mühendislikdergisi
Dicle Üniversitesi Mühendislik Fakültesi
Cilt: 8, Sayı: 3,503-513
Temmuz 2017

Kriptolojide eliptik eğri algoritmasının uygulanması

Aziz Mahmut YÜCELEN[*,1],Abdullah BAYKAL[2], Cengiz COŞKUN[3]

[1]Dicle Üniversitesi, Teknik Bilimler Meslek Yüksekokulu Bilgisayar Programcılığı Bölümü, Diyarbakır
[2]Dicle Üniversitesi, Fen Fakültesi Matematik Bölümü, Diyarbakır
[3]Dicle Üniversitesi İktisadi ve İdariBilimler Fakültesi, Diyarbakır

Makale Gönderme Tarihi: 01.11.2016 Makale Kabul Tarihi: 14.02.2017

Öz

Kriptoloji, geçmişten beri insanların her türlü iletişiminde gizlilik, reddedilemezlik ve doğruluk ihtiyacını karşılamak üzere düşünülmüş ve uygulamaya geçilmiştir.

İster iş amaçlı, isterse sosyal olarak kullanılan internet, bilgi paylaşımının yoğun oldugu bir yapı olması, şifrelemenin önemini açık bir şekilde ortaya koymaktadır. Günümüzde şifrelemeler bankacılık, e-devlet uygulamaları, uzaktan eğitim sistemleri, askeri iletişim sistemleri, uydu, kara ve deniz harp sistemlerinde, kimlik doğrulama ve daha birçok iletişimde aktif bir şekilde kullanılmaktadır.

Bu çalışma ile, eliptik eğri şifreleme algoritmalarının araştırılması, algoritmaların oluşturulması, oluşturulurken kullanılan matematiksel tanımlamalar ve teoremler konusunda bilgi verilmesi ve eliptik eğri algoritması ile çalışan bir java programın geliştirilmesi amaçlanmıştır.

***Anahtar Kelimeler**: Kriptoloji, sayısal imza, El-Gamal eliptik eğri algoritması*

[*]Yazışmaların yapılacağı yazar: Aziz Mahmut YÜCELEN. ayucelen@msn.com

Giriş

Kriptoloji biliminin temel mantığı bilinenin aksine kırılamazlık değil kırılmanın güçlüğü üzerine kuruludur. Bu anlamda geliştirilen algoritmalar bu kırılma zorluğunu elde edebilmek için tek yönlü matematiksel foksiyonlar üretmekte iken diğer taraftan matematiksel analizler ile kırılma yolları ve kırılma algoritmaları üzerine de çalışmalar ve yaklaşımlar geliştirilmektedir. Yakın zamana kadar şifreleme için kullanılan açık anahtar sistemine sahip RSA ve Diffie-Hellman gibi birçok algoritma, aynı anahtar uzunluğuna sahip eliptik eğri şifrelemenin sağladığı güvenliğin yarısını sağlayabildiği gerçeği, araştırmacıları eliptik eğriler konusunda çalışmalara itmiştir fakat bu avantaj diğer konularda dezavantaj olarak kendini gösterebilmektedir. Bu nedenle eliptik eğri şifrelemesinde diğer şifreleme tekniklerine göre işlemci gücü ve buna bağlı sorunların varlığı, araştırmacıları bu dezavantajları ortadan kaldırmaya yönelik çalışmaya sevketmektedir.

Metot

Eliptik Eğri Şifrelemeye Giriş

Günümüzde eliptik eğrilerin şifrelemedeki kullanımı giderek artmakta ve birçok açık anahtarlı şifreleme tekniklerinde eliptik eğriler önemli rol oynamaktadır. Eliptik Eğri Şifreleme nin' (EEŞ)emellerinden biri de düz metindeki karakterlerin yani gönderilecek mesajın, EEŞ'nin mantığı olan iki boyutlu uzaydaki noktalara dönüştürülmesi olayıdır. Bu dönüşüm sadece verilen mesajın Eliptik Eğri (EE) üzerindeki noktalara dönüştürülmesiyle kalmaz, EE üzerindeki noktalara dönüştürülmüş mesajın tekrar düz metini oluşturacak karakterlere ve böylece orijinal metinin oluşmasını sağlar.

Mesajların Eliptik Eğriye Yerleştirilmesi:

Şifrelenmek üzere metni oluşturan karakterlerin her biri Tablo 1. 'de belirtildiği gibi her bir karaktere birer doğal sayı gelecek şekilde birebir bir eşleme yaptırılmaktadır.

Bu durum Tablo 2.'e göre a=0, b=1, c=2, … z=29 şeklinde eşleme yaptırılarak karakterlerin her biri bir anlamda numaralandırılmıştır.

Tablo 1. Örnek karakterler tablosu.

a	b	c	d	e	f	g	h	ı	i
j	k	l	m	n	o	ö	p	q	r
s	ş	t	u	ü	v	w	x	y	z

Tablo 2. Harf ve sayı eşleştirme tablosu.

a=0	b=1	c=2	d=3	e=4	f=5	g=6	h=7	ı=8	i=9
j=10	k=11	l=12	m=13	n=14	o=15	ö=16	p=17	q=18	r=19
s=20	ş=21	t=22	u=23	ü=24	v=25	w=26	x=27	y=28	z=29

Bu eşlemeyi yaparken seçilecek cisim noktalarının sayısı, Tablo 1. karakter sayısı için yeterli olmalıdır.

