Uluslararası İleri Doğa Bilimleri ve Mühendislik Araştırmaları Dergisi
Sayı 9, S. 190-197, 1, 2025

Araştırma Makalesi

IJANSER
https://as-proceeding.com/index.php/ijanser
ISSN:2980-0811

International Journal of Advanced Natural Sciences and Engineering Researches
Volume 9, pp. 190-197, 1, 2025

Research Article

Vigenère ve Eliptik Eğri Şifreleme Sistemlerinin Birleştirilmesiyle Elde Edilen Yeni Bir Şifreleme Sistemi

Hatice ŞATIR[1*] ve Semih YILMAZ [2]

[1]*Matematik / Fen Bilimleri Enstitüsü, Kırıkkale Üniversitesi, Türkiye*
[2]*Aktüerya Bilimleri / İktisadi ve İdari Bilimler Fakültesi, Kırıkkale Üniversitesi, Türkiye*

[*] *satir.hatice@gmail.com*

(Received: 14 January 2025, Accepted: 22 January 2025)

(2nd International Conference on Modern and Advanced Research ICMAR 2025, January 15-16, 2025)

ATIF/REFERENCE: Şatır, H. Yılmaz, S. (2025). Vigenère ve Eliptik Eğri Şifreleme Sistemlerinin Birleştirilmesiyle Elde Edilen Yeni Bir Şifreleme Sistemi. *International Journal of Advanced Natural Sciences and Engineering Researches*, 9(1), 190-197.

Özet **–** Günümüzde teknolojinin ilerlemesine paralel olarak artan bilgi depolanması zorunluluğu ve iletişimin yoğunluğu, kişisel bilgileri ve iletişim süreçlerini istenmeyen kişilerin erişiminden korumayı her geçen gün daha dikkatli olarak ele almamız gereken bir sorun haline getirmiştir. Teknoloji ilerledikçe yeni güvenlik açıkları ortaya çıkmaktadır. Kişisel bilgilerimizin güvenliğini sağlamak için, bilgi şifreleme ilk başvuracağımız koruma yöntemi olarak düşünülmektedir. Şifreleme sistemlerinin tarihinde bilgisayarın icadı, eski şifreleme sistemlerini kullanılamaz hale getiren bir milattır, çünkü bilgisayarların işlem kapasitesi arttıkça bu sistemleri kırmak saniye almayan bir işe dönüşmüştür. Böylece modern şifreleme yöntemlerine geçilmiş ve yüksek düzeyde matematik hesabın çok daha önemli olduğu bir şifreleme ve çözme olgusu oluşmuştur. Tabi ki modern şifreleme yöntemlerini kullanabilmek için gerekli matematik hesap bilgisayarlarla yapılıyor ve bu hesabın daha hızlı nasıl yapılacağı için birçok araştırmacı çalışmalar yürütmektedir.
Modern şifreleme sistemleri çok daha fazla işlem gerektirdiklerinden dolayı eski şifreleme sistemlerine nazaran yavaştırlar. İşlemci kapasitesi normal bilgisayarlardan daha düşük olan akıllı cihazların yaygınlaşmasıyla, bu cihazların işlediği veya sosyal medya iletilerinde bulunan, bulut sistemlerde saklanan v.s. kişisel verilerimizi hızlı şifreleyebilmek adına hem eski hem modern şifreleme sistemlerinin beraber kullanıldığı hibrit sistemlere rağbet artmıştır. Biz bu çalışmamızda eski Vigenère şifreleme sistemi ve modern şifreleme sistemleri oluşturmak için kullanılan Eliptik Eğri yöntemini birleştiren yeni bir hibrit şifreleme sistemi ortaya koyacağız.

Anahtar Kelimeler – Şifreleme, Kriptografi, Vigenère Şifreleme Sistemi, Eliptik Eğri Şifreleme Sistemleri, Hibrit Şifreleme Sistemleri, Asimetrik Şifreleme Sistemleri.

I. GİRİŞ

Şifreleme sistemleri, şifreleme ve şifre çözme yapmak için kullanılacak anahtarları açısından ikiye ayrılır. İlki tek anahtarla şifreleme ve şifre çözme yapılan simetrik yani "gizli anahtarlı" şifreleme sistemleridir. Bu sistemlerde aynı anahtar mesaj gönderecek birimde de mesajı alacak birimde de bulunmalıdır ve gizli tutulmalıdır. Bu tek anahtarın güvenli bir şekilde paylaşılması gerekliliği bu sistemlerdeki en büyük güvenlik problemidir. Eski şifreleme sistemleri simetrik şifreleme mantığına dayalıdır. İkinci olarak ise şifreleme ve şifre çözme için farklı anahtarlar kullanan asimetrik yani "açık anahtarlı" şifreleme sistemleridir. Asimetrik sistemlerde, mesaj alacak birimler birbirleriyle uyumlu olan

bir tanesi açık olarak ilan edilmiş ikincisi gizli olan iki tane anahtar üretirler. Herhangi bir birim, mesaj göndereceği birimin ilan edilmiş olan açık anahtarını kullanarak mesajını şifreleyip, şifreli mesajı karşı birime iletir; şifreli mesajı alan birim ise kendi açık anahtarı ile şifrelenmiş bu metni, kendisindeki gizli anahtar ile şifresiz hâle çevirerek açık mesaja ulaşmış olur.

