T.C.
ERCİYES ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

GENEL LİNEER GRUPLAR KULLANILARAK YAPILAN KRİPTOSİSTEM

(Yüksek Lisans Tezi)

Hazırlayan
Murat KORKMAZ

Danışman
Yrd. Doç. Dr. Emin AYGÜN

Bu çalışma; Erciyes Üniversitesi BAP birimi tarafından Proje Kodu: FYL-2016-6259 nolu projeyle desteklenmiştir.

Mart 2017
KAYSERİ

BİLİMSEL ETİĞE UYGUNLUK

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.

Murat KORKMAZ

YÖNERGEYE UYGUNLUK

" Genel Lineer Gruplar Kullanılarak Yapılan Kriptosistem" adlı Yüksek Lisans tezi, Erciyes Üniversitesi Lisansüstü Tez Önerisi ve Tez Yazma Yönergesi'ne uygun olarak hazırlanmıştır.

Tezi Hazırlayan
Murat KORKMAZ

Danışman
Yrd. Doç. Dr. Emin AYGÜN

Matematik ABD Başkanı
Prof. Dr. Fuat GÜRCAN

Yrd. Doç. Dr. Emin AYGÜN danışmanlığında **Murat KORKMAZ** tarafından hazırlanan **"Genel Lineer Gruplar Kullanılarak Yapılan Kriptosistem"** adlı bu çalışma, jürimiz tarafından Erciyes Üniversitesi Fen Bilimleri Enstitüsü **Matematik** Anabilim Dalında **Yüksek Lisans** tezi olarak kabul edilmiştir.

10/02/2017

JÜRİ:

Başkan : Prof. Dr. Fuat GÜRCAN

Üye : Doç. Dr. İshak ALTUN

Üye : Yrd. Doç. Dr. Emin AYGÜN

ONAY:

Bu tezin kabulü, Enstitü Yönetim Kurulunun 21/03/2017 tarih ve 2017/14-20 sayılı kararı ile onaylanmıştır.

24 / 03 / 2017

Enstitü Müdürü
Prof. Dr. Mehmet AKKURT

TEŞEKKÜR

Eğitim hayatım süresince beni özveri ile yetiştiren tüm öğretmen ve öğretim üyeleri hocalarıma teşekkürü bir borç bilirim. Bu tez çalışmasında bana her türlü kolaylığı sağlayan ve bilgi ve tecrübeleriyle emeğini esirgemeyen danışmanım Sayın Yrd. Doç. Dr. Emin AYGÜN hocama çok teşekkür ederim.

Bu tez çalışmasına maddi destek veren **Erciyes Üniversitesi Bilimsel Araştırma Projeleri Birimi'ne(BAP)(Proje Kodu: FYL-2016-6259)** verdikleri desteklerinden dolayı teşekkür ederim.

Ayrıca eğitim hayatım boyunca maddi ve manevi desteklerini üzerimden hiç eksik etmeyen aileme çok teşekkür ederim.

GENEL LİNEER GRUPLAR KULLANILARAK YAPILAN KRİPTOSİSTEM

Murat KORKMAZ

Erciyes Üniversitesi, Fen Bilimleri Enstitüsü
Yüksek Lisans Tezi, Mart 2017
Tez Danışmanı: Yrd. Doç. Dr. Emin AYGÜN

ÖZET

Bu tez üç bölümden oluşmaktadır.

Birinci bölümde kriptoloji ile ilgili temel tanımlar verilerek bazı şifreleme yöntemleri açıklanmıştır.

İkinci bölümde matrisler ve genel lineer gruplar hakkında temel bilgiler verilmiştir.

Üçüncü bölümde genel lineer grupları kullanarak yapılan şifreleme ve deşifreleme işlemleri açıklanmış, çeşitli örnekler verilmiştir. Genel lineer grupları kullanarak yapılan şifreleme sisteminin özellikleri açıklanmıştır.

Anahtar Kelimeler: Genel Lineer Grup, Otomorfizma, Açık Anahtar Kriptosistem

CRYPTOSYSTEM USING GENERAL LINEAR GROUPS

Murat KORKMAZ
Erciyes University, Graduate School of Natural and Applied Sciences
M. S. Thesis, March 2017
Supervisor: Assist. Prof. Dr. Emin AYGÜN

ABSTRACT

This thesis consists of three chapters.

In the first chapter, some encryption methods are introduced by giving definition about crytoplogy.

Int he second chapter, basic information about matrixes and general linear grops are given.

In the third chapter, encoding and decoding processes using general linear groups are introduced and various examples are given. The characteristics of the encryption system using general linear groups are introduced.

Keywords: General Linear Group, Automorphism, Public Key Criptosystem

İÇİNDEKİLER

2. BÖLÜM

MATRİSLER VE GENEL LİNEER GRUPLAR

3. BÖLÜM

GENEL LİNEER GRUPLAR KULLANILARAK YAPILAN KRİPTOSİSTEM

KISALTMALAR VE SEMBOLLER

Sembol	**Anlamı**
$\mathbb{Z}$	Tamsayılar Kümesi
$\mathbb{Z}_n$	{0,1,2,...n-1 } tamsayılarının cümlesine mod n tamsayıları denir
$\mathbb{Z}_n^*$	$\mathbb{Z}_n$'in çarpımsal grubu
$M(n, K)$	Elemanları K cismine ait olan $n \times n$ tipindeki karesel matrislerin kümesi.
$SL(n, K)$	Özel lineer grup
$GL(n, K)$	Genel lineer grup
GL(2,Z_n)	2. Dereceden Genel Lineer Gruplar
Aut(G)	G'nin otomorfizma grubu
Inn	İç otomorfizma fonksiyonu
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

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

GİRİŞ

Eski çağlardan beri insanlar, örgütler, kurumlar ve devletler gizli bir şekilde haberleşmeye ihtiyaç duymuştur. Haberleşmelerde gizlilik, her zaman üzerinde önemle durulan bir kavram olmuştur. Gizlilikte amaç gönderilen mesajın, alıcısından başka hiç kimse tarafından anlaşılmamasıdır. Bunun içinde insanlar tarih boyunca farklı yöntemler geliştirerek gizli bir şekilde haberleşmeye çalışmıştır. Kriptoloji ise bu gizli iletişimi sağlayan şifreleme bilimidir. Kriptoloji hem mesajın alıcısına iletilmesini hem de alıcı tarafından alınan şifrelenmiş mesajın deşifre edilmesini sağlarken bu işlemler sırasında oluşan güvenlik açıkları ile de ilgilenmektedir. Kriptografi ise gizlilik sistemlerinin tasarım ve araçları ile ilgili Kriptolojinin bir parçasıdır.

Günümüz dünyasında da bilgi çağının gereği olarak şifreleme biliminin önemi gün geçtikçe artmaya devam etmektedir. Sürekli olarak yeni şifreleme yöntemleri geliştirilmekte olup bu işler için çok büyük bütçeler ayrılmaktadır. Yeni şifreleme yöntemleri bulundukça da bu sistemlerin güvenliği, uygulanabilirliği ve maliyeti de tartışılmaktadır. Yeni bulunan şifreleme sisteminin mevcut sistemlere göre artıları ve eksileri de Kriptanalistler tarafından incelenmektedir.

Şifreleme (kriptoloji) kelimesi köken olarak, Yunanca “cruptos (gizli)” ve “logos (bilim)” anlamına gelen kelimelerin birleşmesi ile meydana gelir. Şifreleme matematikle çok iç içe olup özellikle sayılar teorisi üzerine kurulmuş bir sistemdir. Günümüzde ise bilginin saklanmasını ve her türlü gizli iletişimi sağlayan kelime olarak kullanılmaktadır.

Kriptolojinin tarihi yaklaşık bundan 4000 yıl öncesine dayanır. Eski Mısırlılar şifrelemeyi kullanan ilk insanlar olarak bilinmektedir. Metnin içerisindeki bilgiyi gizleyerek okuyanın mantığını karıştırmak için kullandıkları alfabeleri vardır ve sembollerin yerini değiştirerek şifreleme yapmışlardır. Şifrelenmiş bilgi ise sadece bu karışıklığı ve yer değişikliğini bilen kişi tarafından çözülebilmektedir.
Geçmişten günümüze şifrelemenin tarihi aşağıda sunulmuştur;

M.Ö. 1900: Mısırlılar yazdığı kitabelerde standart dışı hiyeroglifler kullanmıştır. Tarihte bilinen ilk yazılı kriptografik belge bu kitabelerdir.
M.Ö. 487: Spartalılar tarafından ilk askeri kriptografik alet bulunmuştur. Sparta ordusunun askerleri Scytale adını verdikleri tahta bir sopanın etrafına şerit halinde deri ya da parşömen sararak şifreleme yapmışlardır. Karşı tarafa açık olarak giden bu şerit aynı uzunlukta bir sopaya sarıldıktan sonra gizli mesaj okunurdu. Birbirinden ayrılan harfler yeniden aynı kalınlıkta olan tahta bir sopaya sarılmadıkça hiçbir anlamı olmuyordu.

Şekil G.1.Scytale [19]

M.Ö. 100-44: Julius Ceasar 'Sezar şifrelemesi' olarak bilinen ve alfabedeki her harfin yerini kendisinden sonra gelen 3 harf kaydırmasıyla elde ettiği şifreleme metodunu devlet haberleşmesinde kullanmıştır. Kriptografinin tarihte görüldüğü ilk belirgin şifreleme örneği bu şifrelemedir.
873: Arapların filozofu olarak bilinen Al-Kindi kriptanaliz üzerine yazılmış ilk makale olan *"Kriptografik Mesajların Deşifresi"* isimli makaleyi yazmıştır.
1460: Leon Alberti tarafından şifreleme tekeri tasarlanmıştır.
1586 : Blaise de Vigenere kriptografi üzerine bir kitap yayınladı ve kendi ismi ile anılan Vigenere Şifreleme sistemini geliştirdi.
1623: Firansis Biken 5 bitlik şifrelemeyi bulmuştur.

1790: Thomas Jefferson tekerlek, disk şifresini geliştirdi ve Strip Cipher makinesini icat etti. Bu makineyi temel alan M-138-A 2.Dünya savaşında ABD donanması tarafından kullanıldı. Thomas Jefferson Amerikan kriptolojisinin öncü ismi olarak bilinir.

Şekil G.2. Jefferson Diski [20]

1854: Charles Wheatstone arkadaşı olan Lyon Playfair'in adını koyduğu playfair şifresini geliştirdi.

1859: Pelini Casa ilk sözlüğünü termografik şifrelemeye göre oluşturmuştur.

1919: Joseph Mauborgne ve Gilbert Vernam mükemmel şifreleme sistemi olan "one-time pad" i buldular.

1920-1930: William Frederick Friedman, Riverbank Laboratuarlarını kurdu, ABD için kriptoanaliz yaptı. 2. Dünya savaşında Japonlar'ın Purple Machine şifreleme sistemini çözdü.

1923: Arthur Scherbius Enigma makinasını icat etti. Almanlar Enigma makinesini geliştirerek 2. Dünya savaşında her türlü askeri bilgilerin şifrelenmesi ve deşifrelenmesi için kullandı. Enigma şifreleme cihazı 116 bitlik anahtar uzunluğuna sahipti. Bu makina İngiliz matematikçi ve kriptolog olan Alan Turing ve ekibi tarafından çözülerek savaşta İngilizlere üstünlük sağlamıştır. Savaştan sonra şifreleme sistemlerinin önemi daha da artarak bilgisayar biliminin doğmasına öncülük etmiştir.

Şekil G.3. Enigma [21]

1933: Japonlar mesajları şifrelemek için Purple makinasını icat ettiler.

1952: ABD'de resmi olarak Ulusal Güvenlik Teşkilatı (NSA) kuruldu. Dünyada en fazla matematikçiye iş fırsatı tanımasıyla ünlenen NSA, kriptografik çalışmalara önemli ölçüde yatırım yapmaktadır.

1970: Dr. Horst Feistel, Lucifer adı verilen ve veri şifreleme Standardı olan DES"in temelini oluşturan şifrelemeyi geliştirdi. DES (Data Encryption Standard) sınıflandırılmış verinin şifrelenmesinde bir standart olarak 1976 yılında ABD tarafından kabul edilmiştir.

1976: Diffie ve Hellman tarafından daha önceki şifreleme sistemlerinden farklı bir şifreleme yöntemi geliştirildi. Bu şifreleme sisteminde hem alıcının hem de gönderenin kendine özel anahtarları vardı.

1977: Ronald Rivest, Adi Shamir ve Leonard Adleman tarafından RSA şifreleme algoritması bulundu. Bu algoritma büyük asal tamsayı çarpanların bulunması mantığına dayanıyordu.

1978: RSA şifrelenmesi ilk kez ACM dergisinde yayınlanmıştır.

1981: California Santa Barbara Üniversitesinde Kriptoloji üzerine ilk konferans olan CRYPTO 81 gerçekleştirildi.
1991: RSA açık anahtar yaklaşımı kullanılarak oluşturulan ISO/IEC 9796 sayısal imza konusunda ilk uluslararası standart olmuştur. 1994'te ABD hükümeti Sayısal İmza Standartlarını belirlemiştir. Bu standartta El-Gamal açık anahtarlı şifreleme sistemi kullanılmıştır.
1994: Run Rivest RC4 şifrelemesini daha sonra RC5 şifrelemesini bulmuştur.
1995: NIST (A.B.D. Teknoloji Standartları Enstitüsü) tarafından SHA-1 özet algoritması standart olarak yayınlandı.
2009: Kriptografi konusunda dünyanın ilk olimpiyatları Belçika'nın Katholieke Üniversitesinde yapıldı.