$q = p^s$ olacak şekilde Z_q da tanımlı EE için s asal olmalıdır. *m,* bir mesajdaki her bir karakterin sayısal değerini ve M ise karakter tablosundaki karakterlerin sayısını göstermek üzere $0 \le m \le M$ ve $q > Mk$ ölçütleri alınır. Yeterince büyük seçilen bir $k \in N$ doğal sayısı, genelde $10 \le k \le 30$ şeklinde bir değerdir. Mesajların noktalara dönüştürülmesi işleminde kullanılan bu $k \in N$ değeri için oluşacak başarısızlık olasılığı $\frac{1}{2^k}$ dir.

Aşağıdaki şekilde tanımlanmış kümenin

$$X = \{x : x = mk + j,\ 1 \le j \le k,\ \ k, j, m \in N\}$$

$x \in X$ değerlerinin her biri

$$y^2 = f(x) = x^3 + ax + b \bmod(q)$$

şeklindeki denklemde yerine yazılarak $f(x)$'in bir tam karesi elde edilmeye çalışılır. Böylece bir m mesajı P_m şeklinde bir noktaya $1-1$ olarak dönüştürülmüş olur.

Örnek : F_{631} üzerinde tanımlı $y^2 = x^3 + x + 1$ şeklindeki EE'ye yukarıdaki örnek karakter tablosunda bulunan 'e' karakterini yerleştirelim.

İlk olarak verilen eliptik eğrinin şifrelemeye uygunluğunu araştıralım. $4*1^3 + 27*1^2 = 31 \neq 0 \pmod{631}$ olduğundan eliptik eğri süpersingüler değildir, böylece eliptik eğrinin şifrelemeye uygun olduğu görülür.

Şimdi Hasse teoremi ile eliptik eğri üzerindeki noktaların sayısının, mesaj yerleştirme işlemi için yeterliliğini kontrol edelim.

$$|N - (q+1)| \le 2\sqrt{q}$$

$$|N - (769+1)| \le 2\sqrt{769} = 55{,}4616$$

$$-55{,}4616 \le N - 770 \le 55{,}4616$$

$$714 \le N \le 825$$

$714 \le N \le 825$ nokta sayısı aralığı, mesaj karakterlerini eliptik eğriye gömmek için yeterlidir. Örnek karakter tablosundaki karakter sayısı $M = 30$ dönüştürülmesini istediğimiz karakter ve eşlendiği sayı $e = 5$ son olarak $k = 12$ olarak alındığında $m = 5,\ k = 12,\ 0 < j \le k$ *için*

$mk + j$	51 52 53 54 55 56 57 58 59 60
x	51 52 53 54 55 56 57 58 59 60

elde edilir.

Herbir x değeri teker teker verilen eliptik eğri denklemine yerleştirilip kontrol edilerek tamsayı bir y'değerine ulaşana kadar belirtilen aralıklarda x'in değeri bir arttırılır.

$$x = 51 \ \textit{için} \quad y^2 = x^3 + 3x$$

$$y^2 = 51^3 + 3*51$$

$$= 132804$$

$$= 294 \pmod{631}$$

Bulunur ki $y^2 = 294 \pmod{631}$ olacak şekilde herhangi bir $y \in F_{631}$ bulunamaz, bu durumda verilen x değeri artırılarak

$$x = 55 \ \textit{için} \quad y^2 = x^3 + 3x$$

$$y^2 = 55^3 + 3*55$$

$$= 166540.0$$

$$= 587 \pmod{631}$$

Bulunur ki $y^2 = 587 \pmod{631}$ olacak şekilde

$$y = 43$$

$$y^2 = 43^2$$

$$= 1849$$

$$= 587 \pmod{631}$$

bir $y \in F_{631}$ bulunur, böylece $e = 5$ mesajı $y^2 = x^3 + 3x$ eliptik eğrisi üzerinde $P_e = (55,43)$ noktasına dönüşmüş olur.

Yerleşik Noktalardan Mesajın Elde Edilmesi

Mesajların EE'ye yerleştirilmesinin aksine, EE üzerindeki bir $P(x,y)$ noktasına karşılık gelecek şekilde yerleşik bir karakteri, $P(x,y)$ noktasından yararlanarak bulmak için

$$m = \left[\frac{x-1}{k} \right] \qquad (1)$$

denkleminden yararlanılır.

Örnek: Yukarıdaki örnekte $e = 5$ mesajı, $y^2 = x^3 + 3x$ EE'sine $P_e = (55,43)$ olarak yerleştirilmişti, şimdi bu noktaya karşılık gelen mesaj

$$m = \left[\frac{x-1}{k} \right] = \left[\frac{55-1}{10} \right] = \left[\frac{54}{10} \right] = [5] = e$$

olarak bulunur.

Eliptik Eğri Tabanlı Geometri

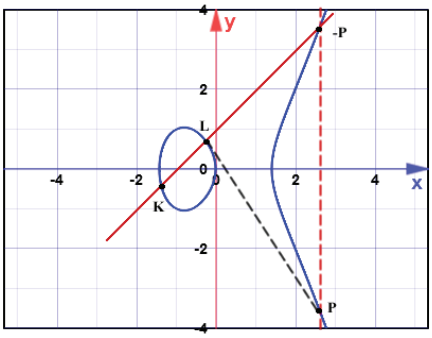
EEŞ diğer şifreleme tekniklerine göre matematiksel arkaplanı daha zengin olduğu için, eğrinin tanımlanacağı cisime ek olarak standart dışı toplama ve çarpma işlemeleri de tanımlanmaktadır.

