T.C.
ERZİNCAN BİNALİ YILDIRIM ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

RSA KRİPTOSİSTEMİ ve $p-1$ ÇARPANLARA AYIRMA ALGORİTMASI

Nurullah BÜTÜN

Danışman: Dr. Öğr. Üyesi İsrafil OKUMUŞ

MATEMATİK
ANABİLİM DALI

ERZİNCAN
2018

Kabul ve Onay Sayfası

Dr. Öğr. Üyesi İsrafil OKUMUŞ danışmanlığında, Nurullah BÜTÜN tarafından hazırlanan bu çalışma 13/09/2018 tarihinde aşağıdaki jüri tarafından Matematik Anabilim Dalı'nda Yüksek Lisans Tezi olarak oybirliği/~~oy çokluğu~~ (3/3.) ile kabul edilmiştir.

Başkan	Prof. Dr. Ercan ÇELİK	İmza:
Üye	Dr. Öğr. Üyesi İsrafil OKUMUŞ	İmza:
Üye	Dr. Öğr. Üyesi Yasemin TAŞYURDU	İmza:

Yukarıdaki sonuç Enstitü Yönetim Kurulunun 12 / 10 / 2018 tarih ve 38/9..... sayılı kararı ile onaylanmıştır.

Prof. Dr. Paşa YALÇIN
Enstitü Müdürü

Bilimsel Etiğe Uygunluk Sayfası

"RSA Kriptosistemi ve $p-1$ Çarpanlara Ayırma Algoritması" isimli "Yüksek Lisans" tezim tarafımca intihal tespit programı ile incelenmiştir. Buna göre tezimde bilimsel etik ihlali ve intihal olarak nitelendirilebilecek herhangi bir durum olmadığını taahhüt ederim.

Bu çalışmadaki tüm bilgilerin, akademik ve etik kurallara uygun bir biçimde elde edildiğini, aynı zamanda bu kural ve davranışların gerektirdiği gibi, bu çalışmanın özünde olmayan tüm materyal ve sonuçları tam olarak aktardığımı ve referans gösterdiğimi beyan ederim. 13/09/2018

Nurullah BÜTÜN

ÖZET

Yüksek Lisans Tezi

RSA KRİPTOSİSTEMİ ve
$p-1$ ÇARPANLARA AYIRMA ALGORİTMASI

Nurullah BÜTÜN

Erzincan Binali Yıldırım Üniversitesi
Fen Bilimleri Enstitüsü
Matematik Anabilim Dalı

Danışman: Dr. Öğr. Üyesi İsrafil OKUMUŞ

RSA kriptosisteminin güvenliği, tamsayıların çarpanlarına ayrımının zorluğu üzerine kuruludur. Bu kriptosistemi kırabilmek için çeşitli çarpanlara ayırma algoritmaları geliştirilmiştir. Bu algoritmalar özel amaçlı ve genel amaçlı algoritmalar olmak üzere iki ana başlık altında çalışılmaktadır. Bu tezde literatürde var olan bazı özel amaçlı çarpanlara ayırma algoritmaları incelenmiş, $p-1$ çarpanlara ayırma algoritması detaylı olarak verilmiştir.

2018, 36 Sayfa

Anahtar Kelimeler: Kriptoloji, $p-1$ Çarpanlara ayırma algoritması, RSA.

ABSTRACT

Master Thesis

RSA CRYPTOSYSTEM and
$p-1$ FACTORİZATİONS ALGORİTHM

Nurullah BÜTÜN

Erzincan Binali Yıldırım University
Graduate School of Natural and Applied Sciences
Department of Mathematics

Supervisor: Asist. Prof. Dr. İsrafil OKUMUŞ

The security of RSA cyrptosystem is based on the difficulty of factorization of integers. Various factorization algorithms have been developed to break RSA cryptosystem. Those algorithms are practically studied in two main titles, special-purpose algorithms and general-purpose algorithms. In this paper, several special-purpose factoring algorithms already existing in the literature are studied and an in depth analysis of $p-1$ factoring algorithm is addressed.

2018, 36 Pages

Keywords: Cryptology, $p-1$ Integer factorization algorithm, RSA.

TEŞEKKÜR

Yüksek lisans tezi olarak sunduğum bu çalışma, Erzincan Üniversitesi Fen Edebiyat Fakültesi Matematik Bölümü'nde hazırlanmıştır.

Tez çalışması ve yazımı sürecinde, bilgisini ve ilgisini benden esirgemeyen, zaman ve mekan mefhumu gözetmeden bana rehberlik edip çalışmalarıma katkı sağlayan, danışmanlığımı üstlenen Sayın Dr.Öğr. Üyesi İsrafil OKUMUŞ'a teşekkürü bir borç bilirim.

Kıymetli görüşlerini ve tecrübelerini savunma süresince paylaşan Sayın Prof. Dr. Ercan ÇELİK'e ve Sayın Dr. Öğr. Üyesi Yasemin TAŞYURDU'na ayrıca teşekkür ederim.

Hayatım boyunca yanımda olan aileme ve pek kıymetli eşime teşekkür eder, şükranlarımı sunarım.

Nurullah BÜTÜN
Eylül, 2018

İÇİNDEKİLER

Sayfa

ALGORİTMALAR LİSTESİ

Sayfa

TABLOLAR LİSTESİ

Sayfa

SİMGELER ve KISALTMALAR

Simgeler

$a\|b$	a böler b'yi
(a,b)	a ile b'nin en büyük ortak böleni
C	Şifreli Metin
d	RSA'da Özel Anahtar
e	RSA'da Genel Anahtar
M	Açık Metin
$\emptyset(n)$	Euler Phi Fonksiyonu
$\equiv$	Denk

Kısaltmalar

GNFS	Genaral Number Field Sieve
RSA	Rivest, Shamir, Adleman
SNFS	Special Number Field Sieve

1. GİRİŞ

Eski çağlardan günümüze kadar insanlık için bilgi büyük bir önem arz etmektedir. Üretilen bilginin saklanması, korunması veya ikinci şahıslara güvenli ve doğru bir şekilde iletilebilmesi her zaman problem teşkil etmiştir. Bilgi güvenliğini sağlayabilmek için Mısırlılardan Romalılara, Sümerlerden Osmanlılara ve günümüz modern toplumlarına kadar her kültür farklı araçlar-metotlar geliştirmiş ve kullanmışlardır. Bu yöntemler insanlığın bilgi birikiminin artışına paralel olarak sürekli gelişim göstermişlerdir. Bilişim teknolojilerinin tarihsel süreçler içinde gelişimi ile bilgi aktarımı, paylaşımı, iletişimi çok daha fazla önem arz etmeye başlamıştır. Bu önem bilginin korunumu ve güvenli haberleşme ihtiyacını doğurmuştur. Bu ihtiyaca binaen çeşitli yöntemler geliştirilmeye çalışılmıştır. Bu yöntemler ise kriptoloji biliminin doğmasını ve gelişmesini sağlamışlardır.

Kriptoloji Yunanca “gizli” anlamına gelen “kript” ve “bilim” anlamına gelen “loji” kelimelerinden türetilmiştir ve iletişimde gizlilik bilimi manasına gelmektedir. Kriptoloji temel olarak Kriptografi ve Kriptanaliz olmak üzere iki bölüme ayrılır. Kriptografi okunabilir durumdaki bir bilginin, istenmeyen taraflarca okunamayacak bir hale dönüştürülmesinde kullanılan şifreleme yapılarının geliştirilmesi üzerine çalışılan bilim dalıdır. Kriptanaliz ise şifreli yapıların kırılmasında kullanılan tekniklerin çalışıldığı alandır.

Günümüzde kullanılan kriptografik algoritmalar kullandıkları anahtar biçimine göre simetrik veya asimetrik olarak adlandırılan iki bölüme ayrılır. Simetrik kriptosistemlerinde hem şifreleme hem de şifre çözme işlemleri için aynı anahtar kullanılır. Asimetrik kriptosistemlerinde ise şifreleme ve şifre çözme işlemleri için farklı anahtarlar kullanılır ve bu anahtarlardan bir tanesiyle şifreleme yapılırken diğeriyle de şifre çözme işlemi gerçekleştirilir.

Kriptografi tarihinde en güçlü gelişme, 1976 yılında, Diffie ve Hellman tarafından "*New Directions in Cryptography*" isimli makaleleri yayınlandığında olmuştur. Bu makalede simetrik şifreleme sistemleri için güvenli anahtar değişimi yapılan bir matematiksel yöntem ileri sürülmüştür.

1978'de Rivest, Shamir ve Adleman "*A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*" isimli makalelerinde yazarların isimlerinin baş harfleri olan ve RSA olarak adlandırılan ilk pratik asimetrik şifreleme ve elektronik imza algoritmasını keşfetmişlerdir. Güvenli ve gizli haberleşmeyi sağlayabilmek adına geliştirilen RSA kriptosistemi, elektronik ticarette, sayısal imzada, kimlik belirlemede ve internet üzerinden yapılan haberleşmelerde kullanılmaktadır.

1985'te Taher El-Gamal Discrete Logaritma problemine dayanan bir diğer pratik asimetrik kripto sistemi "*A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms*" isimli makalesinde ileri sürmüştür.

RSA kriptosisteminin güvenliği büyük sayıların çarpanlara ayrılması problemine dayanmaktadır. Büyük sayıların çarpanlarına ayrılmasının zorluğuna karşılık henüz etkin bir yöntem bulunmuş değildir. 1970'lerden sonra modern kriptolojinin gelişmesiyle birlikte tamsayıların çarpanlarına ayrılması problemi çok önemli bir konu haline gelmiştir.

Geçmişte Fermat (~ 1640), Euler (~ 1750), Legendre (~ 1790), Gauss (~ 1800) gibi ünlü matematikçiler tamsayıların çarpanlarına ayrılması ile ilgili çeşitli çalışmalar yapmışlardır.

