Yüksek Lisans Tezi

Erkam LÜY

Matematik

2012

T.C.
ERCİYES ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
MATEMATİK ANABİLİM DALI

ABELYAN OLMAYAN SONLU GRUPLAR KULLANILARAK ELDE EDİLEN AÇIK ANAHTAR KRİPTOSİSTEM ÜZERİNE

Hazırlayan
Erkam LÜY

Danışman
Yrd. Doç. Dr. Emin AYGÜN

Ocak 2012
KAYSERİ

T.C.
ERCİYES ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
MATEMATİK ANABİLİM DALI

ABELYAN OLMAYAN SONLU GRUPLAR KULLANILARAK ELDE EDİLEN AÇIK ANAHTAR KRİPTOSİSTEM ÜZERİNE

Hazırlayan
Erkam LÜY

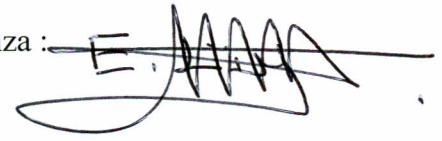
Danışman
Yrd. Doç. Dr. Emin AYGÜN

Yüksek Lisans Tezi

Ocak 2012
KAYSERİ

Bu çalışmadaki tüm bilgilerin, akademik ve etik kurallara uygun bir şekilde elde edildiğini beyan ederim. Aynı zamanda bu kural ve davranışların gerektirdiği gibi, bu çalışmanın özünde olmayan tüm materyal ve sonuçları tam olarak aktardığımı ve referans gösterdiğimi belirtirim.

Adı-Soyadı Erkam LÜY

İmza : 

"Abelyan Olmayan Sonlu Gruplar Kullanılarak Elde Edilen Açık Anahtar Kriptosistem Üzerine" adlı Yüksek Lisans tezi, Erciyes Üniversitesi Lisansüstü Tez Önerisi ve Tez Yazma Yönergesi'ne uygun olarak hazırlanmıştır.

Tezi Hazırlayan

Erkam LÜY

Danışman

Yrd. Doç. Dr. Emin AYGÜN

Prof. Dr. Fuat GÜRCAN

ABD Başkanı

Yrd. Doç. Dr. Emin AYGÜN danışmanlığında **Erkam LÜY** tarafından hazırlanan **"Abelyan Olmayan Sonlu Gruplar Kullanılarak Elde Edilen Açık Anahtar Kriptosistem Üzerine"** adlı bu çalışma jürimiz tarafından Erciyes Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalında yüksek lisans tezi olarak kabul edilmiştir.

02 /01/2012

JÜRİ:

Başkan : Prof. Dr. Fuat GÜRCAN

Üye : Prof. Dr. Hüseyin ALTINDİŞ

Üye : Yrd. Doç. Dr. Emin AYGÜN

ONAY:

Bu tezin kabulü Enstitü Yönetim Kurulunun 17/01/2012 tarih ve 2012/04-09 sayılı kararı ile onaylanmıştır.

17/01/2012

Prof. Dr. Necmettin MARAŞLI
Enstitü Müdürü

TEŞEKKÜR

Bu tez çalışması sürecinde benden desteğini ve yardımlarını esirgemeyen, bilgi ve tecrübesi ile bana yol gösteren ve kendilerinden çok şey öğrendiğim, üzerimde çok emeği bulunan değerli hocalarım Prof. Dr. Hüseyin ALTINDİŞ'e ve Yrd. Doç. Dr. Emin AYGÜN'e teşekkürü borç bilir kendilerine minnet ve şükranlarımı sunarım.

Benden maddi, manevi desteklerini esirgemeyen ebeveynime, çalışma arkadaşlarım Arş. Gör. Tunçar ŞAHAN'a ve Arş. Gör. Hasan ARSLAN'a ayrıca teşekkür ederim.

ABELYAN OLMAYAN SONLU GRUPLAR KULLANILARAK ELDE EDİLEN AÇIK ANAHTAR KRİPTOSİSTEM ÜZERİNE

Erkam LÜY

Erciyes Üniversitesi, Fen Bilimleri Enstitüsü

Yüksek Lisans Tezi, Ocak 2012

Tez Danışmanı : Yrd. Doç. Dr. Emin AYGÜN

ÖZET

Bu tez üç bölümden oluşmaktadır.

Birinci bölümde kriptolojiyle ilgili temel bilgiler ve kullanılan matematiksel tanımlar verilerek bazı şifreleme metodları incelendi.

İkinci bölümde Yarı-Direkt Çarpım yöntemiyle Abelyan olmayan gruplar oluşturuldu. Bu gruplar kullanılarak elde edilen açık anahtar kriptosistem örneklerle açıklandı. Burada Paeng ve arkadaşları [3] tarafından önerilen, değişmeli olmayan sonlu gruplar kullanılarak inşa edilen açık anahtarlı şifreleme metodu özel lineer gruplar için incelendi**.**

Üçüncü bölümde kriptosistemin diğer bazı sistemlere göre neden daha hızlı şifreleme yaptığı ve kırılmasının daha zor olduğu incelendi. Ayrıca sistemin güvenilirliği ve zayıf noktaları örnek verilerek açıklandı.

Anahtar Kelimeler**:** Abelyan Grup, Açık Anahtar Kriptosistem, Özel lineer gruplar, İç otomorfizma, Üreteç.

ON PUBLIC KEY CRYPTOSYSTEM USING FINITE NON ABELIAN GROUPS

Erkam LÜY

Erciyes University, Graduate School of Natural and Applied Sciences

M. S. Thesis, January 2012

Thesis Supervisor: Assist. Prof. Dr. Emin AYGÜN

ABSTRACT

This thesis consists of three chapters,

In the first chapter some criptografic methods are examined and some mathematical definations used in the next chapter are given.

In the second chapter non abelian groups are obtained using semi-direct-produc method. In particular, Public Key Criptosystems Using these Groups are explained with examples. Here, Public Key Criptosystem obtained finite non abelian groups and proposed by Paeng et al. [3] are examined for special linear groups.

In the third chapter we examine why the system is faster and more secure than the other some systems. Also the safety and deficits of the system are explained using some examples.

Keywords: Abelian Group, Public Key Criptosystem, Special linear groups, Inner automorphism, Generator.

İÇİNDEKİLER

ABELYAN OLMAYAN SONLU GRUPLAR KULLANILARAK ELDE EDİLEN AÇIK ANAHTAR KRİPTOSİSTEM ÜZERİNE

2. BÖLÜM
ABELYAN OLMAYAN GRUPLARLA ŞİFRELEME

3. BÖLÜM
SONUÇ, TARTIŞMA ve ÖNERİLER

KISALTMALAR VE SEMBOLLER

$\mathbb{R}$: Reel Sayılar Kümesi

$\mathbb{N}$: Doğal Sayılar Kümesi

$\mathbb{Z}$: Tamsayılar Kümesi

Aut(G): G'nin otomorfizma grubu

Inn: İç otomorfizma fonksiyonu

$\mathbb{Z}_n$: { 0,1,2,...n-1 } tamsayılarının cümlesine mod n tamsayıları denir

$\mathbb{Z}_n^*$: $\mathbb{Z}_n$'in çarpımsal grubu

$\left|\mathbb{Z}_n^*\right|$: $\mathbb{Z}_n^*$'ın mertebesi

$M(n, K)$: Elemanları K cismine ait olan $n \times n$ tipindeki karesel matrislerin kümesi.

$SL(n, K)$: Özel lineer grup

$GL(n, K)$: Genel lineer grup

ord(g): g'nin mertebesi

δ_{ij} :(i, j)-bileşeni (i. satır, j. sütunu) 1 diğer bileşenleri 0 olan matris.

E: Şifre metin

M: Açık metin

CP: Konjugasyon problemi

DLP: Discrete (ayrık) logaritma problemi

NIST: A.B.D. Teknoloji Standartları Enstitüsü

DES: Veri Şifreleme Standardı (Data Encryption Standard)

AES: Gelişmiş Şifreleme Standardı (Advenced Encryption Standard)

UEKAE: Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü

Bu tezdeki örneklerde A şifreleyen kişi, B şifre çözen kişidir.

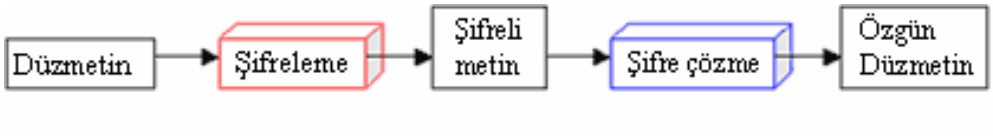
GİRİŞ

Aşağıda Kriptoloji'nin tarihi, önemi, savaşlara nasıl etki ettiği, kullanım alanları ve günümüzde bu konuyla yapılan çalışmalar özet olarak incelendi. Bunun için genellikle, Altındiş [1], Tübitak Uekae [2], Çimen [17], Babaoğlu [20] ve Kara [21] kaynaklarından yararlanılmıştır.

Gizlilik sistemlerinin bağlı olduğu bilim dalı *Kriptoloji* olarak bilinir. Kriptoloji, kişiler arası veya özel devlet kurumları arasındaki mesajlaşmalardan, sistemlerin oluşumunda ve işleyişindeki güvenlik boşluklarına kadar her türlü dalla alakalıdır. *Kriptoloji*, matematiğin hem şifre bilimini (*kriptografi*), hem de şifre analizini (*kriptanaliz*) kapsayan bir dalıdır.

Kriptografi, köken olarak Yunanca gizli saklı anlamına gelen *kryptos* ve yazmak anlamına gelen *graphein* sözcüklerinden türetilmiştir. Kriptografi gizlilik sistemlerinin tasarım ve araçları ile ilgilenen, gizlilik, kimlik denetimi, bütünlük gibi bilgi güvenliği kavramlarını sağlamak için çalışan matematiksel yöntemler bütünüdür. Bu yöntemler, bir bilginin iletimi esnasında karşılaşılabilecek saldırılardan bilgiyi, bilgi göndericisini ve alıcısını koruma amacını taşır. Kriptografi ile ilgilenen bilim adamlarına *kriptograf* denir.

Şifreleme düz bir metnin içeriğini, istenmeyen şahıslar tarafından okunmasını engellemek için iletiyi bir takım yöntemlerle okunamayacak hale getirme işlemidir. Deşifreleme ise şifrelemenin tam tersi olup, şifreli metnin düz metne çevrilmesi işlemidir. Bu Şekil 1.1 ile basitçe şöyle gösterilebilir.



Şekil G.1. Bir Düz Metnin Şifrelenmesi ve Deşifrelenmesi

Kriptanaliz ise bazı teknikler kullanılarak ele geçen şifrelenmiş metinden şifrelenmemiş metni bulma yöntemidir. Kriptanaliz ile uğraşanlara *kriptanalist* denir. Kriptanalistler aynı zamanda kriptografi konusunu da detaylarıyla bilmelidirler, çünkü şifrelerin nasıl tasarlanabileceğini bilmeyen biri nasıl çözüleceği konusunda fikir de yürütemez. Kriptanalistlerin başarısı kriptografları yeni ve daha güvenli sistemler tasarlamaya zorlamıştır. Bu iki bilimin bütününe ise eski Yunancadan gelme *kryptos* (gizli) ve *logos* (bilim) kelimelerinin birleşimi olan *kriptoloji* denmektedir. Kriptoloji ile ilgilenen bilim adamlarına *kriptolog* denir.

Günümüzde yaygın olarak kullanılan ve üzerinde yaygın araştırmalar yapılan kripto temelleri M.Ö. 2000'li yıllara kadar uzanmaktadır. Kriptoloji tarihinin ilk kayıtları Mısır yazıtlarında rastlanan kriptografik öğelerden oluşmaktadır. "Menet Khufu" kasabasında bulunan (Nil Nehri yakınlarında bir kasaba) hiyerogliflerin şifreleri çözüldüğünde, bazılarında daha önce hiç bilinmeyen olan simgelerin kullanılmış olduğu belirlenmiştir. Sadece ilgili kişi tarafından anlaşılabilir olan simgelerin bu kişi dışındakiler tarafından anlaşılmaması için kodlandığı sonucuna varılmıştır. Bunun güvenliği sağlamak üzere uygulanmış bir şifreleme tekniği olduğu kabul edilmektedir. O yıllarda kriptoloji ve şifre kırma faaliyetleri sadece askeri ve diplomatik alanlarda kullanılıyordu ve yok denecek kadar azdı.

M.Ö. 1500'lü yıllarda Mezopotamya'da kripto kullanıldığı tespit edilmiştir. Bölgede bulunan tabletler üzerindeki çivi yazısı şekillerin çözümlenmesinden sonra anlaşılabilir duruma gelmiştir. Ayrıca, aynı yöntemler uygulanarak bazı metinlerin okunamadığı görülmüştür. Yapılan kriptolojik analizler sonrasında okunamayan metinlerden birinin, çömlek yapımı için geliştirilmiş olan bir bileşimin şifreli olarak kaydını içerdiği anlaşılmıştır.

Al-Kindi (Arap Filozof), Modern Kriptolojinin Temellerini Oluşturmuştur

Filozof Al-Kindi'nin (Doğumu: 801 - Ölümü: 873) Risale fi'sihrâci'l-mu'amma'sı mesaj gizleme ve çözme yöntemlerine dair zamanımıza ulaşan en eski eserdir. Kindi, Kriptografi'nin iki temel yöntemi olan "yerine koyma" ve "yer değiştirme" işlemlerini ilk defa tanımlamış ve bu ikisinin birlikte kullanıldığı karma şifreleme sistemlerini tarif etmiştir. Şifrelerin çözülmesine ilişkin olarak, hitabe ve mektupların başlangıç

kısımlarında yer alan muhtemel kelimelerin oluşturduğu zayıflıkların değerlendirilmesi, kelimelerde bir araya gelen ve gelemeyen harflerin analizi, harflerin kullanılma sıklığının istatistiki analizi gibi kriptografinin temel esasları yine Kindi tarafından ortaya konmuştur. Batılı bilginlerden Leon Battista Alberti 1466 yılında ve Trilhemius 1508 yılında yazılı eserler vermiştir. Bu bilim adamları ile Al-Kindi arasındaki yüzyıllar seviyesindeki fark, kriptoloji konusunda arap dünyasının öncü rolünü ortaya koymaktadır.

Başka bir Arap bilgini olan Abdurrahman el-Halil ibn-Ahmet, "Kitab-ül Muamma" adlı kriptoanaliz kitabını M.S. 8. yüzyılda yazmıştır. Bu çalışmada Abdurrahman el-Halil, Bizans imparatoru tarafından gönderilen Yunanca bir şifreli mektubun çözümü yer almaktadır.

Yine bir arap matematikçi olan Abdullah Kelkeşandi de 15. yüzyılda kriptoanaliz çalışmaları yapmıştır.

Anadolu'da M.Ö. 457 yılında Ispartalılar tarafından Scytale olarak adlandırılan kriptolama tekniğinin kullanıldığını görüyoruz. Belirli çaptaki bir silindire şerit şeklindeki kağıdın sarılarak yazının bu şekilde oluşturulan sayfaya yazılması biçiminde özetlenebilecek bu teknik ile sırası karışık olan simgeler-harfler içeren bir şerit elde edildi. Bu şerit üzerindeki yazının okunabilmesi için yazımında kullanılan çapta bir silindire sarılması gerekmekteydi. Mesajın gönderileceği kişide bu silindirin aynısı bulunmaktaydı. (Günümüzdeki modern kripto tekniklerine bir benzetme yapılacak olursa, silindirin çap değeri kripto anahtarına karşılık gelmektedir.)

Kriptoloji Roma imparatorluğu döneminde oldukça gelişmiş ve simgeler üzerinde belirli işlemler kullanılmaya başlanmıştır. M.Ö. 100 yılında doğmuş olan Julius Ceasar, her harfin alfabede kendisinden sonra gelen üçüncü harfle yer değiştirdiği bir kriptolama tekniğini generallerine gönderdiği mesajlarda uygulamıştır. Benzer biçimde General Agustus da, "bir sonraki harfle yer değiştirme" kriptosu kullanmıştır.

Güvenliği düşük ve sabit anahtarlı olan bu yöntem, düşman tarafından bilinmediği için yeterli düzeyde güvenlik sağlanmıştır. (Günümüz kriptoanaliz tekniklerinden "Geçiş Sıklığı Analizi" yöntemiyle bu tipte sabit anahtarlı bir şifrelemenin çözülmesi son derece kolaydır.)

Ayrıca Roma döneminde steganografi de kullanılmıştır. Gönderilecek olan mesaj, saçları kazıtılmış bir kölenin kafasına kolayca silinmeyecek bir madde (mesela kına) ile yazılmakla ve köle saçları uzadıktan sonra karşı tarafa gönderilmekte, karşı taraf ise kölenin saçlarını kazıyarak mesajı okumaktaydı. Bilginin güvenliği bu yöntemde, uygulamanın düşman tarafından bilinmediği varsayımına dayanmaktadır.

Leon Alberti 1404-1472 yılları arasında yaşamış ve 1466-1467 yılları arasında ilk kez çoklu alfabe kullanarak kriptolama yapmıştır. Bu yöntemde, Ceasar şifreleme yöntemine benzer olarak harf kaydırma tekniği uygulanıyordu. Ama Ceasar şifrelemeden farklı olarak kaydırma miktarı sabit olmayıp, kullanıcının kararına göre belirleniyordu. Şifrelenecek metinde Alberti Diski yardımıyla her harfin kriptolu karşılığı bulunuyordu. İçteki çemberi sabit, dıştaki çemberi onun etrafında dönebilen bu disk yardımıyla, her harfin istenilen miktarda ötelenmiş hali kolaylıkla görülebiliyordu.

Blaise de Vigenere, Sezar kripto sisteminin bir türevi olan "Vigenere Sistemi"ni 1586 yılında geliştirdi. Bu sistemde, şifrelenecek olan karakter Ceasar kripto sisteminde olduğu gibi tüm metin boyunca sabit bir miktarda değil, periyodik olarak değişen bir sayı dizisine göre öteleniyordu. Mesela kullanılan şifreleme sayı dizisi 183725 ise, kriptolanacak verinin ilk harfi birinci iki harfi sekiz üçüncü harfi üç ve benzer şekilde altıncı harfi beş karakter öteleniyordu. Yedinci karakter ise tekrar 1 kez ötelenerek, bu kural metnin tamamı şifrelenene dek uygulanıyordu.

Vigenere sistemiyle şifreleme yaparken kolaylık sağlamak için "Vigenere Tablosu" kullanılmaktaydı. Vigenere sistemi 1800'lü yılların ortalarına kadar "kırılması imkansız" olarak nitelendirildi. Charles Babbage, anahtar uzunluğuna dayalı frekans analizi uygulayarak bu şifreyi kırmayı 1854 yılında başardı ve 1864 yılında "Gizli Yazma ve Şifre Çözme Sanatı" adlı kitabında bu yöntemi yayınladı. Babbage'dan bağımsız olarak 1863 yılında Kasiski de aynı saldırı yöntemini geliştirmişti.

l860'lı yıllardaki Amerikan İç Savaşı'nda Güneyliler Vigenere şifreleme yöntemini kullanmışlardır. Yöntemin kırılmazlık lakabına çok güvenen ve sadece 3 farklı anahtar kullanan Güneyliler, Kuzeyli kriptoanalizcilerin işini kolaylaştırmış ve kriptolu metinlerin kolaylıkla kırılabilmesini sağlamışlardır. 620 bin kişinin hayatını kaybettiği savaşı Kuzeylilerin kazanmasında kriptoanaliz faaliyetlerinin de önemli bir payı bulunmakladır.

