RSA Kriptosistemi Parametreleri için Güvenlik Testi Yazılımı

Ersan Akyıldız, Çağdaş Çalık, Mert Özarar, Zaliha Tok, ve Oğuz Yayla

Özet: **RSA kriptosisteminde üretilen açık ve gizli anahtar parametrelerinin güvenilir olması için gereken kriterler çalışılmıştır. Bu kriterler e-imza oluşturma standartlarında ve literatürde bulunmaktadır. Çalışmamızda, bu kriterler test maddeleri halinde sunulmuştur. Ayrıca, söz konusu testleri gerçekleştiren bir yazılım paketi geliştirilmiştir. Yazılım paketi RSA-1024 ve RSA-2048 parametrelerinin testlerini makul sürelerde yapabilmektedir.**

Anahtar Kelimeler: **RSA kriptosistemi, e-imza, güvenlik testi.**

Abstract: **We study the requirements for public key and private key parameters of RSA cryptosystem. The requirements considered are already known in the digital signature standards, directives and literature. We list these requirements in a security testing framework and develop a software package for validating them. The software package is able to test RSA-1024 and RSA-2048 parameters in a reasonable amount of time.**

Keywords: **RSA cryptosystem, digital signatures, security testing.**

I. GİRİŞ

AÇIK anahtarlı kriptosistemler sınıfına ait olan RSA kriptosistemi [7] (kıs. RSA, RSA sistemi), verilerin şifrelenmesi ya da imzalanması amacıyla kullanılır. Dünya'da ve ülkemizde e-imza, SSL/TLS vb. uygulamalarda yaygın olarak kullanılmaktadır. RSA sisteminde kullanılan anahtar ikililerini bilgisayar ortamında üretmek mümkün olmakla birlikte, kişiye/kuruma özel e-sertifikaların kanuni olarak geçerli olması ancak yetkili bir ESHS (Elektronik Sertifika Hizmet Sağlayıcısı) tarafından üretilmeleri koşuluna bağlıdır. Yine yürürlükte olan 5070 Sayılı Elektronik İmza Kanununa [1] göre bu işlem belirli standartlara uygunluk gösteren HSM (Hardware Security Module) cihazlarıyla gerçekleştirilmektedir. Bu tarz cihazların bilgi güvenliği açısından kritik bir konuma sahip olmaları nedeniyle ürettikleri parametrelerin güvenlik testlerinden geçirilmesi gerekir. Bu çalışmada söz konusu testleri gerçekleştiren bir yazılım paketi tanıtılacaktır.

E. Akyıldız: Matematik Bölümü ve Uygulamalı Matematik Enstitüsü, Orta Doğu Teknik Üniversitesi, Ankara, 06800, Türkiye, e-posta: ersan@metu.edu.tr.

Ç. Çalık, M. Özarar, Z. Tok ve O. Yayla: Uygulamalı Matematik Enstitüsü, Orta Doğu Teknik Üniversitesi, Ankara, 06800, Türkiye, e-posta: ccalik@metu.edu.tr, mert.ozarar@gmail.com, zalihayuce@gmail.com, yayla@metu.edu.tr

M. Özarar: TÜRKTRUST Bilgi, İletişim ve Bilişim Güvenliği Hizmetleri A.Ş., Galyum Blok, Kat:2 No:20, Ankara, 06800 Türkiye e-posta: mert.ozarar@gmail.com

Gönderildi: 15 Temmuz 2013; düzeltildi: 15 Temmuz 2013.

*Bu çalışma TÜRKTRUST Bilgi, İletişim ve Bilişim Güvenliği Hizmetleri A.Ş. tarafından desteklenmiştir.

