ELİPTİK EĞRİ ŞİFRELEME ALGORİTMASI KULLANAN DİJİTAL İMZA UYGULAMASI

Tarık YERLİKAYA[1] Ercan BULUŞ[2] Derya ARDA[3]

[1,2,3]Bilgisayar Mühendisliği Bölümü
Mühendislik-Mimarlık Fakültesi
Trakya Üniversitesi, 22100, Edirne
[1]e-posta: tarikyer@trakya.edu.tr [2] e-posta: ercanb@trakya.edu.tr
[3]e-posta: deryaa@trakya.edu.tr

Anahtar sözcükler:ECC, Dijital İmza, Kriptanaliz, RSA, Eliptik Eğriler, DSA, RSA

ABSTRACT

In this study we explain mathemetic behind of the elliptic curves and using of elliptic curves in cryptography. As known in cryptograhy especially in public key cryptography, the mathematic behind of the algorithm is most important for the strength of the algorithms. Also in this paper we discribe the cryptanalysis approachs for elliptic curve cryptography. Especially we explain the algorithm of the elliptic curve cryptography and comparassion with the other public- key crypto (RSA, DH, DSA). Finally we present an application which shows how ECC works while two system identifying each other by digital signature. In this application, a program of C++ will be shown.

1. GİRİŞ

Günümüzde , teknolojinin gelişimiyle birlikte bilgisayarlar ve internet hayatımızda çok büyük yer sahibi olmaya başlamıştır. Daha çok insanın online olduğundan beri internet üzerinden işlemler yapmak kaçınılmaz bir hal almıştır. Bunun en önemli sonucu olarak e-ticaret büyük bir önem kazanmıştır. IP ağlarındaki dezavantajlarından biride güvenliktir, güvenliği sağlamanın yolu da şifreleme ve kimlik denetiminden geçmektedir.E-ticaret ve bankacılık sisteminin gelişimi ile birlikte bu sistemlerin güvenliğinin sağlanması için şifreleme algoritmaları kullanılmaya başlanmıştır.

Şifreleme ve deşifreleme dönüşüm fonksiyonlarının tek ve aynı anahtar kullandığı simetrik kripto sistemler, hızlı ve birçok açıdan etkin olmalarına mutlak ve koşulsuz güvenli kripto sistemler sunabilmelerine karşın, tüm sistem güvenliğinin kullanılan anahtarla belirlenmesi bu sistemlerin en zayıf yanını oluşturmaktadır.

Bilgisayar bilim ve teknolojisinin eriştiği yüksek düzey göz önüne alındığında, simetrik kripto sistemlerin mutlak biçimde korumak zorunda oldukları anahtarların koruma ve dağıtım maliyetinin ne kadar yüksek ve koruma işleminin ne kadar zor olduğu kolayca görülebilir. Sırf bu nedenden ötürü, karşılıklı haberleşme içinde olan iki tarafın güvenli dağıtım kanalları oluşturması özellikle güncel bankacılık sisteminde , yaygın görülen bir örnektir.

Öte yandan, şifreleme ve deşifreleme dönüşüm fonksiyonlarının kullandıkları anahtarlar birbirinden ayrılarak anahtar güvenliği sorunu kesin biçimde çözülebilir. Anılan çözüm, anahtarların farklılığı nedeniyle Asimetrik Kripto sistem olarak bilinen ve ilk kez 1976'da Diffie ve Hellman (EL-GAMAL şifreleme algoritması) tarafından belirlenen yeni bir dönüşüm tekniğiyle elde edilmektedir. Şifreleme ve deşifreleme dönüşüm fonksiyonlarının birbirinden farklı anahtarlar kullanması, şifreleme anahtarının herkes tarafından bilinen açık bir anahtar olmasını sonuçlarken, deşifre anahtarı sadece yetkili alıcı tarafından bilinen gizli anahtar niteliğini yaratmıştır. Şifre anahtarı halka açık tutulduğu için, Asimetrik şifreleme algoritmaları aynı zamanda Halk Anahtarlı Kripto sistemler (public key cryptosystem-PKS) olarak da bilinir.[1]