1925'te bu tipteki ötelemeli şifreleme sisteminin analizini yapmak üzere Friedman bir test geliştirdi. Şifreli metindeki iki harfin açık metindeki aynı karakterden gelme olasılığını irdelemek üzerine kurulmuş olan bu test, Friedman'ın kendi adıyla biliniyordu.

Vernam, kendi adıyla anılan şifreleme sistemini Vigenere şifreleme sistemini temel alarak geliştirdi. Vigenere sisteminde kullanılan periyodik sayı dizisinin periyodunu sonsuza götürmeyi önerdi. Bu durumda, kriptolanacak karakterin kaç kez öteleneceğini belirleyen sayı dizisi kriptolanacak metnin içerdiği karakter kadar sayı içeriyordu. Başka bir ifadeyle her karakter kendisi için özel olan bir sayı kadar öteleniyordu ve bu sayı tekrar kullanılmıyordu. Bu şekilde ortaya çıkan Vernam şifresinin kırılması teorik olarak imkansızdır. Bununla birlikle, her mesajı şifrelemek veya şifresini çözmek için mesaj uzunluğunda şifreleme dizisinin karşı tarafa iletilmesini zorunlu kıldığı için uygulanması oldukça zor bir yöntemdi.

Kriptolojinin gelişim yönünü belirleyen temel etkenlerden biri de Transistörün icadı sonrasında elektronikteki teknolojilerin hızla gelişmesi oldu. Kriptoanaliz çalışmalarında yüksek işlem kapasitesi sağlayan bilgisayarlar ve elektronik devreler temel yapıtaşı olarak kullanılmaya başlandı. Bu kadar güçlü kriptoanalitik saldırı altyapısı karşısında dahi güvenliği sağlayabilecek kripto algoritmalarının tasarımında yine görev matematikçilere düşüyordu.

Bugün de kriptoanalistler ile Kripto algoritması tasarımcıları arasındaki bu denge sürmektedir ve gelecekte de sürecektir. Kripto algoritmalarının güvenliği Kriptoanaliz yeteneklerinin arttığı ölçüde kanıtlanabilir biçimde artırılmak zorundadır. Kripto algoritmalarının güvenilirliğinin sadece kullanılan kripto değişkenlerinin boyuna bağlı olmadığı, geliştirilen matematiksel çözümleme yöntemlerine karşı da dayanıklı olması gerektiği göz önünde tutulmalıdır.

Günümüzde Kriptoloji

Günümüzde elektronik bankacılığın yaygınlaşması ve elektronik ticaretin kullanılmaya başlanması gibi sebepler gizliliği bu alanda da ön plana çıkarmıştır. Dolayısıyla kriptografi alanına büyük çapta ticari ilgi doğmuştur. Bilgisayarların hızlı bir şekilde yaygınlaşması, haberleşme sistemlerinin gelişmesi, özel sektörün dijital formda bilgiyi

koruma ve güvenlik sağlama isteği bu alanda yapılan çalışmaların önemini daha da artırmaktadır.

İletişim tekniklerindeki gelişmeler bilgiyi saklama ve iletme açısından işleri zorlaştırmakta, yeni teknikler geliştirmek için insanları zorlamaktadır. Telefon görüşmeleri uydudan yansımakta; internet üzerinden yapılan her işlem de binlerce bilgisayarlardan geçmektedir. Haberleşme ve bilişimin genel sorunu bilgi güvenliğidir. Özellikle son yıllarda artan internet üzerinden yapılan sanal alışverişler, bireysel bankacılık işlemleri ve e-posta trafiği interneti daha güvenli bir ortam olmaya zorlamaktadır. İnternet üzerindeki ticari işlemler, yılda milyar dolarları aşmaktadır. Rakamlar bu kadar yüksek olunca kriptografik güvenlik yöntemlerinin kullanımı zorunlu hale gelmiştir. İnternet üzerinde ise tam güvenliği sağlamak olanaksızdır. İnternet altyapısında ve haberleşme araç gereçlerinde teknolojiyi belirleyenler, haberleşme ve güvenlik konularında da en avantajlı ülkelerdir. O halde sorun, bilgi ve haberleşme güvenliğinin yüksek oranda sağlanmasının nasıl gerçekleşeceğidir. Bunu sağlayacak olan da şifrebilimdir. Tüm bunlar, günümüzde teknolojinin gelişmesiyle ortaya çıkan güvenlik problemlerinin çözülmesinin ve eski çağlardaki kodlamadan yola çıkan ve günümüzde disiplinlerarası bir bilim haline gelmiş kriptografinin ne denli önemli olduğunu göstermektedir.

1970'lerin başında IBM'de çalışılmaya başlanan ve A.B.D. Teknoloji Standartları Enstitüsü NIST tarafından her dört yılda bir güvenliği onaylanan Veri Şifreleme Standardı kısa adıyla DES (Data Encryption Standard), 1990'lı yıllara kadar tarihte en iyi bilinen kriptolojik mekanizma idi. Fakat 1991'de Biham ve Shamir (RSA'nın S'si) tarafından yapılan diferansiyel atakla DES yara aldı. Atak pek pratik değildi ve uygulama için çok sayıda seçilmiş açık metin gerekiyordu. Asıl darbe iki yıl sonra Japonya'lı Mitsuri Matsui'nin doğrusal kriptanalizi keşfetmesiyle gerçekleşti. Matsui bir sene sonra da pratik bir doğrusal atak düzenleyerek DES'i kırdı.

Bütün bu gelişmeler DES'in artık şifreleme algoritması olarak ömrünü tamamladığını ve 2000'li yılların güvenlik ihtiyacını karşılamaktan uzak olduğunu gösteriyordu. NIST (National Institute of Standards and Technology-Ulusal Standartlar ve Teknoloji Enstitüsü) 1997'de yeni bir şifreleme standardı için yarışma başlattı ve yarışma 2001 yılında sonuçlandı. Rijmen ve Daemen adlı iki Belçikalı kriptoloğun tasarladığı

Rijndael adlı algoritma AES (Advenced Encryption Standard - Gelişmiş Şifreleme Standardı) adıyla yeni standart şifreleme algoritması olarak seçildi. Günümüzde AES tüm dünyada en yaygın kullanılan şifreleme algoritmalarından biridir.

Bugünün kriptografisi şifreleme ve şifre çözmeden daha fazlasını içermektedir. Kimlik denetimi artık gizlilik kadar önemlidir. Herhangi bir iletiye adımızı ekleyip ağ üzerinden gönderdiğimiz zaman kimliğimizi ispatlamak için elektronik yöntemlere ihtiyaç duyarız. Kriptografinin buna sunduğu çözüm sayısal imzadır. İmza; inkâr edememe, veri kaynağı doğrulama, kimlik saptama ve tanıklık gibi çoğu servisin temel taşıdır. Sözleşme zamanında imza, kişinin kimliğinin çok önemli bir kısmını üstlenir. Ayrıca imza kimlik saptama, yetki verme ve onaylama görevlerini yapacak şekilde kişiye özel hazırlanır.

Ülkemizdeki üniversitelerde, özellikle ODTÜ'de Kriptoloji Anabilim Dalında ve TÜBİTAK UEKAE'de (Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü) bu alanda ciddi çalışmalar yapılmaktadır. Ayrıca, Bilgi Teknolojileri ve İletişim Kurumu, Bilgi Güvenliği Derneği, Gazi Üniversitesi ve Orta Doğu Teknik Üniversitesi işbirliği ile düzenlenen "Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı"nın bu sene 5.si düzenlenmiştir.

Bu tez çalışmasının amacı, genel olarak abelyan olmayan sonlu gruplar kullanılarak elde edilen açık anahtar kriptosistem üzerine incelemeler yapmaktır. Kriptoloji ile ilgili genel bilgiler üzerinde duruldu. Şifrelemenin ve deşifrelemenin nasıl yapıldığı ile ilgili bazı şifreleme metodları incelendi, abelyan olmayan grupların nasıl elde edildiklerinden bahsedildi. Sonlu abelyan olmayan gruplar kullanılarak açık anahtar kriptosistemin nasıl elde edildiği üzerinde duruldu. Bu şekilde elde edilen kriptosistemin avantajları ve dezavantajları tespit edildi.

1. BÖLÜM

TEMEL KRİPTOLOJİK KAVRAMLAR

Bu bölümde öncelikle Kriptoloji ile ilgili temel matematiksel kavramlardan bahsedilecektir. Ayrıca Kriptolojide kullanılan bazı terimler, şifreleme çeşitleri incelenen metodla yakından alakalı olan RSA ve EL-GAMAL tipi şifreleme metodları örneklerle açıklandı. Bu bölümde istifade edilen temel kaynaklar Altındiş [1], Tübitak Uekae Dergisi Sayı 1[2], Stinson [16], Bruce[19] ve Koblitz [14],[15] dir.

1.1. Temel Matematiksel Kavramlar

Tanım 1.1.1. *A* ve *B* iki küme olmak üzere *A*'nın her bir elemanını *B*'nin bir elemanına götüren kurala *A*'dan *B*'ye bir *dönüşüm* denir ve $f: A \to B$ şeklinde gösterilir. *A*'dan *B*'ye bir dönüşüme *fonksiyon* denir.

Tanım 1.1.2. *f*, *A*'dan *B*'ye bir dönüşüm olsun. Buna göre $f(A) = \{ f(a): a \in A\}$ kümesine *A*'nın *f* altındaki *görüntüsü* denir ve *Im(f)* ile gösterilir.

$f(A) \subset B$ ise *f* dönüşümüne içine, $f(A) = B$ ise *f*'ye *örten* denir. Her $a_1, a_2 \in A$ olmak üzere $a_1 \neq a_2$ için $f(a_1) \neq f(a_2)$ ise veya $f(a_1) = f(a_2)$ için $a_1 = a_2$ olmasını gerektiriyorsa *f*'ye *birebirdir (veya 1-1)* denir.

f'in 1-1 ve örten olması halinde *f* dönüşümünün tersi mevcuttur**.** Kriptografide 1-1 ve örten fonksiyonlar mesajların şifrelenmesinde, ters fonksiyonlar ise mesajların deşifrelenmesinde kullanılırlar.

Tanım 1.1.3. *G* boş olmayan bir küme ve '·' da *G* üzerinde tanımlı bir ikili işlem olsun. Eğer aşağıdaki şartlar sağlanıyorsa (*G*, ·) sistemine bir *grup* denir.

(i) Her $a, b \in G$ için $a \cdot b \in G$ dir (kapalılık özelliği).

(ii) Her $a, b, c \in G$ için $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ dir (birleşme özelliği).

(iii) Her $a \in G$ için $a \cdot e = e \cdot a = a$ olacak şekilde bir $e \in G$ vardır (birim eleman özelliği).

(iv) Her $a \in G$ için $a \cdot b = b \cdot a = e$ olacak şekilde bir $b \in G$ vardır (ters eleman özelliği). Burada (iii)'deki e elemanına grubun birim (etkisiz) elemanı denir. Ayrıca (iv)'deki b elemanına a nın tersi denir ve $b = a^{-1}$ ile gösterilir.

Bu dört şarta ilave olarak eğer;

(v) Her $a,b \in G$ için $a \cdot b = b \cdot a$ ise (değişme özelliği) varsa bu gruba *abelyan* (*değişmeli*) *grup* denir.

Tanım 1.1.4. G bir grup ve H de G'nin boş olmayan bir alt kümesi olsun. Eğer H kümesi G'de tanımlanan grup işlemi ile bir grup oluyorsa H ye G'nin bir *alt grubu* denir ve $H \leq G$ ile gösterilir.

Tanım 1.1.5. Bir G grubunun elemanlarının sayısına G'nin *mertebesi* denir ve $|G|$ ile gösterilir.

G bir grup, $a \in G$ olsun. $a^n = e$ olacak şekilde bir en küçük pozitif n doğal sayısı varsa bu sayıya a nın *mertebesi* denir ve $|a|$ ile gösterilir. Böyle bir n sayısı yoksa $|a| = \infty$ yazılır.

Tanım 1.1.6. G bir grup, $a \in G$ olsun. $< a > = \{a^n : n \in \mathbb{Z}\}$ kümesine a tarafından *üretilen grup* denir (toplamsal notasyonda $< a > = \{na : n \in \mathbb{Z}\}$). a elemanına $< a >$ grubunun *üretici elemanı* denir. Eğer $G = < a >$ olacak şekilde bir $a \in G$ elemanı varsa G'ye *devirli grup* denir.

Tanım 1.1.7. $(G, .)$ ve $(H, *)$ iki grup ve $f : G \to H$ bir fonksiyon olsun. Eğer f fonksiyonu grup işlemini koruyorsa yani $\forall\, a,b \in G$ için $f(a \cdot b) = f(a) * f(b)$ oluyorsa f'ye *bir grup homomorfizması* veya kısaca *homomorfizma* denir.

Tanım 1.1.8. $f: G \to H$ grup homomorfizması birebir ve örten ise f ye bir *izomorfizma* G ile H gruplarına *izomorfiktirler* veya *eş yapılıdırlar* denir ve $G \cong H$ şeklinde gösterilir.

Tanım 1.1.9. Bir G grubundan kendi üzerine olan bir izomorfizmaya G'nin bir *otomorfizması* denir.

G'nin bir $a \in G$ ve $\forall x \in G$ elemanı için $f_a: G \to G$, $f_a(x) = axa^{-1}$ şeklinde tanımlanan f_a dönüşümü her zaman bir otomorfizmadır. Bu tür bir otomorfizmaya G'nin bir *iç otomorfizması* denir ve G'nin iç otomorfizmalarının kümesi $Inn(G)$ ile gösterilir. G'nin bütün otomorfizmalarının kümesine G'nin *otomorfizmalar grubu* denir ve $Aut(G)$ ile gösterilir.

$$Aut(G) = \{ f: G \to G \mid f, \text{ otomorfizma} \}.$$

Tanım 1.1.10. $a \in \mathbb{Z}_n$ olsun. a'nın mod n'e göre çarpımsal tersi $ax \equiv 1 \pmod{n}$ olacak şekilde $x \in \mathbb{Z}_n$ tamsayısıdır. Eğer böyle bir x tamsayısı mevcutsa tektir ve a'ya *tersinirdir* denir. a'nın tersi a^{-1} ile gösterilir.

Tanım 1.1.11. $\mathbb{Z}_n$'in *çarpımsal grubu* $\mathbb{Z}_n^* = \{ a \in \mathbb{Z}_n : (a, n)=1 \}$ dir. Özel olarak n asal ise $\mathbb{Z}_n^* = \{ a : 1 \le a \le n-1 \}$ dir.

Tanım 1.1.12. $n \ge 1$ olmak üzere n'yi geçmeyen ve n ile aralarında asal olan pozitif tamsayıların sayısını veren fonksiyona *Eulerin* ϕ *fonksiyonu* denir ve $\phi(n)$ ile gösterilir.

Teorem 1.1.1 (Euler Teoremi) $n \ge 2$ olacak şekilde bir tamsayı olsun. $(a,n)=1$ ise $a^{\phi(n)} \equiv 1 \pmod{n}$ dir.

Tanım 1.1.13. ***DLP* (Discrete Logaritma Problemi)** G, n. mertebeden bir devirli grup olsun. α, G'nin bir üreteci ve $\beta \in G$ olsun. $0 \le x \le n-2$ olmak üzere $\alpha^x = \beta$ olacak şekildeki bir tek x tamsayısına α tabanına göre β'nın *discrete* (*ayrık*) *logaritması* denir ve $log_\alpha \beta$ ile gösterilir. Discrete Logaritma Problemi (*DLP*); bir p asalı, $\mathbb{Z}_p^*$'ın α

üreteci ve $\beta \in \mathbb{Z}_p^*$ verildiğinde $\alpha^x \equiv \beta \pmod{p}$ olacak şekilde $0 \le x \le p-2$ tamsayısını bulma problemidir.

Tanım 1.1.14. (Konjugasyon) G bir grup ve $x,y \in G$ için $y = gxg^{-1}$ olacak şekilde bir $g \in G$ varsa x ve y elemanlarına *konjugedir* (*eşleniktir*) denir.

Tanım 1.1.15. *CP* (Konjugasyon Problemi) G bir grup ve $x,y \in G$ için $y = gxg^{-1}$ olacak şekilde bir $g \in G$ bulma problemine *Konjugasyon Problemi* denir.

Tanım 1.1.16. (Koset) G bir grup, $H \le G$ ve $x \in G$ olsun. $xH = \{xh \mid h \in H\}$ ve $Hx = \{hx \mid h \in H\}$ kümelerine sırasıyla, H'nın G deki *sol koseti* ve H'nın G deki *sağ koseti* denir. H'nın G deki tüm sol kosetlerinin cümlesi G/H ile, tüm sağ kosetlerinin cümlesi de $H\backslash G$ ile gösterilir.

Tanım 1.1.17. (**İndeks**) G bir grup ve $H \le G$ olsun. H'ın G deki sol (sağ) kosetlerin sayısına H'ın G deki *indeksi* denir. H' ın G deki indeksi $[G:H]$ ile gösterilir.

Tanım 1.1.18. (Halka) R boştan farklı bir cümle olsun. R üzerinde '+' ve '.' gibi iki tane işlem tanımlansın. (R, + , .) üçlüsü eğer

a) (R , +) bir abelyan grup

b) (R , .) bir yarı grup

c) **(i)** ikinci işlemin birinci işleme soldan dağılma

(ii) ikinci işlemin birinci işleme sağdan dağılma

şartları sağlanıyorsa R'ye bir *Halka* denir. Eğer çarpma işlemine göre birim eleman varsa R'ye *Birimli Halka*, çarpma işlemine göre değişme özelliği varsa *Değişmeli Halka* denir.

Tanım 1.1.19. (Cisim) F birimli ve değişmeli halka olsun. Eğer F deki sıfırdan farklı her elemanın çarpma işlemine göre bir tersi varsa bu takdirde F'ye bir *Cisim* denir.

Tanım 1.1.20. K bir cisim olmak üzere $GL(n,K) = \{ A \in M(n \times n, K) \,|\, \det(A) \neq 0 \}$ cümlesi matrislerde 'toplama' işlemine göre bir gruptur. Bu gruba *genel lineer grup* denir.

Özel olarak $\det(A) = 1$ ise $SL(n,K) = \{ A \in M(n \times n, K) \,|\, \det(A) = 1 \}$ grubuna öz*el lineer grup* denir.

Tanım 1.1.21. G bir grup olsun. $C(G) = \{ x \in G \mid x.y = y.x$, her $y \in G \}$ cümlesine *G'nin merkezi* denir.

Tanım 1.1.22. Çarpanlara ayırma problemine *Faktorizasyon Problemi* adı verilir.

