Karadeniz Fen Bilimleri Dergisi, 15(1), 536-549, 2025. DOI: 10.31466/kfbd.1612836

KFBD

Karadeniz Fen Bilimleri Dergisi
The Black Sea Journal of Sciences
ISSN (Online): 2564-7377 https://dergipark.org.tr/tr/pub/kfbd

Araştırma Makalesi / Research Article

RSA ve Eliptik Matris Tabanlı Hibrit Şifreleme

Eyüp GEDİKLİ[1*], Şerife YILMAZ[2]

Öz

Özellikle kuantum bilgisayarların gelişimi, güvenliğe yönelik yeni algoritmalar ve yaklaşımlar üzerinde daha fazla araştırma yapılmasına yol açmıştır. Asimetrik şifrelemede yaygın olarak kullanılan RSA algoritmasının, Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından artık 2048 bit ve üzeri anahtarlarla kullanılması güvenli kabul edilmektedir. Küçük boyutlu anahtarlar kullanıldığında, birden fazla şifreleme yapılarak güvenlik artırılabilir. Ya da farklı yöntemleri bir arada kullanan hibrit yaklaşımlarla daha güvenli şifreleme sağlanabilir. Bu çalışmada, RSA yönteminin parametrelerine bağlı olarak açık anahtarlardan üretilen bir matris ile blok şifreleme yapılmıştır. Bu amaçla Euler'in totient fonksiyonu ile elde edilen açık anahtarlardan 2x2'lik bir eliptik matris üretilmiştir. Bu matrislerin terslerinin mevcut olması, blok şifrelemede kullanılabilir olmalarını sağlamıştır. RSA algoritmasında kullanılan asal sayılar 50'den küçük olduğunda, 2x2 boyutunda milyarlarca eliptik matris üretilebilir. Bu durum, 50 ile 100 arasındaki asal sayılar için 10^14'e ulaşır. Önerilen yöntemde küçük asal sayılar seçilerek birden fazla açık anahtar kullanılabilir. Bu açık anahtarlardan matris elemanları seçilirken tersinir eliptik matris oluşturma koşulu aranır. Bu eliptik matris kullanılarak blok şifreleme yapılabilir. Böylece hem RSA hem de blok şifreleme ile hibrit şifreleme yapılabilir. Bu hibrit şifrelemenin herhangi bir aşamasında, RSA veya eliptik matris herhangi bir sırada kullanılabilir. Eliptik matrislerin karekök matrislere sahip olması, kullanılan tüm anahtarların maskelenerek paylaşılmasına olanak tanır.

Anahtar Kelimeler: Blok şifreleme, Eliptik matris, Hibrit kriptografi, Hibrit sayılar, Maskeli anahtar paylaşımı, Matris karekökü.

RSA and Elliptic Matrix Based Hybrid Encryption

Abstract

In particular, the development of quantum computers in particular has led to more research on new algorithms and approaches to security. The RSA algorithm, widely used in asymmetric encryption, is now considered secure by the National Institute of Standards and Technology (NIST) when used with keys of 2048 bits or higher. When keys with small sizes are used, security can be increased by performing multiple encryptions. Besides that, encryption which is more secure can be provided with hybrid approaches that use different methods together. In this study, block cipher has been performed with a matrix generated from public keys depending on the parameters of RSA method. For this purpose, a 2x2 elliptic matrix has been generated from the public keys obtained with Euler's totient function. The fact that these matrices can be inverted allowed them to be used in block cipher. When the prime numbers used in RSA algorithm are less than 50, billions of elliptic matrices of dimension 2x2 can be generated. The number of suitable elliptic matrices reaches 10^14 for the prime numbers between 50 and 100. In the method we have proposed, multiple public keys can be used by selecting small prime numbers. When selecting matrix elements from these public keys, the condition of creating an invertible elliptic matrix is required. Block cipher can be done using this elliptic matrix. Thus, a hybrid encryption can be done with both RSA cipher and block cipher. At any stage of this hybrid encryption, RSA or elliptic matrix can be used in any order. The fact that elliptic matrices have square root matrices allows all keys used to be shared by masking.

Keywords: Block cipher, Elliptic matrix, Hybrid cryptography, Hybrid numbers, Masked key sharing, Square root of matrix.

[1]Karadeniz Teknik Üniversitesi, Yazılım Mühendisliği, Of Teknoloji Fakültesi, Trabzon, Türkiye, gediklie@ktu.edu.tr
[2]Karadeniz Teknik Üniversitesi, Matematik, Fen Fakültesi, Trabzon, Türkiye, serifeyilmaz@ktu.edu.tr

[*]Sorumlu Yazar/Corresponding Author

Geliş/Received: 03.01.2025 **Kabul/Accepted:** 15.02.2025 **Yayın/Published:** 15.03.2025

Gedikli, E., Yılmaz, Ş. (2025). RSA ve Eliptik Matris Tabanlı Hibrit Şifreleme. *Karadeniz Fen Bilimleri Dergisi*, 15(1), 536-549.

1. Giriş

Kriptografinin bilinen en eski kullanımı, MÖ 1900 civarında Eski Mısır Krallığı'na ait bir mezarın duvarına oyulmuş standart dışı hiyerogliflerde bulunmuştur (URL-1, 2024). Roma İmparatoru Jül Sezar, MÖ 1. yüzyılda, askeri iletişimde gizliliği sağlamak amacıyla Sezar şifresini geliştirmiştir. 16. yüzyılda, Fransız diplomat Blaise de Vigenère tarafından daha karmaşık ve güvenli bir şifreleme yöntemi Vigenère şifresi geliştirilmiştir (URL-2, 2024). II.Dünya Savaşı sırasında, Almanya'nın Enigma makinesi, şifreleme teknolojisinin önemli bir simgesi haline gelmişti (URL-3, 2024). 19.yüzyılın sonlarında Charles Babbage ve Augustus De Morgan gibi matematikçiler, şifreleme üzerine teoriler geliştirmeye başlamışlardır (Silverman, 1991). Claude E. Shannon, çalıştığı Bell Labs'da, "Kriptografinin matematiksel teorisi" başlıklı bir makale yayınlamıştır (Shannon, 1949). Shannon birçok kişi tarafından matematiksel kriptografinin babası olarak kabul edilir.

