SİMETRİK ve ASİMETRİK KRİPTO SİSTEMLER

Zeynep ERZURUMLU

Yüksek Lisans Tezi
Matematik Anabilim Dalı
Prof. Dr. Hüseyin AYDIN
2013

ATATÜRK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

SİMETRİK ve ASİMETRİK KRİPTO SİSTEMLER

Zeynep ERZURUMLU

MATEMATİK ANABİLİM DALI

ERZURUM
2013

T.C.
ATATÜRK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

TEZ ONAY FORMU

SİMETRİK ve ASİMETRİK KRİPTO SİSTEMLER

Prof. Dr. Hüseyin AYDIN danışmanlığında, Zeynep ERZURUMLU tarafından hazırlanan bu çalışma 12/01/2013 tarihinde aşağıdaki jüri tarafından. Matematik Anabilim Dalı'nda Yüksek Lisans tezi olarak **oybirliği/oy çokluğu (.../...)** ile kabul edilmiştir.

Başkan	: Prof. Dr. Hüseyin AYDIN	*İmza*	:
Üye	: Prof. Dr. Erdal KARADUMAN	*İmza*	:
Üye	: Doç. Dr. Şakir AYDOĞAN	*İmza*	:

Yukarıdaki sonucu onaylıyorum

Prof. Dr. İhsan EFEOĞLU
Enstitü Müdürü

Not: Bu tezde kullanılan özgün ve başka kaynaklardan yapılan bildirişlerin, çizelge, şekil ve fotoğrafların kaynak olarak kullanımı, 5846 sayılı Fikir ve Sanat Eserleri Kanunundaki hükümlere tabidir.

ÖZET

Yüksek Lisans Tezi

SİMETRİK ve ASİMETRİK KRİPTO SİSTEMLER

Zeynep ERZURUMLU

Atatürk Üniversitesi
Fen Bilimleri Enstitüsü
Matematik Ana Bilim Dalı

Danışman: Prof. Dr. Hüseyin AYDIN

Bu tezde simetrik ve asimetrik kripto sistemler tanıtılmış ve bu sistemlere örnekler verilmiştir. Sayısal imza ifade edilerek sayısal imza algoritmalarına ve örneklerine yer verilmiştir. Hash fonksiyonları ve kriptolojik hash fonksiyonları tanıtılmıştır.

2013, 63 sayfa

Anahtar Kelimeler: Asimetrik, Simetrik Kriptoloji, Eliptik Eğri Kriptoloji, Sayısal İmza, Hash Fonksiyonları

ABSTRACT

M.S. Thesis

SYMETRIC and ASYMETRIC CRYPTO SYSTEMS

Zeynep ERZURUMLU

Atatürk University
Graduate of Naturel and Applied Sciences
Departmant of Mathematics

Supervisor: Prof. Dr. Hüseyin AYDIN

In this study, some informations are given about symetric and asymetric crypto systems and some examples for them. Some digital signature systems are introduced in this study. Hash functions are also explicated and cryptographic hash functions are introduced.

2013, 63 page

Keywords: Asymetric , Symetric Cryptography, Eliptic Curve Cryptography, Digital Signature, Hash Functions.

TEŞEKKÜR

Yüksek Lisans Tezi olarak sunduğum bu çalışma Atatürk Üniversitesi Fen Fakültesi Matematik Bölümü'nde yapılmıştır.

Bu tezde çalışmalarımla yakından ilgilenen ve yardımlarını esirgemeyen çok değerli hocam Sayın Prof. Dr. Hüseyin AYDIN'a en içten dileklerimle sonsuz teşekkür eder saygılarımı sunarım.

Çalışmam esnasında matematik bölümünde gerekli ilgi ve yardımı esirgemeyen anabilim dalımızın değerli Öğretim Üyeleri Sayın Prof. Dr. Erdal KARADUMAN'a, Sayın Doç. Dr. İnci GÜLTEKİN'e, Sayın Yrd. Doç. Dr. Nurullah ANKARALIOĞLU'na ayrıca Sayın Arş. Gör. Rukiye ÖZTÜRK'e, Sayın Arş. Gör. Sait TAŞ'a ve matematik bölümünün diğer tüm elemanlarına;

Çalışmalarım boyunca benden sevgilerini, desteklerini ve güvenlerini esirgemeyen değerli aileme en içten dileklerimle sonsuz teşekkürlerimi sunarım.

Zeynep ERZURUMLU

Ocak, 2013

İÇİNDEKİLER

SİMGELER ve KISALTMALAR DİZİNİ

(a.b)	a ile b nin en büyük otak böleni
ÇDHF	Çakışma Dirençli Hash Fonksiyonu
ECC	Eliptik Eğri Kriptoloji(Eliptik Curve Criptography)
ECDSA	Eliptik Eğri Sayısal İmza Algoritması (Eliptik Curve Digital Signature Algorithm)
MAC	Mesaj Kanıtlama Kodu (Mesage Authentication Code)
MDC	Mesaj Değişiklik Bulma Kodu (Manipulation Detection Code)
NIST	Ulusal Güvenlik Teknoloji Enstitüsü
NSA	Ulusal Güvenlik Ajansı (National SecurityAgency)
$\mathbb{R}$	Reel Sayılar kümesi
SHA	Güvenli Hash Algoritması (Security Hash Algorithm)
THYF	Tek Yol Hash Fonksiyonu
$\mathbb{Z}$	Tam sayılar kümesi
$\mathbb{Z}_n^*$	Çarpımsal grup
$\overline{Q_n}$	Modn ye göre kuadratik non-rezidülerin kümesi
Q_n	Modn ye göre kuadratik rezidülerin kümesi
$\mathbb{Q}$	Rasyonel sayılar kümesi
$\oplus$	XOR işlemi
$\|\|$	Birleştirme

ŞEKİLLER DİZİNİ

1. GİRİŞ

Kriptoloji bir verinin şifrelenmesi (kriptografi) ve şifrelenmiş metinin analizini (deşifreleme) içeren matematiğin bir dalıdır. Teknolojideki hızlı gelişmeler verilerin güvenli bir şekilde iletilmesinin önemini artırmıştır. İlk olarak yaklaşık 4000 yıl önce kullanılmıştır. Kripto tarihçisi David Kahn'a göre ilk kriptografik belge M.Ö 1900'lere dayanan bir lordun hayatını anlatan bir hiyegroliftir. 2000 yıl önce Roma imparatoru Julius Ceasar tarafından oluşturulan ve simetrik anahtar şifrelemenin ilk örneği sayılan Ceasar şifresi alfabedeki harfleri kendinden üç sonraki harfe götüren basit yerine koyma şifresidir. Diplomasi ve askeri haberleşmelerde kullanılan gizli haberleşme özellikle 2. Dünya savaşında büyük rol oynamıştır.

Sanayi devrimine kadar ilkel yöntemlerle oluşturulan şifreleme sistemleri, makinelerin icadı ile boyut değiştirmiş ve teknolojinin hızı ile doğru orantılı olarak kırılamayacak şifreleme sistemleri oluşturma çabaları devam etmiştir.

1970'de ABD ileri teknoloji enstitüsü NIST tarafından geliştirilen DES (Data Encryption Standart) tarihte en iyi bilinen sistemdir.

1970'lerde bilgisayar ve matematiğin etkin bir şekilde kullanılmaya başlanması ile şifreleme sistemleri Simetrik ve Asimetrik şifreleme sistemleri olarak ikiye ayrıldı.

Simetrik anahtarlı sistemlere gizli anahtarlı şifreleme de denebilir. Bu sistemlerde kullanıcılar önceden bir araya gelerek ortak bir anahtar üzerinde anlaşırlar veya güvenli bir aracı ile anahtar paylaşımı yaparlar. Bu simetrik anahtar şifrelemenin en büyük dezavantajıdır.

Diffie ve Hellman tarafından yayınlanan "New Directions In Cryptology" adlı makale kriptoloji de bir dönüm noktası olmuştur. Yayınladıkları makale ile anahtar değişimi problemine çözüm getirmişlerdir. 1978 de Rivest, Shamir ve Adleman yayınladıkları

makale ile RSA olarak ifade edilen ilk pratik açık anahtar şifreleme tasarısını öne sürmüşlerdir. RSA modüler aritmetiği kullanarak üs alma işlemine dayanırken; El Gamal 1985'de ayrık logaritma problemine dayanan bir açık anahtar kriptosistem geliştirmiştir. Daha sonraları ayrık logaritma problemi sonlu cisimler üzerinde tanımlı eliptik eğrilerde kullanılarak açık anahtar sistemlere yeni bakış açıları kazandırılmıştır. Daha farklı açık anahtar ve gizli anahtar sistemler vardır. Bunlardan biri de 2011 yılında F. Chen, X. Liao, T. Xiang, H.Zheng tarafından yayınlanan Chebysev Polinomlarına dayalı açık anahtar sistemdir (Kocarev *et al.* 2005).

Teknolojinin hızla ilerlemesi ve internet kullanımının her alanda yaygınlaşması kriptolojinin önemini giderek artırmıştır. Başlangıçta gizlilik için kullanılan kriptoloji internet kullanımının yaygınlaşması ile kimlik ve veri doğrulamada sayısal imza ile kullanım alanı gelişmiştir. Sayısal imzalar açık anahtar sistemler ile oluşturulur. Bir verinin doğruluğu, göndericinin doğrulanması ya da gönderilen veriye göndericinin haberi dışında bilgi eklenmesi ya da bilgi silinmesini önlemek için sayısal imza kullanılır. Sayısal imzalarda özet(hash fonksiyonları) fonksiyonlarından yararlanılır.

2. KURAMSAL TEMELLER

2.1. Temel Matematiksel Kavramlar

Bu bölümde bu çalışmada kullanacağımız bazı tanım, teorem, lemma ve örneklere yer verilecektir.

Tanım 2.1.1: A ve B boştan farklı iki küme olsun. $f \subset A \times B$ aşağıdaki şartları sağlıyorsa bu *f* bağıntısına fonksiyon denir;

1) Her $a \in A$ için öyle bir b$\in B$ vardır ki $(a, b) \in f$ dir.
2) $(a, b_1) \in f$ ve $(a, b_2) \in f$ ise $b_1 = b_2$ dir.

Burada A kümesine *f* fonksiyonun tanım kümesi, B kümesine de değer kümesi denir.

Tanım 2.1.2: $f: A \to B$ fonksiyonu $b \in B$ için ön görüntüsü $f(a) = b$ olacak şekilde bir $a \in A$ vardır. B de en az bir ön görüntüye sahip tüm elemanların kümesine *f*'nin görüntü kümesi denir ve *Im(f)* veya $f(A)$ ile gösterilir.

Tanım 2.1.3: $f: A \to B$ fonksiyon olsun. Eğer, her $x_1, x_2 \in A$ için $f(x_1) = f(x_2)$ iken $x_1 = x_2$ oluyorsa *f* fonksiyonuna bire-bir fonksiyon denir.

Tanım 2.1.4: $f: A \to B$ fonksiyon olsun. $f\ (A) = B$ oluyorsa f fonksiyonuna örten fonksiyon denir.

Tanım 2.1.5: Bir fonksiyon hem bire-bir hem de örten ise bu fonksiyona bire-bir ve örten fonksiyon denir.

Tanım 2.1.6: $f: A \to B$ bire-bir ve örten bir fonksiyon olsun. $\forall\, b \in B$ için $g(b) = a, a \in A$ olacak şekilde $g: B \to A$ bire-bir ve örten fonksiyonu bulunabilir. f den elde edilen bu g fonksiyonuna f 'nin ters fonksiyonu denir ve f^{-1} ile gösterilir.

Tanım 2.1.7: $f: A \to B$ fonksiyon olsun. Eğer $\forall\, a \in A$ için $f(a)$ hesaplamak kolay fakat tüm $b \in Im(f)$ için $f(a) = b$ olacak şekilde $a \in A$ bulmak kolay hesaplanabilir değilse f 'ye tek yol fonksiyon denir.

Tanım 2.1.8: $f: A \to B$ tek yol fonksiyon olmak üzere $f(a) = b$ olacak şekilde herhangi bir $b \in Im(f)$ için; $a \in A$ bulmayı kolaylaştıran bazı ek bilgiler verilmiş ise bu tek yol fonksiyona trapdoor tek yol fonksiyon denir.

Tanım 2.1.9: a ve b tam sayılar olmak üzere eğer $b = a.c$ olacak şekilde c tam sayısı varsa $a,\ b$'yi böler denir ve $a|b$ ile gösterilir.

Teorem 2.1.1: $a, b, c, d \in \mathbb{Z}^+$ olmak üzere aşağıdaki ifadeler doğrudur.

i) $1|a$ ve $a|a$ dır.
ii) Eğer $a|b$ ise $a \leq b$ dir.
iii) $a|b$ ve $b|c$ ise $a|c$ dir.
iv) $a|b$ ve $b|a$ ise $a = b$ dir.
v) Eğer $a|b$ ve $c|d$ ise $ac|bd$ dir.
vi) Eğer $a|b$ ve $a|c$ ise $\forall\, x, y \in \mathbb{Z}\ için\ a|(bx + cy)$ dir.
vii) $(b, c) = 1$ olmak üzere; $ab|c$ ise $a|c$ dir.

Tanım 2.1.10: Pozitif tam sayı bölenleri yalnız 1 ve kendisi olan ve 1 den büyük tam sayılara asal sayı denir.

Teorem 2.1.2 (Bölme Algoritması): Her $a, b \in \mathbb{Z}$ olmak üzere $b = qa + r\ ve\ 0 \leq r < a$ olacak şekilde bir tek $q, r \in \mathbb{Z}$ tam sayı çifti vardır.

Tanım 2.1.11 (En Büyük Ortak Bölen): a ve b sıfırdan farklı tam sayılar olmak üzere

$d|a \; ve \; d|b$ olacak şekilde bir $d > b$ tam sayısı varsa d'ye a ve b'nin ortak böleni denir. a ve b'nin ortak bölenlerinin en büyüğüne a ve b sayılarının en büyük ortak böleni denir ve (a, b) ile gösterilir. $(a, b) = d$ ise d aşağıdaki iki şartı sağlar;

i) $d|a$ ve $d|b$
ii) $c|a$ ve $c|b$ ise, $c|d$ olmalıdır.

Tanım 2.1.12: İki tam sayının en büyük ortak böleni 1 ise yani $(a, b) = 1$ ise a ve b tam sayılarına aralarında asaldır denir.

Tanım 2.1.13 (En Küçük Ortak Kat): Aşağıda verilen iki özelliği sağlayan d, $d > 0$ sayısına a ve b tam sayılarının en küçük ortak katı denir ve $[a, b]$ile gösterilir.

i) $a|d$ ve $b|d$
ii) $a|c$ ve $b|c$ ise, o zaman $d|c$ olmalıdır.

