Avrupa Bilim ve Teknoloji Dergisi
Özel Sayı, S. 284-291, Ekim 2019

Derleme Makale

www.ejosat.com ISSN:2148-2683

European Journal of Science and Technology
Special Issue, pp. 284-291, October 2019

Review Article

Şifreleme Yöntemleri ve RSA Algoritması Üzerine Bir İnceleme

Ayşe Beşkirli[1*], Durmuş Özdemir[2], Mehmet Beşkirli[3]

[1] Kütahya Dumlupınar Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Kütahya, Türkiye (ORCID: 0000-0002-8694-8438)
[2] Kütahya Dumlupınar Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Kütahya, Türkiye (ORCID: 0000-0002-9543-4076)
[3] Şırnak Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Şırnak, Türkiye (ORCID: 0000-0002-4842-3817)

(This publication has been presented orally at HORA congress.)

(First received 1 August 2019 and in final form 25 October 2019)

(**DOI:** 10.31590/ejosat.638090)

ATIF/REFERENCE: Beşkirli, A., Özdemir, D. & Beşkirli, M. (2019). Şifreleme Yöntemleri ve RSA Algoritması Üzerine Bir İnceleme. *European Journal of Science and Technology*, (Special Issue), 284-291.

Öz

Günümüzde, bilişim teknolojilerinin gelişmesiyle birlikte haberleşme ve bilgi güvenliğinin sağlanması için şifrelemenin önemi giderek artmaktadır. Özellikle internet teknolojisinin gelişmesiyle birlikte veri güvenliğinin sağlanması için birçok şifreleme algoritmaları kullanılmaktadır. Şifreleme algoritmaları simetrik ve asimetrik olmak üzere iki başlık altında incelenmektedir. Bu çalışmada ise simetrik ve asimetrik şifreleme algoritmalarının genel özelliklerine yer vermekle birlikte literatürde önemli bir yere sahip asimetrik şifreleme algoritmalarından biri olan RSA algoritması incelenerek RSA algoritmasının şifreleme yöntemleri üzerindeki etkisi analiz edilmiştir. RSA algoritmasının yapısı, genel özellikleri, avantajı ve dezavantajı hakkında bilgilere yer verilmiştir.

Anahtar Kelimeler: Asimetrik şifreleme algoritmaları, RSA algoritması, Kriptografi.

A Review on Encryption Methods and RSA Algorithm

Abstract

Nowadays, with the development of information technologies, the importance of encryption for communication and information security is gradually increasing. Especially internet technology has been developed and many encryption algorithms have been used to provide data security. Encryption algorithms are examined under two headings as symmetric and asymmetric. In this study, the general properties of symmetric and asymmetric encryption algorithms are given and the effect of the RSA algorithm on the encryption methods is analyzed by examining the RSA algorithm which is one of the asymmetric encryption algorithms in the literature. The structure, general properties, advantages and disadvantages of the RSA algorithm are given.

Keywords: Asymmetric encryption algorithms, RSA algorithm, cryptography.

[*] Sorumlu Yazar: Kütahya Dumlupınar Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Kütahya, Türkiye, ORCID: 0000-0002-8694-8438, ayse.beskirli@ogr.dpu.edu.tr

1. Giriş

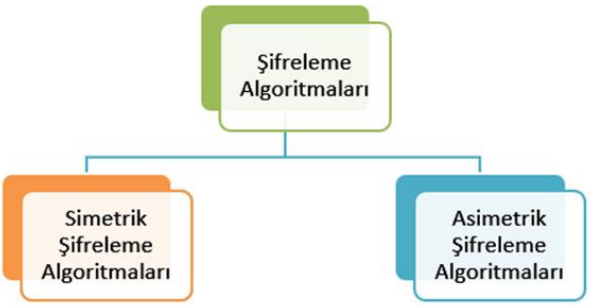
Günümüzde verilerin iletilmesinin yanı sıra verilerin güvenli bir şekilde iletilmesi için iletim esnasındaki gizlilik çok önem taşımaktadır. İletilmek istenen bilgilerin bir başkası tarafından kolayca erişilmemesi için şifreleme yöntemlerine başvurulmaktadır. Bu şifreleme yöntemine kriptoloji denilmektedir. Kriptoloji, cruptos (gizli) ve logos (bilim) kelimelerinin birleşiminden oluşmuştur ve kelime anlamı olarak gizleme bilimi manasına gelmektedir (Yerlikaya, 2006). Kriptolojide orijinal metne, düz metin (plaintext), şifrelenmiş metne ise şifreli metin (ciphertext) denilmektedir (Kodaz ve Botsali, 2010). Düz metnin içeriğini saklamak için şifreleme (encryption) işleminin yapılması gerekmektedir (Fındık, 2004). Bu sayede metnin içindeki bilgi başkalarının anlayamayacağı hale gelmektedir. Şifrelenmiş metni okuyacak olan kişilerin elinde şifreyi çözecek anahtar bulunmalıdır. Bu anahtar sayesinde şifrelenmiş olan metin düz metne çevrilmektedir. Bu işleme şifre çözme (decryption) işlemi denilmektedir (Fındık, 2004). Şekil 1'de şifreleme ve şifre çözme adımları gösterilmiştir.

