dergipark.gov.tr/tujes
Trakya University Journal of Engineering Sciences, 18(1): 85-94, 2017
ISSN 2147–0308
Derleme Makale / Review Article

KRİPTOLOJİDE KULLANILAN ASAL SAYI TEST ALGORİTMALARI

Tarık YERLİKAYA[1], Onur KARA[1*]

[1] *Trakya Üniversitesi, Bilgisayar Mühendisliği Bölümü, 22000 Edirne.*

Özet: Günümüzde şifreleme çok önemli hale gelmiştir. Asimetrik şifreleme yönteminin kırılması zordur. Bu yüzden önemli verileri şifrelerken tercih edilir. Asimetrik şifrelemenin temeli asal sayılara dayanmaktadır. Asal sayıların gizeminin hala çözülememesi bu alana olan ilgiyi arttırmaktadır. Şifrelemenin güçlü olması için yeteri kadar büyüklükte asal sayı bulabilmek önemlidir. Küçük sayıların asal olup olmadığı kısa sürede anlaşabiliyorken büyük sayıların asal olup olmadığını anlamak çok uzun sürmektedir. Bunun içinde asallık testlerine başvurulmaktadır. Asallık testleri sayesinde çok büyük sayıların asal olup olmadığı anlaşılabilmektedir.

Anahtar Kelimeler: Kriptoloji; Asal sayı; Asallık testi

Abstract: Cryptography has gained much more importance today. Asymmetric cryptography as a method is more favored as it is more difficult to break. Asymmetric cryptography is based on prime numbers. The mystery of the prime numbers keeps drawing attention on the subject. In order to make a strong encrypting it is important to find prime numbers that are big enough for encrypting. While it is quite easy to determine whether a small number is prime, it takes a long time to determine whether a large number is prime. For this reason, primality tests are utilized as they help us determine whether a very big number is prime.

Keywords: Cryptology; Prime numbers; Primality test

GİRİŞ

Teknolojinin gelişmesiyle birlikte bilgisayar ve internet hayatımızda büyük yer sahibi olmuştur. Buna paralel olarak internet üzerinden yapılan işlem sayısı da artmıştır. Kullanıcılar ticari işlerini, devlet işlerini, özel işlerini ve benzeri önemli işlevlerini sorunsuz yapabilmesi için güvenliğe dikkat etmesi gerekmektedir.(Yerlikaya, Gençoğlu, Emir, Çankaya, Buluş)

Güvenliği sağlamanın yolu da şifreleme ve kimlik denetiminden geçmektedir. Şifreleme işlemi Simetrik ve Asimetrik şifreleme olmak üzere 2'ye ayrılır. Asimetrik şifrelemenin temelini asal sayılar oluşturur. Kriptografik uygulamalarda "anahtar" olarak kullanılmak üzere çok büyük / çok uzun asal sayılara ihtiyaç duyulmaktadır. (Karaarslan, 2001)

Her dönemde bilim insanlarını teorik açıdan cezbeden asal sayılar, günümüzde elektronik güvenlik protokolleri ve açık anahtar şifreleme gibi kritik uygulamaların merkezinde yer almaktadır. Bu nedenle hem teorik hem uygulama açısından asal sayılar üzerinde yoğun olarak çalışılmaktadır. Asallık tanımından yola çıkarsak, bir n tamsayısının asal olması için 2 ile n arasında hiç bir böleni olmaması gerekir. Bu işlemi ufak sayılar için yapmak mümkün olsa da sayıların büyüklüğü arttıkça bunun hesaplanması mümkün olmamaktadır. Büyük sayıların asal olup olmadıklarını anlamak için daha gelişmiş asallık testleri gerekmektedir.(Granville, 1992)

Uzun yıllardan beri asal sayılar konusunda birçok çalışma yapılmıştır. Bu çalışmalar içerisinde en

önemli olanlar, asallık testleridir. Bir sayının asal olup olmadığını incelemek için kullanılan bu testlerin en eskileri "elek" olarak bilinmektedir. Sonraki buluşlar, matematiksel yöntemlerden yararlanarak oluşturulan çeşitli testlerdir. Böylece çok büyük sayıların asallık kontrolleri kolaylıkla yapılabilmektedir.(Yıltaş, 2003)

MATERYAL VE METOD

Bu çalışmada bir sayının asal olup olmadığının nasıl anlaşılacağı anlatılmıştır. Asal sayı test algoritmalarından Miller&Rabin, Slovay&Strassen ve Fermat testleri karşılaştırılmıştır.

Asal Sayılar

Birden büyük, sadece kendisine ve bire bölünen tam sayılara asal sayı denir. Asal olmayan sayılara ise bileşik sayı denir.(Can, 2002) Örneğin 48259 sayısı asaldır. Çünkü 1 ve 48259'dan başka pozitif böleni yoktur. Ama 111 sayısı 3 ve 37 bölünebildiğinden asal değildir. 1 den büyük her pozitif tam sayının en az iki tane pozitif böleni vardır. Bunlar 1 ve sayının kendisidir. 1 sayısı ise ne asal ne de bileşik sayıdır.