Vigenère şifreleme sistemi bir simetrik şifreleme sistemidir. Bazı sonlu cisimlerde eliptik bir eğri seçilip bu eğrinin noktaları arasında işlemler tanımlanarak oluşturulan değişmeli grup yapısı üzerine inşa edilen eliptik eğri şifreleme sistemi (ECC) ise asimetrik bir yapıdadır.

II. MATERYAL VE YÖNTEM

A. *Vigenère Şifreleme Sistemi*

Simetrik bir şifreleme sistemi olan Vigenère şifreleme sistemi ilk olarak 1553'te Giovan Battista Bellaso tarafından tanımlanmış fakat 19. yüzyılda, yanlışlıkla Blaise de Vigenère'ye (1523-1596) atfedildiği için bugünkü adını almıştır[5].

Vigenère şifreleme sisteminde gizli anahtar genellikle sabit uzunlukta bir kelime veya kelimeler bütünüdür ve $K = "k_1k_2k_3 \dots k_n"$ şeklinde alfabedeki n-tane harf ile gösterilir. Gönderilecek açık mesaj $M = "m_1m_2m_3 \dots m_r"$ olsun, buradan $C = "c_1c_2 \dots c_r"$ şeklindeki şifreli metni

$$c_i = m_i + k_{\left(i-n.\left[\!\left[\frac{i-1}{n}\right]\!\right]\right)} \ (mod\ m)$$

formülü yardımıyla elde edilir. Burada $[\![x]\!]$ fonksiyonu x den küçük en büyük tamsayı sonucunu verir, m ise alfabedeki karakter sayısıdır. C şifreli metninin gönderildiği birim, aynı gizli anahtarı ile bu formülü kullanarak M açık metnine ulaşabilir.

Basit bir örnek olarak, gizli anahtar $K = "icmar"$ ve açık mesaj $M = "Konyadayız"$ olduğunda, alfabe olarak Türkçe alfabe(a:0,b:1,…,z:28) kullanılırsa $c_1 = m_1 + k_{\left(1-5.\left[\!\left[\frac{1-1}{5}\right]\!\right]\right)}(mod\ 29) = 'k'+'i' = 'u'$,

$$c_2 = m_2 + k_{\left(2-5.\left[\!\left[\frac{2-1}{5}\right]\!\right]\right)}(mod\ 29) = 'o'+'c' = 'p', \quad c_3 = 'n'+'m' = 'c', \quad c_4 = 'y'+'a' = 'y',$$

$$c_5 = 'a'+'r' = 'r', \qquad c_6 = 'd'+'i' = 'm', \quad c_7 = 'a'+'c' = 'c',$$

$$c_8 = 'y'+'m' = 'k', \qquad c_9 = 'ı'+'a' = 'ı', \quad c_{10} = 'z'+'r' = 'p',$$

böylece $C = "upcyrmckıp"$ şifreli mesajı elde edilir ve $K = "icmar"$ gizli anahtarına sahip herkes tarafından açık mesaja ulaşılabilir.

B. *Eliptik Eğriler*

K cismi, Reel Sayılar cismi, Rasyonel Sayılar cismi, Karmaşık Sayılar cismi veya bir p asal tamsayısı için $q = p^r \in \mathbb{Z}^+$ olmak üzere F_q sonlu cismi olsun.

Eğer K cismi $char(K) \neq 2\ ve\ 3$ şartını sağlıyorsa, $a, b \in K$ olmak üzere, katlı kökleri elemek için konulan $\Delta := 4a^3 + 27b^2 \neq 0$ şartı altında

$$y^2 = x^3 + ax + b$$

denkleminin çözümü olan noktalar kümesine K cismi üzerinde bir eliptik eğri denir. Bu denklem bir eliptik eğri için Weierstrass denklemi olarak adlandırılır.

Eğer K cismi $char(K) = 2$ şartını sağlıyorsa, $a, b, c \in K$ olmak üzere,

$$y^2 + cy = x^3 + ax + b \quad veya\ y^2 + xy = x^3 + ax^2 + b$$

denkleminin çözümü olan noktalar kümesine K cismi üzerinde bir eliptik eğri denir.

Eğer K cismi $char(K) = 3$ şartını sağlıyorsa, $a, b, c \in K$ olmak üzere,

$$y^2 = x^3 + ax^2 + bx + c$$

denkleminde katlı kökler olmamak üzere bu denklemin çözümü olan noktalar kümesine K cismi üzerinde bir eliptik eğri denir.

Eliptik eğri üzerindeki noktaların bir grup yapısı oluşturabilmesi için sonsuzdaki bir noktaya daha gereksinim vardır. Bu nokta "sonsuzdaki nokta" olarak adlandırılan bir nokta olup genelde $\mathcal{O}$ sembolü ile veya ∞ sembolü ile gösterilir.

