Trakya University Journal of Engineering Sciences
http://dergipark.gov.tr/tujes
ISSN 2147–0308 *Research Article / Araştırma Makalesi*

ASİMETRİK ŞİFRELEMEDE ASAL SAYILAR VE GÜVENLİK

Nursel İŞÇİMEN[1], Tarık YERLİKAYA[2]

[1] *Trakya Üniversitesi, Keşan Yusuf Çapraz Uygulamalı Bilimler Yüksekokulu, Bankacılık ve Sigortacılık Bölümü, Keşan / Edirne / Türkiye*

[2] *Trakya Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Edirne / Türkiye*

Makale Künye Bilgisi: İşçimen, N., Yerlikaya, T., (2023). Asimetrik Şifrelemede Asal Sayılar ve Güvenlik, *Trakya Üniversitesi Mühendislik Bilimleri Dergisi,* 24(1), 11-18.

Öne Çıkanlar

- Asimetrik şifrelemede güvenliğin temeli asal sayılara dayanmaktadır.
- RSA 'da çok büyük asal sayıların çarpımıyla oluşan modül değerinin çarpanlara ayrılması zorluğu veri güvenliğinde etkilidir.
- Veri güvenliği için çoklu asal sayılar tercih edilebilir.

Makale Bilgileri

Makale Tarihçesi:
Geliş:
26 Mayıs 2023
Kabul:
12 Temmuz 2023

Anahtar Kelimeler:
Asimetrik şifreleme;
Şifreleme Güvenliği;
Asal sayılar

Öz

Güvenli olmayan bir ağ ortamında verileri gizlemek ve transferini sağlamak için şifreleme kriptosistemleri kullanılır. Asimetrik şifreleme kriptosistemlerinde verinin güvenle saklanması ve iletişimin güvenli gerçekleşmesi için kullanılan algoritmaların gücü, anahtar gizliliği, cebirsel fonksiyonlar kadar kullanılan asal sayılar da etkilidir. Kriptosistemin güvenliği aynı zamanda saldırılara dayanabilme kapasitesiyle ilişkilidir. Asimetrik şifreleme algoritmalarından biri olan RSA şifreleme algoritması saldırılara karşı gücünü çarpma işleminden almaktadır. Çok büyük sayıların çarpanlara ayrılması zorluğu RSA'nın gücüne güç katmaktadır. RSA'da modN'i oluşturan (N=p.q) p ve q asal çarpan değerlerinin çok küçük ve birbirine yakın olması sistemin güvensizliği sorunu doğurmaktadır. Çalışma kapsamında önerilen RSA algoritma uygulamasıyla bu güvensizlik sorunu incelenmiş ve 2^k (k≥3) adet asal sayı kullanılarak RSA şifreleme yapılmış Normal RSA ile karşılaştırma yapılmıştır.

Prime Numbers in Asymmetric Encryption and Securty

Article Info

Article History:
Received:
May 26, 2023
Accepted:
July 12, 2023

Keywords:
Asymmetric Encryption;
Encryption Securty;
Prime Numbers.

Abstract

Encryption cryptosystems are used to hide and transfer data in an insecure network environment. In asymmetric encryption cryptosystems, the power of algorithms, key secrecy and algebraic functions used for safe data storage and communication are as effective as prime numbers used. The security of the cryptosystem is also related to its capacity to withstand attacks. The RSA encryption algorithm, one of the asymmetric encryption algorithms, takes its power against attacks from multiplication. The difficulty of factoring very large numbers adds to the power of RSA. The fact that the prime factor values of p and q (N=p.q) that make up modN in RSA are very small and close to each other, causes the insecurity of the system. This insecurity problem was examined with the RSA algorithm application proposed within the scope of the study and a comparison was made with Normal RSA using RSA encryption using $2^k (k \geq 3)$ prime numbers.