Asal sayılar ve özellikleri detaylı olarak ilk kez antik Yunanlı matematikçiler tarafından incelemiştir. M.Ö. 500-300 yılları arasında Pythagoras okulunun matematikçileri tarafından asal sayıların temelleri keşfedilmiştir(O'Connor ve Robertson, 2001). Euclid, asal sayılar hakkında birçok önemli sonucu ve aritmetiğin temel teoremini ispatlamıştır. M.Ö. 200 yılında Eratosthenes, asal sayıları hesaplayan "Sieve of Eratosthenes" algoritmasını geliştirdi. Fermat, 17'inci yüzyılda yeni bir teorem buldu. Fermat'ın teoremine göre herhangi bir n sayısının asal olması için obeb(a,n)=1 eşitliğini sağlayan her a sayısı ile $a^{(n-1)} = 1 \pmod n$ eşitliğini sağlaması gerekmektedir. Bu teoremin temelleri 2000 yıl önce geliştirilmiş eski bir Çin hipotezine dayanmaktadır.

Bu hipoteze göre n'nin asal olması için n'nin 2^n - 2'yi bölmesi gerekmektedir. Mersenne, asal olan n değerleri için 2^n-1'in de asal olduğunu iddia etti. Bu eşitliği sağlayan sayılara Mersenne Sayıları denmektedir. Her ne kadar bu formül bütün asal n değerleri için geçerli olmasa da bu formül bilinen en büyük asalların bulunmasını sağlamaktadır. Daha sonraki yıllarda Euler, Fermat'ın teoremini geliştirerek $n \geq 1$ için [1,n] aralığında n'e göreceli asal sayıların adedini veren Euler phi (totient) fonksiyonu Q(n)'i oluşturdu(Menezes ve Oorschot , 1997).

Legendre ve Gauss, büyük n değerleri için n'e yakın asalların yoğunluğunun 1/log n olduğu sonucunu 1798 yılında buldular. Bu sonuç Asal Sayı Teoremi olarak bilinmektedir. Bu teorem 1896 yılında Hadamard ve Valle Poussin tarafından ispatlanmıştır.

Asal sayılar konusunda çözüm bekleyen birçok problem bulunmaktadır. Bunlardan bazıları Riemann hipotezi, Goldbach Sanıtı, Mersenne Asalları, Carmichael Sayıları ve İkiz Asal sayılardır. Mersenne Asalları ve Carmichael Sayıları hakkında bilgiler aşağıda anlatılmıştır. Bu tür problemler çözülürken Sayılar Kuramında ve matematik başta olmak üzere birçok bilim dalında da ilerlemelere yol açıldığı unutulmamalıdır.

Asal sayılar ile ilgili bazı bilgiler şöyledir:

- 0 ve 1 asal sayı olarak kabul edilmez.
- 0 ve 1 dışındaki herhangi bir sayı, ya bileşik sayıdır ya da asal sayıdır.
- En küçük asal sayı olan 2, tek çift asal sayıdır.
- 5'ten büyük hiç bir asal sayı 5 ile bitmez.
- En büyük asal sayı, Mersenne Asalları Büyük İnternet Araştırması (GIMPS) projesindeki gönüllüler ile Dr. Curtis Cooper yaklaşık bir ay süren çalışmalar sonucunda bulundu. 22.338.618 basamaklı bilinen en büyük asal sayı $\mathbf{2^{74,207,281} - 1}$ dir.

Tablo 1. En büyük 10 asal sayı listesi

Sıra	Sayı	Basamak sayısı	Yıl
1	$2^{74,207,281} - 1$	22.338.618	2016
2	$2^{57.885.161} - 1$	17.425.170	2013
3	$2^{43.112.609} - 1$	12.978.189	2008
4	$2^{42.643.801} - 1$	12.837.064	2009
5	$2^{37.156.667} - 1$	11.185.272	2008
6	$2^{32.582.657} - 1$	9.808.358	2006
7	$2^{30.402.457} - 1$	9.152.052	2005
8	$2^{25.964.951} - 1$	7.816.230	2005
9	$2^{24.036.583}$ -1	7.235.733	2004
10	$2^{20.996.011} - 1$	6.320.430	2003

Mersenne Asalları

Asal bir *n* için 2^n - 1 biçiminde yazılan sayılara Mersenne sayıları denir.

n = 2 için $M_2 = 22-1 = 3$

n = 3 için $M_3 = 23-1 = 7$

n = 5 için $M_5 = 25-1 = 31$

n = 7 için $M_7 = 27-1 = 127$

Bu sayıların her biri asal sayıdır. Ama bundan sonraki ilk asal sayısı olan 11 için M_{11}'in Mersenne sayısı olup olmadığını inceleyelim.

n = 11 için $M_{11} = 211-1 = 2047$

2047 = 23 x 89 olduğunda M_{11} sayısı asal değildir.

Tüm asal n sayıları için M_n'nin asal olmadığı görülmektedir. Burada akla gelen soru hangi *n* asalları için M_n sayısının asal olduğudur. Bu sorunun cevabı hala bulunamamıştır. Bu yüzden Mersenne asalların sonsuz sayıda olup olmadığı bilinmemektedir. Şu ana kadar bulunan en büyük asal sayı $2^{74,207,281}$ - 1 bir Mersenne asal sayısıdır. Internet üzerinde en büyük Mersenne sayısını bulmaya yönelik çalışmalar yürütülmektedir.