Günümüzde kriptografi, bilgileri şifrelemek ve şifresini çözmek için bir anahtara sahip algoritmalar kullanılarak yapılmaktadır. Bu anahtarlarla, veriler şifreleme yoluyla "dijital anlamsızlığa" dönüştürülür ve ardından şifre çözme yoluyla orijinal biçimine döndürülür. 1976'da, Whitfield Diffie ve Martin Hellman, açık anahtar şifreleme konseptini tanıtarak bugünkü şifreleme yöntemlerinin temelini atmışlardır (Diffie ve Hellman, 1976). “New Directions in Cryptography” adlıyla yayınlanan çalışmaları, kripto sistemlerinin çalışma biçimini kökten değiştirerek asimetrik anahtar algoritmalarının gelişimine yol açmıştır (Diffie ve Hellman, 1976). Ron Rivest, Adi Shamir ve Leonard Adleman tarafından 1977'de geliştirilen RSA algoritması (Rivest vd., 1978), bugün hala birçok dijital güvenlik uygulamasında kullanılan en yaygın açık anahtar şifreleme yöntemlerinden biridir (Robinson, 2003). RSA, asal sayılar ve büyük sayıların çarpanlarına ayırma probleminden ötürü kırılması zor bir algoritmadır. Öte yandan, daha küçük anahtar boyutlarıyla aynı güvenlik seviyesini sağlayan Eliptik Eğri Kriptografisi (ECC), Neal Koblitz ve Victor S. Miller tarafından 1985'te, ayrı ayrı önerilmiştir (Miller, 1985; Koblitz, 1987). Eliptik eğri protokollerinde, eliptik eğrinin bilinen bir noktasına göre ayrık logaritmasının bulunmasının imkânsız olduğu varsayılmaktadır. Eliptik eğrinin güvenliği, nokta çarpımının hesaplanma hızına ve başlangıç noktası ile çarpım noktasına bakarak elde edilen noktanın hesaplanamamasına dayanmaktadır. Buna “Eliptik Eğrinin Ayrık Logaritma Problemi” denir. Eliptik eğriler üzerindeki noktalara, genellikle nokta toplama veya skaler çarpma şeklinde ifade edilen işlemler uygulanır. Bir noktayı skaler bir sayıyla çarparak özel anahtar (private key) elde edilebilir. Bu özel anahtarlar kullanılarak bir anahtar çiftine ulaşılır (Hankerson vd., 2004). Eliptik eğrinin boyutu aynı zamanda problemin zorluğunu da belirler. Özellikle kuantum bilgisayar tehditlerine ECC’nin daha dayanıklı olduğu savunulmaktadır. Küçük anahtar boyutu sayesinde, özellikle mobil, IoT (Internet of Things) cihazları, SSL/TLS sertifikaları ve Blockchain teknolojileri gibi yerlerde daha yaygın olarak kullanılır.

RSA algoritması, yıllardır şifreleme ve dijital imza işlemlerinde yaygın olarak kullanılan bir yöntemdir. Ancak teknolojik ilerlemeler ve hesaplama gücündeki artış nedeniyle RSA'nın güvenliği tartışma konusu olmuştur. Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technology-NIST), şu anda 2048 bit ve üzeri uzunluklara sahip genel anahtar kullanarak RSA ile güvenliği sağlama yoluna gitmektedir. Ayrıca, SHA-3 ve daha güvenli alternatifler ile birlikte yeni güvenlik protokolleri benimsenmektedir (URL-4, 2024). RSA, Shor's algoritması adı verilen bir yöntemle kuantum bilgisayarlar tarafından kolayca çözülünce, gelecekte güvenlik tehdidi oluşturabileceği düşünülmektedir. Eliptik eğri dijital imza algoritması (Elliptic Curve Digital Signature Algorithm, ECDSA), RSA'ya göre daha kısa anahtarlar kullanarak benzer seviyede güvenlik sağlarken daha yüksek performans gösterir. RSA, özellikle 2048 bit veya üzeri anahtar uzunlukları kullanıldığında hala güvenli kabul edilmektedir. Ancak performans, kuantum bilgisayarlar ve hesaplama yükü nedeniyle gelecekte daha güvenli alternatifler benimsenebilir. NIST, RSA'nın şu anda güvenli bir standart olarak kullanılmasını desteklemesine rağmen gelecekteki olabilecek tehditlere karşı, yeni algoritmalar üzerinde çalışmalarını sürdürmektedir. Günümüzde RSA, yaygın olarak TLS/SSL gibi güvenli iletişim protokolleri, dijital imzalama ve kimlik doğrulama için kullanılmaya devam etmektedir.

Blok şifreleme, sabit uzunluktaki bit grupları üzerine simetrik anahtar ile belirlenmiş bir deterministik algoritmanın uygulanmasıdır (Menezes vd., 1997; Bellera ve Rogaway, 2005). Blok şifreleme, birçok kriptografik protokol tasarımının önemli temel bileşenlerindendir ve dosya şifreleme, veri tabanı şifreleme, VPN ve disk şifreleme gibi büyük boyutlu verilerin şifrelemesinde, yaygın biçimde kullanılmaktadır. Blok şifrelemede, tüm bloklar genelde aynı anahtar ile şifrelenir. Kullanılan anahtar genelde açık metin bloklarıyla aynı boyutta ve blok şeklinde olur. Matris tabanlı şifreleme de bir blok şifreleme türüdür, verileri bir matris işlemi kullanarak şifrelemeye yarar ve genellikle lineer cebir prensiplerine dayanır (Bellare ve Rogaway, 2005; Hoffstein vd., 2014).

Günümüzde şifreleme, anahtar yönetimi (key management), hız ve performans, zayıf şifreleme algoritmaları, yasal düzenlemeler ve "backdoor" talepleri, kullanıcı hataları, kuantum bilgisayarların yükselişi, man-in-the-middle saldırıları, büyük veri ve cloud (bulut) ortamlarında güvenlik, standartlar ve protokoller, sosyal mühendislik saldırıları gibi bazı önemli problemlerle karşı karşıyadır. Bu nedenle şifreleme sistemlerinin sürekli geliştirmesi ve iyileştirmesi gerekmektedir. Yeni yöntemlerin yetmediği durumlarda daha yüksek güvenlik için tekrarlı şifreleme yaklaşımları kullanılabilir. Bu yaklaşımlar; çift şifreleme (double encryption), çift anahtar kullanımı (double key encryption), karmaşık tekrarlı şifreleme, farklı yöntemlerin bir arada kullanılmasıyla hibrit şifreleme şeklinde sınıflandırılabilir.