Ülkemizde ise Orta Doğu Teknik Üniversitesinde yer alan ve 2002 yılında kurulan Uygulamalı Matematik Enstitüsüne bağlı Kriptografi anabilim dalı bulunmaktadır. 2005 yılından itibaren Orta Doğu Teknik Üniversitesi'nde Ulusal Kriptoloji Sempozyumu düzenlenmeye başlanmıştır. NSA'nın Türkiyedeki karşılığı olan Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE) şifreleme alanında önemli çalışmalar yapmaktadır.

1970'lere kadar genellikle askeri ve istihbarat alanında kullanılan şifreleme sistemleri, daha sonra insanların genel amaçları için kullanılmaya başlamıştır. Çünkü Dünyanın her tarafında bilgisayarın, telefonların ve internetin hızlı bir şekilde yaygınlaşarak insanların hayatına girmesiyle elektronik bankacılık, elektronik imza, elektronik haberleşme ve elektronik ticaret kullanılmaya başlamış, bu ise şifreleme sistemlerine olan ihtiyacı daha çok ortaya çıkararak kriptografi alanına büyük ilgi doğmasına sebep olmuştur.

1. BÖLÜM
KRİPTOLOJİ İLE İLGİLİ TEMEL TANIM VE KAVRAMLAR

1.1. Kriptoloji İle İlgili Temel Tanımlar

Tanım 1.1.1. Şifreleme bilimine kriptoloji, kriptoloji ile ilgilenen insanlara kriptograf denir.

Tanım 1.1.2. Gizli bilgilerin çeşitli metotlarla şifrelenmesini, şifrelenen bilginin güvenli bir şekilde alıcıya iletilmesini sağlayan matematiksel yöntemler bilimine kriptografi adı verilir.

Tanım 1.1.3. Kriptografik sistemlerin oluşturduğu şifreleme algoritmalarını inceleyen ve çözmeye çalışan sisteme kriptanaliz, kriptanaliz ile uğraşan kişilere kriptanalist denir.

Tanım 1.1.4. (Açık Metin) Şifrelenecek olan değişime uğramamış bilgiye Açık Metin veya Düz metin denir.

Tanım 1.1.5. (Şifreli Metin) Açık metinin çeşitli dönüşümler uygulanarak değiştirilmiş haline Şifreli Metin denir.

Tanım 1.1.6. (Şifreleme) Açık metne çeşitli dönüşümler uygulayarak farklılaştırma işlemine şifreleme denir.

Tanım 1.1.7. (Deşifreleme) Şifrelenmiş bilginin orijinal hale getirilmesine deşifreleme denir.

Tanım 1.1.8. (Anahtar) Alıcı ve gönderici tarafından bilinen, verilerin şifreleme ve deşifreleme işlemleri için kullanılan algoritmanın gizli kısmına Anahtar denir.

Tanım 1.1.9. (Açık anahtar) Şifreleme sisteminde sadece şifreleme için kullanılan deşifre etmede kullanılmayan anahtara Açık anahtar denir. Açık anahtar şifrelemenin sağladığı en önemli faydalardan biri dijital imzadır. Dijital imzalar mesajın gerçekten istenilen göndericiden geldiğini doğrulamak için kullanılır.

Tanım 1.1.10. (Gizli anahtar) Hem şifreleme işleminde hem de deşifreleme işleminde kullanılan anahtara Gizli anahtar denir. Şifreleme anahtarını bilerek deşifreleme anahtarını, deşifreleme anahtarını bilerek şifreleme anahtarını oluşturmak mümkündür. Herkesin bildiği anahtara Genel Anahtar denir.

Tanım 1.1.11. (Kriptografik Algoritma) Şifreleme ve deşifreleme işlemlerinde kullanılan matematiksel işlemlerin bütününe Kriptografik Algoritma denir.

Tanım 1.1.12. (Simetrik (Gizli) Algoritmalar) Şifreleme ve deşifreleme işlemlerinde aynı olan anahtarın kullanıldığı algoritmalara Gizli Anahtarlı Algoritma denir.

Tanım 1.1.13. (Asimetrik (Açık Anahtarlı) Algoritmalar) Şifreleme ve deşifreleme işlemleri için farklı anahtarların kullanıldığı, deşifreleme anahtarının şifreleme anahtarından elde edilemediği algoritmalara Açık Anahtarlı Algoritma denir.

Tanım 1.1.14. (Gönderici, Alıcı) Şifrelenmiş bilgiyi meşru olarak gönderen kişiye Gönderici, şifrelenmiş bilgiyi alan kişiye Alıcı denir.

Tanım 1.1.15. (Kanal) Bilginin göndericiden alıcıya iletilmesini sağlayan her türlü iletişim aracına kanal denir.

Tanım 1.1.16. (Saldırgan) Alıcı ve gönderici arasındaki haberleşmede, alan veya gönderen kişi olmayan, güvenliği bozarak bilgi etmeye çalışan kimse Saldırgandır.

Tanım 1.1.17. (Saldırı) Yapılan bir kriptosistemin tamamını veya bir kısmını kırabilmek için düzenlenen olumlu veya olumsuz bir eylem Saldırı olarak adlandırılır.

Tanım 1.1.18. (Veri Bütünlüğü) İletilecek mesajın göndericiden alıcıya gidene kadar bilerek veya istenmeyerek değiştirilmesinin engellemesine Veri Bütünlüğü denir.

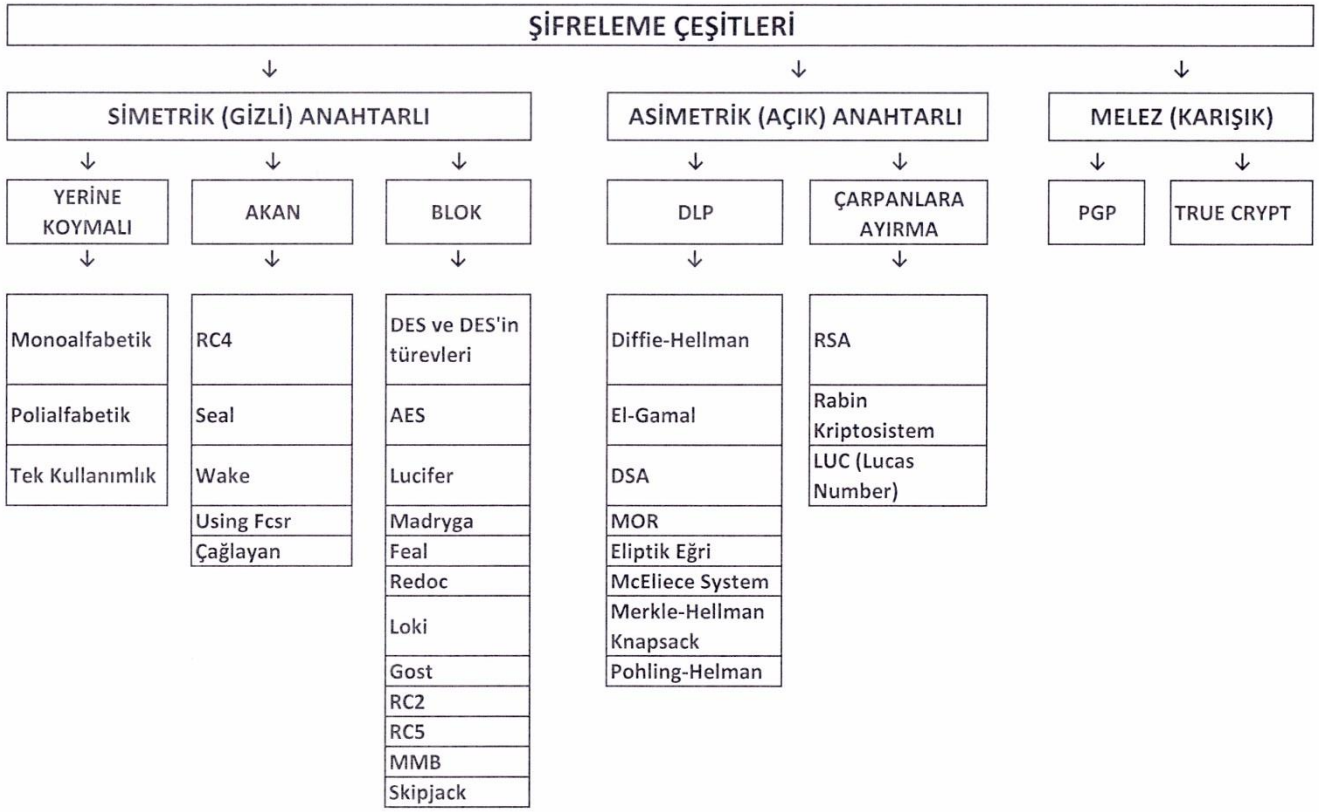
Tanım 1.1.19. (Kimlik Tanımlama ve Doğrulama) Kimlik tanımlama, bir sisteme kişinin kimliği tanıtıldıktan sonra, sistemin bu kişinin kimliğini tespit etmesidir. Kimlik doğrulama ise, sisteme giriş yapan kişinin, sisteme girerken kullandığı kimliğin kendine ait olup olmamasını denetleyen mekanizmadır.

1.2. Şifreleme Sisteminin Sağlaması Gereken Temel Özellikler

1. Şifrelenmiş mesaj, deşifre edildiğinde bilgi kaybı olmamalıdır.
2. Şifrelenmiş mesaj ile düz metin arasındaki ilişki zor kurulmalıdır.
3. Şifreleme algoritmaları farkı türdeki bilgileri güvenli olarak sisteme işleyebilmelidir.
4. Şifreleme işlemleri basitçe ve kolaylıkla gerçekleştirilebilmelidir.
5. Şifreleme işlemlerinde güvenlik seviyesi mümkün olduğunca yüksek düzeyde olmalıdır.
6. Verimi düşürecek, işgücü ve maliyeti çoğaltacak yaklaşımlar içermemelidir.
7. Şifreleme yaklaşımları, açıklarının ortaya çıkarılabilmesi ve daha da geliştirilebilmesi için mümkün olduğunca geniş bir platformda test edilebilmelidir.

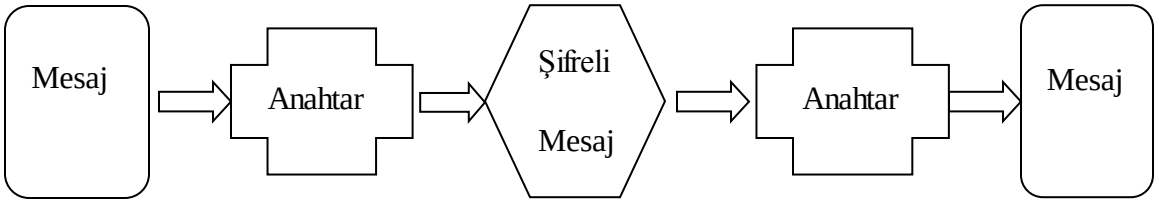
1.3. Şifreleme Çeşitleri

Şifreleme yöntemleri simetrik, asimetrik ve karışık şifrelemeler olarak üç ana kola ayrılır. Bu kısımda şifreleme yöntemlerinin özellikleri açıklanarak karşılaştırması yapılacaktır. İlerde kullanacağımız şifreleme sistemine örnek olması amacıyla açık anahtarlı şifreleme yöntemlerinden El-Gamal, RSA ve Rabin Kriptosisteminin mantığı incelecektir. Şifreleme çeşitleri aşağıdaki gibidir.



Tablo 1.1. Şifreleme Çeşitleri

1.3.1. Gizli Anahtarlı (Simetrik) Kriptosistemler



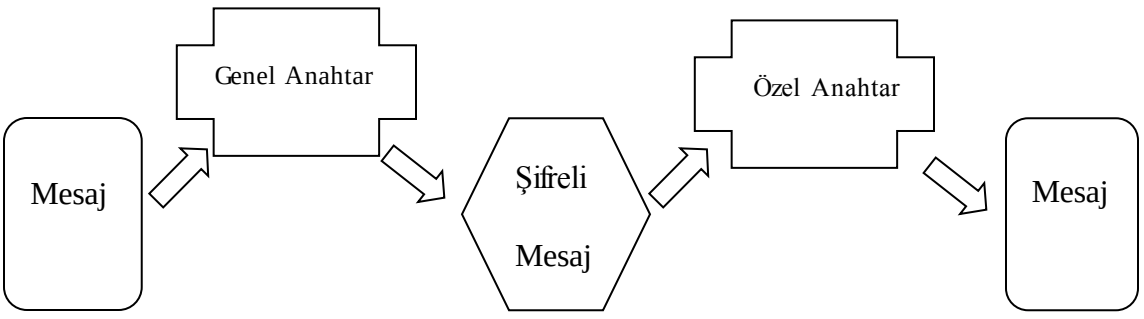
Şekil 1.1. Simetrik (gizli) anahtarlı şifreleme

Bu tip sistemlerin en belirgin özelliği şifreleme ve deşifreleme işlemleri için aynı anahtarın kullanılmasıdır. Şifreleme ve deşifreleme işlemlerinde aynı anahtar kullanıldığından, tarafların belirlediği ortak anahtarın diğer alıcıların eline geçmesi durumunda mesajlaşmanın gizliliği ortadan kalkar ve saldırgan kişiler kolaylıkla mesajı çözebilirler. Bu yüzden gönderici ve alıcının, anahtarın diğer kişilerin eline geçme ihtimalini göz önünde bulundurarak, ortak bir anahtar üzerinde karar vermeleri gerekir.