Carmichael Sayıları

Fermat teoremine göre: n'nin asal sayı olması için ve her a tabanı için a^n-a'yı bölmesi gerekmektedir fakat bu bölme işlemini sağlayan asal olmayan sayılar da vardır. Bu sayılara Carmichael sayıları denir. "$x^{(n-1)}$ = 1 mod n" eşitliğini sağlayan bileşik x sayıları olarak da ifade edilir. Bu sayıların kriterlerini 1899 yılında Korselt şu şekilde belirlemiştir:

1. n, kare bağımsız olmalıdır.
2. n'yi bölen p asal değerleri için (n-1) de (p-1) değerlerine bölünmelidir.

İlk olarak 1910 yılında R. D. Carmichael bu kriterlere uyan sayıların bir kısmını bulmuş. Bundan sonrada bu sayılara Carmichael sayıları denmiştir.

Bu sayılardan bazıları aşağıda verilmiştir.

561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, . . .

Bu sayılar oldukça ender olmasına karşılık sonsuz sayıda olup olmadığı bilinmemektedir. Bu soruna karşılık 1992 yılında Alford, Granville ve Pomerance, x sayısına kadar $x^{2/7}$ den daha fazla Carmichael sayısı olduğunu ispatlamıştır.

Asal Sayı Teoremi

2300 yıl önce Euclid, asal sayıların sonsuz sayıda olduğunu kanıtladı. Bundan sonra ise herhangi bir sayıya kadar kaç tane asal sayı olduğunu hesaplama ihtiyacı duyuldu. Asal Sayı Teoremi de bu sorunu hesaplamak ile ilgilidir. Asal Sayı Teoremi 1791 yılında Gauss tarafından varsayım olarak ortaya atıldı. Bu teoreme eşit başka bir ifade 1798 yılında Legendre tarafından yayınlandı. Asal Sayı Teoremini kanıtlamak için ilk gerçek adım 1850 yılında Chebyshev tarafından atıldı. Asal Sayı Teoremi 1896 yılında, Charles de la Vallee Poussin ve Jacques Hadamard tarafından aynı anda ve birbirlerinden bağımsız olarak kanıtlandı. Bu teorem

rasgele bir x sayısının asal olması olasılığının yaklaşık olarak 1/ loge x olduğunu belirtir.

π(x) = x'e eşit ya da x'ten küçük asalların sayısı verir. Örneğin 25'den küçük asal sayılar = 2, 3, 5, 7, 11, 13, 17, 19, 23 Bu durumda; π(3) = 2, π(10) = 4, π(25) = 9

Tablo 2 x = [10, 10^{10}] için π(x) değerlerini göstermektedir (Caldwell, 2002)

Tablo 2. x = 10^{10}'ye kadar olan π(x) değerleri

X	**π (*x*)**
10	4
100	25
1,000	168
10,000	1,229
100,000	9,592
1,000,000	78,498
10,000,000	664,579
100,000,000	5,761,455
1,000,000,000	50,847,534
10,000,000,000	455,052,511

x'i geçmeyen asalların sayısı π (x), x / ln x 'e asimptotiktir.

$$\lim_{x\to\infty} \frac{\pi(x)\ln x}{x} \to 1 \qquad \text{(Formül 1)}$$

" a(x), b(x) 'e asimptotik" ile belirtilen bu ifadede x sonsuza yaklaşırken a(x) / b(x) oranının 1'e yaklaştığı görülmektedir.

Tablo 3'te 10^{10}'a kadar olan bazı sayılar için elde edilen değerler yer almaktadır (The University of Sheffield, 1999).

x bir asal sayı ise bir sonraki asal sayıya olan ortalama uzaklık yaklaşık olarak ln *x* 'tir. Asal sayı teoremi, asal sayıların dağılımı hakkında kısıtlı da olsa bir fikir vermektedir.

Tablo 3. Asal sayı teoremi ile ilgili 10^{10}'a kadar olan bazı sayılar için elde edilen değerler

x	**π(*x*)**	***x*/ln(*x*)**	**π(*x*)ln(*x*)/*x***
10	4	4.3	0.921034
10^2	25	21.7	1.15129
10^3	*168*	*144.8*	*1.1605*
10^4	1229	1085.7	1.13195
10^5	9592	8685.9	1.10432
10^5	78498	72382.4	1.08449
10^7	664579	620421	1.07117
10^8	5761455	5428681	1.0613
10^9	50847534	48254942	1.05373
10^{10}	455052511	434294482	1.0478

Asal Sayı Test Algoritmaları

Eski zamanlardan beri bir sayının asal olup olmadığını bulmaya yönelik birçok çalışma olmuştur. Günümüzde Asal sayıların şifrelemede önemli bir yeri olduğundan asallık testleri daha da önem kazanmıştır.

M.Ö. 240 yıllarında Erastotenes asallık testi için ilk yöntem olan Erastotenes Kalburu önermiştir. Erastotenes Kalburu'na göre: Eğer sayının kareköküne kadar olan bütün asal sayılar denenmiş ve bir çarpan bulunmamışsa, sayının kendisinden ve 1'den başka çarpanı yok demektir; dolayısıyla bu bir asal sayıdır. Buradaki sorun büyük sayıların çarpanlara ayırmadaki zorluğudur. 17. Yüzyılda Fermat'ın geliştirdiği Fermat teoremi ile çarpanlara ayırma işleminde büyük bir yol sağlanmıştır.

