AES ADAY ŞİFRELEME ALGORİTMALARININ YAZILIM VE DONANIM PERFORMANS KARŞILAŞTIRILMASI VE UYGULAMALARI

Tarık YERLİKAYA[1] **Ercan BULUŞ[2]** **Derya ARDA[3]**

[1,2,3]Bilgisayar Mühendisliği Bölümü
Mühendislik- Mimarlık Fakültesi
Trakya Üniversitesi, Edirne

[1]e-posta: tarikyer@trakya.edu.tr [2] e-posta: ercanb@trakya.edu.tr
[3] e-posta: deryaa@trakya.edu.tr

Anahtar sözcükler:Şifreleme, Kripto, AES, Rijndael, Performans

ABSTRACT

In 1997, a program was created by NİST to discover AES, which is a new standart crypto algorithm, instead of DES crypto algorithm and a selection was made by looking some choosen criterion. In this program, Rijndael crypto algorithm was selected, which was constituted by Rijndael and it has been standardized as AES. In this study, by using the 128,192,256 bit keys of Rijndael crypto algorithm, the ecript and decript algorithms will be examined and the performances of the AES finalists will be compared.

1.Giriş

Teknolojinin geliştiği ve gelişmeye çok hızlı bir şekilde devam edeceği bu bilgi çağında bilgisayarlar ve internet ortamı hayatımızın vazgeçilmez birer unsuru haline gelmiştir. Böyle bir ortamda bilginin korunması ve bir noktadan bir noktaya iletilmesi çok büyük önem kazanmıştır. Verilerin güvenli bir biçimde aktarımı ve elde edilmesi için, kriptografi bilimi aracılığı ile çeşitli şifreleme, anahtarlama ve çözümleme algoritmaları oluşturulmaktadır. Bu yeni oluşturulan şifreleme algoritmaları gelişen teknolojiye uygun bir şekilde oluşturulmalı ve gelişen teknolojilere uygun tasarlanmalıdır.

Şifreleme algoritmalarını yapısal olarak iki ana gruba ayırabiliriz. Simetrik ve Asimetrik şifreleme algoritmaları. Simetrik şifreleme algoritmaları verileri şifrelemesinde ve de şifrelemesinde tek anahtar, Asimetrik şifreleme algoritmaları şifreleme ve deşifrelemede ayrı iki anahtar kullanmaktadır.

Bu yeni oluşturulan algoritmaların standartlaşması için birçok ülke kendi standartlaştırma enstitülerini kurmuştur. Bunların en önemlisi Amerika'da 1960'da kurulan NİST' tir. NİST 1977 yılında bir simetrik şifreleme algoritması olan Des'i bir standart olarak belirlemiştir. Des uzun yıllar güvenilir bir algoritma olarak kullanıldı. Kriptanalistler teknolojinin gelişimine paralel daha güçlü donanıma sahip bilgisayarlar sayesinde Des kırmak için yoğun bir şekilde uğraştılar. Bunun sonucu olarak Des kırılmıştır ve daha güvenli olan Tdes kullanılmaya başlanmıştır. TDES arka arkaya Des şifreleme algoritmasını tekrarlayarak ortaya çıkmıştır. Des'in ve Tdes' in güvenirliğini kaybetmesiyle NİST yeni şifreleme algoritmalara yönelmiştir [1].

1997'de NIST DES'in yerine AES'i seçemek ve geliştirmek için bir program duyurdu. Onlar tek bir standart geliştirmek için şifreleme topluluğundan algoritmalar istediler. 1998 yılında 15 algoritma kabul edildi ve NIST bunların içinden 5 finalisti 1999 yılında seçti. NIST'in planı 2000 yılında standart olması için bir yada birkaç algoritma seçmekti [2].

