, "Comparative Analysis on Different parameters of Encryption Algorithms for Internet Security", International Journal of Computer Sciences and Engineering, vol. 2, no. 4, pp. 76-82, April, 2014.

[8] A. Ramesh, A. Suruliandi, "Performance Analysis of Encryption Algorithms for Information Security", in Circuits, Power and Computing Technologies (ICCPCT), 2013, pp. 840-844.

[9] X. Zhang, H. M. Heys, C. Li, "Energy efficiency of encryption schemes applied to wireless sensor networks", Security and Communication Networks, pp. 789-808, September, 2011.

[10] H.O. Alanazi et al., "New Comparative Study Between DES, 3DES and AES within Nine Factors", Journal Of Computing, vol. 2, no. 3, pp. 152-157, March, 2010.

[11] A. K. Mandal, C. Parakash, A. Tiwari, "Performance Evaluation of Cryptpgraphic Algorithms: DES and AES", in IEEE Students' Conference on Electrical, Electronics and Computer Science, 2012.

[12] A.Ç. Bağbaba, et al. "JPEG Image Encrryption via TEA Algorithm", Signal Processing and Communications Applications Conference (SIU), 2015, pp. 2090-2093.

[13] M.B. Abdelhalim, et a. , "Implementation of a Modified Lightweight Cryptpgraphic TEA Algorithm in RFID System", in 6th International Conference of Internet Technology and Secured Transactions., Abu Dhabi, United Arab Emirates, 2011, pp. 509-513.

[14] T. Doğan. (2009) RC5 Şifreleme Algoritması. [Online] Available: http://bilgisayarkavramlari.sadievrenseker.com/2009/06/05/rc5-sifreleme-algoritmasi/

[15] A. Shamir, "Shamir, How to share a secret", Communications of the ACM, pp.612-613, 1978

[16] A. E. Tümer, "Bina içi kablosuz algılayıcı ağlar için enerji verimli yönlendirme protokollerinin geliştirilmesi", PdD thesis, Fen Bilimleri Enstitüsü, Selcuk Üniversitesi, Konya, 2011.