Bu çalışmada, RSA'da seçilen iki büyük asal sayıya dayalı olarak üretilebilen anahtarlardan birden fazla kullanılması temel alınmıştır. Seçilen genel anahtarlardan, eliptik matris şartlarını

sağlayanlar belirlenmiştir. Eliptik matrislerin tersi alınabilir ve karekök matrisleri vardır. Bu sayede eliptik matrisler blok şifreleme için kullanabilmiştir. RSA'da anahtar açık olarak paylaşılır. Bu yöntemde anahtarlar karekök matris şeklinde paylaşılarak daha güvenli anahtar paylaşımı sağlanabilmektedir. Çalışmada, RSA ile şifreleme ve blok şifreleme farklı sıralarda yapılarak şifreleme işlemi daha karmaşık hale getirilebilir.

2. Materyal ve Metot

Kriptografide, işlenmemiş bilgi olan açık metin (plaintext), şifrelenmiş, dönüştürülmüş bilgi olan şifreli metin (ciphertext), şifreleme ve şifre çözme için kullanılan anahtar (key), şifreleme işlemi (encryption) ve tekrar açık metne dönüştürme işlemi şifre çözme (decryption) temel kavramları kullanılır. Şifreleme türleri, simetrik şifreleme (symmetric encryption), asimetrik şifreleme (asymmetric encryption) ve hashleme (hashing) olarak üçe ayrılabilir. Simetrik şifrelemede (AES, DES, 3DES), aynı anahtar hem şifreleme hem de şifre çözme için kullanılır. Asimetrik şifrelemede (RSA, ECC) açık anahtar (public key) ve özel anahtar (private key) olmak üzere iki anahtar şifreleme ve deşifreleme için ayrı ayrı kullanılır. Şifreleme işlemlerinde genellikle kimlik doğrulama için kullanılan hashleme (MD5,SHA-256), bilgilerin tek yönlü dönüşümüdür ve deşifreleme yapılamaz (Stalling, 2017; URL-4, 2024).

2.1. Rivest-Shamir-Adleman (RSA) Algoritması

1977'de Ron Rivest, Adi Shamir ve Leonard Adleman tarafından geliştirilmiş olan RSA, şifreleme ve deşifreleme için farklı anahtarlar kullanan asimetri şifreleme yöntemlerinden biridir (Rivest vd., 1978). RSA algoritması şu adımlarla gerçeklenir:

- Çarpımlarından n'yi hesaplamak için p ve q diye adlandırılan iki büyük asal sayı seçilir ($n=p\times q$).
- $\phi(n)=(p-1)(q-1)$ hesaplanarak $1<e<\phi(n)$ koşulunda $\phi(n)$ ile arasında asal bir e sayısı seçilir.
- $e.d\equiv 1 \bmod \phi(n)$ koşulunu sağlayan d hesaplanır. d, e için modüler çarpmayı tersine çeviren bir sayıdır.
- Böylece açık anahtar(e,n) ve özel anahtar(d,n) elde edilmiş olur.
- Açık anahtar (e,n) kullanılarak M açık metni $C = M^e \bmod n$ şeklinde şifrelenerek C şifreli metin (ciphertext) elde edilir.
- Özel anahtar (d,n) kullanılarak $M = C^d \bmod n$ ile C den orijinal mesaj M geri elde edilebilir.

2.2. Blok Şifreleme

Blok şifreleme algoritmaları, şifreleme için (*E*) ve şifreyi çözmek için (*D*) işlemlerinden oluşur (Cusick ve Stanica, 2017). İşlemler, *n* bit uzunluğunda bir blok ve *k* bit uzunluğunda bir anahtardan oluşan iki adet girdi alır. İşlemler, *n* bit uzunluğunda blok çıktı üretir. Şifre çözme işlemi (*D*), şifrelemenin ters fonksiyonudur ($D = E^{-1}$). Biçimsel olarak şifreleme fonksiyonu Denklem 1 ile temsil edilmiştir (Bellare ve Rogaway, 2005; Menezes vd., 1997).

$$C = E_K(P) := E(K,P): \{0,1\}^n \; x \; \{0,1\}^n \rightarrow \; \{0,1\}^n \tag{1}$$

Denklem 2'deki fonksiyon, girdi olarak *k* bit anahtar uzunluğuna sahip anahtar (*K*) ve *n* bit blok uzunluğuna sahip *P* dizisini alarak, *n* bitlik *C* dizisini üretir. *P* şifresiz metin ve *C* ise şifreli metin olarak adlandırılır. Her *K* için, $E_K(P)$ fonksiyonu $\{0,1\}^n$ üzerinde tersi alınabilir olmalıdır. *E* fonksiyonunun tersi Denklem 2'de verilmiştir.

$$E_K^{-1}(C) := D_K(C) = D(K,C): \{0,1\}^k \; x \; \{0,1\}^k \rightarrow \; \{0,1\}^k \tag{2}$$

Denklem 2'te, *K* anahtar, *C* şifreli metin ve *P* geri elde edilmiş şifresiz metindir. Blok şifreleme ve deşifreleme $\forall K: D_K\big(E_K(P)\big) = P$ şeklinde genel ifade edilebilir.

2.3. Hibrit Sayılarla Matris Karekökü

Hibrit sayılar, karmaşık, hiperbolik ve dual sayıların bir genellemesidir. Bir hibrit sayı, eliptik, hiperbolik veya parabolik olarak sınıflandırılabilir (Özdemir, 2018; Şık, 2020).