Tablo I
RSA SİSTEMİ PARAMETRELERİ.

n	açık modülüs parametresi
e	açık üst parametresi
d	gizli üst parametresi
p, q	açık modülüs parametresi n'nin asal çarpanları
$\phi(n)$	n'den küçük ve n ile aralarında asal olan sayıların sayısı

II. TANIMLAR

RSA, her kullanıcının bir gizli bir de açık anahtarının olduğu bir açık anahtarlı kriptosistemdir. Sistemi oluşturan parametreler Tablo I'de gösterilmiştir. Açık anahtar (n, e) ikilisi ile, gizli anahtar ise (n, d) ikilisi ile gösterilir. n sayısı, p ve q olarak gösterilen iki asal sayının çarpımından oluşmaktadır. RSA parametreleri p ve q'yu bilen birisi, $\phi(n) = (p-1)(q-1)$ sayısını hesaplayabilmekte ve $\phi(n)$ modülüsünde birbirinin tersi olan e ve d parametrelerini oluşturabilmektedir. Oluşturulan bu sistemde (n, e) açık anahtarı şifreleme ve imza doğrulama işlemlerinde, (n, d) gizli anahtarı ise deşifreleme ve imza üretme işlemlerinde kullanılır. Birçok uygulamada e sayısı işlemlerin daha hızlı yapılabilmesi için *Fermat asal sayısı* olan $2^{16} + 1 = 65537$ olarak seçilmektedir.

RSA sisteminde (n, e)'nin açık bilgi olduğu göz önüne alındığında, gizli anahtar parametresi d'nin bulunmasının, n sayısından p ve q çarpanlarını bulmanın zorluğuna dayandığına inanılır. Bu nedenle, sistemin güvenliğini sağlamak için çarpanlara ayırma algoritmalarına dayanıklı p ve q, dolayısıyla n sayısı oluşturmak önemlidir. Bunun için de p ve q parametreleri standartlarda belirtilen bir takım kriterlere uygun seçilmelidir [3]–[5]. Uygun şekilde seçilen parametreler de ancak n parametresinin büyüklüğü ile orantılı bir güvenlik seviyesi sunarlar. RSA sisteminin güvenlik seviyesi, bu sistemi kırmak için gereken hesaplama gücünün büyüklüğüne bağlıdır. Güvenliği k-bit olan bir sistemi kırmak için 2^k mertebesinde işlem yapmak gerekmektedir. Simetrik anahtarlı kriptosistemlerde güvenlik doğrudan anahtar boyuna karşılık gelirken, RSA'da ise n parametresine bağlı olarak yapılması gereken işlem miktarının hesaplanmasıyla elde edilir. Tablo II, RSA sistemindeki n parametresinin bit cinsinden uzunluğunun (k) hangi güvenlik seviyesine karşılık geldiğini göstermektedir [6].

Tablo II
RSA GÜVENLİK SEVİYELERİ.

Güvenlik seviyesi (bit)	RSA sayısı n (bit uzunluğu: k)
80	1024
112	2048
128	3072
192	7680
256	15360

III. KAPSAM

RSA sisteminin parametrelerinin güvenlik testleri ile ilgili üç modülden oluşan bir yazılım paketi geliştirilmiştir. Bu modüllerin hangi durumlarda ve ne amaçla kullanıldığı aşağıda açıklanmıştır.

1) **(n,e,d) testi.** RSA parametrelerinden gizli ve açık anahtarların bilinmesi, yani $\{n, e, d\}$'nin bilinmesi. Bu durumda amaç n'nin çarpanları olan p ve q asal sayılarını bulmak ve tüm parametrelerin standartlarda belirtilen şartlara uygunluğunu kontrol etmektir.
2) **(n,e) testi.** RSA parametrelerinden sadece açık anahtarın, yani (n, e) ikilisinin bilinmesi durumu. Bu durumda n sayısı çarpanlarına ayrılmaya çalışılır.
3) **Ortak çarpan testi.** Birden fazla RSA açık anahtarının bilinmesi durumu. Bu durumda anahtarların birbirileri ile ortak çarpanının olup olmadığına bakılır. Bu tarz bir ortak çarpanın bulunması, söz konusu n parametrelerinin çarpanlara ayrılması anlamına gelmektedir. Bu test, p ve q parametrelerinin rastsal bir şekilde seçilmediği ve farklı n parametrelerinin aynı asal sayılar tarafından oluşturulduğunu tespit etmek için kullanılır.

IV. YÖNTEM

Bu bölümde RSA parametrelerinin ETSI TS 102 176-1 (2007), FIPS PUB 186-3 (2009) ve IEEE 1363 (2004) standartlarına ve diğer güvenlik gereksinimlerine uygunluğu için gereken test maddeleri sunulacaktır. Aşağıda temel standartlar sırasıyla ETSI, FIPS ve IEEE şeklinde kısaltılmıştır. Belirtilen güvenlik test maddelerinin hangi standardın gereksinimi olduğu parantez içinde belirtilmiştir.