*Sorumlu Yazar: nurselgurakar@trakya.edu.tr

DOI : 10.59314/tujes.1303091

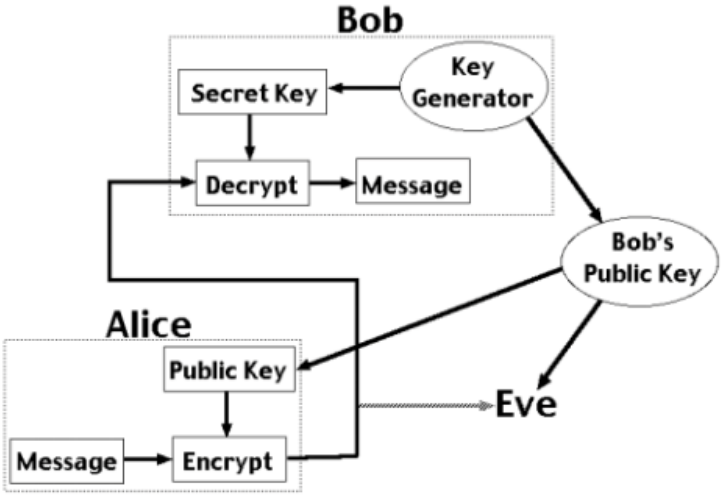
1. Giriş

Bilginin kullanıcılar arasında iletişim kanalları vasıtasıyla anında tek tuşla iletildiği dijital dünya internetin sağladığı avantajlarının yanı sıra istenmeyen kullanıcılara ve onlardan gelebilecek saldırılarla da maruz kalmaktadır. Güvenli olmayan bir ağ ortamında matematiksel teknikleri kullanarak bilgiyi okunamaz bir forma dönüştürerek gizlemek ve transferini sağlamak için şifreleme kripto sistemleri kullanılmaktadır. Kriptoloji, kriptografi ve kriptanalizi barındıran ve iletişimin güvenle gerçekleşmesini inceleyen bilimdir Liestyowati, 2020). Bilgi güvenliği için gereken kodlar, şifreler, kodlamalar insanoğlunun hayatının hemen her alanında farkında olmadan yer almaktadır. Kriptologlara göre kodlar ve şifreler birbirinden farklıdır. Kodlar, harflerin, sözcüklerin veya ifadelerin önceden düzenlenmiş biçimi iken , şifreler ise mesajları okunamaz karmakarışık biçime dönüştürmek için algoritma adı verilen matematiksel prosedürleri kullanmaktadırlar. Şifreleme algoritmaları ve şifre anahtarları, kapı kilit ve kapı anahtarlarına benzer, kilitlerin çalışma biçimi ayı olabilir fakat anahtarlar birbiriyle aynı değildir(Mann, 2002). Matematikçilerin asal sayılara olan hayranlığı ve asal sayıların matematik dışında şifreleme bilimiyle olan kuvvetli ilişkisi geçmişten günümüze pek çok çalışmaya konu olmuştur. Asal sayıların siber güvenliğimize olan etkisininin ne kadar farkındayız? Açık anahtar kriptografisi şifreleme algoritmalarının güvenlik önlemlerini asal sayılarla sağlamaktadır. E-ticaret sistemlerinde kimlik doğrulama yani elektronik imza ve güvenli iletişim açık anahtar kriptografisi ile gerçekleşmektedir (Wolf, C., & Preneel, B. ,2004). Açık anahtarlı kriptosistemler anahtarın güvenle iletiminin güçlüğünü yaşamamak ayrıca paylaşılan genel anahtar vasıtasıyla özel anahtarın elde edilmesini imkansız kılmak amacındadır. (Tuncal, 2008).Tubitak 2010 yılında yayımladığı *Açık Anahtar Altyapısı Eğitim Kitabı'* nda asimetrik şifrelemenin gizlilik, bütünlük, kimlik doğrulama, inkar edilemezlik özelliklerini sağladığını; anahtar uzunluğuna bağlı bir güvenliğe sahip olduğunu fakat simetrik şifreleme algoritmalarına göre daha yavaş bir performansta olduğu belirtilmektedir. Asimetrik şifreleme algoritma düz metin, şifreleme algoritması, özel anahtar, genel anahtar, şifreli metin, deşifreleme algoritması asamalarından meydana gelmektedir (Stallings, 2006). Bu altı ana hat açık anahtarlı şifrelemede ayrıntılı ele alındığında karmaşık bir alt yapıda olsalarda ve temellerinin matematiksel işlemlere dayansa da genel çerçevede oldukça basit bir yapıya sahiptir. Göndericinin özel anahtarını bilmediğimiz halde verileri gizlemek ve göndermek için halka açık olan anahtar vasıtasıyla gerçekleştirilen şifrelemede çok basit gibi görünen ama tersine çevrilmesi güç matematiksel işlemlerden yararlanılır. Güvenliği ve erişilebilirliği arttırdığı için matematiksel güç Asimetrik şifreleme algoritmalarından RSA'da avantaj olarak kabul görmektedir. Göndericinin düz metni olan orijinal mesajlardan şifreli bir mesaj meydana getirmek için bazı algoritmik adımlarla kodlanmaktadırlar (Chaudhury, P., Dhang, S., Roy, M., Deb, S., Saha, J., Mallik, A., ... & Das, R. , 2017). Orijinal veriyi gönderecek taraf alıcının halka açık olan ve iki sayıdan oluşan anahtarını kullanarak şifrelemeyi gerçekleştirir. Davetsiz bir misafirin veri iletimi sırasında gizli anahtarı bulma şansı oldukça azdır. Alıcı; göndericinin şifrelediği bilgiyi yine iki sayıdan oluşan özel anahtarını kullanarak orijinal biçime dönüştürür. Bu kadar kolay gibi görünen bu sürecin arka planı karmaşık matematiksel algoritmalarla sağlanmaktadır. RSA kriptografide matematiksel işlemler için tercih edilen büyük asal sayılardan meydana gelen bileşik sayıların çarpanlarına ayrılması zorluğu verinin parçalanmasını yada uygun anahtar olmadan okunmasını engellemektedir. Rivest ve meslektaşları tarafından kullanılan çarpanlara ayırma algoritmasının o anki en hızlı algoritmaya ve kullanılan bilgisayarın 1 milisaniye hızına sahip olduğu varsayımıyla 200 basamaklı bir çarpanın bulunması