Bu kriptografide zor olmayan şifreleme algoritmaları kullanılır. Hızlı ve kolay uygulanabilir olması sistemin avantajlarındandır. Simetrik şifrelemenin zayıf yönü ise tarafların belirlediği ortak anahtarın, saldırgan kişilere karşı korunmasının zorluğudur.

Günümüzde kullanılan DES (Data Encryption Standart) ve AES simetrik şifreleme sistemlerindendir.

1.3.2. Açık Anahtarlı (Asimetrik) Kriptosistemler



Şekil 1.2. Asimetrik (açık) anahtarlı şifreleme

Simetrik şifrelemede tek bir anahtar varken, asimetrik şifrelemenin bulunması ile gönderici ve alıcının birbirinden farklı anahtarı olmuş bu ise anahtarın saldırganlar tarafından ele geçirildiğinde mesajın deşifre edilme ihtimalini oldukça düşürmüştür.

Bu şifreleme sisteminde gönderici ve alıcının iki farklı anahtarı vardır. Bu anahtarlar genel ve özel anahtar olarak adlandırılır. Bu anahtarların matematiksel olarak birbirleriyle ilişkisi yoktur. Genel ve özel anahtardan birini kullanarak diğer anahtarı elde etmek çok daha zordur.

Şifreleme ve deşifreleme işlemleri için tarafların kendilerinin belirlediği özel anahtarlar kullanıldığından dolayı simetrik şifrelemede ki gibi gizli anahtarın karşı tarafa iletilmesine gerek kalmamıştır. Gizli anahtarın karşı tarafa iletilmesine gerek kalmadığı için sistem oldukça güvenli hale gelmiştir.

Bu sistemin en büyük faydası, daha önceden birbirlerini tanımayan kişiler arasında da mesajların güvenli olarak iletilmesini sağlamasıdır. Sistemin tek zayıf yönü açık anahtarı kullanan kişinin ve anahtar sahibinin doğru şekilde eşleştirilmesidir.

Asimetrik algoritmalara örnek olarak, RSA, Diffie-Hellman, El Gamal ve Mor Kriptosistem verilebilir.

1.3.2.1. 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 ayrık logaritma probleminin (DLP) zorluğuna dayanır.

Anahtar Üretimi:

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

a) Rastgele bir p asal sayısı ve $mod\ p$ ye göre tamsayıların oluşturduğu çarpım grubu Z_p^* nin bir üreteci β'yı oluşturur.

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

c) A'nın açık anahtarı (p, β, β^a) ve A'nın gizli anahtarı ise a olur.

Şifreleme:

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

a) A'nın açık anahtarını (p, β, β^a)alır.

b) Mesajı $\{0,1,\ldots,p\text{-}1\}$ aralığında m tamsayısı olarak ifade eder.

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

d) $\gamma = \beta^k mod p$ ve $\delta = m.(\beta^a)^k mod p$ değerlerini hesaplar.

e) Son olarak $F = (\gamma, \delta)$ kapalı metnini A'ya gönderir.

Deşifreleme:

F kapalı metninden m açık metine ulaşmak için A şunları yapar:

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

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

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

El- Gamal Kriptosistem Örneği

Anahtar Üretimi

a) B şahsı rastgele bir asal sayı p=29 ve mod 29 a göre tamsayıların oluşturduğu çarpım grubu Z_p^* nin bir üreteci olarak 2 yi seçer.

b) $1 \leq a \leq$ p-2 şeklinde olan bir a tamsayısını 10 seçer. $\beta^a \ mod\ p$ değerini hesaplar.

$\beta^a = 2^{10} = 9(29)$

c) B'nin açık anahtarı ve (29, 2, 9) ve gizli anahtarı ise 10 olur.

Şifreleme

A şahsı B için $m=R$ mesajını şifrelemek istesin. A mesajı şifreleme için şunları yapar:

a) A'nın açık anahtarını (29, 2, 9) olur.

b) $m=R$ mesajını $\{0, 1, \ldots, 28\}$arasında bir sayı ile ifade eder. Yani $m=R=20$ dir.

c) $1 \leq k \leq 27$ 'yi sağlayan rastgele bir k tamsayısını 2 olarak seçer.

d) $\gamma = \beta^k = 2^2 = 4(29)$ ve $\delta = m.(\beta^a)^k mod p = 20.9^2 = 25(29)$

e) Son olarak $F = (\gamma, \delta)=(4,25)$ metnini B ye gönderir.

Deşifreleme

a) $\gamma^{-a} = 4^{-10} \equiv 4^{-18} \equiv 24(29)$gizli anahtarıyla $\gamma^{p-1-a} = \beta^{p-1-ak} mod\ p$'yi kullanarak $\gamma^{-a} mod\ p$ değerini hesaplar. ($\gamma^{p-1-a} = \gamma^{-a} = \beta^{-ak}$)olur.

b) $m=\gamma^{-a}.\delta = 24.25 \equiv 20(\ mod\ 29)$ elde edilir. 20 sayısının harf olan karşılığı R harfi olup, deşifreleme işlemi yapılmış olur.

1.3.2.2. RSA Kriptosistemi

Adını Ronald Rivest, Adi Shamir, Leonard Adleman'ın isimlerinin baş harflerinden almıştır. Günümüzde en çok kullanılan açık anahtar şifrelemelerindendir. RSA asimetrik şifrelemede ve dijital imzalarda kullanılır. Bu sistemde kullanılan anahtar ne kadar uzun olursa, şifreleme sisteminin o kadar güvenli olacağı düşünülür. RSA çok büyük asal sayıları oluşturmanın kolaylığına karşın, bu büyük sayıların asal bileşenlerinin bulunmasının zorluğuna dayanmaktadır. Bu sistemde herkese açık bir anahtarla şifreleme işlemi yapılır ve kişilerin şifrelenmiş mesajı okuyabilmesi için kendilerine ait özel anahtarı vardır.

Anahtar Üretimi:

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 $\Phi(n) = (p-1).(q-1)$ değerini hesaplar.

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

d) $e.d \equiv 1 \ (mod\ \Phi(n))$ sağlayacak ve $1 < d < \Phi(n)$ aralığında d değeri hesaplanır.

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

Şifreleme:

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 $[0,n-1]$ aralığında yazar.

c) Sonra $c \equiv m^e (mod\ n)$ değerini hesaplar.

d) Oluşan c şifresini A'ya gönderir.

Deşifreleme:

A şahsı d gizli anahtarını kullanarak ve $m \equiv c^d (mod\ n)$ 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.

RSA Kriptosistem Örneği

Anahtar Üretimi

A şahsı anahtarını şu şekilde oluşturur:

a) İki tane farklı rastgele asal sayıları olarak p=7 ve q=19 seçer.

b) $n = p.q$= 7.19=133 ve $\Phi(n) = (p-1).(q-1)$=6.18=108 değerini hesaplar.

c) $2 < e < \Phi(n)$=108 ve $(\Phi(n), e) = (108, e) = 1$ olacak şekilde bir e tamsayısını 5 olarak seçer.

d) $e.d \equiv 1 \pmod{\Phi(n)}$ sağlayacak ve $1 < d < \Phi(n)$=108 aralığındaki d değeri;

$5.d \equiv 1 \pmod{108}$, d=65(108) olarak bulunur.

e) A'nın açık anahtarı (n, e)=(133,5) ve özel anahtarı d=65 tir.

Şifreleme

B şahsı, A'ya bir m=15 mesajını göndermek istiyor. B, m mesajını şifrelemek için şunları yapar:

a) Öncelikle A'nın açık anahtarı (n,e)=(133,5) alır.

b) m=15 mesajını $[0,n-1]$=[0,132] aralığında yazar.

c) Sonra $c \equiv m^e (mod\ n)$= 15^5(133)=78(133) olarak hesaplar.

d) Bulduğu c şifresini A ya gönderir.

Deşifreleme

A şahsı d=65 gizli anahtarını kullanarak ve $m \equiv c^d (mod\ n)$ işlemini uygulayarak $m \equiv 78^{65} (mod\ 133)$ işlemini yaparak m açık metnini m=15(133) olarak bulur.

1.3.2.3. Rabin Kriptosistemi

1979 yılında Michael O. Rabin tarafından keşfedilen bir kriptosistemdir. RSA Kriptosistemin farklı bir şeklidir. Bu sistemin güvenliği büyük sayıların asal çarpanlarına ayrılmasının zorluğundan kaynaklanır. Deşifreleme aşamasında bir doğru sonucun yanında üç tane yanlış sonuç ürettiğinden dolayı pek kullanılmamaktadır.

Anahtar Üretimi:

a) Rastgele iki tane büyük p ve q asal sayıları seçilir.

b) $n=p.q$ hesaplanır.

c) n açık anahtar, (p, q) gizli anahtardır.

Şifreleme:

a) Şifrelenecek m metni seçilir.

b) Şifrelenecek olan m metni $[0, n-1]$ aralığındaki herhangi bir sayı ile ifade edilir.

c) $c=m^2 \pmod{n}$ hesaplanarak şifrelenmiş metin oluşturulur.

Deşifreleme:

a) $m_p=\sqrt{c} \bmod p$ ve $m_q=\sqrt{c} \bmod q$ hesaplanır.

b) $y_p.p+ y_q.q = 1$ olacak şekilde $y_p$ve $y_q$bulunur.

c)Aşağıdaki işlemler yapıldıktan sonra $r, -r, s$ ve $-s$ olmak üzere 4 tane kök bulunur.

$r = (y_p.p.m_q+y_q.q.m_p) \pmod{n}$

$-r=n- r \pmod{n}$

$s = (y_p.p.m_q - y_q.q.m_p) \pmod{n}$

$-s =n– s \pmod{n}$

Bulunan köklerden sadece bir tanesi şifrelenmiş metindir.

Rabin Kriptosistem Örneği

Anahtar Üretimi

a) $p=7$ ve $q=11$ seçilir.

b) $n = p.q= 7.11=77$

c) $n = p.q= 7.11=77$ açık anahtar, $(p, q)= (7,11)$ gizli anahtardır.

Şifreleme

a) Şifrelenecek olan mesajı, m=20 olarak seçilsin.

b) m=20 mesajı, [0,77-1]=[0,76] aralığındadır.

c) Sonra $c=m^2 \pmod{n}$ hesaplanır.

$c=20^2 (\text{mod}77) \equiv 400 \ (\text{mod}77) \equiv 15 (\text{mod}77)$ şifreli metin oluşturuldu.

Deşifreleme

a) $m_p=\sqrt{c} \ \text{mod} \ p \rightarrow m_7=\sqrt{20^2}=20 \equiv 6 \ (\text{mod} \ 7)$

$m_q=\sqrt{c} \ \text{mod} \ q \ \rightarrow \ m_{11}=\sqrt{20^2}=20 \equiv 9 \ (\text{mod} \ 11)$

b) $y_p.p + y_q.q = 1$ olacak şekilde $y_p$ve $y_q$bulunur.

$y_7.7 + y_{11}.11 = 1$

(7,11)=1/1 olduğundan çözülebilirdir.

11=7.1+4

7=4.1+3

4=3.1+**1**

3=1.3+0

1=4-1.3

=4-1(7-1.4)

=2.4 + (-1).7

=2.(11-1.7) + (-1).7

=(-3).7 +(2) .11

↓ ↓

y_7 y_{11}

y_7=-3 ve y_{11}=2 olarak bulunur.

c) $r = (y_p.p.m_q + y_q.q.m_{\boldsymbol{p}}) \pmod{n}$

$= (y_7.7.m_{11} + y_{11}.11.m_{\boldsymbol{7}}) \pmod{77}$

$= (-3.7.9 + 2.11.6) \pmod{77}$

$= (-189 + 132) \pmod{77}$

$= -57 \pmod{77}$

$= \mathbf{20} \pmod{77}$

$-r = n - r \pmod{n}$

$= 77-20 \pmod{77}$

$= 57 \pmod{77}$

$s = (y_p.p.m_q - y_q.q.m_{\boldsymbol{p}}) \pmod{n}$

$= (y_7.7.m_{11} - y_{11}.11.m_{\boldsymbol{7}}) \pmod{77}$

$= (-3.7.9 - 2.11.6) \pmod{77}$

$= (-189 - 132) \pmod{77}$

$= -321 \pmod{77}$

$= -13 \equiv 64 \pmod{77}$

$-s = n - s \pmod{n}$

$= 77-64 \pmod{77}$

$= 13 \pmod{77}$

Bulduğumuz 4 tane kökten sadece bir tanesi şifrelenmiş olduğumuz metindir.

1.3.3. Simetrik ve Asimetrik Şifreleme Sistemlerinin Karşılaştırması

1950'li yıllara kadar genellikle simetrik algoritmalar kullanılıyorken, bu tarihten sonra asimetrik algoritmalar daha çok kullanılmaya başlamıştır. Çağımızda kullanılan şifreleme sistemlerinde hem simetrik hem de asimetrik şifrelemelerden yararlanılmaktadır. Bu sistemlerin güçlü ve zayıf yanlarını şöyle sıralayabiliriz;

1. Güvenlik boyutu düşünüldüğünde simetrik şifrelemede anahtarın sürekli olarak değişmesi gerekir. Asimetrik şifrelemede kullanılan anahtarların uzun süre değiştirilmesine gerek kalmayabilir.