Şekil 1. Şifreleme ve Şifre Çözme İşlemleri

Kriptoloji, hem şifre bilimini (kriptografi) hem de şifre analizini (kripto analiz) kapsayan matematiksel tekniklerle ifade edilen bir bilim dalıdır. Kriptografinin temel amacında veri güvenliğinin sağlanması için açık verileri gizli verilere dönüştürme işleminin yapılması vardır. Gizlilik, kimlik doğrulama, güvenilirlik, bütünlük gibi bilgi güvenliği gerektiren konular kriptografinin matematiksel yöntemler üzerine çalışılmış önemli konularındandır (Fındık, 2004; Kodaz ve Botsali, 2010; Yerlikaya, 2006). Kısaca kriptografi, anlaşılır bir metni anlaşılmaz hale getirme, anlaşılmaz bir metni ise anlaşılır hale getirme işlemidir.

2. Şifreleme Algoritmaları

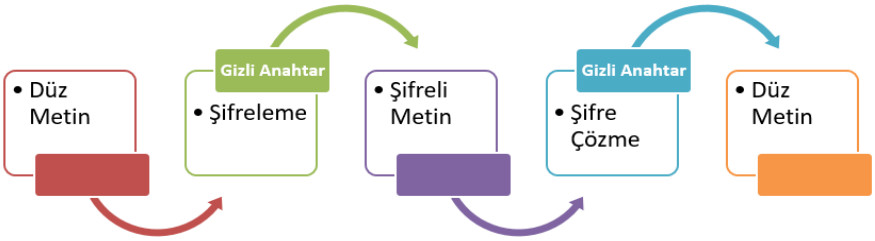
Şifreleme ve şifre çözme işlemleri için çeşitli algoritmalar kullanılmaktadır. Bu algoritmalara kriptografik algoritmalar denilmektedir (Fındık, 2004). Kriptografik algoritmalar, şifreleme ve şifre çözme işlemlerini anahtar kullanarak yapmaktadır. Şifreli metin sadece metin şifreleme işlemi için kullanılan anahtar ile çözülebilmektedir (Okumuş, 2012). Anahtar kullanan şifreleme algoritmaları simetrik şifreleme (gizli anahtar şifreleme) ve asimetrik şifreleme (açık anahtar şifreleme) algoritmaları olmak üzere Şekil 2'deki gibi ikiye ayrılmaktadır.



Şekil 2. Şifreleme Algoritmaları

2.1. Simetrik Şifreleme Algoritmaları

Simetrik şifreleme, gizli anahtarlı şifreleme olarak adlandırılmaktadır. Simetrik şifreleme algoritmalarında bilginin şifrelenmesi ve şifrelenmiş bilginin çözülmesi işlemi aynı anahtar kullanılarak gerçekleştirilmektedir (Yeşilbaş, 2016). Bu anahtar sadece şifreleme işlemi ve şifre çözme işlemini yapacak olan kişilerde bulunmaktadır. Simetrik şifreleme algoritması açık metni ile gizli anahtarı veri girişi olarak alıp, çıktı olarak şifreli metni üretir. Düz metne erişmek ise sadece gizli anahtarın bilinmesiyle mümkün olmaktadır. Yani şifreli metni düz metne çevirme işlemi gizli anahtar kullanarak gerçekleştirilmektedir (Okumuş, 2012). Simetrik şifreleme algoritması diyagramı Şekil 3'te verilmiştir.