Tanım 1. (Özdemir, 2018) Hibrit sayılar kümesi *K* ile gösterilir ve Denklem 3 biçiminde tanımlanır.

$$K = a + bi + c\varepsilon + dh, \qquad \begin{matrix} a,b,c,d \in R, \\ i^2 = -1, \varepsilon^2 = 0, h^2 = 1, \\ ih = -hi = \varepsilon + i \end{matrix} \tag{3}$$

Herhangi bir $Z = a + bi + c\varepsilon + dh$ hibrit sayısı için, *a* değerine skaler kısım denir ve *S(Z)* ile gösterilir. *V(Z)* ile gösterilen $bi + c\varepsilon + dh$ kısmına hibrit sayının vektör kısmı denilir. Herhangi bir $Z = a + bi + c\varepsilon + dh$ hibrit sayısının eşleniği $\overline{Z} = S(Z) - V(Z) = a - bi - c\varepsilon - dh$ biçiminde tanımlanır. Hibrit sayılarda çarpım işlemi aşağıdaki Tablo 1'e göre yapılır.

Tablo 1. Hibrit sayıların çarpma işlemi.

.	*i*	*ε*	*h*
i	*-1*	*1-h*	*ε+1*
ε	*h+1*	*0*	*-ε*
h	*-ε-1*	*ε*	*1*

Tanım 2. $Z = a + bi + c\varepsilon + dh$ bir Z hibrit sayısı için türlük sayısı reeldir ve Denklem 4 ile hesaplanır (Özdemir, 2018). $\Delta(Z)$ türlük sayısının değerine göre türler belirlenir (Denklem 5).

$$\Delta(Z) = -(b-c)^2 + c^2 + d^2 \tag{4}$$

$$\begin{cases} Z\ eliptik & \Delta(Z) < 0\ ise; \\ Z\ hiperbolik & \Delta(Z) > 0\ ise; \\ Z\ parabolik & \Delta(Z) = 0\ ise. \end{cases} \tag{5}$$

Teorem 1. (Özdemir, 2018) *A* matrisi, *Z* hibrit sayısına karşılık gelen *2x2* türünden reel girdili matris olsun. Bu durumda aşağıdaki eşitlikler sağlanır:

- $\rho = \left||Z|\right| = \sqrt{\det(A)}$,
- $\Delta(Z) = \left(\frac{izA}{2}\right)^2 - \det A$
- $P(\lambda) = \lambda^2 - (izA)\lambda + detA,\ \Delta_A = (izA)^2 - 4detA = 4\Delta(Z)$ değeri, *A* matrisininin karakteristik polinomudur.
- Z^{-1} sayısının tanımlı olması için gerek ve yeter koşul $\det(A) \neq 0$ olmasıdır.

Bu Teorem'e göre, determinant ve izine bağlı olarak *2x2* matrisler sınıflandırılabilir. Bu sınıflandırma $\Delta_A = (izA)^2 - 4detA$ olmak üzere, Denklem 6'ye denktir.

$$\begin{matrix} A\ eliptik & \Delta_A < 0\ ise; \\ A\ hiperbolik & \Delta_A > 0\ ise; \\ A\ parabolik & \Delta_A = 0\ ise. \end{matrix} \tag{6}$$

Teorem 2. $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ bir reel matris olsun. Eğer, *A* bir eliptik matris ise, *A* matrisinin iki tane karekökü vardır (Özdemir, 2019; Şık, 2020). Bu kökler Denklem 7 ile hesaplanabilir.

$$\sqrt{A} = \pm \frac{1}{\sqrt{izA + 2\sqrt{detA}}} \begin{bmatrix} a + \sqrt{detA} & b \\ c & d + \sqrt{detA} \end{bmatrix} \tag{7}$$

Bir hibrit sayının karekökü, hibrit sayının parabolik, eliptik ve hiperbolik türlü olmasına ve bunların yanında timelike, spacelike veya lightlike karakterlerinde olmasına göre değişmektedir (Özdemir, 2018). Hibrit sayılar yardımıyla verilen yönteme göre, bir matrisinin reel köklerinin sayısı matrisin türüne ve karakterine göre sınıflandırılabilir (Özdemir, 2018). Buna göre, bir matrisin karekökü olmayabileceği gibi, 1, 2, 4 veya sonsuz çoklukta karekökü olabilir. Bunlardan eliptik sınıfındaki matrislerin karekökü, mutlakları birbirine eşit iki tane çıkmaktadır (Özdemir, 2019).

3. Bulgular ve Tartışma

Bu çalışmada, RSA algoritmasının genel anahtarları ile oldukça fazla sayıda eliptik matris üretilebildiği ve eliptik matrislerin karekökünün bulunması sunulmuştur. Eliptik matrislerin zıt işaretli tek karekök matrisi vardır (Denklem 7).

3.1. RSA Genel Anahtarlarının Bulunması

RSA algoritması, büyük asallarla çalışılarak güvenlik sağlamaktadır. Burada alt seviye sistem üzerindeki testler için $p=19$ ve $q=23$ alınarak bir örnek verilmektedir. Tablo 3'te, bazı farklı küçük (p,q) değerleri için olabilecek genel anahtar sayıları verilmiştir.

$p=19$ ve $q=23$ değerleri için olabilecek RSA anahtarlarını oluşturalım. RSA için modüler alan $n=p\times q$ den $n=437$ olarak hesaplanır. Euler'in totient fonksiyonuyla $\phi(n)=(p-1)\times(q-1)$ eşitliğinden $\phi(n)=18\times22=396$ elde edilir. $1<e<\phi(n)$ ve $gcd(e,\phi(n))=1$ koşulunu sağlayan sayılar genel anahtarın e değerleri olabilir. Özel anahtarın d değeri, $e\cdot d\equiv1 \pmod{\phi(n)}$ modüler terslik koşulunu sağlamalıdır.

Tablo 2. $(p, q)= (19,23)$ için (e,d) çiftleri.