Teorem 2.1.3 (Aritmetiğin Temel Teoremi): $n \geq 2$ olan her n tam sayısı ya asaldır ya da asalların çarpımı şeklinde (çarpanların sıra değişikliği hariç) tek türlü yazılır. Yani p_i ler farklı asallar ve e_i ler doğal sayılar olmak üzere $n = {p_1}^{e_1}{p_2}^{e_2}{p_3}^{e_3} \ldots . {p_t}^{e_t}$ dır.

Teorem 2.1.4 (Euclid Algoritması): a ve b, $b \leq a$ olacak şekilde pozitif tam sayılar olsun. Eğer $b|a$ ise $(a, b) = b$ olur. Eğer b a' yı bölmezse; Bölme Algoritması ard arda aşağıdaki gibi uygulanırsa;

$a = q_0 b + r_0, 0 < r_0 < b$
$b = q_1 r_0 + r_1, 0 < r_1 < r_0$
$r_0 = q_2 r_1 + r_2, 0 < r_2 < r_1$
$r_1 = q_3 r_2 + r_3, 0 < r_3 < r_2$

.
.
.

ifadeleri elde edilir. Bu durumda $r_0 > r_1 > r_2$ ... şeklinde negatif olmayan tam sayıların bir dizisi ve adımların sonlu bir sayısından sonra sıfır kalanı elde edilecektir, yani

$r_{k-2} = q_k r_{k-1} + r_k, 0 < r_k < r_{k-1}$
$r_{k-1} = q_{k+1} r_k + 0,\ r_{k+1} = 0$

olacak şekilde bir pozitif k tam sayısı vardır. Son sıfır olmayan r_k kalanı a ile b'nin en büyük ortak bölenidir.

Tanım 2.1.14: $n \geq 1$ için $\varphi(n)$, [1, n] aralığında n ile aralarında asal olan tam sayıların sayılarını göstersin.φ fonksiyonuna Euler'in φ fonksiyonu denir.

Tanım 2.1.15: f özdeş olarak sıfır olmayan bir fonksiyon ve $(m, n) = 1$ olsun. $f(m.n) = f(m).f(n)$ ise f fonksiyonuna çarpımsaldır denir. Eğer $\forall\, m, n$ için $f(m.n) = f(m).f(n)$ oluyorsa f fonksiyonu komple çarpımsaldır denir.

Teorem 2.1.5: Euler φ fonksiyonu aşağıdaki özellikleri sağlar;

i) p asal ise $\varphi(p) = p - 1$
ii) $\varphi(n)$ çarpımsaldır yani $\varphi(m.n) = \varphi(m).\varphi(n)$
iii) $n = {p_1}^{e_1}{p_2}^{e_2}{p_3}^{e_3} \ldots . {p_t}^{e_t}$ ise $\varphi(n) = n.\left(1 - \frac{1}{p_1}\right).\left(1 - \frac{1}{p_2}\right) \ldots (1 - \frac{1}{p_t})$ dır.

Tanım 2.1.16: a ve b tam sayılar ve m sıfırdan farklı bir tam sayı olmak üzere

$m|(a - b)$ ise a tam sayısı b tam sayına m modülüne göre kongürenttir(denktir) denir ve $a \equiv b(mod n)$ ile gösterilir.

Teorem 2.1.6: $a, b, c, d\ ve\ 0 \neq m$ tam sayılar olmak üzere;

i) $a \equiv a(modm)$
ii) $a \equiv b(modm)$ ise $b \equiv a(modm)$ dır.
iii) $a \equiv b(modm)$ ve $b \equiv c(modm)$ ise $a \equiv c(modn)$ dir.
iv) $a \equiv b(modm)$ ise $a \pm c \equiv b \pm c(modm)$
v) $a \equiv b(modm)$ ve $c \equiv d(modm)$ ise $ac \equiv bd(modn)$ dir.
vi) $ac \equiv bc(modm)$ ve (c, m) =1 ise $a \equiv b(modm)$
vii) $a \equiv b(modm)$ ise $\forall\, n \in \mathbb{Z}^+\ a^n \equiv b^n(modm)$ dır.

Teorem 2.1.7 (Çin Kalan Teoremi): $m_1, m_2, \dots, m_r$ ikişer ikişer aralarında asal pozitif tam sayılar olsun. Bu durumda;

$x \equiv a_1(modm_1)$
$x \equiv a_2(modm_2)$
.
.
.
$x \equiv a_r(modm_r)$

lineer kongürans sistemi $M = m_1 m_2 \dots m_r$ modülüne göre bir tek çözüme sahiptir.

Teorem 2.1.8:

i) Euler Teoremi: $(a, m) = 1$ olmak üzere $a^{\varphi(m)} \equiv 1(modm)$ dir.

ii) Fermat Teoremi: p asal ve p $a'nın$ bir çarpanı olmasın. Bu takdirde $a^{p-1} \equiv 1(modp)$ dir.

Teorem 2.1.9: p asal sayı olsun;

i) $\forall\, a \in \mathbb{Z}$ için $r \equiv s(mod(\varphi(p))$ ise $a^r \equiv a^s(modp)$
ii) $\forall\, a \in \mathbb{Z}$ için $a^p \equiv a(modp)$

Tanım 2.1.17: Boştan farklı bir A kümesi üzerinde bir ikili işlem $*: A \times A \to A$ şeklinde bir dönüşümdür.

Tanım 2.1.18: G boştan farklı bir küme ve bu küme üzerinde bir ikili işlem $*$ olsun. Buna göre aşağıdaki şartlar sağlanırsa (G, $*$) cebirsel yapısına grup denir.

i) $\forall\, a, b, c\ \in G$ için $a * (b * c) = (a * b) * c$ (Birleşme özelliği)
ii) $\forall\, a \in G$ için $a * e = e * a = a$ olacak şekilde bir $e \in G$ vardır. (Etkisiz eleman)
iii) G kümesinde her bir a için $e, G'nin$ birim elemanı olmak üzere; $a * a^{-1} = a^{-1} * a = e$ olacak şekilde $a^{-1} \in G$ vardır (Ters eleman öz.).

Eğer bu şartlara ilave olarak $\forall\, a, b \in G$ için $a * b = b * a$ ise G grubuna değişmeli (abelyen) grup denir.

Gruplar grup işleminin toplamsal veya çarpımsal özelliğine göre toplamsal grup ya da çarpımsal grup olarak adlandırılır. Toplamsal gruplarda bir a elemanı için na a'nın kendisi ile n kez işleme sokulması ve çarpımsal gruplarda a elemanının n kez kendisi ile işleme sokulması a^n ile gösterilir.

Tanım 2.1.19: $(G,*)$ bir grup olsun. Eğer G kümesi sonlu ise gruba sonlu grup denir. Eğer G grubu sonlu grup değilse $(G,*)$ grubuna sonsuz grup denir. Sonlu bir grubun eleman sayısına grubun mertebesi ya da kardinalitesi denir ve $o(G)$ veya $|G|$ ile gösterilir.

Tanım 2.1.20: G bir grup olmak üzere G de $G = \{a^n : n \in N\}$ olacak şekilde bir $a \in G$ varsa G' ye devirli grup denir. Böyle bir a elemanına G'nin üreteci denir ve $G = < a >$ ile gösterilir.

Tanım 2.1.21: G bir grup ve $a \in G$ için $a^n = 1$ olacak şekilde en küçük pozitif n tam sayısına a elemanının mertebesi denir $o(a)$ ile gösterilir. Eğer böyle bir n sayısı yoksa a elemanının mertebesi sonsuzdur denir.

Tanım 2.1.22: $\mathbb{Z}_n$ de çarpımsal tersleri olan elemanların oluşturduğu küme $\mathbb{Z}_n^*$çarpma işlemine göre bir grup oluşturur. $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n : (a,n) = 1\}$ dır. $\mathbb{Z}_n^*$ çarpımsal grubunu mertebesi φ tanım 2.1.14. verilen Euler fonksiyonu olmak üzere $|\mathbb{Z}_n^*| = \varphi(n)$ dir.

Tanım 2.1.23: a ile m aralarında asal tam sayılar olsun. $a^t \equiv 1(modm)$ olacak şekilde en küçük t tam sayısına a'nın m modülüne göre mertebesi ya da a'nın m modülüne ait üssü denir. $Ord_m a = t$ şeklinde gösterilir.

Tanım 2.1.24: Eğer a'nın m modülüne göre mertebesi $\varphi(m)$ ise a ya m modülüne göre ilkel(primitif) kök denir.

Örnek 2.1.1: $3^6 \equiv 1(mod7)$ ve $\varphi(7) = 6$ olduğundan $Ord_7 3 = \varphi(7)$ olup 3, mod7 de bir ilkel köktür.

2.1.25 Tanım: $a \in \mathbb{Z}_n^*$ olsun $o(a) = \varphi(n)$ ise $a'ya\ \mathbb{Z}_n^*$ da bir ilkel kök ya da üreteç denir.

Teorem 2.1.10: $n > 0$ tam sayısı ilkel köke sahip ise ilkel köklerinin sayısı $\varphi(\varphi(n))$ tanedir.

Tanım 2.1.26 (Kuadratik Rezidü) : $0 < x < n$ için $x^2 \equiv q(modn)$ olacak şekilde bir x tam sayısı varsa q'ya $modn$'ye göre bir kuadratik rezidü(karesel kalan) aksi takdirde $modn$ de kuadratik rezidü(karesel kalan) değildir denir. $modn$'ye göre kuadratik rezidülerin kümesi Q_n ve kuadratik olmayan rezidülerin kümesi $\overline{Q_n}$ ile gösterilir.

Örnek 2.1.2: mod11'a göre kuadratik rezidü ve kuadratik rezidü olmayan sayıları bulalım.

$1^2 \equiv 1(mod11)$
$2^2 \equiv 4(mod11)$
$3^2 \equiv 9(mod11)$
$4^2 \equiv 5(mod11)$
$5^2 \equiv 3(mod11)$
$6^2 \equiv 3(mod11)$
$7^2 \equiv 5(mod11)$
$8^2 \equiv 9(mod11)$
$9^2 \equiv 4(mod11)$
$10^2 \equiv 1(mod11)$ olup mod11 de kuadratik rezidülerin kümesi $Q_{11} = \{1,3,4,5,9\}$ ve kuadratik rezidü olmayanların kümesi $\overline{Q_{11}} = \{2,6,7,8,10\}$ dır.

Teorem 2.1.11: p, bir tek asal sayı olmak üzere p nin kuadratik rezidülerin sayısı ile kuadratik olmayan rezidülerinin sayısı eşit olup $(p-1)/2$ tanedir.

Teorem 2.1.12: p tek asal ve α, $\mathbb{Z}_p^*$ bir üreteci olsun. $x \in \mathbb{Z}_p^*$ nin $modn$'ye göre kuadratik rezidü olması için gerek ve yeter şart i bir çift tam sayı olmak üzere;

$x \equiv a^i(modp)$ olmasıdır.

Tanım 2.1.27: $a \in Q_n$ olsun, $x \in \mathbb{Z}_n^*$ eğer $x^2 = a(modn)$ ise $x'e\ a(modn)$'nin bir karekökü denir.

Tanım 2.1.28 (Legendre Sembolü): p, bir tek asal ve a da p ile bölünemeyen bir tam sayı olsun.

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & a \in Q_p \\ -1 & a \in \overline{Q_p} \end{cases}$$

olarak tanımlanır.

Tanım 2.1.29 (Halka): R, boş olmayan bir küme olsun. R üzerinde her $a, b \in R$ için

$+: (a.b) \to a + b,\ .: (a, b) \to a.b$ biçiminde tanımlı ve sırasıyla, toplama ve çarpma denilen "+" ve "." ikili işlemleri verilsin. Eğer aşağıdaki şartlar sağlanırsa $(R, +)$ cebirsel yapısına halka denir.

i. (R, +) değişmeli bir grup,

ii. $\forall\ a, b, c \in R$ için $(a.b).c = a.(b.c)$

iii. $\forall\ a, b, c \in R$ için,

$a.(b + c) = a.b + a.c$ ve $(a + b).c = a.c + b.c$

$(R, +, .)$ halkası verilsin. Eğer ikinci işlem değişmeli ise halka değişmeli, ikinci işlem birimli ise halka birimli olur. Halkada toplama işleminin birim elemanına halkanın sıfırı denir ve 0_R ile gösterilirken çarpma işleminin birim elemanına halkanın birim elemanı denir 1_R ile gösterilir.

Tanım 2.1.30 (Karakteristik): Eğer R halkasında $\forall\ r \in R$ için $nr = 0_R$ olacak biçimde bir pozitif n tam sayısı varsa bu n sayılarının en küçüğüne R nin karakteristiği denir. Eğer böyle bir pozitif tam sayı yoksa R nin karakteristiği 0 olarak tanımlanır. R nin karakteristiği $kar(R)$ ile gösterilir.

Örnek 2.1.3: $\mathbb{R}, \mathbb{Z}, \mathbb{Q}$ halkalarının karakteristiği 0 dır. m pozitif bir tam sayı olmak üzere $kar(\mathbb{Z}_m) = m$ dir.

Tanım 2.1.31: R birimli ve değişmeli bir halka $0_R \neq 1_R$ olsun. Eğer R'nin sıfırdan farklı her elemanı tersinir ise R'ye cisim denir.

2.2. Kriptolojide Kullanılan Temel Kavramlar

Kriptografi (cryptography): Anlaşılır bir mesajı anlaşılmaz şekle dönüştürme ve mesajı orijinal haline dönüştürme prensipleri ve yöntemlerini içeren sanat veya bilimdir.

Açık metin (plaintext-P): Anlaşılır orijinal metin.

Şifreli metin (ciphertext-C): Dönüştürülen metin.

Şifreleyici (cipher): Anlaşılır bir metni, yerlerini değiştirme ve/veya yerine koyma yöntemlerini kullanarak anlaşılmaz şekle dönüştürmek için kullanılan bir algoritma.

Anahtar (key-K): Sadece gönderici ve alıcının bildiği şifreleyici tarafından kullanılan kritik bilgiler.

Şifreleme (encipher (encode)-E): Açık metni bir şifreleyici ve bir anahtar kullanarak şifreli metne dönüştürme süreci.

Şifre çözme (decipher (decode)-D): Şifreli metni bir şifreleyici ve bir anahtar kullanarak açık metne dönüştürme süreci.

Kriptoanaliz (cryptanalysis): Bilgi ve anahtar olmaksızın anlaşılmaz mesajı anlaşılır mesaj olarak geri dönüştürme prensipleri ve yöntemleridir. Aynı zamanda kod kırma (codebreaking) olarak da adlandırılır.

Kriptoloji (cryptology): Kriptografi ve kriptoanalizin her ikisi.