2. Simetrik şifrelemeler, asimetrik şifrelemelere göre çok daha hızlı çalışır.

3. Anahtar uzunluğu simetrik şifrelemelerde kısa, asimetrik şifrelemeler de uzundur.

4. Simetrik şifrelemede kullanılan anahtarın karşı tarafa iletilmesi gerekirken, asimetrik şifrelemelerde gizli anahtarın iletilmesi gerekmez.

5. Asimetrik şifreleme yöntemiyle şifrelenmiş bir bilgiyi aynı anda farklı kullanıcılara göndermek için aynı bilginin her alıcı için ayrı ayrı şifrelenmesi gerekir. Bu ise sisteme fazladan yük getirmektedir.

2. BÖLÜM
MATRİSLER VE GENEL LİNEER GRUPLAR

Bu bölümde öncelikle Matrisler ve Genel Lineer Gruplar hakkında temel matematiksel kavramlardan bahsedilecektir. Bunun için genellikle Altındiş [1], Majid [3] ve Öztürkmenoğlu [4] kaynaklarından yararlanılmıştır.

2.1. Temel Kavramlar

Tanım 2.1.1. Bir ve kendisinden başka pozitif böleni olmayan 1 den büyük olan doğal sayılara asal sayı denir.

Tanım 2.1.2. (a,b)=1 ve $a, b \in \mathbb{Z}$ ise a ve b sayılarına aralarında asal sayılar denir.

Tanım 2.1.3. t, sıfırdan büyük pozitif tamsayı olmak üzere t ile aralarında asal olan pozitif tamsayıların sayısını veren fonksiyona Eulerin $\emptyset$ fonksiyonu denir ve $\emptyset(t)$ile gösterilir.

Tanım 2.1.4. m tane satır ve n tane sütun oluşturacak biçimde dizilmiş $m.n$ tane sayının oluşturduğu tabloya bir $m\times n$ matris denir. Bir $m\times n$ matris olan A genellikle aşağıdaki gibi gösterilir.

$$A=\begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix}$$

veya $A = [a_{ij}]$, $1 \leq i \leq m$; $1 \leq j \leq n$.

Tanım 2.1.5. Matrisler için dört işlem (toplama, çıkarma, çarpma ve skaler çarpım) tanımlanmıştır. Farklı boyutlarda olan iki matrisin çarpılabilmesi için, ilk matrisin sütun sayısı ile ikinci matrisin satır sayısının aynı olması gerekir.

Tanım 2.1.6. Bir matris ile bir skalerin çarpımı, matrisin her elemanının o skalerle çarpılmasıyla oluşan matristir.

Örnek 2.1.7. $a\begin{bmatrix} p & q \\ r & s \end{bmatrix}=\begin{bmatrix} ap & aq \\ ar & as \end{bmatrix}$

Örnek 2.1.8. $3\begin{bmatrix} 2 & -1 \\ 4 & 5 \end{bmatrix}=\begin{bmatrix} 6 & -3 \\ 12 & 15 \end{bmatrix}$

Tanım 2.1.9. $m\times m$ boyutlu bir A kare matrisinin determinantı, det(A) veya $|A|$ olarak ifade edilir.

$A=\begin{bmatrix} a & b \\ c & d \end{bmatrix} \Rightarrow |A|=\begin{bmatrix} a & b \\ c & d \end{bmatrix} = ad-bc$ şeklinde hesaplanır.

Örnek 2.1.10. $A=\begin{bmatrix} 5 & 3 \\ 2 & 6 \end{bmatrix} \Rightarrow |A|=\begin{bmatrix} 5 & 3 \\ 2 & 6 \end{bmatrix}$ =5.6-3.2=30-6=24

Tanım 2.1.11. Determinantı sıfırdan farklı bir A kare matrisi ve I birim matris olmak üzere $AxB=BxA=I$ şartını sağlayan B matrisine A matrisinin tersi denir ve $B=A^{-1}$ olarak gösterilir.

Tanım 2.1.12. m pozitif bir tamsayı ve $m|a-b$ ise a sayısı b sayısına m modülüne göre kongrüentir (denktir) denir ve bu durum $a \equiv b \pmod{m}$ ile gösterilir.

Tanım 2.1.13. A ve B iki küme f, A dan B ye bir bağıntı olmak üzere $\forall\, a\in A$ için, f bağıntısı ile bağlı B de bir ve yalnız bir eleman bulunabiliyorsa, f ye A dan B ye bir fonksiyon denir ve $f: A \rightarrow B$ ile gösterilir.

Tanım 2.1.14. f ve g, A dan B ye iki fonksiyon olmak üzere a_1, $a_2 \in A$ için, $f(a_1)= f(a_2)$ olması $a_1= a_2$ olmasını gerektiriyorsa, f ye birebirdir (veya 1-1) denir.

Tanım 2.1.15. f, A'dan B'ye bir fonksiyon olsun. O halde $f(A) = \{ f(a): a\in A\}$ olarak tanımlanır. Buradaki $f(A)$ 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.
f'in 1-1 ve örten olması halinde f^{-1} dönüşümüne, f dönüşümünün tersi denir.
Yani $f: A \to B$ 1-1 ve örten ise, $f^{-1}: B \to A$ dönüşümü $a \in A$ ve $b \in B$ için $a = f^{-1}(b) \Leftrightarrow b = f(a)$ olarak tanımlanır ve $f^{-1}(B) = \{ a \in A: f(a) \in B \}$'dir.

Tanım 2.1.16. G boş olmayan bir küme ve $*$ da G üzerinde tanımlı bir ikili işlem olsun. Aşağıdaki şartları sağlayan $(G, *)$ sistemine bir grup denir.

(i) $\forall a, b \in G$ için $a*b \in G$'dir (kapalılık özelliği).
(ii) $\forall a, b, c \in G$ için $(a*b)*c = a*(b*c)$ dir (birleşme özelliği).
(iii) $\forall a \in G$ için $a*e = e*a = a$ olacak şekilde bir $e \in G$ vardır (birim eleman özelliği).
(iv) $\forall a \in G$ için $a*b = b*a = e$ olacak şekilde bir $b \in G$ vardır (ters eleman özelliği).

Tanım 2.1.17. $(G, *)$ bir grup ve $\forall a, b \in G$ için $(a*b) = (b*a)$ değişme özelliği sağlanıyorsa bu gruba abelyan (değişmeli) grup denir.

Tanım 2.1.18. G bir grup ve H da 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 2.1.19. $f: G \to H$ bir fonksiyon ve (G, o) ve $(H, ¤)$ herhangi iki grup olmak üzere $\forall a, b \in G$ için $f(aob) = f(a) ¤ f(b)$ oluyorsa, f'e G'den H'a bir homomorfizma denir. Homomorfizma aynı zamanda işlemleri koruyan bir dönüşümdür.
Tanım 2.1.20. $f: G \to H$ grup homomorfizması olsun. Eğer bu homomorfizma birebir ve örten ise f ye bir izomorfizma denir. G'den H'ye bir izomorfizma tanımlanıyorsa G ve H gruplarına izomorfiktirler ya da eş yapılıdırlar denir ve $G \cong H$ ile gösterilir.

Tanım 2.1.21. Bir G grubundan kendi üzerine tanımlanan bir izomorfizmaya G'nin bir otomorfizması denir.

Tanım 2.1.22. 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.

Tanım 2.1.23. (Halka) Boştan farklı bir R cümlesinde '+' ve '$*$' işlemleri tanımlansın. Aşağıdaki şartları sağlayan $(R, +, *)$ cebirsel yapısına halka denir.

i) $(R, +)$ bir değişmeli grup

ii) '$*$'ın birleşme özelliği var

iii) '$*$'ın'+' üzerine soldan ve sağdan dağılma özellikleri var

Ayrıca '$*$' işlemi değişmeli ise halkaya değişmeli halka, birimli ise halkaya birimli halka denir.

Tanım 2.1.24. (Cisim) Birimli ve değişmeli olan bir F halkasındaki sıfırdan farklı her elemanın çarpma işlemine göre bir tersi varsa, F'ye bir Cisim denir.

Tanım 2.1.25. K bir cisim olmak üzere $GL(n,K) = \{A \in M(n \times n, K) | \det(A) \neq 0\}$ grubuna genel lineer grup denir.

Tanım 2.1.26. $SL(n,K) = \{A \in M(n \times n, K) | \det(A) = 1\}$ grubuna özel lineer grup denir.

3. BÖLÜM
GENEL LİNEER GRUPLAR KULLANILARAK YAPILAN KRİPTOSİSTEM

Bu bölümde Genel Lineer Gruplar hakkında temel bilgiler verilmiş, bu gruplar kullanılarak yapılan kriptosistemin mantığı açıklanıp örneklerle detaylandırılarak sistemin nasıl çalıştığı anlatılmıştır. Bunun için genellikle Majid [3] kaynağından yararlanılmıştır.

Bu grupları kullanarak yapılan şifrelemelerde İngiliz alfabesi kullanıldığından, İngiliz alfabesindeki harflerin sayılara karşılık gelen tablosu aşağıda verilmiştir.

Harf	A	B	C	D	E	F	G	H	I	J	K	L	M	N
Sayı	0	1	2	3	4	5	6	7	8	9	10	11	12	13
Harf	O	P	Q	R	S	T	U	V	W	X	Y	Z		
Sayı	14	15	16	17	18	19	20	21	22	23	24	25		

Tablo 3.1. İngiliz alfabesinin sayısal değerleri

3.1. Genel Lineer Grubun Alt Grubu

H alt grubu derecesi 2 olan Genel Lineer Gruplar arasındadır. $GL(2,\mathbb{Z}_n)$ aşağıdaki gibi tanımlanır.

$$H=\begin{pmatrix} a_1 & b_1 \\ b_1 & a_1 \end{pmatrix}, a_1, b_1 \in \mathbb{Z}_n \text{ve } a_1^2\text{-}b_1^2 \neq 0$$

H alt grubunun bu elemanları $\mathbb{Z}_n$ halkasının $\mathbb{Z}_n^*$ birim grubuna aittir. Bu H alt grubunun $GL(2,\mathbb{Z}_n)$ alt grubunun, bir abeliyan grubu olduğu kolayca doğrulanabilir.

1) $H_1=\begin{pmatrix} a_1 & b_1 \\ b_1 & a_1 \end{pmatrix}$, $H_2=\begin{pmatrix} c_1 & d_1 \\ d_1 & c_1 \end{pmatrix} \in H$

$H_1H_2 \in H$ olduğunu göstermek zorundayız. Şimdi her iki matrisi de çarpalım.

$$M=H_1H_2=\begin{pmatrix} a_1c_1+\ b_1d_1 & a_1d_1+\ b_1c_1 \\ a_1d_1+\ b_1c_1 & a_1c_1+\ b_1d_1 \end{pmatrix},$$

$\det(H_1H_2)=\det(H_1)\det(H_2) \in \mathbb{Z}_n^*$ dolayısıyla kapalıdır.

2) $H_1=\begin{pmatrix} a_1 & b_1 \\ b_1 & a_1 \end{pmatrix} \in H,\ det(H_1)=\mu \in \mathbb{Z}_n^*$, biliyoruz ki $H_1^{-1} \in H$, çünkü

$H_1^{-1}=\begin{pmatrix} \mu^{-1}a_1 & -\mu^{-1}b_1 \\ -\mu^{-1}b_1 & \mu^{-1}a_1 \end{pmatrix}$, $\det(H_1^{-1})=\mu^{-1} \in \mathbb{Z}_n^*$ olduğundan her elemanın tersi mevcuttur.

3) $H_1=\begin{pmatrix} a_1 & b_1 \\ b_1 & a_1 \end{pmatrix}$, $H_2=\begin{pmatrix} c_1 & d_1 \\ d_1 & c_1 \end{pmatrix} \in H$ olmak üzere komutatif olması için $H_1H_2=H_2H_1$ olmalıdır.

$$H_1H_2=\begin{pmatrix} a_1c_1+\ b_1d_1 & a_1d_1+\ b_1c_1 \\ a_1d_1+\ b_1c_1 & a_1c_1+\ b_1d_1 \end{pmatrix}$$

$$=\begin{pmatrix} c_1\,a_1+d_1b_1 & c_1b_1+d_1a_1 \\ c_1b_1+d_1a_1 & c_1\,a_1+d_1b_1 \end{pmatrix}$$

$$=H_2H_1$$

olur ki bu durumda komutatif alt grubu elde edilmiş olur.

$\mathbb{Z}_n$ halkasının rastgele elemanları a ve b olsun. $M_2(\mathbb{Z}_n^*)$ halkasında bu elamanlara karşılık gelen matris M olmak üzere, M'nin H grubu içinde olma olasılığı nedir ? Biz bu duruma n'nin iki değerine göre cevap vermeye çalışacağız.

1.Durum

r ve s asal sayı ve $n=rs$ ise;

$\mathbb{Z}_n$ halkasının eleman sayısı ve tersinir elemanlarının sayısı aşağıdaki gibi olur.

$$|\mathbb{Z}_n|=rs,\ \varphi(\mathbb{Z}_n)=\varphi(n)=(r\text{-}1)(s\text{-}1)$$

M matrisinin H grubunda olmama olasılığı P ise bu değer aşağıdaki gibi bulunabilir.

$$P = 1\text{-}\frac{\varphi(n)}{n} = 1\text{-}\frac{(r-1)(s-1)}{rs} = \frac{1}{r}+\frac{1}{s}\text{-}\frac{1}{rs}$$

p ve q asallarının bit uzunluğu 90 'na eşit ya da daha büyük ise bu taktirde;

$$P \leq 2^{-89}$$

olasılığına sahip olur.