Bundan böyle işlemlerimizi $char(K) \neq 2\ ve\ 3$ şartını sağlayan K cismi üzerinde yapacağız, diğer cisimler için de benzer hesaplamalar yapılabilir.

$$E = \{(x, y) \in K \times K : \ y^2 = x^3 + ax + b \ \} \cup \{\infty\}$$

kümesi, $P_1 = (x_1, y_1),\ P_2 = (x_2, y_2) \in E$ için $\infty + P_1 = P_1 + \infty = P_1$ ve

$$m = \begin{cases} \dfrac{y_2 - y_1}{(x_2 - x_1)} & eğer\ P_1 \neq P_2 \\ \dfrac{(3\,x_1^2 + a)}{2y_1} & eğer\ \ P_1 = P_2 \end{cases} \quad \text{için} \quad \begin{matrix} x_3 = m^2 - x_1 - x_2 \\ y_3 = m(x_1 - x_3) - y_1 \end{matrix}$$

olmak üzere $P_3 = P_1 + P_2 = (x_3, y_3)$ şeklinde tanımlı toplama işlemine göre bir değişmeli gruptur. E kümesine K cismi üzerindeki bir eliptik eğri grubu denir. Burada $-P_1 = (x_1, -y_1)$ olduğu kolayca görülebilir.

$A \in E$ ve $n \in \mathbb{Z}$ için $n.A \coloneqq \underbrace{A + A + A + \cdots + A}_{n-tane} = \infty$ olmak üzere n tamsayısına A noktasının mertebesi denir.

$A \in E \subset K$ mertebesi m olan bir nokta ve $B \in E$ olsun. $0 \leq l \leq m - 1$ için $B = l.A$ olacak şekildeki l tam sayısına A tabanında B nin ayrık logaritması denir ve $l = \log_A B$ şeklinde gösterilir. $A, B \in E$ için l tamsayısını bulma problemine eliptik eğrinin ayrık logaritma problemi (ECDLP) denir. Bu problemin polinomsal sürede çözümü henüz olmadığından, matematiksel olarak bilgisayarda çözümü zor bir problemdir.

C. *Eliptik Eğri Diffie-Hellman Anahtar Alışverişi:*

Sonlu bir K cismi üzerinde bir eliptik eğri grubu E olsun. Simetrik bir şifreleme metodu ile iletişim kuracak iki birim B1 ve B2 olsun. B1 ve B2 birimleri ortak bir anahtar elde etmek için öncelikle ürettiği alt grubun mertebesi büyük olacak şekilde bir $P \in E$ noktası belirlerler ve sonrasında her ikisi de gizledikleri sırasıyla b_1, b_2 tamsayılarını seçerek $P_{B1} = b_1 P, P_{B2} = b_2 P$ noktalarını hesaplayıp birbirlerine gönderirler ve B1 birimi $h \coloneqq b_1(b_2 P) = (b_1 b_2)P$ noktasını hesaplarken B2 birimi ise $b_2(b_1 P) = (b_1 b_2)P = h$ noktasını hesaplar. Dolayısıyla h anahtarı üzerinde anlaşmış olurlar. Böylece asimetrik bir yolla yapılan bu anahtar anlaşmasına Diffie-Hellman anahtar anlaşması denir. İletişimi gözleyen dış bir birim E, F, P, P_{B1}, P_{B2} değerlerini bildiği halde ECDLP 'nin zorluğundan b_1, b_2 tamsayılarını bulamaz, dolayısıyla h ortak anahtarına ulaşamaz.

D. *Eliptik Eğri El Gamal Şifreleme Sistemi:*

Sonlu bir K cismi üzerinde bir eliptik eğri grubu E ve bir $P \in E$ noktası seçilsin öyle ki P nin mertebesi $n \coloneqq |E|$ tamsayısı olsun. Bu şifreleme sistemi ile Banu bir $M \in E$ mesajını Ayşe'ye göndermek istesin. Burada tüm açık ve şifreli metinler, bilinen dönüşümler yardımıyla eliptik eğrinin noktaları ile ifade edilebiliyor ve tersi yapılabiliyor olmalıdır. Ayşe mesaj alabilmek için gizli anahtarları olacak $s \in \mathbb{Z}$ tamsayısını seçip $A = sP$ değerini hesaplar ve açık anahtar olarak (E, K, P, A) bilgilerini ilan eder. Banu bir $k \in \mathbb{Z}$ gizli tamsayısını seçerek $C_1 = kP\ ,\ C_2 = M + kA$ hesabını yapar ve bu $C_1, C_2 \in E$ noktalarını Ayşe'ye gönderir. Ayşe ise kendi gizli anahtarını kullanarak

$$C_2 - sC_1 = M + kA - s(kP) = M + kA - k(sP) = M + kA - kA = M$$

hesabıyla Banu'nun mesajına ulaşır. Şematik olarak:

	$\underline{Banu}$	$\underline{Ayşe}$
1. *anahtar oluşturma*:	$M\ (gizli),\quad k\ (gizli)$	$s(gizli), A = sP\ (açık),$
2. $şifreleme\ ve\ deşifreleme$:	$C_1 = kP\ ,\ C_2 = M + kA\ \longrightarrow$	$C_2 - sC_1 = M$

şeklindedir.