$\boldsymbol{E_K}$ dönüşümler ailesinden seçilen birebir ve örten bir fonksiyon olmak üzere şifreleme işlemi, anahtar ailesinin bir elemanı ile m mesajından $\boldsymbol{E_K(m) = c}$ olacak şekilde bir c şifreli mesajını elde etme işlemi iken, E'nin tersi olan D fonksiyonu ile $\boldsymbol{D_K(c) = m}$ olacak şekilde c şifreli metninden m mesajına ulaşmaya deşifreleme denir.

3. MATERYAL ve YÖNTEM

3.1. Kriptolojik Sistemler

Kriptoloji şifrelemede deşifrelemede kullanılan anahtarların özelliklerine göre açık anahtar (asimetrik kriptoloji) veya gizli anahtar kriptoloji (simetrik kriptoloji) olarak ikiye ayrılır.

3.1.1 Simetrik (Gizli anahtarlı) Kripto Sistemler

Simetrik anahtarlı kripto sistemler şifreleme anahtarından (e), deşifreleme anahtarı (d) ve deşifreleme anahtarından şifreleme anahtarı kolaylıkla elde edilebilmektedir. Çoğunlukla şifreleme ve deşifreleme anahtarı aynıdır. Haberleşecek iki grup ortak bir anahtar belirler. Gönderici girdi olarak bir m mesajını ve e anahtarını kullanarak c şifreli metni elde eder, şifreli metni alan alıcı d anahtarı yardımı ile m mesajını elde eder burada e den d ve d den e kolaylıkla elde edilebilir.(çoğunlukla d=e) Simetrik anahtar şifrelemede sistemin güvenliği anahtara bağlıdır. Simetrik anahtar şifrelemenin en büyük dezavantajı anahtar paylaşımıdır. Simetrik anahtar şifreleme bilginin gizliliğine hizmet eder ancak teknolojinin gelişmesiyle bilgi gizliliğinin yanı sıra sayısal imza ve kimlik doğrulamada büyük önem kazanmıştır. Bilinen en eski simetrik anahtar şifreleme Ceasar şifresidir.

Simetrik anahtar kripto sistemler akış şifreleri ve blok şifreler olarak ikiye ayrılır.

Blok Şifreleme: Şifreleme ve deşifreleme işlemi metnin sabit uzunluklu bloklara bölünerek blok blok işleme tutulmasıyla yapılır. En iyi bilinen blok şifre olan DES(Data Encryption System) blok boyu 64 bit olarak belirlenmiştir. Blok şifre sistemleri yerine koyma(substitution) ve yer değiştirme (transposition) şifreleri ve bu ikisinin birlikte kullanıldığı çarpım şifreleri olarak üç kısımda incelenebilir

Yerine Koymalı (Substitution) Kripto Sistem

Yerine koymalı kripto sistemler metindeki karakterin (ya da bir grup karakterin) diğer bir grup karakterle yer değiştirdiği blok şifrelerdir.

i . Basit Yerine Koymalı Şifreleme

Tanım 3.1: $\mathcal{A}$ bir alfabe , $\mathcal{M}$; $\mathcal{A}$ üzerindeki tüm t şeritlerinin kümesi olsun, $\mathcal{K}$ ise $\mathcal{A}$ üzerindeki tüm permütasyonların kümesi; her $\pi \in \mathcal{K}$ için, E şifreleme dönüşümü olmak üzere basit yerine koyma şifre;

$E_\pi(m) = \big(\pi(m_1)\pi(m_2) \dots \pi(m_t)\big) = (c_1 c_2 \dots c_t)$ olarak tanımlanır. Burada

$m \in (m_1, m_2, \dots, m_t)$ dır. Diğer bir deyişle t – şeritlerdeki her bir sembol, sabit bir π permüstasyonu ile $\mathcal{A}$ daki başka sembollerin yerini alır. Ceasar şifresi basit yerine koyma şifresine örnek olarak verilebilir.

Ceasar Şifresi:

Julius Ceasar tarafından kullanılmış, alfabedeki her harfi kendisinden üç sonraki harfe dönüştüren bir şifreleme sistemidir. Şifre çözerken de bu işlemin tersi uygulanır.

Ceasar Şifresi Türk alfabesine uygularsak mod 29 göre çalışmamız gerekir. Şifrelemek istediğimiz metni $C \equiv P + 3(mod29), 0 \leq P \leq 28$ bağıntısına göre açık metni (plaintext), şifreli metne (ciphertext)'e dönüştürür. Deşifreleme işlemi için ise $P \equiv C - 3(mod29), 0 \leq P \leq 28$ kullanılarak şifreli metinden açık metin elde edilir.

Örnek 3.1: "MATEMATİK BÖLÜMÜ'' mesajını Ceasar şifresini kullanarak şifreleyelim. Alfabedeki harfler 0 ile 28 arasında kendisine karşılık gelen sayısal denkliklere dönüştürülür.

A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
M	N	O	O	P	R	S	Ş	T	U	Ü	V	Y	Z	
15	16	17	18	19	20	21	22	23	24	25	26	27	28	

Mesajın kolay anlaşılmasını önlemek için 3'erli bloklara ayıralım ve mesajımızı sayısal olarak ifade edelim;

MAT EMA TİK BÖL ÜMÜ, her harfin sayısal karşılığını yazarsak

15 0 23 5 15 0 23 11 13 1 18 14 25 15 25 olur. $C \equiv P + 3(mod29)$ bağıntısını kullanılarak

18 3 26 8 18 3 26 14 16 4 21 17 28 18 28 oluşturulur, sayılar harflere dönüştürülürse şifreli metin

ÖÇV ĞÖÇ VLÇ DSO ZÖN olarak elde edilir.

$P \equiv C - 3(mod29)$ kullanılarak elde edilen sayısal değerlerin harf olarak karşılıkları yazılır ve bloklar birleştirilerek açık metine ulaşılır.

ii. Çoklu Alfabetik Yerine Koymalı Şifreleme

Tanım 3.2: Bir çoklu alfabetik şifre $\mathcal{A}$ alfabesi üzerindeki t uzunluklu blokların aşağıdaki şartları sağladığı blok şifredir:

1) $\mathcal{K}$ Anahtar uzayı, p_i $\mathcal{A}$ kümesi üzerinde tanımlı permütasyonlar olmak üzere t-nin $(p_1, p_2, \dots, p_t)$ bütün sıralı permütasyonlarından oluşur.

2) $m = (m_1 m_2 \dots m_t)$ mesajının şifreleme işlemi $e = (p_1, p_2, p_3, \dots, p_t)$ anahtarı altında şifrelenmesi $E_e(m) = (p_1(m_1)p_2(m_2) \dots p_t(m_t))$ ile verilir.

Deşifreleme anahtarı $e = (p_1, p_2, \dots, p_t)$ anahtarına karşılık $d = (p_1^{-1}, p_2^{-1}, \dots, p_3^{-1})$ anahtarıdır.

Çoklu anahtarlı sistemlerde açık metindeki her harf ayrı bir alfabe ile şifrelenir. Vigenere şifresi çoklu alfabetik şifreye örnektir.

Örnek 3.2 (Vigenere Şifresi) : $\mathcal{A}$=(A, B, …V,Y,Z) olsun ve $t = 4$ olsun $e = (p_1, p_2, p_3, p_4)$ olmak üzere p_1 her harfi kendisinin 3 harf sağındaki harfe, p_2 her harfi kendisinin 5 sağındaki harfe, p_3 her harfi kendisinin 4 harf sağına, p_4 her harfi kendisinin 7 harf sağına götürsün.

m= CEBİR VE SAYILAR TEORİSİ mesajını şifreleyelim öncelikle mesajı dörderli bloklara ayıralım.

CEBİ RVES AYIL ARTE ORİS İ, her bir bloğa p_1, p_2, p_3, p_4 uygularsak şifreli metin

c= EIEY TCHZ ÇÇLS ÇÜYJ RÜMZ L olarak elde edilir.

Yer Değiştirme (Transposition) Şifreler:

Tanım 3.3: t blok uzunluklu simetrik anahtar blok şifreleme sistemi düşünelim $\mathcal{K}, \{1,2,3, \dots t\}$ kümesindeki tüm permütasyonların kümesi olsun. Her $e \epsilon \mathcal{K}$ için şifreleme fonksiyonu

$E_e(m) = (m_{e(1)}m_{e(2)} \dots m_{e(t)})$ ile tanımlanır. Burada $m \epsilon \mathcal{M}$ dır. Böyle dönüşümlerin kümesi basit yer değiştirme şifreleme olarak adlandırılır. Deşifreleme anahtarı e permütasyonun tersi olan d=e^{-1} dır.

Basit yer değiştirme şifreleme bir bloğun içindeki sembollerin sayını korur bu yüzden kolaylıkla kriptoanaliz edilir.

Örnek 3.3: **t**=5 ve e=(13524) olsun. m= BU SİSTEM KOLAY KIRILABİLİR MESAJINI şifrelemek için öncelikle mesajı 5 erli bloklara ayıralım. İstenilirse eksik kalan bloklar mesajın anlamını bozmayacak harflerle doldurulabilir. Eksik kalan son bloğa mesajın anlamı bozmayacak şekilde A eklendi.

BUSİS TEMKO LAYKI RILAB İLİRA mesaja e uygulanırsa;

$E_e(m) = SİSBU\ \ MKOTE\ \ YKILA\ LABRI\ \ İRAİL$ şifreli metni elde edilir. Deşifreleme içim ise d=(14253) kullanılır.

Daha yüksek güvenlik sağlamak için yer değiştirme ve yerine koymalı şifre sistemleri bir sistemde kullanılabilir. Böylece daha güvenilir bir sistem elde edilir. Bu sistemler çarpım şifreleri olarak adlandırılır. Çarpım şifreleri en güvenilir simetrik anahtar şifrelerdir. Bir yerine koyma ve yer değiştirme şifresinin bileşkesine devir denir.

3.1.1.a. DES (Data Encryption Standart)

DES 1976 yılında IBM tarafından tasarlanmış ve NIST(ABD Teknoloji Enstitüsü) tarafından 4 yılda bir güvenirliliği onaylanan bir algoritmadır. DES de blok uzunluğu 64 bit, anahtar uzunluğu ise 56 bittir. Geliştirildiği dönemde çok güvenli olmasına karşın bilgisayar teknolojisindeki ilerlemeler sebebiyle yetersiz kalmıştır. DES aşırı güvenlik gerektirmeyen uygulamalarda rahatlıkla kullanılabilir.

DES algoritması 16 döngüden oluşan Feistel yapısıdır. İlk döngüye girmeden önce başlangıç permütasyonu uygulanır.

64 bitlik bloklar 32 bitlik iki kısma ayrılır ve 16 döngü bu ayrılan parçalara uygulanır sonunda başlangıçtaki pemütasyonun tersi uygulanır. Deşifreleme işleminde de aynı algoritma kullanılır.

DES bünyesinde bulunan tüm yerine koyma işlemleri ve XOR işlemleri çok hızlı bir yapıya sahip olmalıdır. DES algoritmasının RSA laboratuvarlarında gerçekleştirilen araştırmalarda, DES'in RSA'ya oranla yazılım şeklindeki testlerde 100 kat, donanım şeklindeki testlerde 1000 kat daha hızlı olduğu görülmüştür **(**Frösen 1995**).**

Akış Şifreleri(Stream Ciphers):

Akış şifreleri simetrik anahtar şifrelemenin önemli bir sınıfıdır. Akış şifreleri blok uzunluğu birbirine eşit olan basit blok şifreler olarak düşünülebilir. Şifrelenen metnin her bir sembolü için deşifreleme dönüşümü değişebilir olması bu sistemleri daha avantajlı kılar.

Akan şifre sistemleri mesajın her bir karakterini (bitini) ayrı ayrı şifreler. Şifreleme işlemi mesaj uzunluğunda bir anahtar seçilerek yapılır. Anahtarın her biti mesajın her biti ile $mod2$ de toplanır. Bu işleme XOR işlemi denir ve $\oplus$ ile gösterilir.

$m = m_1 m_2 m_3 \dots m_t$ mesajını $k = k_1 k_2 k_3 \dots k_t$ anahtarı ile şifreleme işlemi

$c_i = m_i \oplus k_i$ şeklinde yapılır.

Şifreleme işleminde kullanılan iki tip anahtar dizisi vardır .

i)Tam Rastgele(true random) Dizi: Dizideki her bir bit birbirinden bağımsız olarak elde edilir.

ii) Pseudo Rastgele (Pseudo Random) Dizi: Dizinin her biti kendinden önce gelen bitlere bağlıdır aynı zamanda her bit kendinden sonra gelen bitleri etkiler.

3.1.2 Asimetrik Anahtarlı Kripto sistemler

Asimetrik (açık anahtar) kripto sistemler her kullanıcının biri gizli (private key),diğeri açık(public key) iki anahtar kullanıldığı şifreleme sistemidir. Gizli anahtar sadece kullanıcı tarafından bilinirken açık anahtar herkes tarafından bilinebilir.

Açık anahtarlı kripto sistemler ile bir veriyi güvenli şekilde göndermek için metni alıcının açık anahtarı ile şifreler, şifrenin çözümü sadece bu açık anahtara karşılık gelen gizli anahtar ile mümkündür.

Asimetrik anahtarlı kripto sistemler, simetrik sistemlerin en büyük dezavantajı olan anahtar paylaşımı problemini çözmüştür.

3.1.2.a. RSA Açık Anahtar Şifreleme

En çok bilinen açık anahtarlı kripto sistemlerden biri olan Ron Rivest, Adi Shamir ve Len Adelman tarafından, 1978 yılında “Dijital İmza Elde Etme Metodu ve Açık Anahtarlı Kripto Sistemler” adlı bir makale ile yayınlanmıştır. RSA gizliliğin yanı sıra sayısal imza sağlamak için kullanılabilir. Bu sistemin güvenirliği tam sayılarda çarpanlara ayırma probleminin çözümünün zorluğuna dayanır.

RSA sisteminde şifreleme yaparken alıcının açık anahtarı ile mesaj şifrelenir ve mesajın deşifrelenmesi sadece alıcını kendisinin bildiği özel anahtarı yapılır. Böylece anahtar

paylaşımı sorunu ortadan kalkar. Bu sistemde bir B kişisi A kişisine mesaj göndermek istesin öncelikle anahtar oluşturma algoritmasını verelim(Rivest *et al.*1978),

A şahsı anahtarını oluştururken;

1) Her biri birbirinden farklı ve yeterince büyük p ve q asallarını oluşturur.
2) $n = p.q$ ve $\varphi(n) = (p-1)(q-1)$' i hesaplar.
3) $\big(e, \varphi(n)\big) = 1$ olacak şekilde $1 < e < \varphi(n)$ tam sayısı seçer.
4) Genişletilmiş Euclid algoritmasını kullanarak $ed \equiv 1(mod\ \varphi(n))$ olacak şekilde bir tek $1 < d < \varphi(n)$ tam sayısını bulur.
5) A'nın açık anahtarı (n, e) ve gizli anahtarı d dir.