Fermat Teoremine göre: her a tamsayısı için p , (a^p-a)'yı böler. Bu teorem, asallık testleri ile ilgilenen kişilerin referans noktası olmuştur. O zamandan sonra asallık testi ile ilgili birçok algoritma

geliştirmiştir. Onlardan bazıları 1976 yılında Miller daha sonrada Rabin Genişletilmiş Riemann hipotezine dayanan olasılık algoritmaları geliştirdiler. 1983'te Adleman, Pomeiance ve Rumely algoritmaları geliştirildi. 1986'da Coldwaser ve Kilian eliptik eğrilerine dayanan bir algoritma ürettiler. Son olarak 2002 yılında Manindra Agrawal, Nitin Saxena ve Neeraj Kayal tarafından AKS Asallık testi geliştirilmiştir.

Asal sayı testlerini gerçekleştirirken temelde dikkat edilmesi gerekenler aşağıda belirtilmiştir.

1. Çift sayıları test etmeye gerek yoktur.
2. Asallığı test edilen sayıların; 3, 5, 7, 11 … gibi küçük asal sayılara bölünüp bölünmediğine bakarak birçok sayı elenebilir. Örneğin 23 sayısına kadar olan asal sayılar alınırsa, asal sayı olmayanların en azından 2/3'ü ayıklanabilir ve 3 kat daha hızlı sonuca gidilebilir (Segre, 2000).

Erastotenes Kalburu

Asallık testlerinin en basit metodu olan Erastotenes Kalburu M.Ö. 300'de Eratosthenes tarafından geliştirildi. Eratosthenes Kalburu sürekli bileşik sayıları eleyerek ilerler ve en sonunda kalan sayılar asal sayı olur. Bu yöntem $O(n\sqrt{n})$ zaman karmaşıklığına sahiptir. Verilen bir sayıya kadar olan bütün asal sayıları kesin olarak bulur. Fakat sayılar büyüdükçe asal sayıları bulmak için harcanan zaman çok fazla artar.

Eratosthenes Kalburu işleyişi:

1. Bir sayı belirlenir ve 2 den başlayarak bu sayıya kadar olan tüm sayılar yazılır.
2. Asal sayılar adında bir liste tutulur ve bu listeye ilk asal sayı olan 2 eklenir.
3. Yazılmış olan sayılar içinden 2 ve 2'nin tüm katları silinir.
4. Silme işleminden sonra kalan ilk tek sayı asaldır. Bu sayı Asal sayılar listesine eklenir.
5. Bu tek sayı ve tüm katları yazılmış olan sayılardan silinir.
6. Yazılmış olan sayılarda herhangi bir sayı kalmayıncaya kadar 4. ve 5. adımlar tekrarlanır.

Asal sayı test algoritmaları sayının asal olduğunu kanıtlayan(Bu durumda kanıtlanmış asal) ya da büyük olasılıkla asal denir. Sayı muhtemel asal çıkıyorsa bu tür testlere olasılıklı asallık testleri; eğer matematiksel olarak ispatlıyorsa buna da Gerçek asallık testleri denir.(Yerlikaya, 2006)

a. Kesin *(Deterministic)* Asallık Testleri

Bu tür asallık testleriyle ile bir sayının asal olup olmadığını kesin olarak belirlemek mümkündür. Bu tür yöntemler genellikle çarpanlara ayırmaya dayanmaktadır.

Kesin Asallık Testleri büyük sayıları test ederken çok fazla zamana ihtiyaç duyduğundan kullanışlı değildir. Aynı zamanda bu yöntemler çok karışıktır, uygulamada bir hata yapma olasılığı, olası asallık testinde hata yapma olasılığından daha fazladır (Silverman, 1997).

En çok kullanılan yöntemlerin bazıları: Cyclotomic Ring Testi, Lucas-Lehmer Testi ve AKS Testidir.

b. Olası Asallık Testleri

Olası Asallık Testlerini(OAT) geçen sayının yüksek olasılıkla asal olduğunu ispatlanır. OAT'de asal sayı üretmek için öncelikle *n* bitlik bir rastsal sayı üretilir. Daha sonra asallık deneyine tabi tutulur. Testi geçen asal sayılır seçilir ve istenilen yerde kullanılır. OAT'de hata payını en aza düşürmek için geçilmesi gereken test sayısı arttırılabilir. Bu sayede çok küçük bir hata payı ile sayının asal olup olmadığı anlaşılır. 2^{-100} den daha düşük bir hata payı ile bir sayının asal olduğu belirlenebilir (RSA, 1998). Bu deneyler, Kesin Asallık Testlerinden hızlı olduğu için daha çok tercih edilir.

En çok kullanılan OAT'nin bazıları şunlardır :

1. Fermat Testi

2. Lehmann Testi
3. Solovay Strassen Testi
4. Miller&Rabin Testi

Tanık (witness) Kavramı

Bir sayının asal olmadığını yani bileşik sayı olduğunu anlamak için çarpanlarına ayırmaya çalışılır. Fakat çarpanların yoğunluğu genelde çok az olduğundan bu yöntem etkili değildir. Bunun yerine OAT kullanılarak daha etkin bir çalışma yapılabilir. OAT, tanık kavramına dayanmaktadır ve tanıklık fonksiyonları olarak da adlandırılırlar. Tanık, n sayısının bileşikliğini göstermek için kullanılan 1 ile n arasında bulunan herhangi bir sayıdır. Tanıklık fonksiyonlarına göre, tanık sayıların yoğunluğu (d değeri) değişmektedir ve bu değerler Tablo 4'da gösterilmiştir. Daha büyük d değerleri, itimat eşiğine daha hızlı yaklaşma demektir (Segre, 2000).