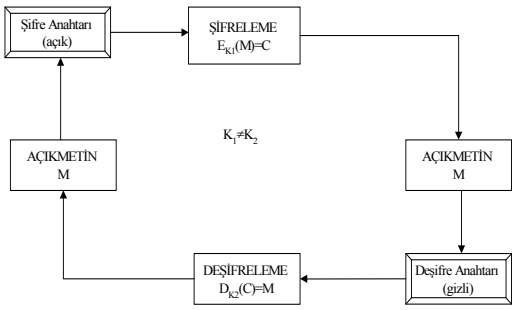
Bu çalışmada Asimetrik şifreleme algoritmalarının en önemlisi ve günümüzde kullanılan, Eliptik Eğri Şifreleme algoritmasını(ECC) algoritmasını inceleyeceğiz.

2. AÇIK ANAHTARLI ŞİFRELEME ALGORİTMALARINA BAKIŞ

Asimetrik Kripto sistemlerin en karakteristik özelliği; açık olan halk anahtarının ve ilişik kriptogranın, herkese açık ve dolayısıyla güvensiz bir kanaldan iletilebilmesidir

Asimetrik Kripto sistemlerin genel özelikleri aşağıda verildiği gibidir:

- Açık anahtar (Kp, p:public) ve gizli anahtar (K_s, s:secret) çiftinin oluşturulması basit olmalı ve alıcı tarafından polinomiyal zaman içinde yapılabilmelidir.
- Şifreleme işlemi **:**
  $C = E_{Kp}(M)$ olup, gönderici tarafından polinomiyal zamanda yapılabilmelidir.
- Alıcı tarafından yapılan deşifre işlemi, yine yalnız alıcı tarafından bilinen gizli anahtarla (K_s):$M = D_{Ks}(C)$ olarak ve polinomiyal zamanda gerçekleştirilebilmelidir.
- Düşman kriptanalist açık anahtardan (Kp) giderek, gizli anahtarı (K_s) oluşturmaya kalktığında çözümsüz bir sorunla karşı karşıya gelmelidir.
- Düşman kriptanalist, açık anahtar ve kriptogram (Kp, C) ikilisinden hareketle açık metni (M) bulmaya çalıştığında, yine çözümsüz bir sorunla karşılaşmalıdır.[1]



Şekil 1. *Asimetrik şifreleme algoritmalarının yapıları*

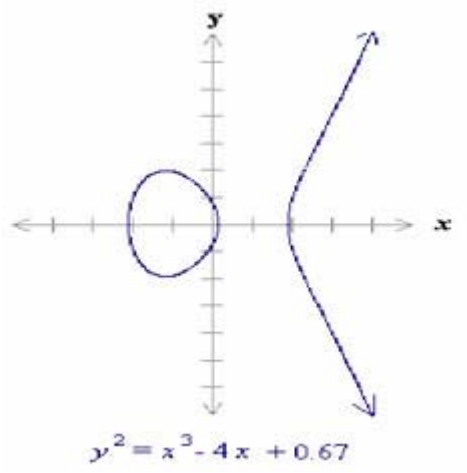
3. ELİPTİK EĞRİLER

Gerçel sayılar üzerinde bir eliptik eğri tanımlaması (x,y) noktalarının kümesi şeklinde olmaktadır. Bu eğrinin eşitliği Formül 1'deki gibi olmaktadır.

$y^2 = x^3 + ax + b$, x, y, a ve b sayıları gerçek sayılardır. (1)

a ve b'nin her seçiminde farklı bir eliptik ürün çıkmaktadır. Örneğin a = -4 ve b = 0,67 seçimi

$y^2 = x^3 - 4x + 0{,}67$ eliptik eğri denklemini vermektedir. Bu eğrinin çizimi Şekil 2'de görülmektedir.[16]



Şekil 2. *Eliptik Eğri Grafiği*

Eğer $x^3 + ax + b$ tekrarlamayan çarpanlar içerirse veya buna karşılık eğer $4a^3 + 27b^2 \neq 0$ ise eliptik eğri $y^2 = x^3 + ax + b$ grup formunda kullanılabilir. Gerçek sayılar üzerindeki eliptik eğri grubu benzer eliptik eğriler üzerindeki noktalardan oluşmakta ve beraberinde özel bir nokta olan O sonsuzluk noktası olarak adlandırılır.[2]