girişiminin 4 milyar yıllık hesaplama süresi gerektirdiği belirtilmektedir (Mollin, Richard A. ,2002). Bu durum çarpanlara ayırmanın sadece insanlar için değil aygıtlar için de ne derece zor olduğunun açık bir kanıtıdır.

2. RSA Algoritması

İlk kez 1977'de Ron Rivest, Adi Shamir ve Leonard Adleman tarafından ve isimlerinin baş harflerinden oluşan RSA şifreleme ve şifre çözme algoritması bir tür açık anahtar şifrelemesidir (Mathur, H., & Alam, Z., 2015). RSA 'da iyi bir veri güvenliği elde etmek için anahtar oluşturma alanlarıyla ilgili katı kurallara uyulması, anahtarın yeterince büyük uzunluklarda kullanılması, asal sayıların güvenilir şekilde üretilmesi gerekmektedir. RSA algoritması temeli bit cinsinden istenen anahtar uzunluğu nBit olan ve herbiri yaklaşık olarak nBits/2'ye eşit boyutta olarak üretilen iki farklı p ve q asal sayısı üzerine kurulmuştur (Ivanov, A., & Stoianov, N. (2023).



Şekil 1.RSA Algoritması (Mathur, H., & Alam, Z., 2015)

Şemayı incelediğimizde RSA'nın genel hatlarını nasıl gerçekleştiğini görmekteyiz. Alice Bob'a gizli bir bilgi gönderecekse Bob'un oluşturduğu anahtar çiftinden halka açık olanı kullanması gerekmektedir. Bob Alice'e iki bileşenden oluşan (E,N) açık anahtarını gönderir ve Alice de bu anahtarı kullanarak göndereceği bilgiyi kilit altına almış olur. Şifrelediği bu bilgiyi güvenli olmasa da artık bir kanal aracılı ile Bob'a gönderir. Bob kendi özel anahtarı olan (D,N) ile şifreli bilgiyi deşifreleyerek orijinal metne ulaşır. Bob dışında hiçkimse onun özel anahtarı olmadan deşifreleme basamağını gerçekleştiremez. Dolayısıyla Eve orijinal metne erişmek istiyorsa direkt olarak Bob'un özel anahtarına ulaşmalı ya da N'yi çarpanlarına ayırıp D Yi hesaplamalıdır. Çok büyük asal sayılarla matematiksel algoritmalarını gerçekleyen RSA da çarpanlara ayırma işi oldukça zaman alıcı ve aygıtlar için bile zorlayıcıdır. En sık kullanılan açık anahtar şifreleme algoritmalarından RSA, tamsayı çarpanlara ayırma problemi gibi matematiksel problemlerin çözülmesindeki zorluğa dayanmaktadır (Ivanov, A., & Stoianov, N. (2023). Çok büyük asal sayıları çarpanlarına ayırma metodu bulunmadığı sürece RSA güvenliğinin güvende olduğu ifade edilmektedir (Liestyowati, D. ,2020). Uzun yıllardır RSA tabanlı kriptografik sistemleri kırmak için güvenlik açıklarını belirlemek , matematiksel saldırı modelleri oluşturmak amacıyla yapılan çalışmalarda şu ana kadar 2048 bit veya daha büyük uzunluktaki RSA anahtarını kırabilecek bir saldırı yaklaşımı geliştirilemediği görülmektedir (Ivanov, A., & Stoianov, N. (2023). Son üç yüz yıldır pek çok matematikçinin çalışmasında konu olmasının bile büyük sayıların çarpanlarına ayrılmasının zorluğunnun ispatlandığına dair bir kanıt olmadığı ve RSA sistem güvenliğinin varsayımdan ibaret olduğu, ayrıca belirlenebilmiş net bir algoritmanın olmadığı aktarılmaktadır (Aksuoğlu, 2010).