(5,317)	(7,283)	(13,61)	(17,233)	(19,271)	(23,155)	(25,301)	(29,41)	(31,115)	(35,215)	(37,289)
(41,29)	(43,175)	(47,59)	(49,97)	(53,269)	(59,47)	(61,13)	(65,329)	(67,331)	(71,251)	(73,217)
(79,391)	(83,167)	(85,205)	(89,89)	(91,235)	(95,371)	(97,49)	(101,149)	(103,223)	(107,359)	(109,109)
(113,389)	(115,31)	(119,203)	(125,377)	(127,343)	(131,263)	(133,265)	(137,185)	(139,151)	(145,325)	(149,101)
(151,139)	(155,23)	(157,169)	(161,305)	(163,379)	(167,83)	(169,157)	(173,293)	(175,43)	(179,323)	(181,361)
(185,137)	(191,311)	(193,277)	(197,197)	(199,199)	(203,119)	(205,85)	(211,259)	(215,35)	(217,73)	(221,353)
(223,103)	(227,239)	(229,313)	(233,17)	(235,91)	(239,227)	(241,373)	(245,257)	(247,295)	(251,71)	(257,245)
(259,211)	(263,131)	(265,133)	(269,53)	(271,19)	(277,193)	(281,365)	(283,7)	(287,287)	(289,37)	(293,173)
(295,247)	(299,347)	(301,25)	(305,161)	(307,307)	(311,191)	(313,229)	(317,5)	(323,179)	(325,145)	(329,65)
(331,67)	(335,383)	(337,349)	(343,127)	(347,299)	(349,337)	(353,221)	(355,367)	(359,107)	(361,181)	(365,281)
(367,355)	(371,95)	(373,241)	(377,125)	(379,163)	(383,335)	(389,113)	(391,79)	(395,395)		

$p=19$ ve $q=23$ alındığında, e değerlerini belirlemek için, $1< e <396$ aralığında, 396 sayısıyla aralarında asal olan sayıları belirlememiz gerekmektedir. 396'nın asal çarpanları 2 ve 3'tür. Yani, e değerleri 2 ve/veya 3 bölünemeyen sayılar olarak seçilir. Buradan $gcd(e,396)=1$ koşulunu sağlayan

119 tane *e* sayısı belirlenebilir. Tanım gereği, modüler terslik koşuluna göre her *e* için bir *d* elde edilebilir. Buna göre e değerleri ve onlara karşılık olabilecek *d* değerleri için Tablo 2'de *(e,d)* çiftleri verilmiştir. Tablo 2'de, RSA algoritmasında $p=19$ ve $q=23$ olduğunda seçilebilecek genel ve özel anahtar *(e,d)* çiftlerinden 7 tanesi birbirine eşittir ve *56* tanesi simetriktir.

3.2. *e*'lerden *2x2*'lik Eliptik Matris Oluşturma

Tanım 2'ye göre bir matrisin eliptik olması için, $\Delta_A < 0$ veya $\Delta_Z < 0$ ve $\det(A) \neq 0$ koşulu sağlanmalıdır. Şekil 1'deki sözde kod ile, genel anahtarların bulunduğu E dizi elemanlarının tüm kombinasyonları ile *2x2* lik matrisler oluşturulup, eliptik matris koşulunu sağlayan ve tersi alınabilen matrisler belirlenmiştir.

```
E % dizisi genel anahtarların e'lerinden oluşmaktadır.
for each i,j,m,n in E
        EM = [E_i  E_j ; E_m  E_n]
        Δ(Z) = −(E_j − E_m)^2 + E_m^2 + E_n^2    //Hibrit sayının hesaplanması

        if Δ(Z) < 0 & det(EM)<0
                EM          //Tersinir Eliptik matris
        end
end
```

Şekil 1. 2x2 boyutlu eliptik matris bulan sözde kod

Tablo 2'deki, $p=19$ ve $q=23$ değerlerinden üretilebilen *119* adet genel anahtara göre *119!*119!*119!*119!* adet *2x2*'lik matris oluşturulabilir. Şekil 1'deki sözde kod ile bu kombinasyonlardan *21.570.913* adet tersi olan eliptik matris belirlenebilmiştir. Eliptik matris elemanlarının *2* veya *3*'ü eşit olabilmekte veya hepsi farklı olabilmektedir. $(p,q)=(19,23)$ için *21.570.913* eliptik matrisin, *2* elemanı eşit *869.827* tane, *3* elemanı eşit *2859* tane ve elemanların tamamı birbirinden farklı *20.698.227* tane matris vardır.

p ve *q* değerlerinin farklı seçimleri için genel anahtar ve oluşabilecek eliptik eğri sayıları Tablo 3'te verilmiştir. Tablonun ilk sütununda RSA algoritması için oldukça küçük olan *p* ve *q* asalları verilmiştir. Tabloda $\phi(n)$ sayısı ile *e*'lerin sayısı arasında bir doğru orantı gözükmemektedir. Bu ilişki daha büyük sayılarda, çarpanlardan ötürü doğru orantıya sahip olabilir. Benzer şekilde, *e*'lerin sayısının aynı olduğu durumlarda eliptik matris sayıları da aynı değildir. Tersi olan eliptik matrislerde, *2* elemanı eşit, *3* elemanı eşit ve *4* elemanı da farklı olanlar ayrı sütunlarda verilmiştir. *4* ve *2*'şer elemanı eşit matrisler tersinir eliptik matris değildir. Tablo 3'te en önemli nokta, $\phi(n)$ ve *e*'lerin sayısına göre eliptik matris sayıları üstel olarak artmaktadır. Tabloda 50'nin altındaki *(p,q)*

değerleri için hesaplamalar yapılmış, daha yüksek değerlerde uzun hesaplama süresine ve yüksek bellek kapasitesine ihtiyaç duyulmaktadır.

Tablo 3. Bazı *p* ve *q* için, *e* ve eliptik matris sayıları.