4. ELİPTİK EĞRİLERİN ŞİFRELEMEDE KULLANILMASI

Eliptik eğri gruplarının sonlu alanlar üzerinde tanımlanmasının kripto sistem için temel alınması ilk olarak Neal Koblitz ve Victor Miller in 1985.tarafından önerilmiştir [4]. Eliptik eğri yaklaşımı standart RSA sisteminden daha zengin matematiksel prosedürler içermektedir. Bu kripto sistemin temel birimleri eliptik eğri üzerindeki (x,y) noktalarıdır ve Formül 2'de gösterilmiştir.[9]

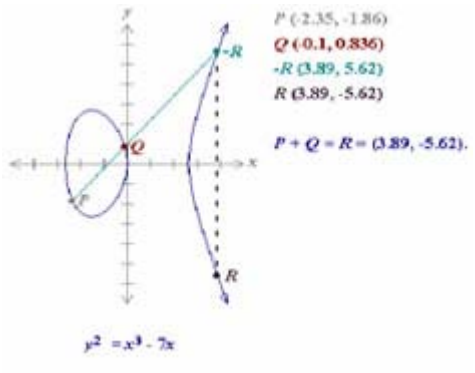
$y^2 = x^3 + ax + b$ birlikte

$x, y, a, b \in IFp = \{1, 2, 3, \ldots, p-2, p-1\}$ (2)

Herhangi bir kripto sistem için temel bir durum, o sistemin kapalı olmasıdır. Örneğin sistemin diğer elemanları içindeki sistemin sonuçlarının elamanları üzerindeki herhangi bir işlem. Bu kuralın eliptik eğrilerde sistemin kapalılığını sağlaması için standart olmayan toplama ve çıkarma işlemleri tanımlanması gereklidir

3.1. Eliptik Eğriler Üstünde Matematiksel İşlemler

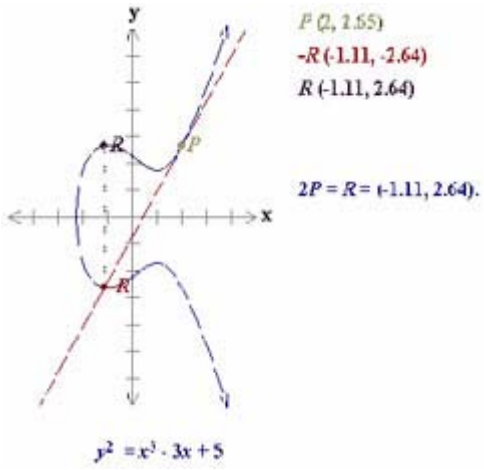
P ve Q eliptik eğri üstünde iki farklı nokta olsun. P ve Q noktalarını toplamak için ilk önce P ve Q noktaları üstünden gecen bir doğru çizilir. Bu doğru eliptik eğri üstünde sadece -R adı verilen bir noktada kesmektedir. –R noktasının x eksenin göre tersini aldığımızda R noktasına ulaşırız. Bu nokta P ve Q noktasının toplamı olmaktadır.[8]



Şekil 3. P+Q = R

Bir P noktasını çift katlı yapmak için, bir teğet çizgisi çizip eğriyi kestiği diğer noktayı buluruz. Eğer bu noktaya R diyecek olursak ;

P + P = R eşitliği sağlanır[7]



Şekil 4. P + P = R

4. ELİPTİK EĞRİ ŞİFRELEME ALGORİTMASI (ECC)

Eğer EC üzerindeki P(x,y) noktası kendini tekrar kendini ekliyorsa; n kere.

P+P+P+.....+P=nP=Q
← n kere →

.EC'de kullanılan P(x,y),Q(x,y) bulunması kolay olsa da n 'i bulmak çok zordur.

P ve Q biliniyor olsa da n'i hesaplamak oldukça zordur. Bu ayrık logaritma problemi (ECDLP)bir sürü EC ile birleşip güvenlik sistemi olan ECC'nin temelini oluşturur(Elliptic Curve Cryptosystem).