Tablo 4. Tanıklık Fonksiyonlarında yoğunluk (d) değerleri

Tanıklık Fonksiyonları (Olası Asallık Testleri)	**Tanık Sayıların Yoğunluğu (d değeri)**
Lehmann	0,5
Miller&Rabin	0,75
Solovay – Strassen	0,5

OAT'ye sokulan bir sayının i iterasyon sonunda asal ilan edilmesine rağmen bileşik olma olasılığı vardır. Tanık sayıların yoğunluğu d olarak kabul edilirse, bir sayının bileşik olma olasılığı Formül 2 ile hesaplanmaktadır. Bir sayının asal olma olasılığı ise Formül 3 ile hesaplanmaktadır.

$$P(\text{bileşik sayı}) = (1-d)^i \quad \text{(Formül 2)}$$

$$P(\text{asal sayı}) = 1 - P(\text{bileşik sayı}) = 1 - (1-d)^i \quad \text{(Formül 3)}$$

Miller&Rabin testinde yoğunluk daha fazla olduğu için daha az adımda seçilen eşiğe ulaşılabilir. Lehmann yönteminin bir rastsal sayı için uygulanması sonucunda 1 veya -1 çıkarsa sayı testi geçmektedir. Yine de o sayının bileşik olma olasılığı 0,5 den daha az olmakla beraber hala mümkündür. OAT sonucunda hata payının daha da düşmesi için iterasyon değeri arttırılabilir. Aslında bu oranlar oldukça abartılıdır. Çoğu rastsal sayı için, rastsal seçilen bir a değerinin tanık olma olasılığı %99,99 'dur (Schneier, 1996).

Yalancı-tanıklık (non-witness) Kavramı

Bir bileşik n sayısı için, W(n) kümesi n'in asal olmadığını kanıtlayabilecek sayılardan yani tanık sayılardan oluşsun. Tümleyen küme L(n), $L(n) = Z_n - W(n)$ elemanlarından oluşacaktır ve bu kümenin elemanları yalancı-tanık olarak adlandırılır. Eğer testlerde parametre olarak yalancı-tanıklar kullanılırsa yanlış sonuçlara ulaşılması mümkündür. Çünkü testler bileşik sayının asal olduğunu bildireceklerdir. Bu tür yanlışlıklarla karşılaşmamak için bu tür testleri (yeteri kadar büyük bir t sayısı için) t kere tekrarlamamız hata olasılığını daha da düşürecektir (Menezes ve Oorschot, 1997). Miller&Rabin testi için yalancı-tanıkların sayısının çok az olduğu Higgins'ın yaptığı araştırmalarda ortaya çıkmıştır (Higgins, 2000).

Fermat Testi

Pierre de Fermat'ın teoremine göre herhangi bir n sayısının asal olması için [1, n-1] aralığından alınan bir a sayısı ile $a^{(n-1)} = 1 \pmod n$ eşitliği sağlaması gerekmektedir. Bu test, olası asallık testlerinin temelini oluşturmaktadır (Menezes ve Oorschot, 1997). 256 bit rasgele bir sayının bu testi geçip asal olmama olasılığı 10^{22}'de 1'dir (Rivest, 1990).

Örneğin: a=2 ve n=3 için $2^{3-1} = 1 \pmod 3$ $2^2 = 1 \pmod 3$ $4 = 1 \pmod 3$ görüldüğü gibi n=3 sayısının asal olduğunu hesapladık.

Fermat testi, Carmichael sayılarını tespit etmekte başarısız kalmaktadır. Diğer OAT, Fermat'ın teoremini temel olarak alsalar da aynı zamanda diğer birçok durumu da kontrol ettiklerinden daha gerçeğe

yakın sonuçlar döndürmektedirler. Fermat Teoreminin karşıtı doğru değildir. Yani $n \neq a$ ve $a^{n-1} \equiv 1 \pmod n$ olması *n* nin asal olmasını gerektirmez.

Lehmann Testi

n sayısının asal sayı olup olmadığını test etmek için rastgele olarak seçilen a sayılarıyla, b değeri Formül 4 ile hesaplanır (Segre, 2000). Eğer bütün b değerleri 1 veya –1 ise, fakat yalnız 1 veya yalnız -1 değilse n asal olarak kabul edilebilir (Menezes ve Oorschot, 1997).

$$b = a^{((n-1)/2)} \pmod n \qquad \text{(Formül 4)}$$

Legendre'nin geliştirdiği n/a Legendre sembolü bu foknsiyonun temellerini oluşturur. Legendre Sembolü'nün aldığı değerler ve açıklamaları Tablo 5'de belirtilmiştir (Menezes ve Oorschot, 1997).