Bu çalışmada beş AES finalistinin algoritma yapılarını, yazılım ve donanım performanslarını karşılaştırılıcaktır. Ayrıca en iyi algoritma seçilen Rijndael şifreleme algoritmasının farklı anahtar uzunluklarındaki uygulaması gerçekleştirilecektir

2.AES (Advanced Encryption Standard)

Des'in yerine getirilen AES, daha hızlı daha güçlü ve daha ucuz olmalıydı. Yazılımda kullanıldığı zaman daha hızlı olmakla birlikte donanımda da kolay kullanılabilmeliydi (Smart kart vs). Uzun zaman kullanımda olan Des gibi o da saldırılara uzun süre karşı koymalıydı. Bir çok algoritma uzun süre incelendikten sonra beş tane finalistte karar kılındı.Bunlar **Serpent, Rc6, Rijndael, Twofish** ve **Mars** şifreleme algoritmalarıydı. Bu noktadan sonra bu algoritmalar arasından hangisinin standartlaşması gerektiği hakkında yoğun çalışmalar yapıldı.Bu beş finalist arasında şifreleme ve deşifreleme hızlarının yanında yazılım ve donanım uygunluğu,kolay uygulanması ve en önemli olarak güvenlik performansı açısından incelendi. Bu çalışmalardan

sonra Rijndael şifreleme algoritması birinci olarak seçildi [3].

2.1 Beş AES Finalisti

Mars: Mars, IBM tarafından geliştirilmiştir ve algoritma yapısı olarak Des'e hiçbir özelliği benzememektedir. Mars donanımla birleştiği noktada son derece akla uygun bir şekilde dizayn edilmiş ve de son derece hızlıdır. Bunun anlamı şudur ki: Smart kartlara uygulamak için MARS'ın 70 bin civarında gate'e ihtiyacı vardır. Mars anahtar uzunluğunun 128-448 bit olması gerekmektedir.

Serpent: Cambridge Üniversitesi, Halfa-İsrail ve Bergen Üniversitesi-Norveç tarafından geliştirilen bir şifreleme algoritmasıdır. Serpent temel olarak DES'e benzer, diğer algoritmalarla aynı tipte ve değişkenler temelde son derce anlaşılır bir yapıya sahiptir. 20 yıldan fazla bir çok analizlere direndi. Serpent anahtar alanı 40-256 bit olanağı sağlar. Şifreleme deşifreleme hızı Mars şifreleme algoritmasına göre daha yavaştır.

Rc6: Rc6, Rsa laboratuarlarında geliştirilmiştir. Rc6 ve diğer AES adaylarının arasındaki en büyük bir fark tablolar arası geçiş kullanılmaz, bu byte genişliği azaltır(Smart kartları için önemli bir faktör). Maalesef Rc6, diğer algoritmalar ile karşılaştırıldığında en yavaş şifreleme algoritmadır. Çünkü bu algoritma temelde uygulanan basit donanım operasyonlarını kullanır, 100 saniyede 1Gigabit civarında yetenekli olması gerekir. Bu daha sonra yeterli iken çoğu güncel uygulamaların sorunları 10 yıl içinde ortaya çıkabilir. Rc6 daima anahtar genişliğinin 256 bitten daha geniş olmasını ister.

Rijndael: Rijndael, bir Alman bankası tarafından geliştirildi ve bir çok ATM'lerde kullanıldı, ve bu gösteriyor ki bir çok önyargıları bu önledi. Rijndael'in anahtar genişliği 8bit işlemciler için oldukça etkileyicidir, kod uzunluğu 1K'nın üzerindedir ve 256 bitlik anahtar kullanıldığında RAM'in gereksinimi 52 bytedir(daha küçük anahtarlar olmadıkça). ANSI C de 27Mbit/s ile 128bitlik anahtarı ve 19.8Mbit/s ile 256 bit anahtarı çalıştırır. C++'ı kullanmak numaraları %250 oranında arttırır, 70.5 Mbit/s ile 128 bit anahtarı ve 51.2 Mbit/s ile 256 bit anahtarı çalıştırır.

Twofish: Twofish, bir US Counterpane Systems şirketi tarafından geliştirilmiştir. 256 bit üzerindeki anahtar boyutlarını destekler,çok aşırı hızlıdır .

3. BEŞ AES FİNALİSTİNİN PERFORMANSININ KARŞILAŞTIRILMASI

Şifreleme algoritmalarının dizayn edilmesindeki ana amaç güvenlik olmalıdır. Gerçek dünyada performansla uygulama maliyetleri birbiriyle alakalıdır. En önemli özellikleri: algoritmaların performanslar ve maliyetlerdir.