B şahsı A ya şifreli mesaj gönderirken şifreleme için;

1) A 'nın açık anahtarı (n, e) alır.
2) M mesajını $[0, n-1]$ aralığında ifade edilir.
3) $c \equiv m^e(modn)$ hesaplar ve c şifreli metni A ya gönderir.

Deşifreleme için A, kendi özel anahtarı ile $m \equiv c^d(modn)$ ile açık metni elde eder.

Örnek 3.4: $p = 7\ ve\ q = 13$ asallarını seçelim $n = 7.13 = 91\ \ \varphi(n) = 6.12 = 72$ ve $1 < e < \varphi(n)\ \ (e, \varphi(n)) = 1$ olacak şekilde $e = 5$ seçelim $5.29 \equiv 1(mod72)$ olacak şekilde $d = 29$ sayısı seçelim. Açık anahtarımız $(n, e) = (91,5)$ ve gizli anahtar $d = 29$ olur. Şifrelenecek mesajımız $m = 15$ olsun. Şifreli metin $c \equiv 15^5(mod91)$ hesaplanarak $c \equiv 71(mod91)$ bulunur. Deşifreleme için $m \equiv 71^{29}(mod91)$ hesaplanarak $m = 15$ olarak bulunur.

3.1.2.b. Ayrık (Discrete) Logaritma Problemi

Sayılar teorisinde hesaplanması kolay fakat tersinin hesaplanması zor olan problemler vardır. Örneğin RSA, farklı ve yeterince büyük p ve q asallarından n=p.q sayısını elde etmek kolay iken; n bilinirken p ve q elde etmenin zorluğuna dayanır. Bunun gibi diğer bir problem ise sonlu cisimlerde kuvvet alma problemidir.

Ayrık logaritma problemi p bir asal sayı α, $\mathbb{Z}_p^*$ de bir primitif kök iken $\beta \in \mathbb{Z}_p^*$ olmak üzere $\alpha^x = \beta(modp)$ olacak şekilde $0 \leq x \leq p-2$ tam sayısını bulma problemidir.

3.1.2.c. Diffie Hellman Anahtar Paylaşımı

Diffie-Hellman 1976 de yayınladıkları "New Directions In Cryptography" adlı makale ile anahtar paylaşımı problemine ilk pratik çözümü getirmişlerdir. Ayrık logaritma probleminin çözümünün zorluğuna dayanan bu sistem ile tarafların daha önce bir araya gelmesine gerek duyulmadan açık bir kanal üzerinden mesajlarını birbirlerine göndererek ortak anahtar oluşturmalarını sağlanır (Diffie and Hellman 1976).

p yeteri kadar büyük bir asal sayı ve g, $\mathbb{Z}_p^*$ de bir primitif kök olsun. p ve g herkes tarafından bilinsin A ve B kişileri anahtar oluştururken;

1) A, $0 \leq a \leq p-2$ şartını sağlayan rastgele bir a tam sayısı seçer ve $c \equiv g^a(modp)$ hesaplar ve B' ye gönderir.
2) B, $0 \leq b \leq p-2$ şartını sağlayan rastgele bir b tam sayısı seçer ve $d \equiv g^b(modp)$ hesaplar ve A'ya gönderir.
3) A ortak anahtar olarak; $k=d^a = (g^b)^a$ hesaplar, B de aynı şekilde $k=c^b = (g^a)^b$ hesaplar. A ile B ortak k anahtarında anlaşmış olurlar.

3.1.2.d. El Gamal Açık Anahtar Şifreleme

1985 de El Gamal; Diffie ve Hellman anahtar paylaşımını kullanarak yeni bir açık anahtar kripto sistem önerdi. Her iki sistemin de güvenliği sonlu cisimlerde ayrık logaritma probleminin çözümünün zorluğuna dayanıyordu.

El Gamal açık anahtar şifreleme algoritması için öncelikle anahtar oluşturma algoritmasını verelim;

A şahsı anahtar oluştururken;

p; yeterince büyük ve rastgele bir asal sayı olmak üzere $\mathbb{Z}_p^*$ çarpımsal gurubunun bir α pirimitif kökünü (üretecini) bulur ve,

1) $1 \leq \mathrm{a} \leq p-2$ olacak şekilde bir a tam sayısı seçer ve a^{a} (modp) değerini hesaplar.
2) A' nın açık anahtarı (p, a, a^{a}) ve A'nın gizli anahtarı a olur.

El Gamal Şifreleme;

B şahsı mesajı şifrelerken:

A nın açık anahtarı (p, a, a^{a}) alır ve,

1) Mesajı $\{0,1,2,\ldots,p-1\}$ aralığında bir m tam sayısı ifade eder.
2) $1 \leq k \leq p-2$ olacak şekilde rastgele bir k tam sayısı seçer.
3) $c_1 \equiv a^k (modp)$ ve $\mathrm{c}_2 \equiv \mathrm{m}(a^{\mathrm{a}})^{\mathrm{k}} (modp)$ yi hesaplar.
4) c=(c_1, c_2) şifreli metnini A' ya gönderir.

A mesajı deşifrelerken;

1) a gizli anahtarını kullanarak $(c_1)^{-a}(modp)$ yani $a^{-ak}(modp)$ değerini hesaplar. $(c_1)^{-a}.c_2(modp)$

hesaplayarak m değerini bulur. Burada ($(c_1)^{-a}.c_2(modp) \equiv a^{-ak}ma^{ak}(modp) \equiv m(modp)$) dır.

3.2. Eliptik Eğri Kripto Sistemler

Bu bölümde eliptik eğri kavramı genel olarak tanıtılacak ve kriptolojide kullanılan eliptik eğriler hakkında bilgi verildikten sonra eliptik eğriler üzerinde ayrık logaritma problemine dayalı eliptik eğri kripto sistemler ifade edilecektir.

3.2.1. Eliptik Eğriler

Herhangi bir F cismi üzerindeki eliptik eğriler 3. Dereceden homojen polinom olan Weistrass eşitliği yardımı ile;

$$y^2z + axyz + byz^2 = x^3 + cx^2z + dxz^2 + ez^3 \quad (3.1)$$

$$y^2 + axy + by = x^3 + cx^2 + dx + e \quad (3.2)$$

şeklinde tanımlanır. Burada katsayılar F cisminin elemanıdır. Eğer $Kar(F) = 2$ ise

3.2. denklem,

$$y^2 + ay = x^3 + bx + c \quad (3.3)$$

şeklinde olup; $Kar(F) = 3$ ise

$$y^2 = x^3 + ax^2 + bx + c \tag{3.4}$$

şekline dönüşür. Eğer $Kar(F) \neq 2$ veya 3 ise bu denklem

$$y^2 = x^3 + ax + b \tag{3.5}$$

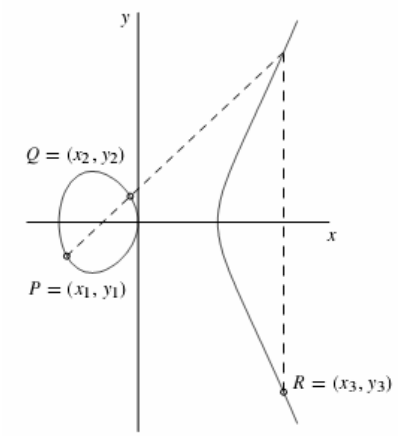
olur.

Biz bundan sonra reel sayılarda tanımlı eliptik eğrilerle ilgileneceğiz. Reel sayılarda tanımlı eliptik eğriler (3.5) eşitliğindeki gibi olup $a, b \in \mathbb{R}$'dir. Kriptolojide eliptik eğrilerin kullanılması için eliptik eğri üzerindeki noktaların bir grup oluşturması gerekir. Bir eliptik eğri çok katlı köke sahip değilse (singüler değil) yani $\Delta = 4a^3 + 27b^2 \neq 0$ ise eliptik eğri üzerindeki noktalar sonsuzdaki nokta ile birlikte toplamsal bir grup teşkil ederler.

Eliptik Eğri Üzerinde Toplama İşlemi (Geometrik Yaklaşım):

Eliptik eğri üzerindeki toplama işlemi geometrik olarak tanımlanmıştır. Eliptik eğri üzerindeki bir $P(x, y)$ noktasının negatifi P noktasının x eksenine göre simetriği olan $-P(x, -y)$ noktasıdır. E eliptik eğrisi üzerindeki P ve Q noktalarını toplamı aşağıdaki gibidir;

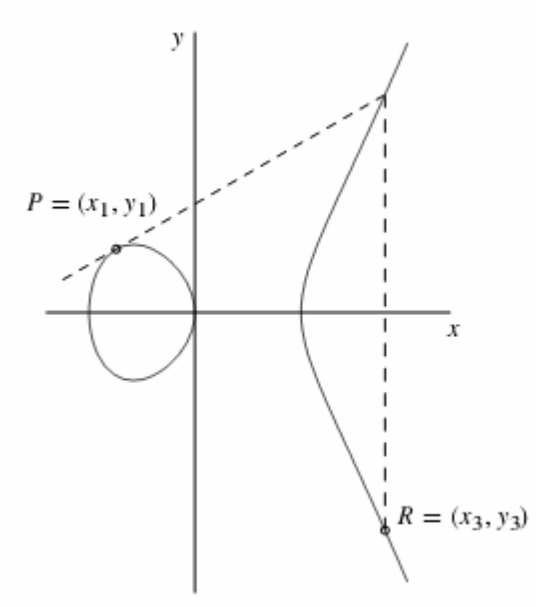
$1) P \neq Q \; ve \; Q \neq -P$ İken; P ve Q noktalarından geçen doğru eğriyi üçüncü bir noktada keser ve bu noktaya –R denirse P ile Q'nun toplamı bu noktanın x eksenine göre simetriği olan R noktasıdır.



Şekil 3.1. P+Q=R(Toplama işlemine geometrik yaklaşım)

1) P ve –P noktalarını birleştiren doğru eğriyi üçüncü bir noktada kesmez. $P + (-P) = 0$ olup sonsuzluk noktası denilen O noktasına eşittir. $P + O = P$ olup O noktasına toplamsal grubun birim elemanı denir.

2) P noktasını kendisi ile toplamaya P noktasının çiftlenmesi denir. $P(x, y)$ noktasını kendisi ile toplarken $y \neq 0$ için P noktasından çizilen teğet eğriyi ikinci bir noktada keser. Bu noktaya –R noktası dersek $P + P = 2P = R$ olur.



Şekil 3.2. P+P=2P (P noktasının çiftlenmesi)

$y = 0$ durumunda eğriye çizilen teğet dikey bir doğru olup eğriyi ikinci bir noktada kesmez. Bu durumda $P + P = 2P = O$ olur.

Eliptik Eğrilerde Toplama İşlemi (Cebirsel Yaklaşım):

Eliptik eğrilerde toplama işlemi cebirsel olarak aşağıdaki gibi ifade edilir.

1) $P \neq Q \; ve \; Q \neq -P$ iken $P + Q = R$ toplamı P ve Q noktalarından geçen doğrunun eğimi

$s = \frac{y_P - y_Q}{x_P - x_Q}$

olmak üzere;

$x_R = s^2 - x_P - x_Q$ ve $y_R = -y_P + s(x_P - x_R)$

olur.

2) P noktasının çiftlenmesi ($y_P \neq 0$) iken;

$y^2 = x^3 + ax + b$ ile verilen denklemin P noktasında çizilen teğetin eğimi

$s = \frac{3(x_P)^2 + a}{2y_P}$

olmak üzere;

$x_R = s^2 - 2x_p$

ve

$$y_R = -y_P + s(x_P - x_R)$$

olur.

Örnek 3.5:

$y^2 = x^3 - x + 4$ eliptik eğrisi $\Delta \neq 0$ olup reel sayılar üzerinde bir grup oluşturur. Bu eliptik eğri üzerindeki P(0,-2) ve $Q(-1,2)$ noktaları için;

$$s = \frac{y_p - y_Q}{x_p - x_Q}$$

$$s = \frac{2 - (-2)}{-1 - 0} = -4$$

$$x_R = s^2 - x_P - x_Q$$

$$x_R = 16 - 0 - (-1) = 17$$

$$y_R = -y_P + s(x_P - x_R)$$

$$y_R = 2 + (-4)(0 - 17) = 70 \Rightarrow$$

$$P + Q = R = (17,70)$$

dır.

Örnek 3.6:

$y^2 = x^3 - x + 4$ eliptik eğrisi üzerindeki $P(-1,2)$ noktası için P+P=2P hesaplayalım;

$$s = \frac{3(x_P)^2 + a}{2y_P}$$

olup;

$$s = \frac{3(-1)^2 - 1}{2.2} = \frac{1}{2}$$

$$x_R = s^2 - 2x_p$$

$$x_R = (\frac{1}{2})^2 - 2(-1) = \frac{9}{4}$$

ve

$$y_R = -y_P + s(x_P - x_R)$$

$$y_R = -2 + \frac{1}{2}\left(-1 - \frac{9}{4}\right) = \frac{-29}{8}$$

olup;

$$R = 2P = (\frac{9}{4}, -\frac{29}{8})$$

dır.

3.2.2. Sonlu Cisimler Üzerinde Tanımlı Eliptik Eğriler

Kriptolojik açıdan daha hızlı ve hassas hesaplamalar yapmak için sonlu cisimler üzerinde tanımlı eliptik eğriler daha kullanışlıdır. Sonlu cisimler üzerinde tanımlanan eliptik eğriler sayesinde gerçel sayılar üzerinde yuvarlamadan kaynaklanan hataların önüne geçilmiş olur.

p bir asal sayı olmak üzere F_p üzerinde tanımlı bir eliptik eğri $modp$ ye göre tanımlı tam sayılardan oluşur. F_p üzerinde tanımlı eliptik eğrilerdeki işlemler gerçel sayılar üzerinde tanımlı işlemlere benzer şekilde $modp$ de yapılır. F_p üzerinde tanımlı bir eliptik eğri

$$y^2 = x^3 + ax + b(modp) \qquad a, b \in F_p \tag{3.6}$$

şeklindedir. Eğer $\Delta = 4a^3 + 27b^2$ değeri $modp$ 'de sıfırdan farklı ise bu eğri üzerindeki noktalar sonsuzluk noktası ile birlikte bir grup oluşturur.

F_p de tanımlı eliptik eğri üzerinde sonlu sayıda nokta vardır. Bu noktalar aşağıdaki gibi teşkil edilir;

$0 \leq x \leq p-1$ aralığındaki x değeri için $x^3 + ax + b(modp)$ değeri hesaplanır. Sonuç $modp$ ye göre çift katlı köke sahipse(karesel kalan ise) P(x,y) E (F_p) nin bir noktasıdır. Bu durumda her x değeri için iki y değeri olur. Aksi takdirde P noktası E (F_p) nin bir elemanı değildir.