Nokta Ekleme

$K(x_K, y_K)$ *ve* $L(x_L, y_L)$, EE üzerinde biribirinden farklı iki noktanın eklenerek $P(x_P, y_P)$ şeklinde başka bir noktanın oluşturulması işlemidir.

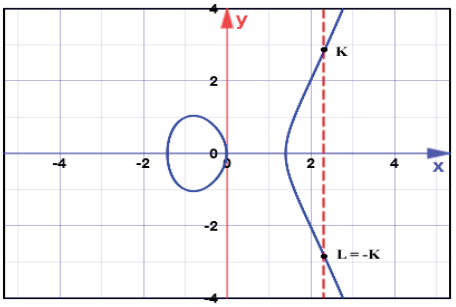
Geometrik Yaklaşım

$K(x_K, y_K)$, $L(x_L, y_L)$ *ve* $P(x_P, y_P)$, $K \neq L$ olmak üzere, eğer $x_K \neq x_L$ ise K ve L noktalarını birleştiren doğru, eğriyi üçüncü bir $-P$ noktasında keser, bu $-P$ noktasının x-eksenine göre simetriği olan P noktası $K + L$ işleminin sonucudur. $K + L = P$ işlemi geometrik olarak Şekil 1.'de gösterilmiştir.



Şekil 1. Nokta ekleme.

Eğer $x_K = x_L$ ise K ve L noktaları x-eksenine göre simetrik olur, bu durumda K ve L noktaları eğriyi sonsuzdaki 'O' noktasında keser. Böylece $K + L = O$ bulunur ve bu durum Şekil 2'de geometrik olarak gösterilmiştir.



Şekil 2. Nokta ekleme sonsuz durumu.

Aritmetik Yaklaşım

$K(x_K, y_K)$, $L(x_L, y_L)$, $P(x_P, y_P)$, $K \neq L$ aynı eliptik eğri üzerindeki noktalar , $m_{K,L}$ ise

$$m_{K,L} = \frac{y_L - y_K}{x_L - x_K} \qquad (2)$$

şeklinde K ve L noktalarını birleştiren doğrunun eğimi olmak üzere $K + L = P$ işlemini sağlayan $P(x_P, y_P)$ noktası, $x_K \neq x_L$ ise

$$\begin{aligned} x_P &= m_{K,L}^2 - x_L - x_K \\ y_P &= m_{K,L}(x_P - x_L) + y_L \end{aligned} \qquad (3)$$

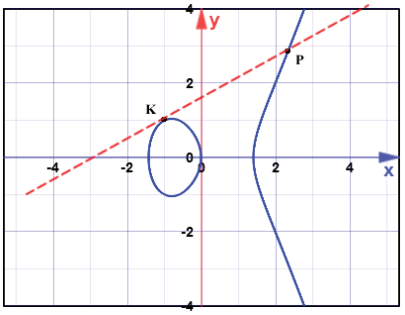
$x_K = x_L$ *ve* $y_K \neq y_L$ ise $L = -K$ dır ve $m_{K,L} = \infty$ olduğu için bu iki noktayı birleştiren doğru y-eksenine paraleldir dolayısıyla bu doğru eğriyi sonsuzdaki O noktasında keser böylece $K + L = O$ sonucuna ulaşılır.

Nokta Çiftleme

Nokta çiftleme, EE üzerindeki herhangi bir K noktasının kendisine eklenmesiyle farklı noktaların oluşturulmasıdır.

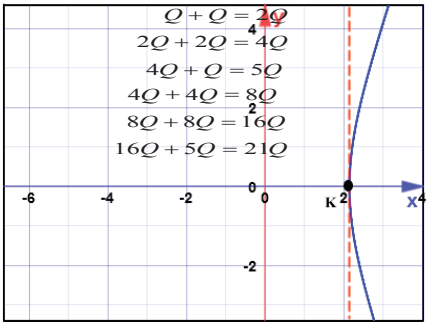
Geometrik Yaklaşım

$y_k \neq 0$ olmak üzere bir $K(x_k, y_k)$ noktasının kendisi ile toplamı, eğrinin $K(x_k, y_k)$ noktasındaki teğetinin eğriyi kestiği ikinci bir noktanın x-eksenine göre simetriğidir ve bu durum Şekil 3'de ifade edildiği gibi $K + K = 2K$ olur.



Şekil 3. Nokta çiftleme.

Eğer $y_k = 0$ ise $K(x_k, y_k)$ noktasındaki eğrinin teğeti y-eksenine paralel olduğu için bu teğet eğriyi sonsuz noktada keser bu durum Şekil 4. te ifade edildiği gibi $K + K = O$ dur.



Şekil 4. Nokta çiftleme sonsuz durumu.

Aritmetik Yaklaşım

EE üzerindeki $K(x_k, y_k)$ noktasının kendisi ile toplamı olan $K + K = 2K = P(x_P, y_P)$ noktası eğer $y_k \neq 0$ ise

$$x_P = m_{K,L}^2 - 2x_K$$
$$y_P = m_{K,L}(x_P - x_K) + y_K \qquad (4)$$

şeklinde bulunur.

Eğer $K(x_k, y_k)$ noktası için $y_k = 0$ ise eliptik eğrinin bu noktadaki teğet doğrusu y-eksenine paralel olduğu için nokta çiftleme işleminin sonucu $K + K = O$ şeklinde sonsuz noktadır.