RSA kriptosistemi parametrelerinin testi üç durumda ele alınmıştır:

A. (n, e, d) parametreleri bilindiği durumda,
B. (n, e) parametreleri bilindiği durumda,
C. $(n_1, n_2, \ldots, n_l)$ parametreleri bilindiği durumda.

A. (n, e, d) testi

Bu teste RSA açık ve gizli anahtarını oluşturan $\{n, e, d\}$ parametrelerinin tamamı girdi olarak verilir. Bu girdilere sırasıyla aşağıdaki işlemler uygulanır:

1) n sayısının bit uzunluğu (k) Tablo II'de verilen güvenlik seviyesini sağlamalıdır. (ETSI, FIPS, IEEE)
2) e sayısı 65537 ve 2^{256} arasında tek tamsayı olmalıdır. (FIPS)
3) d sayısı $2^{k/2}$ den büyük olmalıdır. (ETSI, FIPS, IEEE)
4) Factorn(n, e, d) algoritması (bkz. EK: Algoritma 1) ile n sayısını bölen p sayısı ve sonra da q sayısı bulunur. Aşağıdaki testler yapılır:

Tablo III
P1, P2, Q1 VE Q2 SAYILARININ BİT UZUNLUĞU.

n (bit uzunluğu)	p1, p2, q1 ve q2 (bit uzunluğu)
1024	> 100
2048	> 140
3072	> 170

a) p ve q sayılarının Miller-Rabin (MR) [4] ve Lucas (L) [4] olasılıksal asallık testlerinin birlikte uygulanması ile asal olmama olasılıkları 2^{-100}'den az olmalıdır. Bu amaçla asal sayıların bit uzunluğuna göre aşağıda belirtilen miktarlardaki Miller-Rabin (MR) ve Lucas (L) olasılıksal asallık testleri uygulanmalıdır. (ETSI, FIPS, IEEE)
   i) 512 bit asallar için 7MR + 1L
   ii) 1024 asallar için 4MR + 1L
   iii) 1536 asallar için 3MR + 1L
   iv) 2048 asallar için 3MR + 1L
b) p ve q sayıları $2^{(k-1)/2} \leq p, q \leq (2^{k/2} - 1)$ aralığında olmalıdır. (FIPS)
c) p ve q sayıları arasındaki fark $2^{(k/2)-100}$'den büyük olmalıdır. (FIPS)
d) $(p\pm1)$ ve $(q\pm1)$ sayıları aşağıdaki şartları sağlamalıdır.
   i) $(p-1)$ sayısının en büyük asal böleni $p1$,
   ii) $(p+1)$ sayısının en büyük asal böleni $p2$,
   iii) $(q-1)$ sayısının en büyük asal böleni $q1$,
   iv) $(q+1)$ sayısının en büyük asal böleni $q2$ olsun.
   $p1$, $p2$, $q1$ ve $q2$ asal bölenleri Eliptik Eğri Çarpanlara Ayırma Algoritması [8] ile bulunur. Bu asallar Tablo III'deki minimum bit uzunlukları değerlerini sağlamalıdır. (FIPS)

Bu test basamakları sayesinde RSA kriptosisteminin aşağıda belirtilen güvenlik maddeleri test edilmiş olur:

1) Sistemin gerçek güvenlik derecesi,
2) Kök alma ataklarına karşı sistemin güvenilirliği,
3) Gizli anahtar d'nin güvenliği,
4) p ve q sayılarının asallıkları,
5) Eliptik Eğri temelli (ECM) çarpanlara ayırma yöntemine karşı sistemin dayanıklılığı,
6) Fermat çarpanlarına ayırma yöntemine karşı sistemin dayanıklılığı,
7) $p-1$ ve $p+1$ çarpanlarına ayırma yöntemlerine karşı sistemin dayanıklılığı.