Örnek 3.7:

p=11 için $y^2 = x^3 + x - 1$ eliptik eğrisi için $\Delta = 4.1^3 + 27.1^2 = 31 \equiv 9(mod 11)$ Δ 0' dan farklı olduğundan F_{11} de bir grup oluşturur. (1,1) eliptik eğri denklemini sağlar.

$1^2(mod11) \equiv (1^3 + 1 - 1)(mod11)$ olup (1,1) eliptik eğri üzerindedir.

Sonlu Cisimlerde Tanımlı Eliptik Eğrilerde Aritmetik

F_p üzerinde tanımlı ve $\Delta = 4a^3 + 27b^2$değeri 0'dan farklı olma şartını sağlayan eliptik eğri üzerindeki noktalar bir toplamsal değişmeli grup oluşturur. F_p de tanımlı bir eliptik eğri üzerindeki bir $P(x, y)$ notasının negatifi $-P(x, (-y(modp))$ dır. İki noktanın toplanması ve nokta çiftlenmesi işlemleri $modp$ de yapılır. P ve Q ∈ E(F_p) olmak üzere nokta toplama ve nokta çiftleme işlemi aşağıdaki gibi yapılır;

1) $P \neq Q$; $P \neq -Q$ olmak üzere $P + Q = R$ için;

$$s \equiv \frac{y_p - y_Q}{x_p - x_Q}(modp)$$

olmak üzere;

$$x_R \equiv (s^2 - x_P - x_Q)(modp)$$

$$y_R \equiv -y_p + s(x_p - x_R)(modp)$$

2) P noktasının çiftlenmesi $y_p \neq 0$ ise ;

$$P + P = 2P = R$$

$y^2 \equiv (x^3 + ax + b)(modp)$ ile verilen denklemin P noktasında çizilen teğetin eğimi

$$s \equiv \frac{3(x_P)^2 + a}{2y_P}(modp)$$

olmak üzere;

$x_R \equiv (s^2 - 2x_P)(modp)$

$y_R \equiv -y_p + s(x_p - x_R)(modp)$

3) $P + (-P) = O$

olur.

Örnek 3.8:

F_{11} de $y^2 = x^3 + x - 1$ eliptik eğrisi üzerindeki $P(1,1)$ ve $Q(2,8)$ noktaları için $P + Q = R$ hesaplayalım;

$s \equiv \frac{y_p - y_Q}{x_p - x_Q}(modp)$

için;

$s \equiv \frac{8-1}{2-1} \equiv 7(mod11)$

$x_R \equiv (s^2 - x_P - x_Q)(modp)$

$x_R \equiv (7^2 - 1 - 2) \equiv 2(mod11)$

$y_R \equiv -y_p + s(x_p - x_R)(modp)$

$y_R \equiv -1 + 7(1 - 2) \equiv 3(mod11)$

olup;

$P + Q = R = (2,3)$

olur.

Eliptik eğrilerde skaler çarpma olarak adlandırılan $k.P$; P noktasının kendisi ile k defa toplanması demektir. Bu işlem P'nin k katının alınması olarak da ifade edilebilir. F_p üzerinde tanımlı bir eliptik eğri için eliptik eğri üzerinde olan herhangi bir P noktası sonsuzdaki nokta elde edilene kadar kendisi ile toplanması ile eliptik eğri üzerindeki noktalar elde edilebilir.

Örnek 3.9:

F_{11} de $y^2 = x^3 + x - 1$ eliptik eğrisi üzerindeki $P(1,1)$ başlangıç noktası olarak alınırsa sonsuzdaki nokta ile birlikte eliptik eğri üzerinde 5 nokta vardır. Bu noktalar;

P=(1,1) , 2P=(2,8) , 3P=(2,3) , 4P=(1,-1)

şeklindedir.

Sonlu cisimler üzerinde tanımlı eliptik eğriler üzerindeki toplam nokta sayısını belirlememizde yardımcı olacak Hasse teoremi aşağıda verilmiştir.

3.1. Teorem (Hasse Teoremi):

F_p sonlu cismi üzerinde tanımlı eliptik eğri üzerindeki toplam nokta sayısı n olmak üzere;

$$|n - (p - 1)| \leq 2\sqrt{p} \qquad (3.7)$$

olup n değeri Eş.(3.7) ile sınırlandırılır (Washigton 2003).

3.2.3. Eliptik Eğriler Üzerinde Ayrık Logaritma Problemi (ECDLP)

Eliptik eğrilerde ayrık logaritma problemi bir skaler çarpma işlemine dayanır. P eliptik eğri üzerinde bir nokta iken $kP = Q$ eşitliğinde P ve Q verilmişken k skalerinin bulunmasının zorluğuna dayanır. Bu işleme Q noktasının P tabanın göre ayrık logaritmasını bulma da denir. Eliptik eğriler üzerindeki ayrık logaritma problemi; klasik ayrık logaritma probleminden daha zordur. Yine de sonlu abelyen gruplarda bu problemin kolay çözülebilmesini önlemek için (r grubun mertebesini bölen en büyük asal iken yaklaşık $\sqrt{r}$ işlem gerekir); E ve p dikkatli seçilmelidir. Böylece $N = \left|F_p(E)\right|$ büyük bir asala bölünebilir.

Örnek 3.10 :

$p = 11$ için; F_{11} de $y^2 = x^3 + x + 6$ eliptik eğrisi üzerinde $P(10,2)$ ve $Q(5,9)$ noktaları için; Q nun P tabanında ayrık logaritmasını bulalım. Bunun için $k.P = Q$ eşitliğini sağlayan k değeri bulunmalıdır. P, Q elde edilene kadar kendisi ile toplayalım.

$P + P = 2P$

$s \equiv \frac{3x^2+1}{2y}(mod11)$ P noktasından geçen teğetin eğimi olmak üzere;

$s \equiv \frac{3.10^2+1}{2.2}(mod11)$

$= (3 + 1)(4)^{-1}(mod11)$

$= 4.3(mod11) \equiv 1$

$x_{2P} \equiv (1 - 2.10)(mod11) \equiv -19(mod11) \equiv 3$

$y_{2P} \equiv \big(-2 + 1.(10 - 3)\big)(mod11) \equiv 7$ olup;

$2P = (3,5)$ olur. $P + 2P = 3P$ hesaplayalım;

$s \equiv (5-2)(3-10)^{-1}(mod11)$

$s \equiv 3.(-7)^{-1} mod11 \equiv 3.4^{-1}(mod11) \equiv 3.3(mod11) \equiv 9$

$x_{3P} \equiv (9^2 - 10 - 3)(mod11) \equiv -9(mod11) \equiv 2$

$y_{3P} \equiv \big(-2 + 9.(10-2)\big)(mod11) \equiv 4$

$3P = (2,4)$

olur.

$P + 3P = 4P$

hesaplayalım;

$s \equiv (4-2)(2-10)^{-1}(mod11) \equiv 2.(-8)^{-1}(mod11)$

$s \equiv 2.3^{-1}(mod11) \equiv 2.4(mod11) \equiv 8$

$x_{4P} \equiv (8^2 - 10 - 2)(mod11) \equiv 8(mod11) \equiv 8$

$y_{3P} \equiv \big(-2 + 8.(10-8)\big)(mod11) \equiv 3$

olup;

$4P = (8,3), 5P = (7,2), 6P = 0$

olup; Q'nun P tabanında ayrık logaritması 6 dır.

Kriptolojik uygulamalarda kolay deşifrelemeyi önlemek için hesaplanması daha çok zaman alan noktalar kullanılmalıdır.

3.2.4. Eliptik Eğrilerde Diffie -Hellman Anahtar Paylaşımı

Eliptik eğri kriptoloji açık anahtarlı bir kripto sistemdir. Güvenirliliği eliptik eğri ayrık logaritma probleminin çözümünün zorluğuna dayanır. Eliptik eğrinin tanımlandığı asal cisim F, P başlangıç noktası ve skaler çarpım sonucu elde edilen Q noktası ve E eliptik açık anahtar; k skaleri gizli anahtardır. Burada $n.P = 0$ şartını sağlayan en büyük n olacak şekilde başlangıç noktası seçmeye dikkat edilmelidir. Anahtar değişimi yapacak A ve B kişileri aşağıdaki işlem basamağını izler (Koblitz 1987),

1) A, $k_A < n$ olacak şekilde bir k_A tam sayısı seçer ve $k_A.P$'yi hesaplar. Burada k_A, A'nın gizli anahtarı, $k_A.P = P_A$ da A' nın açık anahtarıdır.
2) B, $k_B < n$ olacak şekilde bir k_B tam sayısı seçer ; $k_B.P = P_B$ hesaplar. B nin açık anahtarı $k_B.P$ ve gizli anahtarı k_B dir.
3) A; B'nin açık anahtarını alarak $k_A.P_B$ yi; B ise aynı şekilde $k_B.P_A$ hesaplar.

$k_A.P_B = k_A(k_B.P) = k_B(k_A.P) = k_B.P_A$ olur.

3.2.5. Eliptik eğrilerde şifreleme ve deşifreleme

Eliptik eğrilerde şifrelenecek bir mesajın eliptik eğri üzerinde bir nokta olarak ifade edilmesi gerekir. Ancak; her nokta eliptik eğri üzerinde olmayabilir.

Bir A kişisi M mesajını B kişisine göndermek istesin. P; E eliptik eğrisi üzerinde bir başlangıç noktası olsun. Şifreleme işlemi aşağıdaki gibi yapılır (Koblitz 1987),

A rastgele bir n_A tam sayısı seçer ve P_M mesajından şifreli $C_m = (n_A.P, P_m + n_A P_B)$ şeklinde elde eder ve B ye gönderir.

Şifreli metni alan B şifreli metinden açık metini aşağıdaki gibi elde eder;

$P_m = P_m + n_A P_B - P_B(n_A . P)$ elde eder.

Örnek 3.11:

p=17 için, $y^2 = x^3 - x + 4$ eliptik eğrisi üzerinde $P = (1,2)$ noktasını başlangıç nokta olarak alalım. B nin açık anahtarı $P_B = 4P = (2,1)$ olsun. A eliptik eğri üzerindeki $P_M = (11,10)$ mesajını şifrelemek istesin; A rastgele bir $n_A = 5$ seçsin;

A şifreli metni;

$C_M = (5(1,2), (11,10) + 5(12,13))$

$C_M = \big((15,13), (11,10) + (13,4)\big)$

$C_M = ((15,13), (11,7))$ olarak elde eder ve B ye gönderir. B ise şifreli metinden açık metini

$P_m = P_m + n_A P_B - n_B(n_A . P)$

$= (11,7) - 4\big(5(1,2)\big)$

$= (11,7) - 4(15,13)$

$= (11,10)$

elde eder.

3.3. Sayısal İmza

Sayısal imza elektronik ortamda bir mesajın imzalanması işlemi olup geleneksel imzanın elektronik ortamdaki karşılığı olarak düşünülebilir. Sayısal imza elektronik ortamdaki bir mesaja bazı algoritmalar ile eklenir. Sayısal imza imzalanan metne göre değişiklik gösterir. Sayısal imza üç temel özelliğe sahiptir. Bunlar;

i. Veri Bütünlüğü: Verinin izinsiz değiştirilmesinin önlenmesi.
ii. Kimlik Doğrulama: Mesajı alan ve gönderen kişilerin kimliklerinin doğrulanması.
iii. İnkar Edilemezlik: Bireylerin elektronik ortamda gerçekleştikleri işlemleri inkar etmelerini önlenmesi.

Sayısal imza; imzanın oluşturulması ve imzanın doğrulanması olarak iki kısımdan oluşur. Bir A kişisi bir m mesajının sayısal imzasını elde etmek için bölüm 3.5 de verilen hash fonksiyonları yardımı ile mesajın bir özeti ya da mesaj belirteci denilen sayıyı kendi gizli anahtarı ile şifreler ve mesaja ekleyerek mesajı gönderir(gerekiyorsa mesajı da şifreler). Mesajı alan B kişisi (eğer mesaj şifrelenmişse mesajı deşifreler) mesajın içindeki sayısal imzayı A'nın açık anahtarı ile deşifreleyerek özet mesajı elde eder ve orijinal mesaja A'nın uyguladığı özet fonksiyonu uygulayarak bir özet elde eder. İmzanın içindeki özet ile B'nin bulduğu özet aynı ise mesaj göndericisinin doğruluğu ve mesajın gönderilme esnasında değişmediği anlamına gelir.

İki tür imza sistemi vardır. Bunlar;

1) Sonuna Eklemeli Sayısal İmza Sistemi:

Bu tür sayısal imza sistemlerinde imzayı doğrulamak için orijinal mesaj doğrulama algoritmasının girişlerinden biri olmalıdır. Bu sistemler daha çok kriptografik hash fonksiyonlarına dayalıdır. Bu sistemlere örnek olarak DSA, El-Gamal imza sistemleri verilebilir.

2) Mesajın Geri Alınabildiği Sayısal İmza Algoritmaları:

Mesajın geri alınabildiği sayısal imza algoritmalarında orijinal mesajın doğrulama algoritmasında bir giriş olarak verilmesine gerek yoktur. Mesaj imzanın kendisinden elde edilebilir. Bu sistemlere örnek olarak RSA, Rabin imza sistemleri verilebilir (Menezes *et al.* 1978).

3.4. Sayısal İmza Algoritmaları

$\mathcal{M}$ sonlu sayıda mesajların kümesi, $\mathcal{S}$ sonlu sayıda olası tüm imzaların kümesi, $\mathcal{K}$ anahtar uzayı sonlu sayıda anahtarların kümesi olmak üzere sayısal imza imzalama dönüşümü S_K ve doğrulama dönüşümü V_K olsun($S_K: \mathcal{M} \to \mathcal{S}$ ve $V_K: \mathcal{M} \times \mathcal{S} \to \{doğru, yanlış\}$) . S_K imzalama dönüşümü imza üretmek için kullanılır ve gizli tutulurken; V_K doğrulama dönüşümü üretilen imzaları doğrulamak için kullanılır ve doğru veya yanlış gibi çıktılar verir ve açıktır.

Sayısal imza geleneksel imzadan farklı olarak tek kullanımlık olabilir. Eğer bir A kişisi bir B kişisinin imza sadece bir defaya mahsus kullanmasını istiyorsa imzaya tarih gibi eklentiler yaparak daha fazla kullanımını önleyebilir.

3.4.1. RSA Sayısal İmza Algoritması

A, B'ye göndereceği bir m mesajını RSA algoritması ile imzalamak istesin. Bu takdirde;

M mesaj uzayı,
M_s imzalama uzayı,
S, imza uzayı,
R, M' den M_s'ye 1-1 fonksiyon,
M_R=Im(R) olup R nin görüntü kümesidir.
RSA için M ve M_s $\mathbb{Z}_n$ dir ve bir R: M→ $\mathbb{Z}_n$

seçilir ve R herkese açıktır.