1.2. Kriptolojide Kullanılan Bazı Terimler

Tanım 1.2.1. (Açık Anahtar) Açık anahtarlı kriptografide anahtara herkes tarafından erişilebilir. Sadece eşi olan özel anahtara sahip kişi tarafından açılması istenen verileri şifrelemek için ya da özel anahtar sahibi tarafından şifrelenmiş verileri çözmek için kullanılır. Bir açık anahtar sistemi sadece mesajın şifrelenmesinde kullanılır.

Tanım 1.2.2. (Açık Anahtarlı Algoritmalar) Şifrelemenin ve deşifrelemenin farklı anahtarlar yardımıyla yapıldığı kriptografik algoritmalardır. Deşifreleme anahtarının şifreleme anahtarından elde edilemediği algoritmalardır. Açık anahtar ve onun eşi olan özel anahtar beraber bir anahtar çifti oluşturur. Çift anahtarlı kriptografi (double key cryptography) veya asimetrik algoritmalar da denir. RSA , El-Gamal gibi şifreleme algoritmaları ve Diffie-Hellman anahtar değişim algoritması en çok bilinenleridir.

Tanım 1.2.3. (Açık Metin) Metinlerin şifrelenmemiş, normal, okunabilir hallerine Açık Metin (Plaintext) veya Düz metin denir.

Tanım 1.2.4. (Alıcı, Gönderici) Haberleşmede bilgiyi alan kişiye Alıcı (receiver) denir. Bir haberleşmede bilgiyi meşru olarak gönderen kişiye Gönderici (Sender) denir. Bu çalışmada alıcı B ile gönderici A ile gösterilmiştir.

Tanım 1.2.5. (Anahtar) Verileri şifrelemek veya deşifrelemek için kullanılan algoritmanın bilinmeyen kısmını oluşturan parçasına Anahtar(Key) denir.

Tanım 1.2.6. (Kanal) Bilginin bir kullanıcıdan diğerine iletimi için gereken fiziksel iletişim ortamıdır. Örneğin bilgisayar bağlantısı, telefon kablosu, radyolink ve uydu üzerinden diğer kullanıcıya ulaşan bağlantının tümü.

Tanım 1.2.7. (Kimlik Belirleme) Herhangi bir servisi almak isteyen birinin, gerçekten de kendi iddia ettiği kişi olduğunun belirlenmesine Kimlik Belirleme (Authentication) adı verilir.

Tanım 1.2.8. (Kod)

a) Bilginin kısaltılarak kayıt edildiği ya da tanımlandığı karakter dizisi.

b) Bilgisayarın tanıyacağı formda özel semboller kullanılarak bilginin gösterilmesi ya da tanımlanması.

Tanım 1.2.9. (Kriptanaliz) Bir kriptografik sistemin girdi veya çıktılarını inceleyerek, bilgi ve anahtar olmaksızın orijinal verilere ulaşmayı amaçlayan analize Kriptanaliz (Cryptanalysis) denir. Aynı zamanda kod kırma (codbreaking) olarak da adlandırılır. Ayrıca Kriptanalizin uygulamacılarına Kriptanalist denir.

Tanım 1.2.10. (Kriptografi) Kodunu yalnız alıcısının açabileceği şekilde düzenlenen, mesajların içeriğini gizleme ve mesajı tekrar eski orijinal haline geri dönüştürme prensipleri ve yöntemlerini içeren gizli dönüşümler bilimine Kriptografi (Cryptography) denir.

Tanım 1.2.11. (Kriptografik Algoritma) Şifreleme ve deşifreleme işlemlerinde kullanılan matematiksel işlemlerin bütünüdür.

Tanım 1.2.12. (Kriptoloji) Çözülebilmesi çok zor matematik problemlerini inceleyen kriptografi (cryptography) ile bu problemleri çözmeyi hedefleyen ve saldırıları belirleyen kriptoanalizi (cryptanalysis) içeren bilim dalına Kriptoloji (Cryptology) denir. (kriptoloji = kriptografi + kriptanaliz).

Tanım 1.2.13. (Özel-Gizli-Kişisel Anahtar) Açık anahtarlı kriptografide sadece sahibi tarafından bilinmesi gereken, kullanıcının kendisine ait olan iki anahtarından gizli tutulan anahtara Özel-Gizli-Kişisel Anahtar (Private Key) adı verilir. Karşılık gelen açık anahtarla şifrelenmiş verileri çözmek veya veri imzalamak için kullanılır. Sistemin

güvenlik açısından dayanak noktası özel anahtarın sahibi dışında kullanılmamasıdır. Bu yüzden, özel anahtarın korunması gereklidir.

Tanım 1.2.14. (Saldırgan, Saldırı) Taraflar arasındaki haberleşmede mesajı alan veya gönderen kişi olmayıp güvenliği kırmaya çalışan zararlı kimseye Saldırgan (Adversary) denir. Bir kriptosistemin bir kısmını veya tamamını kırmak için yapılan başarılı veya başarısız teşebbüslere Saldırı (attack) adı verilir.

Tanım 1.2.15. (İmza Doğrulama) Elektronik ortamdaki yazışmalara eklenen, yazıyı gönderenin kimliğini ve gönderilen yazının iletim sırasında bozulmadığını kanıtlamaya yarayan bölümüne İmza Doğrulama (Signature Schema) adı verilir. Sayısal imza, yazının içeriğine ve imzalayanın gizli anahtarına bağlı bir kriptografik yöntemle atıldığı için, sayısal imzanın doğrulanmasında, imzayı atanın açık anahtarı kullanılır.

Tanım 1.2.16. (Simetrik Algoritmalar) Şifreleme ve deşifreleme işlemlerinde aynı anahtarın kullanıldığı algoritmalardır. Tek anahtarlı kriptografi veya gizli anahtarlı algoritmalar da denir.

Tanım 1.2.17. (Şifreleme) Açık metni anlaşılmaz hale getirme, şifreli metne dönüştürme işlemine Şifreleme (Encryption) denir. Amaç; veriyi, gerekli anahtar olmadan çözülebilmesi imkânsıza mümkün olduğunca yakın şekilde kodlamaktır.

Tanım 1.2.18. (Şifre Çözme) Şifrelenmiş veriyi çözüp eski haline getirme işlemine Şifre Çözme (Decryption) adı verilir.

Tanım 1.2.19. (Şifre Kırma) Kullanılan şifreleri öğrenmek amacıyla yapılan işleme Şifre Kırma (Crack) adı verilir. Genellikle art niyetli kişilerce, çıkar amaçlı uygulandığı için yasadışı olarak kabul edilmektedir.

Tanım 1.2.20. (Şifreli Metin) Metinlerin şifrelenerek anlaşılamaz hale getirilmiş biçimlerine Şifreli Metin (Ciphertext) denir.

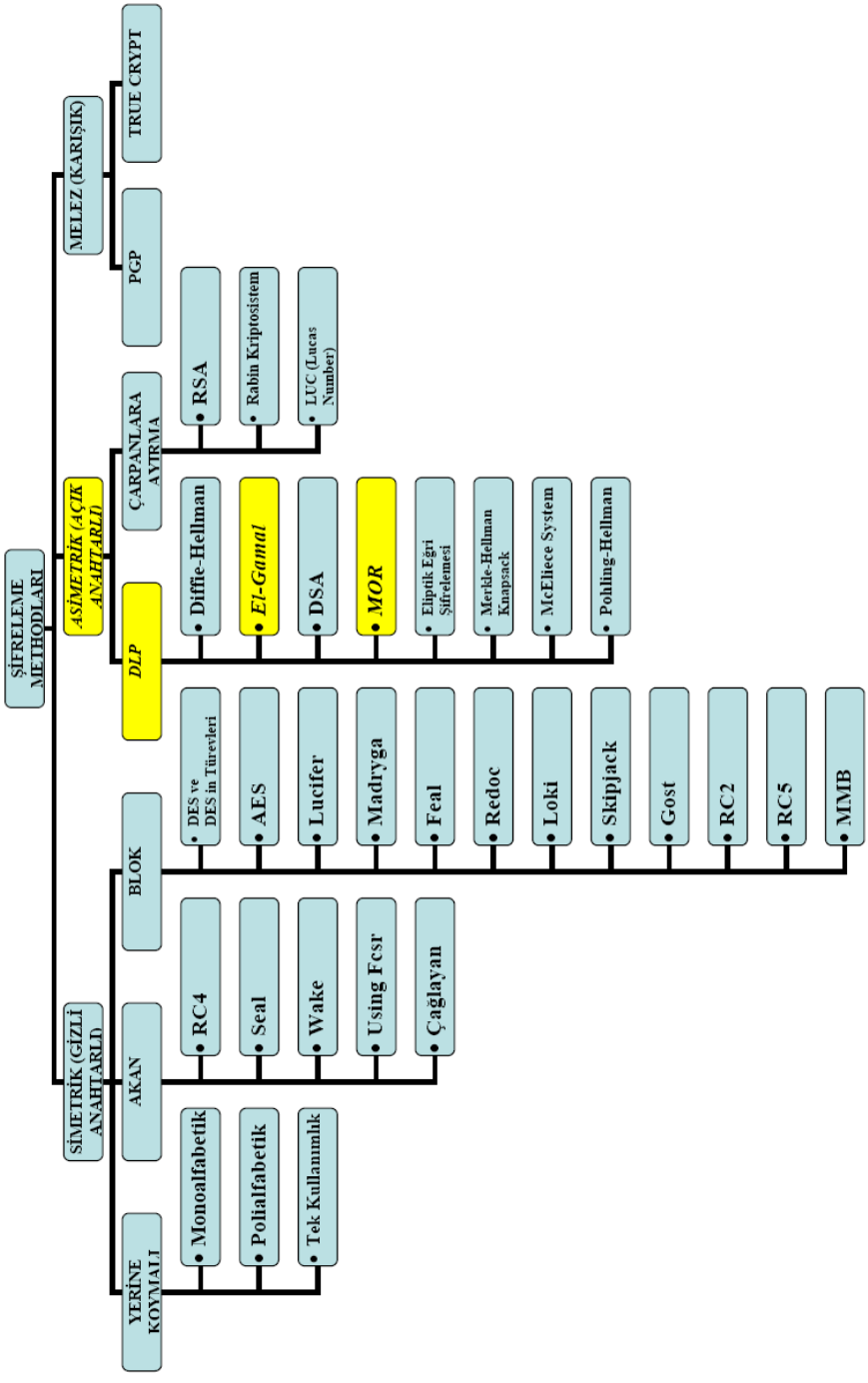
Tanım 1.2.21. (Veri Bütünlüğü) Bilginin göndericiden alıcıya gitmesi esnasında yanlışlıkla ya da bilerek değiştirilmesinin önlenmesine Veri Bütünlüğü (Data Integrity) denir.

Kriptografideki temel bazı kavramlar verildi. Şimdi ise şifreleme metotlarından bahsedilebilinir.

1.3. Şifreleme Metodları

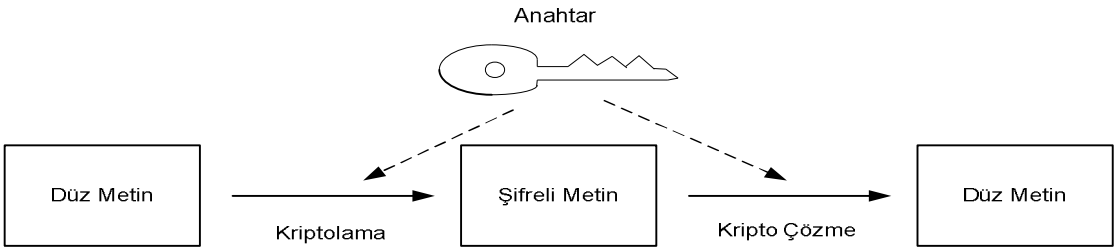
Şifreleme metodları simetrik (gizli anahtarlı), asimetrik (açık anahtarlı) ve karışık (melez) şifrelemeler olmak üzere üç ana başlık altında toplanabilir. Bunlar

Tablo 1.1. Şifreleme çeşitleri



Bu tezde incelenecek olan sistem bir açık anahtarlı kriptosistem çeşididir. Neden açık anahtarlı sistem kullanılıyor? Açık anahtarlı kriptosistem ile gizli anahtarlı kriptosistemin farkı ne? Bunlara açıklık getirilmeye çalışılmıştır.

1.3.1. Gizli Anahtarlı (Simetrik) Kriptosistemler



Şekil 1.1. Simetrik (gizli) anahtar şifrelemesi

Bu tür şifrelemelerde, şifreleme ve deşifreleme işlemleri için aynı anahtar kullanılır. Simetrik anahtar şifrelemede; şifreleme anahtarından deşifreleme, deşifreleme anahtarından da şifreleme anahtarı hesaplanabilir. Çoğu simetrik şifrelemelerde ise şifreleme ve deşifreleme anahtarları aynıdır ve gönderici ile alıcının iletişime başlamadan önce ortak bir anahtar üzerinde anlaşmaları gerekir.

Simetrik şifrelemelerin güvenliği anahtarın gizli kalmasına bağlıdır. Anahtarın açığa çıkması durumunda herkes mesajları şifreleyip deşifreleyebileceğinden iletişimin gizliliği ortadan kalkar.

Bu algoritmaların avantajı basit ve kolay uygulanabilirliği, hızlı ve verimli olmalarıdır. Ancak bu algoritmaların en zayıf tarafı ise şifreleme ve deşifreleme için aynı anahtarın kullanılıyor olmasıdır. Tek bir anahtarın güvenliğini nasıl sağlanabilir? Diğer alıcılara bu anahtar güvenli bir şekilde nasıl gönderilebilir? Diğer alıcıların anahtarı gizli tutacağından nasıl emin olunabilinir? Dolayısıyla bu algoritmaların kullanılması paylaşımın olmadığı durumlarda daha uygundur. Bu algoritmalar bilgisayarlardaki dosyaların veya sabit disklerin şifrelenmesi gerektiğinde rahatlıkla kullanılabilir.

Gizli anahtarlı şifreleme yöntemine örnek olması açısından bu yöntemlerinden birisi olan Ceasar şifreleme metoduna bir örnek aşağıda yapılmıştır.

Örnek 1.3.1.1.

Bu tür şifrelemelerde açık metindeki her bir harf veya sembol başka bir harf veya sembole dönüştürülerek şifre metin elde edilir. Bu yapılırken de hangi dilde mesaj gönderilecekse o dilin standart alfabesi kullanılır ve her bir harf bir sayıya dönüştürülür. Türk Alfabesi kullanılarak aşağıdaki tablo oluşturulur.

Tablo 1.2. Türk alfabesinin sayısal değerleri

Harf	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O
Sayı	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17

Harf	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z
Sayı	18	19	20	21	22	23	24	25	26	27	28

Ceasar alfabedeki her bir harfi kendinden üç sonra gelen harfle değiştirerek şifre metnini elde etmiştir. Yani Ceasar şifreleme metodu için : $E \equiv M + 3(29)$, $0 \le E \le 28$ bağıntısı kurulabilir. Buradaki M açık metindeki her bir harfin sayısal karşılığı, E ise şifre metinde bu harflere karşılık karşılık gelen sayısal değerlerdir. Bu karşılık getirme aşağıdaki tablo ile verilmiştir.

Tablo 1.3. Ceasar şifreleme metodunda harflere karşılık gelen sayısal değerler

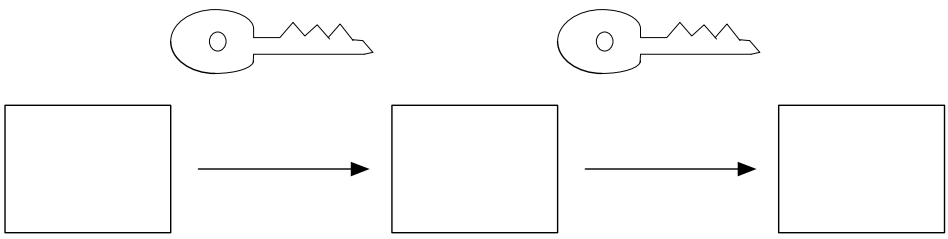
Açık Metin,M	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Şifre Metin,E	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R

Açık Metin,M	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z
	18	19	20	21	22	23	24	25	26	27	28
Şifre Metin,E	21	22	23	24	25	26	27	28	0	1	2
	S	Ş	T	U	Ü	V	Y	Z	A	B	C

Ceasar şifrelemesi ile **'' SALDIRI BAŞLADI ''** metni şifrelenirse tablodan harflere karşılık gelen sayısal değerler 21 0 14 4 10 20 10 1 0 22 14 0 4 10 olup her biri için $E \equiv M + 3(29)$, $0 \le E \le 28$ bağıntısı kullanılırsa 24 3 17 7 13 23 13 4 3 25 17 3 7 13 rakamları elde edilir. Bu rakamlar tekrar harfe dönüştürülürse **''UÇOGKTK DÇÜOÇGK''** şifre metni ortaya çıkar. Alıcı bu mesajı deşifre ederken önce harfleri sayısal eşitliklerine çevirir. Daha sonra da $E \equiv M - 3(29)$, $0 \le M \le 28$ bağıntısı ile açık metin bulunur.

1.3.2. Açık Anahtarlı (Asimetrik) Kriptosistemler

Simetrik şifrelemelerin tarihi binlerce yıllık geçmişe sahip olmasına rağmen asimetrik şifrelemelerin uzun bir geçmişe sahip olduğu söylenemez. Simetrik kriptografideki anahtar dağıtım problemi, asimetrik şifreleme ile çözülmüştür. Simetrik şifrelemede gizli anahtarın herhangi bir yolla karşı tarafa ulaştırılması gerekirken asimetrik şifrelemelerde gizli anahtarın hiçbir şekilde karşı tarafa gönderilmesi gerekmez. Asimetrik şifrelemelerde açık anahtar ve özel anahtar olmak üzere iki farklı anahtar kullanılır. Şifreleme için açık anahtar kullanılırken, şifre metni çözmek için özel anahtar kullanılır. Açık anahtarın gizli tutulmasına gerek yokken özel anahtarın kesinlikle gizli tutulması gerekmektedir ve özel anahtarın saklanması sahibinin kendi sorumluluğu altındadır. Açık anahtara sahip kişi bilgileri şifreleyebilir ancak şifre metni deşifre edemez.



Şekil 1.2. Asimetrik (açık anahtar) şifreleme

Asimetrik şifrelemelerde gönderici, alıcının açık anahtarını elde eder ve bu anahtarı kullanarak mesajı şifreler. Şifrelenen bu mesajın açık anahtar ile deşifresi mümkün değildir. Şifreli metin alıcıya ulaştığında alıcı, kendi özel anahtarını kullanarak şifreli metni çözebilir.

Açık anahtarlı şifrelemelerin en temel amacı, önceden güvenlik anlaşmasına sahip olmayan taraflar arasında da mesajların güvenli olarak alışverişini sağlayabilmektir. Bu şifrelemelerde gizli anahtarın hiçbir şekilde karşı tarafa gönderilmesi gerekmediğinden oldukça yüksek güvenlik sunmaktadır. Asimetrik şifrelemelerin bir diğer avantajı ise inkâr edilemeyecek dijital imzalar sağlayabilmesidir.