Şekil 3. Simetrik Şifreleme Algoritması Diyagramı

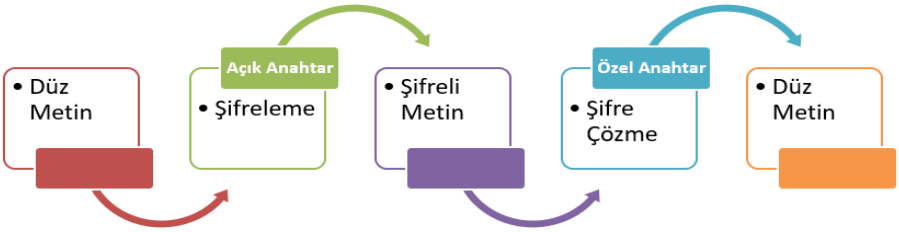
Literatürde birçok simetrik algoritma çeşitleri bulunmaktadır. Bu algoritmalardan bazılarının adı, geliştiricisi ve geliştirme tarih bilgilerine Tablo 1'de yer verilmiştir (Kodaz ve Botsali, 2010).

Tablo 1. Simetrik Şifreleme Algoritmaları

Algoritmanın Adı	Geliştiren	Tarihi
LUCİFER	IBM (ABD)	1970
DES	IBM (ABD)	1977
FEAL (Shimizu ve Miyaguchi, 1987)	Shimizu ve Miyaguchi (Japonya)	1987
GOST 28147 – 89 (Zabotin vd., 1989)	I. A. Zabotin, G. P. Glazkov, V. B. Isaeva (Sovyetler Birliği)	1989
RC2	Rivest, RSA Data Security (ABD)	1992
IDEA	Lai-Massey, Eth Zurich (İsviçre)	1992
BLOWFISH (Schneier, 1993)	Bruce Schneier, Counterpane Systems (ABD)	1993
SAFER	Massey, Cylink Corporation (ABD)	1993
SCİPJACK (Clipper Chip)	NSA (ABD)	1993
RC5	Rivest, RSA Data Security (ABD)	1995
AES	Joan Daemen ve Vincent Rijmen (ABD)	1997
ASEKAL – 55 (Erkan, 2010)	Aselsan (Türkiye)	2009

2.2. Asimetrik Şifreleme Algoritmaları

Asimetrik şifreleme, açık anahtarlı şifreleme olarak adlandırılmaktadır. Simetrik şifreleme algoritmasından farklı olarak asimetrik şifreleme algoritmasında açık ve özel anahtar olmak üzere iki farklı anahtar bulunmaktadır (Kodaz ve Botsali, 2010; Okumuş, 2012; Yerlikaya, 2006). Şifreleme anahtarına açık anahtar, şifre çözüm anahtarına ise özel anahtar ismi verilmektedir. Şifre çözme işlemi için kullanılan anahtar ile şifreleme işlemi için kullanılan anahtarlar birbirinden farklıdır (Fındık, 2004). Şifre anahtarının herkese açık olması gerektiğinden bu algoritmalara açık anahtarlı algoritmalar denilmiştir. Bu sebepten dolayı bir kullanıcının açık anahtarı ile şifrelenen bir metin sadece bu kullanıcıya ait olan özel anahtar ile metnin şifresi çözülebilmektedir. Şekil 4'te asimetrik şifreleme algoritması diyagramı gösterilmiştir.



Şekil 4. Asimetrik Şifreleme Algoritması Diyagramı

Literatürde birçok asimetrik şifreleme algoritması bulunmaktadır. Tablo 2'de asimetrik şifreleme algoritmalarından bazıları verilmiştir.

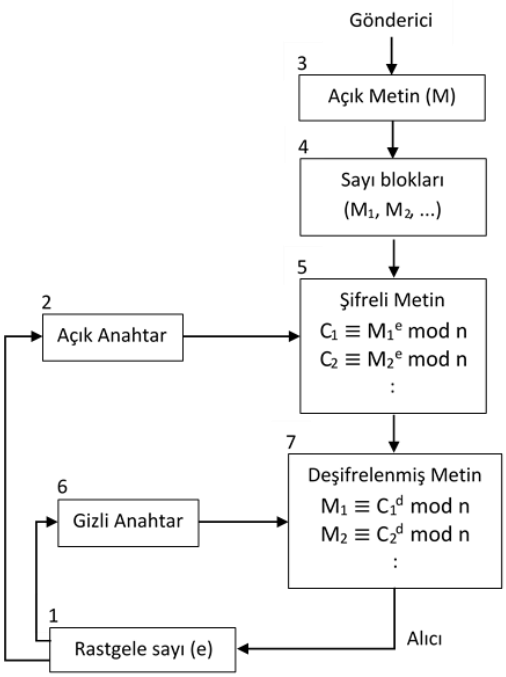
Tablo 2. Asimetrik Şifreleme Algoritmalarından Bazıları