3. RSA Anahtar oluşturma Öneri Algoritması

Çalışmada standart RSA'dan farklı olarak anahtar oluşturmada çoklu asal sayı kullanılarak (2'den fazla asal sayı ile) şifreleme yapılmıştır. Güvenlik açısından daha küçük bitlerle güvenlik araştırılmıştır. Hinek, M. J. 2008 de yaptığı çalışmasında RSA güvenliğinde çoklu asal sayıların kullanımını incelemiş ve 80 bit çoklu asal sayı kullanımı 1024 bit temel RSA ile aynı güvenliğin sağlandığını ifade etmiştir. RSA şifreleme sisteminin modülünde iki adetten daha fazla çarpan kullanılması, özel anahtar hesabında aritmetik bir avantaj sağlayacağı ve doğru parametre seçimi sayesinde çarpanlara ayırma probleminin zorluğu açısından aynı güvenlik düzeyine ulaşmak için daha büyük bir modülle çalışmak zorunda kalınmayacağı belirtilmektedir (Hinek, M. J., Low, M. K., & Teske, E. ,2003). Kamardan ve arkadaşlarının 2018'de gerçekleştirdiği Multi-prime RSA çalışmasında şifre çözme hızı ve bellek tasarrufu açısından standart RSA'dan verimli olduğu belirtilmiştir. Ayrıca 2000 yılında Compaq tarafından yapılan deneysel sonuçların Multi-prime RSA sayesinde şifre çözmenin, standart RSA'dan hemen hemen 4 kat daha hızlı olduğunu belirtmiştir (Kamardan, M. G., Aminudin, N., Che-Him, N., Sufahani, S., Khalid, K., & Roslan, R. , 2018). Ağlar üzerinde güvenliği sağlamak için değiştirilmiş bir RSA şifreleme sistemi kullanan Ivy ve arkadaşları asal sayı algoritmasını geliştirmek amacıyla dört asal sayı kullanarak algoritmayı gerçekleştirmişlerdir. Ayrıca bu tekniğin, ağlar üzerinde daha fazla verimlilik ve güvenilirlik sağladığını ifade etmektedirler (Ivy, B. P. U., Mandiwa, P., & Kumar, M. , 2012). Rivest ve Silvermen güçlü asal sayıların kullanımı çarpanlara ayırma saldırılarına karşı ek koruma sağlamadığını belirtmektedirler. RSA kripto sisteminde güçlü asal sayıların kullanılmasının yaygın bir inanış olduğunu ve gereksiz olduğunu hatta yalnızca aynı büyüklükteki "rastgele" asal sayılar kullanılarak elde edilene göre güvenlikte ihmal edilebilir bir artış meydana geldiğini belirtmektedirler. Çalışmalarında güçlü asalları üretmenin ekstra maliyeti dışında kullanılmalarının zararlı görünmediğini, ancak onları kullanmanın fazla koruma sağlamadığını, gerçek koruma için yeterince büyük p ve q asal sayılarını seçilmesi gerektiğini açıklamışlardır. Güçlü asalların rastgele asalların sağladığından daha az koruma sağladığını savunmaktadırlar (Rivest, R. L., & Silverman, R. D., 1999). Güçlü veri güvenliğinin sağlanması büyük kriptografik anahtar çiftleri yani büyük genel anahtar ve özel anahtar aracılığı ile sağlanabilir. Bunun sonucunda bellek kısıtlamalı aygıtlar, küçük aygıtlar için hesaplama büyük maddi yüke neden olmaktadır. Günümüz dijital dünyasında küçük cihazlar oldukça sıklıkla kullanılmaktadır. Küçük aygıtların güçlü güvenlikte çalışması için RSA tercih edilirliği ilk sırada yer almayacaktır. (Mahto, D., Khan, D. A., & Yadav, D. K. , 2016). Peki çok büyük asal sayılar kullanmak gerçekten gereklimi? Daha küçük asal sayılarla da güvenli şifreleme yapmak mümkün mü?