Nokta Çarpımı

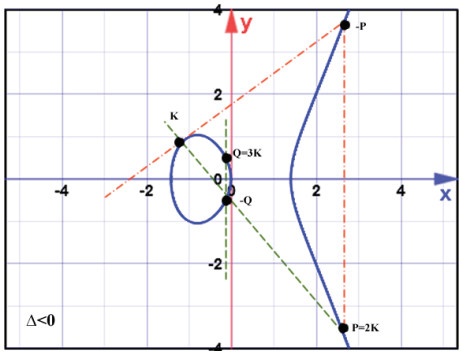
Eliptik eğrilerde nokta çarpımı;

(i) Nokta ekleme ile K, L gibi farklı iki nokta toplanarak K+L=Q gibi diger bir nokta elde edilerek

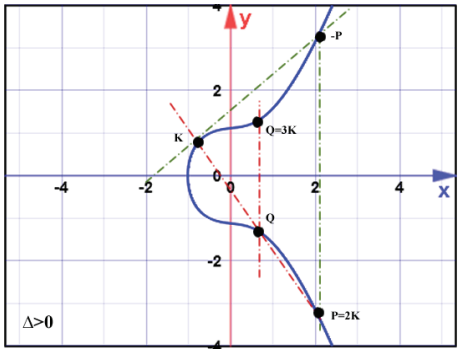
(ii) Nokta çiftleme ile K gibi bir noktadan yararlanarak $K + K = 2K$ gibi bir farklı nokta elde edilerek yapılabilir.

$Q \in E(a,b)$, $k \in Z^+$ *ve* $0 < k < n-1$ $n = \#E(a,b)$ için $K = kQ$ şeklinde farklı bir noktaya tekrarlı olarak nokta ekleme ve çiftleme işlemi yapılarak istenen sonuca en az işlem yapılarak ulaşılabilir.

Örnek: k=21 ve Q üreteç noktası ile $kQ = 21Q$ noktasına ile ulaşılabilir. Eliptik eğrilerde nokta çarpım işlemi, Şekil 5. ve Şekil 6'da geometrik olarak gösterilmiştir.



Şekil 5. $\Delta < 0$ *eğriler için nokta çarpımı.*



Şekil 6. $\Delta > 0$ *eğriler için nokta çarpımı.*

Eliptik Eğri Tabanlı El-Gamal Şifreleme ve Deşifrelemesi (Friswell 2010)

EE tabanlı şifrelemeler açık anahtar sistemine dayalı olduğundan bu sistem güvenli olmayan bir ortamda karşılıklı ön bilgilerin gönderilmesiyle başlamakta, bu başlangıç işlemindeki ön bilgiler, *cisim parametreleri* olarak adlandırılmaktadır. Bu sistemin kırılmasının zorluğu eliptik eğri ayrık logaritma problemine dayanmaktadır. (Yavuz 2008).

Başlangıç Cisim Parametreleri:
El-Gamal EEŞ kullanılacak olan parametreleri (p, a, b, L, n) olmak üzere;

- p eliptik eğride kullanılacak olan asal sayı
- (a,b) $y^2 = x^3 + ax + b$ şeklinde, bir F cismi üzerinde tanımlı E eliptik eğrisini oluşturan skalerler
- L ise E eliptik eğrisi üzerindeki üreteç noktası
- n asal sayısı ise üreteç noktasının derecesi yani L üreteç noktasından başlayıp sonsuz O noktasına kadar olan noktaların sayısı şeklindedir.

Anahtar Oluşturma:
Bir 'p' asal sayısı için F_p üzerinde tanımlı bir $L \notin E(F_p)$ noktasının derecesi, n asal sayısı olmak üzere, L noktasıyla oluşturulan devirli alt grup

$$\langle L \rangle = \{L, 2L, 3L, 4L, ...(n-1)L\} \qquad (5)$$

şeklindedir. Bu devirli alt guruptaki n sayısı, L noktasının derecesi olup anahtar oluşturmak için gerekli olan ve $1 \le d \le n-1$ aralığında rasgele 'd' tamsayısı seçilerek $K = dL$ şeklinde ikinci bir nokta olan K noktası elde edilir. Bu K noktası şifrelemede kullanılacak olan açık anahtar, d tamsayısı ise özel anahtardır.

Mesaj Şifreleme:
Şifreleme işleminde ilk olarak gönderici L üreteç noktası ve 'd' özel anahtarıyla $K = dL$ şeklinde kendi açık anahtarını üretir daha sonra alıcının açık anahtarı Q ve EE üzerindeki noktalara gömülen M mesajı ile

$$\begin{aligned} U_1 &= dL \\ U_2 &= M + dQ \\ U &= (dL, M + dQ) \end{aligned} \qquad (6)$$

şeklinde $U = (dL, M + dQ)$ gönderilecek şifreli metin oluşturulur.