RSA kriptosistemine karşı çeşitli saldırılar geliştirilmiştir. Bunların önemli kısmını ise çarpanlara ayırma algoritmaları oluşturmaktadır. Günümüzde tamsayıların çarpanlara ayrılması ile ilgili algoritmalar özel amaçlı ve genel amaçlı olmak üzere iki grupta çalışılmaktadır. Genel amaçlı çarpanlara ayırma algoritmaların çalışma zamanı verilen N yarı asal sayısının büyüklüğüne bağlıdır. Özel amaçlı çarpanlara ayırma algoritmaların çalışma zamanı ise verilen N yarı asal sayısını oluşturan çarpanların belirli özelliklerine veya N yarı asal sayısının bazı belirli özelliklerine bağlıdır. Bu nedenle RSA Kripto sisteminde asal sayılar seçilirken ve N sayısı oluşturulurken özel amaçlı algoritmalar göz önünde bulundurulması bir zorunluluktur.

Pollard (1974) $p-1$ olarak isimlendirilen özel amaçlı bir algoritma ileri sürmüştür. Montgomery (1980) genel amaçlı Quadratic Sieve algoritmasını geliştirmiştir. Pomerance (1981) genel amaçlı Quadratic Sieve algoritmasını geliştirmiştir. Williams

(1982) $p+1$ olarak isimlendirilen özel amaçlı bir algoritma ileri sürmüştür. Lenstra (1983) eliptik eğri çarpanlara ayırma metodunu geliştirmiştir. Pollard (1988) Özel Sayı Cismi Elemesi (SNFS) olarak adlandırılan algoritmayı sunmuştur. Lenstra vd. (1990) Genel Sayı Cisim Elemesi (GNFS) adı verilen bir genel amaçlı çarpanlara ayırma algoritması sunmuşlardır ve bu algoritma günümüzde bilinen en hızlı genel amaçlı çarpanlara ayırma algoritmasıdır.

Ülkemizde, Asimetrik Şifreleme, RSA ve Çarpanlara Ayırma Algoritmaları ile ilgili olarak, Pamukçu (2006), Buluş (2006), Aybak (2010), Yücelen (2011), Nuriyeva (2010), Okumuş (2012), Külen (2013), Hassanpour (2015) lisansüstü çalışmalar yapmışlardır.

Pamukçu, "Kriptografi için Faktorizasyon Metotları" isimli tezinde sayılar teorisi ile ilgili temel bilgileri vermiş, RSA'yı örneklerle anlatmış ve literatürde var olan bazı çarpanlara ayırma algoritmalarını anlatıp algoritmaların maple kodlarını vermiştir.

Buluş, "Temel Şifreleme Algoritmaları ve Kriptanalizlerinin İncelenmesi" isimli tezinde temel şifreleme algoritmalarını (Vigenere, Hill, Affine, Öteleme, Yer Değiştirme, Permütasyon Şifrelemeleri vb.) ve bunların kriptanalizlerini incelemiştir.

Aybak, "Sayı Cismi Çarpanlara Ayırma Yöntemi" isimli tezinde Fermat, Dixon, Quadratic Sieve ve Sayı Cismi çarpanlara ayırma yöntemlerini inceleyip bunların Mapple 11 kodlarını vermiştir.

Nuriyeva, "Çarpanlara Ayırma Algoritmaları Üzerine" isimli tezinde literatürde var olan genel amaçlı ve özel amaçlı çarpanlara ayırma algoritmalarını incelemiştir. Burada yöntemlerin matematik alt yapısını vermeden algoritmaları tanıtmayı yeğlemiştir. Ancak tez, algoritmaların yazılım programlarına aktarımı açısından önemli bir çalışmadır.

Yücelen, "Kriptolojide Eliptik Eğri Algoritması" isimli tezinde eliptik eğri şifrelemenin matematiksel temelleri ve tanımlarını yapmış, El-Gamal eliptik eğri şifreleme uygulamasını geliştirmiştir. Eliptik eğri şifreleme algoritmasını RSA şifreleme algoritması ile karşılaştırmış, avantajlı yönlerini ortaya koymuştur.

Mert ve Şeker, “RSA Şifreleme Sistemine Karşı Yeni Bir Çarpanlara Ayırma Saldırısı” isimli makalelerinde literatürde var olan bazı çarpanlara ayırma algoritmalarını incelemişler ve daha hızlı sonuç veren yeni bir algoritma ileri sürmüşlerdir: Ters Kalbur Çarpanlara Ayırma Ağacı.

Okumuş, “RSA Kriptosisteminin Hızını Etkileyen Faktörler” isimli tezinde RSA’ da şifreleme ve şifre açma üzerine olan yöntemleri incelemiş, Rebalanced CRT-RSA Şifre Açma Algoritması ile Montgomery Radix-4 Modüler Çarpım Algoritmasını geliştirmiştir.

Külen, “Kriptolojide Bazı Şifreleme Yöntemlerinde Cebirsel Yaklaşımlar” isimli tezinde geçmişten günümüze kullanılmış bazı temel şifreleme sistemlerindeki (Değiştirme, Kaydırma, Affine, Pigben, Vigenere, Hill, Permütasyon Şifrelemeleri ve Mors Kodu ile RSA Şifreleme Sistemi) cebirsel yaklaşımları açıklamıştır.

Hassanpour, “Asal Sayıların Şifreleme Teorisindeki Uygulamaları” isimli tezinde güvenli iletişim, kimlik belirleme-tespit, sayısal imza, sertifika dağıtımı, elektronik ticaret gibi konuları incelemiş, şifrelemede kullanılan eliptik eğriler hakkında bilgi vermiştir.

Yüksek Öğretim Kurumunun Ulusal Tez Merkezi veri tabanında yapılan taramalar neticesinde, tez konusuyla ilgili olarak taratılan anahtar kelimelerle ilgili şu sonuçlara ulaşılmıştır:

Tablo 1.1. "Şifreleme-Çarpanlara Ayırma" ile ilgili ulusal çerçevede yapılan lisansüstü çalışmalara dair sayısal veriler:

Taratılan Anahtar Kelimeler	**Matematik**		**Bilgisayar Bilimleri**		**Elektrik-Elektronik Mühendisliği Bilimleri**	
	Yüksek Lisans	Doktora	Yüksek Lisans	Doktora	Yüksek Lisans	Doktora
"RSA"	1	1	10	1	6	-
"Eliptik Eğri"	3	1	7	1	9	-
"Çarpanlara Ayırma"	7	2	-	-	-	-
"Asal Sayılar"	2	-	-	-	-	-
"Kriptoloji"	7	-	5	-	2	-
"Kriptografi"	3	3	11	-	1	2
"Kriptoanaliz-Kriptanaliz	1	-	5	2	1	-
"Şifreleme"	17	3	56	14	33	5
Toplam	**41**	**10**	**94**	**18**	**52**	**7**

(İlgili veriler Ulusal Tez Merkezi'nin veri tabanından, 02.07.2018 tarihli taramalar neticesinde elde edilmiştir.)

Bu verilerden de anlaşılacağı üzere Kriptoloji bilimi sadece matematikçilerin ilgisini çekmemektedir, matematikçilerin yanında bilgisayar bilimleri ve elektrik-elektronik bilimleri üzerinde çalışan araştırmacıların da yoğun ilgilerine mazhar olmuştur. Bu çalışmada lisans eğitimini matematik dışında yapmış araştırmacılar da göz önünde bulundurularak, okuyucunun ilgisine sunulan algoritmaların matematiksel temelleri geniş bir şekilde ve elemanter seviyede tutarak verilmeye çalışılmıştır.

Bu çalışma beş bölümden oluşmaktadır. Giriş bölümünden sonra, Kuramsal Temeller adını alan ikinci bölümde çalışmada kullanılan temel tanım ve kavramlar verilmiştir.

Materyal ve Yöntem adını alan üçüncü bölümde, RSA kriptosistemi incelenmiştir.

Araştırma Bulguları adını alan dördüncü bölümde, RSA kriptosisteminin kırılması için geliştirilen bazı özel amaçlı algoritmalar incelenmiştir.

Son bölüm olan Sonuç bölümünde, tezde incelenen metotların gelişimi ile ilgili bilgi verilmiştir.

2. KURAMSAL TEMELLER

Bu bölümde araştırma konumuz olan özel amaçlı çarpanlara ayırma algoritmalarında kullanılan bazı temel tanım ve teoremler verilmiştir.

Tanım 2.1: a ve b tamsayılar olsun. Eğer $b = a.c$ olacak şekilde bir c tamsayısı varsa a, b'yi böler denir ya da a ile b bölünür denir ve $a|b$ seklinde gösterilir. Eğer a, b yi bölmüyorsa bu durum $a \nmid b$ ile gösterilir (Arıkan ve Halıcıoğlu, 2015).

Teorem 2.2: (Bölünebilirliğin Özellikleri) $a, b, c, d \in \mathbb{Z}^+$ olsun. Buna göre aşağıdaki ifadeler doğrudur.

i. $1|a$ ve $a|a$ dır.
ii. Eğer $a|b$ ise $a \leq b$ dir.
iii. Eğer $a|b$ ve $b|c$ ise $a|c$ dir.
iv. Eğer $a|$b ve $b|a$ ise bu taktirde $a = b$ dir.
v. $a|b$ olması için gerek ve yeter şart $\forall$c $\in \mathbb{Z}^+$ için $a.c|b.c$ olmasdır.
vi. Eğer $a|b$ ve $c|d$ ise $a.c|b.d$ dir.
vii. Eğer $a|b$ ve $a|c$ ise o zaman $\forall x, y \in \mathbb{Z}$ için $a|(b.x + c.y)$ dir.
viii. Eğer $(b, c) = 1$ ve $a.b|c$ ise $a|c$ dir (Taşçı, 2010).