2. Durum

r asal ve $l \geq 2$ olmak üzere $n=r^l$, ise bu durumda $\mathbb{Z}_n$ halkasının eleman sayısı ve tersinir elemanlarının sayısı aşağıdaki gibi olur.

$$|\mathbb{Z}_n|=r^l,\ \varphi(\mathbb{Z}_n)=\varphi(n)=r^{l-1}(r-1).$$

Yukardakine benzer olarak M matrisinin H grubunda olmama olasılığı P ise bu değer aşağıdaki gibi bulunabilir.

$$P = 1-\frac{\varphi(n)}{n} = 1-\frac{r^{l-1}(r-1)}{r^l} = \frac{1}{r}$$

p ve q asallarının bit uzunluğu 90 'na eşit ya da daha büyük ise bu taktirde;

$$P \leq 2^{-90}$$

olasılığına sahip olur. Her iki durumda da olasılık ihmal edilebilir düzeyde olduğundan rastgele $\mathbb{Z}_n$ üzerindeki M matrisi H alt grubundadır.

3.2. İkinci Dereceden Genel Lineer Gruplar

Bu bölümde önceki kısımda açıklanan iki duruma bağlı olarak iki farklı Kriptosistem incelenmiştir. Tartışılan iki kriptosistemin, ayrıntılı olarak anahtar üretimi, şifreleme ve deşifreleme algoritmaları yapılarak sistemlerin algoritmaları detaylı olarak ele alınmıştır.

3.2.1. Birinci Kriptosistem

Anahtar Üretimi:

A şahsı aşağıdakilerini yapar:

1. $n=rs$ veya $n=r^l$ olacak şekilde r ve s asal sayılarını seçer($r \neq s$, $l \geq 2$)

2. Rastgele dört tam sayı a, b, c ve $d \in \mathbb{Z}_n$ seçer.

3. 2. Adımda seçilen dört tam sayıdan iki matris üretir.

$$A=\begin{pmatrix} a & b \\ b & a \end{pmatrix},\quad B=\begin{pmatrix} c & d \\ d & c \end{pmatrix}.$$

4. Rastgele seçilen üyeler H grubunda ise devam eder, değilse 2. adıma tekrar döner.

5. $M_2(\mathbb{Z}_n)$ halkasında 2 tane komutatif iç otomorfizma tanımlar. Bu otomorfizmalar

$A \in M_2(Z_n)$, A ve B matrisleri H'ın elemanları olmak üzere,

$f: V \to A^{-1}VA$, $g: V \to B^{-1}VB$ şeklinde tanımlar.

6. $M_2(\mathbb{Z}_n)$ halkasında tanımlı aşağıdaki otomorfizmaları oluşturur.

$\rho = f^2 g$, $\sigma = fg^2$,

$\rho: V \to (A^2B)^{-1})V(A^2B)$, $\sigma: V \to (AB^2)^{-1}V(AB^2)$

Buradaki ρ ve σ otomorfizmaları $\rho = fg^{-1}\sigma$, $\sigma = f^{-1}g\rho$ eşitliklerini de sağlar.

7. $GL(2,\mathbb{Z}_n)'$den H grubuna ait olmayan rastgele tersinir bir N matrisi seçer.

8. N^{-1},$\rho(N)$ *ve* $\sigma(N^{-1})$ matrislerini hesaplar.

9. Dolayısıyla açık anahtarı (n, $\rho(N)$, $\sigma(N^{-1})$), özel anahtarı ise (A,B) şeklinde olur.

Şifreleme:

B şahsı sırayla aşağıdakileri yapar:

1. $\mathbb{Z}_n$ halkası üzerinde 2x2'lik matrisler bir dizisi olarak m açık metnini oluşturur.

$m^{(1)}, m^{(2)}, m^{(3)}, \ldots, m^{(k)}$.

2. $\forall m^{(i)}$, ($i=1,2,\ldots,k$) mesajı için H grubundan rastgele bir $X^{(i)}$ matrisini seçer.

3. $\forall i=1,2,\ldots,k$ için $\vartheta^{(i)}: V \to (X^{(i)})^{-1}V(X^{(i)})$, $V \in M_2(\mathbb{Z}_n)$ otomorfizmasını tanımlar.

4. $\forall i=1,2,\ldots,k$ için $\vartheta^{(i)}(\rho(N))$, $\vartheta^{(i)}\left(\sigma(N^{-1})\right)$ ve $m^{(i)}\vartheta^{(i)}\left(\rho(N)\right)$ matrislerini hesaplar.

5. $\forall i=1,2,\ldots,k$ için rastgele tersinir $\mu \in \mathbb{Z}_n$ seçer ve metnini aşağıdaki şekilde şifreler:

$C=(C^{(1)}, C^{(2)}, \ldots, C^{(k)})$ $\quad C^{(i)}=(C_1^{(i)}, C_2^{(i)})$

$C_1^{(i)} = \mu_i^{-1}\vartheta^{(i)}(\sigma(N^{-1}))$, $\quad C_2^{(i)} = \mu_i m^{(i)}\vartheta^{(i)}(\rho(N))$.

Deşifreleme:

A şahsı aşağıda verilen adımları takip ederek şifrelenmiş mesajı deşifre eder.

1. Belirlediği özel anahtarı kullanarak $\forall i=1,2,\ldots,k$ için,

$d^{(i)} = f^{-1}g(C_1^{(i)}) = f^{-1}g(\mu_i^{-1}\vartheta^{(i)}(\sigma(N^{-1}))$ değerini hesaplar.

2. $\forall i=1,2,\ldots,k$ için, $m^{(i)} = C_2^{(i)}d^{(i)} = (\mu_i m^{(i)}\vartheta^{(i)}(\rho(N))d^{(i)}$ matrislerini hesaplar

3. Son olarak $m^{(1)}, m^{(2)}, m^{(3)}, \ldots, m^{(i)}$ matris dizilerinden faydalanarak orijinal mesajı elde eder.

3.2.2. İkinci Kriptosistem

Anahtar Üretimi:

A şahsı aşağıdaki adımları izler:

1. Rastgele p ve q asal sayılarını seçer öyle ki $p \neq q$ ve $n=pq$ hesaplar veya $n=p^r$, $r \geq 2$

2. Rastgele bir $D \in GL(2,\mathbb{Z}_n)$ matrisi seçer.

3. Aşağıdaki matrisleri hesaplar.

$I=D^2$, $J=D^3$, I^2J ve IJ^2

4. Rastgele bir $N \in GL(2,\mathbb{Z}_n)$ matrisi seçer.

5. $\forall V \in M_2(\mathbb{Z}_n)$ matrisi için aşağıdaki otomorfizmaları tanımlar

$\rho=x^2\delta$, $\sigma = x\delta^2$

$\rho: V \rightarrow (I^2J)^{-1}V(I^2J)$, $\sigma: V \rightarrow (IJ^2)^{-1}V(IJ^2)$

Bu otomorfizmalar x, δ, ρ ve σ birbirleri ile yer değiştirebilir. Çünkü bunlara karşılık gelen matrisler I, J, I^2J ve IJ^2 bazı üsleri D matrisinin farklı tamsayı kuvvetleridir.

6. Aşağıdaki matrisleri hesaplar.

IJ, $\rho(N)$, $\sigma(N^{-1})$

7. Açık anahtarı $(n, IJ, \rho(N), \sigma(N^{-1}))$ ve özel anahtarı (I,J) dir.

Şifreleme:

B şahsı aşağıdaki adımları izler

1. $\mathbb{Z}_n$ halkası üzerinde açık metinleri temsil eden 2x2'lik matrislerin bir m açık dizisini seçer. $m^{(1)}, m^{(2)}, m^{(3)}, \ldots, m^{(k)}$

2. $\forall\, m^{(i)}$ dizisi ($i=1,2,\ldots,k$) ve k_i tamsayısı için rastgele bir $X^{(i)}=(IJ)^{k_i}$ matrisini hesaplar.

3. $\forall i=1,2,\ldots,k$ için aşağıdaki otomorfizmaları tanımlar,

$$\vartheta^{(i)}: V\rightarrow (X^{(\dot{\mathrm{I}})})^{-1}V(X^{(\dot{\mathrm{I}})}),\ V\in M_2(\mathbb{Z}_n)$$

4. $\forall i=1,2,\ldots,k$ için,

$$\vartheta^{(\mathrm{i})}(\rho(\mathrm{N}), \vartheta^{(\mathrm{i})}\left(\sigma(N^{-1})\right) \text{ ve } m^{(\mathrm{i})}\vartheta^{(\mathrm{i})}\left(\rho(N)\right) \text{ matrislerini hesaplar.}$$

5. $\forall i=1,2,\ldots,k$ için rastgele $\mu\in\mathbb{Z}_n^*$ birimi seçer ve metnini aşağıdaki şekilde şifreler.

$$\mathrm{C}=(\,C^{(1)},C^{(2)},\ldots,C^{(k)}) \qquad C^{(i)}=(C_1^{(i)}, C_2^{(i)}),$$

$$C_1^{(i)}=\mu_i^{-1}\vartheta^{(\dot{\mathrm{I}})}(\sigma(N^{-1}), \quad C_2^{(i)}=\mu_i m^{(i)}\vartheta^{(i)}(\rho(N)).$$

Deşifreleme:

A şahsı aşağıda verilen adımları takip ederek şifrelenmiş mesajı deşifre eder.

1. Belirlediği özel anahtarı kullanarak $\forall i=1,2,\ldots,k$ için

$d^{(i)}=x^{-1}\,\delta\,(C_1^{(\dot{\mathrm{I}})})=x^{-1}\,\delta\,(\mu_i^{-1}\vartheta^{(i)}(\sigma(N^{-1}))$ değerini hesaplar.

2. $\forall i=1,2,\ldots,k$ için

$m^{(i)}=C_2^{(i)}d^{(i)}=(\mu_i m^{(i)}\vartheta^{(i)}(\rho(N))d^{(i)}$ matrislerini hesaplar.

3. Son olarak A şahsı $m^{(1)},m^{(2)},m^{(3)},\ldots,m^{(i)}$ matris dizilerinden faydalanarak orijinal mesajı elde eder.

3.3. Sayısal Uygulamalar

Birinci Kriptosistem ve İkinci Kriptosistem için çeşitli örnekler verilerek sistemin daha iyi anlaşılması sağlanacaktır.

Örnek 3.3.1.

ESNEK KÜMELER metnini şifreleyelim.

Anahtar Üretimi

1) 2 asal sayı p=2, q=13 seçelim, $n=p.q$=26 olur.

2) $\mathbb{Z}_{26}$ 'dan rastgele 4 tam sayıyı sırasıyla 3,4,8 ve 11 alalım.

3) A ve B matrislerini bu sayılardan aşağıdaki şekilde oluşturalım.

$$A=\begin{pmatrix}8 & 3\\ 3 & 8\end{pmatrix},\quad B=\begin{pmatrix}4 & 11\\ 11 & 4\end{pmatrix}$$

4) $\det A=3$, $\det B=25$ olarak bulunur ve 26 moduna göre terslerini $(\det A)^{-1}=3^{-1}=9$ ve $(\det B)^{-1}=25^{-1}=25$ olarak buluruz. Bu yüzden A ve B matrisleri $M_2(\mathbb{Z}_{26})$ halkasının içindedir.

5) $M_2(\mathbb{Z}_{26})$ halkasında 2 tane iç otomorfizma tanımlayalım.

$\forall V\in M_2(\mathbb{Z}_{26})$ matrisi için $x: V\to A^{-1}VA,\quad \delta: V\to B^{-1}VB$

6) $M_2(\mathbb{Z}_{26})$ halkasında 2 tane otomorfizma tanımlayalım.