Mesaj Deşifreleme:
Deşifreleme işleminde alıcı kendi açık anahtarını oluşturmak için kullandığı özel anahtar k ve göndericiden alınan şifrelenmiş M metnini

$$\begin{aligned} &U = (dL, M + dQ) \ \text{için}\ U_1 = dL \ \text{ve}\ U_2 = M + dQ \\ &\Rightarrow kU_1 = k(dL) = d(kL) = dQ \\ &\Rightarrow M = U_2 - kU_1 = (M + dQ) - dQ \ \text{olarak bulur.} \end{aligned}$$

Örnek : Z_{769} üzerinde tanımlı $y^2 = x^3 + x + 1$ eliptik eğrisi ile "e=5" mesajı, $k = 10$ için eliptik eğri üzerindeki (53,323) noktasına yerleşir, şimdi bu mesajı karşı tarafa şifreleyerek gönderelim. Öncelikle gönderici kendi açık anahtarını oluşturmak için rasgele bir özel anahtar seçer, bu örnek için gönderici özel anahtar d_G=2 seçilsin, üreteç nokta L=(1,100) olarak seçilirse açık anahtar

$$K = d_G L = 2L$$

formülünden K = 2L bulunur, burada nokta çiftleme yöntemiyle L = (1,100) noktası için

$$egim = m = \frac{(3x_1 + a)}{2y_1} \ \text{mod}(769)$$

$$= \frac{3*1^2 + 1}{2*100} = \frac{770}{200} \text{mod}(769) = 325$$

bulunur ve eğimden yararlanarak K noktasının apsisi

$$x_K = m^2 - 2x_1 \ \text{için}$$

$$= (325)^2 - 2*1 \ \text{mod}(769) = 512$$

ve ordinatı

$$y_K = m(x_1 - x_K) - 2x_1 \ \text{mod}(631) \ \text{için}$$

$$= (325(1 - 512) - 2) \text{mod}(769)$$

$$= 182$$

olarak elde edilir. Böylece $K = (512,182)$ bulunmuş olur, benzer olarak alıcı da kendi açık anahtarını aynı yöntemle elde eder, rasgele bir özel anahtar seçer, bu örnek için gönderici özel anahtar d_A=6 olarak seçilirse açık anahtar

$$Q = d_A P = 2P$$

formülünden Q=6P bulunur, burada iki nokta çiftleme ve bir toplama işlemi kullanılır, bu yöntem ile $P = (1,100)$ üreteç noktası seçildiğinde;

$P + P = 2P$ işlemi için

$$egim = m = \frac{\left(3x_1^2 + a\right)}{2y_1} \mod(769)$$

$$= \frac{3*1^2+1}{2*100} = \frac{770}{200} \mod(769) = 325$$

olarak bulunur ve eğimden yararlanarak 2P noktasının apsisi

$$x_K = m^2 - 2x_1 \ için$$

$$= (325)^2 - 2*1 \mod(769) = 512$$

ve ordinatı

$$y_K = m(x_1 - x_K) - 2x_1 \mod(631) \ için$$

$$= (325(1-512) - 2) \mod(769)$$

$$= 182$$

$$2P = (512,182) \ dir.$$

2P+2P=4P işlemi için

$$egim = m = \frac{\left(3x_1^2 + a\right)}{2y_1} \mod(769)$$

$$= \frac{3*(512)^2+1}{2*182} = \frac{786433}{364} \mod(769) = 350$$

bulunur ve eğimden yararlanarak 4P noktasının apsisi

$$x_K = m^2 - 2x_1 \ için$$

$$= (350)^2 - 2*512 \mod(769) = 743$$

ve ordinatı

$$y_K = m(x_1 - x_K) - 2x_1 \mod(631) \ için$$

$$= (350(512-743) - 2*512) \mod(769)$$

$$= 482$$

$$4P = (743,482) \ dir.$$

4P+2P=6P işlemi için

$$egim = m = \frac{y_2 - y_1}{x_2 - x_1} \mod(769)$$

$$= \frac{482-182}{743-512} = \frac{300}{231} \mod(769) = 231$$

bulunur ve eğimden yararlanarak 6P noktasının apsisi

$$x_K = m^2 - x_1 - x_2 için$$

$$= (231)^2 - 512 - 743 \mod(769) = 583$$

ve ordinatı

$$y_K = m(x_1 - x_K) - 2y_1 \mod(769) \ için$$

$$= (231(512-583) - 182) \mod(769)$$

$$= 335$$

olarak elde edilir. Böylece alıcının açık anahtarı $6P = (583,335)$ bulunmuş olur. Metnin şifrelenmesi için alıcı ve gönderen kendi aralarında açık anahtarlarını paylaşır daha sonra gönderen

$$U = (dL, M + dQ)$$

$$= (2*(1,100), (53,323) + 2(583,335))$$

$$= ((512,182), (53,323) + (243,65))$$

$$= ((512,182), (463,598))$$

şeklinde gerekli işlemleri yaparak şifrelenmiş mesajı ((512,182),(463,598)) olarak elde eder. Deşifreleme işleminde ise alıcı, göndericinin açık anahtarını kendi özel anahtarı ile çarpar ve

$U = (dL, M + dQ) = ((512,182), (463,598))$ ve $P = (1,100)$ *için*
$U_1 = dL = 2P \quad U_2 = M + dQ = (463,598)$ ve $k = 6$ *anahtarı*
$\Rightarrow kU_1 = k(dL) = 6(2P) = 12P = d(kL) = dQ = (243,65)$
$\Rightarrow M = U_2 - kU_1 = (M + dQ) - dQ$
$= (463,598) - (243,65)$
$= (463,598) + (243,-65)$
$= (463,598) + (243,704)$
$= (53,323)$
bulunur.
$\frac{[x-1]}{k} = \frac{[53-1]}{10} = [5] = e$

orijinal mesajı elde edilir.