E. *Eliptik Eğri ve Vigenère Hibrit Şifreleme Sistemleri:*

Bhatia ve Dave [1] Vigenère ve Eliptik Eğri El-Gamal Şifreleme Sistemlerini hibrit kullanan bir çalışma yapmışlardır. Özet olarak yazarlar, kullandıkları alfabe üzerinden Diffie-Hellman Anahtar Anlaşması ile bir Vigenère ortak anahtarı belirleyip, açık metni bir kez Vigenère Şifreleme Sistemi ile şifrelemiş, bu şifreli metni de üst üste iki kez Eliptik Eğri El-Gamal Şifreleme Sistemi ile şifreleyerek nihai şifreli metni elde etmişlerdir.

Trung vd. ise [2]'de Vigenère ve Eliptik Eğri El-Gamal Şifreleme Sistemlerini hibrit kullanan bir çalışma yapmışlardır. Özet olarak, öncelikle kullanılan alfabe ile oluşturulmuş bir Vigenère ortak anahtarı belirlemiş açık metni bir kez Vigenère Şifreleme Sistemi ile şifreleyip bu şifreli metnin her karakterini sonlu cisim üzerindeki eliptik eğrinin bir sabit P üreteç noktası ile çarparak, eliptik eğrideki bir noktayla eşleme yapmışlar ve bu noktaların dönüştürülmesiyle şifreli metni elde etmişlerdir. Kullanılacak sonlu cisim F ve eliptik eğri katsayıları ile bu eliptik eğrideki noktalar bilindikten sonra yazarların kullandıkları şifreleme algoritması m karakterli alfabe üzerinde aşağıdaki gibidir:

$$C_i = \left[\left(P_i + K_j\right) mod\ m\right]P$$

burada, P_i açık metnin bir karakteri, K_j Vigenère anahtarının bir karakteri ve P eliptik eğrideki bir üreteç nokta olmak üzere; C_i, şifreli metnin karakterine karşılık gelen eliptik eğri noktasıdır.

III. BULGULAR

Biz bu çalışmada Vigenère Şifreleme Sistemi ve Eliptik Eğri ayrık logaritma problemini kullanarak aşağıdaki hibrit şifreleme sistemini tasarladık.

A. *Anahtar Oluşturma Algoritması:*

Sonlu bir F cismi üzerinde bir eliptik eğri grubu E ve bir $P \in E$ üreteç noktası seçilsin. P noktasının mertebesi t olsun. Herhangi v-tane $r_i \in \mathbb{Z}^+, r_i \leq t$ tamsayıları seçilsin ve $V = (r_1P, r_2P, \dots, r_vP)$ Vigenère anahtarı olarak ilan edilsin. Dolayısıyla açık anahtar (F, E, P, V), gizli anahtar ise $(r_1, r_2, \dots, r_v)$ olsun.

B. *Şifreleme Algoritması:*

Yukarıdaki açık ve gizli anahtar sahibine mesaj göndermek isteyen kişi aşağıdaki adımlarla şifreli metni oluşturur:

Adım1: m karakterden oluşan mesajı, $M_1, M_2, \dots, M_m \in E$ olacak şekilde kodlar.

Adım2: Rastgele v-tane $k_1, k_2, \dots, k_v \in \mathbb{Z}, 0 < k_i < t$ tamsayıları seçer

$$C_{1,i} = k_iP, \qquad 1 \leq i \leq v \leq m$$

$$C_{2,j} = k_{\left(j-v.\left[\left[\frac{j-1}{v}\right]\right]\right)} \cdot \left(r_{\left(j-v.\left[\left[\frac{j-1}{v}\right]\right]\right)}P\right) + M_j\ , \qquad 1 \leq j \leq m$$

olmak üzere $C_{1,i}, C_{2,j}$ noktalarını hesaplar ve bu $v + m$ −tane noktayı C şifreli metnine dönüştürür. Burada eğer E eliptik eğrisinin nokta sayısı çok fazla ise ve tüm mesaj tek bir nokta ile ifade edilebilirse sadece $C_{1,1}, C_{2,1} \in E$ noktalarıyla da şifreli mesaj oluşturulabilir.

C. *Deşifreleme Algoritması:*

C şifreli metnini alan kişi kendisine ait $(r_1, r_2, \dots, r_v)$ gizli anahtarını kullanarak

$$C_{2,i} - r_{\left(i-v.\left[\left[\frac{i-1}{v}\right]\right]\right)}C_{1,\left(i-v.\left[\left[\frac{i-1}{v}\right]\right]\right)}$$
$$= k_{\left(i-v.\left[\left[\frac{i-1}{v}\right]\right]\right)} \cdot \left(r_{\left(i-v.\left[\left[\frac{i-1}{v}\right]\right]\right)}P\right) + M_i - r_{\left(i-v.\left[\left[\frac{i-1}{v}\right]\right]\right)}\left(k_{\left(i-v.\left[\left[\frac{i-1}{v}\right]\right]\right)}P\right) = M_i\ ,\ 1 \leq i \leq m$$

hesabını yapıp açık metne ulaşır.

D. *Algoritma için örnekler:*

Ayşe $\mathbb{Z}_{23}$ cisminde $y^2 = x^3 + x + 4$ eliptik eğrisini seçsin, bu eliptik eğrinin oluşturduğu E eliptik eğri grubu aşağıdaki 29 tane noktaya sahiptir.