A anahtar oluştururken;

1) Yeterince büyük birbirinden farklı p ve q asalları seçer.

2) n=p.q ve $\varphi(n) = (p-1).(q-1)$ değerlerini hesaplar.
3) $1 < e < \varphi(n)$ ve $(e, \varphi(n)) = 1$ olacak şekilde bir e tam sayısı seçer.
4) Öklid algoritması kullanarak $1 < d < \varphi(n)$ ve $e.d \equiv 1(mod\varphi(n))$ olacak şekilde d sayısını hesaplar.
5) A'nın açık anahtarı (n, e), gizli anahtarı ise d olur.

A imzalama işleminde;

1) $m' = R(m)$ hesaplar, m' $[1, n-1]$ aralığında bir tam sayıdır.
2) $s \equiv (m')^d (modn)$ hesaplar.
3) A'nın m mesajının imzası s olur.

B imzayı doğrularken;

1) A' nın açık anahtarı (n,e) alır ve $m' \equiv s^e (modn)$ hesaplar.
2) $m' \in M_R$ olduğunu doğrular eğer değilse imzayı reddeder.
3) $m = R^{-1}(m')$ elde eder.

Örnek 3.12:

Anahtar oluşumu;

A, $p = 7927$ ve $q = 6997$ asallarını seçsin, $n = p.q = 55465219$ ve $\varphi(n) = 7926 \times 6996 = 5545029$ olur. A $e = 5$ olarak seçsin ve $e.d \equiv 1(mod5545029)$ olacak şekilde $d = 44360237$ elde eder. A'nın gizli anahtarı $d = 44360237$ olur.

İmzalama;

R: $M \to \mathbb{Z}_n$ kolaylık açısından R olarak birim fonksiyonu $R(x) = x$ seçelim. $m = 31229978$ mesajını imzalamak için;

$m' = R(m), m' = 31229978$ ve

$s \equiv (m')^d (mod n) \equiv 31229978^{44360237} (mod 55465219) \equiv 30729435$

Doğrulama;

$m' \equiv s^e (mod n) \equiv 30729435^5 (mod 5545029) \equiv 31229978$

ve son olarak;

$R^{-1}(m') = R^{-1}(31229978) = 31229978$

RSA Sayısal İmza Sistemine Olabilecek Ataklar:

Eğer bir saldırgan n' yi çarpanlarına ayırabilirse, $\varphi(n)$ elde edebilir. Genişletilmiş Öklid algoritması ile $\varphi(n)$'den açık anahtar e'yi kullanarak $e.d = 1(mod n)$ olacak şekilde d elde eder. Bu şekilde gizli anahtarı ele geçiren saldırgan sistemin tümünü kırabilir. Bu ataktan kaçınmak için A p ve q seçerken çarpanlara ayrılması zor olacak şekilde seçmelidir.

RSA imza sistemi çarpımsal özelliğe sahiptir. Yani eğer $s_1 \equiv {m_1}^d (mod n)$ ve $s_2 \equiv {m_2}^d (mod n)$ sırasıyla m_1 ve m_2 gibi iki mesajın imzası iken; $s \equiv s_1 s_2 (mod n)$

$s \equiv (m_1 m_2)^d (mod n)$ özelliğine sahiptir.($m \equiv m_1 . m_2 (mod n)$; $m \in M_R$). Böylece s bir imza değeri olabilir. Bu yüzden R fonksiyonu seçilirken çarpımsal olmamasına dikkat edilmelidir($a, b \in M, R(a.b) \neq R(a).R(b)$).

3.4.2. DSA (Digital Signature Algorithm) Sayısal İmza Algoritması

DSA 1991 yılında NIST tarafından DSS (Digital Signature System) de kullanılmak üzere önerilmiştir. DSA El-Gamal gibi ayrık logaritma problemine dayanır.

Öncelikle DSA algoritmasında kullanılacak alan parametrelerini ifade edelim.

Her iki taraf aşağıdaki gibi kendi alan parametrelerini oluşturur.

1) $q|p-1$ olacak şekilde yeterince büyük p ve q asalları seçer.
2) Bir $h \in \mathbb{Z}_p$ için $g \equiv h^{\frac{p-1}{q}}$ (modp) hesaplanır.($g \neq 1$)
3) Böylece g, p, q alan parametreleri olur.

DSA anahtar çifti üretilirken g, p, q parametrelerine sahip A kişisi;

1) $1 \leq x \leq q-1$ olacak şekilde rastgele bir x tam sayısı seçilir.
2) $y \equiv g^x(modp)$ hesaplanır.
3) A' nın açık anahtarı y, gizli anahtarı x olur.

DSA imza üretilmesi;

1) $1 \leq k \leq q-1$ olacak şekilde rastgele bir k tam sayısı seçilir.
2) $x \equiv g^k(modp)$ ve $r \equiv x(modq)$ hesaplanır.
3) h, m mesajının bir özet fonksiyon yardımı ile elde edilmiş özeti (NIST, DSA da özet fonksiyon olarak SHA-1 kullanılmasını önermiştir) ve k^{-1} k nın modq ya göre tersi olmak üzere;
$s \equiv k^{-1}.(h+x.r)(modq)$ hesaplanır. Eğer s=0 ise 1. Adıma geri dönülür.

4) A'nın imzası (r,s) olur.

DSA imza doğrulama algoritması;

B, A'nın gönderdiği imzayı doğrulamak için g, p, q alan parametreleri ve A'nın açık anahtarı y ile;

1) r ve s nin $[1, q-1]$ arasında tam sayılar olduğu doğrular.
2) A nın kullandığı özet fonksiyon ile mesajın özetini h hesaplar.
3) $w \equiv s^{-1}(modq)$ hesaplar ve $u_1 \equiv h.w(modq)$ ile $u_2 \equiv r.w(modq)$ hesaplar.
4) $x \equiv g^{u_1} y^{u_2}(modp)$ ve $v \equiv x(modq)$ değerlerini hesaplar.
5) $v = r$ koşulu sağlanıyorsa imza doğrudur.

DSA'nın güvenliği ayrık logaritma probleminin zorluğuna dayanır. DSA sadece imzalama için kullanılır, bir şifreleme algoritması değildir. İmzalama hızları aynı olsa bile doğrulamada RSA, DSA'dan 10 ile 40 kat daha hızlıdır (Kaliski 1991).

3.4.3. Eliptik eğri sayısal imza (ECDSA) algoritması

Eliptik eğri sayısal imza algoritmasına geçmeden önce eliptik eğri alan parametrelerini verelim. q bir asal sayı olmak üzere F_q üzerinde tanımlı $y^2 = x^3 + ax + b$ eliptik eğrisi, P eliptik eğri üzerindeki herhangi bir nokta, n P' nin mertebesi ($n.P = 0$) ve h özet fonksiyon olmak üzere alan parametreleri;

$$D = (q, F_q(E), a, b, P, n, h)$$

dir (Khalique et all 2010).

ECDSA Anahtar Oluşturma;

$D = (q, F_q(E), a, b, P, n, h)$ alan parametreleri ile birlikte her A kişisi aşağıdaki gibi anahtar oluşturur,

1) $[1, n-1]$ aralığından rastgele bir d tam sayısı seçer.
2) $Q = dP$ hesaplar.
3) A' nın açık anahtarı Q, gizli anahtarı d olur.

ECDSA İmza Algoritması;

A m mesajını imzalamak için yukarda verilen alan parametreleri ile aşağıdaki gibi imza oluşturur,

1) $1 \leq k \leq n-1$ olacak şekilde rastgele bir k tam sayısı seçer.
2) $kP = (x_1, y_1)$ ve $r \equiv x_1 (mod n)$ (x_1 0 ile $q-1$ arasında bir tam sayı olduğu kabul edilir.) hesaplar. Eğer r sıfır ise 1. Adıma geri dönülür.
3) $k^{-1} mod n$ hesaplar.
4) $s \equiv k^{-1}(h(m) + dr)(mod n)$ hesaplar (Eğer s=0 ise 1. Adıma geri dönülür).
5) m mesajının imzası (r, s) olur.

ECDSA İmza Doğrulama Algoritması;

B A' nın gönderdiği imzayı doğrulamak için $D = (q, F_q(E), a, b, P, n, h)$ bilgileri ve açık anahtar Q ile birlikte aşağıdakileri yapar,

1) r ve s'nin $[1, n-1]$ aralığında olduğunu kontrol eder.
2) $w \equiv s^{-1}(mod n)$ ve $h(m)$ hesaplar.
3) $u_1 \equiv h(m)w(mod n),\ u_2 \equiv rw(mod n)$ hesaplar.
4) $u_1 P + u_2 Q = (x_0, y_0)$ ve $v = x_0 (mod n)$ hesaplar.
5) $v = r$ ise imza doğru olarak kabul edilir.

Örnek 3.13:

F_{11} de tanımlı $y^2 = x^3 + x + 6$ eliptik eğrisi üzerinde P(2,7) noktasını alalım. P noktasının mertebesi $13P = 0$ olup $n = 13$, $q = 11$ ve h özet fonksiyonu olmak üzere m mesajının özeti $h(m) = 5$ olsun. A kişisi bir m mesajını imzalamak istesin;

Anahtar oluşturma;

1) A [1,12] arasında $d = 7$ seçsin.
2) $Q = 7P = (7,2)$ olur. A'nın gizli anahtarı d=7ve açık anahtarı Q olur.

İmzalama;

1) $1 \leq k \leq 12$ olacak şekilde $k = 9$ seçsin.
2) $k^{-1} mod(13) \equiv 3$ ve $r \equiv x_1 (mod n) \equiv 7 (mod 13)$
3) $s \equiv k^{-1}(h(m) + dr)(mod n)$

$\equiv 3(5 + 7.7)(mod 13) = 6$ olup $s = 6$ olur.

4) m mesajının imzası (r, s) = (7, 6) olur.

Doğrulama;

1) İmzayı alan B (r, s) = (7,6) r ile s nin [1, 12] olduğunu kontrol eder.
2) $w \equiv s^{-1}(mod n) \equiv 6^{-1}(mod 13)$, $w = 11$ ve $h(m) = 5$ bulunur.
3) $u_1 \equiv h(m)w(mod n) \equiv 5.11(mod 13) \equiv 3$, $u_1 = 3$

$u_2 \equiv rw(mod n) \equiv 7.11(mod 13) \equiv 12$ hesaplar.

4) $u_1 P + u_2 Q = 3P + 12Q = (8,3) + (5,2) = (7,9)$ ve $v \equiv 7(mod 13)$ hesaplar.

5) $v = r$ olup imza doğrudur.

DSA ve ECDSA her ikisi de El-Gamal sistemine dayanır ve her ikisinde de aynı imzalama algoritması $s \equiv k^{-1}(h(m) + dr)(modn)$ kullanılır ve özet fonksiyon olarak SHA-1 kullanılması önerilir. ECDSA gizli anahtar d ve her imza için seçilen k değeri istatiksel olarak tektir ve tahmin edilemezken DSA daki sadece rastgeledir (Johnsan *et al.*2007).

Şimdi sayısal imzada kullanılan hash(özet) fonksiyonları tanıtalım.

3.5. Hash Fonksiyonları

Kriptografik hash fonksiyonları modern kriptolojide önemli bir yer tutar. Genel anlamda hash fonksiyonu geniş tanım kümelerini daha kısa görüntülere dönüştürür.

Hash fonksiyonları girdi olarak bir mesajı alır ve çıktı olarak hash kod, hash değeri, mesaj özeti ya da kısaca hash denilen değeri üretir. Tam olarak h fonksiyonu sonlu keyfi uzunluklu değerleri sabit uzunluklara dönüştürür.

Hash fonksiyonları sayısal imzada kullanılır. Bir mesajın hash değeri bulunur ve mesaj yerine hash değeri imzalanır. En çok bilinen hash fonksiyonları SHA, MD4, MD5 dir. Hash fonksiyonlarının farklı bir grubu olan mesaj doğrulama kodları (MACs) simetrik sistemlerde mesaj doğrulanmasına izin verir.

Tanım 3.1: (Hash Fonksiyonu):

Bir hash fonksiyonu aşağıdaki iki özelliği sağlayan h fonksiyonudur;

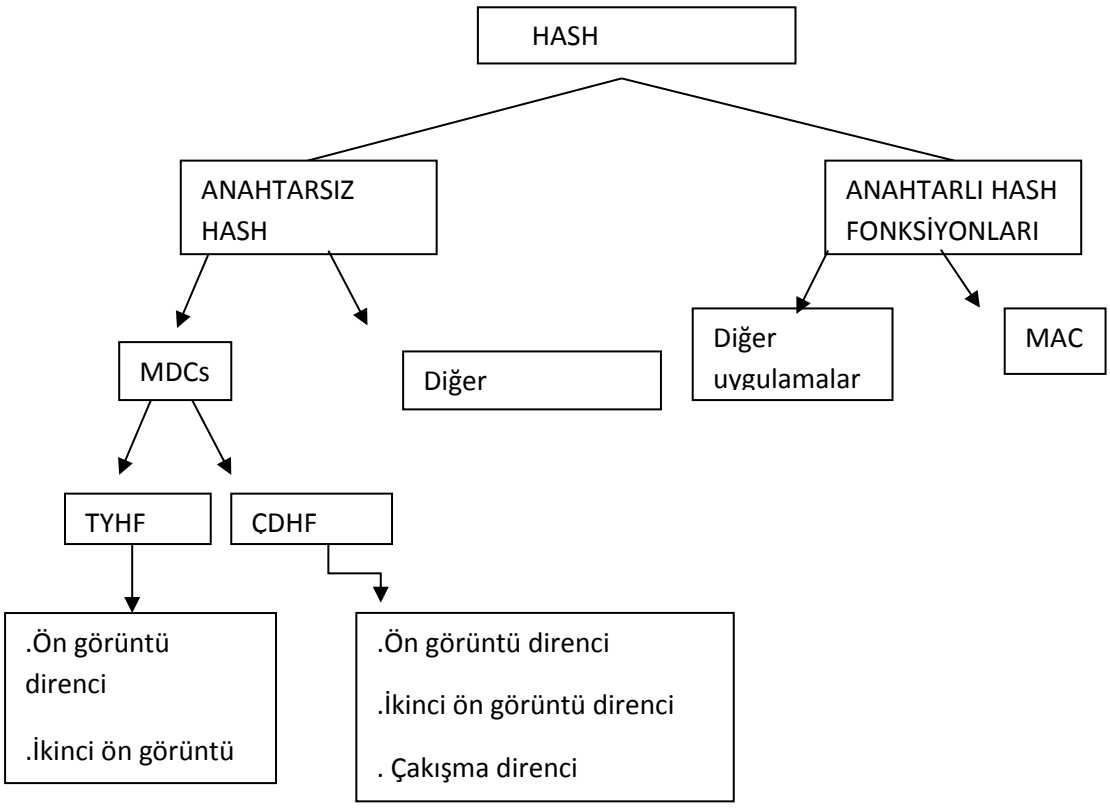
1) Sıkıştırma (Compression): Keyfi ve sonlu bit uzunluğundaki bir x girdisini sabit bit uzunluğundaki $(n - bit)$ çıktıya dönüştürme.