Eliptik Eğri Tabanlı Sayısal İmza Algoritması

Eliptik eğri sayısal imza algoritması için p asal ve $E(a,b)$ $F(p)$ üzerinde tanımlı bir eliptik eğri, $T = (r,t)$ ise derecesi q gibi ANSI X9.62

gereği ikilik tabanda $q > 2^{160}$ şeklinde en az 160 bitlik uzunluğa sahip bir asal tamsayı olan bir üreteç nokta olsun(Rodrigez ve Ark. 2007).

İmzalama

Öncelikle gönderen $1 < o_G < q-1$ olacak şekilde bir o_G özel anahtar seçer ve

$$P_G = o_G T \tag{7}$$

gibi bir P_G açık anahtarı oluşturur. Bir Q mesajının gönderen tarafından imzalama işlemi için $1 < z < q-1$ olacak şekilde başka bir rasgele sayı seçilir ve ardından Q mesajı

$$\begin{aligned} U &= zT = (w,e) \\ h &= w \mod (q) \\ c &= (Q + o_G h)/z \mod (q) \end{aligned} \tag{8}$$

hesaplamaları ile bulunan (h,c) çifti ile imzalanmış olur, burada dikkat edilmesi gereken husus (h,c) çiftinin her bir parametresinin sıfırdan farklı olmasıdır, olmaması durumunda rasgele seçilen z tamsayısı, ilgili parametreler sıfır olmaktan kurtarılana kadar değiştirilir ve işlemler tekrarlanır.

İmza Doğrulama

Alıcı tarafı mesaj ile gelen imzayı doğrulamak için $1 < a < q-1$ olacak şekilde bir a rasgele tamsayısını seçer ve daha sonra imza olarak gönderilen (h,c) çiftinin her bir parametresi için

$$1 < h, c < q \tag{9}$$

doğrulamasını yapar ve

$$\begin{aligned} b &= Q/c \mod(q) \\ n &= h/c \mod(q) \\ bT + no_G &= (i,j) \\ m &= i \mod(q) \end{aligned} \tag{10}$$

değerlerini hesaplar, eğer m=h bulunursa imza doğrulanmış olur.

Eliptik Eğri Tabanlı El-Gamal İmzalama Şeması

Eliptik eğri El-Gamal sayısal imza algoritması (EEESİA) için p asal ve $E(a,b)$ $F(p)$ üzerinde tanımlı bir eliptik eğri, $T = (r,t)$ ise derecesi q gibi asal olması gerekmeyen bir üreteç nokta olsun (Babinkostova 2011).

İmzalama

Burada imzalama yöntemi Eliptik Eğri Tabanlı Sayısal İmza Algoritması ile aynıdır, burada dikkat edilmesi gereken ilk husus EEESİA'nda imza hesaplanırken kullanılan

$$c = (Q + o_G h)/z \mod (q)$$

yerine

$$c = (Q - o_G h)/z \mod (q)$$

kullanılmasıdır, ikinci husus ise (h,c) çiftinin her bir parametresinin sıfırdan farklı olmasıdır, olmaması durumunda rasgele seçilen z tamsayısı, ilgili parametreler sıfır olmaktan kurtarılana kadar değiştirilir ve işlemler tekrarlanır.

İmza Doğrulama

Burada imza doğrulama yöntemi Eliptik Eğri Tabanlı Sayısal İmza Algoritması aynıdır sadece EEESİA'nın doğrulama işlemlerindeki

$$bT + no_G = (i,j)$$

yerine

$$bT - no_G = (i,j)$$

olduğuna dikkat edilmelidir. Eğer $m = h$ bulunursa imza doğrulanmış olur.

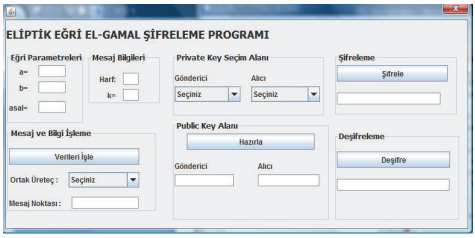
Ayrık Logaritma ve Eliptik Eğri Ayrık Logaritma Problemi

Ayrık logaritma problemi, $m^x = y$ şeklindeki bir eşitlik için $x = \log_m^y$ şeklindeki x değerlerinin bulunması temeline dayanmaktadır (Coultas 2008)(Katz ve Ark. 2007). Eliptik eğri ayrık logaritma problemi ise kısaca bir eliptik eğri üzerindeki P ve Q noktası bilindiğinde $Q = kP$ şeklindeki bir denklemden k tamsayısının elde edilmesi problemidir (Cohen

ve Ark. 2005). Bu noktadan hareketle eliptik eğri El-Gamal şifre çözme ve Diffie-Hellman anahtar degisim protokolü ayrık logaritma problemine dayanan başlıca algoritmalardır.