5. ECC ALGORİTMASININ KRİPTANALİZİ

ECC şifreleme algoritması ECDLP (Eliptik eğri ayrık logaritma problemi) problemi üstüne kurulmuş bir şifreleme sistemi olduğunu söylemiştik. ECC algoritması üstüne yapılan kriptanalizler bu problemin çözümü üzerine yapılan çalışmalarla gerçekleştirilebilir.[4]

Bu çalışmaların en önemlileri

1. Pollard'ın Rho Algoritması
2. Gaudry – Hess – Smart Attack (Ghs)
3. Weil Descent

ECDLP'yi çözmek için kullanılan algoritmalardan en bilineni ve en genel-amaçlı olan algoritma Pollard' ın rho algoritmasıdır. Tüm-üssel olarak çalışma zamanı $(pr)^{1/2}/2$ nokta toplamıdır. Sabitlenmiş bir Fq alanı, Pollard'ın rho metoduna maksimum rezistansı ile r asal olmak ve olabileceği kadar büyük bir sayı olması koşulu ile E de bir eliptik eğri seçimi yapılmaktadır. Örneğin r≈q. kriptanalistlerin karşılaştığı zorluklar, bu eğrileri hızlı çözebilecek eliptik eğri ayrık logaritmik problemler keşfetmek olmuştur[7]

Sonlu bir A alanı eliptik eğri kriptografisinde eğer k üzerindeki tüm eliptik eğriler ayrık logaritma problemi için örnekleniyor ise örneklerin zayıf olduğu söylenmektedir. Bunlar Pollard'ın rho metodu ile daha zor örneklerin çözümünden daha kısa sürede çözülebilmektedir.

5. GELECEK NEDEN ECC?

Çoğu kuruluş çalışanların verimliliğini arttırmak ve ağ üzerinde uygun bir işbirliği sağlamak için kablosuz ağ sistemini yaygınlaştırıyor.Bu ağ sistemlerinin korunması büyük bir önem teşkil eder.Çünkü kablosuz ağ trafiği kolayca engellenmeye açık olabilir.

Kablosuz ağ kullanıcılarının isteklerine bakıldığında güvenliğin en önemli koşul olduğu gözlenir.Bununla birlikte kablosuz donanımlara güvenlik düzeyinin kurulması kaynakların sınırlarına karşı bir meydan okuma,kaynakların sınırlarını zorlama anlamına gelebilir (depolama,batarya ömrü,güç oluşumu gibi).Çözüm ise bu kaynaklardan bazılarının küçük pratik değerlerle tüketilmesiyle elde edilebilir.

Sonuçta,araştırmacılar zorlanmış kaynakların ortamının güvenliğine yer bulma uyuşması içinde

bulurlar bazen kendilerini.Olumlu gelişme ise araştırmacıların güvenlik sistemlerini ECC ile sağlanmış performans konularına uyuşturma zorunluluklarının olmamaması oldu.

Bazı güvenlik sistemleri 1024-bit RSA genel anahtarlama planının uygulamasını yaymaya çalışıyor çünkü kuruluşlar bunun yeterince iyi olduğunu düşünüyorlar.

Bununla birlikte bu tehlikeli bir yaklaşım.Çünkü genel anahtarlama sisteminin güvenliği kullanılan simetrik şifrelemeyle birebir eşleşmiş olmalı.Tablo 1 de görüldüğü gibi, 1024-bit RSA simetrik şifrelemede kullanılan 128-bit güvenlik seviyesiyle uyuşmuyor.Bu gereksinimi karşılamak yani genel anahtarlama planını eşleştirmek için istenen 3072-bit RSA yada 256-bit ECC kullanılmasıdır.