Aday algoritmaların çeşitli platformlardaki performanslarını karşılaştıracağız. Bu platformlar; 32 bit işlemci, 64 bit işlemci, 8 bit akıllı kart işlemci ve donanım olacaktır [4].

3.1 32 Bit İşlemcide Performans Karşılaştırılması

Mars: Mars geniş operatör sistemli, yönlendirme ve çarpma yapan 82'e 32 bitlik S-kutusu içeren hızlı bir yazılım sistemidir. Mars blok başına 390 saatle AES finalistleri içinde en hızlısı olarak düşünülür. Bu hızının sebebi değişik derleme sistemi kullanılmasıdır. Mars şifrelemesinin 3 basamağı vardır; giriş ileri karıştırma, cryptographic öz ve son karıştırma [4].

Rc6: Rc6 en zarif ve AES finalistlerinin kolayca anlaşılanıdır. AES'in hedef platformunda, Assembly dilinde blok başına 250 saatle en hızlı algoritmadır. RC6 birçok platformda istenilen sonucu vermemektedir. Genellikle donanım uyuşmazlığı vardır.

Rijndael: Rijndael bir diğer kare varvasyonudur. Bütün platformlarda çok iyi çalışan hızlı bir yazılımdır(cipher). Temiz matematiksel yapısı övünç kaynağıdır. Şifreleme ve şifre çözme algoritmaları tam olarak mantıklı olmasa da genel yapıları ve performansları tartışılmazdır [4].

Serpent: Serpent 32 bit işlemcilerde "bit-slice" uygulamalarına imkan sağlamak için dizayn edilmiştir. Assembly dilinde Serpent, Des uygulamasından daha yavaştır. (45 saat/byte).

Twofish: Twofish Pentium da AES parçalarının en hızlısı ve Pentium Pro 2 de en iyi ikinci hızlısıdır. Sadece basit RISK işlemlerinde kullanılır ve performansı diğer 32 bit platformlarla karşılaştırılabilir.

3.2 Smart Kart Performansının Algoritmalar Üzerindeki Yorumu

Mars: Mars 2 KB ROM gerektirdiği için , bu durum S-kutusunda bazı sorunlara yol açar. Bu büyüklük tek başına diğer AES finalistlerinin toplamından büyüktür. Kod büyüklüğü hakkında bir tahmin yapılamaz, fakat genellikle 3 KB'nin altındadır.

Mars'ın üzerindeki fly-subkey jenerasyonu bulunmaz ve aynı zamanda RAM'de 160 Byte subkey gerektirir. 16 byte Plaintext ve 16 Byte anahtar eklendiğinde diğer değişkenlerde arttırılır.Mars'ta bu kullanımların çarpımların kullanımı değişkenlerin rotasyona uğraması ve artışlar zamanlaşmış artıkları mümkün kılar.

Rc6: RC6'nın küçük kod boyutu Smart Card kelimelerini taşımalıdır. 8 bit Cpu'lardaki zayıf performansı küçük bir sorundur. Fakat Cpu'ların

çoğunda bir problem olmaz.RC6 da fly-subkey jenerasyonu bulunmaz ve RAM de 176 Byte subkey gerektirir. 16 Byte Plaintext ve anahtar eklendiğinde diğer değişkenleri artırır.

Rijndael: Rijndael Smart Card'ın içinde DR98b dikkate alınarak dizayn edilmiştir. Üzerindeki fly-subkey RAM'i minimum kullanılmasında izin verir. Eğer subkey'ın hesaplanması için 160 Byte bulunursa rijndael daha hızlı olabilirdi. Sadece negatif değerler üzerinde deşifreleme fonksiyonlarının yerine getiremez.

Serpent: ROM ayak izi çok küçüktür.(1 KB'nin altında). Serpent üzerindeki fly-key programı çok küçük RAM kullanımına izin verir.

Twofish: Twofish Smart card'lar dikkate alınarak dizayn edilmiştir. Subkey'i fly da hesaplanabilirdi. Şifreleme ve deşifreleme RAM'in 60 Byte'ı kullanılarak yapılabilirdi. Şifreleme ve deşifreleme aynı hızdadır. Biraz daha RAM kullanılabilirse Twofish'in şifrelemesi ve deşifrelemesi daha hızlı olabilirdi.