Açık anahtar kriptografisi Whitfield Diffie ve Martin Hellman'ın 1976'da buldukları anahtar paylaşım protokolüyle doğmuştur. İki sene sonra tarihin ilk açık anahtarlı şifreleme algoritması RSA; Rivest, Shamir ve Adleman tarafından tasarlanmıştır. DSA (Digital Signature Algorithm), Merkle-Hellman(Knapsack), El-Gamal, Eliptik Eğri Algoritması (ECC), Diffie-Hellman Anahtar Anlaşması ve MOR Kriptosistemi asimetrik şifrelemeye örnek olarak verilebilir.

Burada açık anahtarlı şifreleme metotlarından RSA ve 2. bölümde incelenen metoda çok yakın olan EL-GAMAL tipi şifreleme metodları incelenmiştir.

1.3.2.1. RSA Algoritması

RSA, 1978 yılında "Dijital imza elde etme metodu ve açık anahtarlı kriptosistemler" adlı bir makale ile yayınlandı. Adını Ronald Rivest, Adi Shamir, Leonard Adleman'ın soyadlarının baş harflerinden alan RSA, göndericinin bir metodla ve herkes tarafından bilinen açık bir anahtarla mesajlarını şifrelediği bir şifre sistemi olarak tanımlanır. Daha önceki simetrik anahtarlı sistemlerin tersine anahtarı bilmek deşifre anahtarını ortaya çıkarmaz. RSA algoritması, asimetrik şifrelemenin ve elektronik imzanın temelini oluşturan uygulamalardan birisidir. Bu sistemin güvenliği tamsayılarda çarpanlara ayırma probleminin zorluğuna dayanmaktadır.

RSA kriptosisteminde kişilere şifreli mesaj gönderilebilmesi için o kişilerin açık anahtarlarına ihtiyaç vardır. Mesajı alan kişinin de mesajı okuyabilmesi için gizli bir anahtarının olması gerekir. RSA kullanılarak anahtar çifti üretme, şifreleme ve deşifreleme aşamaları aşağıda verilmiştir:

1.3.2.1.1. Anahtar Oluşturma Algoritması

Her A kişisi anahtarını şu şekilde oluşturur:

a) İki tane farklı rastgele ve yaklaşık aynı uzunlukta olan p ve q asal sayılarını seçer.

b) $n = p.q$ ve $\Phi(n) = (p\text{-}1).(q\text{-}1)$ değerini hesaplar.

c) $2 < e < \Phi(n)$ ve $(\Phi(n), e)=1$ olacak şekilde bir e tamsayısı seçer,

d) $e.d \equiv 1 \pmod{\Phi(n)}$ sağlayacak şekilde ve $1 < d < \Phi(n)$ aralığında d değeri hesaplar.

e) A'nın açık anahtarı (n, e) ve özel anahtarı d'dir.

1.3.2.1.2. Şifreleme Algoritması

B şahsı, A'ya bir m mesajını göndermek istiyor. B, m mesajını şifrelemek için şunları yapar:

a) Öncelikle A'nın açık anahtarı (n,e)'yi alır.

b) m mesajını $[0 , n\text{-}1]$ aralığında yazar.

c) Sonra $E \equiv m^e \pmod{n}$ değerini hesaplar.

d) Oluşan E şifresini A'ya gönderir.

1.3.2.1.3. Deşifreleme Algoritması

A şahsı d gizli anahtarını kullanarak ve $m \equiv E^d \pmod{n}$ işlemini uygulayarak m açık metnine ulaşır.

RSA anahtar oluşumunda e ve d tamsayıları sırasıyla şifreleme üssünü ve deşifreleme üssünü ve n ise mod sayısını gösterir. RSA'yı günümüz teknolojisinde güvenli biçimde kullanabilmek için p ve q asalları en az 512 bitten oluşmalıdır. Böylece iki asalın çarpımı ''n'' 1024 bit olur. Günümüz bilgisayarlarıyla 1024 bitlik bir sayının çarpanlarına ayrılıp asal çarpanlarının bulunması ise yıllar sürecek bir işlem süresi gerektirir. Burada verilecek örneklerde kolaylık açısından küçük sayılar seçilmiştir.

Örnek 1.3.2.1.1.

''MESAJI ŞİFRELE''

cümlesi RSA algoritması ile şifrelensin.

$$p = 43,\ q = 59$$

olmak üzere n=43.59 için $\Phi(n)=(p\text{-}1).(q\text{-}1)$=2436 olur. e için $2 < e < \Phi(n)$ olup e=13 olsun.

$$(n,e)=(2537,13)$$

olur. Mesaj ikili bloklara ayrılıp sayısal değerleri bulunsun. Burada E şifreli metni ve m de şifrelenecek her bir bloğu temsil etmek üzere;

ME SA JI Şİ FR EL EA

(Sondaki A harfi son bloğu tamamlamak için keyfi seçilmiştir) şeklinde sayısal karşılıkları yazılır.

1505 2100 1210 2211 0620 1514 0500

Her bir m bloğunu şifrelemek için $m^{13} \equiv E \ (mod\ 2537)$ bağıntısı kullanılarak birinci blok

$$1505^{13} \equiv 1075 \ (mod\ 2537)$$

olur. Diğer bloklar için de aynı işlem tekrar edilirse

1075 0466 0780 0029 0072 0752 2330

şifre metnini elde edilir.

Deşifrelemede kullanılacak olan d yi bulmada kullanılacak mod ise $mod(\ \Phi(43.59)\ ) = mod(42.58\ ) = mod(\ 2436\ )$ olarak bulunur. e=13 ün tersi Öklid algoritması kullanılarak $e^{-1} = d = 937$ olarak bulunur.

$$E^{937} \equiv m \ (\text{mod}\ 2537\ )$$

kullanılarak her bir blok deşifre edilir.

$$1075^{937} \equiv 1505 \ (\text{mod}\ 2537\ )$$

olup diğer bloklar için de aynı işlemler uygulanırsa açık metin:

1505 2100 1210 2211 0620 1514 0500

olarak bulunur.

RSA algoritmasına yapılan saldırılardan en önemlisi, elde edilen açık anahtar kullanılarak gizli anahtara ulaşılmaya çalışılmasıdır. Saldırgan, n sayısının çarpanları olan p ve q değerlerini hesaplamaya çalışır. Eğer bu değerler hesaplanabilirse özel

anahtara ulaşılabilir. Burada en zor kısım n sayısını çarpanlarına ayırma işlemidir. Ancak n değerinin yeterince büyük seçilmemesi veya (p, q) çiftinin ve e değerinin iyi seçilememesi durumunda RSA'nın güvenli olduğu söylenemez.

1.3.2.2. El-Gamal Kriptosistemi

El-Gamal açık anahtarlı şifre sistemi, anahtar transferi modunda Diffie-Hellman anahtar anlaşması (Diffie-Hellman Key Agreement) olarak görülebilir. Güvenilirliği ayrık logaritma problemi ve Diffie-Helman probleminin kolay çözülememesine dayanır. 1985 yılında Mısırlı bir matematikçi olan Taher EL-GAMAL tarafından önerilmiştir. Bu sistem ise yine açık anahtarlı kriptosistem olmakla beraber RSA dan farklı olarak ayrık logaritma probleminin (DLP) zorluğuna dayanmaktadır.

1.3.2.2.1. Anahtar Oluşturma Algoritması

Her kişi kendi açık anahtarını ve buna bağlı gizli anahtarını oluşturur. Bunu oluşturmak için *B* şahsı şunları uygular:

a) Çok büyük rastgele bir p asal sayısı ve *mod p* ye göre tamsayıların oluşturduğu çarpım grubu Z_p^* nin bir üreteci β 'yı seçer.

b) $1 \leq a \leq p$-2 şeklinde olan bir a tamsayısı seçer ve $\beta^a \, mod \, p$ değerini hesaplar.

c) *B*'nin açık anahtarı (p, β , β^a) ve *B*'nin gizli anahtarı ise a olur.

1.3.2.2.2. Şifreleme Algoritması

A şahsı *B* için *m* mesajını şifrelemek istesin. *A* mesajı şifreleme için şunları yapar:

a) *B*'nin açık anahtarını (p, β , β^a) alır.

b) Mesajı { 0,1,…, p-1 } aralığında m tamsayısı olarak ifade eder.

c) $1 \leq k \leq p$-2 'yi sağlayan rastgele bir k tamsayısı seçer.

d) $\gamma = \beta^k$ ve $\delta = m.(\beta^a)^k$ değerlerini *modp* ye göre hesaplar.

e) Son olarak $E = (\gamma, \delta)$ kapalı metnini *B*'ye gönderir.

1.3.2.2.3. Deşifreleme Algoritması

E kapalı metninden m açık metine ulaşmak için *B* şunları yapar:

a) a gizli anahtarıyla $\gamma^{p-1-a} = \beta^{p-1-ak}$'*yi* kullanarak γ^{-a} değerini *mod p* ye göre hesaplar. ($\gamma^{p-1-a} = \gamma^{-a} = \beta^{-ak}$) olur.

b) $\gamma^{-a}.\delta$ *mod p* değerini hesaplayarak *m*'yi bulur.

$$\gamma^{-a}.\delta \equiv \beta^{-ak}.m.\ \beta^{ak} \equiv m \quad (\ mod\ p\ )$$

Örnek 1.3.2.2.1.

Anahtar Oluşturma

B şahsı bir $p = 2357$ asal sayısı ve $\beta = 2 \in \mathbb{Z}^*_{2357}$ bir üretecini seçer. Buna ilave olarak gizli anahtar ($a = 1751$) seçer ve

$$\beta^a = 2^{1751} \equiv 1185\ (2357)$$

değerini hesaplar. *B*'nin açık anahtarı (p , β , β^a) = *(2357 ,2, 1185)* olur.

Şifreleme

m = 2035 mesajını şifrelemek için *A* şahsı rastgele bir k=1520 tamsayısı seçer ve

$$\gamma = 2^{1520} \equiv 1430\ (2357)$$

$$\delta = 2035.1185^{1520} \equiv 697\ (2357)$$

değerlerini hesaplar. Son olarak *A* şahsı E= (γ , δ) = *(1430, 697)*'yi *B*şahsına gönderir.

Deşifreleme

B gelen kapalı metni çözmek için

$$\gamma^{p-1-a} = 1430^{-1751} \equiv 1430^{605} \equiv 872\ (2357)$$

işlemiyle γ^{-a} yı bulur ve m mesajına da

$$m = 872.697 \equiv 2035\ (2357)$$ işlemiyle ulaşır.

Örnek 1.3.2.2.2.

Asal 3 basamaklı en büyük asal olan 997 olarak alınsın.

Anahtar Oluşturma

p =997 asalı seçilsin

α =7 üretecini seçilsin

a =8 gizli anahtarını seçilsin

$\alpha^a = 7^8 \equiv 147(997)$

$(p,\ \alpha\ ,\alpha^a)$ karşı tarafa yollanır.

Şifreleme

M=GÜNEŞ=72516522 (0) mesajı şifrelenirse

*Asal 3 basamaklı alındığı için 3 basamak şeklinde ayrıldı.

725.165.220.

önce 725 için yapılırsa

k=11 rastgele sayısı olmak üzere

$\gamma = \alpha^k = 7^{11} \equiv 571(997)$ i hesaplanır

$\delta = m.\alpha^{a.k} = 725.147^{11} \equiv 638(997)$

$(\gamma, \delta) = (571, 638)$ şeklinde karşı tarafa yollanır.

Deşifreleme

$\gamma^{-a} = 571^{-8} \equiv x(997) \Rightarrow 571^8 x \equiv 1(997) \Rightarrow 958x \equiv 1(997)$

$\Rightarrow x \equiv 409(997)$

Yani $\gamma^{-a} = 571^{-8} \equiv 409(997)$ dir.

M= $\gamma^{-a}\delta = 409.638(997) \equiv 725(997)$

olup mesaj 725=GÜ değerine ulaşır.

Aynı şey 165 için yapılırsa

Şifreleme

$\delta = m.\alpha^{a.k} = 165.147^{11} = 165.958(997) \equiv 544(997)$

B=$(\gamma = 571, \delta = 544)$ ü karşı tarafa yollanır.

$\gamma^{-a} = 571^{-8} \equiv 409(997)$

Deşifreleme

$m = \gamma^{-a}.\delta = 409.544 \equiv 222496 \equiv 165(997)$

olup 165=NE de elde edilmiş oldu.

Aynı şey 22 için yapılırsa

Şifreleme:

$\delta = m.\alpha^{a.k} = 22.147^{11} = 22.958(997) \equiv 21076 \equiv 139(997)$

B=$(\gamma = 571, \delta = 139)$ u karşı tarafa yollanır.

Deşifreleme:

$\gamma^{-a} = 571^{-8} \equiv 409(997)$

$m = \gamma^{-a}.\delta = 409.139 \equiv 22(997)$ elde edilir 'GÜNEŞ' mesajı El-Gamal metodu ile şifrelenmiş sonra da tekrar deşifre edilmiş olur.

1.3.2.2.4. El-gamal Şifreleme Metodunda Güvenlik İçin Her Seferinde Kuvvet Değişmek Zorundadır

Taher El-Gamal, 1985 yılında El-Gamal şifreleme metodunu önerdiği makalesinde her seferinde kuvvetin değişmek zorunda olduğunu belirtiyor. İncelenen sistemde ise her seferinde kuvvet değişmek zorunda değildir. Bu ise daha hızlı şifreleme yapılmasını sağlıyor. Burada kuvvetin neden her seferinde değişmek zorunda olduğu açıklanmıştır.

El-Gamal makalesinde eğer k değişmezse

$C_{1,1} \equiv \alpha^k \pmod P \quad C_{2,1} \equiv M_1.K \pmod P$

$C_{1,2} \equiv \alpha^k \pmod P \quad C_{2,2} \equiv M_2.K \pmod P$ olup buradan $M_1 / M_2 \equiv C_{2,1} / C_{2,2} \pmod P$

olacağını belirtmektedir. Eğer M_1 biliniyorsa M_2 kolayca hesaplanabilir. Yani *k* nın değişme sebebi şayet M_1 biliniyorsa M_2 nin bulunmaması içindir. Şöyle ki

Örnek 1.3.2.2.2. de M=GÜNEŞ=7251522(0) i *p*=997 asalı α =7 üreteci *a* =8 gizli anahtarı ve *k*=11 rastgele sayısı seçilip şifrelenmişti. $\gamma_{1,1} = \alpha^k = 7^{11} \equiv 571(997)$ ve $\gamma_{1,2} = \alpha^k = 7^{11} \equiv 571(997)$ ve

$\delta_{1,2} = m_1.K = m_1.\alpha^{a.k} \equiv 725.958(997) \equiv 638(997)$

$\delta_{2,2} = m_2.K = m_2.\alpha^{a.k} \equiv 165.958(997) \equiv 544(997)$ olduğundan $\frac{638}{544} = \frac{m_1}{m_2}(997)$ olur.

Yani m_1 i bilen m_2 yi hemen elde edebilir. m_1 mesajı 725 idi. Dolayısıyla

$$\frac{638}{544} = \frac{725}{m_2}(997)$$

$\Rightarrow 725.544 \equiv 638 m_2(997)$ kogrüansı çözüldüğü zaman $m_2 \equiv 165(997)$ olarak bulunur. Gerçekten de m_1 mesajı = GÜ = 725 ve m_2 mesajı da NE = 165 idi. Dolayısıyla El-Gamal şifreleme metodunda *k* (şifreleyenin seçtiği rastgele üs) her seferinde değiştirilmelidir. Değiştirilmezse bir mesajı çözen diğer tüm mesajları çözer.

1.3.3. Açık anahtarlı ve Gizli anahtarlı şifreleme sistemlerin Karşılaştırılması

Açık anahtarlı ve Gizli anahtarlı şifreleme sistemleri, birbirlerini bütünleyen avantajlara sahiptirler. Günümüzde kullanılan kriptografi sistemleri genellikle her ikisinin de gücünden faydalanılarak yapılmaktadır. Bu sistemlerin bazı avantajlarını ve dezavantajlarını şöyle sıralayabiliriz:

1. Gizli anahtarlı şifrelemede anahtar uzunluğu, açık anahtarlı şifrelemeye göre daha kısadır.

2. Gizli anahtarlı şifrelemede, iki farklı taraf arasında gerçekleşen iletişim için anahtarı her iki tarafın da bilmesi ve gizli tutması zorunlu iken, açık anahtarlı şifrelemede tarafların sadece kendilerine ait özel anahtarı gizli tutmaları yeterlidir.

3. Gizli anahtarlı şifrelemelerde açık anahtarlı şifrelemelere göre çok hızlı şifreleme yapılır.

4. Gizli anahtarlı şifrelemede anahtarın güvenlik açısından sık sık değiştirilmesi gerekirken, açık anahtarlı şifrelemede genel-özel anahtar çiftinin uzun zaman değiştirilmesine gerek duyulmayabilir.

2. BÖLÜM

ABELYAN OLMAYAN GRUPLARLA ŞİFRELEME

Bu bölümde Braid grubunun ve Matris grubunun abelyan olmayışları, Yarı Direk Çarpım Metodu ve bu metod ile iki abelyan gruptan abelyan olmayan grupların nasıl elde edildiği gösterildi. Ayrıca incelenecek sistem için neden SL$(2, Z_p)$ ya da GL$(2, Z_p)$ gruplarını kullanılıp diğer abelyan olmayan grupların kullanılmadığı ve neden sonlu grup kullanılıp da sonsuz grup kullanılmadığı açıklandı. Daha sonra ise abelyan olmayan sonlu gruplar kullanılarak elde edilen açık anahtar kriptosistemin mantığı, birkaç özelliği, kırılmasının neden zor olduğu ve neden daha hızlı bir sistem olduğu örneklerle açıklandı. Bunun için genellikle, Paeng [3],[4], El-Gamal [5], Yamamura [6], Mahalanobis [8],[9] ve Stickel [10] kaynaklarından yararlanılmıştır.

2.1. Matris Grupları ve Abelyan Olmayışı

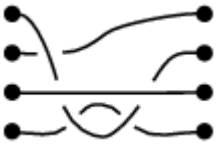
Bir K cisimi üzerinde tersinir matrisleri içeren, matrislerdeki çarpma işlemine göre olan gruba Matris Grupları denir. Matrislerde çarpma işlemi değişmeli değildir. Dolayısıyla Matris Grupları abelyan olmayan bir gruptur.

2.2. Braid Grubu ve Abelyan Olmayışı

Tanım 2.2.1. Bu tanımda *n=4* alındı. Bir masa üzerinde yatan dört noktalı iki küme düşünülsün. Her nokta dikey doğru üzerinde düzenlenmiş ve bir küme diğer kümenin karşısında bulunuyor (Aşağıdaki çizimlerde bunlar siyah noktalar).

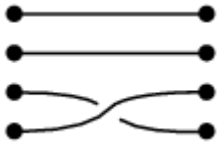
Dört ipliği kullanarak, ilk kümenin her noktası ikinci kümenin bir noktasına bağlanıyor. Böyle bir bağlantının ismi ‘Braid’ dir. Sık bazı iplikler diğerlerinin üstünden ya da altından geçerler. Aşağıdaki iki bağlantı farklı braidlerdir.