(p, q)	*ϕ(n)*	***e*'lerin sayısı**	**2 eleman eşit (3 farklı e)**	**3 elemanı eşit (2 farklı e)**	**Tüm elemanlar farklı (4 farklı e)**	**Eliptik matris sayısı**
(5, 13)	48	15	1241	38	2985	4264
(7, 13)	72	23	5154	96	20901	26151
(11, 13)	120	31	13404	180	76366	89950
(7, 17)	96	31	13481	181	76768	90430
(11, 19)	180	47	49844	429	447857	498130
(5, 29)	112	47	50067	431	449608	500106
(7, 41)	240	63	123983	786	1,52E+06	1,65E+06
(13, 17)	192	63	124090	786	1,52E+06	1,65E+06
(13, 23)	264	79	248513	1244	3,87E+06	4,12E+06
(5, 71)	280	95	437411	1811	8,25E+06	8,69E+06
(19, 23)	396	119	869827	2859	2,07E+07	2,16E+07
(13, 41)	480	127	1,06E+06	3266	2,70E+07	2,81E+07
(11, 61)	600	159	2,10E+06	5145	6,72E+07	6,93E+07
(19, 37)	648	215	5,24E+06	9449	2,28E+08	2,33E+08
(37, 43)	1512	431	4,27E+07	38216	3,75802E+14	3,8008E+14

Tanım gereği, *2x2*'lik eliptik matrislerin ters işaretli eşit iki karekökü vardır. Tablo 4'de, *p=19* ve *q=23* için *119* genel anahtardan üretilmiş *21.570.913* adet eliptik matrislerden bazı örnekler, örnek matrisin tersi ve örnek matrisin hibrit sayıya dayalı olarak hesaplanmış pozitif karekök matrisleri verilmiştir. Karekök matrislerin karesi orijinal matrisi sağlamaktadır. Negatif karekök matrislerin karesi de aynı olacağından ayrıca verilmemiştir.

Tablo 4'deki eliptik matrislerin belirli bir patterninin olmadığını görebiliriz. Bu farklı zorlukta RSA genel anahtarlar sayısı belirlemeye imkan verir. Tablo 3'te farklı *(p,q)* değerleri için *e*'lerden oluşabilen tersinir *2x2* boyutlarında eliptik matris sayısı ve özellikleri verilmiştir. Buradan, genel anahtarlardan farklı sayılarda seçerek *2x2* boyutlarında eliptik matris oluşturulabileceği görülmektedir. Genel anahtarlarla RSA'ya göre şifrelenip bloklara ayrılan şifreli metin, eliptik matrislerle blok şifrelemeye tabi tutulabilir. Ya da blok şifreleme daha önceki safhalarda gerçekleştirilebilir. Şifre çözerken işlem sırasının tersi yapılarak açık metin elde edilebilir. Blok şifrelemenin herhangi bir sırada yapılabilmesi, farklı RSA genel anahtarlarından blok şifreleme anahtarı oluşturulabilmesi, RSA'ya göre nispeten daha küçük birden fazla asal sayılar kullanılabilmesi, genel ve blok anahtarın karekök olarak paylaşılarak gizlenmesi gibi farklı hibrit krigtografi yöntemleri geliştirilebilir.

Tablo 4. *(p,q)=(19,23)* için tersinir *2x2* Eliptik matris ve mutlak karekök matrisleri.

Eliptik Matris (*EM*)	**Tersi ($(EM)^{-1}$)**	***Eliptik Matris Pozitif İşaretli Karekökü***
[23, 389; 179, 73]	[-0,00107428773251707, 0,00572462914998823; 0,00263421238521309, -0,000338474217094420]	[8,01231643487116 + 8,06124740695431i, 12,9834656945707 - 10,8110102378158i; 5,97439681061221 - 4,97473221740109i, 9,68114235962318 + 6,67165740209367i]
[61, 373; 109, 145]	[-0,00455802841694958, 0,0117251351691186; 0,00342637998239658, -0,00191751540299258]	[6,99649648155433 + 6,10814450893582i, 15,9162970467711 - 9,18819537530526i; 4,65114310482052 - 2,68502224104095i, 10,5808636449023 + 4,03895305712445i]
[83, 367; 67, 139]	[-0,0106497088568802, 0,0281182960465829; 0,00513331290223721, -0,00635917866993564]	[6,77527313168250 + 4,08527015314373i, 18,9393199625065 - 8,00524207174393i; 3,45758702312788 - 1,46144746268895i, 9,66519661369983 + 2,86376182612013i]
[101, 361; 23, 163]	[0,0199754901960784, -0,0442401960784314; -0,00281862745098039, 0,0123774509803922]	[9,07345218513776, 17,1194778786834; 1,09071465709063, 12,0136395216429]
[119, 353; 101, 41]	[-0,00133229349450835, 0,0114707220380841; 0,00328199129134984, -0,00386690063040229]	[9,92889516706042 + 4,23631107071912i, 15,1199969720631 - 9,72277857644738i; 4,32611811381975 - 2,78187149071157i, 6,58793266331843 + 6,38468707344687i]
[139, 347; 23, 181]	[0,0105367330306206, -0,0202002561415764; -0,00133892187681919, 0,00809174525555944]	[11,1933014701212, 14,3820098417785; 0,953274427553040, 12,9340634682615]
[161, 335; 59, 149]	[0,0352746212121212, -0,0793087121212121; -0,0139678030303030, 0,0381155303030303]	[10,7739488889361, 15,9707775982264; 2,81276381580704, 10,2018613331787]
[179, 325; 73, 205]	[0,0158057054741712, -0,0250578257517348; -0,00562837316885119, 0,0138010794140324]	[11,8414188634458, 13,1397961727274; 2,95140037110493, 12,8926025572640]
[221, 305; 35, 7]	[-0,000766871165644172, 0,0334136722173532; 0,00383435582822086, -0,0242112182296231]	[13,9348865731916 + 0,827044009477580i, 16,6188995306021 - 6,04312518626363i; 1,90708683138057 - 0,693473382030253i, 2,27441280417894 + 5,06713840246255i]
[239, 293; 95, 35]	[-0,00179763739085773, 0,0150487930148947; 0,00487930148947098, -0,0122752953261428]	[13,8739727465219 + 1,83023495968129i, 13,6619124443719 - 5,73244901858330i; 4,42963031472808 - 1,85864387974544i, 4,36192449173736 + 5,82142813302940i]
[299, 251; 23, 127]	[0,00394409937888199, -0,00779503105590062; -0,000714285714285714, 0,00928571428571429]	[17,0776111526615, 8,95921805337240; 0,820964204093885, 10,9382266698725]
[317, 233; 89, 47]	[-0,00805070229530662, 0,0399109284001371; 0,0152449468996232, -0,0542994176087702]	[16,3997190257547 + 0,619926686594114i, 11,4960082478601 - 2,31523770901381i; 4,39117911613539 - 0,884361184988107i, 3,07816440377095 + 3,30282016914231i]
[337, 215; 53, 103]	[0,00441756733573512, -0,00922113570080631; -0,00227311717275691, 0,0144535940984732]	[17,9363522646841, 7,87492138204520; 1,94125968952742, 9,36550759771397]
[395, 395; 193, 35]	[-0,000560807562890562, 0,00632911392405063; 0,00309245313251082, -0,00632911392405063]	[18,0406074415885 + 2,42940868317891i, 13,9836431448826 - 6,41462378178689i; 6,83251424547429 - 3,13423389844271i, 5,29602128422715 + 8,27564807923785i]