Tablo 1. ECC ile Diğer Algoritmaların Anahtar Uzunluklarının Karşılaştırılması

Güvenlik (Bits)	Simetrik Şifreleme algoritmaları	DSA / DH	RSA	ECC
80	Skipjack	1024	1024	160
112	3DES	2048	2048	224
128	AES-128	3072	3072	256
192	AES-192	7680	7680	384
256	AES-256	15360	15360	512

5.1 ECC'nin Yararları

Küçük anahtar kullanımının sağladığı avantajlar arasında hız,küçük anahtarlar yada sertifikalar bulunur. Bu avantajlar, aşağıdaki kaynaklardan herhangi birinin sınırlı olduğu ortamlarda gerçekten çok önemlidir:

-işlemci gücü
-saklama kapasitesi
-bant genişliği
-güç tüketimi

Sonuç olarak, ECC'nin smart kartlar,cep telefonları, PDA'lar, sayısal posta işaretleri gibi zorunlu ortamlara tam olarak uygun olduğudur.

6. ECC İLE DİJİTAL İMZA UYGULAMASI

Yaptığımız uygulamada ECC kullanarak dijital imza uygulaması gerçekleştirdik. C++ programlama dili kullandık.

Gerçekleştirdiğimiz programda öncelikle eliptik eğriyi seçiyoruz. Programımız eliptik eğri üstündeki kullanacağımız bütün noktaları göstermektedir.

Örneğin iki kişi uygun eliptik eğriyi seçiyor.

$y^2 = x^3 - x + 200$, $p=751$; Ep (-1, 200)

ve daha sonra bu eliptik eğri üstünde bir nokta belirliyorlar. G=(0,379).

Dijital imza gerçekleştirecek bu kişiler kendilerinin bileceği gizli anahtarları belirliyorlar.

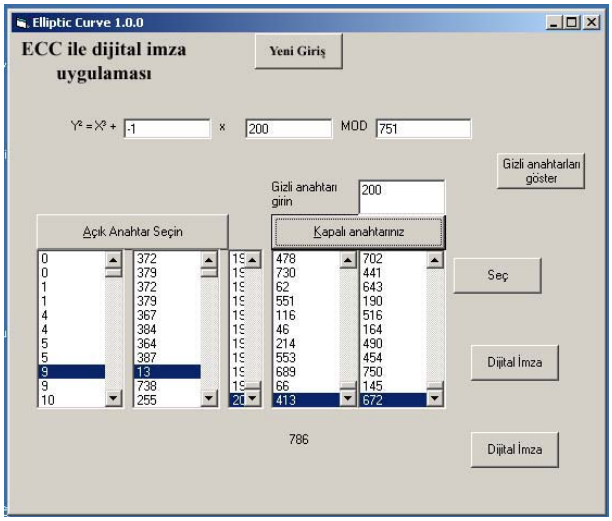
$K_A = 251$, $K_A * G = P_A$ (236,370)
$K_B = 370$, $K_B * G = P_B$ (426,527)

Bu noktada P_A ve P_B kişilerin açık anahtarları oluyor. Birbirlerinin açık anahtarlarını kullanarak

$C = K_A * P_B$ and $C = K_B * P_A$

Yukarıdaki işlemi gerçekleştiriyorlar. Birbirlerinin gizli anahtarlarını bilmeden aynı sonuca ulaşabiliyorlar. Ve dijital imzayı gerçekleştiriyorlar.

Programımız ayrıca şifreleme ve deşifreleme işlemlerini gerçekleştirmektedir. Aşağıda şekil programımızın formatını göstermektedir.



Şekil 5. Dijital İmza Uygulama Programının Gösterimi

7. SONUÇ

Açık anahtarlı şifreleme algoritmaları çözülmesi zor matematiksel problemler üzerine kurulmuş algoritmalardır. Bu algoritmaların daha güvenli hale getirmek için büyük anahtar değerleri kullanılmaktadır. Büyük anahtar değerlerini kullanmak birçok uygulamada şifreleme ve deşifreleme sürelerini uzatmaktadır..Şifreleme algoritmalarının güçlü güvenliğe sahip olmaları yanında yeni donanımlarla gerçekleştirilebilmeleri , kolaylık ve performansı yüksek olması göz önünde bulundurulmalıdır Aynı şekilde yazılım olarakta

kolaylığı ve işlemciyi fazla meşgul etmemesi gerekmektedir

Bu çalışmada ECC şifreleme algoritmasını inceledik. ECC şifreleme algoritması ECDLP matematiksel problem üstüne kurulmuş bir şifreleme algoritmasıdır. ECC şifreleme algoritmasının en büyük özelliği diğer açık anahtar şifreleme sitemlerinin güvenliğini daha düşük anahtar değerleriyle sağlayabilmesidir.Bu çalışmada da bahsettiğimiz gibi 1024 -bitlik anahtar kullanan RSA şifreleme algoritmasının sağladığı güvenlik gücünü, 160 bit anahtar kullanan ECC sağlayabilmektedir. Bu açık anahtarlı algoritmalar içinde çok önemli bir avantajdır.