3.3 Donanım Performansının Karşılaştırılması

AES finalistlerinin şifreleme ve deşifreleme işlemleri genel olarak hızlı görünür. AES finalistlerinin karşılaştırılması ise oldukça zordur. Birçok tahmin edici karışık farklı işlem teknolojisi, farklı ölçüm büyüklükleri ve dizayn metodları kullanılır [4].

Mars: Mars donanım uygulamasını kullanışsız yapar. Bir uygulama tam bir çarpıcı tam bir yönlendirici ve geniş bir S-kutusu Rom'u gerektirir. Blokların her biri makul performanslı küçük donanım modülü oluşturmakla geniş ve sınırlıdır. Mars kağıdı diğer finalistlerden daha geniş olan 70000 "cell" büyüklüğünü kabul eder. Mars'ın donanımdaki anahtar çevikliği düşüktür [3].

Rc6: Bu algoritmanın basitliği donanım için çok uygundur. Birçok kullanışlı hız-büyüklük tradeoff'u vardır. Zaman çarpıcı ve yönlendirici kullanması veya tekli çarpıcı ve yönlendirici kullanması gibi.

Rijndael: Rıjndael donanımı çok iyi tamamlar ve işletir. Rijndael'in donanımdaki en büyük ilişkisi tam paralel versiyonu 16-256 Byte ROM gerektirmesidir. Bu yüksek performans dizaynı için makul değildir. Ama kapı aşama S-kutusu özellikle donanım büyüklüğünü kesmektedir. Rıjndael'in düşük performanslı versiyonunu bir kaç tane S-kutusu ROM'la oluşturmak oldukça kolaydır. Donanımla deşifrelemeyi oluşturmak cip büyüklüğünü 2 katına çıkarmakla mümkündür.

Serpent: Serpent donanımı çok makul şekilde tamamlar. Değiş tokuş uygulamasını çok iyi oluşturur. Tam paralel versiyonu toplam 256 S-kutusu gerektirir. Devir fonksiyonu çok hızlı çalışır ve devir performans başına çok iyi sonuç verir. Deşifreleme çarpık permütasyon ve lineer değiştirme gerektirir. Donanımdaki anahtar çevikliği çok iyidir.

Twofish: Twofish akıllarda donanım performans uygulamalarının başından ilan edilmiştir. Algoritmayı yüksek hız ve alçak kapı sayma uygulamasındaki birçok uygun boşluk-zaman değiş tokuşu vardır. Anahtar çevikliği şifreleme ve deşifreleme için yüksektir. Çünkü anahtar programlaması fly'ın her yönünde çalışabilir. Bu özellik hiçbir adayda yoktur.

3.4 Fonksiyon Anahtar Uzunluklarının Performansı

Mars, Serpent ve Rc6'ın hızları anahtar uzunluğuna bağlı değildir. Twofish, şifreleme ve deşifrelemenin hızları anahtar değerden bağımsızdır. Ama; uzun anahtarları setup yapmak çok uzun zaman alır. Rıjndael uzun anahtarlar için oldukça yavaş bir şekilde şifreleme ve deşifreleme yapar ve uzun anahtarları setup yapmak için çok büyük zaman alır [4].

Tablo 1. *Algoritmaların anahtar setup yapısı*

Algoritma İmi	Anahtar Setup	Şifreleme
MARS	DEĞİŞMEZ	DEĞİŞMEZ
RC6	DEĞİŞMEZ	DEĞİŞMEZ
RIJNDAEL	ARTAR	128 : 10 Döngü 192 : %20 Yavaş 256 : %40 Yavaş
SERPENT	DEĞİŞMEZ	DEĞİŞMEZ
TWOFISH	ATAR	DEĞİŞMEZ

3.5 Yazılım Performansı

32 bitlik Cpu'daki verimlilik NİST'in ortaya koyduğu performans kriterlerinden biridir. Modern CPU'nun mimarisi çok karmaşıktır. Bu yüzden karşılaştırma için kullanılır. Bugün en yüksek mikroişlemciler 32 bit mimari kullanmaktadır. Bu mikroişlemciler Intel-Pentium ailesinden, ARM ailesinin 32 bit Smart Card'larına benzeyen Cpu'lara kadar değişir. Bunların mimaride en etkili olması bizim için şaşırtıcı değildir. Çünkü bütün AES finalistleri 32 bitlik sistemi kullanır. 2 bit Cpu ile kaplanan performans boşluğu gerçekten oldukça büyüktür. Bu 386'dan 6800'e kadar değişir. Yada Pentium ailesinin en eskilerinde en yeni Cpu'larına kadar değişir.