3.3. Uygulama Örneği

Önerimiz doğrultusunda şöyle bir hibrit yaklaşım kullanabiliriz. Mesajı ilk başta bloklara ayırıp, her bloktaki elemanı, eliptik matristeki karşılığı olan anahtar ile RSA algoritmasına göre şifreleyelim. Ardından bu RSA ile şifreli mesajı eliptik matris ile çarparak blok şifreleme yapalım. Bu şifreli mesaj alıcı tarafta, eliptik matris karekökünün karesi ve ardından tersi alınarak elde edilen matris ile çarpılsın. Bu işlem sonucunda RSA şifreli mesajı elde edilecektir. Özel anahtarlar kullanılarak, RSA deşifreleme her eleman için ayrı ayrı yapılınca mesaj geri elde edilmiş olacaktır.

p=19 ve *q=23* için Tablo 4'ün ilk satırındaki eliptik matrisi $EM = \begin{bmatrix} 23 & 389 \\ 179 & 73 \end{bmatrix}$ seçelim. Bu satırda, matrisin tersi ve karekökü de verilmiştir. Şifrelenecek mesajımız '*UZAY*' olsun. Bunu, ASCII karşılığı $Mesaj = \begin{bmatrix} 85 & 90 \\ 65 & 89 \end{bmatrix}$ şeklinde matris olarak gösterebiliriz. Mesajın her bir elemanı, RSA ile *EM* anahtarlarıyla ayrı ayrı şifrelensin (Denklem 9).

$$C_{Mesaj} = C_{RSA}(\text{Mesaj}, \text{EM}) = \begin{bmatrix} RSA(85, pk(23{,}437) & RSA(90, pk(389{,}437) \\ RSA(65, pk(179{,}437) & RSA(89, pk(73{,}437) \end{bmatrix} \quad (9)$$

$$C_{Mesaj} = \begin{bmatrix} 16 & 260 \\ 373 & 412 \end{bmatrix}$$

Denklem 9'da *pk(e,n)*, genel anahtarı temsil etmektedir. *RSA(açık_metin, anahtar)* fonksiyonu, *(açık_metin^e mod n)*'yi hesaplar. C_{RSA} şifrelenecek mesajı ve eliptik matrisi girdi olarak alır.
Ardından EM blok anahtarı ile blok şifreleme yapabiliriz. Bunun için RSA ile şifrelenmiş bloğu EM ile çarpmamız yeterlidir. Denklem 10 ile gönderilecek şifreli mesaj elde edilmiş olur.

$$CM_{RSA\_Blok} = C_{RSA}(Mesaj, EM) * EM = \begin{bmatrix} 46908 & 25204 \\ 82327 & 17573 \end{bmatrix} \quad (10)$$

Alıcıya CM_{RSA_Blok} mesajı ve *hibrit_anahtar=(karekök(EM), n)* gönderilir. Alıcı, normalde herkese açık olan genel anahtarları ve eliptik matrisi üretmek için karekök matrisin karesini alır. Daha sonra matrisin tersini *EM^{-1}=inverse(EM)*'yi hesaplar. Örnekte verilen eliptik matrisin tersi ve karekökü Tablo 4'te verilmiştir.
Blok şifrelemeyi çözmek için şifreli mesaj *EM^{-1}* ile çarpılır. Böylece blok şifre çözülerek RSA ile şifrelenmiş blok *(D_{RSA})* geri elde edilir (Denklem 11).

$$D_{RSA\_mesaj} = CM_{RSA_{Blok}} * EM^{-1} = \begin{bmatrix} 16{,}0 & 260{,}0 \\ 373{,}0 & 412{,}0 \end{bmatrix} \quad (11)$$

Daha sonra RSA deşifreleme yapılacaktır. Eliptik matristeki genel anahtarlara karşılık özel anahtarlar *DM=[155 113;323 217]* olacaktır(Tablo 2). Bu anahtarlar kullanılarak deşifrelenmiş mesaj Denklem 12 ile geri elde edilmiş olur.

$$D_{Mesaj} = D_{RSA}\left(D_{RSA\_mesaj}, \mathrm{DM}\right) = \begin{bmatrix} RSA(16, dk(155{,}437)) & RSA(260, dk(113{,}437)) \\ RSA(373, dk(323{,}437)) & RSA(412, dk(217{,}437)) \end{bmatrix} \quad (12)$$

$$D_{Mesaj} = \begin{bmatrix} 85 & 90 \\ 65 & 89 \end{bmatrix}$$

Denklem 12'de, *dk(d,n)* genel anahtarı temsil etmektedir. *RSA(gizli_metin, ozel_anahtar)* fonksiyonu, *(gizli_metin^d mod n)*'yi hesaplar. D_{RSA} deşifrelenecek mesajı ve yeniden elde edilmiş eliptik matrisi girdi olarak alır.

Bu örnekte önce RSA ile her eleman şifrelenmiş daha sonra blok şifreleme yapılmıştır. Elemanların tamamı için aynı anahtarlarla RSA şifreleme birden fazla yapılabilir. Veya 1-2 elemanı RSA ile şifreledikten sonra blok şifreleme, ardından tekrar diğer elemanları RSA ile şifreleme yapılabilir. Deşifreleme esnasında işlemlerin tersi sırada uygulanması yeterli olacaktır.

4. Sonuçlar ve Öneriler

RSA algoritması için NIST, artık en az *2048* bit uzunluğunda anahtar kullanılmasını önermektedir. Kuantum bilgisayar teknolojisindeki gelişmeler karşısında bu önlemin ne kadar başarılı olabileceği henüz kesin bilinememektedir.