4. Gereç ve Yöntem:

Bu çalışmada Lone, & Khalique, 2016'da önerdikleri çoklu asal sayı RSA algoritmasından yararlanılmıştır. Gerçekleştirilen öneri algoritması için anahtar üretim aşamaları, şifreleme ve deşifreleme basamakları 8 asal sayı için aşağıdaki gibidir. Bu çalışmasında bu anahtar üretim algoritması kullanılmış fakat örnek alınan çalışmadan farklı olarak sınırlı asal sayı kümeleri ile uygulamaların güvenlik üzerindeki etkileri araştırılmıştır. Çalışma İ5 -2500k işlemci 3.3 GH ve 12gb ram özelliklere sahip bilgisayarda yapılmıştır.

8 Asal Sayı İle Anahtar Üretimi:

Girdi:

- 8 asal sayı seç: $p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8$

Çıktı:

- Genel anahtar bileşenleri: {E, n}
- Özel anahtar bileşenleri:{D, n}

Prosedür:

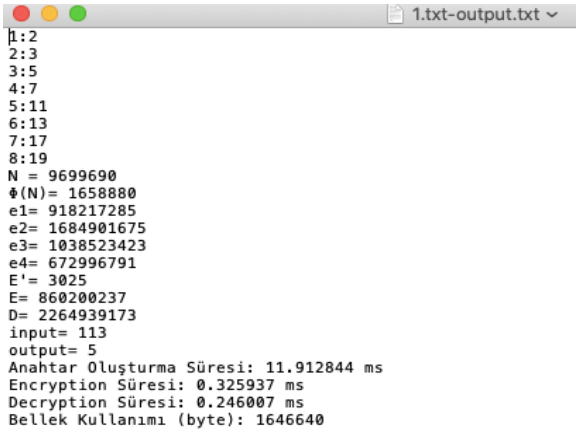
- $n \leftarrow p_1 . p_2$
    - $m \leftarrow p_3 . p_4$
    - $o \leftarrow p_5 . p_6$
- $p \leftarrow p_7 . p_8$
    - $N_1 \leftarrow n\ .m$
    - $N_2 \leftarrow o\ .p$
- $N \leftarrow N_1 . N_2$

/*n, m, o ve p'nin Euler phi değerlerini hesaplanması*/:

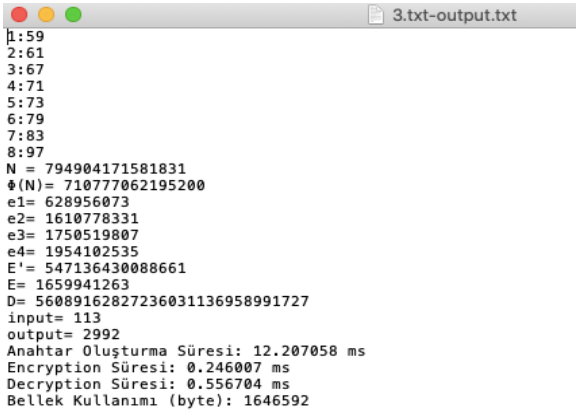
- $\phi(n) \leftarrow (p_1 - 1).(p_2 - 1)$
- $\phi(m) \leftarrow (p_3 - 1).(p_4 - 1)$
- $\phi(o) \leftarrow (p_5 - 1).(p_6 - 1)$
- $\phi(p) \leftarrow (p_7 - 1).(p_8 - 1)$