$E = \{\infty, (0,2), (0,21), (1,11), (1,12), (4,7), (4,16), (7,3), (7,20), (8,8), (8,15), (9,11), (9,12), (10,5), (10,18), (11,9), (11,14), (13,11), (13,12), (14,5), (14,18), (15,6), (15,17), (17,9), (17,14), (18,9), (18,14), (22,5), (22,18)\}$.

Alfabe Türkçe alfabe (a:0,b:1,…,z:28) kullanıp, üreteç noktası olarak $P = (7,3)$ ve Vigenère anahtarı olarak

$$r_1 = 10, r_2 = 20, r_3 = 13, r_4 = 19 \rightarrow$$
$$V = (r_1P, r_2P, r_3P, r_4P) = \big((14{,}5), (8{,}8), (15{,}17), (14{,}18)\big)$$

seçsin. Ayşe'nin açık anahtarı $\Big(\mathbb{Z}_{23}, (1{,}4), (7{,}3), \big((14{,}5), (8{,}8), (15{,}17), (14{,}18)\big)\Big)$ şeklindedir. Burada kullanılacak şifreleme sistemi tamamen açık bir şekilde belirtilmelidir, dolayısıyla çalışılan sonlu cisim, eliptik eğrinin katsayıları, üreteç noktası ve aşağıdaki tablo gibi alfabeyi eliptik eğri noktalarına gömme fonksiyonu ilan edilmiş olmalıdır.

Banu "yarın yarımda kafede" mesajını Ayşe'ye şifreli olarak göndermek için Ayşe'nin açık anahtarını okur. Alfabeyi eliptik eğri noktalarına gömmek için aşağıdaki herkes tarafından bilinen tabloyu kullanır:

a	0	∞	ğ	8	(10,18)	n	16	(15,6)	u	24	(1,11)
b	1	(7,3)	h	9	(8,15)	o	17	(13,12)	ü	25	(4,16)
c	2	(22,18)	ı	10	(14,5)	ö	18	(11,14)	v	26	(18,14)
ç	3	(18,9)	i	11	(11,9)	p	19	(14,18)	y	27	(22,5)
d	4	(4,7)	j	12	(13,11)	r	20	(8,8)	z	28	(7,20).
e	5	(1,12)	k	13	(15,17)	s	21	(10,5)			
f	6	(0,21)	l	14	(17,14)	ş	22	(9,11)			
g	7	(9,12)	m	15	(17,9)	t	23	(0,2)			

Daha sonra mesajını E eliptik eğrisinin noktalarıyla ifade eder,
"(22,5)(∞)(8,8)(14,5)(15,6)(22,5)(∞)(8,8)(14,5)(17,9)(4,7)(∞)(15,17)(∞)(0,21)(1,12)(4,7)(1,12)"
bu noktalar M_i lerdir ve $m = 18$-tanedir. Şifreleme yapmak için Vigenère anahtarı uzunluğu kadar k_i seçer ve $C_{1,i}$ leri hesaplar:

$$k_1 = 11, k_2 = 4, k_3 = 21, k_4 = 6 \rightarrow$$

$$C_{1,1} = k_1P = 11.(7{,}3) = (11{,}9) \rightarrow "i"$$
$$C_{1,2} = 4.(7{,}3) = (4{,}7) \rightarrow "d"$$
$$C_{1,3} = 21.(7{,}3) = (10{,}5) \rightarrow "s"$$
$$C_{1,4} = 6.(7{,}3) = (0{,}21) \rightarrow "f".$$

sonrasında $C_{2,i}$ leri hesaplar

$$C_{2,1} = k_{\left(1-4.\left[\left[\frac{1-1}{4}\right]\right]\right)}.\left(r_{\left(1-4.\left[\left[\frac{1-1}{4}\right]\right]\right)}P\right) + M_1$$
$$= k_1.(r_1P) + M_1 = 11.(14{,}5) + (22{,}5) = (0{,}2) + (22{,}5) = (10{,}5) \rightarrow "s"$$
$$C_{2,2} = k_2.(r_2P) + M_2 = 4.(8{,}8) + (\infty) = (9{,}11) + (\infty) = (9{,}11) \rightarrow "ş"$$
$$C_{2,3} = k_3.(r_3P) + M_3 = 21.(15{,}17) + (8{,}8) = (13{,}11) + (8{,}8) = (18{,}9) \rightarrow "ç"$$
$$C_{2,4} = k_4.(r_4P) + M_4 = 6.(14{,}18) + (14{,}5) = (22{,}5) + (14{,}5) = (10{,}18) \rightarrow "ğ"$$
$$C_{2,5} = k_1.(r_1P) + M_5 = (0{,}2) + (8{,}8) = (17{,}14) \rightarrow "l"$$
$$C_{2,6} = k_2.(r_2P) + M_6 = (9{,}11) + (22{,}5) = (8{,}8) \rightarrow "r"$$
$$C_{2,7} = k_3.(r_3P) + M_7 = (13{,}11) + (\infty) = (13{,}11) \rightarrow "j"$$
$$C_{2,8} = k_4.(r_4P) + M_8 = (22{,}5) + (8{,}8) = (11{,}14) \rightarrow "ö"$$
$$C_{2,9} = k_1.(r_1P) + M_9 = (0{,}2) + (14{,}5) = (4{,}7) \rightarrow "d"$$
$$C_{2,10} = k_2.(r_2P) + M_{10} = (9{,}11) + (17{,}9) = (10{,}18) \rightarrow "ğ"$$
$$C_{2,11} = k_3.(r_3P) + M_{11} = (13{,}11) + (4{,}7) = (15{,}6) \rightarrow "n"$$
$$C_{2,12} = k_4.(r_4P) + M_{12} = (22{,}5) + (\infty) = (22{,}5) \rightarrow "y"$$
$$C_{2,13} = k_1.(r_1P) + M_{13} = (0{,}2) + (15{,}17) = (9{,}12) \rightarrow "g"$$
$$C_{2,14} = k_2.(r_2P) + M_{14} = (9{,}11) + (\infty) = (9{,}11) \rightarrow "ş"$$
$$C_{2,15} = k_3.(r_3P) + M_{15} = (13{,}11) + (0{,}21) = (11{,}14) \rightarrow "ö"$$
$$C_{2,16} = k_4.(r_4P) + M_{16} = (22{,}5) + (1{,}12) = (18{,}9) \rightarrow "ç"$$
$$C_{2,17} = k_1.(r_1P) + M_{17} = (0{,}2) + (4{,}7) = (22{,}5) \rightarrow "y"$$
$$C_{2,18} = k_2.(r_2P) + M_{18} = (9{,}11) + (1{,}12) = (22{,}5) \rightarrow "y".$$