Tablo 5. Legendre Sembolü Değerleri ve Açıklamaları

$\frac{a}{n}$	+1	eğer a, mod n'ye göre "quadratic residue" ise
	-1	eğer a, mod n'ye göre "non-quadratic residue" ise
	0	Eğer a, n'i bölerse

Euler'in teoremine göre, obeb(a,n) =1 ve n bir asal sayıysa Formül 5'deki eşitlik sağlanmaktadır. Bu teorem verilen n sayısının asal olup olmadığını test etmek için kullanılabilir. Sonuç olarak a tabanına göre Euler sözde asalı Formül 7'de olduğu gibi de ifade edilebilir. Yeteri kadar a sayısı denediği zaman n'in asal olup olmadığı anlaşılabilmektedir.

$$\left(\frac{a}{n}\right) = a^{(n-1)/2} \pmod n \qquad \text{(Formül 5)}$$

$$a^{(n-1)/2} = \left(\frac{a}{n}\right) \pmod n \qquad \text{(Formül 6)}$$

$$b = a^{((n-1)/2)} \pmod n \qquad \text{(Formül 7)}$$

Pretty Good Privacy (PGP) ilk başlarda $a^{(n-1)}$ değerini sadece bir a değeri için hesaplıyordu. Buradan çıkan sonuç 1 ise n'in asal olduğunu varsayıyorlardı. Ama bazı sayıların bu formülü sağladığı halde asal olmadığı görülmüştür. Carmichael Sayıları olarak bilinen bu sayılar bütün a değerleri için $a^{(n-1)} = 1 \mod n$ eşitliğini sağlamaktadır. Aynı sorun $a^{(n-1)/2} = 1 \mod n$ formülündeki a sayısı içinde geçerli olabilir. Eğer t adet rastsal seçilmiş a sayısı kullanıldıysa ve n asal değilse b değerinin 1 veya –1 den farklı sayı gelme olasılığı en azından $2^{(-t)}$ olmaktadır. t sayısını olabildiğince büyük alınırsa bu olasılık azaltılabilir. Böylece testin daha kesin sonuçlar vermesini sağlanabilir.

Slovay & Strassen Testi

Açık-Anahtar Kriptografisinde kullanılmış ilk testtir. Slovay-Strassen Algoritmasında n sayısının asal olup olmadığını bulmak için Jacobi Semboli kullanılmaktadır. Jacobi Sembolü n asal ise Legendre Sembolüne eşit olmaktadır. Algoritmanın aşamaları aşağıdaki gibidir(Schneier, 1996):

1. n 'den ufak rastsal bir sayı olan a seçilir
2. Eğer gcd (a,n) ≠ 1 ise o zaman n testi geçemez ve asal olmadığı anlaşılır.
3. $j = a^{(n-1)/2} \mod n$ hesaplanır.
4. Jacobi sembolü olan J (a, n) hesaplanır.
5. Eğer j ≠ J (a, n) ise n testi geçemez ve kesin olarak asal değildir.
6. Eğer j = J (a, n) ise n'nin asal olmama olasılığı %50'den fazla olamaz.

Slovay & Strassen Testi yerine kendisinden daha hızlı ve en az onun kadar doğru olan Miller-Rabin'in kullanılması önerilmektedir (Menezes ve Oorschot, 1997).

Miller&Rabin Testi

Miller-Rabin Testi (M&R Testi) güçlü asallık testi olarak bilinir. M&R Testinde, n sayısının asal olup olmadığını test etmek için ilk önce Formül 8'i sağlayan s ve r değerleri hesaplanır (Menezes ve Oorschot, 1997).

$n - 1 = 2^s r$ (Formül 8)

[1, n-1] aralığından taban olarak kullanılacak bir a değeri seçilir. Formül 9 veya Formül 10'daki eşitlik sağlanıyorsa n sayısının a tabanına göre güçlü asal olduğu kabul edilir (Menezes ve Oorschot, 1997).

$a^r = 1 \pmod n$ (Formül 9)

$a^{2^j r} = 1 \pmod n \ (0 \leq j \leq s-1)$ (Formül 10)

n sayısının asallığını test ederken; n aday asal sayısı 2'den büyük ve tek herhangi bir tamsayı, a taban değeri ise 2 … n-1 dizisinden seçilmiş rastsal bir sayı olsun. C(n,a) bileşik "boolean" fonksiyonunun özellikleri aşağıda belirtilmiştir (SCM, 2000):

• Eğer n asal ise, C(n,a) fonksiyonu sonucu "2 … n-1" aralığındaki her a için yanlış (false) olmalıdır.

• Eğer n bileşik ise C(n,a) fonksiyonu sonucu "2 … p-1" aralığındaki a'ların en fazla ¼ 'ü için yanlış olmalıdır. Eğer taban a için test başarısız olursa; n, a tabanına güçlü sözde asal olarak tanımlanır.

Bu test, diğer rastsal tabanlar için tekrarlanabilir. Bu test ile n sayısının kesin olarak asal olup olmadığı ispatlanabilir. Bunu yapmak için n sayısının asallık testini 1/4 n +1 adet taban için uygulamak gerekmektedir. Ancak büyük sayılar için bu çok zaman alacağından sadece belirli bir kısmında uygulanmaktadır. Bu yüzdende n sayısının asal olup olmadığı olası olarak belirlenmektedir. Asal olma olasılığını azaltmak için çok fazla tabanla bu işlem yapılmalıdır. Asal olma olasılığını hesaplamada t adet taban için testi geçen sayının maksimum $(¼)^t$ asal olacağı anlaşılır. Mesela test 30 kez tekrarlandığında, testi geçen sayının asal olmama olasılığı en fazla $8{,}3 \times 10^{-25}$ olacaktır. Bu da: 0,000000000000000000000000083 olmaktadır (SCM, 2000). Daha gerçekçi hesaplamalar da yapılmıştır. x bit asal adaylarında (x>100), bir tabanla uygulanan bir testin hatalı sonuç döndürme olasılığı k katsayısı için $(\frac{1}{4x})\ (2^{k/2})^{1/2}$ 'den daha düşük olmaktadır. 256 bitlik bir n sayısı için, 6 test sonucunda hatalı cevap alma olasılığı 2^{-51}'den daha düşük olmaktadır(Schneier, 1996).