B. (n, e) testi

Bu test girdi olarak RSA parametresi n'yi alarak, bu sayıyı çarpanlarına ayırmaya çalışır. Aşağıdaki çarpanlara ayırma algoritmaları sırayla uygulanır:

1) n sayısının bit uzunluğu Tablo II'de verilen güvenlik seviyesini sağlamalıdır. (ETSI, FIPS, IEEE)
2) e sayısı 65537 ve 2^{256} arasında tek tamsayı olmalıdır. (FIPS)
3) n sayısının küçük böleni olmamalıdır. n sayısının 2^{140}'dan küçük böleni Eliptik Eğri Çarpanlara Ayırma Algoritması [8] ile aranır. (ETSI, FIPS, IEEE)

4) Fermat Çarpanlara Ayırma Algoritması [2] ile n sayısının çarpanı aranır. (ETSI, FIPS, IEEE)

Bu test basamakları sayesinde RSA kriptosisteminin aşağıda belirtilen güvenlik maddeleri test edilmiş olur:

1) Sistemin gerçek güvenlik derecesi,
2) Kök alma ataklarına karşı sistemim güvenilirliği,
3) p ve q sayılarının büyüklüğü,
4) p ve q sayılarının birbirine uzaklığı.

C. Ortak çarpan testi

Bu testin amacı, RSA açık anahtar parametresi n'lerden oluşan $\{n_1, \cdots, n_l\}$ kümesi içinde herhangi farklı iki n_i ve n_j sayısının $(1 \leq i < j \leq l)$ ortak çarpanı olup olmadığına bakmaktır. Böyle bir çarpanın bulunması halinde, yani $d = gcd(n_i, n_j) \neq 1$ ise, bu sayıların bir çarpanı olarak d sayısı bulunmuş olur.

Bu teste girdi olarak verilecek sayılarının $n = p.q$ biçiminde iki tek asal sayının çarpımı olacağı varsayılmakla birlikte, test prosedürüne konulan ek bir kontrol ile bu biçimde olmayan n sayılarını da dikkate alan bir yöntem uygulanabilir.

Verilen $\{n_1, \cdots, n_l\}$ kümesi için P_t sayısı ilk t elemanın çarpımı olsun, yani $P_t = \prod_{i=1}^{t} n_i$. Bu durumda $gcd(P_t, n_{t+1})$ kontrol edilerek n_{t+1} sayısının daha önceki sayılardan herhangi biri ile ortak çarpanı olup olmadığı bulunur. Ortak çarpan var ise n_{t+1}'in hangi eleman ile ortak çarpanı olduğu tek tek karşılaştırma yapılarak bulunur. Eğer ortak çarpan yok ise P_{t+1}'in sonraki değeri $P_{t+1} = P_t.n_{t+1}$ formülüne göre bulunur ve işlem benzer şekilde devam eder.

Diğer bir ifadeyle $p_s = gcd(n_s, n_1 n_2 \ldots n_{s-1})$ hesabı her $s = 1, 2, \ldots, l$ için yapılır. p_s sayısı birden farklı ise n_s sayısının bir asal çarpanı bulunmuştur.

Böylelikle aynı p veya q asal sayılarının sistemde birden fazla n sayısında olup olmadığı test edilmiş olur.

V. Yazılımın Karmaşıklığı

Yazılımın her bir modülünün karmaşıklığı aşağıdaki şekilde özetlenebilir.