Teorem 2.3: (Tamsayılarda Bölme Algoritması) $\forall a, b \in \mathbb{Z}^+$ için $b = q.a + r$ ve $0 \leq r < a$ olacak şekilde bir tek $q, r \in \mathbb{Z}^+$ tamsayı çifti vardır (Taşçı, 2010).

Tanım 2.4: a ve b sıfırdan farklı tam sayılar olmak üzere $c|a$ ve $c|b$ olacak şekilde bir $c > 0$ tamsayısı varsa c ye a ve b nin ortak böleni denir (Taşçı, 2010).

Tanım 2.5: Aşağıdaki özellikleri sağlayan pozitif d tamsayısına a ve b'nin en büyük ortak böleni denir ve $d = ebob(a, b) = (a, b)$ ile gösterilir (Arıkan ve Halıcıoğlu, 2015).

i. $d|a$ ve $d|b$ dir.
ii. c tamsayısı için $c|a$ ve $c|b$ ise $c|d$ dir.

Teorem 2.6 : Sıfırdan farklı iki tamsayının en büyük ortak böleni tektir (Taşçı, 2010).

Tanım 2.7: p, 1'den büyük pozitif tamsayı olsun. Eğer p'nin 1 ve p den başka pozitif böleni yoksa p ye bir asal sayı denir. 1'den büyük ve asal olmayan bir tamsayıya birleşik tamsayı denir (Asar vd., 2009).

Tanım 2.8: Birbirinden farklı iki asal sayının çarpımından oluşan birleşik sayıya ise yarı asal sayı denir (Ishmukhametov, 2013).

Tanım 2.9: (İyi Sıralama Prensibi): Pozitif tamsayıların boş olmayan her alt kümesi bir en küçük elemana sahiptir (Taşçı, 2010).

Lemma 2.10: 1'den büyük her tam sayının en az bir asal böleni vardır (Altındiş, 2005).

İspat: Aksini kabul ederek ispatımızı yapalım. Kabul edelim ki asal böleni olmayan pozitif bir tam sayı vardır. O zaman asal böleni olmayan pozitif tam sayılar cümlesi boş değildir ve iyi sıralama prensibine göre bir en küçük elemanı vardır. Bu elemana n dersek $n|n$ ve n nin asal böleni olmadığından n asal değildir,

$$n = ab, \qquad 1 < a < n, \qquad 1 < b < n$$

şeklinde yazılabilir, $a < n$ olduğundan a nın bir asal böleni olmalıdır. a nın herhangi bir böleni n nin de bir böleni olacağından n nin asal böleni olmasın kabulüne aykırıdır. O halde her pozitif tam sayının en az bir asal böleni vardır.

Teorem 2.11: Asal sayıların sayısı sonsuzdur (Bayraktar, 1988).

İspat: Kabul edelim ki asal sayılar sonludur. Bu takdirde bir en büyük p asal sayısı vardır. p ye eşit veya p den küçük asal sayıların çarpımı m ile gösterilirse,

$$m + 1 = (2.3.5.7 \ldots . p) + 1 > p$$

yazılabilir. En büyük asal sayı p olduğundan $m + 1$ asal olamaz. Şayet $m + 1$ birleşik bir sayı ise Lemma 2.10 dan dolayı $m + 1$ in bir asal çarpanı vardır. $m + 1$ in p den daha büyük bir asal çarpanının olması gerekir. Çünkü yukarıdaki eşitlikten dolayı p ye eşit veya p den daha küçük asallarla $m + 1$ in bölümünden kalan 1 dir. Fakat en büyük asal p idi. O halde en büyük bir asal sayı yoktur, yani asal sayılar cümlesi sonsuzdur.

Teorem 2.12: Eğer n bileşik sayı ise n'nin $\sqrt{n}$'yi geçmeyen bir asal çarpanı vardır (Bayraktar, 1988).

Örnek 2.13: 101 sayısının asal sayı olup olmadığı incelenirse: yukarıdaki önermenin karşıt tersi de doğru olacaktır. Yani n doğal sayısı için $\sqrt{n}$'yi geçmeyen bir asal çarpanı yoksa n bileşik sayı değildir, asal sayıdır. O halde $\sqrt{101}$'i geçmeyen asal sayıların 101'i bölüp bölmedikleri kontrol edilmelidir. $\sqrt{101} < 11$ olduğundan 10'a kadar olan asal sayıları kontrol etmek yeterlidir. 101 sayısı 2,3,5 ve 7 sayılarına tam bölünmediği için Teorem 2.12 gereği asal sayıdır.

Tanım 2.14: a, b iki tamsayı olmak üzere $(a, b) = 1$ ise a ve b ye aralarında asaldır denir (Taşçı, 2010).

Teorem 2.15: (Öklid Algoritması) a, b tam sayılar ve $a > 0$ olsun. Bölme algoritması art arda uygulanarak aşağıdaki eşitlikler elde edilir.

$$b = q_0 a + r_0,\ 0 \leq r_0 < a$$

$$a = q_1 r_0 + r_1,\ 0 \leq r_1 < r_0$$

$$r_0 = q_2 r_1 + r_2,\ 0 \leq r_2 < r_1$$

$$r_1 = q_3 r_2 + r_3,\ 0 \leq r_3 < r_2$$

$$\vdots$$

$$r_{n-1} = q_{n+1} r_n + r_{n+1},\ 0 \leq r_{n+1} < r_n$$

$r_{n+1} = 0$ olduğu için r_n değeri a ve b tamsayılarının en büyük ortak böleni olur yani $obeb(a, b) = r_n$ dir. Bu algoritmadaki işlemler sonsuza kadar gitmez, çünkü 0 ile a tamsayısı arasında sonlu sayıda tamsayı vardır (Asar vd., 2009).

Örnek 2.16: Öklid algoritması ile 101 ve 36 sayılarının $obeb$ lerini bulalım:

$$101 = 2.36 + 29$$

$$36 = 1.29 + 7$$

$$29 = 4.7 + 1$$

$$7 = 7.1 + 0$$

en sondaki sıfırdan farklı kalan 1 olduğundan $obeb\ (101{,}36) = 1$ dir.

Tanım 2.17: (Lineer Diophantine Denklemleri) a, b ve c tamsayılar, $ab \neq 0$ ve x ile y değişkenleri tamsayı olmak üzere

$$ax + by = c$$

şeklindeki denklemlere iki değişkenli lineer Diophantine denklemleri denir (Altındiş, 2005).

Teorem 2.18: a, b, c tamsayılar olmak üzere iki değişkenli $ax + by = c$ lineer Diophantine denkleminin tam sayılarda bir çözümünün olması için gerek ve yeter şart $(a, b) = d$ olmak üzere $d|c$ olmasıdır (Bayraktar, 1988).

Örnek 2.19: $30x + 45y = 100$ lineer Diophantine denkleminde $(30{,}45) = 15$ ve $15 \nmid 100$ olduğundan bu denklemin tam sayılarda çözümü yoktur.

Teorem 2.20: a, b, c tamsayılar, $(a, b) = d$ ve $d|c$ olmak üzere $ax + by = c$ lineer Diophantine denkleminin bir çözümü (x_0, y_0) ikilisi ise denklemin her (x, y) çözümü, m tamsayı olmak üzere;

$$x = x_0 + \frac{b}{d}m$$

$$y = y_0 - \frac{a}{d}m$$

dir (Bayraktar, 1988).

Teorem 2.21: (En Büyük Ortak Bölenin Lineer Formu) a ve b sıfırdan farklı iki tamsayı olsun. $d = (a, b)$ ise $d = ax + by$ olacak şekilde $x, y \in \mathbb{Z}$ vardır. Bu x ve y tamsayıları Öklid algoritması tersten işletilerek bulunabilir (Bayraktar, 1988). Bu algoritmaya ise "Genelleştirilmiş Öklid Algoritması" denir.

Örnek 2.22: $101x + 36y = 1$ eşitliğini sağlayan x ve y tamsayılarını bulalım. Bir önceki örnekte Öklid algoritması tersten işletilerek,

$$1 = 29 - 4.7$$

$$= 29 - 4.(36 - 1.29)$$

$$= 5.29 - 4.36$$

$$= 5.(101 - 2.36) - 4.36$$

$$= 5.101 - 14.36$$

$x = 5$ ve $y = -14$ bulunur. k tamsayı olmak üzere $x = 5 + 36k$ ve $y = -14 - 101k$ dir. $k = 1$ için $(x, y) = (41, -115)$ olur.

Teorem 2.23: a veya b sıfırdan farklı olmak üzere a ve b tam sayılarının aralarında asal olması için gerek ve yeter şart;

$$ax + by = 1$$

olacak şekilde x ve y tam sayılarının bulunmasıdır (Taşçı, 2010).

Tanım 2.24: a ve b tamsayılar ve $n > 0$ olan bir tamsayı olsun. Eğer $n|a - b$ ise a tamsayısı b tamsayısına n modülüne göre kongrüenttir (denktir) denir ve $a \equiv b(mod\ n)$ şeklinde gösterilir (Altındiş, 2005).

Teorem 2.25: (Kongrüansın Özellikleri) $\forall a, b, c, a_1, b_1 \in \mathbb{Z}$ ve $n \neq 0$ tamsayısı için aşağıdakiler doğrudur (Taşçı, 2010).

i. $a \equiv b(mod\ n)$ ancak ve ancak a ve b , n ye bölündüklerinde aynı kalanı verir.
ii. $a \equiv a(mod\ n)$ dır.
iii. $a \equiv b(mod\ n)$ iken $b \equiv a(mod\ n)$ dır.
iv. $a \equiv b(mod\ n)$ ve $b \equiv c(mod\ n)$ ise $a \equiv c(mod\ n)$
v. $a \equiv a_1(mod\ n)$ ve $b \equiv b_1(mod\ n)$ ise bu takdirde $a + b \equiv a_1 + b_1(mod\ n)$ ve $a.b \equiv a_1.b_1(mod\ n)$ dir.