M&R Testinde, bileşik sayıların asal sanılma olasılığı daha azalmaktadır. a sayılarının en az 1/3 'ünün tanık olması garantidir (Schneier, 1996). Bu test için yalancı-tanıkların çok az olduğu Higgins'ın yaptığı araştırmada ortaya çıkmıştır (Higgins, 2000). Bununla birlikte, testi geçen bileşik sayıların varlığı da bilinmektedir. Alford, Granville ve Pomerance tarafından bu bileşik sayıların varlığı kanıtlanmıştır. Bleichenbacher, 100'den küçük ve eşit tabanlar kullanıldığında M&R testini geçen 55 basamaklı bir bileşik sayı bulmuştur. M&R testinin 2, 3, 5, 7, 11, 13 ve 23 tabanlarına göre uygulandığında 10^{16}' dan küçük sayılar için doğru bir asallık testi olduğu kanıtlanmıştır. Çeşitli tabanlar için kullanılabilecek aralıklar Jaeschke tarafından belirlenmiştir (Maurer, 1994).

M&R Testinin Uygulaması

n rastsal sayısının M&R asallık testi için ilk önce n-1'in ikiye bölünme sayısı olan s değeri ile Formül 10'daki eşitliği sağlayan r değeri hesaplanır. Geriye kalan aşamaların adım adım uygulanması aşağıda verilmiştir (Schneier, 1996):

1. n den küçük olacak bir rastsal a sayısı bulunur.
2. j = 0 olarak ayarlanıp $z = a^r \bmod n$ hesaplanır.
3. Eğer (z = 1) veya (z = n – 1) ise n asallık testini geçer ve asal olabilir.
4. Eğer (j > 0) ve (z = 1) ise n asal değildir.

5. j = j + 1 olarak ayarlanır. Eğer (j < s) ve (z ≠ n-1) ise ($z = z^2 \bmod n$) olarak ayarlanır ve 4. Adıma geri dönülür. Eğer (z = n – 1) ise n asallık testini geçer ve asal olabilir.
6. Eğer (j = s) ve (z ≠ n - 1) ise o zaman n sayısı asal değildir.

M&R Testinde Asal Taban Almanın Avantajları

M&R Testi güçlü asallık testi olarak bilinir. Böyle olmasına rağmen bu testi yanıltan sayılar vardır. M&R Testini yanıltan sayılara güçlü yalancı tanık denir. Bazı bileşik sayılar, çok az sayıda güçlü yalancı tanığa sahiptir. Mesela bileşik 105 (3 x 5 x 7) sayısının yalancı tanıkları 1 ve 104'tür. Buradan varılan genelleme şudur: Bir n sayısı 2 veya daha fazla ilk tek asal sayının çarpımından oluşuyorsa bu sayının yalancı tanıkları sadece 1 ve n-1 olmaktadır. Güçlü yalancı tanıklar yüzünden M&R testinde yanlış sonuçlara varılmaması için taban olarak ilk asalların (2, 3, 5, 7 gibi) alınması önerilmektedir. Birçok bileşik sayı için güçlü yalancı tanıkların adedi, $Q(n)$[36] fonksiyonu için maksimum Q(n) / 4 olmaktadır (Menezes ve Oorschot, 1997).

Frobenius Testi

Frobenius Sözde Asalı, Sonlu Alan kuramına dayanmaktadır. Ayrıca bu kurama dayanan Frobenius testinin diğer testlerin genelleştirilmesi ve güçlendirilmesi ile oluşturulduğu belirtilmektedir (Grantham, 1998).

Frobenius testi ile bir bileşik sayıyı asal olarak belirleme hata oranının 1/7710 olduğu ölçülmüştür. Frobenius testinin M&R testinden üç kat daha yavaş çalıştığı ama 3 round'lu M&R testinin hata oranının en fazla $(1/4)^3=1/64$ olduğu belirtilmiştir. Bu da Frobenius testinin aynı zaman aralığında M&R testinden daha az hata oranı ile çalıştığını göstermektedir (Grantham, 1998).

Pratikte Asal Sayı Üretme Esasları

Asal sayı üretmek için aşağıda belirtilen aşamalar adım adım uygulanmalıdır:

1. n-bit rastsal sayı p üretilir.
2. İlk bit ve son bit'ler 1 olacak şekilde ayarlanır (Son bit'in 1 olması o sayının tek olmasını sağlamakta, ilk bit'in 1 olması da asal sayının istenilen (required) uzunlukta olduğunu belirlemektedir).
3. p'nin ufak asal sayılara (3,5,7,11 …) bölünmediği kontrol edilmelidir. Birçok uygulamada 256'dan küçük bütün asallarla kontrol ederken, en etkin olanı 2000'den küçük asallara bölünmediğini kontrol etmektir.
4. Miller&Rabin testi bir rastsal a değeri için uygulanır. Eğer p bu testi geçerse başka rastsal a değerleri için bu test tekrarlanabilir. Ufak a değerleri seçilmelidir ki hesaplamalar daha hızlı olsun. Testte kullanılacak a değerlerinin sayısı 5 (Seth, 1999) veya 10 (Segre, 2000) olarak seçilebilir. Eğer p değeri bu testlerden birisini geçemezse asal bir sayı değildir ve başka bir p değeri yaratılıp aynı işlemlerden geçirilmesi gerekecektir [11,17].
5. Miller&Rabin testini geçen sayılar, Lucas veya Frobenius testine sokularak daha güvenilir sonuçlar elde edilebilir (Silverman, 1997).