$\rho=x\,\delta^2,\qquad \sigma=x^2\delta$

$\rho: V\to (AB^2)^{-1}V(AB^2),\quad \sigma: V\to (A^2B)^{-1}V(A^2B)$

7) Rastgele bir $N\in GL(2,\mathbb{Z}_n)$ matrisi seçelim. Öyle ki N, H grubuna ait değildir.

$$N=\begin{pmatrix}13 & 2\\ 6 & 5\end{pmatrix},\quad N^{-1}=\begin{pmatrix}5 & 24\\ 20 & 13\end{pmatrix}$$

8) $\rho(N)=(AB^2)^{-1}N(AB^2),\quad \sigma(N^{-1})=(A^2B)^{-1}N^{-1}(A^2B)$

Aşağıdaki matrisleri hesaplayalım.

$$A^2=\begin{pmatrix}8 & 3\\ 3 & 8\end{pmatrix}\begin{pmatrix}8 & 3\\ 3 & 8\end{pmatrix}=\begin{pmatrix}21 & 22\\ 22 & 21\end{pmatrix}$$

$$B^2=\begin{pmatrix}4 & 11\\ 11 & 4\end{pmatrix}\begin{pmatrix}4 & 11\\ 11 & 4\end{pmatrix}=\begin{pmatrix}7 & 10\\ 10 & 7\end{pmatrix}$$

$$A^2B=\begin{pmatrix}21 & 22\\ 22 & 21\end{pmatrix}\begin{pmatrix}4 & 11\\ 11 & 4\end{pmatrix}=\begin{pmatrix}14 & 7\\ 7 & 14\end{pmatrix},\qquad (A^2B)^{-1}=\begin{pmatrix}10 & 21\\ 21 & 10\end{pmatrix}$$

$$AB^2=\begin{pmatrix}8 & 3\\ 3 & 8\end{pmatrix}\begin{pmatrix}7 & 10\\ 10 & 7\end{pmatrix}=\begin{pmatrix}8 & 23\\ 23 & 8\end{pmatrix},\qquad (AB^2)^{-1}=\begin{pmatrix}20 & 1\\ 1 & 20\end{pmatrix}$$

$$\rho(N)=\begin{pmatrix}20 & 1\\ 1 & 20\end{pmatrix}\begin{pmatrix}13 & 2\\ 6 & 5\end{pmatrix}\begin{pmatrix}8 & 23\\ 23 & 8\end{pmatrix}=\begin{pmatrix}6 & 19\\ 3 & 24\end{pmatrix}\begin{pmatrix}8 & 23\\ 23 & 8\end{pmatrix}=\begin{pmatrix}17 & 4\\ 4 & 1\end{pmatrix}$$

$\sigma(N^{-1})=\begin{pmatrix}10 & 21\\ 21 & 10\end{pmatrix}\begin{pmatrix}5 & 24\\ 20 & 13\end{pmatrix}\begin{pmatrix}14 & 7\\ 7 & 14\end{pmatrix}=\begin{pmatrix}2 & 19\\ 19 & 10\end{pmatrix}\begin{pmatrix}14 & 7\\ 7 & 14\end{pmatrix}=\begin{pmatrix}5 & 20\\ 24 & 13\end{pmatrix}$

Genel anahtarımız $(n,\rho(N),\sigma(N^{-1}))=\left(26,\begin{pmatrix}17 & 4\\ 4 & 1\end{pmatrix},\begin{pmatrix}5 & 20\\ 24 & 13\end{pmatrix}\right)$

Özel anahtarımız ise $\left(A=\begin{pmatrix}8 & 3\\ 3 & 8\end{pmatrix},\ B=\begin{pmatrix}4 & 11\\ 11 & 4\end{pmatrix}\right)$ olur.

Şifreleme

1) ESNEK KÜMELER metnini 4'lü bloklara bölerek 2x2 tipinde matrisler oluşturalım.

$m_{1}=\begin{pmatrix}\mathrm{E} & \mathrm{S}\\ \mathrm{N} & \mathrm{E}\end{pmatrix}=\begin{pmatrix}4 & 18\\ 13 & 4\end{pmatrix}, m_{2}=\begin{pmatrix}\mathrm{K} & \mathrm{K}\\ \mathrm{U} & \mathrm{M}\end{pmatrix}=\begin{pmatrix}10 & 10\\ 20 & 12\end{pmatrix}$ ve $m_{3}=\begin{pmatrix}\mathrm{E} & \mathrm{L}\\ \mathrm{E} & \mathrm{R}\end{pmatrix}=\begin{pmatrix}4 & 11\\ 4 & 17\end{pmatrix}$

2) Rastgele X matrisi seçelim, $X=\begin{pmatrix}17 & 12\\ 12 & 17\end{pmatrix}$ ve $X^{-1}=\begin{pmatrix}15 & 20\\ 20 & 15\end{pmatrix}$

3) $M_2(\mathbb{Z}_{26})$ halkası üzerinde ϑ otomorfizmasını tanımlayalım.

$\vartheta: V \to X^{-1}VX$, $\forall V \in M_2(\mathbb{Z}_{26})$ için.

4) $\vartheta(\rho(N))=X^{-1}\rho(N)X=\begin{pmatrix}15 & 20\\ 20 & 15\end{pmatrix}\begin{pmatrix}17 & 4\\ 4 & 1\end{pmatrix}\begin{pmatrix}17 & 12\\ 12 & 17\end{pmatrix}$

$=\begin{pmatrix}23 & 2\\ 10 & 17\end{pmatrix}\begin{pmatrix}17 & 12\\ 12 & 17\end{pmatrix}=\begin{pmatrix}25 & 24\\ 10 & 19\end{pmatrix}$

$\vartheta(\sigma(N^{-1}))=X^{-1}\sigma(N^{-1})X=\begin{pmatrix}15 & 20\\ 20 & 15\end{pmatrix}\begin{pmatrix}5 & 20\\ 24 & 13\end{pmatrix}\begin{pmatrix}17 & 12\\ 12 & 17\end{pmatrix}$

$=\begin{pmatrix}9 & 14\\ 18 & 23\end{pmatrix}\begin{pmatrix}17 & 12\\ 12 & 17\end{pmatrix}=\begin{pmatrix}9 & 8\\ 10 & 9\end{pmatrix}$

5) Şimdi $\mathbb{Z}_{26}$' dan rastgele bir μ elemanını, $\mu = 21$ seçelim ve 26 moduna göre tersini, μ^{-1}=5 olarak buluruz.

6) Şifreli metni hesaplayalım.

$C = (C_1, C_2)$

$C_1=\mu^{-1}\vartheta(\sigma(N^{-1}))= 5\begin{pmatrix}9 & 8\\ 10 & 9\end{pmatrix}=\begin{pmatrix}19 & 14\\ 24 & 19\end{pmatrix}$

$C_2= \mu m_1\vartheta(\rho(N))= 21\begin{pmatrix}4 & 18\\ 13 & 4\end{pmatrix}\begin{pmatrix}25 & 24\\ 10 & 19\end{pmatrix}$

$=\begin{pmatrix}6 & 14\\ 13 & 6\end{pmatrix}\begin{pmatrix}25 & 24\\ 10 & 19\end{pmatrix}=\begin{pmatrix}4 & 20\\ 21 & 10\end{pmatrix}$

Deşifreleme

Düz metni elde etmek amacıyla aşağıdaki adımları gerçekleştirelim.

1) Özel anahtarı kullanarak D matrisini hesaplayalım.

$D= x^{-1}\delta(C_1) = (A^{-1}B)^{-1}C_1(A^{-1}B)$

$A=\begin{pmatrix}8 & 3\\ 3 & 8\end{pmatrix}, A^{-1}=\begin{pmatrix}20 & 25\\ 25 & 20\end{pmatrix}$

$A^{-1}B=\begin{pmatrix}20 & 25\\ 25 & 20\end{pmatrix}\begin{pmatrix}4 & 11\\ 11 & 4\end{pmatrix}=\begin{pmatrix}17 & 8\\ 8 & 17\end{pmatrix}$

$(A^{-1}B)^{-1}=\begin{pmatrix}1 & 24\\ 24 & 1\end{pmatrix}$

$D=\begin{pmatrix}1 & 24\\ 24 & 1\end{pmatrix}\begin{pmatrix}19 & 14\\ 24 & 19\end{pmatrix}\begin{pmatrix}17 & 8\\ 8 & 17\end{pmatrix}$

$=\begin{pmatrix}23 & 2\\ 12 & 17\end{pmatrix}\begin{pmatrix}17 & 8\\ 8 & 17\end{pmatrix}=\begin{pmatrix}17 & 10\\ 2 & 21\end{pmatrix}$

2) Aşağıdaki matris işlemlerini hesaplayarak sonunda düz metni elde ederiz.

$m_1= C_2D=\begin{pmatrix}4 & 20\\ 21 & 10\end{pmatrix}\begin{pmatrix}17 & 10\\ 2 & 21\end{pmatrix}=\begin{pmatrix}4 & 18\\ 13 & 4\end{pmatrix}=\begin{pmatrix}\mathrm{E} & \mathrm{S}\\ \mathrm{N} & \mathrm{E}\end{pmatrix}$

Aynı işlemleri m_2 ve m_3 matrisleri için yapalım.

$$C_2 = \mu m_2 \vartheta\,(\rho(N)) = 21\begin{pmatrix}10 & 10\\ 20 & 12\end{pmatrix}\begin{pmatrix}25 & 24\\ 10 & 19\end{pmatrix} = \begin{pmatrix}2 & 2\\ 4 & 18\end{pmatrix}\begin{pmatrix}25 & 24\\ 10 & 19\end{pmatrix}$$

$$= \begin{pmatrix}18 & 8\\ 20 & 22\end{pmatrix}$$

$$m_2 = C_2 D = \begin{pmatrix}18 & 8\\ 20 & 22\end{pmatrix}\begin{pmatrix}17 & 10\\ 2 & 21\end{pmatrix} = \begin{pmatrix}10 & 10\\ 20 & 12\end{pmatrix} = \begin{pmatrix}\mathrm{K} & \mathrm{K}\\ \mathrm{U} & \mathrm{M}\end{pmatrix}$$

$$C_3 = \mu m_3 \vartheta\,(\rho(N)) = 21\begin{pmatrix}4 & 11\\ 4 & 17\end{pmatrix}\begin{pmatrix}25 & 24\\ 10 & 19\end{pmatrix} = \begin{pmatrix}6 & 23\\ 6 & 19\end{pmatrix}\begin{pmatrix}25 & 24\\ 10 & 19\end{pmatrix}$$

$$= \begin{pmatrix}16 & 9\\ 2 & 11\end{pmatrix}$$

$$\mathrm{m}_3 = C_3 D = \begin{pmatrix}16 & 9\\ 2 & 11\end{pmatrix}\begin{pmatrix}17 & 10\\ 2 & 21\end{pmatrix} = \begin{pmatrix}4 & 11\\ 4 & 17\end{pmatrix} = \begin{pmatrix}\mathrm{E} & \mathrm{L}\\ \mathrm{E} & \mathrm{R}\end{pmatrix}$$

Uyarı: Şifrelenecek kelime, 2x2 matrisler kullanıldığı için dörtlü bloklara ayrılarak yapılmaktadır. Eğer kelime uzunluğu dördün bir katı değilse uygun harfler kelimenin sonuna eklenerek şifreleme yapılır.

Örnek 3.3.2.

OKULA GEL metnini şifreleyelim.

Anahtar Üretimi

1) 2 asal sayı p=2, q=13 seçelim, n=$p.q$=26 olur.

2) $\mathbb{Z}_{26}$ 'dan rastgele 4 tam sayıyı sırasıyla 2, 5, 6 ve 7 alalım.

3) A ve B matrislerini oluşturalım.

$$A=\begin{pmatrix}7 & 2\\ 2 & 7\end{pmatrix},\quad B=\begin{pmatrix}6 & 5\\ 5 & 6\end{pmatrix}$$

4) $\det A=19$, $\det B=11$ olarak bulunur ve 26 moduna göre terslerini $(\det A)^{-1}=19^{-1}=11$ ve $(\det B)^{-1}=11^{-1}=19$ olarak buluruz.

Bu yüzden A ve B matrisleri $M_2(\mathbb{Z}_{26})$ halkasının içindedir.

5) $M_2(\mathbb{Z}_{26})$ halkasında 2 tane iç otomorfizma tanımlayalım.

$x: V \to A^{-1}VA$, $\delta: V \to B^{-1}VB$,

$\forall V \in M_2(\mathbb{Z}_{26})$ matrisi için.

6) $M_2(\mathbb{Z}_{26})$ halkasında 2 tane otomorfizma tanımlayalım.

$\rho = x\,\delta^2$, $\sigma = x^2\delta$

$\rho: V \to (AB^2)^{-1}V(AB^2)$, $\sigma: V \to (A^2B)^{-1}V(A^2B)$

7) Rastgele bir $N \in GL(2,\mathbb{Z}_n)$ matrisi seçelim. Öyle ki N, H grubuna ait değildir.

$$N=\begin{pmatrix}5 & 3\\ 1 & 2\end{pmatrix},\quad N^{-1}=\begin{pmatrix}4 & 7\\ 11 & 23\end{pmatrix}$$

8) $\rho(N)=(AB^2)^{-1}N(AB^2)$, $\sigma(N^{-1})=(A^2B)^{-1}N^{-1}(A^2B)$

Aşağıdaki matrisleri hesaplayalım.

$$A^2=\begin{pmatrix}7 & 2\\ 2 & 7\end{pmatrix}\begin{pmatrix}7 & 2\\ 2 & 7\end{pmatrix}=\begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix}$$

$$B^2=\begin{pmatrix}6 & 5\\ 5 & 6\end{pmatrix}\begin{pmatrix}6 & 5\\ 5 & 6\end{pmatrix}=\begin{pmatrix}9 & 8\\ 8 & 9\end{pmatrix}$$

$$A^2B=\begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix}\begin{pmatrix}6 & 5\\ 5 & 6\end{pmatrix}=\begin{pmatrix}16 & 17\\ 17 & 16\end{pmatrix},\qquad (A^2B)^{-1}=\begin{pmatrix}20 & 21\\ 21 & 20\end{pmatrix}$$

$$AB^2=\begin{pmatrix}7 & 2\\ 2 & 7\end{pmatrix}\begin{pmatrix}9 & 8\\ 8 & 9\end{pmatrix}=\begin{pmatrix}1 & 22\\ 22 & 1\end{pmatrix},\qquad (AB^2)^{-1}=\begin{pmatrix}19 & 24\\ 24 & 19\end{pmatrix}$$

$$\rho(N)=\begin{pmatrix}19 & 24\\ 24 & 19\end{pmatrix}\begin{pmatrix}5 & 3\\ 1 & 2\end{pmatrix}\begin{pmatrix}1 & 22\\ 22 & 1\end{pmatrix}=\begin{pmatrix}15 & 1\\ 9 & 6\end{pmatrix}\begin{pmatrix}1 & 22\\ 22 & 1\end{pmatrix}=\begin{pmatrix}11 & 19\\ 11 & 22\end{pmatrix}$$

$$\sigma(N^{-1})=\begin{pmatrix}20 & 21\\ 21 & 20\end{pmatrix}\begin{pmatrix}4 & 7\\ 11 & 23\end{pmatrix}\begin{pmatrix}16 & 17\\ 17 & 16\end{pmatrix}=\begin{pmatrix}25 & 25\\ 18 & 9\end{pmatrix}\begin{pmatrix}16 & 17\\ 17 & 16\end{pmatrix}=\begin{pmatrix}19 & 19\\ 25 & 8\end{pmatrix}$$

Genel anahtarımız $(n, \rho(N), \sigma(N^{-1}))=\left(26,\begin{pmatrix}11 & 19\\ 11 & 22\end{pmatrix},\begin{pmatrix}19 & 19\\ 25 & 8\end{pmatrix}\right)$

Özel anahtarımız ise $\left(A=\begin{pmatrix}7 & 2\\ 2 & 7\end{pmatrix},\ B=\begin{pmatrix}6 & 5\\ 5 & 6\end{pmatrix}\right)$ olur.