Buradan Banu $C = "idsfsşçğlrjödğnygşöçyy"$ şifreli metnini Ayşeye iletir.
Ayşe aldığı şifreli metni çözmek için ilk olarak metindeki harflerin nokta karşılıklarını bulur:

$$C = "idsf\text{s}şçğ\text{l}rjödğnygşöçyy"$$

$$\rightarrow "(11,9)(4,7)(10,5)(0,21)(10,5)(9,11)(18,9)(10,18)(17,14)(8,8)(13,11)(11,14)(4,7)(10,18)(15,6)(22,5)(9,12)(9,11)(11,14)(18,9)(22,5)(22,5)"$$

bunlar, "$C_{1,i}, C_{2,i}$" lerdir, $C_{1,1} = (11,9), C_{1,2} = (4,7), C_{1,3} = (10,5), C_{1,4} = (0,21)$. Şimdi Ayşe

$$M_i = C_{2,i} - r_{\left(i-v.\left[\left[\frac{i-1}{v}\right]\right]\right)} C_{1,\left(i-v.\left[\left[\frac{i-1}{v}\right]\right]\right)}$$

formülü ile açık mesaja, gizli $r_1 = 10, r_2 = 20, r_3 = 13, r_4 = 19$ sayılarını kullanarak aşağıdaki şekilde ulaşır:

$$M_1 = C_{2,1} - r_{\left(1-v.\left[\left[\frac{1-1}{v}\right]\right]\right)} C_{1,\left(1-v.\left[\left[\frac{1-1}{v}\right]\right]\right)} = C_{2,1} - r_1 C_{1,1} = (10,5) - 10.(11,9) = (10,5) - (0,2)$$
$$= (10,5) + (0,-2) = (10,5) + (0,21) = (22,5) \rightarrow "y"$$

$$M_2 = C_{2,2} - r_2 C_{1,2} = (9,11) - 20.(4,7) = (9,11) - (9,11) = (9,11) + (9,12) = (\infty) \rightarrow "a"$$
$$M_3 = C_{2,3} - r_3 C_{1,3} = (18,9) - 13.(10,5) = (18,9) - (13,11) = (18,9) + (13,12) = (8,8) \rightarrow "r"$$
$$M_4 = C_{2,4} - r_4 C_{1,4} = (10,18) - 19.(0,21) = (10,18) - (22,5) = (10,18) + (22,18) = (14,5) \rightarrow "ı"$$
$$\vdots$$
$$M_{18} = C_{2,18} - r_2 C_{1,2} = (22,5) - 20.(4,7) = (22,5) - (9,11) = (22,5) + (9,12) = (1,12) \rightarrow "e".$$

İkinci bir örnek olarak, alfabeyi değiştirmeden daha fazla nokta sayısına sahip bir eliptik eğride şifreleme şu şekilde olabilir:

Ayşe $\mathbb{Z}_{107}$ cisminde $y^2 = x^3 + 3x - 2$ eliptik eğrisini seçsin, bu eliptik eğrinin oluşturduğu E eliptik eğri grubu aşağıdaki 107 tane noktaya sahiptir.