2) Hesaplama Kolaylığı: Bir x girdisi ve h fonksiyonu verildiğinde $h(x)$ hesaplamak kolaydır.

Hash fonksiyonu mesajın özetidir. Hash fonksiyonunda $h(x)$'i hesaplamak kolay iken $h(x)$ verilmişken x hesaplamak zor olmalıdır.

Hash fonksiyonları fonksiyonel olarak birçok sınıflandırmaya ayrılabilir ama biz bu bölümde iki kısım hash fonksiyonlarından bahsedeceğiz.

Hash fonksiyonları genel sınıflandırılması Şekil 3.3'deki gibidir.



Şekil 3.3. Hash fonksiyonlarının sınıflandırılması (Menezes *et al.* 1996)

1) Değişiklik Bulma Kodları(MDCs) (Modification Detection Codes)

Manipulation Detection (Hile Tespiti) Kodları veya mesaj bütünleme kodları olarak da bilinirler. MDCs'ın amacı bir temsilci görüntü ya da hash değeri sağlamaktadır. MDCs anahtarsız hash fonksiyonlarının bir sınıfıdır.

2) Mesaj Kanıtlama Kodları (MACs) (Mesage Authentication Codes)

MACs'ın amacı herhangi ilave bilgi kullanmadan mesajın doğrulanması ve mesaj bütünlüğünün sağlanmasıdır. MACs mesaj ve gizli anahtar gibi iki parametreye sahiptir ve anahtarlı hash fonksiyonlarının bir sınıfıdır.

MDCs ile MACs kodları arasındaki fark anahtardır. Kodlama algoritmaları herkese açıktır; ancak girdi olarak bir mesaj verildiğinde MDCs için herhangi biri hash değerini hesaplayabilirken; MACs ile sadece gizli anahtarı bilen bir kişi hash değerini hesaplayabilir.

3.5.1. Temel Özellikler ve Tanımlar

Hash fonksiyonları için önemli üç özelliği verelim. Anahtarsız hash fonksiyonu h, x_1 ve x_2 girdi ve $y_1$ve y_2 çıktılar olsun.

1) Ön Görüntü Direnci:

Olası tüm çıktılar için hash değeri bu olan bir x girdisi hesaplanabilir olmamalıdır. Yani herhangi bir y çıktısı verildiğinde $h(x) = y$ olacak şekilde x ön görüntüsü bulmak kolay olmamalıdır.

2) İkinci Ön Görüntü Direnci:

Aynı çıktı değerine sahip farklı iki girdi bulunması hesaplanabilir olmamalıdır. Yani $h(x_1) = h(x_2)$ iken $x_1 \neq x_2$ olacak şekilde ikinci ön görüntü bulunması kolay olmamalıdır.

3) Çakışma Direnci:

Aynı çıktı değeri için x_1 ve x_2 gibi farklı iki girdi bulmanın hesaplanması kolay olmamalıdır. Yani h(x_1) = h(x_2) olacak şekilde herhangi x_1, x_2iki girdisi bulmak kolay olmamalıdır.

Ön görüntü direnci yerine tek yol fonksiyonu, ikinci ön görüntü direnci yerine zayıf çakışma direnci, çakışma direnci yerine ise güçlü çakışma direnci ifadeleri de kullanılabilir.

Tanım 3.2 (Tek Yol Hash Fonksiyonu)(TYHF) :

Bir tek yol hash fonksiyonu Tanım 3.1 deki özelliklere ilave olarak ön görüntü direnci ve ikinci ön görüntü direncine sahip olan hash fonksiyonudur. Tek yol fonksiyona zayıf tek yol fonksiyon da denilebilir.

Tanım 3.3 (Çakışma Dirençli Hash Fonksiyonu)(ÇDHF):

Çakışma dirençli bir hash fonksiyonu Tanım 3.1'e ek olarak çakışma direnci ve ikinci ön görüntü direncine sahip olan hash fonksiyonudur. Çakışma dirençli hash fonksiyon yerine güçlü tek yol hash fonksiyonu da denilebilir.

Örnek 3.13:

$g(x) \equiv x^2(modn)$ fonksiyonu ön görüntü direncine sahip olmasına rağmen ikinci ön görüntü direncine sahip değildir.

$g(x) \equiv x^2(mod5)$ düşünelim x = 7 için $g(7) = 4$ oup ; $g(x) = 4$ olacak şekilde x = 2 değeri bulmak kolaydır. Bu ise ikinci ön görüntü direnci ile çelişir.

3.5.2. Özellikler Arasındaki İlişkiler

Teorem 3.2:

Hash fonksiyonlarında çakışma direnci ikinci ön görüntü direncini gerektirir (Menezes *et al.*1996).

İspat: h çakışma direncine sahip bir hash fonksiyonu olsun. Eğer h ikinci ön görüntü direncine sahip değilse bir x_1 girdisi için, $h(x_1) = h(x_2)$ olacak şekilde x_2 bulunabilir. Bu durumda aynı h çıktısına sahip farklı (x_1, x_2) değerleri bulunmuş olur. Bu ise çakışma direnci ile çelişir.

"Çakışma direnci ön görüntü direncini garanti etmez." Bunu bir örnek ile açıklayalım.

Örnek 3.14:

Reel sayılarda tanımlı $f(x) = x + 1$ fonksiyonu çakışma direnci özelliğine sahiptir ancak ön görüntü direnci yoktur.

Tekrarlı Hash Fonksiyonlarına Genel Bir Bakış

Anahtarsız hash fonksiyonlarının birçoğu girdi ve çıktı uzunluğu sabit olan bir f hash fonksiyonunun tekrarlı olarak uygulanması ile elde edilir. Sonlu ve keyfi uzunluklu bir x girdisi sabit r uzunluklu bloklara(x_i)bölünür. Genellikle x' in uzunluğunu r'nin katı yapmak için belli bir kurala bağlı olarak x'e bit ekleme (padding) yapılır. Her r uzunluklu x_i girdisi f fonksiyonuna sokulur. f 'nin ilk çıktısı x_{i+1} tekrar f fonksiyonuna sokulur ve son girdi bloğuna kadar bu işlem devam eder.

$x = x_1x_2x_3 \dots x_t$ girdisi ile birlikte tekrarlı hash fonksiyonlarının bir modellemesi aşağıdaki gibi verilebilir;

H_0=IV; $H_i = f(H_{i-1}, x_i), 1 \leq i \leq t; h(x) = g(H_t)$

H_{i-1} $i-1$ ile i arasında $n-$ bitlik zincir değişkeni görevi görür. H_0 önceden tanımlanmış bir başlangıç değeridir. Keyfi bir g dönüşümü $n-$bitlik zincir değerlerini m bitlik $g(H_t)$ değerlerine dönüştürmek için kullanılır.

Herhangi bir çakışma dirençli sıkıştırma fonksiyonu f, çakışma dirençli bir h fonksiyonuna genişletilebilir.

Algoritma 3.1 (Özetlemede Merkle'nin Meta Metodu):

Girdi: Çakışma dirençli sıkıştırma fonksiyonu f

Çıktı: Anahtarsız çakışma dirençli hash fonksiyonu h

1) Farz edelim ki f, $n+r$ bitlik girdileri n bitlik çıktılara dönüştürsün.(örneğin $n = 128$ ve $r = 512$)

2) b bit uzunluklu x girdilerin $x = x_1x_2x_3 \dots x_t$ gibi her biri r uzunluklu bloklara ayıralım. Gerekirse son blok 0 bit ile r bite tamamlanır.

3) Doğruluğu kanıtlanmış b'nin ikili temsilini elde etmek için ekstra bir final bloğu x_{t+1} tanımlayalım.($b < 2^r$ kabul edelim)

4) 0'ın j bitlik şeridini 0^j ile gösterelim. x'in $n-$ bitlik hash değeri olan $h(x) = H_{t+1} = f(H_t||x_{t+1})$ sonucu $H_0 = 0^n, H_i = f(H_{i-1}||x_i), 1 \leq i \leq t+1$ hesaplanır.

h'nin çakışma dirençlidir çünkü h'ın çakışma dirençli olmaması herhangi bir $i.$ adımda f'nin de çakışma dirençli olmaması demektir.

Algoritma 3.2 (Merkle- Damgard Güçlendirmesi):

b bit uzunluğundaki $x = x_1x_2x_3 \dots x_t$ (x_i ler r uzunluklu bloklar) kabul edelim mesajı özetlemeden önce doğruluğu kanıtlanmış b'nin ikili temsilini içeren bir final x_{t+1} parça bloğu eklenir.($b < 2^r$ kabul edilir.)

Hash fonksiyonlarını uygulamada kullanılan biçimlendirme ve başlangıç değerlerinden bahsedelim.

Blok blok özetleme(hashing) metotlarında genellikle özetlemeden önce ilgili blok uzunluğunun bir katı olacak şekilde girdiye bit eklenir. Bu işleme doldurma(padding) denir.

Bir x girdisine($n-$bit blok uzunluğu) uzunluğunun katı olacak şekilde gereken sayıda 0 bit eklenerek yapılabildiği gibi; x'e sadece 1 bit eklenir ve bit uzunluğu n'nin katı olacak şekilde 0 bit (belki hiç) x'e eklenir.

3.5.3. Anahtarsız Hash Fonksiyonları (MDCs)

Anahtarsız hash fonksiyonları kullandıkları sıkıştırma fonksiyonunun yapısına göre üç kısımda incelenebilir.

i. Blok Şifrelere Dayanan Hash Fonksiyonları

İterasyonda kullanılan f fonksiyonu herhangi bir blok şifre sistemi olarak seçilir. Bir (n, r) blok şifresi; r bitlik anahtar kullanarak n bitlik açık metinden n bitlik şifreli metne; terslenebilir bir fonksiyon tanımlar, eğer E böyle bir fonksiyon ise $E_k(x)$ x'in k anahtarı altında şifrelenmesini gösterir.

$n-$bitlik blok şifreden hash fonksiyonu elde etme tek uzunluklu $(n - bit)$ ve çift uzunluklu $(2n - bit)$ hash değerleri üretenler olmak üzere iki kısımda incelenir. 2^{64} işlemin hesaplanmaz olduğu düşüncesinin doğruluğunu varsayarsak tek uzunluklu hash fonksiyonlarının amacı $n = 64$ bit blok uzunluklu şifreleri için TYHF üretmektir veya $n = 128$ bit blok uzunluklu şifreler için ÇDHF üretmektir.

ii. Modüler Aritmetiğe Dayalı Hash Fonksiyonları

Modüler aritmetiğe dayalı hash fonksiyonlarının ana fikri $modm$ ye dayalı sıkıştırma fonksiyonlarını iterasyonda fonksiyon olarak kullanmaktır. Çarpanlara ayırma ve Ayrık logaritma problemi kullanılabilir. MASH–1 ve MASH–2 bu tür algoritmalardır.

iii. Özelleştirilmiş(Customized) Hash Fonksiyonları

Özel olarak hash için tasarlanmış ve optimize hıza sahip fonksiyonlardır. MD ailesi ve SHA örnek olarak verilebilir

Bazı Mesaj Özet Fonksiyonları

MD4

MD–4 Ron Rivest tarafından1990 yılında tasarımlanmış olan bir tek yol hash fonksiyonudur. MD mesaj özetidir ve mesaj girdisi için 128-bitlik hash değeri üretir.

Rivest geliştirdiği algoritmada (Rivest 1991) 512 bitlik mesaj bloklarda tekrarlı yapı içinde her blok üç farklı döngüde işlemden geçirilir. Aynı hash değerine sahip iki mesaj bulmak yaklaşık 2^{64} uygulama gerektirir. Daha önceden belirlenmiş hash değerini sağlayan girdi bulmak ise 2^{128} uygulama gerektirir. Ancak MD4 üretildikten kısa bir süre sonra kırılmış ve Rivest tarafından MD4 güçlendirilerek MD5 geliştirilmiştir.

MD5

MD5, MD4'ün güçlendirilmiş şeklidir. MD4 üç döngüden oluşurken MD5 dört döngüden oluşur çalışma mekanizmaları benzerdir ve MD5 de 128-bitlik hash değerleri üretir. MD4'de mesaj 512 bitlik bloklarda 16.32 bitlik alt bloklar halinde işleme sokulur ve dört tane 32 bitlik çıktı üretilir.

SHA–1(Secure Hash Algorithm)

SHA, NSA tarafından DSS için üretilmiş olup 1994'de NIST tarafından yayınlanmıştır. Bu standart SHA-1, SHA-256, SHA-384, SHA-512 gibi dört standart yayınlanmıştır.

SHA-1, DSA'nın güvenliğini sağlamak için gereklidir. 264 bitten küçük boyutlu mesaj uzunluğu için SHA-1 160 bitlik bir çıktı üretir. Bu mesaj özeti DSA için bir girdi olur ve DSA bu girdi ile birlikte sayısal imza üretir.

SHA-1, Rivest tarafından geliştirilen MD4'e benzer prensiplerle çalışır. SHA-1 dört döngüden oluşur ve her döngü 20 adımdır. Mesaj 512 bitlik bloklara ayrılır eğer gerekiyorsa bit doldurma işlemi ile mesaj 512 bitin katlarına tamamlanır.

3.5.4. Anahtarlı Hash Fonksiyonları (MACs)

Anahtarlı hash fonksiyonlarının özel bir amacı bir mesajı kanıtlamaktır. Birçok sayıda MDC algoritmaları olmasına karşın MAC algoritmaları daha az sayıdadır. MACs daha önce bahsettiğimiz tek yol hash fonksiyonları ile aynı özelliklere sahiptir ancak MACs da bir anahtar da vardır. MACs simetrik sistemlerde mesaj doğrulamada kullanılabilir. MACs sayısal imza sistemlerinde zayıf olduğu için güvenli simetrik sistemlerde doğrulama için kullanılır. MACs sadece doğrulama değil bir kullanıcının dosyasının değişip değişmediğini belirlemesinde de kullanılır.

Blok Şifrelere Dayanan MACs

Blok şifrelere dayalı en yaygın kullanılan MACs CBC(Cipher-Blok-Chaining)'e dayanır. Blok şifre için DES kullanılırsa blok uzunluğu n = 64 bit ve MAC anahtarı olarak 56 bit kullanılır.