Şifreleme

1) OKULA GEL metnini 4'lü bloklara bölerek 2x2 tipinde matrisler oluşturalım.

$m_1=\begin{pmatrix}O & K\\ U & L\end{pmatrix}=\begin{pmatrix}14 & 10\\ 20 & 11\end{pmatrix}, m_2=\begin{pmatrix}A & G\\ E & L\end{pmatrix}=\begin{pmatrix}0 & 6\\ 4 & 11\end{pmatrix}$

2) Rastgele X matrisi seçelim, $X=\begin{pmatrix}5 & 2\\ 2 & 5\end{pmatrix}$ ve $X^{-1}=\begin{pmatrix}25 & 16\\ 16 & 25\end{pmatrix}$

3) $M_2(\mathbb{Z}_{26})$ halkası üzerinde ϑ otomorfizmasını tanımlayalım.

$\vartheta: V \to X^{-1}VX$, $\forall V \in M_2(\mathbb{Z}_{26})$ için.

4) $\vartheta\ (\rho(N))=X^{-1}\rho(N)X=\begin{pmatrix}25 & 16\\ 16 & 25\end{pmatrix}\begin{pmatrix}11 & 19\\ 11 & 22\end{pmatrix}\begin{pmatrix}5 & 2\\ 2 & 5\end{pmatrix}$

$=\begin{pmatrix}9 & 21\\ 9 & 22\end{pmatrix}\begin{pmatrix}5 & 2\\ 2 & 5\end{pmatrix}=\begin{pmatrix}9 & 19\\ 11 & 24\end{pmatrix}$

$\vartheta\ (\sigma(N^{-1}))=X^{-1}\sigma\,(N^{-1})X=\begin{pmatrix}25 & 16\\ 16 & 25\end{pmatrix}\begin{pmatrix}19 & 19\\ 25 & 8\end{pmatrix}\begin{pmatrix}5 & 2\\ 2 & 5\end{pmatrix}$

$=\begin{pmatrix}17 & 5\\ 19 & 10\end{pmatrix}\begin{pmatrix}5 & 2\\ 2 & 5\end{pmatrix}=\begin{pmatrix}17 & 7\\ 11 & 10\end{pmatrix}$

5) Şimdi $\mathbb{Z}_{26}$' dan rastgele bir μ elemanını, $\mu = 7$ seçelim ve 26 moduna göre tersini, μ^{-1}=15 olarak buluruz.

6) Şifreli metni hesaplayalım.

$C = (C_1, C_2)$

$C_1=\mu^{-1}\vartheta\ (\sigma\,(N^{-1})) = 15\begin{pmatrix}17 & 7\\ 11 & 10\end{pmatrix}=\begin{pmatrix}21 & 1\\ 9 & 20\end{pmatrix}$

$C_2= \mu m_1 \vartheta(\rho(N))= 7\begin{pmatrix}14 & 10\\ 20 & 11\end{pmatrix}\begin{pmatrix}9 & 19\\ 11 & 24\end{pmatrix}$

$=\begin{pmatrix}20 & 18\\ 10 & 25\end{pmatrix}\begin{pmatrix}9 & 19\\ 11 & 24\end{pmatrix}=\begin{pmatrix}14 & 6\\ 1 & 10\end{pmatrix}$

Deşifreleme

Düz metni elde etmek amacıyla aşağıdaki adımları gerçekleştirelim.

1) Özel anahtarı kullanarak D matrisini hesaplayalım.

$D= x^{-1}\delta(C_1) = (A^{-1}B)^{-1}C_1(A^{-1}B)$

$A=\begin{pmatrix}7 & 2\\ 2 & 7\end{pmatrix}$, $A^{-1}=\begin{pmatrix}25 & 4\\ 4 & 25\end{pmatrix}$

$A^{-1}B=\begin{pmatrix}25 & 4\\ 4 & 25\end{pmatrix}\begin{pmatrix}6 & 5\\ 5 & 6\end{pmatrix}=\begin{pmatrix}14 & 19\\ 19 & 14\end{pmatrix}$

$(A^{-1}B)^{-1}=\begin{pmatrix}10 & 5\\ 5 & 10\end{pmatrix}$

$D=\begin{pmatrix}10 & 5\\ 5 & 10\end{pmatrix}\begin{pmatrix}21 & 1\\ 9 & 20\end{pmatrix}\begin{pmatrix}14 & 19\\ 19 & 14\end{pmatrix}$

$=\begin{pmatrix}21 & 6\\ 13 & 23\end{pmatrix}\begin{pmatrix}14 & 19\\ 19 & 14\end{pmatrix}=\begin{pmatrix}18 & 15\\ 21 & 23\end{pmatrix}$

2) Aşağıdaki matris işlemlerini hesaplayarak sonunda düz metni elde ederiz.

$m_1= C_2\ D= \begin{pmatrix}14 & 6\\ 1 & 10\end{pmatrix}\begin{pmatrix}18 & 15\\ 21 & 23\end{pmatrix}=\begin{pmatrix}14 & 10\\ 20 & 11\end{pmatrix}=\begin{pmatrix}\mathrm{O} & \mathrm{K}\\ \mathrm{U} & \mathrm{L}\end{pmatrix}$

Aynı işlemleri m_2 matrisi için yapalım.

$C_2= \mu m_2\vartheta\ (\rho\,(N))= 7\begin{pmatrix}0 & 6\\ 4 & 11\end{pmatrix}\begin{pmatrix}9 & 19\\ 11 & 24\end{pmatrix}=\begin{pmatrix}0 & 16\\ 2 & 25\end{pmatrix}\begin{pmatrix}9 & 19\\ 11 & 24\end{pmatrix}$

$=\begin{pmatrix}20 & 20\\ 7 & 14\end{pmatrix}$

$m_2= C_2D= \begin{pmatrix}20 & 20\\ 7 & 14\end{pmatrix}\begin{pmatrix}18 & 15\\ 21 & 23\end{pmatrix}=\begin{pmatrix}0 & 6\\ 4 & 11\end{pmatrix}=\begin{pmatrix}\mathrm{A} & \mathrm{G}\\ \mathrm{E} & \mathrm{L}\end{pmatrix}$

Örnek 3.3.3.

KAPALI ANAHTARLI ŞİFRELEME metnini şifreleyelim.

Anahtar Üretimi

1) 2 asal sayı p=2, q=13 seçelim, n=$p.q$=26 olur.

2) $\mathbb{Z}_{26}$ 'dan rastgele 4 tam sayıyı sırasıyla 4, 7, 8 ve 11 alalım.

3) A ve B matrislerini oluşturalım.

$$A=\begin{pmatrix}11 & 8\\ 8 & 11\end{pmatrix},\quad B=\begin{pmatrix}7 & 4\\ 4 & 7\end{pmatrix}$$

4) $\det A=5$, $\det B=7$ olarak bulunur ve 26 moduna göre terslerini, $(\det A)^{-1}=5^{-1}=21$ ve $(\det B)^{-1}=7^{-1}=15$ olarak buluruz.

Bu yüzden A ve B matrisleri $M_2(\mathbb{Z}_{26})$ halkasının içindedir.

5)$M_2(\mathbb{Z}_{26})$ halkasında 2 iç tane otomorfizma tanımlayalım.

$x: V \to A^{-1}VA,\quad \delta: V \to B^{-1}VB,$

$\forall V \in M_2(\mathbb{Z}_{26})$ matrisi için.

6) $M_2(\mathbb{Z}_{26})$ halkasında 2 tane otomorfizma tanımlayalım.

$\rho = x\,\delta^2,\qquad \sigma = x^2\delta$

$\rho: V \to (AB^2)^{-1}V(AB^2),\quad \sigma: V \to (A^2B)^{-1}V(A^2B)$

7) A şahsı rastgele bir $N \in GL(2,\mathbb{Z}_n)$ matrisi seçelim. Öyle ki N, H grubuna ait değildir.

$$N=\begin{pmatrix}7 & 2\\ 3 & 5\end{pmatrix},\quad N^{-1}=\begin{pmatrix}19 & 8\\ 25 & 11\end{pmatrix}$$

8) $\rho(N)=(AB^2)^{-1}N(AB^2)$, $\sigma(N^{-1})=(A^2B)^{-1}N^{-1}(A^2B)$

Aşağıdaki matrisleri hesaplayalım.

$$A^2=\begin{pmatrix}11 & 8\\ 8 & 11\end{pmatrix}\begin{pmatrix}11 & 8\\ 8 & 11\end{pmatrix}=\begin{pmatrix}3 & 20\\ 20 & 3\end{pmatrix}$$

$$B^2=\begin{pmatrix}7 & 4\\ 4 & 7\end{pmatrix}\begin{pmatrix}7 & 4\\ 4 & 7\end{pmatrix}=\begin{pmatrix}13 & 4\\ 4 & 13\end{pmatrix}$$

$$A^2B=\begin{pmatrix}3 & 20\\ 20 & 3\end{pmatrix}\begin{pmatrix}7 & 4\\ 4 & 7\end{pmatrix}=\begin{pmatrix}23 & 22\\ 22 & 23\end{pmatrix},\qquad (A^2B)^{-1}=\begin{pmatrix}19 & 18\\ 18 & 19\end{pmatrix}$$

$$AB^2=\begin{pmatrix}11 & 8\\ 8 & 11\end{pmatrix}\begin{pmatrix}13 & 4\\ 4 & 13\end{pmatrix}=\begin{pmatrix}19 & 18\\ 18 & 19\end{pmatrix},\qquad (AB^2)^{-1}=\begin{pmatrix}23 & 22\\ 22 & 23\end{pmatrix}$$

$$\rho(N)=\begin{pmatrix}23 & 22\\ 22 & 23\end{pmatrix}\begin{pmatrix}7 & 2\\ 3 & 5\end{pmatrix}\begin{pmatrix}19 & 18\\ 18 & 19\end{pmatrix}=\begin{pmatrix}19 & 0\\ 15 & 3\end{pmatrix}\begin{pmatrix}19 & 18\\ 18 & 19\end{pmatrix}=\begin{pmatrix}23 & 4\\ 1 & 15\end{pmatrix}$$

$\sigma(N^{-1})=\begin{pmatrix}19 & 18\\ 18 & 19\end{pmatrix}\begin{pmatrix}19 & 8\\ 25 & 11\end{pmatrix}\begin{pmatrix}23 & 22\\ 22 & 23\end{pmatrix}=\begin{pmatrix}5 & 12\\ 11 & 15\end{pmatrix}\begin{pmatrix}23 & 22\\ 22 & 23\end{pmatrix}=\begin{pmatrix}15 & 22\\ 11 & 15\end{pmatrix}$

Genel anahtarımız $(n,\rho(N),\sigma(N^{-1}))=\left(26,\begin{pmatrix}23 & 4\\ 1 & 15\end{pmatrix},\begin{pmatrix}15 & 22\\ 11 & 15\end{pmatrix}\right)$

Özel anahtarımız ise $\left(A=\begin{pmatrix}11 & 8\\ 8 & 11\end{pmatrix},\ B=\begin{pmatrix}7 & 4\\ 4 & 7\end{pmatrix}\right)$ olur.

Şifreleme

1) KAPALI ANAHTARLI ŞİFRELEME metnini 4'lü bloklara bölerek 2x2 tipinde matrisler oluşturalım.

$m_{1=}\begin{pmatrix}\mathrm{K} & \mathrm{A}\\ \mathrm{P} & \mathrm{A}\end{pmatrix}=\begin{pmatrix}10 & 0\\ 15 & 0\end{pmatrix}$, $m_{2=}\begin{pmatrix}\mathrm{L} & \mathrm{I}\\ \mathrm{A} & \mathrm{N}\end{pmatrix}=\begin{pmatrix}11 & 8\\ 0 & 13\end{pmatrix}$, $m_{3=}\begin{pmatrix}\mathrm{A} & \mathrm{H}\\ \mathrm{T} & \mathrm{A}\end{pmatrix}=\begin{pmatrix}0 & 7\\ 19 & 0\end{pmatrix}$

$m_{4=}\begin{pmatrix}\mathrm{R} & \mathrm{L}\\ \mathrm{I} & \mathrm{S}\end{pmatrix}=\begin{pmatrix}17 & 11\\ 8 & 18\end{pmatrix}$, $m_{5=}\begin{pmatrix}\mathrm{I} & \mathrm{F}\\ \mathrm{R} & \mathrm{E}\end{pmatrix}=\begin{pmatrix}8 & 15\\ 17 & 4\end{pmatrix}$, $m_{6=}\begin{pmatrix}\mathrm{L} & \mathrm{E}\\ \mathrm{M} & \mathrm{E}\end{pmatrix}=\begin{pmatrix}11 & 4\\ 12 & 4\end{pmatrix}$

2) Rastgele X matrisi seçelim, $X=\begin{pmatrix}7 & 2\\ 2 & 7\end{pmatrix}$ ve $X^{-1}=\begin{pmatrix}25 & 4\\ 4 & 25\end{pmatrix}$.