Not: Genelleştirilmiş Öklid Algoritması ile $d = (a, b)$ ise $d = ax + by$ olacak şekilde x ile y tamsayıları bulunabiliyordu. Bu algoritma

$$ax \equiv d \ (mod\ b)$$

$$by \equiv d \ (mod\ a)$$

lineer kongrüans denklemlerini sağlayan x ve y değerlerini bulmak için de kullanılabilir.

Tanım 2.26: $a.x \equiv 1\ (mod\ n)$ denkliğini sağlayan x sayısına a'nın n modülüne göre aritmetik tersi denir (Taşçı, 2010).

Teorem 2.27: a'nın n modülüne göre aritmetik tersinin olması için gerek ve yeter şart $(a, n) = 1$ olmasıdır (Taşçı, 2010).

Tanım 2.28: (Eulerin ϕ Fonksiyonu) $n \geq 1$ olmak üzere n'yi ve n ile aralarında asal olan pozitif tam sayıların sayısına Euler fonksiyonu denir ve $\phi(n)$ ile gösterilir (Taşçı, 2010).

Teorem 2.29: p asal sayı ise $\phi(p) = p - 1$ dir (Bayraktar, 1988).

Teorem 2.30: $a, b \in \mathbb{Z}$ olmak üzere $obeb(a, b) = 1$ ise $\phi(a.b) = \phi(a).\phi(b)$ dir (Bayraktar, 1988).

Sonuç 2.31: p ile q asal sayılar iseler $\phi(p.q) = \phi(p).\phi(q) = (p-1).(q-1)$ olur. (Bayraktar, 1988).

Teorem 2.32: $a|bc$ ve $(a, b) = 1$ ise $a|c$ dir (Taşçı, 2010).

Teorem 2.33: p asal ve $p|bc$ ise $p|b$ veya $p|c$ dir (Taşçı, 2010).

Teorem 2.34: p asal $a_1, a_2, \dots, a_n$ pozitif tamsayılar olmak üzere $p|a_1 a_2 \dots a_n$ ise $1 \leq i \leq n$ olan herhangi bir i için $p|a_i$ dir (Taşçı, 2010).

Teorem 2.35: i: 1,2, … , n için $(a, b_i) = 1$ ise $(a, b_1 b_2 \dots b_n) = 1$ dir (Taşçı, 2010).

Tanım 2.36: $0,1,2,3,\dots,m-1$ tam sayılarına m modülüne göre en küçük kalanlar sistemi adı verilir. Bu m tane tam sayıdan herhangi iki tanesi m modülüne göre birbirine kongruent olmadıklarından aynı zamanda m modülüne göre komple kalanlar sistemi adı verilir (Altındiş, 2005).

Tanım 2.37: Komple kalanlar içinde m yi geçmeyen ve m ile aralarında asal olan kalanlara indirgenmiş kalanlar denir, indirgenmiş kalanların sayısı $\phi(m)$ tanedir (Altındiş, 2005).

Teorem 2.38: $a_1, a_2, \dots, a_{\phi(m)}$ sayıları m modülüne göre indirgenmiş kalanlar ve $(k,m)=1$ ise $ka_1, ka_2, \dots ka_{\phi(m)}$ de indirgenmiş kalanlardır (Altındiş, 2005).

İspat: İspatı yapmak için $ka_1, ka_2, \dots, ka_{\phi(m)}$ sayılarının herbirinin m ile aralarında asal ve herhangi ikisinin m modülüne göre her birine kongrüent olmadığı gösterilmelidir. $a_1, a_2, \dots, a_{\phi(m)}$ indirgenmiş kalanlar olduklarından herbir i için $(a_i, m)=1$ ve $i \neq j$ için $a_i \neq a_j (mod\ m)$ dir. $(a_i, m)=1$ ve $(k,m)=1$ için $(ka_1, m)=1$ dir. (Teorem 2.35) Şimdi herhangi iki kalanın birbirine kongrüent yani $i \neq j$ için $ka_i \equiv ka_j (mod\ m)$ olduğunu kabul edelim. $(k,m)=1$ olduğundan $a_i \equiv a_j (mod\ m)$ ve $i=j$ olur ki bu bir çelişkidir, o halde $i \neq j$ için $ka_1 \neq ka_j (mod\ m)$ dir.

Teorem 2.39: (Euler Teoremi): $n > 1$ ve $(a,m) = 1$ ise

$$a^{\phi(m)} \equiv 1\ (\ mod\ m\ )$$

dir (Altındiş, 2005).

İspat: $a_1, a_2, \dots, a_{\phi(m)}$ değerleri m modülüne göre indirgenmiş kalanlar olsun. O zaman $aa_1, aa_2, \dots, aa_{\phi(m)}$ de indirgenmiş kalanlar olacaktır (Teorem 2.38) ve $1 \leq i \leq \phi(m)$ olan her bir i için bir tek j, $1 \leq j \leq \phi(m)$ vardır ki, $aa_i \equiv aa_j (m)$ dir. Bu $\phi(m)$ tane kongrüansın çarpımı alınırsa

$$\prod_{i=1}^{\phi(m)} aa_i \equiv \prod_{j=1}^{\phi(m)} a_j\ (mod\ m)$$

$$a^{\phi(m)}.\prod_{i=1}^{\phi(m)} a_i \equiv \prod_{j=1}^{\phi(m)} a_j\ (mod\ m)$$

olur. $(a_i, m) = 1$ olduğundan $\left(\prod_{i=1}^{\phi(m)} a_i, m\right) = 1$ olur, her iki taraf $\prod_{i=1}^{\phi(m)} a_i$ kısaltılırsa

$$a^{\phi(m)} \equiv 1(mod\ m)$$

elde edilir ki bu da teoremin ispatıdır.

Örnek 2.40: $m = 187$ ve $(a, m) = 1$ olacak şekilde $a = 3$ alalım.

$$\phi(187) = \phi(11).\phi(17)$$

$$= (11 - 1).(17 - 1)$$

$$= 10.16 = 160$$

olur. Teorem 2.39 den dolayı $3^{160} \equiv 1\ (mod\ 187)$ dir.

Teorem 2.41: (Fermat Teoremi): p asal ve $p \nmid a$ olmak üzere

$$a^{p-1} \equiv 1(mod\ p)$$

dir (Altındiş, 2005).

İspat: Teorem 2.29 den $\phi(p) = p - 1$ olup bu eşitlik Euler teoreminde yerine yazılırsa teoremin ispatı kolayca elde edilir.

Fermat teoremi $p - 1$ çarpanlara ayırma algoritmasının temel mantığını oluşturur.

Örnek 2.42: $p = 7$ ve $a = 2$ alalım.

$$2^6 \equiv 64 \equiv 1\ (mod\ 7)$$

dir.

2.1. Hızlı Modüler Üs Hesaplama

Modern kriptosistemlerin bazılarında belli modüllerde, büyük sayıların yüksek mertebeden üslerini hesaplamak gerekir. İleride RSA kriptosisteminde de kullanacağımız hızlı modüler üs hesaplamaya dair bir örnek aşağıda verilmiştir.

Örnek 2.43: $15^{77} \equiv x \ (mod\ 221)$ denkliğini sağlayan x tamsayısını bulalım.

$$15^1 \equiv 15 \ (mod\ 221)$$
$$15^2 \equiv 4 \ (mod\ 221)$$
$$15^4 \equiv (15^2)^2 \equiv 4^2 \equiv 16 \ (mod\ 221)$$
$$15^8 \equiv (15^4)^2 \equiv 16^2 \equiv 35 \ (mod\ 221)$$
$$15^{16} \equiv (15^8)^2 \equiv 35^2 \equiv 120 \ (mod\ 221)$$
$$15^{32} \equiv (15^{16})^2 \equiv 120^2 \equiv 35 \ (mod\ 221)$$
$$15^{64} \equiv (15^{32})^2 \equiv 35^2 \equiv 120 \ (mod\ 221)$$
$$15^{77} \equiv 15^{64}.15^8.15^4.15^1 \equiv 120.35.16.15 \equiv 19 \ (mod\ 221)$$

olur. Yani $15^{77} \equiv x \ (mod\ 221)$ denkliğinde $x = 19$ dur.

2.2. Brahmagupta-Fibanacci Özdeşlikleri

Brahmagupta-Fibonacci özdeşliklerinden ilk defa milattan sonra III. yüzyılda Diophantus, Arithmetica adlı eserinde bahsetmiştir. Daha sonra, Hintli matematikçi ve gökbilimci olan Brahmagupta tarafından bu özdeşlik genelleştirilerek Brahmagupta Özdeşliği adıyla yeniden anılmış ve Pell eşitliği diye bilinen çalışmasında bu özdeşliği kullanmıştır.

Brahmagupta özdeşliği, Muhammed al-Fazari tarafından Sanskritçeden Arapçaya tercüme edilmiştir ve 1126 yılında Latinceye çevrilmiştir. Bu özdeşlikten 1225 yılında Fibonacci'nin "Book of Squares" adlı kitabında bahsedilmiştir. Özdeşliğin dört farklı formu mevcut olup burada tezde kullanılan bir tanesini incelenmiştir.

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2 \quad (2.1)$$
$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2 \quad (2.2)$$

$$(a^2 + nb^2)(c^2 + bd^2) = (ac - nbd)^2 + n(ad + bc)^2 \quad (2.3)$$
$$(a^2 + nb^2)(c^2 + bd^2) = (ac + nbd)^2 + n(ad - bc)^2 \quad (2.4)$$

Yukarıda verilen (2.1) eşitliği Euler'in çarpanlara ayırma algoritmasında kullanılmaktadır. Bu eşitliğin elde edilişi;

$$\begin{aligned}(a^2+b^2)(c^2+d^2) &= a^2c^2+a^2d^2+b^2c^2+b^2d^2\\ &= (ac)^2+(ad)^2+(bc)^2+(bd)^2\\ &= (ac)^2-2acbd+(ad)^2+(bc)^2+2abcd+(bd)^2\\ &= (ac-bd)^2+(ad+bc)^2\end{aligned}$$

şeklindedir.