Eliptik Eğri El-Gamal Şifreleme Program Tanıtımı

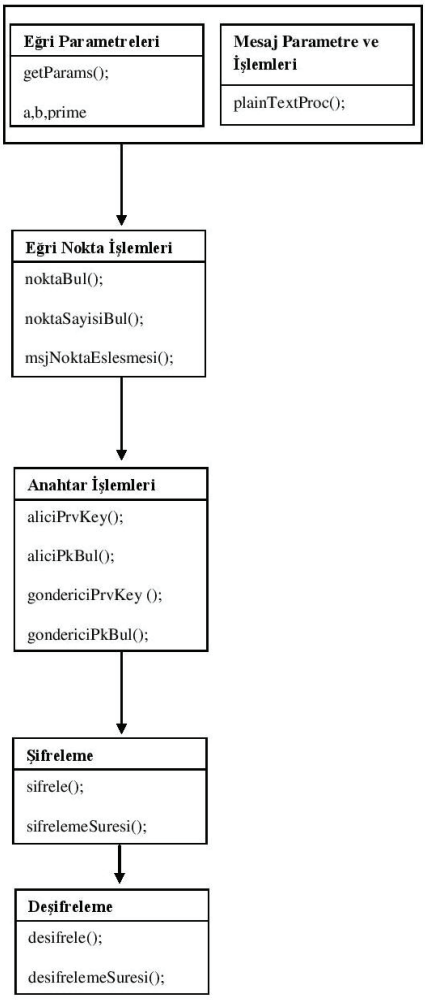
Örnek şifreleme programı, java programlama dili ile standart kriptoloji kütüphaneleri kullanılmadan temel düzeye indirgenip NetBeans IDE 6.9 kullanılarak yazılmış ve UML Diagramı Şekil 8'de verilmiştir İlk olarak masaüstü uygulaması çalıştırıldığında Şekil 7 görüntülenir.



Şekil 7. Java uygulamasının ekran görüntüsü

Sırasıyla, eliptik eğri parametreleri olan a, b ve asal sayı girildikten hemen sonra 'Mesaj Bilgileri' sekmesinde şifrelenecek harf ve uygun bir 'k' değeri girilir, 'Mesaj ve Bilgi işleme' sekmesindeki 'Verileri İşle' butonuna basılır, bu butonun görevi, girilen parametrelerin EEŞ için uygun olup olmadığını sınar, üreteç noktası oluşturur, şifrelenecek harfi EE üzerindeki bir noktaya dönüştürür ve son olarak gönderici ve alıcının private key bilgilerini oluşturur. Üreteç noktası, gönderenin ve alıcının private keyleri belirlenmesinin ardından 'Public Key' sekmesindeki 'Hazırla' butonuna basılarak iki tarafında public keyleri oluşturularak tüm safhalar tamamlanır, böylece 'Şifreleme' sekmesindeki 'Şifrele' butonuna basılarak EE noktası şifrelenir, 'Deşifreleme' sekmesindeki 'Deşifrele' butonuna basılarak da şifrelenmiş metin deşifre edilir.

UML Diagramı



Şekil 8. Uml diagramı

Bulgular ve Tartışma

Hazırlanan algoritmanın hız değerleri milisaniye (msn) cinsinden $E_{631}(1,1)$ eğrisi üzerinde oluşturulan bir M noktasının şifrelenmesi ve yeniden deşifre edilerek yeniden M noktasının elde edilmesi için gereken süreler 192,224 ve 256 bit cisimler için Tablo 3.'de verilmiştir.

Tablo 3. ElGamal algoritması (msn) hız değerleri

	192 bit	**224 bit**	**256 bit**
Sifreleme	8,230	12,342	15,237
Desifreleme	4,120	6,301	7,643
Toplam	12,350	18,643	22,880

Yukarıda ki Tablodan görüleceği gibi EEŞ sisteminde çalışılan cisimler büyüdükçe zaman maliyetleride artmaktadır fakat EEŞ sisteminin RSA ve diğer güçlü şifreleme tekniklerine göre üstünlüğü, aynı güvenlik seviyesini daha az anahtar uzunluğu ile gerçekleştirmesidir.

Tablo 4. Anahtar uzunluğu ve güvenlik karşılaştırılması (Cohen ve Ark. 2005)

	Bant Genisligi		Anahtar Uzunlugu	
	2000 bitlik uzun mesajlar için imza büyüklügü (bit)	100 bit uzunlugundaki mesajın sifrelendikten sonrası uzunlugu	Açık Anahtar (bit)	Gizli Anahtar (bit)
RSA	1024	1024	1088	2048
ECC	320	321	161	160

Tablo 4.'te bu durum açıkça ortaya çıkmakta, anahtar uzunluğunun şifreleme sistemlerine göre kıyaslanması verilmektedir (Cohen ve Ark. 2005).

Sonuç ve öneriler

Günümüz teknolojisinin vazgeçilmez unsurlarından biri olan güvenilirliğin, elektronik iletişimde önemi zamanla artamakta ve buna paralel olarak hızına yetişilmekte güçlük çekilecek ilerlemelere sebep olmaktadır. Teknolojinin ilerlemesine paralel olarak RSA, DES, 3DES ve diğer şifreleme sistemlerine ECC Eliptik Eğri Şifreleme gibi güçlü sistemler geliştirilmiştir. Eliptik eğri şifreleme bu anlamda diğer güvenli ve hızlı olarak nitelendirilen şifreleme tekniklerine göre aynı güvenlik seviyesinde düşük anahtar uzunluğunu kullanması, geleceğin bu sistemlere ihtiyaç duyacağını göstermektedir. Bellek ve islemci açısından kısıtlamanın olmadığı ortamlarda, EEŞ sistemleri yüksek güvenlik seviyesini alternatiflerine göre daha kısa anahtar boylarıyla gerçeklestirebilmektedir.

EEŞ sistemlerde hız sorunun çözümüne yönelik arayışlar devam etmekte olup çözümü ile ilgili olarak;

- Farklı koordinat sistemlerinde çalışmak
- Daha az aritmetik işlem gerektiren EEŞ elde edilen hız va anahtar boyutuna sahip yeni yöntemlerin araştırılması
- Daha az sayıda nokta toplama ve çarpma işlemlerine gereksinim duyan yeni algoritmaların geliştirilmesi

şeklinde sıralanabilir.