Algoritma	Tarihi
Diffie Hellman (Diffie ve Hellman, 1976)	1976
RSA (Rivest vd., 1978)	1978
El Gamal (ElGamal, 1985)	1985
Eliptik Eğri (Koblitz, 1987)	1987

Asimetrik şifreleme algoritması olarak birçok algoritma önerilmiştir. Bu algoritmalar içerisinden RSA en yaygın olarak bilinen algoritmalardandır. RSA algoritmasının kripto analizi asal sayılara ve çarpanlara ayırmaya dayalı olması bu algoritmanın çözülme olasılığını zorlaştırmaktadır. Bu sebepten dolayı günümüzde halen kullanılan bir algoritmadır.

3. RSA Algoritması

Asimetrik şifreleme algoritması olan RSA, 1978 yılında Ron Rivest, Adi Shamir ve Leonard Adleman tarafından geliştirilmiştir (Rivest vd., 1978). Algoritmanın ismi, geliştiren kişilerin soy isimlerinin baş harflerinden oluşmaktadır. RSA algoritması hem şifreleme hem de dijital imza amacıyla kullanılabilmektedir (Kodaz ve Botsali, 2010). Aynı zamanda S/MINE, MOSS, PGP ve PEM gibi gizli haberleşmeler ile bazı SSL ve PCT protokollerinde RSA algoritması sıklıkla kullanılmaktadır (Yerlikaya, 2006). Son zamanlarda web siteleri için kredi kartı güvenlik sertifikası yönetiminde de RSA algoritması kullanılmaktadır (Fındık, 2004). Açık anahtarlı şifreleme tekniği olan RSA, çok büyük iki asal sayının çarpımından oluşan bir tamsayı oluşturma yöntemine dayanmaktadır (Akben ve Subaşı, 2005). RSA algoritmasının güvenirliği kullanılan asal sayıların büyüklüğü ile orantılı olması avantaj iken şifrelemede ve şifre çözme işlemlerinde yavaş kalması en büyük dezavantajlarındandır (Jaiswal vd., 2014). RSA algoritmasının Şekil 5'te akış şemasına yer verilmiş ve işlem adımları numaralandırılarak gösterilmiştir.



Şekil 5. RSA Algoritmasının Akış Şeması

RSA algoritması matematiksel yöntemler ile çalışan iki ayrı anahtar bulunmaktadır. Bu anahtarlardan biri açık diğeri gizli anahtardan oluşmaktadır. Açık anahtar herkese paylaşılır, şifreli metin göndermek isteyen bir kullanıcı bu açık anahtarı kullanarak metni şifreler ve gönderir. Ancak şifreli metnin çözülebilmesi gizli anahtara sahip olan kullanıcıya bağlıdır. Yani gizli anahtar kimde ise şifreli metni o çözmektedir. RSA algoritmasının anahtar oluşturma adımları aşağıdaki gibidir.

p ve q asal sayı, C ve M tam sayı olmak üzere;

İki tane asal sayı seçilir. Bu asal sayılar p ve q olsun.

- Bu iki sayının çarpılmasıyla oluşan sayı mod işleminde kullanılmak üzere denklem 1' deki gibi hesaplanır.

$$n = p * q \quad (1)$$

- Euler sayısı denklem 2' deki gibi p ve q asal sayılarının birer eksiği çarpılarak hesaplanır.

$$\varphi(n) = (p - 1) * (q - 1) \quad (2)$$

- $1<e<\varphi(n)$ aralığında ve EBOB $(\varphi(n), e) = 1$ olmak koşulu ile rastgele bir e sayısı üretilir.
- (e, n) şifreleme işleminde kullanılmak üzere oluşturulan açık anahtardır.
- $1< d <\varphi(n)$ aralığında ve $(e * d) \bmod \varphi(n) = 1$ ifadesini gerçekleşmesi şartı ile d sayısı üretilir.
- (d, n) deşifreleme işleminde kullanılmak üzere oluşturulan gizli anahtardır.

3.1. Şifreleme

- Açık anahtar olan (e, n) bilgiyi gönderecek olan kişi tarafından elde edilir.
- Açık metin $M \in [0, n - 1]$ aralığında olmak şartıyla bir tamsayıya dönüştürülür.
- Şifreli metin $C \equiv M^e \bmod n$ şeklinde hesaplanır.
- Bilgiyi gönderecek olan kişi C şifreli metnini bilgiyi alacak olan kişiye gönderir.