AES adayları bu tür işlemlere dayalıdır. Bizi cesaretlendiren şudur ki; trend, sonraki jenerasyondaki işlem kodlarında daha iyi performans gösterir. Ama gelecek jenerasyon işlemcileri bu çalıştırma sistemleri ile oldukça yavaş performans gösterecektir. Burada önemli olan nokta şudur ki; AES algoritmalarının performansları değişik Cpu'larda kötü bir şekilde değişim gösterebilir. Örnek olarak RC6 küçük marjiniyle Pentium II/III ailesinin en hızlı algoritmasıdır. Ama bunun hızı, Pentium'daki ve PA,RISC'deki en hızlı adayların hızının yarısından daha azdır. Çünkü bütün adaylar oldukça iyi bir hıza sahiptir [4].

3.5.1 Yazılım Performansının Karşılaştırılması

128 anahtarları için Rıjndael ve Twofısh en hızlı algoritmadır. Mars ve Rc6 orta hızlı ve Serpent ise en yavaş olanıdır. Daha büyük anahtarlar uzunlukları için Rijndael algoritması yavaş ilerler. Bazı uygulamalarda da Mars'tan daha yavaş çalışır. Bu eğilim, C'de ve Assembly dilde doğrudur. Buna rağmen Serpent diğerlerinden Assembly dili performansına yakın olan C kodu üretmeye daha yakındır [4].

3.5.2 8 Bit Smart Kart'la Limitlenmiş Hafıza Üzerinde Performas

Burada RAM'in gereksinimleri saat hızından daha önemlidir. Her bir CPU ailesi daha yüklü miktarda ve daha çok eleman içerir.
Bazı adaylar için, RAM' in gereksinimlerinin performansı şifreleme ve deşifrelemenin performansına bağlıdır.

Tablo 2. *RAM' in gereksinimlerine göre AES finalistlerinin karşılaştırılması.*

Agoritma Adı	Smart Kart RAM(bayt)
MARS	100
RC6	210
RİJNDAEL	52
SERPENT	50
TWOFİSH	60

3.6 En Yüksek Düzeydeki Güvensiz Değişkenlerin Yazılım Performansı

Biham algoritmalarının en düşük düzeydeki güven değişkenlerine göre kıyaslanması fikrini ortaya koymuştur. Farklı dizayn grupları, birbirinden daha az yada daha çok tutucudur. Biham güvenli bir yol olan döngülerin, en düşük numaralarının belirlemek suretiyle algoritmaları normalleştirmiştir. Bu Biham' ın en iyi tahminidir [3].

Sonra iki standart devre ekledi. NİST üzerindeki yorumlarında Lars Knudsen, farklı algoritmalardaki döngülerin numaralarını değiştirmek için başka bir başparmak kuralı getirdi. " "r"" nin, döngülerin en yüksek numarası olmasına izin ver ki; tüketici anahtar araştırmasından daha atak bir çalışma olsun. ". bu kural bize yeni karşılaştırma ölçüsünü vermiştir.
Bu kıyaslama için, ölçme faktörünü farklı bir çalışma için burada bırakıyoruz ve döngülerin en yüksek numaralarının en iyi şifreleme atağı için kıyaslıyoruz (Bu 256 bit brüt zorlayarak araştırmadan daha kolaydır.). buna da şöyle bir isim veriyoruz. (" En yüksek güvensiz değişkenler").