E
$= \{(0,31), (0,76), (2,36), (2,71), (3,26), (3,81), (7,24), (7,83), (15,23), (15,84), (16,41), (16,66), (17,19), (17,88), (20,51), (20,56), (21,21), (21,86), (22,36), (22,71), (23,6), (23,101), (25,41), (25,66), (28,45), (28,62), (31,52), (31,55), (32,21), (32,86), (36,18), (36,89), (37,30), (37,77), (39,7), (39,100), (40,5), (40,102), (41,53), (41,54), (42,32), (42,75), (44,28), (44,79), (46,40), (46,67), (52,48), (52,59), (53,25), (53,82), (54,21), (54,86), (58,3), (58,104), (61,1), (61,106), (62,3), (62,104), (65,16), (65,91), (66,41), (66,66), (69,44), (69,63), (71,10), (71,97), (73,17), (73,90), (75,25), (75,82), (77,34), (77,73), (78,5), (78,102), (79,2), (79,105), (80,52), (80,55), (82,53), (82,54), (83,36), (83,71), (86,25), (86,82), (88,12), (88,95), (91,53), (91,54), (93,23), (93,84), (94,3), (94,104), (95,38), (95,69), (96,5), (96,102), (100,13), (100,94), (101,37), (101,70), (103,52), (103,55), (104,47), (104,60), (106,23), (106,84), \infty\}$

Alfabe Türkçe alfabe (a:0,b:1,…,z:28) kullanıp, üreteç noktası olarak $P = (23,6)$ ve Vigenère anahtarı olarak

$$r_1 = 19, r_2 = 100, r_3 = 32 \rightarrow$$
$$V = (r_1 P, r_2 P, r_3 P) = \big((41,54), (73,90), (91,54)\big)$$

seçsin. Ayşe'nin açık anahtarı $\Big(\mathbb{Z}_{107}, (3,-2), (23,6), \big((41,54), (73,90), (91,54)\big)\Big)$ şeklindedir. Banu "tek gel" mesajını Ayşe'ye şifreli olarak göndermek için Ayşe'nin açık anahtarını okur. Alfabedeki $i.\ a_i$ karekteri eliptik eğri noktalarına $(i+1).P$ ile eşleşecek şekilde gömülsün, örneğin b alfabedeki numarası 1 olduğundan $2P = (96,5)$ olacaktır.

Daha sonra mesajını E eliptik eğrisinin noktalarıyla ifade eder,
"(36,89)(0,76)(93,23)(73,17)(0,76)(80,52)"
bu noktalar M_i lerdir ve $m = 6$-tanedir. Şifreleme yapmak için Vigenère anahtarı uzunluğu kadar k_i seçer ve $C_{1,i}$ leri hesaplar:

$$k_1 = 20, k_2 = 95, k_3 = 6 \rightarrow$$
$$C_{1,1} = k_1 P = 20.(23,6) = (62,104)$$
$$C_{1,2} = 95.(23,6) = (16,66)$$
$$C_{1,3} = 6.(23,6) = (52,59)$$

sonrasında $C_{2,i}$ leri hesaplar

$$C_{2,1} = k_{\left(1-3.\left[\left[\frac{1-1}{3}\right]\right]\right)}.\left(r_{\left(1-3.\left[\left[\frac{1-1}{3}\right]\right]\right)}P\right) + M_1$$
$$= k_1.(r_1P) + M_1 = 20.(41,54) + (36,89) = (20,56) + (36,89) = (54,21)$$
$$C_{2,2} = k_2.(r_2P) + M_2 = 95.(73,90) + (0,76) = (36,18) + (0,76) = (66,66)$$
$$C_{2,3} = k_3.(r_3P) + M_3 = 6.(91,54) + (93,23) = (2,71) + (93,23) = (21,86)$$
$$C_{2,4} = k_1.(r_1P) + M_4 = (20,56) + (73,17) = (106,84)$$
$$C_{2,5} = k_2.(r_2P) + M_5 = (36,18) + (0,76) = (66,66)$$
$$C_{2,6} = k_3.(r_3P) + M_6 = (2,71) + (80,52) = (58,3)$$

Buradan Banu $C = "(62,104)(16,66)(52,59)(54,21)(66,66)(21,86)(106,84)(66,66)(58,3)"$ şifreli metnini Ayşeye iletir. Burada her nokta harflerle eşleşmediğinden eliptik eğrinin noktaları gönderiliyor, bu kodlamayı C="062104016066052059054021066066021086106084066066058003" olarak veya farklı biçimlerde yapmak da mümkündür.

Ayşe aldığı şifreli metni çözmek için ilk olarak metni nokta nokta listesi olarak ifade eder

$$C = "062104016066052059054021066066021086106084066066058003"$$
$$\rightarrow "(62,104)(16,66)(52,59)(54,21)(66,66)(21,86)(106,84)(66,66)(58,3)"$$

bunlar, "$C_{1,i}, C_{2,i}$" lerdir, $C_{1,1} = (62,104), C_{1,2} = (16,66), C_{1,3} = (52,59)$. Şimdi Ayşe

$$M_i = C_{2,i} - r_{\left(i-v.\left[\left[\frac{i-1}{v}\right]\right]\right)}C_{1,\left(i-v.\left[\left[\frac{i-1}{v}\right]\right]\right)}$$

formülü ile açık mesaja, gizli $r_1 = 19, r_2 = 100, r_3 = 32$ sayılarını kullanarak aşağıdaki şekilde ulaşır:

$$M_1 = C_{2,1} - r_{\left(1-v.\left[\left[\frac{1-1}{v}\right]\right]\right)}C_{1,\left(1-v.\left[\left[\frac{1-1}{v}\right]\right]\right)} = C_{2,1} - r_1C_{1,1} = (54,21) - 19.(62,104) = (54,21) - (20,56)$$
$$= (54,21) + (20,-56) = (54,21) + (20,51) = (36,89) \rightarrow "t"$$