/*N'nin Euler phi değerlerini hesapla */

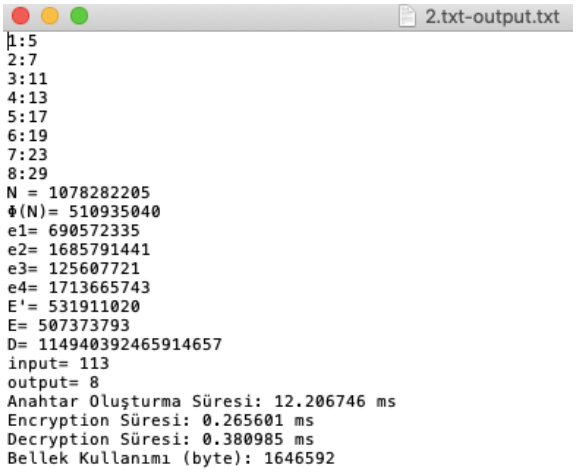
- $\phi(N) \leftarrow \phi(n).\phi(m).\phi(o).\phi(p)$
- Rastgele bir e_1 sayısı bul , $1 < e_1 < \phi(n)$ ve $gcd(e_1, \phi(n)) = 1$
- Rastgele bir e_2 sayısı bul , $1 < e_2 < \phi(m)$ ve $gcd(e_2, \phi(m)) = 1$
- Rastgele bir e_3 sayısı bul , $1 < e_3 < \phi(o)$ ve $gcd(e_3, \phi(o)) = 1$
- Rastgele bir e_4 sayısı bul , $1 < e_4 < \phi(p)$ ve $gcd(e_4, \phi(p)) = 1$
- Hesapla $A_1 \leftarrow {e_1}^{e_2} mod N_1$
- Hesapla $A_2 \leftarrow {e_3}^{e_4} mod N_2$
- Hesapla $E' \leftarrow {A_1}^{A_2} mod(N)$
- Rastgele bir E sayısı bul , $1 < E < \phi(n).E'$, $gcd(E, \phi(n).E') = 1$
- Rastgele bir D sayısı hesapla, $D \leftarrow E^{-1} mod(\phi(N).E')$ (Lone, & Khalique, (2016) https://onlinelibrary.wiley.com/doi/full/10.1002/sec.1619)



Şekil 2. Çok küçük 8 asal sayı uygulama örneği



Şekil 3. Çok küçük 8 asal sayı uygulama örneği



Şekil 4. Çok küçük 8 asal sayı uygulama örneği

Tablo 1. Uygulama sonuçları ortalama değerler tablosu.

Anahtar oluşturma süresi (ms)	Şifrelem süresi (ms)	Deşifrele me süresi (ms)	Bellek Kullanımı (byte)
12	0.25	0.5	1646608

Şekiller ve tablo incelendiğinde Standart RSA kripto sistemi meydana getiren temel üç ana aşama RSA anahtar oluşturma önerisi kripto sistemi için de aynen gerçekleştiği görülmektedir. Anahtar Üretimi, Şifreleme, deşifreleme ve bellek kulanımında gerçekleşen uygulama sonuçları RSA anahtar oluşturma önerisi güvenliğini arttırmak için yeterli olup olmadı incelenmelidir. RSA anahtar oluşturma önerisi çoklu asal sayı kullanılması sonucu algoritmanın güvenliğini kırmanın asal sayıların küçük seçilmesine rağmen zorluk seviyesini arttıracağı düşünülmektedir. Bu algoritmanın gelecekte daha ayrıntılı olarak tartışılarak güvenliğe olan katkılarının araştırılması umulmaktadır.

5. Sonuçlar ve Değerlendirme

Bilgi güvenliği, tüm alanlarda kullanıcılar arasında iletişimin en önemli unsurudur. Şifreleme, şifre çözme ve anahtar oluşturma algoritmalarının standart RSA dan farklı olarak çoklu asal sayı ile gerçekleşerek veriler için maksimum güvenliği sağlamak hedeflenmiştir. Yapılan çarpanlara ayırma uygulamalarında, GNFS, modül N'i oluşturan çoklu asal çarpanlara ulaşılamadığı gözlenmiştir. Çoklu asal kullanımı sayesinde küçük aygıtlarda kullanılabilecek kolay kırılmayan şifreleme gerçekleşeceği ve bunun için çok büyük sayılara ihtiyaç duyulmayacağı düşünülmektedir. Farklı asal sayı kümeleri ile çalışma geliştirilmeli ve sonuçları karşılaştırılmalıdır. Aslında şifreleme tekniklerinin hepsi bilinen tüm saldırılara karşı tamamen güvende değildir. Gelecekteki teknolojik gelişmeler doğrultusunda çarpanlara ayırmada gücü çok yüksek aygıtlar ya da yeni bir çarpanlara ayırma algoritması geliştirilmesi durumunda

çok güçlü ve çoklu asal sayılarla çalışan şifrelemeye ihtiyaç doğabilir.