3. METERYAL ve YÖNTEM

Kriptografik algoritmalar anahtar kullanma biçimine göre iki bölüme ayrılırlar;

1. Simetrik kriptografi (Tek anahtarlı şifreleme)
2. Asimetrik kriptografi (Çift anahtarlı şifreleme)

3.1. Simetrik Kriptografi

Tek anahtarlı şifreleme algoritmaları olarak da adlandırılan bu şifreleme sistemlerinde mesajı şifrelemek ve şifreli mesajın şifresini çözmek için aynı anahtar kullanılır. Elindeki mesajı şifrelemek isteyen kişi önce bir anahtar üretir. Bu anahtarla düz metni şifreler. Şifreli mesajı çözmek istediği zamanda aynı anahtarı kullanarak şifreyi çözer ve ilk metni elde eder.

3.2. Asimetrik Kriptografi

Çift anahtarlı şifreleme algoritmaları olarak da adlandırılan bu şifreleme sistemlerinde bir genel anahtar ve bu anahtarla arasında matematiksel bir ilişki bulunan bir özel anahtar üretilir. Herhangi bir düz metni şifrelemek için genel anahtar ve şifreli mesajı çözmek için ise özel anahtar kullanılır. Günümüzde yaygın olarak kullanılan bazı asimetrik algoritmalar şunlardır:

- "RSA" - Rivest-Shamir-Adleman, 1978
- "El-Gamal" - Taber ElGamal, 1985
- "Eliptik Eğri" - Miller-Koblitz, 1986

Günümüzde kullanılan modern kriptografik algoritmalar üç aşamadan oluşur;

1. Anahtar oluşturma (Key Generation)
2. Şifreleme (Encryption)
3. Şifre çözme (Decryption)

3.3. RSA Kriptosistemi

RSA açık anahtarlı ilk şifreleme metodu olup, hem mesaj şifreleme hem de elektronik imza amacıyla kullanılan algoritma, 1978 yılında Ron Rivest**,** Adi Shamir ve Len Adleman tarafından "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems" isimli makalede yayınlanmıştır. Güvenliği, tam sayıları çarpanlarına ayırmanın algoritmik zorluğuna dayanır. Bu metodun aşamaları aşağıdaki gibidir.

Anahtar Oluşturma

Şifreli bilgiyi almak isteyen taraf aşağıdaki işlemleri yaparak kendi anahtarlarını oluşturur;

- İki adet birbirinden bağımsız rastgele büyük p ve q asal sayıları yaklaşık olarak aynı büyüklükte olmak üzere üretir.
- $n = p.q$ ve $\phi(n) = (p-1).(q-1)$ değerlerini hesaplar.
- $(e, \phi(n)) = 1$ ve $1 < e < \phi(n)$ şartlarını sağlayan rastgele bir e sayısı seçer.
- Öklid Algoritmasını kullanarak $1 < d < \phi(n)$ ve $e.d \equiv 1\ (mod(\phi(n))$ şartlarını sağlayan *d* sayısı hesaplar.
- Bilgiyi alacak tarafın açık anahtarı $\boldsymbol{n}$ ve $\boldsymbol{e}$ sayıları ve gizli (özel) anahtarı ise $\boldsymbol{d}$ sayısı olur.

Şifreleme

- Şifreli bilgiyi almak isteyen taraf diğer tarafa kendi açık anahtarı olan $\boldsymbol{n}$ ve $\boldsymbol{e}$ sayılarını gönderir.
- Bilgiyi şifreleyecek olan taraf şifrelemek istediği mesajı $(\boldsymbol{M})$ $[0, n-1]$ aralığında bir tamsayıya dönüştürür ve

$$C \equiv M^e \pmod{n}$$

değerini hesaplayarak şifreli metin ($\boldsymbol{C}$)'yi elde eder.

- Şifreli bilgiyi gönderen taraf şifreli metin C' yi şifreli bilgiyi alacak tarafa gönderir.

Deşifreleme

- Bilgiyi alan taraf kendi özel anahtarını kullanılarak

$$M \equiv C^d (\text{mod } n)$$

değerini hesaplayarak düz metni elde eder.

Algoritmanın açıklaması aşağıda verilmiştir.

- $M^{\phi(n)} \equiv 1(mod\ n)$
- $e.d \equiv 1(mod\ \phi(n))$
- $e.d = k.\phi(n) + 1$
- $C^d \equiv M^{e.d} \equiv M^{k.\phi(n)+1} \equiv (M^{\phi(n)})^k.M \equiv M(\ mod\ n\ )$

Örnek 3.1: RSA şifrelemesine bir örnek aşağıda verilmiştir:

Anahtar oluşturma

$p = 13$ ve $q = 17$ olacak şekilde

$$n = p.q = 13.17 = 221$$

olsun.

$$\begin{aligned} \phi(n) &= (p-1).(q-1) \\ &= (13-1).(17-1) \\ &= 12.16 \\ &= 192 \end{aligned}$$

olur. $\big(e, \phi(n)\big) = 1$ olacak şekilde $e = 5$ olsun. $ed \equiv 1\ (mod\ \phi(n)\ )$ olacak şekilde d'yi tespit edelim. Öklid algoritması ile;

$$\begin{aligned} 192 &= 38.5 + 2 \\ 5 &= 2.2 + 1 \\ 2 &= 2.1 + 0 \end{aligned}$$

olur. Öklid algoritması tersten işletilerek d bulunur;

$$1 = 5 - 2.2$$

$$= 5 - 2.(192 - 38.5)$$
$$= 77.5 - 2.192$$

o halde $d = 77$ olur. $77.5 \equiv 1\ (mod\ 192)$ dir. Açık anahtar çifti $(e, n) = (5{,}221)$ ve gizli (özel) anahtar $d = 77$ olur.

Şifreleme

Şifrelenecek mesaj $M = 19$ olsun.

$$C \equiv M^e\ (mod\ n)$$
$$19^5 \equiv 15\ (mod\ 221)$$

olarak şifreli metin $C = 15$ olur.

Deşifreleme

Deşifreleme için $C^d \equiv x\ (mod\ n)$ denkliğindeki x tamsayısı bulunursa;

$$15^{77} \equiv x\ (mod\ 221)$$

$x = 19$ olarak bulunur ki bu da şifrelenen mesaj $M = 19$ dur.

3.4. RSA Kriptoanalizi

RSA'da anahtar oluşturmak için ilk adım iki asal sayı seçerek bunların çarpımından elde edilen yarı asal sayıyı kullanarak gerçekleştirilir. Elde edilen yarı asal sayı genel anahtarın bir parçasını oluşturur. Eğer bu yarı asal sayının çarpanları bulunabilirse özel anahtar kolayca bulunabilir.

RSA'nın kırılması N sayısının çarpanlarına ayrılmasıyla mümkündür. Fakat verilen her hangi iki asal sayıyı çarpmak kolay olmasına karşın, verilen her hangi bir yarı asal sayının çarpanlarını bulmak kolay değildir.

RSA kriptosisteminde şifreli metni kırabilmek için özel anahtar d'ye ihtiyaç vardır. d ise $(mod\ \phi(n))$'e göre açık anahtarın bir parçası olan e'nin aritmetik tersidir. Eğer açık anahtarın diğer bir parçasını oluşturan n yarı asal sayısı çarpanlarına ayrılabilirse, $n = p.q$ idi, $\phi(n)$ rahatlıkla hesaplanabilir. Daha sonra $e.d \equiv 1\ (mod\ \phi(n))$ denkliğinden özel anahtar d bulunur ve $M \equiv C^d\ (mod\ n)$ denkliği vasıtası ile orijinal metne ulaşılabilir.

Çarpanlara ayırma algoritmaları; Genel amaçlı çarpanlara ayırma algoritmaları(General Purpose Factorization Algoritms) ve Özel amaçlı çarpanlara ayırma algoritmaları (Special Purpose Factorization Algorithms) olmak üzere iki guruba ayrılmaktadır.

Genel amaçlı çarpanlara ayırma algoritmalarının çalışma zamanı verilen N yarı asal sayısının büyüklüğüne bağlıdır. Bu grupta yer alan ve günümüzde RSA'nın kriptanalizi için kullanılan algoritmalar şunlardır:

- "Quadratic sieve" - C. Pormanance, 1981
- "General Number Field Sieve" - A.K. Lenstra, 1983

Özel amaçlı çarpanlara ayırma algoritmaların çalışma zamanı ise verilen N sayısını oluşturan çarpanların belirli özelliklerine veya N sayısının bazı belirli özelliklerine bağlıdır. Bu nedenle RSA Kripto sisteminde asal sayılar seçilirken ve N sayısı oluşturulurken özel amaçlı algoritmalar göz önünde bulundurulması bir zorunluluktur. Bu nedenle özel amaçlı algoritmalar RSA da kullanılan yarı asal sayıyı oluştururken büyük öneme sahiptirler. Günümüzde bilinen bazı özel amaçlı algoritmalar şunlardır:

- Trial division (Basit Bölme Algoritması)
- Fermat
- Euler
- Pollard $p-1$
- Williams $p+1$
- Eliptic curve

Eliptik eğri çarpanlara ayırma algoritması (Eliptic curve) başlı başına bir çalışma sahasıdır. Eliptik eğriler üzerinde tanımlanan özel bir toplama işlemi marifetiyle algoritma geliştirilmiştir. Willams'ın $p+1$ çarpanlara ayırma algoritması ise Lucas dizilerinin bazı özelliklerinden faydalanılarak geliştirilmiştir. Çalışma yapısı $p-1$ algoritması ile benzerlikler gösterir. Bu tezde konu ile ilgili temel mantık oluşturması açısından yukarıda zikredilen ilk dört algoritma incelenmiştir.