Algoritma 3.3 (CBC-MACs):

Girdi: x bilgisi; E blok şifresi ve E blok şifresi için gizli MAC anahtarı k

Çıktı: x üzerinde tanımlı MAC (n, E' nin blok uzunluğu)

1)Doldurma ve Bloklama: Eğer gerekiyorsa x bit doldurma işlemi uygulanır ve $x,\ x_1, x_2, x_3 \ldots x_t$ gibi n blok uzunluklu bloklara ayrılır.
2) CBC işlemi: E_k k anahtarı ile birlikte şifreleme dönüşümü olsun. H_t blokları aşağıdaki gibi hesaplanır;

$H_1 \leftarrow E_k(x_1)$; $H_i \leftarrow E_k(H_{i-1} \oplus x_i), 2 \leq i \leq t$ (Bu standart CBC olup IV = 0 ve şifre metin blokları $C_i = H_i$ alınır.)

3) MAC'ın gücünü artırmak için isteğe bağlı işlemler: $k' \neq k$ olacak şekilde ikinci bir gizli anahtar kullanarak $H'_t \leftarrow E_{k'}^{-1}(H_t), H_t \leftarrow E_k(H'_t)$ hesaplanır.
4) MAC, n blokluk H_t bloğudur.

MDCs den üretilen MACs, Hash'a dayalı MACs lar gibi Anahtarlı hash fonksiyonları üretilebilir. MDC algoritmasından MAC oluşturma öneri gizli bir k anahtarını bir MDC girdisinin bir kısmı olarak dahil etme fikrine dayanırken, Hash'a dayanan anahtarlı hash fonksiyonu üretmek için kriptolojik hash fonksiyonu (MD4, MD5, SHA-1 vb.) ve gizli bir k anahtarı gerekir.

4. ARAŞTIRMA BULGULARI ve TARTIŞMA

4.1. Chebyshev Polinomlarına Dayalı Açık Anahtar Algoritmaları

4.1.1. Chebyshev Polinomları

Tanım 4.1: $n \geq 0$ bir tam sayı ve $x \in R$ bir değişken n. dereceden Chebysev Polinomu

$$T_n\,(x) = 2x\ T_{n-1}\,(x) - T_{n-2}\,(x) \tag{4.1}$$

$$T_0\,(x) = 1 \qquad T_1\,(x) = x$$

şeklinde tanımlanır.

Tanımdan;

$T_0\,(x) = 1,$

$T_1\,(x) = x,$

$T_2\,(x) = 2x^2\text{-}1,$

$T_3\,(x) = 4x^3\text{-}3x,$

$T_4\,(x) = 8x^4 - 8x^2 + 1,$

.
.
.

$$\begin{cases} T_n(x) = \cos\,(n\ arccos\,(x)) & x \in [-1,1] \\ T_n(x) = \cos h\,(n\ \text{arccosh}(x)) & x \in (1,\infty) \end{cases} \tag{4.2}$$

Propozisyon 4.1:

1) $T_r(T_s) = T_s(T_r)$

2) $T_n\left(\frac{x+x^{-1}}{2}\right) = \frac{x^n+x^{-n}}{2}$ (Chein *et al.* 2011)

Yeni bir açık anahtar algoritma inşa etmek için Kocarev arkadaşları tarafından bu özellik çalışıldı.

$T_n(x)$, reel sayılarda kriptolojik açıdan güvenli değildir. Bu yüzden Kocarev ve arkadaşları bu tanımı aşağıdaki gibi genelleştirmişlerdir.

Tanım 4.2: $n \geq 0 \quad x \in \mathbb{Z}_N$ N pozitif tam sayı ve $T_0(x) = 1$ ve $T_1(x) = x$ olmak üzere;

$$T_n(x) \equiv 2x\ T_{n-1}(x) - T_{n-2}(x)(modN) \tag{4.3}$$

şeklinde olur.

Propozisyon 4.1 $\mathbb{Z}_N$ de de geçerlidir.

4.2. $\mathbb{Z}_N$ Üzerindeki Chebyshev Polinomlarına Dayalı Açık Anahtar Kriptoloji

Kocarev ve arkadaşları tarafından önerilen açık anahtar algoritması aşağıdaki gibidir (Kocarev *et al.* 2005).

Farz edelim ki Âlice, Bob ile haberleşmek istesin;

1) Bob, büyük bir s tam sayısı oluşturur, rastgele $x \in \mathbb{Z}_N$ seçer ve $T_s(x)(modN)$ hesaplar $(x, T_s(x))$ Bob'un açık anahtarı "s" gizli anahtarıdır.

2) Bob'a mesaj göndermek için Âlice, Bob'un açık anahtarı $(x, T_s(x))$'i alır ve mesajını $m \in \mathbb{Z}_N$, $\mathbb{Z}_N$ deki bir sayı gibi temsil eder, büyük ve rastgele bir r tam sayısı üretir ve

$C_1 \equiv T_r(x)(modN)$, $C_2 \equiv M \times T_r(T_s)(x)(modN)$ ifadesini hesaplayarak şifreli metin (C_1, C_2) elde eder ve Bob'a gönderir.

1) Şifreli metni aldığında Bob, gizli anahtar s ile

$$T_s(C_1) \equiv T_s\big(T_r(x)\big) \equiv T_{rs}(x) \equiv T_r\big(T_s(x)\big)(modN)$$

Hesaplayarak M $\equiv \frac{C_2}{T_s(T_r(x))}(modN)$ açık metnini elde eder.

Bu algoritma N asal iken doğru fakat N bileşik iken algoritma bazı zorluklarla karşılaşabilir. $T_r\big(T_s(x)\big)$'in tersi her zaman olmayabilir ki bu Rabin'in açık anahtar algoritması (Rabin 1979) ile aynı problemdir. $T_r\big(T_s(x)\big)(modN)$ nin tersi yok ise M tek değildir. Bunu çözmenin iki basit yolu vardır.

1) Şifrelenecek metni belirlemek için ekstra bilgi eklemek.
2) Seçtiğimiz r için , $T_r\big(T_s(x)\big)$ ile N'nin ortak böleni yeni bir r (aralarında asal olacak şekilde) seçilir.

Örnek 4.1:

Bir A kişisi, B kişisine bir M mesajını göndermek istesin. $N = 9797 = 97.101$ ve $x = 32$. B gizli anahtar olarak 4000'i seçsin. $T_{4000}(32)(mod9797) \equiv 3637$. Buradan B'nın açık anahtarı (32, 3637) olur. A'nın açık metni 601 olsun. Rastgele bir $r = 5000$ seçsin ve $C_1 = T_{5000}(32)(mod9797) = 1213$ $T_{5000}\big(T_{4000}(32)\big)(mod9797) \equiv 3637$

$C_2 \equiv 601.3637(mod9797) \equiv 1106$ ve sonra şifreli metni $C = (1213,1106)$ elde eder ve B'ye gönderir.

4.3. Chebysev Polinomlarına Dayalı Sayısal İmza Sistemi

1) B, büyük bir s tam sayısı oluşturur, rastgele $x \in \mathbb{Z}_N$ seçer ve $T_s(x)(modN)$ hesaplar $(x, T_s(x))$ Bob'un açık anahtarı '' s'' gizli anahtarıdır.

İmzalama Algoritması

2) A imzalama için, B'nin açık anahtarı $(x, T_s(x))$'i alır ve m mesajının $h(m)$ hesaplar, $h(m)$ $\mathbb{Z}_N$ deki bir sayı gibi temsil eder, büyük ve rastgele bir r tam sayısı üretir ve

$S_1 \equiv T_r(x)(modN)$, $S_2 \equiv h(m) \times T_r(T_s)(x)(modN)$ hesaplayarak mesajı (S_1, S_2) elde eder ve imzayı mesaja ekleyerek B' ye gönderir.

Doğrulama algoritması

1) B, gizli anahtarı s ile

$$T_s(S_1) \equiv T_s\big(T_r(x)\big) \equiv T_{rs}(x) \equiv T_r\big(T_s(x)\big)(modN)$$

Hesaplayarak $v \equiv \frac{S_2}{T_s(T_r(x))}$ $(modN)$ açık metnini elde eder.

2) Aynı özet fonksiyonu kullanarak $r = h(m)$ elde eder.
3) $v = r$ ise imza doğrudur.

Örnek 4.2:

$N = 11$ için B anahtar oluştururken $s = 3$ ve $x = 2,\ 2 \in \mathbb{Z}_{11}$ olarak seçsin bu durumda B' nin açık anahtarı $(x\ , T_s\ (x)\ )\ \equiv (2\ , T_3\ (2)\ )(mod 11) = (2{,}4)$ olur. B'nin gizli anahtarı ise $s\ =\ 3$ tür.

m mesajının özeti $h(m)\ =\ 4$ olsun. A m mesajını imzalarken $r = 5$ olarak seçsin. A, B'nin açık anahtarı (2,4) yardımı ile $S_1 \equiv T_5\ (2)(mod 11) \equiv 10(mod 11)$, $S_1 =\ 10$ ve $S_2 \equiv 4\ \times T_5(T_3)(2)(mod 11) \equiv 4 \times 10(mod 11) \equiv 7$ olarak bulur. $(S_1\ , S_2) = (10, 7)$ m mesajına ekleyerek B'ye gönderir.

İmzayı doğrulamak için B, m mesajına aynı özet fonksiyonu uygular $r\ =\ h(m)\ =$ 4 hesaplar. Kendi gizli anahtarı ile $T_s(S_1) \equiv T_3(10)(mod 11) \equiv 10$ ve

$$v\ \equiv \frac{S_2}{T_s(T_r(x))}\ (mod N)$$

$$v\ \equiv \frac{7}{10}(mod 11) \equiv 7.10^{-1}(mod 11) \equiv 7.10(mod 11)$$

hesaplar,

$$v\ =\ 4$$

olarak bulur.

$v\ =\ r\ =\ 4$ olup imza doğrudur.

Burada hesaplama kolaylığı açısından küçük sayılar kullanılmıştır ancak güvenlik açısından yeterince büyük sayılar kullanılmalıdır.

5. SONUÇ

Kriptoloji gelişen teknoloji ve internet kullanımının yaygınlaşması ile önemini artırmaya devam etmektedir. Teknolojideki bu gelişmeler özellikle sayısal imza algoritmaları kullanımını giderek artırmaktadır. Açık anahtar şifrelemede yeni arayışlar ve güvenli sistemler oluşturma çabası devam etmektedir. Bu çalışmada gizli ve açık anahtar kripto sistemler tanıtılmış ve son zamanlarda açık anahtar şifreleme için Kocarev ve arkadaşlarının önerdiği $\mathbb{Z}_N$ Üzerindeki Chebyshev Polinomlarına Dayalı Açık Anahtar Kriptoloji tanıtılmış ve örnek verilmiştir. Ayrıca bu açık anahtar sistemden faydalanarak bir sayısal imza algoritması verilmiş ve örneklendirilmiştir. Bu sistemlerde N asal olarak seçildiği zaman verilen algoritmalar doğrudur ancak N bileşik olduğunda her zaman kullanılamayabilir. N bileşik iken $\mathbb{Z}_N$ halkasında Chebyshev Polinomu tarafından üretilen dizinin periyodu Chen ve arkadaşları tarafından analiz edilmiştir. Yayınladıkları makalede periyot dağılımını incelemek için rekürans bağıntısını elde etmede klasik cebirsel teorileri kullanılmıştır. Buna göre eğer N özenle seçilmezse, periyot dağılımının zayıf olduğu ortaya çıkmıştır. Atakları etkisiz kılmak için Chebyshev polinomları tarafından üretilen dizinin periyodunu yeterince yüksek kılmak gerekmektedir. Bu yüzden N dikkatli seçilmelidir.

KAYNAKLAR

Chein F., Liao, Xiang. T., Zheing. H., 2011. Security analysis of the pubic key algorithm based on Chebyshev polinomials over the integer ring $\mathbb{Z}_N$.İnformation Sciences, 181, 5110-5118 .

Çetin, Ö., 2006. Eliptik Eğri Kriptografisi. Y. Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara.

Diffie. W., Hellman. D., 1976. New directions in cryptography. IEEE Transactions on Information Theory , 22 (6), 644–654.

ElGamal. T., 1985, A Public Key Cryptosystem and a Signature Scheme Based on discrete logarithm problem. IEEE Transactions on information Theory, Springer, 31(4), 469-472.

Frösen. J., 1995, Practical Cryptosystems and Their Strength**,** Proceedings of HUT Seminar on Network Security. Helsinki University of Technology**,** Helsinki, 38 45

Husemöller.D., 1987.,Eliptic Curves Second Edition.Springer, 510, Newyork.

Johnson, D.B., Menezes, A.J., 2007. Elliptic Curve DSA(ECDSA): An Enhanced DSA.Scientific Commons.

Kaliski B.,1991. Letter to NIST regarding DSS,

Khalique, A., Singh, K. ,Sood, S. , 2010. İmplemention of Eliptic Curve Digital Signature Algorithm. İnternatiol Journal of Computer Aplıcations, 2(3), 21-27.

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

Kocarev L., Makraduli j., P. Amato., 2005 Public-key encryption based on Chebyhev polynomials. Circuits, Systems, and Signal Processing ,24 (5) , 497–517.

Menezes, J., Oorshot, P., Vanstone, S., 1996. Handbook of Aplied Cryptography. Crc Press,780 p.

National Institute of Standards and Technology, NIST FIPS PUB 186, "Digital Signature Standard," U.S.Department of Commerce, May 1994.

Odtü Uyguamalı Matematik Ensitisü Kriptolojiye Giriş Ders Notları 2004.

Rabin M.1979, Digitalized signatures and public-key functions as intractable as factorization. Technical Report TR-212, Massachusetts Institute of Technology, Cambridge, MA, USA,

Rivest. R., Shamir A., Adleman A., 1978, Method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM 21 (2), 120-129.

Rivest, R.L., 1991. The MD4 Message Digest Algorithm. *Advances in Cryptology CRYPTO '90 Proceedings*,Springer–Verlag, 303–311.

Soyalıç, S., 2005. Kriptografik Hash Fonksiyonları ve uygulamaları. Y. Lisans Tezi , Erciyes Üniversitesi Fen Bilimleri Enstitüsü , Kayseri.

Schneier, B., 1996. Applied Cryptography Second Eduation. John Willey&Sons, İnc. 1125 p.

Washington, L. C., 2003.Elliptic Curves, Number Theory and Cryptography. Chapman&Hall/Crc, 428.

ÖZGEÇMİŞ

1988 yılında Amasya'da doğdu. İlk ve orta öğrenimini Amasya da tamamladı. 2006 tarihinde Atatürk Üniversitesi Fen Fakültesi Matematik Bölümüne yerleşerek lisans öğrenimine başladı ve 2010 yılında mezun oldu. Aynı yıl Matematik Anabilim Dalında Yüksek Lisans öğrenimine başladı. 2011 yılında öğretmen olarak göreve başladı. Halen lisansüstü eğitimine devam etmektedir.