6. Kaynakça

Aksuoğlu, A. (2010). Rsa algoritmasının iyileştirilmesi için yeni bir yaklaşım (Doctoral dissertation, Anadolu University (Turkey))

Anonim,TubitakAçıkAnahtarAltyapısıEğitimKitabı,2010. http://www.kamusm.gov.tr/tr/bilgideposu/belgeler/teknik/aaa/index.html?kriptoanalizyontemleri.html

Chaudhury, P., Dhang, S., Roy, M., Deb, S., Saha, J., Mallik, A., ... & Das, R. (2017, August). ACAFP: Asymmetric key based cryptographic algorithm using four prime numbers to secure message communication. A review on RSA algorithm. In *2017 8th Annual Industrial Automation and Electromechanical Engineering Conference (IEMECON)* (pp. 332-337). IEEE.

Compaq 2000 Cryptography using Compaq Multiprime technology in a parallel processing environment ftp://ftp.compaq.com/pub/solutions/CompaqMultiPrimeWP.pdf

Hinek, M. J. (2008). On the security of multi-prime RSA. *Journal of Mathematical Cryptology*, *2*(2), 117-147.

Hinek, M. J., Low, M. K., & Teske, E. (2003). On some attacks on multi-prime RSA. In Selected Areas in Cryptography: 9th Annual International Workshop, SAC 2002 St. John's, Newfoundland, Canada, August 15–16, 2002 Revised Papers 9 (pp. 385-404). Springer Berlin Heidelberg.

https://math.berkeley.edu/~kpmann/encryption.pdf

Ivanov, A., & Stoianov, N. (2023). Implications of the Arithmetic Ratio of Prime Numbers for RSA Security. *International Journal of Applied Mathematics and Computer Science*, *33*(1), 57-70.

Ivy, B. P. U., Mandiwa, P., & Kumar, M. (2012). A modified RSA cryptosystem based on 'n'prime numbers. *International Journal Of Engineering And Computer Science*, *1*(2), 63-66.

Kamardan, M. G., Aminudin, N., Che-Him, N., Sufahani, S., Khalid, K., & Roslan, R. (2018, April). Modified Multi Prime RSA Cryptosystem. In *Journal of Physics: Conference Series* (Vol. 995, No. 1, p. 012030). IOP Publishing.

Liestyowati, D. (2020, March). Public key cryptography. In *Journal of Physics: Conference Series* (Vol. 1477, No. 5, p. 052062). IOP Publishing.

Lone, A. H., & Khalique, A. (2016). Generalized RSA using 2k prime numbers with secure key generation. *Security and communication networks*, *9*(17), 4443-4450.

Mahto, D., Khan, D. A., & Yadav, D. K. (2016, June). Security analysis of elliptic curve cryptography and RSA. In *Proceedings of the world congress on engineering* (Vol. 1, pp. 419-422).

Mann, C. C. (2002). A Primer in Public-Key Encryption. *The Atlantic*.

Mathur, H., & Alam, Z. (2015). Analysis in symmetric and asymmetric cryptology algorithm. *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, *4*(1).

Mollin, Richard A. 2002. RSA and PUBLIC-KEY CRYPTOGRAPHY. Florida, Boca Raton:CRC Press LLC.

Rivest, R. L., & Silverman, R. D. (1999). AreStrong'Primes Needed for RSA?

Stallings, W. (2006). Cryptography and network security principles and practices 4th edition.

Tuncal, T. (2008). Bilgisayar güvenliği üzerine bir araştırma ve şifreleme-deşifreleme üzerine uygulama (Master's thesis, Maltepe Üniversitesi, Fen Bilimleri Enstitüsü).

Wolf, C., & Preneel, B. (2004). Asymmetric cryptography: Hidden field equations. *Cryptology ePrint Archive*.