Teknolojinin gelişimiyle birlikte yeni oluşturulan şifreleme algoritmaları bu donanımsal yapıya uyum sağlamalıdır. Yeni oluşturulan kablosuz ağlarda güvenliğin sağlanması çok önemlidir. Güvenliğin sağlanmasıyla birlikte, kablosuz ağlarda kullanılacak şifreleme algoritmalarının kısıtlı bant genişliğini kullanmaları çok önemlidir. ECC de düşük anahtar kullanımıyla kablosuz ağlar için çok önemli bir şifreleme algoritmasıdır.

Sonuç olarak ECC, RSA şifreleme algoritmasının yerini alabilecek çok önemli avantajlara sahip bir açık anahtarlı şifreleme algoritmasıdır.

KAYNAKLAR

[1] Koblitz, N.: A course in Number theory and Cryptography, Springer Verlag , 1994.

[2] A.Koltuksuz, "Securing .NET Architecture With Elliptic Curve Cryptosystems", İzmir Institute of TechnologyCollege of Engineering Department of Computer Engineering İzmir, Turkey, 2005

[3] A. Koltuksuz. "Elektronik Ticarette Güvenlik, Özgürlük Denetimi, Doğruluk-Bütünlük ve Sayısal İmza ", 4.Türkiye İnternet Konferansı, 1998, istanbul, Türkiye

[4] J. Pollard, "Monte Carlo methods for index computation mod *p*", *Mathematics of Computation*, 32 (1978), 918-924.

[5] A. Koltuksuz, " Cryptography in Action" ISCIS'99, 1999

[6] N.P. Smart. How secure are elliptic curves over composite extension fields? Advances in Cryptology - EUROCRYPT '01, Springer-Verlag LNCS 2045, 30{39, 2001

[7] N. Koblitz: Elliptic Curve Cryptosystems. Math Comp Vol. 48, (1987) 203-209.

[8] Elliptic Curve Cryptography http://en.wikipedia.org/wiki/Public-key_cryptography

[9]http://www.certicom.com/index.php?action=ecc_tutorial,ecc_tut_2_1_2

[10] Victor S. Miller" Use Elliptic Curve In Cryptography".Exploratory Computer Science

[11] T. El Gamal. "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. Advances in Cryptology: Proceedings of CRYPTO" 84, Springer Verlag, pp. 10-18, 198

[12] Ernst Kani. "The State Of The Art Of Elliptic Curve Cryptography", Queen's University

[13] Bruce SCHNEIDER*,1996."Applied Cryptography,second edition,New York*

[14] T. YERLİKAYA, E. BULUŞ, "New Generation Public Key Crypto: Elliptic Curve Cryptography", International Scientific Conferance, GABROVO 2004

[15] Masophia LESAOANA. ,"*A Comparison of RSA and Elliptic Curve Cryprography*

[16] Scutt A.Vanstone. ,"Next Generation Security for Wireless: Elliptic curve cryptography". Certicom

[17] Eric W. EVERSTİENE,Partial Key Exposure Attack OnLlow-Exponent RSA,

[18] M.Aydos, E. Savas and C.K.Koc. "Implementating Network Security Protocols based on Elliptic Curve Cryptography"

[19] R. Lercier, Finding good random elliptic curves for cryptosystems defined F2*n* , Advances in Cryptology—EUROCRYPT '97, Lecture Notes in Computer Science, Springer-Verlag, 1233 (1997) pp. 379–392.

[20] Vanstone, Scott, Menezes, Alfred *Introduction to Elliptic Curve Cryptograph Technology.* New York *:* Springer-Verlag. (2002).