Diğer taraftan aşağıdaki iki bağlantı iplikleri çekerek aynı yapılabilir. Bunlar aynı braidler olarak düşünülür.

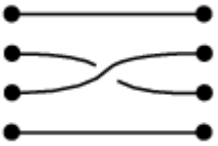


Bütün iplikler soldan sağa hareket etmeyi gerektirir. Şu durum ise braid değildir:

Herhangi iki braid şu şekilde işleme tabi tutulur:



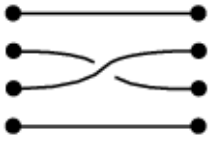
ile



şunu verir:

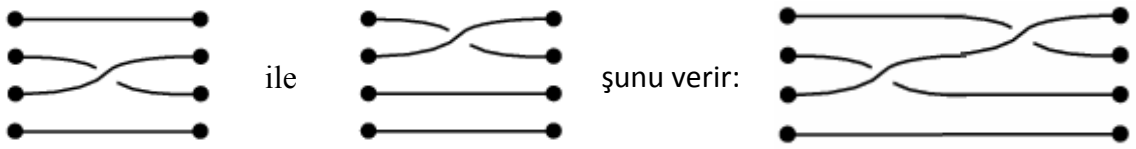
Matematikte n iplik üzerinde Braid Grup B_n ile ifade edilir. Eğer $n>1$ ise B_n sonsuz gruptur. Farklı iki Braid ile yapılan işlemin sonucu farklı iplikleri verir. Dolayısı ile Braid grubu aşağıda görüldüğü gibi abelyan değildir.

ile



şunu verir:

Fakat



Braid grubu abelyan olmayan sonsuz gruptur. Sonsuz grup olduğu için imza doğrulaması yapmak çok zordur. Dolayısıyla sonlu abelyan olmayan grup kullanmak daha avantajlıdır.

2.3. Yarı Direk Çarpım

Tanım 2.3.1 : H, K ve G boştan farklı gruplar olmak üzere aşağıdaki şartlar sağlanıyorsa H ile K nın yarı direk çarpımı G ye eşittir.

i- $G = H.K$ dır.

ii- $H \cap K = \{e\}$ dir.

iii- H veya K dan bir tanesi normal alt grup diğeri alt grup. (Ama ikisi normal alt grup değil.)

Örnek 2.3.1: $H = \{e,(12)\}$, $K = \{e,(123),(132)\}$ gruplarına yarı direk çarpım uygulanırsa $S_3 = \{e,(12),(13),(23),(123),(132)\}$ grubu elde edilir.

i- $H.K = e.e = e$, $e.(123) = (123)$, $e.(132) = (132)$, $(12).e = (12)$,
$(12).(123) = (1).(23) = (23)$, $(12).(132) = (13).(2) = (13)$ olup
$H.K = S_3 = \{e,(12),(13),(23),(123),(132)\}$ elde edilir.

ii- $H \cap K = \{e\}$ dir.

iii- $[S_3 : K] = [6:3] = 2$ olduğundan $K \lhd S_3$ tür. Ayrıca $H \leq S_3$ olduğundan yarı direk çarpımın tüm şartlarını sağlar. Dolayısıyla S_3 grubu H ve K gruplarının yarı direk çarpımı olarak elde edilmiş olur.

Burada *H* ve *K* grupları abelyan gruplar olmamalarına rağmen yarı direk çarpım sonucu elde edilen S_3 grubu abelyan olmayan bir gruptur.

Abelyan olmayan gruplar bu şekilde yarı direk çarpımla elde edilir. Yarı direk çarpımın sonucunun abelyan olması ancak iki grubun da abelyan olması ve işlemin birim dönüşüm olması ile mümkündür. Şifreleme sisteminde her abelyan olmayan grup kullanılmamaktadır çünkü

1- Çalışılan grubun mertebesinin büyük olması gerekiyor matris grubunun eleman sayısı çok ama S_3 grubunun sınırlı elemanı vardır.

2- Üzerinde çalışılan grubun *p*. mertebeden alt grubunun oluşabilmesi lazım ama S_3 grubunun *p*. mertebeden alt grubu oluşturulamaz.

3- Grubun üreteçler cinsinden ifadesi kolay olmalı ve seçilen elemanların kuvvetlerini almak kolay olmalı.

4- Eleman sayısı büyük olan ve rakam kullanılabilecek bir grup seçilirse şifreleme ve deşifreleme daha doğru ve güvenli yapılabilir. Matris grubu kullanılırsa K harfine 13 rakamı karşılık gelecek şekilde şifreleme yapılabilir ama S_3 grubu kullanılırsa K harfine grubun hiçbir elemanı karşılık gelmez.

İşte bu gibi sebeplerden dolayı her abelyan olmayan grup kullanılmıyor. Genellikle $\mathrm{SL}(2, Z_p)$ grubunu ya da $\mathrm{GL}(2, Z_p)$ grubu kullanılmaktadır.

2.4. Sistemin Algoritması

Diffie-Helmann'ın $< Inn(g) >$ üzerindeki anahtar anlaşmasına göre verici ve alıcı bir $Inn(g^{ab}) \in < Inn(g) >$ fonksiyonunda anlaşırlar. Bunun yanında *M*, *m* açık metninin kodlandığı matris olmak üzere, *M*'nin $Inn(g^{ab})$ altındaki görüntüsü $Inn(g^{ab})(M) = E$ (gizli metin) de Diffie-Helmann'ın anahtar değişimi anlaşmasına göre bulunur. Bir $M \in SL(2, \mathbb{Z}_p)$ mesajına ait gizli metin, $\phi = Inn(g)^b$ fonksiyonu ile deşifre edilir**.**

A **''** *M* **''** açık metnini şifreleyerek B'ye göndermek istesin. Burada A öncelikle şifreleme için uygun şartları taşıyan bir $g \in SL(2, \mathbb{Z}_p)$ seçecek ve kendi gizli anahtarı

olarak seçtiği $a \in \mathbb{Z}_p^*$ ile $Inn(g^a)$'yı hesaplayıp $Inn(g)$ ve $Inn(g^a)$ fonksiyonlarını B'ye gönderecektir. B de kendi gizli anahtarı $b \in \mathbb{Z}_p^*$ ile A'dan gelen $Inn(g)$ ve $Inn(g^a)$ fonksiyonlarını kullanarak $\phi = Inn(g)^b$ ve $Inn(g^a)^b$ fonksiyonlarını hesaplayacak ve M mesajını $Inn(g^a)^b$ fonksiyonu ile şifreleyip $E = Inn(g^{ab})(M)$ şifreli metnine ulaşacaktır. Bu şifreli metin ile $\phi = Inn(g)^b$'yi yani (E, ϕ) çiftini A'ya gönderecektir. A da kendi gizli anahtarı a'yı kullanarak $\phi^{-a} = (Inn(g)^b)^{-a}$ fonksiyonunu bulacak ve B'nin gönderdiği ''E'' şifreli metnin kodlandığı matristen ϕ^{-a}'yı kullanarak $\phi^{-a}(E) = M$ ile açık metnin kodlandığı matrise ulaşmış olacaktır.

2.5. $SL(2,\mathbb{Z}_p)$ Grubunun Üreteçler Cinsinden İfadesi

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ olmak üzere}$$

$SL(2,\mathbb{Z}_p)$ grupları S ve T üreteçleri yardımıyla üretilebilir**.** Yani $n \in \mathbb{N}$, $i_0, i_{n+1} \in \{0,1\}$ ve $j_k \in \mathbb{Z}_p$, $1 \le k \le n$ olmak üzere $SL(2,\mathbb{Z}_p)$deki her A matrisi aşağıdaki gibi yazılabilir;

$$A = S^{i_0} T^{j_1} S T^{j_2} \ldots S T^{j_n} S^{i_{n+1}}.$$

$SL(2,\mathbb{Z}_p)$ grubundaki matrisleri S ve T üreteçlerinin çarpımı olarak ifade edebilmek için aşağıdaki durum kullanılabilir:

$SL(2,\mathbb{Z}_p)$ grubundaki bir A matrisinin (2,1). adresindeki değeri sıfırdan farklı ise bu taktirde A matrisi, $j_1, j_2, j_3 \in \mathbb{Z}_p$ olmak üzere,

$$A = T^{j_1} S T^{j_2} S T^{j_3}$$

ile gösterilebilir ve bu ifade basitçe şöyle hesaplanır:

$$T^{j_1}ST^{j_2}ST^{j_3} = \begin{pmatrix}1 & j_1\\ 0 & 1\end{pmatrix}\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & j_2\\ 0 & 1\end{pmatrix}\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & j_3\\ 0 & 1\end{pmatrix}$$
$$= \begin{pmatrix}j_1j_2-1 & j_1j_2j_3-j_3-j_1\\ j_2 & j_2j_3-1\end{pmatrix}$$

$A \in SL(2,\mathbb{Z}_p)$ ve $a_3 \neq 0$ olmak üzere $A = \begin{pmatrix}a_1 & a_2\\ a_3 & a_4\end{pmatrix}$ için

$$j_1 = (a_1+1)j_2^{-1}$$
$$j_2 = a_3$$
$$j_3 = (a_4+1)j_2^{-1}$$

eşitlikleri kullanılarak j_1, j_2, j_3 değerleri bulunup yerine yazılarak da $SL(2,\mathbb{Z}_p)$ grubunun her elemanı S ve T üreteçlerinin çarpımı olarak yazılabilir.

2.6. Sistemin Algoritması

2.6.1. Anahtar Oluşturma Algoritması

1. g birim matristen farklı ve p asal olmak üzere *ord(g)=p* olacak şekilde bir $g \in SL(2,\mathbb{Z}_p)$ seçilir.

2. Gizli anahtar, rastgele seçilmiş bir $a \in \mathbb{Z}_p^*$ değerinden oluşur.

3. Açık anahtar, $Inn(g)$ ve $Inn(g^a)$ fonksiyonlarından oluşur. ($\{Inn(g)(\gamma_i)\}, 1 \le i \le n$ ve $\{Inn(g^a)(\gamma_i)\}, 1 \le i \le n$ için).

2.6.2. Şifreleme Algoritması

1. Şifrelenecek $M \in SL(2,\mathbb{Z}_p)$ mesajın kodlandığı matris, $SL(2,\mathbb{Z}_p)$ grubunun γ_i üreteçlerinin çarpımı olarak ifade edilir yani bir $k \in \mathbb{N}$ ve $1 \le j \le k$ için $i_j \in \{1,...,n\}$ olmak üzere $M = \gamma_{i_1} \cdots \gamma_{i_k}$ olarak yazılır.

2. $b \in \mathbb{Z}_p^*$ seçilir ve bununla $(Inn(g^a))^b$ ile $\{(Inn(g^a))^b(\gamma_i)\}, 1 \le i \le n$ ifadeleri hesaplanır.

3. $E = Inn(g^{ab})(M) = (Inn(g^a))^b(M) = \prod_{j=1}^{k}(Inn(g^a))^b(\gamma_{i_j})$ çarpımları hesaplanır.

4. $\phi = Inn(g)^b$ ile $\{Inn(g^b)(\gamma_i)\}, 1 \le i \le n$ ifadeleri hesaplanır.

5. Açık metin M matrisi için gizli metin çifti (E, ϕ)dir.

2.6.3. Deşifreleme Algoritması

1. γ_i , $SL(2,\mathbb{Z}_p)$ grubunun üreteçleri olmak üzere gizli metin çiftinin birinci bileşeni E üreteçlerin çarpımı olarak belirlenir yani herhangi bir $l \in \mathbb{N}$ için $1 \le j \le l$ ve $i_j \in \{1,...,n\}$ olmak üzere $E = \gamma_{i_1} \cdots \gamma_{i_l}$ olarak belirlenir.

2. ϕ^{-a} ile $\{\phi^{-a}(\gamma_i)\}$, $1 \le i \le n$ ifadeleri hesaplanır.

3. $\phi^{-a}(E) = \prod_{j=1}^{l} \phi^{-a}(\gamma_{i_j})$ çarpımları hesaplanır.

2.7. ''g'' Matrisinin Seçimi

Paeng ve arkadaşları [4] makalelerinde ''$c \in Z_p^{\,*}, c \neq 0, A \in SL(2,Z_p)$ olmak üzere $SL(2,Z_p)$ grubunda p mertebeli bir g elemanı tarafından oluşturulan bir alt gruba ulaşmak için $\delta_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ veya $\delta_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ olmak üzere g elemanı $g = A(I + c\delta_{12})A^{-1}$ veya $g = A(I + c\delta_{21})A^{-1}$ şeklinde seçilmelidir.'' diye öneriyorlar. Bu şekilde seçilmesi kuvvetin kolay alınmasını sağlar. İncelenirse

$g = A(I + c\delta_{12})A^{-1}$ veya $g = A(I + c\delta_{21})A^{-1}$ olmak üzere her tarafın n. kuvveti alınırsa: $g^n = (A(I + c\delta_{12})A^{-1})^n$ olup

$g^n = \overbrace{(A(I + c\delta_{12})A^{-1})(A(I + c\delta_{12})A^{-1})(A(I + c\delta_{12})A^{-1}).....(A(I + c\delta_{12})A^{-1})}^{n \tan e}$ olur. Bu ifade açılırsa $g^n = (A(I + c\delta_{12})^n A^{-1})$ i elde edilir. Bu ise $g^n = (A(I + cn\delta_{12})\ A^{-1})$ olması demektir. Yani g'nin n. kuvvetini almak kolaydır. Dolayısıyla g matrisinin bu şekilde seçilmesi

1- g'nin kuvvetlerini almak kolaydır.

2- g'yi böyle almak $SL(2,Z_p)$'nin p mertebeli bir alt grubu oluşmasını sağlar. Örneğin $p = 29$ için $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}\cdots\cdots\begin{pmatrix} 1 & 28 \\ 0 & 1 \end{pmatrix}$ olup 29 eleman olur.

3- p büyütülebilir ve p'nin büyük olması kırılmasını zorlaştırır.

İşte bu üç sebepten dolayı ''g'' matrisini $g = A(I + c\delta_{12})A^{-1}$ veya $g = A(I + c\delta_{21})A^{-1}$ şeklinde seçmek oldukça faydalıdır.

Bu örnekde işlemlerin kolay yapılabilmesi için *a*, *b* ve *p* sayıları küçük seçilmiştir.

Örnek 2..7.1.

A "GEL" açık metnini B'ye göndermek istesin

$\left.\begin{matrix} G=7 \\ E=5 \\ L=14 \end{matrix}\right\}$ dir.

B:

1- Öncelikle B *g* matrisini belirler

Şu biliniyor ki $\delta_{12}=\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ olmak üzere

g=A(I+cδ_{12})A^{-1} veya g=A(I+cδ_{21})A^{-1} şeklinde seçilmelidir.

$c=1$ $ord(g)=29=n=29$ ve

$A=\begin{pmatrix} 7 & 12 \\ 0 & 25 \end{pmatrix}$ seçilsin. g= A(I+cδ_{12})A^{-1} i kullanılsın.

Bu takdirde $g\equiv\begin{pmatrix} 7 & 12 \\ 0 & 25 \end{pmatrix}(29)$ olur.

2- B a=5 $\in$ $\mathbb{Z}_p^*$ gizli anahtarını seçer ve bu a=5 ile $Inn(g^a)$ yı hesaplar.

$A=\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}\in \mathrm{SL}(2,\mathbb{Z}_p)$, I=$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ ve c ve n için $g^n\equiv\begin{pmatrix} 1-cna_1a_3 & cn(a_1)^2 \\ -cn(o_3)^2 & 1+cno,o_3 \end{pmatrix}$

şeklinde hesaplanır.

$A=\begin{pmatrix} 7 & 12 \\ 0 & 25 \end{pmatrix}$ ve $g=\begin{pmatrix} 1 & 20 \\ 0 & 1 \end{pmatrix}$ olmak üzere a=5 için formülden $g^a\equiv\begin{pmatrix} 1 & 13 \\ 0 & 1 \end{pmatrix}(29)$

bulunur.

3- B *Inn*(g) ile $Inn(g^a)$ fonksiyonlarını A'ya gönderir

$g=\begin{pmatrix}1 & 20\\ 0 & 1\end{pmatrix}$ $g^a=\begin{pmatrix}1 & 13\\ 0 & 1\end{pmatrix}$ olduğundan B'nin A'ya göndereceği açık anahtar

$(Inn(g), Inn(g^a)) = (Inn(\begin{pmatrix}1 & 20\\ 0 & 1\end{pmatrix}), Inn(\begin{pmatrix}1 & 13\\ 0 & 1\end{pmatrix}))$ çiftidir.

A:

1- $b=17 \in \mathbb{Z}_p^*$ gizli anahtarını seçer. Bununla $\varnothing = Inn\ (g^b)$ yı hesaplar. Aynı yukarıdaki metod ile g^n formülünden $g^{17} \equiv \begin{pmatrix}1 & 21\\ 0 & 1\end{pmatrix}$ olarak bulunur.

$\varnothing = Inn(g^b) = Inn(\begin{pmatrix}1 & 21\\ 0 & 1\end{pmatrix})$ olur.

2- $Inn(g^a)^b$ yi hesaplar yine aynı metod ile $g^{ab} = g^{5.17} = g^{85}$ $\begin{pmatrix}1 & 18\\ 0 & 1\end{pmatrix}$ olur. Dolayısıyla

$Inn(g^a)^b = Inn(\begin{pmatrix}1 & 18\\ 0 & 1\end{pmatrix})$ olur.

Şimdi de M = "GEL" mesajı yani 7 5 14 $Inn(g^a)^b$ ile şifrelenirse

3- $Inn(g^a)^b$ (M) = E yi hesaplar.

Bunun için öncelikle şifrelenmek istenen mesaj matris üreteçlerin çarpımı olarak nasıl ifade edilebilir o incelenirse

A- G=7 için yapılırsa mesaj matrisi

$M=\begin{pmatrix}7 & 0\\ 23 & 14\end{pmatrix}$ olsun

$\begin{pmatrix}J_1J_2-1 & J_1J_2J_3-J_3-J_1\\ J_2 & J_2J_3-1\end{pmatrix} = \begin{pmatrix}7 & 0\\ 23 & 14\end{pmatrix}$ eşitliğinden

$J_1=18\ \ J_2=23\ \ \ J_3=12$

$M=T^{18}ST^{23}ST^{12}$ olur.

$M=\begin{pmatrix}7 & 0\\ 23 & 14\end{pmatrix}=\begin{pmatrix}1 & 18\\ 0 & 1\end{pmatrix}\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & 23\\ 0 & 1\end{pmatrix}\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & 12\\ 0 & 1\end{pmatrix}$ şeklinde mesaj üreteçlerin çarpımı olarak ifade edilmiş olur.

B- Aynı şekilde E=5 için yapılırsa mesaj matrisi

$M=\begin{pmatrix}5 & 0\\ 23 & 14\end{pmatrix}$ olsun $J_1=28\ J_2=23, J_3=12$ olur. Dolayısıyla

$M=\begin{pmatrix}5 & 0\\ 23 & 14\end{pmatrix}=\begin{pmatrix}1 & 28\\ 0 & 1\end{pmatrix}\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & 23\\ 0 & 1\end{pmatrix}\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & 12\\ 0 & 1\end{pmatrix}$ olur.