4. ARAŞTIRMA BULGULARI

4.1. Özel Amaçlı Çarpanlara Ayırma Algoritmaları

Bu bölümde RSA'nın kriptoanalizi için kullanılan özel amaçlı çarpanlara ayırma algoritmalarından bazıları detaylı olarak incelenmiştir.

4.1.1. Basit bölme çarpanlara ayırma algoritması

Teorem 2.12'den N bileşik sayısının karekökünden küçük bir asal çarpanı olduğunu biliyoruz. En basit özel amaçlı çarpanlara ayırma algoritması olan basit bölme (trial division-basit bölme algoritması) olarak adlandırılan bu yöntemde eğer N sayısını oluşturan asal çarpanlardan biri çok küçük ise bu çarpan N'nin 3'ten başlanarak sırası ile 3,5,7,… şeklinde pozitif tek sayılara bölünüp bölünmediğini kontrol edilerek bulunabilir. Bundan dolayı N sayısının asal çarpanları yeterince büyük seçilmelidir. Algoritmanın genel yapısı aşağıda verilmiştir.

Algoritma 4.1. Basit Bölme Çarpanlara Ayırma Algoritması

GİRDİ : p ve q asallar olmak üzere $N = pq$ şeklindeki N sayısı

ÇIKTI : p ile q asalları

Adım 1: Başla

Adım 2: N sayısını oku

Adım 3: $i \leftarrow 3$

Adım 4: Döngüyü Başlat

Adım 5: Eğer ($N \bmod i = 0$) ise $i, \frac{N}{i}$ sayılarını yaz ve Adım 8'e git.

Adım 6: $i \leftarrow i + 2$

Adım 7: Adım 5'e git.

Adım 8: Döngüyü bitir.

Adım 9: Bitir.

RSA da kullanılacak olan N anahtarı oluşturulurken bu sayının basit bölme algoritmasına karşı dayanıklı olması için asal çarpanlarından her birinin çok küçük olmaması gerekir. Yani her iki asal çarpanda yeterince büyük seçilmelidir.

Örnek 4.1: $N = 1921$ sayısının çarpanlarını Basit Bölme Algortitmasını kullanarak hesaplayalım. Sırası ile $i = 3,5,7,\ldots$ değerlerini $\lfloor\sqrt{N}\rfloor = 44$'e kadar mod i de 0 bulana dek hesaplanırsa;

$$1921 \equiv 1(mod\ 3)$$

$$1921 \equiv 1(mod\ 5)$$

$$1921 \equiv 3(mod\ 7)$$

$$1921 \equiv 4(mod\ 9)$$

$$1921 \equiv 7(mod\ 11)$$

$$1921 \equiv 10(mod\ 13)$$

$$1921 \equiv 1(mod\ 15)$$

$$1921 \equiv 0(mod\ 17)$$

olduğundan 17 N'nin bir çarpanıdır. Böylece diğer çarpanı ise 113 bulunur. $N = 1921 = 17.113$ dir.

4.1.2. Fermat çarpanlara ayırma algoritması

Fermat'ın çarpanlara ayırmak için kullandığı yöntem iki kare farkı elde etmeye dayanır. a ve b tamsayılar ve p, q asal sayılar olmak üzere $N = pq$ sayısı

$$N = a^2 - b^2 \tag{4.1}$$

denklemini sağlayan a ve b tamsayıları elde edildiğinde, N sayısını veren çarpanlar $(a + b)(a - b)$ şeklinde bulunmuş olur. Basitçe algoritmanın elde edilişi şu şekildedir:

(4.1) denkleminden

$$a^2 = N + b^2$$

$$a = \sqrt{N + b^2} \tag{4.2}$$

yazılabilir.

(4.2) denkleminde sırası ile $b = 1,2,3,\ldots$ değerleri için a'nın tamsayı değerine ulaşıldığında elde edilen b ve a için

$$p = a + b \text{ ve } q = a - b \tag{4.3}$$

hesaplanır ve N sayısının asal çarpanları bulunmuş olur.

(4.3) denkleminden

$$p - q = 2b \text{ ve } b = \frac{p-q}{2}$$

olup eğer $p - q$ değeri çok küçük ise b değeri de o kadar küçük olacağından algoritmanın p ile q sayılarını bulma süresi $p - q$ ile doğru orantılıdır.

Algoritmanın genel yapısı aşağıda verilmiştir.

Algoritma 4.2. Fermat Çarpanlara Ayırma Algoritması

GİRDİ : p ve q asallar olmak üzere $N = pq$ şeklindeki N sayısı

ÇIKTI : p ile q asalları

Adım 1: Başla

Adım 2: N sayısını oku

Adım 3: $b \leftarrow 1$

Adım 4: Döngüyü Başlat

Adım 5: $a = \sqrt{N + b^2}$ değerini hesapla

Adım 6: Eğer a tamsayı ise $a + b$ ve $a - b$ değerlerini yaz ve Adım 9 ya git.

Adım 7: $b \leftarrow b + 1$

Adım 8: Adım 5'e git.

Adım 9: Döngüyü sonlandır.

Adım 10: Bitir.

Bu yöntem, N sayısının çarpanları arasındaki fark çok küçük olduğunda kullanışlıdır. Bu nedenle RSA da kullanılacak olan N anahtarı oluşturulurken birbirine çok yakın olmayan p ve q asalları seçilmelidir.

Örnek 4.2: $N = 85$ sayısının çarpanlarını Fermat algortitması kullanarak hesaplayalım. Sırası ile $b = 1,2,3,\ldots$ değerlerini kullanarak $a = \sqrt{85 + b^2}$ tamsayı değerlerini bulana kadar işlem tekrarlanırsa;

- $b = 1$ için $a = \sqrt{86}$
- $b = 2$ için $a = \sqrt{89}$
- $b = 3$ için $a = \sqrt{94}$
- $b = 4$ için $a = \sqrt{101}$
- $b = 5$ için $a = \sqrt{110}$
- $b = 6$ için $a = \sqrt{121} = 11$

olup bu son adımda a'nın değeri tamsayı olduğundan

$$p = a + b = 17$$
$$q = a - b = 5$$

olarak elde edilmiş olur.

4.1.3. Euler çarpanlara ayırma algoritması

Bu yöntemde a, b, c, d tam sayılar olmak üzere N tamsayısı hem

$$N = a^2 + b^2 \tag{4.4}$$

hem de

$$N = c^2 + d^2 \tag{4.5}$$

olarak yazılabiliyorsa ve bu a, b, c, d sayıları bir algoritma yardımı ile hesaplandığında aşağıdaki işlemler vasıtası ile p ile q asalları elde edilebilir.

Eşitlik (4.4) ve (4.5) den

$$N = a^2 + b^2 = c^2 + d^2$$

olup

$$a^2 - c^2 = d^2 - b^2$$

$$(a-c).(a+c) = (d-b)(d+b) \tag{4.6}$$

yazılabilir.

Ayrıca,

$$(a-c, d-b) = k$$
$$(a+c, d+b) = l$$

olsun, en büyük ortak bölen tanımı gereğince

$$\begin{matrix} a-c = kx \\ d-b = ky \end{matrix} \quad (x,y) = 1 \tag{4.7}$$

$$\begin{matrix} a+c = lx' \\ d+b = ly' \end{matrix} \quad (x',y') = 1 \tag{4.8}$$

yazılır.

Bu (4.7) ve (4.8) değerleri (4.6) denkleminde yerlerine yazılırsa

$$kx.lx' = ky.ly'$$
$$xx' = yy'$$

elde edilir.

$(x,y) = 1$ ve Teorem 2.32 gereğince $x|y'$,

$(x',y') = 1$ ve Teorem 2.32 gereğince $y'|x$ olup dolayısıyla $x = y'$ dir.

Benzer düşünceyle $y = x'$ elde edilir. Bu değerler (4.8) de yazılırsa

$$a + c = ly$$
$$d + b = lx \tag{4.9}$$

elde edilir.

Son olarak (4.7) ve (4.9) eşitlikleri kullanılarak N sayısının çarpanları aşağıdaki işlemler yardımı ile bulunabilir.

(4.5) formunda verilen N sayısı için;

$$4N = (2c)^2 + (2d)^2$$

yazılabilir.

Buradan

$$4N = (a + c - (a - c))^2 + (d + b + (d - b))^2$$

$$4N = (ly - kx)^2 + (lx + ky)^2 \tag{4.10}$$

ikinci bölümde verilen (2.1) özdeşliği kullanılarak

$$(kx - ly)^2 + (ky + lx)^2 = (k^2 + l^2)(x^2 + y^2) \tag{4.11}$$

yazılabilir.

Artık (4.11) eşitliği (4.10) de kullanılırsa,

$$4N = (k^2 + l^2)(x^2 + y^2)$$

elde edilir.

Buradan N sayısının çarpanları kolayca hesaplanabilir.

Bu yöntem, N sayısı hem $N = a^2 + b^2$hem de $N = c^2 + d^2$ olarak yazılabiliyorsa kullanışlıdır.

Örnek 4.3: $n = 2501$ olsun.

$2501 = 50^2 + 1^2 = 49^2 + 10^2$.

Buradan

$$a = 50, \quad b = 1,$$
$$c = 49, \quad d = 10.$$

değerleri için

$$k = (a - c, d - b) = (1,9) = 1$$
$$l = (a + c, d + b) = (99,11) = 11$$
$$x = \frac{a - c}{k} = 1, \qquad y = \frac{d - b}{k} = 9$$

Buradan,

$$(1^2 + 11^2)(1^2 + 9^2) = 122.82 = 4.61.41$$

olup $N = 61.41$ elde edilir.