Kaynaklar

Cohen H.,Frey G.,Avanzi R.,Doche C.,Lange T.,Nguyen K., ve Vercauteren F. (2005), *Handbook of Elliptic and Hyperelliptic Curve Cryptography,* Chapman & Hall/CRC, CRC Press Company, T&F Group

Coultas M.(2008),Elliptic Curves and Cryptography, Technical Report , 13

Enge A.(1999), *Elliptic Curve and Their Applications to Cryptography*, Kluwer Academic Publisher Group , 95

Friswell R.(2010),*Elliptic Curves, Cryptography and Factorisation*, Durham University Department of Mathmatical Sciences, 4. 65-72

Hankerson D. , Menezes A. , Vanstone S. (2003) *Guide to Elliptic Curve Cryptography* Springer-Verlag, 76-79

Katz J.,Lindell Y. (2007),*Introduction to Modern Cryptography*, Chapman & Hall/CRC, CRC Press Company, 277

McReynolds J.(2008),Elliptic Curves and Cryptography, Technical Report, 34.

Rodríguez-Henríquez F., Pérez A., Saqib A.N., Koç Ç.K. (2007). *Cryptographic Algorithms on Reconfigurable Hardware*. Springer, 19-24.

Standarts for Efficent Cryptography (2000),SEC 1: Elliptic Curve Cryptography, Technical Report, 3

Yavuz İ. (2008), Eliptik Eğri Kriptosisteminin FPGA Üzerinde Gerçeklenmesi. *Yüksek Lisans Tezi,* İTU Fen Bilimleri Enstitüsü, İstanbul

Washington L.C.(2008),*Elliptic Curves Number Theory and Cryptography* Second Edition, Chapman & Hall/CRC T&F Group, 12-18

BabinkostovaL. http://math.boisestate.edu/ ~liljanab/ Crypto2Spring10/eceg1.htm , (15.03.2011)

Implementation of elliptic curve algorithm in cryptology

Extended abstract

In this study, it's aimed to explore the elliptic curve encryption algorithms, to build the algorithms, to provide information on mathematical basis and to implement a sample java program on elliptic curve algorithm.

Contemporarily, the use of elliptic curves on cryptography gradually ascends and it plays an essential role in public key cryptography. One of the very important basics of elliptic curve cryptography is to transform the characters in the text that is to be transmitted to the points on xy coordinate system. This transformation not only converts the text to points on the ellyptic curve but also helps to get the original text from the points placed on the elliptic curve.

Since the elliptic curve cryptography is based on public key encryption, the process starts with the transmission of the setting parameters over an insecure media. These setting parameters are called the field parameters. The strength of the ellyptic curve cryptography stems from the difficulty of solution of eliptic curve discrete logarithm(Yavuz, 2008).

In encryption, sender first sets his own public key K by K=dL where L is generator point, and d is private key. Let M be the text to transmit, she then prepares the encrypted message U, using the receiver's public key Q by:

$$U_1 = dL$$
$$U_2 = M + dQ$$
$$U = (dL, M + dQ)$$

The receiver, then decrypts the text message M from received message U, using her private key k, that she used to create her own public key, by:

$$U = (dL, M + dQ) \quad U_1 = dL \text{ and } U_2 = M + dQ$$
$$\Rightarrow kU_1 = k(dL) = d(kL) = dQ$$
$$\Rightarrow M = U_2 - kU_1 = (M + dQ) - dQ$$

Sample encryption program that is introduced in this article is programmed in java pogramming language in NetBeans IDE 6.9 without using standard cryptology libraries such that basic java language is employed. When the program first starts, a screen as in fig.1 is displayed.

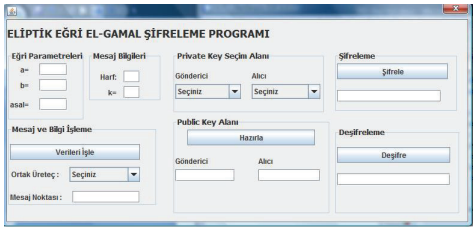


Fig. 1. A screenshot of the introduced java program

Table 1. *El Gamal algorithm (msn) speed values*

	192 bit	***224 bit***	***256 bit***
Encryption	*8,230*	*12,342*	*15,237*
Decryption	*4,120*	*6,301*	*7,643*
Total	*12,350*	*18,643*	*22,880*

As the chart above shows, as the objects in the Elliptic Curve Encryption system are growing, the times are increasing.

The superiority of elliptic curve algorithm over RSA and such other encryption algorithms is that it provides the same level of security with a smaller length key.

Table 2. *A comparison of Key Lengths and Security (Cohen et al., 2005)*

	Band Width		*Key Length*	
	Key lengths for messages longer than 2000 bits (bit)	*Length of the 100 bit message after encryption*	*Public Key (bit)*	*Private Key (bit)*
RSA	*1024*	*1024*	*1088*	*2048*
ECC	*320*	*321*	*161*	*160*

This situation is clearly observable in Table 1 where a comparison of key lengths with respect to the encryption algorithms is given. (Cohen et al., 2005).

In parallel with the progress of technology, encryption algorithms such as RSA, DES, 3DES, ECC Elliptic Curve Cryptography and others have been developed. Enabling the use of smaller lengths for the keys, while providing the same level of security, elliptic curve encryption, seems to be a need in the near future.

Keywords: *Cryptology, Numeric signature, El-Gamal Elliptic Curve Algorithm*