C- Aynı şekilde L=14 için yapılırsa mesaj matrisi

$M=\begin{pmatrix}14 & 0\\ 23 & 14\end{pmatrix}$ olsun $J_1\equiv J_3=12\ J_2=23$ olur. Dolayısıyla

$M=\begin{pmatrix}14 & 0\\ 23 & 14\end{pmatrix}=\begin{pmatrix}1 & 28\\ 0 & 1\end{pmatrix}\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & 23\\ 0 & 1\end{pmatrix}\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & 12\\ 0 & 1\end{pmatrix}$ olur. Dolayısıyla mesaj matrisleri üreteçler cinsinden ifade edilmiş olunur. Şifrelenirse

E= $Inn(g^{ab})(M)=Inn(\begin{pmatrix}1 & 18\\ 0 & 1\end{pmatrix})(M)$ şöyle hesaplanır:

1- G=7 için yapılırsa

i- $Inn(\begin{pmatrix}1 & 18\\ 0 & 1\end{pmatrix})\ (\begin{pmatrix}1 & 18\\ 0 & 1\end{pmatrix})=\begin{pmatrix}1 & 18\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 18\\ 0 & \end{pmatrix}\begin{pmatrix}1 & 18\\ 0 & 1\end{pmatrix}^{-1}=\begin{pmatrix}1 & 18\\ 0 & 1\end{pmatrix}$ olur. Yani

$Inn\ (\begin{pmatrix}1 & 18\\ 0 & 1\end{pmatrix})\ (\begin{pmatrix}1 & 18\\ 0 & 1\end{pmatrix})=\begin{pmatrix}1 & 18\\ 0 & 1\end{pmatrix}$ olur. Aynı şekilde devam edilirse;

ii- $Inn\ (\begin{pmatrix}1 & 19\\ 0 & 1\end{pmatrix})\ (\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix})=\begin{pmatrix}18 & 23\\ 1 & 11\end{pmatrix}$

iii- $Inn\ (\begin{pmatrix}1 & 18\\ 0 & 1\end{pmatrix})\ (\begin{pmatrix}1 & 23\\ 0 & 1\end{pmatrix})=\begin{pmatrix}1 & 23\\ 0 & 1\end{pmatrix}$

iv- $Inn\left(\begin{pmatrix}1 & 18\\ 0 & 1\end{pmatrix}\right)\left(\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\right)=\begin{pmatrix}18 & 23\\ 1 & 11\end{pmatrix}$

v- $Inn\left(\begin{pmatrix}1 & 18\\ 0 & 1\end{pmatrix}\right)\left(\begin{pmatrix}1 & 12\\ 0 & 1\end{pmatrix}\right)=\begin{pmatrix}1 & 12\\ 0 & 1\end{pmatrix}$

Şeklinde bulunan bu matrisler çarpılırsa

$$E=\begin{pmatrix}1 & 18\\ 0 & 1\end{pmatrix}\begin{pmatrix}18 & 23\\ 1 & 11\end{pmatrix}\begin{pmatrix}1 & 23\\ 0 & 1\end{pmatrix}\begin{pmatrix}18 & 23\\ 1 & 11\end{pmatrix}\begin{pmatrix}1 & 12\\ 0 & 1\end{pmatrix}=$$

$\begin{pmatrix}1697 & 32731\\ 52 & 1021\end{pmatrix}\equiv\begin{pmatrix}15 & -68\\ 23 & 6\end{pmatrix}\equiv\begin{pmatrix}15 & 19\\ 23 & 6\end{pmatrix}$ (29) elde edilir. Yani $m_1 = (1,1) = 15$ olup

G=7 nin şifrelenmiş hali $m=15$ olarak bulunur.

2- E=5 için yapılırsa

i- $Inn\left(\begin{pmatrix}1 & 18\\ 0 & 1\end{pmatrix}\right)\left(\begin{pmatrix}1 & 18\\ 0 & 1\end{pmatrix}\right)=\begin{pmatrix}1 & 18\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 28\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 18\\ 0 & 1\end{pmatrix}^{-1}=\begin{pmatrix}1 & 28\\ 0 & 1\end{pmatrix}$ yani

$Inn\left(\begin{pmatrix}1 & 18\\ 0 & 1\end{pmatrix}\right)\left(\begin{pmatrix}1 & 28\\ 0 & 1\end{pmatrix}\right)=\begin{pmatrix}1 & 28\\ 0 & 1\end{pmatrix}$ olur. Aynı şekilde devam edilirse

ii- $Inn\left(\begin{pmatrix}1 & 18\\ 0 & 1\end{pmatrix}\right)\left(\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\right)=\begin{pmatrix}18 & 23\\ 1 & 11\end{pmatrix}$

iii- $Inn\left(\begin{pmatrix}1 & 18\\ 0 & 1\end{pmatrix}\right)\left(\begin{pmatrix}1 & 23\\ 1 & \end{pmatrix}\right)=\begin{pmatrix}1 & 23\\ 0 & 1\end{pmatrix}$

iv - $Inn\left(\begin{pmatrix}1 & 18\\ 0 & 1\end{pmatrix}\right)\left(\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\right)=\begin{pmatrix}18 & 23\\ 1 & 11\end{pmatrix}$

v- $Inn\left(\begin{pmatrix}1 & 18\\ 0 & 1\end{pmatrix}\right)\left(\begin{pmatrix}1 & 12\\ 0 & 1\end{pmatrix}\right)=\begin{pmatrix}1 & 12\\ 0 & 1\end{pmatrix}$ elde edilir.

Bu sonuçlar çarpılırsa

E= $\begin{pmatrix}1 & 28\\ 0 & 1\end{pmatrix}\begin{pmatrix}18 & 23\\ 1 & 11\end{pmatrix}\begin{pmatrix}1 & 23\\ 0 & 1\end{pmatrix}\begin{pmatrix}18 & 23\\ 1 & 11\end{pmatrix}\begin{pmatrix}1 & 12\\ 0 & 1\end{pmatrix}=\begin{pmatrix}2217 & 43391\\ 52 & 1021\end{pmatrix}$ olup mod 29 a göre $\begin{pmatrix}13 & 7\\ 23 & 6\end{pmatrix}$ olur yani $m_2(1,1)=13$ olup E=5 in şifrelenmiş hali $K=13$ olur.

3- L=14 için yapılırsa

i- *Inn* ($\begin{pmatrix}1 & 18\\ 0 & 1\end{pmatrix}$) ($\begin{pmatrix}1 & 12\\ 0 & 1\end{pmatrix}$) = $\begin{pmatrix}1 & 12\\ 0 & 1\end{pmatrix}$

ii- *Inn* ($\begin{pmatrix}1 & 12\\ 0 & 1\end{pmatrix}$)($\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$) = $\begin{pmatrix}18 & 23\\ 1 & 11\end{pmatrix}$

iii- *Inn* ($\begin{pmatrix}1 & 18\\ 0 & 1\end{pmatrix}$)($\begin{pmatrix}1 & 23\\ 0 & 1\end{pmatrix}$) = $\begin{pmatrix}1 & 23\\ 0 & 1\end{pmatrix}$

Iv- *Inn* ($\begin{pmatrix}1 & 18\\ 0 & 1\end{pmatrix}$)($\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$) = $\begin{pmatrix}18 & 23\\ 1 & 11\end{pmatrix}$

v- *Inn* ($\begin{pmatrix}1 & 18\\ 0 & 1\end{pmatrix}$) ($\begin{pmatrix}1 & 12\\ 0 & 1\end{pmatrix}$) = $\begin{pmatrix}1 & 12\\ 0 & 1\end{pmatrix}$ elde edilir.

Bu sonuçlar çarpılırsa

E= $\begin{pmatrix}1 & 12\\ 0 & 1\end{pmatrix}\begin{pmatrix}18 & 23\\ 1 & 11\end{pmatrix}\begin{pmatrix}1 & 23\\ 0 & 1\end{pmatrix}\begin{pmatrix}18 & 23\\ 1 & 11\end{pmatrix}\begin{pmatrix}1 & 12\\ 0 & 1\end{pmatrix}=\begin{pmatrix}1385 & 26605\\ 52 & 1021\end{pmatrix}$ olur. Bu matris mod 29 a göre $\begin{pmatrix}22 & 12\\ 23 & 6\end{pmatrix}$ olur. Yani $m_3(1,1)=22$ olup L = 14 ün şifrelenmiş hali $Ş=22$ olarak bulunmuş olur.

Dolayısıyla "*GEL*" mesajının şifreli hali "*MKŞ*" olarak elde edilir.

4- A B'ye $(E,\varnothing)$ yi yollar.

$E_1=\begin{pmatrix}15 & 19\\ 23 & 6\end{pmatrix}$ $E_2=\begin{pmatrix}13 & 7\\ 23 & 6\end{pmatrix}$ $E_3=\begin{pmatrix}22 & 12\\ 23 & 6\end{pmatrix}\varnothing=\begin{pmatrix}1 & 21\\ 0 & 1\end{pmatrix}$ idi

Yani A B'ye ayrı ayrı

$(E_1, \varnothing)$, $(E_2, \varnothing)$, $(E_3, \varnothing)$ yi yollar.

B:

1- Kendi gizli anahtarı *a*=5 ile $\varnothing^{-a}$ yı yani

(Inn(g^b))$^{-a}$ yı hesaplar (Yine g^n formülünden)

$g^{-ab} = \begin{pmatrix} 1 & 11 \\ 0 & 1 \end{pmatrix}$ olarak bulunur. Dolayısıyla $\varnothing^{-a} = Inn\left(\begin{pmatrix} 1 & 11 \\ 0 & 1 \end{pmatrix}\right)$ olur.

2- Deşifreleme: $\varnothing^{-a}$ (E) = $\varnothing^{-a}$ Inn (g^{ab}) (M)= (Inn(g^b))$^{-a}$ Inn (g^{ab}) (M) = M yi elde eder.

Bunun için önce şifrelenmiş metin E üreteçlerin çarpımı olarak yazılmalı.

E = $\begin{pmatrix} J_1 J_2 - 1 & J_1 J_2 J_3 - J_3 - J_1 \\ J_2 & J_2 J_3 - 1 \end{pmatrix}$ den $J_1 J_2 J_3$ bulunmalı.

A- $E_1 = \begin{pmatrix} 15 & 19 \\ 23 & 6 \end{pmatrix}$ için yapılırsa Yani G ye karşılık gelen için

$J_1 = 7$ $J_2 = 23$ $J_3 = 23$ olur.

E= $T^{J_1} S T^{J_2} S T^{J_3}$ den

E= $T^7 S T^{23} S T^{23} = \begin{pmatrix} 1 & 7 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 23 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 23 \\ 0 & 1 \end{pmatrix}$ üreteçlerin çarpımı

olarak yazılır ve $\varnothing^{-a} = Inn\left(\begin{pmatrix} 1 & 11 \\ 0 & 1 \end{pmatrix}\right)$ E'nin her bir üreteci ile ayrı ayrı çarpılırsa

i- $Inn\left(\begin{pmatrix} 1 & 11 \\ 0 & 1 \end{pmatrix}\right)\left(\begin{pmatrix} 1 & 7 \\ 0 & 1 \end{pmatrix}\right) = \begin{pmatrix} 1 & 11 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 7 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 11 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 7 \\ 0 & 1 \end{pmatrix}$

ii- $Inn\left(\begin{pmatrix} 1 & 11 \\ 0 & 1 \end{pmatrix}\right)\left(\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\right) = \begin{pmatrix} 11 & 23 \\ 1 & 18 \end{pmatrix}$

iii- $Inn\left(\begin{pmatrix}1 & 11\\ 0 & 1\end{pmatrix}\right)\left(\begin{pmatrix}1 & 23\\ 0 & 1\end{pmatrix}\right)=\begin{pmatrix}1 & 23\\ 0 & 1\end{pmatrix}$

iv- $Inn\left(\begin{pmatrix}1 & 11\\ 0 & 1\end{pmatrix}\right)\left(\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\right)=\begin{pmatrix}11 & 23\\ 1 & 18\end{pmatrix}$

v- $Inn\left(\begin{pmatrix}1 & 11\\ 0 & 1\end{pmatrix}\right)\left(\begin{pmatrix}1 & 23\\ 0 & 1\end{pmatrix}\right)=\begin{pmatrix}1 & 23\\ 0 & 1\end{pmatrix}$ olup bu sonuçlar çarpılırsa

$M=\begin{pmatrix}1 & 7\\ 0 & 1\end{pmatrix}\begin{pmatrix}11 & 23\\ 1 & 18\end{pmatrix}\begin{pmatrix}1 & 23\\ 0 & 1\end{pmatrix}\begin{pmatrix}11 & 23\\ 1 & 18\end{pmatrix}\begin{pmatrix}1 & 23\\ 0 & 1\end{pmatrix}=\begin{pmatrix}761 & 28051\\ 52 & 29172\end{pmatrix}$ olup mod 29 a göre $\begin{pmatrix}7 & 8\\ 23 & 27\end{pmatrix}$ olur. Dolayısıyla M nin deşifrelenmiş hali $7=G$ olarak elde edilir.

B- $E_2=\begin{pmatrix}13 & 7\\ 23 & 6\end{pmatrix}=\begin{pmatrix}J_1J_2-1 & J_1J_2J_3-J_3-J\\ J_2 & J_2J_3-1\end{pmatrix}$ den

$J_1=17\ \ J_2=23\ J_3=23$ E= $T^{J_1}ST^{J_2}ST^{J_3}$ den E= $T^{17}ST^{23}ST^{23}$ olur.

$E=\begin{pmatrix}1 & 17\\ 0 & 1\end{pmatrix}\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & 23\\ 0 & 1\end{pmatrix}\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & 23\\ 0 & 1\end{pmatrix}$ üreteçlerin çarpımı

olarak yazılır ve $\varnothing^{-a}=$ Inn $\left(\begin{pmatrix}1 & 11\\ 0 & 1\end{pmatrix}\right)$ E nin her bir üreteci ile ayrı ayrı çarpılırsa

i- $Inn\left(\begin{pmatrix}1 & 11\\ 0 & 1\end{pmatrix}\right)\left(\begin{pmatrix}1 & 17\\ 0 & 1\end{pmatrix}\right)=\begin{pmatrix}1 & 11\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 17\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 11\\ 0 & 1\end{pmatrix}^{-1}=\begin{pmatrix}1 & 17\\ 0 & 1\end{pmatrix}$

ii- $Inn\left(\begin{pmatrix}1 & 11\\ 0 & 1\end{pmatrix}\right)\left(\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\right)=\begin{pmatrix}11 & 23\\ 1 & 18\end{pmatrix}$

iii- $Inn\left(\begin{pmatrix}1 & 11\\ 0 & 1\end{pmatrix}\right)\left(\begin{pmatrix}1 & 23\\ 0 & 1\end{pmatrix}\right)=\begin{pmatrix}1 & 23\\ 0 & 1\end{pmatrix}$

iv- $Inn\left(\begin{pmatrix}1 & 11\\ 0 & 1\end{pmatrix}\right)\left(\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\right)=\begin{pmatrix}11 & 23\\ 1 & 18\end{pmatrix}$

v- $Inn(\begin{pmatrix}1 & 11\\0 & 1\end{pmatrix})(\begin{pmatrix}1 & 23\\0 & 1\end{pmatrix}) = \begin{pmatrix}1 & 23\\0 & 1\end{pmatrix}$ olup bu sonuçlar çarpılırsa

$M = \begin{pmatrix}1 & 17\\0 & 1\end{pmatrix}\begin{pmatrix}11 & 23\\0 & 18\end{pmatrix}\begin{pmatrix}1 & 23\\0 & 1\end{pmatrix}\begin{pmatrix}11 & 23\\0 & 18\end{pmatrix}\begin{pmatrix}1 & 23\\0 & 1\end{pmatrix} = \begin{pmatrix}1281 & 47621\\52 & 1957\end{pmatrix}$ olup mod 29'a göre

$= \begin{pmatrix}5 & 3\\23 & 1957\end{pmatrix}$ e eşittir. Dolayısıyla K nın deşifrelenmiş hali $5 = E$ olarak elde edilir.

C- $E_3 = \begin{pmatrix}22 & 12\\23 & 6\end{pmatrix}$ için

$J_1 = 1\ J_2 = 23\ J_3 = 23$ olur. E= $T^{J_1}ST^{J_2}ST^{J_3}$ den

$E = TS\ T^{23}ST^{23} = \begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}\begin{pmatrix}0 & -1\\1 & 0\end{pmatrix}\begin{pmatrix}1 & 23\\0 & 1\end{pmatrix}\begin{pmatrix}0 & -1\\1 & 0\end{pmatrix}\begin{pmatrix}1 & 23\\0 & 1\end{pmatrix}$ üreteçlerin çarpımı olarak

yazılır ve $\varnothing^{-a} = Inn(\begin{pmatrix}1 & 11\\0 & 1\end{pmatrix})$ E'nin her bir üreteci ile ayrı ayrı çarpılırsa

i- $Inn(\begin{pmatrix}1 & 11\\0 & 1\end{pmatrix})(\begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}) = \begin{pmatrix}1 & 11\\0 & 1\end{pmatrix}\begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}\begin{pmatrix}1 & -11\\0 & 1\end{pmatrix} = \begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}$

ii- $Inn(\begin{pmatrix}1 & 11\\0 & 1\end{pmatrix})(\begin{pmatrix}0 & -1\\1 & 0\end{pmatrix}) = \begin{pmatrix}11 & 23\\1 & 18\end{pmatrix}$

iii- $Inn(\begin{pmatrix}1 & 11\\0 & 1\end{pmatrix})(\begin{pmatrix}1 & 23\\0 & 1\end{pmatrix}) = (\begin{pmatrix}1 & 23\\0 & 1\end{pmatrix})$

iv- $Inn(\begin{pmatrix}1 & 11\\0 & 1\end{pmatrix})(\begin{pmatrix}0 & -1\\1 & 0\end{pmatrix}) = \begin{pmatrix}11 & 23\\1 & 18\end{pmatrix}$

v- $Inn(\begin{pmatrix}1 & 11\\0 & 1\end{pmatrix})(\begin{pmatrix}1 & 23\\0 & 1\end{pmatrix}) = (\begin{pmatrix}1 & 23\\0 & 1\end{pmatrix})$ olup bu sonuçlar çarpılırsa

$M = \begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}\begin{pmatrix}11 & 23\\1 & 18\end{pmatrix}(\begin{pmatrix}1 & 23\\0 & 1\end{pmatrix})\begin{pmatrix}11 & 23\\1 & 18\end{pmatrix}(\begin{pmatrix}1 & 23\\0 & 1\end{pmatrix}) = \begin{pmatrix}449 & 16309\\52 & 1957\end{pmatrix}$ olup mod 29 a

göre $\begin{pmatrix}14 & 11\\23 & 14\end{pmatrix}$ e eşittir. Dolayısıyla Ş nin deşifrelenmiş hali $14 = L$ olarak elde edilir.