Her seferde rastsal p değeri oluşturmak yerine, ilk seferden sonra başlangıç rastsal sayısını arttırarak asal bir sayı bulana kadar da işleme devam edilebilir [11,17].

Asallık testinin yeterince kuvvetli olması için, testte sayının basamak adedi kadar taban (a değeri) alınması tavsiye edilmektedir (Pinch, 1994). Dikkat etmemiz gereken temel kriter, hata oranının 2^{-100} 'den daha büyük olmaması gerektiğidir (Silverman, 1997). Digital Signature Standard (DSS)'de; üretilen sayıların asallığını test ederken, Miller&Rabin algoritmasının en az 50 kez kullanılmasıyla kabul

edilecek bir hata olasılığına, yani 2^{-100} 'e ulaşılabileceği belirtilmektedir (Burrows, 1994).

SONUÇ VE ÖNERİLER

Kesin veya Olası Asallık testleri uygulanmadan önce bu sayıların Ufak Asallara Bölme testinden geçirilmesi testlerden daha kısa sürede sonuç almamıza olanak sağlamaktadır. Tek sayıların 3, 5 ve 7 ile bölüp bölünmediğinin testinin bu sayıların %54'ünü, 100'den küçük asallara bölmenin %76'sını, 256'dan küçük sayılara bölmenin ise %80'ini elediği tespit edilmiştir.

Lehmann testi, Slovay&Strassen'in bir varyasyonudur. Bu yüden Lehmann dışındaki diğer üç temel testi karşılaştırdığımızda Miller&Rabin testinin daha iyi olduğu ortaya çıkmaktadır. Bunun nedenleri ise Fermat testi, Carmichael sayılarını bulmakta zayıf kalmaktadır. Solovay&Strassen testi, çalışma zamanı olarak daha uzun sürmekte ve Jacobi sembol hesaplamaları yüzünden uygulanması daha zordur. Slovay&Strassen testi $(1/2)^t$ hata payıyla çalışırken Miller&Rabin testi $(1/4)^t$ hata payıyla daha gerçeğe yakın sonuçlar sunmaktadır.

Miller&Rabin testi en kötü şartlarda bile en fazla diğerleri kadar çalışmaktadır. Miller&Rabin ile birlikte Lucas veya Frobenius testlerinin birlikte kullanılması önerilmektedir. Bu sayede hata payı çok aza indirilmiş olacaktır.

KAYNAKLAR

1. BURROWS, J.H., Digital Signature Standard (DSS), *Federal Information Processing Standards Publication*, 1994.
2. CALDWELL, Chris K., The University of Tennesse at Martin, *Practical Applications of Prime Numbers*, 2002.
3. CAN, Ö., Asal Sayı Örüntüleri Ve Goldbach Sanısı Üzerine Bir Çalışma, 2002
4. GRANTHAM, J., A Probable Prime Test with High Confidence, *Journal of Number Theory*, 72, 1998.
5. GRANVILLE A., Primality Testing & Carmichael Numbers, Notices Amer. Math. Soc. 39, 696-700,1992.
6. HIGGINS, B.C., The Rabin-Miller Probabilistic Primality Test, Some Results on the Number of Non-Witnesses to Compositeness, 2000.
7. KARAARSLAN, E., Büyük Ölçekli Rastsal ve Asal Sayı Üretimi, 2001.
8. MAURER, U.M., Fast Generation of Prime Numbers& Secure Public-Key Cryptographic Parameters, *Journal of Cryptography*, 1994.
9. MENEZES, A. and OORSCHOT, P., Handbook of Applied Cryptography, CRC Press, 1997
10. O'CONNOR, J.J. and ROBERTSON, E.F., Prime Numbers, 2001.
11. PINCH, R.G.E., Some Primality Testing Algortihms, Proc 4th Rhine workshop on Computer Algebra, Karlsruhe, 1994.
12. RIVEST, R., Finding Four Million Large Random Primes, Advances in Cryptology, CRYPTO'90, LNCS 537, 625-626, 1990.
13. RSA, RSA FAQ v4, Frequently Asked Questions About Today's Cryptography – What's Primality Testing?, 1998.
14. SCHNEIER B., Applied Cryptography (Second Edition), John Wiley & Sons Inc, 1996.
15. SCM, Theory of the Miller&Rabin Test, Scheme Library, 2000.
16. SEGRE, A., Computer and Network Security, Iowa Üniversitesi "Data Security" Ders Notları, 2000.
17. SETH, A., The Data Encryption Page Newsletter , 1, 1–2, 1999.
18. SILVERMAN, R.D., Fast Generation of Random, Strong RSA Primes, RSA Laboratories' Crypto Bytes Magazine, 1997.
19. The University of Sheffield, Department of Pure Mathematics, 1999.
20. YERLIKAYA, T., Yeni Şifreleme Algoritmalarının Analizi, 2006.
21. YERLIKAYA, T., GENÇOĞLU, H., EMIR, M.K., ÇANKAYA, M., BULUŞ, E., Rsa Şifreleme Algoritması Ve Aritmetik Modül Uygulaması.
22. YILTAŞ, D., Kriptolojide Kullanılan Asal Sayı Test Algoritmalarının Performans Açısından Karşılaştırılması, 2003.