$$M_2 = C_{2,2} - r_2C_{1,2} = (66,66) - 100.(16,66) = (66,66) - (36,18) = (66,66) + (36,89) = (0,76) \rightarrow "e"$$
$$M_3 = C_{2,3} - r_3C_{1,3} = (21,86) - 32.(52,59) = (21,86) - (2,71) = (21,86) + (2,36) = (93,23) \rightarrow "k"$$
$$M_4 = C_{2,4} - r_1C_{1,1} = (106,84) + (20,51) = (73,17) \rightarrow "g"$$
$$M_5 = C_{2,5} - r_2C_{1,2} = (66,66) + (36,89) = (0,76) \rightarrow "e"$$
$$M_6 = C_{2,6} - r_3C_{1,3} = (58,3) + (2,36) = (80,52) \rightarrow "l".$$

IV. TARTIŞMA

Bir hibrit şifreleme sistemi, açık anahtarlı şifreleme sistemin rahatlığını, simetrik anahtarlı şifreleme sistemin verimliliğiyle birleştiren bir sistemdir[4]. Dolayısıyla [1]de yapılan çalışma tam anlamıyla bir hibrit şifreleme değildir, şifreleme sistemlerinin peş peşe uygulanarak güvenliğin artırılmasıdır. Bundan dolayı bizim çalışmamızla kıyaslanması gerekli değildir.

Trung vd. tarafından yapılan [2] deki çalışmada verilen şifreleme fonksiyonunu incelersek,

$$C_i = \left[\left(P_i + K_j\right) mod\ m\right]P$$

şeklindeki fonksiyonda köşeli parantez içinde yapılan işlem Vigenère şifreleme sistemini uygulamak iken, farklı C_i noktalarının sayısı alfabedeki karakter sayısıyla aynı olacaktır. Burada dikkat edilmesi gereken nokta alfabenin eliptik eğri noktalarına gömülmesinin [2]'de ve bizim çalışmamızda verilen örnekler kadar basit olmayacağıdır, bu örneklerde tablo kullanılarak şifreli metnin çözümü çok kolaydır ama büyük asal sayılarla tanımlanan sonlu cisimlerde alfabeyi sonlu cisim noktalarına dönüştürecek olan dönüşüm formüllerinin hesaplamaları çok zor olacaktır. [2]'de verilen şifreleme sistemi bir simetrik şifreleme sistemidir. Aynı zamanda [2]'de verilen şifreleme sisteminin Vigenère anahtarı alfabe üzerinden seçilmektedir. Bizim çalışmamızda ise Vigenère anahtarı eliptik eğrinin noktaları üzerinden seçilmiştir ayrıca şifreli metin eliptik eğri noktalarının tümünü kullanan bir noktalar kümesidir. [2] çalışmasında eliptik eğri noktalarının sadece alfabedeki karakter sayısı kadarı kullanılmaktadır, öyleyse nokta sayısı çok fazla olan eliptik eğriler kullanılırken [2] çalışmasındaki kriptografi sisteminde bir güvenlik artışı olmazken bizim çalışmamızda tanımladığımız kriptografi sisteminde güvenlik nokta

sayısına paralel oranda artacaktır. Dolayısıyla çalışmamız, Eliptik Eğri El-Gamal Şifreleme Sisteminin, Vigenère Şifreleme sistemi eklenerek güçlendirilmiş bir hibrit versiyonudur.

V. SONUÇLAR

Çalışmada algoritmasını vererek tanımladığımız asimetrik yapıdaki şifreleme sistemi, hesaplama açısından hemen hemen Eliptik Eğri El-Gamal Şifreleme Sistemi kadar büyüklükte bir işlem hacmine rağmen güvenlik açısından kırılması çok daha zor bir hibrit şifreleme sistemi örneği olacaktır.

KAYNAKLAR

[1] D. Bhatia and M. Dave, "Elliptic Curve Layered: A Secure Polyalphabetic Vignere Cryptographic Algorithm for Textual Data," *Journal of Scientific Research*, Institute of Science, BHU Varanasi, India, vol. 65/1, pp. 222-229, 2021.

[2] M. M. Trung, L. P. Du, D. T. Tuan, N. V. Tanh, N. Q. Tri, "Design a cryptosystem using elliptic curves cryptography and Vigenère symmetry key", *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 13/2, pp. 1734–1743, Apr. 2023.

[3] N. Koblitz, *A Course in Number Theory and Cryptography*, 2nd ed., Berlin, Germany: Springer-Verlag, 1991. ISBN 3-540-94293-9.

[4] S. A. Ijaz, A. B. Kamalrulnizam, I. Subariah, "A Generic Hybrid Encryption System (HES)", *Research Journal of Applied Sciences, Engineering and Technology*, vol. 5(9), pp. 2692-2700, 2013. DOI:10.19026/rjaset.5.4793.

[5] A. McAndrew, Introduction To Cryptography With Open-Source Software, CRC Press Taylor & Francis Group, ISBN 13: 978-1-4398-2571-6 (eBook - PDF)