Dolayısıyla ‘’ GEL ’’ mesajının şifrelenmiş hali ‘’ MKŞ ‘’ ve tekrar deşifrelenmiş hali ‘’ GEL ’’ olarak elde edilmiş olur.

Aşağıdaki örnekte ‘’ GEL ’’ mesajı yine aynı metod ile fakat bu sefer matris değiştirilerek yapılmıştır.

Örnek2.7.2. A “GEL” açık metnini B’ye göndermek istesin

$$\left.\begin{matrix} G=7 \\ E=5 \\ L=14 \end{matrix}\right\} \text{dir.}$$

B:

1- B g matrisini belirlesin.

Şu biliniyor ki $\delta_{12}=\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ olmak üzere

g= A(I+c δ_{12}) A^{-1} veya g= A(I+c δ_{12}) A^{-1} şeklinde seçilmelidir.

$c=1$ $ord(g)=29=n=29$ ve

$A=\begin{pmatrix} 35 & 11 \\ 0 & 5 \end{pmatrix}$ seçilsin, g= A(I+c δ_{12}) A^{-1} seçilsin.

Bu takdirde $g\equiv\begin{pmatrix} 1 & 7 \\ 0 & 1 \end{pmatrix}(29)$ olur.

2- B $a=7\in\mathbb{Z}_p^*$ gizli anahtarını seçsin. Bu a=7 ile $Inn(g^a)$ yı hesaplamalı.

$A=\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}\in \text{SL}(2,\mathbb{Z}_p)$, I=$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ ve c ve n için $g^n\equiv\begin{pmatrix} 1-cna_1a_3 & cn(a_1)^2 \\ -cn(o_3)^2 & 1+cno,o_3 \end{pmatrix}$

şeklinde hesaplanır.

$A=\begin{pmatrix} 35 & 11 \\ 0 & 5 \end{pmatrix}$ ve $g=\begin{pmatrix} 1 & 7 \\ 0 & 1 \end{pmatrix}$ olduğundan a=7 için formülden $g^7\equiv\begin{pmatrix} 1 & 20 \\ 0 & 1 \end{pmatrix}(29)$

bulunur.

3- B *Inn* (*g*) ile $Inn(g^a)$ fonksiyonlarını A'ya gönderir.

$g = \begin{pmatrix} 1 & 7 \\ 0 & 1 \end{pmatrix}$ $g^a = \begin{pmatrix} 1 & 20 \\ 0 & 1 \end{pmatrix}$ olduğundan

B'nin A'ya göndereceği açık anahtar

$(Inn(g), Inn(g^a)) = (Inn(\begin{pmatrix} 1 & 7 \\ 0 & 1 \end{pmatrix}), Inn(\begin{pmatrix} 1 & 20 \\ 0 & 1 \end{pmatrix}))$ çiftidir.

A:

1- b=19 $\in$ $\mathbb{Z}_p^*$ gizli anahtarı seçer. Bununla $\varnothing$=Inn (g^b) yi hesaplamalı. Aynı yukarıdaki metod ile g^n formülünden $g^{19} \equiv \begin{pmatrix} 1 & 17 \\ 0 & 1 \end{pmatrix}$ olarak bulunur.

$\varnothing = Inn(g^b) = Inn(\begin{pmatrix} 1 & 17 \\ 0 & 1 \end{pmatrix})$ olur.

2- $Inn(g^a)^b$ yi hesaplamalı. Yine aynı metod ile $g^{a.b} = g^{7.19} = g^{133}$ $\begin{pmatrix} 1 & 162925 \\ 0 & 1 \end{pmatrix}$ olup mod 29 a göre $\begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}$ olur. Dolayısıyla $Inn(g^a)^b = Inn(\begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix})$ olur.

Şimdi de m = "GEL" mesajı yani 7 5 14'ü $Inn(g^a)^b$ ile şifrelensin.

3- $Inn(g^a)^b$ (M) = E hesaplanmalı.

A- G=7 için mesaj matrisi

$M = \begin{pmatrix} 7 & 0 \\ 19 & 16 \end{pmatrix}$ olsun

$\begin{pmatrix} J_1 J_2 - 1 & J_1 J_2 J_3 - J_3 - J_1 \\ J_2 & J_2 J_3 - 1 \end{pmatrix} = \begin{pmatrix} 7 & 0 \\ 19 & 16 \end{pmatrix}$ eşitliğinden

$J_1 = 5$ $J_2 = 19$ $J_3 = 7$ olarak bulunur. $M = T^5 S T^{19} S T^7$ olur.

$M=\begin{pmatrix}7 & 0\\ 19 & 16\end{pmatrix}=\begin{pmatrix}1 & 5\\ 0 & 1\end{pmatrix}\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & 19\\ 0 & 1\end{pmatrix}\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & 7\\ 0 & 1\end{pmatrix}$ olur. Dolayısıyla mesaj üreteçlerin çarpımı olarak ifade edilmiş olur.

B- Aynı şekilde E=5 için mesaj matrisi

$M=\begin{pmatrix}5 & 0\\ 19 & 16\end{pmatrix}$ olsun $J_1=11\ J_2=19\ J_3=7$ olur. $M=T^{11}ST^{19}ST^{7}$ olur.

$M=\begin{pmatrix}14 & 0\\ 19 & 16\end{pmatrix}=\begin{pmatrix}1 & 13\\ 0 & 1\end{pmatrix}\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & 19\\ 0 & 1\end{pmatrix}\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & 7\\ 0 & 1\end{pmatrix}$ olur.

Dolayısıyla mesaj üreteçlerin çarpımı olarak ifade edilmiş olur.

C- L=14 için mesaj matrisi

$M=\begin{pmatrix}14 & 0\\ 19 & 16\end{pmatrix}$ olsun. $J_1=13\ J_2=19\ J_3=7\ m=T^{13}ST^{19}ST^{7}$ olur.

$m=\begin{pmatrix}14 & 0\\ 19 & 16\end{pmatrix}=\begin{pmatrix}1 & 13\\ 0 & 1\end{pmatrix}\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & 19\\ 0 & 1\end{pmatrix}\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & 7\\ 0 & 1\end{pmatrix}$ olur. Dolayısıyla mesaj üreteçlerin çarpımı olarak ifade edilmiş olur.

Şimdi E = $Inn(g^{ab})(M)=Inn(\begin{pmatrix}1 & 11\\ 0 & 1\end{pmatrix})(M)$ i hesaplanmalı.

E= $Inn(g^{ab})(M)=Inn(\begin{pmatrix}1 & 18\\ 0 & 1\end{pmatrix})(M)$ şu şekilde hesaplanır:

1- G=7 için yapılırsa

i- $Inn(\begin{pmatrix}1 & 3\\ 0 & 1\end{pmatrix})\ (\begin{pmatrix}1 & 5\\ 0 & 1\end{pmatrix})=\begin{pmatrix}1 & 3\\ 0 & 1\end{pmatrix}\ (\begin{pmatrix}1 & 5\\ 0 & 1\end{pmatrix})\ \begin{pmatrix}1 & 3\\ 0 & 1\end{pmatrix}^{-1}=\begin{pmatrix}1 & 5\\ 0 & 1\end{pmatrix}$ olur.

Aynı şekilde devam edilirse

ii- $Inn\ (\begin{pmatrix}1 & 3\\ 0 & 1\end{pmatrix})\ (\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix})=\begin{pmatrix}3 & -10\\ 1 & -3\end{pmatrix}$

iii- $Inn\left(\begin{pmatrix}1 & 3\\ 0 & 1\end{pmatrix}\right)\left(\begin{pmatrix}1 & 19\\ 0 & 1\end{pmatrix}\right) = \begin{pmatrix}1 & 19\\ 0 & 1\end{pmatrix}$

iv- $Inn\left(\begin{pmatrix}1 & 3\\ 0 & 1\end{pmatrix}\right)\left(\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\right) = \begin{pmatrix}3 & -10\\ 1 & -3\end{pmatrix}$

v- $Inn\left(\begin{pmatrix}1 & 3\\ 0 & 1\end{pmatrix}\right)\left(\begin{pmatrix}1 & 7\\ 0 & 1\end{pmatrix}\right) = \begin{pmatrix}1 & 7\\ 0 & 1\end{pmatrix}$ olup

bu sonuçlar çarpılırsa

$$E = \begin{pmatrix}1 & 5\\ 0 & 1\end{pmatrix}\begin{pmatrix}3 & -10\\ 1 & -3\end{pmatrix}\begin{pmatrix}1 & 19\\ 0 & 1\end{pmatrix}\begin{pmatrix}3 & -10\\ 1 & -3\end{pmatrix}\begin{pmatrix}1 & 7\\ 0 & 1\end{pmatrix}$$

$= \begin{pmatrix}151 & 596\\ 19 & 75\end{pmatrix}$ olup bu matris mod 29 da

$= \begin{pmatrix}6 & 16\\ 19 & 17\end{pmatrix}$ olur. Sonuç olarak $m_1 = (1,1) = 6$ olup G=7 nin şifrelenmiş hali 6=F olarak bulunmuş olur.

2- Benzer şekilde E=5 için yapılırsa E'nin şifrelenmiş hali D=4 olarak bulunmuş olur.

3- Benzer şekilde L=14 için yapılırsa L'nin şifrelenmiş hali K=13 olarak bulunmuş olur.

Dolayısıyla ''GEL'' mesajının şifreli hali ''FDK'' olarak elde edilir.

4- A B'ye $(E, \varnothing)$ yi yollar.

$E_1 = \begin{pmatrix}6 & 16\\ 19 & 17\end{pmatrix}$ $E_2 = \begin{pmatrix}4 & 2\\ 19 & 17\end{pmatrix}$ $E_3 = \begin{pmatrix}13 & 7\\ 19 & 17\end{pmatrix}$ idi. $\varnothing = \begin{pmatrix}1 & 17\\ 0 & 1\end{pmatrix}$ idi.

Yani A B'ye ayrı ayrı

$(E_1, \varnothing)$, $(E_2, \varnothing)$, $(E_3, \varnothing)$ yi yollar.

B:

1- Kendi gizli anahtarı a=7 ile $\varnothing^{-a}$ yı yani

(Inn(g^b))$^{-a}$ yı hesaplar (Yine g^n formülünden)

$g^{-ab} = \begin{pmatrix} 1 & 26 \\ 0 & 1 \end{pmatrix}$ olarak bulunur. Dolayısıyla $\varnothing^{-a}$ = Inn ($\begin{pmatrix} 1 & 26 \\ 0 & 1 \end{pmatrix}$) olur.

2- Deşifreleme: $\varnothing^{-a}$ (E) = $\varnothing^{-a}$ Inn (g^{ab}) (m)

= (*Inn*(g^b))$^{-a}$ *Inn* (g^{ab}) (M) = M yi elde eder.

Bunun için önce şifrelenmiş metin E üreteçlerin çarpımı olarak yazılmalıdır.

E = $\begin{pmatrix} J_1 J_2 - 1 & J_1 J_2 J_3 - J_3 - J_1 \\ J_2 & J_2 J_3 - 1 \end{pmatrix}$ den $J_1 J_2 J_3$ bulunmalı.

A- $E_1 = \begin{pmatrix} 6 & 16 \\ 19 & 17 \end{pmatrix}$ için yapılırsa (Yani G ye karşılık gelen için)

$J_1 = 8$ $J_2 = 19$ $J_3 = 4$ olur.

E= $T^{J_1} S T^{J_2} S T^{J_3}$ den

E= $T^8 S T^{19} S T^4$

E = $\begin{pmatrix} 1 & 8 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 19 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix}$ üreteçlerin çarpımı olarak yazılır ve

$\varnothing^{-a}$ = Inn ($\begin{pmatrix} 1 & 26 \\ 0 & 1 \end{pmatrix}$) değeri E'nin her bir üreteci ile ayrı ayrı çarpılırsa:

i- *Inn* ($\begin{pmatrix} 1 & 26 \\ 0 & 1 \end{pmatrix}$) ($\begin{pmatrix} 1 & 8 \\ 0 & 1 \end{pmatrix}$)= $\begin{pmatrix} 1 & 26 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 8 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 26 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 8 \\ 0 & 1 \end{pmatrix}$

ii- *Inn* ($\begin{pmatrix} 1 & 26 \\ 0 & 1 \end{pmatrix}$) ($\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$) = $\begin{pmatrix} 26 & 19 \\ 1 & 3 \end{pmatrix}$

iii- *Inn* ($\begin{pmatrix} 1 & 26 \\ 0 & 1 \end{pmatrix}$) ($\begin{pmatrix} 1 & 19 \\ 0 & 1 \end{pmatrix}$) = $\begin{pmatrix} 1 & 19 \\ 0 & 1 \end{pmatrix}$

iv- *Inn* ($\begin{pmatrix} 1 & 26 \\ 0 & 1 \end{pmatrix}$) ($\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$) = $\begin{pmatrix} 26 & 19 \\ 1 & 3 \end{pmatrix}$

v- *Inn* ($\begin{pmatrix} 1 & 26 \\ 0 & 1 \end{pmatrix}$) ($\begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix}$) =$\begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix}$ olup bu sonuçlar çarpılırsa

M = $\begin{pmatrix} 1 & 8 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 26 & 19 \\ 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 19 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 7 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 26 & 19 \\ 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1573 & 9005 \\ 48 & 277 \end{pmatrix}$ olup mod 29 a göre $\begin{pmatrix} 7 & 15 \\ 19 & 16 \end{pmatrix}$ olur. Dolayısıyla $m_1 = (1,1) = 7$ olup F= 6 nın deşifrelenmiş hali G=7 olarak bulunmuş olur.

B- Benzer şekilde $E_2 = \begin{pmatrix} 4 & 2 \\ 19 & 17 \end{pmatrix}$ için yapılırsa (Yani E ye karşılık gelen için)

D'nin deşifrelenmiş hali E=5 olarak bulunmuş olur.

C- Benzer şekilde $E_3 = \begin{pmatrix} 13 & 7 \\ 19 & 17 \end{pmatrix}$ için yapılırsa (Yani L ye karşılık gelen için)

K'nın deşifrelenmiş hali L=14 olarak bulunmuş olur. Sonuç olarak '' GEL '' mesajının şifrelenmiş hali '' FDK '' ve tekrar deşifrelenmiş hali '' GEL'' olarak elde edilmiş olur.

3. BÖLÜM

SONUÇ, TARTIŞMA ve ÖNERİLER

Bu bölümde abelyan olmayan sonlu gruplar kullanılarak elde edilen açık anahtar kriptosistemin avantajları ve dezavantajları açıklandı. Ayrıca DLP'nin zorluğuna dayanan kriptosistemleri kırmak için bilinen en etkili metodlarden birisi olan index calculus metodunun bu sistemi neden kırmakta çok zorlandığı açıklandı. Bunun için genellikle, Paeng [3],[4], El-Gamal [5], Yamamura [6], Mahalanobis [8],[9] ve Stickel [10] kaynaklarından yararlanılmıştır.

3.1. İndex Calculus Metodu

Diskre logaritmaları hesaplamak için bilinen en etkili metod index calculus metodudur. Burada bu metod ile ilgili kısa bir genel bilgi verilecektir. Metod eskisi gibi küçük asalların bir cümlesi olan B faktör tabanını kullanıyor. Kabul edelim ki $B = \{p_1, p_2, ..., p_B\}$ olsun.

İlk basamak (hesaplamaya geçmeden önceki basamak) faktör tabanındaki B asalların logaritmasını bulmaktır.

İkinci basamak istenilen bir B elemanının diskre logaritmasını hesaplamaktır. (ilk basamaktaki faktör tabanındaki elemanların diskre logaritmalarını kullanarak)

$$\alpha^{x_j} \equiv p_1^{a_{1j}} p_2^{a_{2j}} ... p_B^{a_{Bj}} \pmod{p} \qquad 1 \le j \le C \text{ dir.}$$

Bu eşitlikte her tarafın α tabanında logaritmasını alınırsa $log_\alpha\left(\alpha^{x_j}\right) \equiv log_\alpha\left(p_1^{a_{1j}} p_2^{a_{2j}} ... p_B^{a_{Bj}}\right) (mod\ p-1)$

$$\Rightarrow x_j\, log_\alpha{}^{\alpha} \equiv log_\alpha{}^{p_1^{a_{1j}}} + log_\alpha{}^{p_2^{a_{2j}}} + ... + log_\alpha{}^{p_B^{a_{Bj}}} \pmod{p-1}$$

$$\Rightarrow \qquad x_j \equiv a_{1j}\, log_\alpha{}^{p_1} + a_{2j}\, log_\alpha{}^{p_2} + ... + a_{Bj}\, log_\alpha{}^{p_B} \pmod{p-1}, \quad 1 \le j \le C$$

elde edilir. *p*-1 modülüne göre bir tek çözüm olduğu umuluyor. Bu takdirde faktör tabanındaki elemanların logaritması hesaplanabilir.

Bir metod keyfi bir *x* değeri alıp *p* modülüne göre α^x i hesaplama ve daha sonra α^x in *p* modülüne göre *B* deki faktörlerin hepsine sahip mi değil mi onu belirlemedir.

Hesaplamaya geçilmeden önceki basamağın başarılı bir şekilde gerçekleştirildiği var sayılsın.

İstenilen $log_\alpha{}^B$ logaritması şu şekilde hesaplanıyor: Rastgele bir s $(1 \le s \le p-2)$ tamsayısı seçiliyor ve $\gamma = \beta\alpha^s \,(mod\ p)$ hesaplanıyor. Daha sonra γ B faktör tabanı üzerine çarpmaya çalışılıyor. Eğer bu yapılabilirse bu takdirde

$\beta\alpha^s \equiv p_1{}^{c_1} p_2{}^{c_2} \ldots p_B{}^{c_B} \,(mod\ p)$ formunda bir kongrüans elde edilir. Bu ise denk bir şekilde aşağıdaki gibi yazılabilir:

$log\left(\beta\alpha^s\right) = log\,\beta + log\,\alpha^s = log_\alpha{}^\beta + s\,log_\alpha{}^\alpha$ olduğundan;

$log_\alpha{}^\beta + s \equiv c_1\, log_\alpha{}^{p_1} + \ldots + c_B\, log_\alpha{}^{p_B} \,(mod\ p-1)$ yazılabilir. Bu ifadede $log_\alpha{}^\beta$ hariç her şey bilindiğinden $log_\alpha{}^\beta$ hesaplanabilir.

Burada bir örnek algoritmadaki iki basamağı göstermek için yapılacak.

Örnek 3.1.1. $p = 10.007$ ve $\alpha = 5$ asal elemanı *p* modülüne göre logaritmanın tabanı olsun. Faktör tabanı olarak $B = \{2,3,5,7\}$ alınsın.

$log_5{}^5 = 1$ olduğundan belirlenen faktör tabanının 3 logaritması olur.