4.1.4. Pollard $p - 1$ çarpanlara ayırma algoritması

Özel amaçlı çarpanlara ayırma yöntemlerinden bir diğeride 1974 yılında J. M. Pollard tarafından "*Theorems of factorization and primality testing*" isimli makalesinde yayınlanmış olup kısaca $p - 1$ algoritması olarak bilinir. Algoritmanın teorik alt yapısı şu şekildedir.

p ve q farklı asallar olmak üzere $N = pq$ sayısı için $(a, N) = 1$ olacak şekilde bir a tamsayısı seçelim.

Fermat'ın teoreminden

$$a^{p-1} \equiv 1 \pmod{p} \tag{4.12}$$

dir.

(4.12) denkliğin her iki tarafının m. kuvveti alınırsa

$$a^{(p-1)m} \equiv 1 \pmod{p} \tag{4.13}$$

elde edilir.

$$p - 1 = \prod_{i=1}^{k} \alpha_i^{\beta_i} = {\alpha_1}^{\beta_1}.{\alpha_2}^{\beta_2} \dots {\alpha_k}^{\beta_k}$$

olsun ve ${\alpha_k}^{\beta_k} = B$ alalım o zaman $(p - 1)|B!$ olup B değeri (4.13) de kullanılırsa

$$a^{B!} \equiv 1 \pmod{p}$$

denkliği elde edilir. Buradan da

$$p|(a^{B!} - 1) \tag{4.14}$$

olur.

Ayrıca, bölme algoritmasından

$$a^{B!} - 1 = N.s + r \tag{4.15}$$

olacak şekilde s ve r tamsayıları vardır. Buradan

$$r = (a^{B!} - 1) - N.s$$

dir.

$p|N$ ve (4.14) gözönüne alınırsa Teorem 2.2 (vii) gereğince

$$p|r \tag{4.16}$$

olduğu açıktır.

Ayrıca, (4.15) eşitliğinden

$$(a^{B!} - 1) - r = N.s$$

elde edilir.

Tanım 2.1'den

$$N|[(a^{B!} - 1) - r]$$

yazılır ve Tanım 2.24'den

$$r \equiv (a^{B!} - 1) \bmod N \tag{4.17}$$

elde edilir.

son olarak, (4.16) ve (4.17) göz önüne alındığında

$$p|[(a^{B!} - 1) \bmod N]$$

olup

$$\Big(\big((a^{B!} - 1) \bmod N\big), N\Big) = p$$

sonucu elde edilir.

Bu son eşitlik bize algoritmanın oluşturulması için en önemli yaklaşımı vermektedir.

Algoritmanın genel yapısı aşağıda verilmiştir.

Algoritma 4.3. $p - 1$ Çarpanlara Ayırma Algoritması

GİRDİ : p ve q asallar olmak üzere $N = pq$ şeklindeki N sayısı

ÇIKTI : p ile q asalları

Adım 1: Başla

Adım 2: N sayısını oku

Adım 3: $a \leftarrow 2, j \leftarrow 2$

Adım 4: Döngüyü Başlat

Adım 5: $a \leftarrow a^j \ (mod\ N)$ değerini hesapla

Adım 6: $d = (a-1, N)$ değerini hesapla

Adım 7: Eğer $d \neq 1$ ise $d, \frac{N}{d}$ sayılarını yaz ve Adım 10'e git.

Adım 8: $j \leftarrow j + 1$

Adım 9: Adım 5'e git.

Adım 10: Döngüyü sonlandır.

Adım 11: Bitir.

Bu yöntemde, şayet p asalı için $p-1$ sayısının en büyük asal çarpanı yeterince küçük bir değere sahipse, bu asalla oluşturulan N bileşik sayının çarpanı Algoritma 4.3 ile kolayca hesaplanabilir. Yukarıda verilen algoritma, konunun mantığı kolayca kavransın diye, basit düzeyde kurulan bir algoritmadır. Pollard tarafından verilen orjinal algoritma daha hızlı sonuca varmayı hedefleyen bir algoritma olup iki aşamalıdır. Orjinal algoritmaya Menezes (1996) dan ulaşılabilir.

Bu nedenle RSA da kullanılacak olan N anahtarı oluşturulurken yukarıda belirtilen özellikleri sağlamayan p ve q asalları seçilmelidir.

Örnek 4.4: $N = 18923$ olsun. $(a, N) = 1$ şartını sağlaması için $a = 2$ alınsın.

$a^{2!} = 2^2 = 4$ ve $2^2 \equiv 4 (\text{mod } 18923)$ olup

$$((a^{2!} - 1) mod N, N) = (3, 18923) = 1$$

dir, dolayısıyla devam edilmesi gerekir.

$a^{3!} = (a^{2!})^3 = 4^3 = 64 \equiv 64 \text{ (mod } 18923)$ olup

$$((a^{3!} - 1) mod N, N) = (63, 18923) = 1$$

dir, dolayısıyla devam edilmesi gerekir.

$a^{4!} = (a^{3!})^4 = 64^4 \equiv 11438 \text{ (mod } 18923)$ olup

$$((a^{4!} - 1) mod N, N) = (11437, 18923) = 1$$

dir, dolayısıyla devam edilmesi gerekir.

$a^{5!} = (a^{4!})^5 = 11438^5 \equiv 17909 \text{ (mod } 18923)$ olup

$$((a^{5!}-1) mod N, N) = (17908, 18923) = 1$$

dir, dolayısıyla devam edilmesi gerekir.

$a^{6!} = (a^{5!})^6 = 17909^6 \equiv 16066 \pmod{18923}$ olup

$$((a^{6!}-1) mod N, N) = (16065, 18923) = 1$$

dir, dolayısıyla devam edilmesi gerekir.

$a^{7!} = (a^{6!})^7 = 16066^7 \equiv 11431 \pmod{18923}$ olup

$$((a^{7!}-1) mod N, N) = (11430, 18923) = 127$$

bulunur ki bu da N sayısının asal çarpanlarından biri olur. Diğer çarpan ise $18923/127 = 149$ yapar. Sonuç olarak $18923 = 127.149$ elde edilmiş olur.

RSA kriptosisteminin kırılabilmesi için, tamsayıları çarpanlarına ayırabilmek adına yapılan tüm çalışmalar büyük önem arz etmektedir. Bu çalışmalardan biri de, özel amaçlı çarpanlara ayırma algoritmalarından biri olan Williams'ın $p+1$ çarpanlara ayırma algoritmasıdır (Ayrıntılı bilgi için bakınız: Williams, 1982). Tezde bu algoritma ayrıntılı olarak incelenmemiştir ancak ileriki sayfalarda bahsi geçecek olan Güçlü Asal Sayı Algoritmasında kullanılacağı için hakkında kısaca açıklama yapmakta fayda vardır:

RSA'da kullanılacak olan p asalı Pollard'ın algoritmasına karşı dayanıklı olması için $p-1$ tamsayısının en büyük asal çarpanı yeterince büyük seçilmelidir. Yani Pollard'ın algoritmasının sonuca ulaşma süresi $p-1$ tamsayısının en büyük asal çarpanı ile doğru orantılıdır. Williams'ın $p+1$ çarpanlara ayırma algoritması da Lucas sayılarının ve fonksiyonlarının bazı özelliklerini kullanarak, $p-1$ algoritmasına benzer biçimde sayıyı çarpanlarına ayırır. Bu algoritmanın sonuca ulaşma süresi ise $p+1$ tamsayısının en büyük asal çarpanı ile doğru orantılıdır. Yani RSA'da kullanılacak olan p asalı Williams'ın algoritmasına karşı dayanıklı olması için $p+1$ tamsayısının en büyük asal çarpanı yeterince büyük seçilmelidir.

Tezde bu kısma kadar RSA'ya karşı, saldırı niteliğinde olan özel amaçlı çarpanlara ayırma algoritmalarından bazıları incelendi. Peki bu saldırılara karşı dayanıklı asal sayılar üretilebilir mi? Aşağıda bu soruya cevap olabilecek Gordon'un güçlü asal sayı üretimi yapan algoritması verilmiştir.

4.2. Güçlü Asal Sayı Algoritması

Tanım 4.5: (Güçlü Asal Sayı Algoritması) r, t, s asal sayılar olmak üzere;

i. $p-1$ sayısının en büyük asal çarpanı r
ii. $r-1$ sayısının en büyük asal çarpanı t
iii. $p+1$ sayısının en büyük asal çarpanı s

olacak şekilde üretilen p asal sayısına *güçlü asal sayı* denir (Gordon, 1984).

Algoritma 4.4. Güçlü Asal Sayı için Gordon Algoritması

GİRDİ**:** s ile t asal sayılar
ÇIKTI: Güçlü asal sayı p
Adım 1: Herhangi bir i sayısı seçilir.
Adım 2: $i = i_0, i_0+1, i_0+2, \ldots$ olamk üzere $2it+1$ dizisindeki ilk asal sayı bulunur. Bulunan bu sayı r olarak seçilir.
Adım 3: $p_0 = 2(s^{r-2} mod\ r)s - 1$ değeri hesaplanır.
Adım 4: Herhangi bir j sayısı seçilir. $j = j_0, j_0+1, j_0+2, \ldots$ olmak üzere $p_0 + 2jrs$ dizisindeki ilk asal sayı bulunur.
Adım 5: Bulunan bu sayı istenilen $p = p_0 + 2jrs$ asal sayısıdır.

Gordon Algoritması ile üretilen p asal sayısının güçlü asal sayı olduğu aşağıdaki gibi görülebilir:

$p \neq s$ olduğunu varsayılırsa;

$$s^{r-1} \equiv 1\ (mod\ r) \tag{4.18}$$

yazılır.

r ile s sayıları asal sayılar olduğundan Fermat teoreminden dolayı (4.18) denkliğinin doğru olduğunu görülebilir. Bu nedenle,

$$p_0 = 2(s^{r-2} \ mod \ r \ )s - 1$$

olur.

$$p_0 \equiv 1 \ (mod \ r) \ \text{ ve } \ p_0 \equiv -1 \ (mod \ s)$$

olur. Sonuç olarak;

- $p - 1 = p_0 + 2jrs - 1 \equiv 0 \ (mod \ r)$ olup, $r|(p-1)$ yazılır.
- $r - 1 = 2it \equiv 0 \ (mod \ t)$ olup $t|(r-1)$ yazılır.
- $p + 1 = p_0 + 2jrs + 1 \equiv 0 \ (mod \ s)$ olup, $s|(p+1)$ yazılır.