3.2. Şifre Çözme

- Şifre çözmek için oluşturulan gizli anahtar (d) kullanılarak $M \equiv C^d \bmod n$ eşitliğinin sağlanması sonucunda açık metin elde edilir.

Tablo 3'te RSA algoritmasının anahtar oluşturma, şifreleme ve şifre çözme adımları örnek olarak verilmiştir.

Tablo 3. RSA Algoritması Örneği

RSA Algoritması	İşlem
p ve q asal sayılar	p = 7 ve q= 17 olsun.
$n = p * q$	$n = 7 * 17 = 119$
$\varphi(n) = (p - 1) * (q - 1)$	$\varphi(n) = (7 - 1)* (17 - 1) = 96$
$1< e < \varphi(n)$ aralığında ve EBOB($\varphi(n)$, e) = 1	e = 11
b = e, n	b = 11, 119
$C_b(M) = M^e \pmod n$	$C_{11,\,119}(M) = M^{11} \pmod{119}$
$(e * d) \bmod \varphi(n) = 1$ ve $1< d < \varphi(n)$	$d = 35, (11*35) = 1 \pmod{96}$
m = d, n	b = 35, 119
$M_m(C) = C^d \pmod n$	$M_{35,119}(C) = C^{35} \pmod{119}$

Algoritmanın güvenirliğini artırmak için ilk önce yapılması gereken anahtar oluşturma aşamasında p ve q asal sayılarının büyük olması önemlidir. Çünkü bu büyük sayıların asal çarpanlarına ayrılması zor olduğundan şifrenin kırılması da zor olacaktır. Bu ilk aşama için tablodaki örneğe göre açık anahtar oluşturmada p=7 ve q=17 asal sayıları alındığında ve kısıtları belli rastgele seçilen e sayısı 11 olduğunda, n denkleminden elde edilen sayı 119'dur. Gizli anahtarda ise aynı şartlarda d = 35 ve n = 119 olarak bulunmaktadır.

Şifreleme:

- Bilgiyi alacak olan kullanıcı herkesin bilgisine açık bir kanaldan e=11 ve n=119 olan açık anahtarlar karşı tarafa gönderilir.
- Bilgiyi paylaşacak olan kullanıcının açık metni (M) kısıtlar dahilinde rastgele seçilen 45 sayısı olsun.
- Şifreli metin $C = 45^{11}$ (mod 119) işlemine göre C = 12 olarak bulunmaktadır.
- Bilgiyi paylaşacak olan kullanıcı C = 12 sayısını, bilgiyi karşı tarafa tekrar göndermek için herkesin bilgisine açık bir kanal kullanılır.

Şifre Çözme:

- Bilgiyi alacak olan kullanıcı $M = 12^{35}$ (mod 119) eşitliğini sağlayan M sayısını 45 bularak açık metni elde etmiş olur.

4. RSA Algoritması Neden Önemli?

Çeşitli problemlere uygulanmaya başlanan RSA algoritması, birçok gerçek dünya problemlerinde ve mühendislik alanında kullanılmaktadır. Özellikle son yıllarda RSA algoritması ile ilgili çok sayıda çalışma bulunmaktadır.

Lee ve Chang (1998) şifreleme işlemlerinin hızlı gerçekleşmesini sağlamak için küçük ortak anahtarın dinamik olarak büyütülmesini sağlayan bir yöntem önermişlerdir.

Somani vd. (2010) Bulut bilişimde verilerin güvenliğini geliştirmek için RSA algoritmasını ve dijital imza algoritmasını önermişlerdir.

Dubey vd. (2012) Bulut kullanıcısı ile bulut sağlayıcısı için MD5 ve RSA algoritmasını kullanarak verilerin toplanması ile paylaşılması için güvenli bir sistem tasarladıklarını böylece güvenilir hesaplamaların yapılabileceğini söylemişlerdir.

Patidar ve Bhartiya (2013) RSA algoritmasının hızlandırılması için modifiye edilmiş RSA algoritmasını önermişlerdir. Önerilmiş olan algoritmada iki asal sayı yerine üç asal sayı kullanarak hız ve güvenlik üzerine çalıştıklarını söylemişler ve orijinal RSA ile kıyaslamışlardır. Kıyaslama sonuçlarına göre önerilen algoritmanın daha güvenilir olduğunu söylemişlerdir.