‘‘Şanslı’’ üs lerin bazı örnekleri 4063, 5136 ve 9865 olarak seçilmiş olsun. $x = 4063$ ile $5^{4063} \equiv 42(10.007)$ i hesaplanır. $42 = 2 \times 3 \times 7$ olduğundan bu $log_5{}^2 + log_5{}^3 + log_5{}^7 \equiv 4063(10.006)$ kongrüansını verir. Benzer bir şekilde $5^{5136} \equiv 54(10.007)$ olduğundan ve $54 = 2 \times 3^3$ olduğundan bu da $log_5{}^2 + 3\,log_5{}^3 \equiv 5136(10.006)$ kongrüansını ve son olarak $5^{9865} \equiv 189(10.007)$ ve $189 = 3^3 \times 7$ olduğundan bu da $3\,log_5{}^3 + log_5{}^7 \equiv 9865(10.006)$ kongrüansını verir.

Dolayısıyla 3 bilinmeyen ve 3 kongrüansa sahip olunur. 10.006 moduna göre tek çözüm olmalı. Bu sistemi çözmek için denklemleri beraber çözme yöntemi kullanılabilinir. Denklemler çözülürse:

$$\begin{aligned} log_5{}^2 + log_5{}^3 + log_5{}^7 &\equiv 40603(10.006) \\ log_5{}^2 + 3\,log_5{}^3 &\equiv 5136(10.006) \\ 3\,log_5{}^3 + log_5{}^7 &\equiv 9865(10.006) \end{aligned}$$

$log_5{}^2 = x \quad log_5{}^3 = y \quad log_5{}^7 = z$ denirse

$$\begin{aligned} x + y + z &\equiv 40603(10.006) \\ x + 3y &\equiv 5136(10.006) \\ 3y + z &\equiv 9865(10.006) \end{aligned}$$ elde edilir.

2. denklem (-) ile çarpılırsa;

$$\left.\begin{aligned} x + y + z &\equiv 40603(10.006) \\ -x - 3y &\equiv -5136(10.006) \end{aligned}\right\} \Rightarrow z - 2y \equiv -1073(10.006)$$ ı elde edilir.

$$\left.\begin{aligned} z - 2y &\equiv -1073(10.006) \\ 3y + z &\equiv 9865(10.006) \end{aligned}\right\} \Rightarrow 5y \equiv 10.938(10.006) \Rightarrow 5y \equiv 932(10.006)$$

$$\begin{aligned} \Rightarrow \quad 2001.5y \equiv 10.005y &\equiv 1864932(10.006) \\ -y &\equiv 3816(10.006) \\ y &\equiv -3816(10.006) \\ y &\equiv 6190(10.006) \end{aligned}$$

$\Rightarrow log_5{}^3 = 6190$ bulunur.

Benzer şekilde $log_5{}^2 = 6578$ ve $log_5{}^7 = 1301$ olarak bulunur.

Kabul edelim ki $log_5{}^{9451}$ değerini bulmak istiyoruz. Keyfi s üssü $s = 7736$ olarak seçilsin. Bu takdirde $9451.5^{7736} \equiv 8400(10.007)$ olur. $8400 = 2^4.3^1.5^2.7^1$ B üzerindeki çarpanları olduğundan şu elde edilir:

$$\begin{aligned} log_5{}^{9451} &\equiv 4\,log_5{}^{2} + log_5{}^{3} + 2\,log_5{}^{5} + log_5{}^{7} - s\,(mod\ 10.006) \\ &\equiv (4.6578) + 6190 + (2.1) + 1301 - 7736\,(mod\ 10.006) \\ &= 26312 + 6190 + 2 + 1301 - 7736 \equiv 26.069\,(10.006) \\ &\equiv 6057\,(10.006) \end{aligned}$$

$$\Rightarrow \quad log_5{}^{9451} = 6057$$

Doğrulamak için hesaplanırsa gerçektende $5^{6057} \equiv 9451\,(mod\,10.007)$ dir. Dolayısıyla DLP problemi çözülmüş oldu. Yani $5^x \equiv 9451\,(mod\,10.007)$ olacak şekildeki x= 6057 olarak bu metod ile bulunmuş oldu.

3.2. İndex Calculus Metodu İle İlgili Önemli Sonuç

İncelenen sistemde grup olarak $SL\left(2,\mathbb{Z}_p\right)$ ve $GL(2,Z_p)$ seçildiği için elemanlar matrislerden oluşuyor. Dolayısıyla matrisin kuvveti alınmak ve index calculusla çözülmek istendiği zaman $g^x \equiv \beta(p)$ olacak şekildeki x aranıyor demektir. Burada g matris olduğundan index calculus metodu uygulanırsa her tarafın logaritması alındığında $log_a{}^g$ olur. Bu ise log içinde matris demektir. Ayrıca mesela $42 = 2 \times 3 \times 7$ şeklinde yazılmıştı. Matrisi çarpanlarına ayrırmak zordur. Dolayısıyla incelenen sistemde (seçilen G grubunda) index calculus metodu matris grubundan dolayı çok kısıtlayıcı kalır. Bu ise sistemi kırmak isteyenlerin işini oldukça zorlaştırmaktadır.

Hatırlanacağı üzere El-Gamal metodu incelenirken kuvvetin her seferinde değişmek zorunda olduğu belirtilmişti .

3.3. Bu Sistemde El-Gamal Metodundaki Gibi Her Seferinde Kuvvet Değişmek Zorunda Değil

GEL örneğindeki G ve E bu şekilde incelenirse:

$M_1 = G = 7$, $M_2 = E = 5$ olsun.

A:

1- $g \equiv \begin{pmatrix} 1 & 20 \\ 0 & 1 \end{pmatrix}$ i seçsin.

2- $a = 5$ seçsin.

3- $Inn(g^a) = g^5 = \begin{pmatrix} 1 & 13 \\ 0 & 1 \end{pmatrix}$ i hesaplasın.

4- A $(Inn(g), Inn(g^a)) = (Inn(\begin{pmatrix} 1 & 20 \\ 0 & 1 \end{pmatrix}), Inn(\begin{pmatrix} 1 & 13 \\ 0 & 1 \end{pmatrix}))$ i B ye yollasın.

B:

1- $b = 17$ seçsin.

2- $Inn(g^b) = g^{17} = \begin{pmatrix} 1 & 21 \\ 0 & 1 \end{pmatrix} = \gamma_1$ i hesaplasın.

3- $Inn(g^{ab}) = g^{85} = \begin{pmatrix} 1 & 18 \\ 0 & 1 \end{pmatrix}$ i hesaplasın.

4- Mesajı $M_1 = G = 7$ yi $M_1 = \begin{pmatrix} 7 & 0 \\ 23 & 14 \end{pmatrix}$ olarak belirlesin.

5- $Inn(g^{ab})\ M_1 = \begin{pmatrix} 1 & 18 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 7 & 0 \\ 23 & 14 \end{pmatrix} \begin{pmatrix} 1 & 18 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 15 & 19 \\ 23 & 6 \end{pmatrix} = \delta_1$ yı hesaplar. *G=7* nin şifrelenmiş hali *15=M* olur.

Aynı işlemleri $M_2 = E = 5$ için yaparsa M_2 nin şifrelenmiş matrisi $\begin{pmatrix} 13 & 7 \\ 23 & 6 \end{pmatrix} = \delta_2$ olup *E=5* in şifrelenmiş hali *13=K* olur.

6- (γ_1, δ_1) i ve (γ_1, δ_2) yi A ya yollar.

A:

1- Kendi gizli anahtarı $a = 5$ ile γ_1^{-a} yı yani $Inn(g^{17})^{-5} = g^{-85} = \begin{pmatrix} 1 & 11 \\ 0 & 1 \end{pmatrix}$ i hesaplar.

2- $\gamma_1^{-a} . \delta_1 = M_1$ den

$Inn\left(\begin{pmatrix}1 & 11\\ 0 & 1\end{pmatrix}\right)\begin{pmatrix}15 & 19\\ 23 & 6\end{pmatrix} = \left(\begin{pmatrix}1 & 11\\ 0 & 1\end{pmatrix}\right)\begin{pmatrix}15 & 19\\ 23 & 6\end{pmatrix}\begin{pmatrix}1 & 11\\ 0 & 1\end{pmatrix}^{-1} = \begin{pmatrix}7 & 8\\ 23 & 27\end{pmatrix}$ ye ulaşır ve *7=G* yi elde etmiş olur.

Aynı şekilde M_2 için de $\begin{pmatrix}5 & 3\\ 23 & 14\end{pmatrix}$ ulaşır ve *E=5* i elde etmiş olur.

M_1 ve M_2 nin şifrelenmesinde burada *b*=17 olup ikisinde de aynı kuvvet kullanıldı.

$$\gamma_1 = \mathrm{Inn}(g^{17}) = g^{17} = \begin{pmatrix}1 & 21\\ 0 & 1\end{pmatrix} \rightarrow \delta_1 = \mathrm{Inn}(g^{ab})\ M_1\,(modp)$$

$$\gamma_2 = \mathrm{Inn}(g^{17}) = g^{17} = \begin{pmatrix}1 & 21\\ 0 & 1\end{pmatrix} \rightarrow \delta_2 = \mathrm{Inn}(g^{ab})\ M_2\,(modp)$$ elde edilir.

El-Gamal metodunda aynı bu şekilde yazılıp taraf tarafa bölünmüştü ve M_1 bilinince M_2 elde edilmişti. Burada taraf tarafa bölme olmaz çünkü *Inn* bir fonksiyondur. Taraf tarafa bölme olsa bile g^{ab} bilinmediği için M_1 bilinse bile M_2 elde edilemez. Dolayısıyla bu sistemde fonksiyon kullanıldığı için her seferinde kuvvet değişmek zorunda değildir. Bu ise daha hızlı şifreleme ve deşifreleme yapılmasını sağlamaktadır.

3.4. Sonuç

Şifrelemede önemli olan şifrelemenin ve deşifrelemenin hızlı bir şekilde yapılması ve aynı zamanda kırılmanın çok zor olması veya çok fazla zaman almasıdır.

1- Gizli anahtarlı kriptosistemlerde önemli olan anahtarın sadece şifreleyen ve deşifreleme yapan tarafından bilinmesidir. Şayet anahtar birisinin eline geçerse tüm sistem çöker(Ceasar şifreleme metodunda olduğu gibi). Dolayısıyla anahtarı karşı tarafa güvenli bir şekilde yollamak da ayrıca bir problemdir ve güvenliği azaltır. Yani açık anahtarlı sistemler en azından karşı tarafa yollama meselesinde sıkıntılı olmadığı için gizli anahtarlı sistemlerden daha güvenlidir.

2- Şimdiye kadar açık anahtarlı kriptosistemlerin birçoğu abelyan gruplara dayanarak inşa edilmiştir. (El-Gamal örneğinde olduğu gibi) . Bu tezin ikinci bölümünde ise abelyan olmayan sonlu gruplar kullanılarak elde edilen açık anahtar kriptosistem incelendi. Abelyan olmayan sonlu gruplar kullanarak şifreleme yapıldığında üçüncü bölümde görüldüğü gibi şifrelemede her seferinde kuvvet değişmek zorunda değildir. Bu ise daha hızlı şifreleme ve deşifreleme yapılmasını sağlar. Dolayısıyla daha hızlı bir sistem olduğu için daha güvenli bir sistemdir.

3- Sonlu abelyan olmayan grup kullanılmasının sebebi de imza doğrulamadır. İmza doğrulama abelyan olmayan sonsuz gruplar kullanıldığında (Braid grup gibi) çok zor iken abelyan olmayan sonlu gruplar kullanıldığında daha kolay olduğu için abelyan olmayan sonlu gruplar kullanan sistem daha avantajlıdır.

4- Açık anahtarlı kriptosistemler genel itibariyle DLP'nin zorluğuna dayanan (El-Gamal gibi) ve ÇARPANLARA AYIRMA'nın zorluğuna dayanan (RSA gibi) sistemler olarak ikiye ayrılır. Burada incelenmiş olan ve Paeng ve arkadaşlarının makalelerinde önerdikleri kriptosistem DLP' nin zorluğuna dayanan ve El-Gamal'ı baz alan bir sistem. Üçüncü bölümde görüldüğü gibi DLP'yi çözmek için bilinen en önemli ve hızlı metod olan İndex Calculus metodu abelyan olmayan bazı önerilen gruplar kulllanıldığında DLP'yi çözmek için işlememekte veya çok zorlanmaktadır. İşte bu yüzden kırılması çok zordur.

İşte yukarıda belirtilen sebeplerden dolayı *ABELYAN OLMAYAN SONLU GRUPLAR KULLANILARAK ELDE EDİLEN AÇIK ANAHTAR KRİPTOSİSTEM* diğer bazı sistemlere nazaran çok daha güvenli ve avantajlıdır.

Bu sistemin dezavantajı ise 2. bölümde ifade edildiği gibi sistemin uygulanabileceği abelyan olmayan grup sayısının çok olmamasıdır.

3.5. Öneriler

El-Gamal sistemi ile Paeng ve arkadaşlarının yaptığı sistem karşılştırıldığında El-Gamal sisteminde abelyan olan Z_p^* grubunu kullanılır. Paeng ve arkadaşlarının yaptığı sistemde ise abelyan olmayan $2x2$ tipindeki Matris grubunu kullanılır. Ayrıca Paeng ve arkadaşları iç otomorfizma fonksiyonu kullanmaktadır. Matris kullanılınca index calculus ile kırılma zorlaşmaktadır. Fonksiyon kullanılınca hızlanılmaktadır. Burada üç öneride bulunulabilir:

1- Matris grubu yerine köşegenleştirilebilen matrisler kullanılıp inceleme yapılabilir Çünkü köşegen matrislerin kuvvetini almak kolaydır.

2- İç otomorfizma fonksiyonun yerine tersi olan ve daha hızlı şifreleme ve deşifreleme yapılmasını sağlayan başka bir fonksiyon düşünülebilir.

3- $2x2$ tipindeki Matris grubu yerine *3x3* tipindeki Matris grubu kullanılabilir. Fakat bunun için öncelikle bu grubu üreteçler cinsinden ifade etmek gereklidir.

KAYNAKLAR

1. Altındiş, H., 2011. Sayılar Teorisi ve Uygulamaları, Lazer Ofset, Ankara, 308 s.
2. Çeşmeci, M.Ü., 2009. Elektronik Çağ Öncesi Dönem Kriptololoji Tarihi. **Tübitak Uekae Dergisi, 1:** 20 – 32.
3. Paeng, S. H., et al., 2001. New Public Key Cryptosystem Using Finite Non Abelian Groups. *Advances in cryptology—CRYPTO 2001 (Santa Barbara, CA),* 470–485,Lecture Notes in Comput. Sci., 2139, *Springer, Berlin,* 94A62
4. Paeng, S. H., et al., 2003. Improved Public Key Cryptosystem Using Finite Non Abelian Groups.
5. El-Gamal, T., 1985. A Public Key Cryptosystem and A Signature Scheme Based on Discrete Logarithms. **IEEE Transactions on Information Theory, Vol. IT-31, No.4**
6. Yamamura, A., 1998. A Public Key Cryptosystem Using the Modular Group. *1th International Public Key Cryptografy Conference PKC 1998 , LNCS 1431*
7. Tobias, C., 2003. *Security Analysis of the MOR Cryptosystem, PKC 2003 LNCS 2567 pp 175- 186 Springer-Verlag, Berlin Heidelberg*
8. Mahalanobis, A. , 2007. A Simple Generalization of the El-Gamal Cryptosystem to Non-Abelian Groups, **arXiv e-prints: 0607011v5**
9. Mahalanobis, A.A, 2011. Simple Generalization of the El-Gamal Cryptosystem to Non-Abelian Groups II, **arXiv e-prints: 0706.3305v5**
10. Stickel, E., 2004.A New Public-Key Cryptosystem In Non-Abelian Groups,.Proceedings of The Thirteenth International Conference on Information Systems Development Advances in Theory, Practice and Education**: 70-80**.
11. Lee, I. S. , et al. 2004. On the Securyty of MOR Public Key Cryptosystem. **Asiacrypt, LNCS 3329:387-400**.
12. Ko, K. H., et al, 2000. New Public-Key Cryptosystem Using Braid Groups. **Advences in Cryptology – Crypto 2000 Lecture Notes In Comput.Sci, Berlin:** 166-183.
13. Thomas, T., Lal A. K., 2006. Group Signature Schemes Using Braid Groups. **arXiv e-prints: 0602063v1**.
14. Koblitz, N., 1986. Eliptic Curve Cryptosystems. **Mathematics of Computation, Volume 48, Number 177:** 203-209.

15. Koblitz, N., 1994. A Course in Number Teory and Cryptografy, Springer-Verlag , Yer, New York , 235 pp.
16. Stinson, D., 1995. Cryptography: Theory and Practice, CRC Press, New Jersey, 573 pp.
17. Çimen, C. , Akleylek, S., Akyıldız, E., 2007. Şifrelerin Matematiği: Kriptografi, ODTÜ Bilim ve Toplum Kitapları Dizisi, Ankara, 131s.
18. Menezes, A., van Oorschot, P., Vanstone, S., 1996. Handbook of Applied Cryptography, CRC Press, 754 pp.
19. Bruce, S., YIL. Applied Cryptografy, Second Addition Protocols, Algoritms and Source Code in C, Mountain View, Oak Park, 662 pp.
20. Babaoğlu, A., 2009. Kriptolojinin Geçmişi: Bir Şifreleme Algoritması Kullanmadan Önce Son Kullanım Tarihine Bakın!. **Bilim Teknik, 500 24- 42 s**.
21. Kara, O. 2009. II. Dünya Savaşından Günümüze Kriptoloji: Enigma'dan AES'e Şifreleme. **Bilim Teknik , 500:** 28-34.
22. TÜBİTAK, UEAK – Açık Anahtar Altyapısı Eğitim Kitabı, http:www.kamusm.gov.tr/tr/bilgideposu/belgeler/teknik/aaa/index.html?temelkriptoloji.htm
23. Kara, O., 2009. Kriptografinin Yapıtaşları Kriptografik Algoritmalar ve Protokoller. . **Bilim Teknik , 500:** 34-50.
24. Henk, C.A. , van Tilborg, YIL. Fundamentals of Cryptology A Professional Reference and Interactive Tutorial Eindhoven University of Technology The Netherlands. Kluwer Academic Publishers, London, 503 pp.

ÖZGEÇMİŞ

Adı Soyadı : Erkam LÜY

Baba Adı : Hacı

Anne Adı : Havva Dilek

Doğum Yeri : KAYSERİ

Doğum Tarihi : 04.09.1985

İlk okulu Kırşehir, Kocaeli ve Kırıkkale'de, orta okulu Kırıkkale Anadolu Lisesinde ve liseyi Çorum Fen Lisesinde okudu. 2005 yılında kaydolduğu Erciyes Üniversitesi Fen-Edebiyat Fakültesi Matematik Bölümü'nden 2009 yılında mezun oldu. 2009 yılında Erciyes Üniversitesi Fen Bilimleri Enstitüsü Matematik Bölümünde yüksek lisans öğrenimine başladı. 2010 yılı aralık ayında aynı enstitüde Araştırma Görevlisi olarak göreve başladı. Halen görevine devam etmektedir.

Adres: Yenidoğan Mah. Erciyes Üniversitesi TOKİ blokları C3-5 Blok No:20

Talas/KAYSERİ

E-posta : erkamluy@erciyes.edu.tr