1) (n, e, d) testi için $p-1$, $p+1$, $q-1$ ve $q+1$'in çarpanlarının incelendiği testler haricindeki tüm testler ihmal edilebilir düzeyde çalışma süresi gerektirmektedir. $p-1$, $p+1$, $q-1$ ve $q+1$ sayılarının çarpanlarına bakıldığı durumda ise bu sayıların büyüklüğü (512-bit ya da 1024-bit) ve dolayısıyla hangi uzunluğa kadar olan çarpanların arandığına göre ve çarpanlara ayırma yönteminin kesinlik derecesini belirten deneme sayısına göre değişmektedir. 1024-bit RSA anahtarları için p ve q yaklaşık 512-bit olmakta ve standartlara göre de $p-1$, $p+1$, $q-1$ ve $q+1$'in en az 100 bitten büyük bir asal çarpanının olması istenmektedir. Bu dört sayı için de çarpan arama işlemi birbirinden bağımsızdır ve paralel olarak gerçekleştirilebilir, bu sayede testlerin ard arda çalıştırıldığı seri uygulamaya oranla 4 kat avantaj sağlanmış olur. 1024-bit RSA anahtarları için GMP-ECM [8] uygulamasının 30-basamaklı çarpan arama parametreleri kullanılmış ve 3.2 Ghz işlemcili bir masaüstü bilgisayarda ortalama 10 dakikada sayının 100 bitin altındaki çarpanları bulunmuştur. 2048-bit RSA için ise GMP-ECM [8] uygulamasının 40-basamaklı sayıları çarpanlara ayırma parametreleri kullanılmış ve 3.2 Ghz işlemcili bir masaüstü bilgisayarda ortalama 1 günde 140 bitten küçük çarpanlar tesbit edilebilmiştir.
2) (n, e) testinin başarılı olması n sayısının çarpanlarına ayrılması ve dolayısıyla RSA sisteminin kırılması anlamına gelir. Bu yüzden RSA parametrelerinin standartlara uygun seçildiği durumlarda bu testin başarı ile sonuçlanması beklenmemektedir. Bu testin başarılı olacağı iki durum vardır. Birincisi p veya q'un bit uzunluğunun oldukça düşük olması durumudur. Bu durumun testi için ECM methodu [8] ile n sayısının 140 bite kadar olan çarpanları aranmıştır. Bu test ortalama 1 gün sürmektedir. İkinci durumda n sayısının çarpanları p ve q'nun birlerine çok yakın olmasıdır. Bu durumda testin istenen çalışma süresine göre uygun değer verilebilir.
3) Ortak çarpan arama testi modülüs sayısı n'lerin adedi l sayısına doğrusal olarak bağlı bir işlem karmaşıklığı gerektirir, dolayısıyla bu testi gerçekleştirmek modern işlemcili bilgisayarlarda en fazla dakikalar mertebesinde vakit almaktadır. Örneğin 10,000 adet 1024-bitlik RSA modülüsünün ortak çarpan arama işlemi 5 dakikadan kısa bir sürede tamamlanmaktadır.

VI. Sonuç

Bu çalışmada RSA e-imza sistemini oluşturan parametrelerin testi için geliştirilen yazılım paketi sunulmuştur. Testler, açık ve gizli parametrelerin bilinmesine bağlı olarak üç farklı kategoriye ayrılmıştır. Her bir test için yapılacak işlemler özet olarak maddeler halinde belirtilmiştir. Bu maddeleri test eden yazılım paketi oluşturulmuştur. Yazılımın karmaşıklığı $p\pm1$ ve $q\pm1$ sayılarının çarpanlarının bulunması hariç çok düşüktür. $p\pm1$ ve $q\pm1$ sayılarının çarpanlarının bulunması için de en uygun deneme yöntemi yazılımın içine dahil edilmiştir.

Ek

Verilen (n, e, d) üçlüsünden n sayısının p ve q asal çarpanlarının bulunması aşağıda verilen Factorn(n, e, d) algortiması ile bulunur.

Algoritma 1 Factorn: n sayısının p ve q asal çarpanlarının bulunması

Girdi: n, e, d
Çıktı: p, q

$ed - 1 = 2^s t$ şartını sağlayan t tek sayısı bulunur.
for $a = 2$'den n'ye **do**
  $x = a^t - 1 \pmod n$
  $d = gcd(x, n)$
  if $(d! = 1)$ ve $(d! = n)$ **then**
    $p = d$
    $q = n/p$
    DUR.
  end if
end for

KAYNAKÇA

[1] Türkiye Cumhuriyeti 5070 Sayılı Elektronik İmza Kanunu: http://www.tbmm.gov.tr/kanunlar/k5070.html
[2] Cohen H., A course in computational algebraic number theory, Graduate Texts in Mathe-matics 138, Springer, 1993.
[3] ETSI TS 102 176-1 v1.2.1, Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms., 2005.
[4] FIPS PUB 186-3, Digital Signature Standard (DSS), 2009.
[5] IEEE 1363-2000, Standard Specifications for Public-Key Cryptography, 2000.
[6] NIST Special Publication 800-57, Recommendation for Key Management - Part 1: General (Revision 3), 2012.
[7] Rivest, R.; Shamir, A.; Adleman L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM 21 (2): (1978). 120–126. doi:10.1145/359340.359342
[8] Zimmermann, P.; Dodson B. "20 years of ECM." Algorithmic number theory. Springer Berlin Heidelberg, 2006. 525-542.