Şifreleme, esasında veriyi anlaşılmaz hale getirip tekrar geri döndürebilmektir. Bu noktadan bakıldığında veriyi anlamsızlaştırmak için bilinen yöntemler karmaşık şekillerde uygulanarak güvenlik seviyesi artırılmıştır.

RSA büyük asal sayılarla çalışırken, matris üretimi için daha küçük asal sayıların kullanılması, birden fazla genel anahtarın *e* parametresi ile oldukça fazla sayıda eliptik matris üretilebildiği çalışmada görülmüştür. Bu durumda, daha küçük boyutlarda genel anahtar/anahtarlar ile asimetrik RSA şifreleme yapılabilir. Sonrasında bu anahtarlar ile oluşturulan eliptik matris aracılığıyla simetrik blok şifreleme yapılarak daha güvenli bir kriptografi elde edilebilir.

Çalışmada 100'den küçük asal sayılar için eliptik matris sayısının *10^14* den fazla olduğu görülmektedir. Buradan RSA algoritmasındaki çarpanları bulma problemine ilaveten oldukça fazla eliptik matris seçeneğinin olduğu ve kırılmasının çok daha zor olacağı görülebilir. Ayrıca, anahtarı bilen için küçük anahtar boyutlarıyla çalışmak, hesaplama açısından büyük avantaj sağlayacaktır. Bu da düşük kapasiteli IoT gibi sistemler için ECC'ye iyi bir alternatif olmaktadır.

RSA algoritmasında, genel anahtar herkesin görebildiği açık anahtardır. Simetrik şifrelemede anahtarlar gizlenerek paylaşılır. Çalışmada, genel anahtarlardan oluşan eliptik matrisin karekök matrislerinin olduğu gösterilmiştir. Anahtar paylaşımında karekök matrisler paylaşılarak güvenlik bir seviye daha yukarı çıkarılabilir. Bu yaklaşımda, aynı zamanda RSA algoritmasının genel anahtarları da gizlenmiş olur. Çünkü karekök matris elemanları ile $\phi(n)$ aralarında asal olmayacaktır.

Blok şifreleme özellikle büyük veri transferinde ve saklanmasında daha çok tercih edilmektedir. Çalışmada hem RSA algoritmasının küçük anahtarlarla kullanılabilmesi ve bu anahtarlara dayalı blok şifreleme yapılabileceği üzerine durulmuştur. Ayrıca blok anahtar paylaşımında doğrudan anahtarın paylaşılmasının gerekmediği, bunun yerine blok anahtarının karekökünün paylaşılabileceği gösterilmiştir. Blok anahtarın belirli standartlarda paylaşılmasına ek olarak karekök ile temsili anahtarı ayrıca maskelemektedir.

Yaklaşımda RSA küçük boyutlu anahtarları, eliptik matris ile blok şifreleme, simetrik anahtarın gizlenmesi gibi ayrı ayrı yöntemler önerilmiştir. Önerilen yaklaşımların kombinasyonları ile farklı hibrit sistemler oluşturulabilir. Örneğin, RSA küçük genel anahtarların bazıları ile RSA şifreleme, ardından blok şifreleme daha sonra tekrar RSA küçük genel anahtarları ile şifreleme yapılabilir.

Sonraki çalışmalar için düzlem eğrisi olan eliptik eğrilerin blok şifrelemede kullanımı araştırılabilir. Bu çok daha küçük anahtar boyutlarıyla şifreleme sağlayabilir.

Yazarların Katkısı

Tüm yazarlar çalışmaya eşit katkıda bulunmuştur.

Çıkar Çatışması Beyanı

Yazarlar arasında herhangi bir çıkar çatışması bulunmamaktadır.

Araştırma ve Yayın Etiği Beyanı

Yapılan çalışmada araştırma ve yayın etiğine uyulmuştur.

Kaynaklar

Bellare M., and Rogaway P. (2005). *Introduction to Modern Cryptography*. USA: California University Press.

Cusick T. W., and Stanica P.(2017). *Cryptographic Boolean Functions and Applications*. Academic Press.

Diffie W., and Hellman M., E. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*. 22(6): 644–654.

Hankerson D., Vanstone S., and Menezes A. (2004). *Guide to Elliptic Curve Cryptography*. Springer Professional Computing (SPC).

Hoffstein J., Pipher J., and Silverman J. H. (2014). *An Introduction to Mathematical Cryptography*. New York, USA: Springer Science+Business Media.

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

Menezes A. J., Oorschot P. C., and Vanstone S. A. (1997). *Chapter 7: Block Ciphers:Handbook of Applied Cryptography*. Boca Raton, London New York: CRC Press Taylor & Francis Group.

Miller V. (1985). Use of elliptic curves in cryptography. Advances in cryptology-CRYPTO 85, *Springer Lecture Notes in Computer Science*, 218.

Özdemir M. (2018). Introduction to Hybrid Numbers. *Adv. Appl. Clifford Algebras*, 28(11).

Özdemir M. (2019). Finding n-th roots of a 2_2 Real Matrix using De Moivre's Formula. *Adv. Appl. Clifford Algebras*, 29(2).

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

Robinson S. (2003). Still Guarding Secrets after Years of Attacks, RSA Earns Accolades for its Founders. *SIAM News.* 36(5).

Shannon C. E. (1949). Communication theory of secrecy systems. *The Bell System Technical Journal*, 28(4),656-715.

Silverman K., (1991). *Edgar A Poe: Mournful and Never-ending Remembrance*, New York: Harper Collins Publishers.

Stallings W., (2017). *Cryptography and Network Security: Principles and Practice*. Pearson.

Şık İ. A., (2020). *2x2 Türünden matrislerin karekökünün hesaplama yöntemleri*, Yüksek Lisans Tezi, Akdeniz Üniversitesi, Fen Bilimleri Enstitüsü, Antalya.

URL-1: http://www.cypher.com.au/crypto_history.htm (Erişim Tarihi: 21 Aralık 2024).

URL-2: https://crypto.interactive-maths.com/vigenegravere-cipher.html#google_vignette (Erişim Tarihi: 21 Aralık 2024).

URL-3 : https://www.egress.com/blog (Erişim Tarihi: 21 Aralık 2024).

URL-4 : https://www.nist.gov (Erişim Tarihi: 21 Aralık 2024).