Tablo 3. *Şifreleme algoritmalarının döngü sayısı*

Algoritma Adı	Döngü
MARS	9-16
RC6	15-20
RİJNDAEL	8-14
SERPENT	9-32
TWOFİSH	6-16

Yukarıdaki tabloda en iyi şekilde yayınlanmış olan şifreleme sonuçlarını veriyoruz.

Eğer çok zayıf bir anahtar sınıfı varsa ve eğer atağın zorluk derecesi 2'den yüksek değilse ve zayıf anahtar zamanını bulma olasılığı varsa atakları sayarız. Bağlantılı bir anahtar atağı varsa yine aynı hesaplamayı yaparız. Mars çok karmaşıktır. Çünkü 4 farklı döngü fonksiyonu vardır. Mars' ı dizayn eden grup, algoritmanın şifreleme gücünün "core"' de olduğuna inanmaktadır. Çünkü biz bu döngüler üzerinde yoğunlaşıyoruz. Mars "core"' sinde döngü atağı vardır. Simetrik olarak 8' den 3' e kadar inen 4 farklı döngü fonksiyonu olan "chipper"' a karşı bir atak vardır.

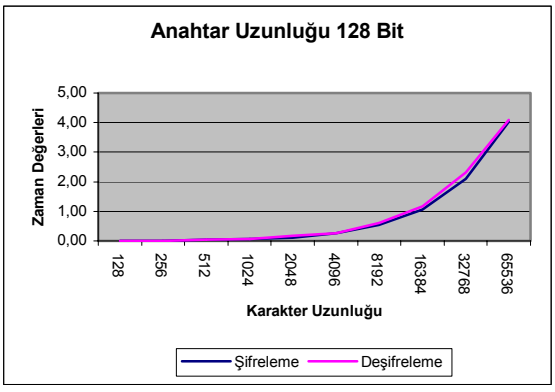
RC6, 15 atağa karşılık bir döngüye sahiptir. Bu atak ayanı zamanda zayıf anahtar sınıfına da uygulanabilir. Bu atak 2 anahtarda bir için uygulanabilir ve atağın zorluk dercesi 2 dir. RC6 dizaynları, 16 döngünün ataklanabileceğini öne sürmektedir. Çünkü somut bir atağı yoktur.Rijndael, 8 döngüye karşılık farklı bir atağa sahiptir.
Serpent , 9 döngüye karşılık bir atağa sahiptir.
Twofish 6 döngüye karşılık bir atağa sahiptir.

4.UYGULAMA

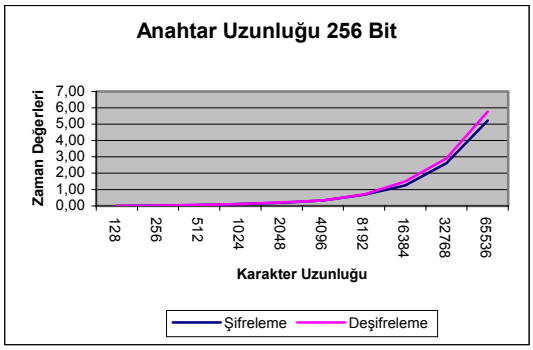
AES finalistlerinin arasında yazılım ve donanım performansı olarak en iyi algoritma seçilen Rijndael şifreleme algoritmasını Visual C++' ta şifreleme ve deşifreleme yapan bir uygulama programı gerçekleştirildi. Rijndael şifreleme algoritmasının belirli uzunluktaki mesaj verilerinin şifreleme ve deşifreleme süreleri aşağıdaki grafiklerde verilmiştir. Bu performans analizini yaparken Pentium IV 2000 Mhz işlemciye sahip bilgisayar kullanılmıştır.

Ayrıca Rijndael şifreleme algoritmasının şifreleme işlemini adım adım nasıl yapıldığı sayısal bir örnekle açıklanmıştır (128 Bitlik anahtar kullanılarak) [3].