Bu nedenle,

- $p - 1$ sayısının bir asal çarpanı r,
- $r - 1$ sayısının bir asal çarpanının t,
- $p + 1$ sayısının bir asal çarpanı s

olduğu görülebilir. (Okumuş, 2012).

Örnek 4.6: $t = 3$ ve $s = 2$ olsun.

Adım 1: $i = 4$ olsun.

Adım 2: $r = 2it + 1$ idi.

$i_0 = 4$ için $r_0 = 25$

$i_1 = i_0 + 1 = 5$ için $r_1 = 31$ dizideki ilk asal olduğundan $r = 31$ olur.

Adım 3: $p_0 = 2(s^{r-2} mod \ r \ )s - 1$ idi.

$p_0 = 2.(2^{29} mod \ 31 \ ).2 - 1 = 63$ olur.

Adım 4: $j = j_0, \ j_0 + 1, \ j_0 + 2, \ldots$ olmak üzere $j_0 = 1$ alınarak $p_0 + 2jrs$ dizisindeki ilk asal,

$j_0 = 1$ için $p_0 + 2jrs = 63 + 2.1.31.2 = 187$

$j_1 = 2$ için $p_0 + 2jrs = 63 + 2.2.31.2 = 311$

olarak bulunur.

Adım 5: O halde aranılan güçlü asal sayı $p = 311$ olarak bulunur.

Burada;

$p - 1 = 310$'nun bir asal çarpanı $r = 31$,

$r - 1 = 30$'un bir asal çarpanı $t = 3$,

$p + 1 = 312$'nin bir asal çarpanı $s = 2$

dir.

5. SONUÇ ve ÖNERİLER

Bu tezde RSA'nın kriptoanalizi için geliştirilen, özel amaçlı çarpanlara algoritmalarından olan dört farklı metot (Basit Bölme Çarpanlara Ayırma Algoritması, Fermat Çarpanlara Ayırma Algoritması, Euler Çarpanlara Ayırma Algoritması, Pollard $p-1$ Çarpanlara Ayırma Algoritması) ayrıntılı olarak incelenmiş, bu metotlarla ilgili çeşitli örnekler çözülmüştür. RSA'nın güvenliği açısından şifrelemede kullanılacak olan anahtar seçiminde bu algoritmaların göz önüne alınması gerekir. Bu tip çarpanlara ayırma algoritmalarına dayanıklı asal sayılar bulup şifrelemede kullanmak, şifreli mesajın çözülmesini-kırılmasını zorlaştıracaktır. Nitekim dayanıklı-güçlü asal sayı üretimi ile ilgili olan Gordon'un Güçlü Asal Sayı Algoritması tezin son kısmında verilmiştir. Böylece RSA'ya saldırı niteliğinde olan bazı çarpanlara ayırma algoritmalarına karşı savunma niteliğinde olan bir güçlü asal sayı üretim algoritması da okuyucuya sunulmuş olmuştur.

Algoritmaların matematik alt yapıları, lisansını matematik dışında yapmış araştırmacılar da düşünülerek ayrıntılı bir şekilde verilmeye çalışılmış, okuyucunun farklı bir kaynağa başvurmadan tüm sorularının cevaplarını tezin içinde bulması amaçlanmıştır.

KAYNAKLAR

Şahin, M. "Kriptoloji, RSA Kriptosistemi",

http://acikders.ankara.edu.tr/course/view.php?id=26

Son Erişim Tarihi: 02.07.2018

Altındiş, H. (2005) "Sayılar teorisi ve uygulamaları", 2. Baskı, ***Erciyes Üniversitesi Fen Edebiyat Fakültesi Matematik Bölümü***, Kayseri, 1-141.

Arıkan, A. ve Halıcıoğlu, S. (2015) "Cebire Giriş", ***Palme Yayıncılık***, Ankara.

Arıkan, A. ve Halıcıoğlu, S. (2013) "Soyut Matematik", ***Palme Yayıncılık***, Ankara.

Asar, A., Arıkan, A. ve Aynur, A. (2009) "Cebir", ***Eflatun Yayınevi***, Ankara.

Aybak, L. (2010) "Sayı Cismi Çarpanlara Ayırma Yöntemi", Yüksek Lisans Tezi, ***Ankara Üniversitesi Fen Bilimleri Enstitüsü***, Ankara.

Balcı, M. (1999) "Analiz", Cilt 1, ***Balcı Yayınları***, Ankara.

Balcı, M. (1997) "Analiz", Cilt 2, ***Balcı Yayınları***, Ankara.

Bayraktar, M. (2010) "Analiz", ***Nobel yayın Dağıtım***, Ankara.

Bayraktar, M. (1988) "Soyut Cebir ve Sayılar Teorisi", ***Atatürk Üniversitesi Basımevi***, Erzurum.

Buluş, H. N. (2006) "Temel Şifreleme Algoritmaları ve Kriptanalizlerinin İncelenmesi", Yüksek Lisans Tezi, ***Trakya Üniversitesi Fen Bilimleri Enstitüsü,*** Edirne.

Çallıalp, F. (2001) "Örneklerle Soyut Cebir", ***Birsen Yayınevi***, İstanbul.

Diffie, W., and Hellman, M. (1976) New directions in cryptography. ***IEEE Trans. Inform. Theory*** IT-22, 644-654.

ElGamal, T. (1985) "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", ***IEEE Transactions on Information Theory,*** 31 (4): 469–472.

Gordon, J. A. (1984) "Strong RSA Keys", ***Electronics Lett.*** 20 (12), 514-516.

Hassanpour, A. A. (2015) "Asal Sayıların Şifreleme Teorisindeki Uygulamaları", Yüksek Lisans Tezi, ***Atatürk Üniversitesi Fen Bilimleri Enstitüsü***, Erzurum.

Irmak, H. (2008) "Soyut Matematik", ***Pegem Akademi***, Ankara.

Ishmukhametov, Sh. T. And Sharifullina, F.F. (2013), "On Distribution of Semiprime Numbers", ***Kazan (Volga Region) Federal University,*** ul. Kremlyovskoya18, Kazan, 420008 Russia.

Koblitz, N. (1994) "A course in Number theory and Cryptography", ***Springer Verlag***.

Külen, F. (2013) "Kriptolojide Bazı Şifreleme Yöntemlerinde Cebirsel Yaklaşımlar", Yüsek Lisans Tezi, ***Gaziosmanpaşa Üniversitesi Fen Bilimleri Enstitüsü***, Tokat.

Menezes, A. J. , Oorschot, P.C.V. and Vanstone, S.A. (1996) "Handbook of Applied Cryptography", ***CRC Press***.

Mert, C. ve Şeker, S. E. (2014) "RSA Şifreleme Sistemine Karşı Yeni Bir Çarpanlara Ayırma Saldırısı", ***EÜFBED-Fen Bilimleri Enstitüsü Dergisi,*** Cilt-Sayı: 7-1 Sayfa:105-132.

Nuriyeva, F. (2010) "Çarpanlara Ayırma Algoritmaları Üzerine", Yüksek Lisans Tezi, ***Ege Üniversitesi Fen Bilimleri Enstitüsü,*** İzmir.

Okumuş, İ. (2012) "RSA Kriptositeminin Hızını Etkileyen Faktörler", Doktora Tezi, ***Atatürk Üniversitesi Fen Bilimleri Enstitüsü,*** Erzurum.

Pamukçu, B. (2006) "Kriptografi için Faktorizasyon Metodları", Yüksek Lisans Tezi, ***Fatih Üniversitesi Fen Bilimleri Enstitüsü,*** İstanbul.

Pollard, J. M. (1974) "Theorems of factorization and primality testing", ***Proceedings of the Cambridge Philosophical Society,*** 76 (3): 521–528.

Rivest, R., Shamir, A. and Adleman, L. (1978) "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", ***Communications of the ACM***, v. 21(2): 120-126.

Song, Y. Y. (2008) "Cryptanalytic Attacks on RSA", **Springer Science + Business Media,** LCC. New York, USA.

Taşçı, D. (2011) "Lineer Cebir", ***Öziş Matbaacılık***, 4. Baskı, Ankara.

Taşçı, D. (2010) "Soyut Cebir", ***Öziş Matbaacılık***, 2. Baskı, Ankara.

Williams, H. C. (1982) "A $p+1$ Method of Factoring. Math. Comp." vol:39, no:159, 225-234.

Yücelen, A. M. (2011) "Kriptolojide Eliptik Eğri Algoritması", Yüksek Lisans Tezi, ***Dicle Üniversitesi Fen Bilimleri Enstitüsü,*** Diyarbakır.

ÖZGEÇMİŞ

Nurullah BÜTÜN, 1986 Soma (MANİSA) doğumludur. İlk ve orta öğrenimini Samsun'un Terme ilçesinde tamamladı. 2005 yılında başladığı Sakarya Üniversitesi Fen-Edebiyat Fakültesi Matematik Bölümünü 2009 senesinde bitirdi. 2009-2010 yıllarında tamamladığı askerlik görevi akabinde 2011 senesinde Ondokuz Mayıs Üniversitesinde Pedogojik Formasyon eğitimini tezsiz yüksek lisans programını bitirerek tamamladı. Aynı sene Gümüşhane-Kelkit Anadolu Sağlık Meslek Lisesine matematik öğretmeni olarak atanmış, 2017 senesinde ise Kelkit 15 Temmuz Şehitler Anadolu Lisesine tayin olmuştur. Evli ve bir çocuk babasıdır.