Ayele ve Sreenivasarao (2013) RSA için iki ortak anahtar içeren bir yöntem önermişlerdir. İki ortak anahtarın ayrı olarak gönderilmesi saldırganın anahtar hakkında fazla bilgi sahibi olmamasına ve metinin şifresinin çözülmemesine sebep olduğunu söylemişlerdir. Önerilen RSA'nın daha az hız ile yüksek güvenlik sağladığını söylemişlerdir.

Jaiswal vd. (2014) Ağ üzerinden veri alışverişi sırasında hesaplanma zamanın hızlanması ve güvenirliğinin daha iyi olması için modifiye edilmiş olan RSA algoritmasını önermişlerdir. Orijinal RSA ile önerilen RSA'nın karşılaştırılması sonucunda önerilmiş olan RSA'nın daha iyi güvenlik sağladığı ve işlem hızının arttırıldığı sonucuna varmışlardır.

Thangavel vd. (2015) ESRKGS adı verilen modifiye edilmiş ve geliştirilmiş bir RSA anahtar üretim algoritması önermişlerdir. Önerilmiş olan algoritmada iki asal sayı yerine dört büyük asal sayı kullanmışlardır. Yapmış oldukları deney sonuçlarına göre önermiş oldukları algoritmanın yüksek oranda güvenli ve kolay kırılamayacağını kanıtladıklarını söylemişlerdir.

Çavuşoğlu vd. (2017) RGN ve RSA algoritmasının birlikte kullanılmasıyla oluşan kaos tabanlı hibrit RSA (CRSA) şifreleme algoritması tasarlamışlardır. Oluşturulan bu algoritmayla metin ve görüntü şifrelemesinin yapıldığını ifade etmişlerdir. Yaptıkları güvenlik analiz sonuçlarının klasik RSA ile karşılaştırılması sonucunda önerdikleri algoritmanın daha iyi sonuçlar verdiğini görmüşlerdir.

El Makkaoui vd. (2017) bulut bilişiminde veri gizliğinin sağlanması ve şifre çözme işlemini hızlandırmak için hızlı bulut-RSA'yı önermişlerdir. Elde ettikleri simülasyon sonuçlarına göre hızlı-RSA'nın çalışma zamanında iyi bir performans sergileyerek öngörülen güvenlik seviyesini sağladığını belirtmişlerdir.

Stergiou vd. (2018) IoT ve cloud teknolojilerinin entegrasyonunda AES ve RSA algoritmalarını kullanmışlardır. Şifreleme işlemlerinde RSA algoritmasının kullanılmasıyla IoT'un işlevinde daha yüksek düzeyde iletişim güvenliğinin sağlanabileceği sonucuna varabildiklerini belirtmişlerdir.

Liu vd. (2018) RSA algoritmasını kullanarak güvenli ve sağlam bir dijital görüntü şeması filigran modeli önermişlerdir. Gizli verilerin güvenliğini garanti altına almak için asimetrik şifreleme algoritmalarından biri olan RSA algoritmasını kullanmışlardır. Yapmış oldukları deney sonuçlarına göre önerdikleri yöntemin daha iyi sağlamlık, daha az şifreleme süresi ve büyük veri gömme kapasitesine sahip olan diğer yaklaşımlara göre daha iyi performans göstermiş olduğunu aktarmışlardır.

Taha vd. (2018) mobil bulut bilişim siteminde veri güvenliğinin sağlanması için hibrit RSA algoritmasını önermişlerdir. Sonuçlara göre veri güvenliğinin arttığını ve veriyi şifrelemek için harcanan sürenin azaldığını söylemişlerdir.

Subhashini ve Srivaramangai (2018) tarafından bulut bilişim ile ilgili yaptıkları çalışmada bulutta bulunan verilerin güvenli bir şekilde korunmadığı taktirde verilerin risk altında olabileceğini söylemişlerdir. Bundan dolayı bulut sistemde güvenliği üst düzeyde tutmak için çeşitli kriptografik algoritmaların olduğunu söylemişler ve bu algoritmaların iyileştirilmesi ile ilgili genel bir bakış sunarak tartışma gerçekleştirmişlerdir.

Palathingal vd. (2018) bulut sistemlerinde verilerin güvenirliğinin sağlanması için steganografi yöntemini kullanmışlardır. Sistemdeki verilerin daha güvenli olması için RSA algoritmasını diğer algoritmalarla entegre ettiklerini ve bulut bilişim sisteminde verilerin güvenliği için güçlü bir yapı olduğunu vurgulamışlardır.