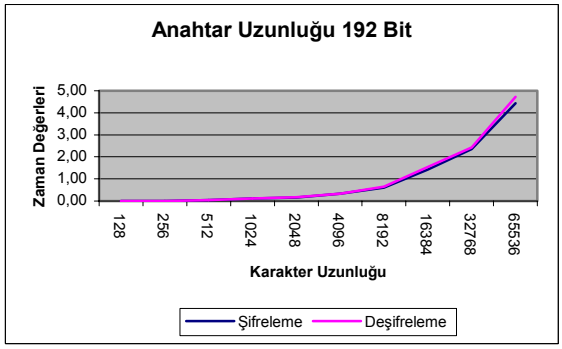
Tablo 4. *128 bit anahtar uzunluğuna sahip RİJNDAEL algoritmasının şifreleme ve deşifreleme süreleri*



Tablo 5. *192 bit anahtar uzunluğuna sahip RİJNDAEL algoritmasının şifreleme ve deşifreleme süreleri*



Tablo 6 *256 bit anahtar uzunluğuna sahip RİJNDAEL algoritmasının şifreleme ve deşifreleme süreleri*



5.SONUÇ

Biz bu çalışmada AES finalistlerinin karşılaştırmasını yaptık. Bu karşılaştırmayı yaparken şifreleme algoritmalarının yazılım ve donanım üzerindeki performanslarını inceledik. Bu şifreleme algoritmalarının güçlü güvenliğe sahip olmaları yanında yeni donanımlarla gerçekleştirilebilmeleri ve bu gerçekleştirilirken kolaylık ve performansı yüksek olması göz önünde bulundurulmalıdır. Aynı şekilde yazılım olarakta kolaylığı ve Cpu'u fazla meşgul etmemesi gerekmektedir.

Sonuç olarak günümüzde teknolojinin gelişimiyle hızlı, güçlü bilgisayarlar hayatımızın içine girmiştir. Bu bilgisayarlar bize birçok konuda yarar sağlaması yanında kriptografi bilimi açısından bir dezavantaj oluşturmuştur. Hızlı ve güçlü bilgisayarlar, şifreleme algoritmalarına karşı yapılan saldırılar da güçlenmekte ve daha hızlı sonuç alınmaktadır. Yeni oluşturulacak şifreleme algoritmalarının güvenliğinin yanında yazılım ve donanım performansları göz önünde bulundurulmalıdır ve yeni teknolojilerle paralel gelişmelidir.

Bu beş AES finalistinden bu performans kriterlerini göz önünde bulundurulduğunda en iyisi Rijndael şifreleme algoritmasıdır. Fakat bu şifreleme algoritması donanımsal olarak çok iyi performans vermesine rağmen 256 bit anahtar kullanımında döngü sayısı fazla olduğundan hız açısından yavaştır.

KAYNAKLAR

[1] Schneıer B., APPLİED CRYPTOGRAPHY,SECOND EDİTİON, 1996 NEW YORK

[2] NİST INSTİTUDE OF STANDARDS ON TECHNOLOGY www.nist.gov

[3] Daemen J. & Rijmen V., A SPECİFİCATİON FOR RİJNDAEL ,THE AES ALGORİTHM, 2000

[4]. Schneıer B., Kelsey J., Whitng D, Wagner D, Hall C., Ferguson H. Performance Comparison of AES Submission, 1999

[5] Stallings W.,Crypyography and Network Security New Jersey, 1997

[6] Srinivas R.,AES:Crypyography Advances in Future, 2000

[7] Daemen J., rijmen V., A Specificatian for Rijndael, The AES Algorithm, 2001

[8] Tsai M., AES Finalist Algorithm, 1999

[9] Patel D.,The AES Winner,S V RGİONAL ENGİNEERİNG COLLAGE, İndiana,2000

[10] Arda D., Buluş E., Türk Alfabesi ve Yapısal Özellikleri Kullanılarak Tek Alfabeli Yerine Koymada Şifreleme ve Kriptanaliz, 20. TÜRKİYE BİLİŞİM KURULTAYI, 2003 İstanbul

[11] Yerlikaya T., Buluş E., RSA Şifreleme Algoritmasının İncelenmesi ve Kriptanalizi ve AES Finalistlerinin Karşılaştırılması, 20. TÜRKİYE BİLİŞİM KURULTAYI, 2003 İstanbul

[12] Sakallı T. , Buluş E. , "DES'in Donanım Üzerindeki Uygulaması ve Performansı", 19. TÜRKİYE BİLİŞİM KURULTAYI, 2002 İstanbul