RSA algoritması ile literatürde yer alan AES ve DES algoritmalarının bazı özelliklerinin karşılaştırılması Tablo 4'te verilmiştir.

Tablo 4. AES, DES ve RSA Algoritmalarının Özellikleri

Özellikler	AES	DES	RSA
Tarihi	1997	1977	1978
Anahtar uzunluğu	128, 192, 256 bit	56 bit	>1024 bit
Blok uzunluğu	128 bit	64 bit	En az 512 bit
Şifreleme ve şifre çözme anahtarı	Aynı	Aynı	Farklı
Algoritma türü	Simetrik şifreleme algoritması	Simetrik şifreleme algoritması	Asimetrik şifreleme algoritması
Şifreleme hızı	Hızlı	Orta	Yavaş
Şifre çözme hızı	Hızlı	Orta	Yavaş
Güç tüketimi	Düşük	Düşük	Yüksek
Güvenirliği	Güvenli	Yeteri kadar güvenli değil	Güvenli
Kullanılan anahtar	Şifreleme ve şifreyi çözmek için kullanılan anahtar aynı	Şifreleme ve şifreyi çözmek için kullanılan anahtar aynı	Şifreleme ve şifre çözmek için kullanılan anahtar farklı
Devir sayısı	10, 12, 14	16	1
Başlama hızı	Hızlı	Hızlı	Hızlı
Truva atı	Kanıtlanmamış	Yoktur	Yoktur

RSA algoritmasının güvenirliğinin sağlanması için anahtar oluşturulma esnasında çok büyük asal sayılarla işlem yapıldığından sistem yavaş çalışmaktadır. Ancak bu işlem yoğunluğundan dolayı şifrenin kırılması zor olmakla birlikte algoritmanın güvenirliği de artmaktadır. Tablo 4'e bakıldığında RSA'nın güvenirliğinin diğer algoritmalara göre daha iyi olduğu ancak yavaş çalıştığı görülmektedir.

5. Sonuçlar

Bu çalışmada simetrik ve asimetrik şifreleme algoritmalarının genel özellikleri incelenmiş ve asimetrik şifreleme algoritması olan RSA algoritması hakkında bilgilere yer verilmiştir. Simetrik şifreleme algoritmaları tek anahtar kullanarak şifreleme ve deşifreleme işlemi yapmaktadır. Simetrik şifreleme algoritmasında düz metin gizli anahtar yardımı ile şifrelenir. Aynı gizli anahtar ile deşifreleme işlemi de gerçekleştirilmektedir. Asimetrik şifreleme algoritmalarından biri olan RSA algoritmasında ise biri açık diğeri gizli olmak üzere iki farklı anahtar bulunmaktadır. RSA algoritmasında açık anahtar ile şifrelenen düz metin sadece özel anahtar ile deşifrelenmektedir. RSA algoritması ile ilgili güncel literatür taramasında daha çok bulut sistemlerin şifrelenmesi ile görüntü şifreleme üzerine yoğun çalışmalar bulunmaktadır. Bunun sebebi RSA'nın güvenirliğinin yüksek olması ile ilgilidir. RSA algoritmasının güvenirliği çok büyük asal sayı seçmeye bağlıdır. Ancak büyük asal sayılarla işlem yapılması matematiksel zorluğa sebep olduğundan algoritma yavaş çalışmaktadır. Bu durum RSA algoritması için bir dezavantajdır. Eğer bu dezavantajlar giderilirse RSA algoritması daha güvenilir ve hızlı bir algoritma olacaktır. Bunun için RSA algoritmasının diğer algoritmalarla hibritlenmesi sonucunda elde edilecek olan yeni hibrit algoritmanın daha güvenilir ve hızlı bir algoritma olacağı düşünülmektedir.

Kaynaklar

Akben, S. B., & Subaşı, A. (2005). RSA ve eliptik eğri algoritmasının performans karşılaştırması. *KSÜ Fen ve Mühendislik Dergisi, 8*(1), 35-40.

Ayele, A. A., & Sreenivasarao, V. (2013). A modified RSA encryption technique based on multiple public keys. *International Journal of Innovative Research in Computer and Communication Engineering, 1*(4), 859-864.

Çavuşoğlu, Ü., Akgül, A., Zengin, A., & Pehlivan, I. (2017). The design and implementation of hybrid RSA algorithm using a novel chaos based RNG. *Chaos, Solitons & Fractals, 104*, 655-667.

Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE transactions on Information Theory, 22*(6), 644-654.

Dubey, A. K., Dubey, A. K., Namdev, M., & Shrivastava, S. S. (2012). *Cloud-user security based on RSA and MD5 algorithm for resource attestation and sharing in java environment.* Paper presented at the Software Engineering (CONSEG), 2012 CSI Sixth International Conference on.

El Makkaoui, K., Beni-Hssaneb, A., Ezzatia, A., & El-Ansarib, A. (2017). Fast Cloud-RSA Scheme for Promoting Data Confidentiality in the Cloud Computing. *Procedia Computer Science, 113*, 33-40.

ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE transactions on Information Theory, 31*(4), 469-472.

Erkan, H. (2010). ASELSAN Kriptografik Algoritma Tasarım Yetenekleri. *Aselsan, 23*(81), 26.

Fındık, O. (2004). *Şifrelemede kaotik sistemin kullanılması.* (Yüksek Lisans Tezi), Selçuk Üniversitesi Fen Bilimleri Enstitüsü.

Jaiswal, R. J., Soni, R., & Mahale, P. (2014). Reformed RSA algorithm based on Prime Number. *NCETIT-2014*, 0975-8887.

Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of computation, 48*(177), 203-209.

Kodaz, H., & Botsali, F. M. (2010). Simetrik ve asimetrik şifreleme algoritmalarının karşılaştırılması. *Selçuk Teknik Dergisi, 9*(1), 10-23.

Lee, W.-b., & Chang, C.-C. (1998). Using RSA with low exponent in a public network. *Computer Communications, 21*(3), 284-286.

Liu, Y., Tang, S., Liu, R., Zhang, L., & Ma, Z. (2018). Secure and robust digital image watermarking scheme using logistic and RSA encryption. *Expert Systems with Applications, 97*, 95-105.

Okumuş, İ. (2012). *RSA Kriptosisteminin hızını etkileyen faktörler / The factors affecting speed of the RSA cryptosystem.* (Doktora Tezi), Atatürk Üniversitesi, Fen Bilimleri Enstitüsü.

Palathingal, A. G., George, A., Thomas, B. A., & Paul, A. R. (2018). Enhanced Cloud Data Security using Combined Encryption and Steganography.

Patidar, R., & Bhartiya, R. (2013). *Modified RSA cryptosystem based on offline storage and prime number.* Paper presented at the Computational Intelligence and Computing Research (ICCIC), 2013 IEEE International Conference on.

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM, 21*(2), 120-126.

Schneier, B. (1993). *Description of a new variable-length key, 64-bit block cipher (Blowfish).* Paper presented at the International Workshop on Fast Software Encryption.

Shimizu, A., & Miyaguchi, S. (1987). *Fast data encipherment algorithm FEAL.* Paper presented at the Workshop on the Theory and Application of of Cryptographic Techniques.

Somani, U., Lakhani, K., & Mundra, M. (2010). *Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing.* Paper presented at the Parallel Distributed and Grid Computing (PDGC), 2010 1st International Conference on.

Stergiou, C., Psannis, K. E., Kim, B.-G., & Gupta, B. (2018). Secure integration of IoT and cloud computing. *Future Generation Computer Systems, 78*, 964-975.

Subhashini, M., & Srivaramangai, P. (2018). A Study on Cloud Computing Securities and Algorithms.

Taha, A. A., Elminaam, D. S. A., & Hosny, K. M. (2018). An Improved Security Schema For Mobile Cloud Computing Using Hybrid Cryptographic Algorithms.

Thangavel, M., Varalakshmi, P., Murrali, M., & Nithya, K. (2015). An Enhanced and Secured RSA Key Generation Scheme (ESRKGS). *journal of information security and applications, 20*, 3-10.

Yerlikaya, T. (2006). *Yeni şifreleme algoritmalarının analizi.* (Doktora Tezi), Trakya Üniversitesi Fen Bilimleri Enstitüsü.

Yeşilbaş, E. (2016). *Cebirsel Kriptoloji Yöntemleri ve Bazı Uygulamaları.* (Yüksek Lisans Tezi), Recep Tayyip Erdoğan Üniversitesi, Fen Bilimleri Enstitüsü.

Zabotin, I., Glazkov, G., & Isaeva, V. (1989). Cryptographic protection for information processing systems. *Government Standard of the USSR, GOST*, 28147-28189.