3) $M_2(\mathbb{Z}_{26})$ halkası üzerinde ϑ otomorfizmasını tanımlayalım.

$\vartheta: V \to X^{-1}VX$, $\forall V \in M_2(\mathbb{Z}_{26})$ için.

4) $\vartheta(\rho(N))=X^{-1}\rho(N)X=\begin{pmatrix}25 & 4\\ 4 & 25\end{pmatrix}\begin{pmatrix}23 & 4\\ 1 & 15\end{pmatrix}\begin{pmatrix}7 & 2\\ 2 & 7\end{pmatrix}$

$=\begin{pmatrix}7 & 4\\ 13 & 1\end{pmatrix}\begin{pmatrix}7 & 2\\ 2 & 7\end{pmatrix}=\begin{pmatrix}5 & 16\\ 15 & 7\end{pmatrix}$

$\vartheta(\sigma(N^{-1}))=X^{-1}\sigma(N^{-1})X=\begin{pmatrix}25 & 4\\ 4 & 25\end{pmatrix}\begin{pmatrix}15 & 22\\ 11 & 15\end{pmatrix}\begin{pmatrix}7 & 2\\ 2 & 7\end{pmatrix}$

$=\begin{pmatrix}3 & 12\\ 23 & 21\end{pmatrix}\begin{pmatrix}7 & 2\\ 2 & 7\end{pmatrix}=\begin{pmatrix}19 & 12\\ 21 & 11\end{pmatrix}$

5) Şimdi $\mathbb{Z}_{26}$' dan rastgele bir μ elemanını, $\mu = 17$ seçelim ve 26 moduna göre tersini, μ^{-1}=23 olarak buluruz.

6) Şifreli metni hesaplayalım.

$C = (C_1, C_2)$

$C_1 = \mu^{-1}\vartheta\,(\sigma(N^{-1})) = 23\begin{pmatrix}19 & 12\\ 21 & 11\end{pmatrix} = \begin{pmatrix}21 & 16\\ 15 & 19\end{pmatrix}$

$C_2 = \mu m_1 \vartheta(\rho(N)) = 17\begin{pmatrix}10 & 0\\ 15 & 0\end{pmatrix}\begin{pmatrix}5 & 16\\ 15 & 7\end{pmatrix}$

$$= \begin{pmatrix}14 & 0\\ 21 & 0\end{pmatrix}\begin{pmatrix}5 & 16\\ 15 & 7\end{pmatrix} = \begin{pmatrix}18 & 16\\ 1 & 24\end{pmatrix}$$

Deşifreleme

Düz metni elde etmek amacıyla aşağıdaki adımları gerçekleştirelim.

1) Özel anahtarı kullanarak D matrisini hesaplayalım.

$D = x^{-1}\delta(C_1) = (A^{-1}B)^{-1}C_1(A^{-1}B)$

$A = \begin{pmatrix}11 & 8\\ 8 & 11\end{pmatrix}$, $A^{-1} = \begin{pmatrix}23 & 14\\ 14 & 23\end{pmatrix}$

$A^{-1}B = \begin{pmatrix}23 & 14\\ 14 & 23\end{pmatrix}\begin{pmatrix}7 & 4\\ 4 & 7\end{pmatrix} = \begin{pmatrix}9 & 8\\ 8 & 9\end{pmatrix}$

$(A^{-1}B)^{-1} = \begin{pmatrix}25 & 24\\ 24 & 25\end{pmatrix}$

$D = \begin{pmatrix}25 & 24\\ 24 & 25\end{pmatrix}\begin{pmatrix}21 & 16\\ 15 & 19\end{pmatrix}\begin{pmatrix}9 & 8\\ 8 & 9\end{pmatrix}$

$= \begin{pmatrix}1 & 24\\ 21 & 1\end{pmatrix}\begin{pmatrix}9 & 8\\ 8 & 9\end{pmatrix} = \begin{pmatrix}19 & 16\\ 15 & 21\end{pmatrix}$

2) Aşağıdaki matris işlemlerini hesaplayarak sonunda düz metni elde ederiz.

$m_1 = C_2\,D = \begin{pmatrix}18 & 16\\ 1 & 24\end{pmatrix}\begin{pmatrix}19 & 16\\ 15 & 21\end{pmatrix} = \begin{pmatrix}10 & 0\\ 15 & 0\end{pmatrix} = \begin{pmatrix}\mathrm{K} & \mathrm{A}\\ \mathrm{P} & \mathrm{A}\end{pmatrix}$

Aynı işlemleri m_2, m_3, m_4, m_5 ve m_6 matrisleri için yapalım.

$$C_2 = \mu m_2 \vartheta(\rho(N)) = 17 \begin{pmatrix} 11 & 8 \\ 0 & 13 \end{pmatrix} \begin{pmatrix} 5 & 16 \\ 15 & 7 \end{pmatrix} = \begin{pmatrix} 5 & 6 \\ 0 & 13 \end{pmatrix} \begin{pmatrix} 5 & 16 \\ 15 & 7 \end{pmatrix}$$

$$= \begin{pmatrix} 11 & 18 \\ 13 & 13 \end{pmatrix}$$

$$m_2 = C_2 D = \begin{pmatrix} 11 & 18 \\ 13 & 13 \end{pmatrix} \begin{pmatrix} 19 & 16 \\ 15 & 21 \end{pmatrix} = \begin{pmatrix} 11 & 8 \\ 0 & 13 \end{pmatrix} = \begin{pmatrix} \mathrm{L} & \mathrm{I} \\ \mathrm{A} & \mathrm{N} \end{pmatrix}$$

$$C_3 = \mu m_3 \vartheta(\rho(N)) = 17 \begin{pmatrix} 0 & 7 \\ 19 & 0 \end{pmatrix} \begin{pmatrix} 5 & 16 \\ 15 & 7 \end{pmatrix} = \begin{pmatrix} 0 & 15 \\ 11 & 0 \end{pmatrix} \begin{pmatrix} 5 & 16 \\ 15 & 7 \end{pmatrix}$$

$$= \begin{pmatrix} 17 & 1 \\ 3 & 20 \end{pmatrix}$$

$$m_3 = C_3 D = \begin{pmatrix} 17 & 1 \\ 3 & 20 \end{pmatrix} \begin{pmatrix} 19 & 16 \\ 15 & 21 \end{pmatrix} = \begin{pmatrix} 0 & 7 \\ 19 & 0 \end{pmatrix} = \begin{pmatrix} \mathrm{A} & \mathrm{H} \\ \mathrm{T} & \mathrm{A} \end{pmatrix}$$

Aynı işlemler yapılarak m_4, m_5 ve m_6 matrisleri sırasıyla şifrelenir ve deşifrelenir.

Örnek 3.3.4.

Anahtar Üretimi

Anahtar üretmek için aşağıdaki adımları gerçekleştirelim.

1) Bir asal sayı p=7 seçelim, n=p^2=49 olur.

2) Rastgele bir matris $D = \begin{pmatrix} 5 & 3 \\ 1 & 7 \end{pmatrix} \in GL(2, \mathbb{Z}_{49})$ alalım.

3) Matrisleri hesaplayalım.

$$I = D^2 = \begin{pmatrix} 28 & 36 \\ 12 & 3 \end{pmatrix}, \quad J = D^3 = \begin{pmatrix} 29 & 42 \\ 14 & 8 \end{pmatrix}$$

$$I^2 = \begin{pmatrix} 40 & 38 \\ 29 & 0 \end{pmatrix}, \quad J^2 = \begin{pmatrix} 8 & 35 \\ 28 & 15 \end{pmatrix}$$

$$I^2J = \begin{pmatrix}40 & 38\\ 29 & 0\end{pmatrix}\begin{pmatrix}29 & 42\\ 14 & 8\end{pmatrix} = \begin{pmatrix}26 & 24\\ 8 & 42\end{pmatrix}$$

$$IJ^2 = \begin{pmatrix}28 & 36\\ 12 & 3\end{pmatrix}\begin{pmatrix}8 & 35\\ 28 & 15\end{pmatrix} = \begin{pmatrix}7 & 1\\ 33 & 24\end{pmatrix}$$

4) Rastgele bir $N \in GL(2,\mathbb{Z}_{49})$ seçelim.

$$N = \begin{pmatrix}8 & 3\\ 5 & 4\end{pmatrix},\quad N^{-1}=\begin{pmatrix}6 & 20\\ 17 & 12\end{pmatrix}$$

5) $M_2(\mathbb{Z}_{49})$ halkasında aşağıdaki otomorfizmaları tanımlayalım.

$x: V \to I^{-1}VI, \qquad \delta: V \to J^{-1}VJ, \qquad \forall\, V \in M_2(\mathbb{Z}_{49})$

$\rho = x^2\delta, \qquad \sigma = x\delta^2$

$\rho: V \to (I^2J)^{-1}V(I^2J), \qquad \sigma: V \to (IJ^2)^{-1}V(IJ^2)$

6) Aşağıdaki matrisleri hesaplayalım.

$$IJ = \begin{pmatrix}42 & 43\\ 47 & 38\end{pmatrix}$$

$$(I^2J)^{-1} = \begin{pmatrix}35 & 15\\ 5 & 45\end{pmatrix},\ (IJ^2)^{-1} = \begin{pmatrix}47 & 45\\ 15 & 28\end{pmatrix}$$

$$\rho(N) = \begin{pmatrix}35 & 15\\ 5 & 45\end{pmatrix}\begin{pmatrix}8 & 3\\ 5 & 4\end{pmatrix}\begin{pmatrix}26 & 24\\ 8 & 42\end{pmatrix} = \begin{pmatrix}12 & 18\\ 20 & 48\end{pmatrix}\begin{pmatrix}26 & 24\\ 8 & 42\end{pmatrix}$$

$$= \begin{pmatrix}15 & 15\\ 22 & 46\end{pmatrix}$$

$$\sigma(N^{-1}) = \begin{pmatrix}47 & 45\\ 15 & 28\end{pmatrix}\begin{pmatrix}6 & 20\\ 17 & 12\end{pmatrix}\begin{pmatrix}7 & 1\\ 33 & 24\end{pmatrix} = \begin{pmatrix}18 & 10\\ 27 & 48\end{pmatrix}\begin{pmatrix}7 & 1\\ 33 & 24\end{pmatrix}$$

$$= \begin{pmatrix}15 & 13\\ 9 & 3\end{pmatrix}$$

7) Genel anahtarımız,

$$\left(n = 49, \rho(N) = \begin{pmatrix} 15 & 15 \\ 22 & 46 \end{pmatrix}, \sigma(N^{-1}) = \begin{pmatrix} 15 & 13 \\ 9 & 3 \end{pmatrix}, \ IJ = \begin{pmatrix} 42 & 43 \\ 47 & 38 \end{pmatrix}\right)$$

ve özel anahtarımız $\left(I = \begin{pmatrix} 28 & 36 \\ 12 & 3 \end{pmatrix}, J = \begin{pmatrix} 29 & 42 \\ 14 & 8 \end{pmatrix}\right)$ olur.

Şifreleme

Aşağıdaki adımları gerçekleştirelim.

1) $M_2(\mathbb{Z}_{49})$ da açık metinleri temsil eden bir matris m olsun.

$$m = \begin{pmatrix} 9 & 1 \\ 5 & 2 \end{pmatrix} \in M_2(\mathbb{Z}_{49})$$

2) Rastgele bir k tamsayısı için k=2 seçelim ve matrisleri hesaplayalım.

$$X=(IJ)^2 = \begin{pmatrix} 12 & 10 \\ 36 & 35 \end{pmatrix}, X^{-1}=\begin{pmatrix} 21 & 8 \\ 19 & 10 \end{pmatrix}$$

3) $M_2(\mathbb{Z}_{49})$ halkası üzerinde ϑ otomorfizmasını tanımlayalım.

$\vartheta: V \to X^{-1}VX, \quad \forall V \in M_2(\mathbb{Z}_{49})$ için.

4) Matrisleri hesaplayalım.

$$\vartheta(\rho(N))=X^{-1}\rho(N)X = \begin{pmatrix} 21 & 8 \\ 19 & 10 \end{pmatrix}\begin{pmatrix} 15 & 15 \\ 22 & 46 \end{pmatrix}\begin{pmatrix} 12 & 10 \\ 36 & 35 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 46 \\ 15 & 10 \end{pmatrix}\begin{pmatrix} 12 & 10 \\ 36 & 35 \end{pmatrix}$$

$$= \begin{pmatrix} 2 & 3 \\ 1 & 10 \end{pmatrix}$$

$$\vartheta(\sigma(N^{-1}))=X^{-1}\sigma(N^{-1})X= \begin{pmatrix} 21 & 8 \\ 19 & 10 \end{pmatrix}\begin{pmatrix} 15 & 13 \\ 9 & 3 \end{pmatrix}\begin{pmatrix} 12 & 10 \\ 36 & 35 \end{pmatrix}$$

$$= \begin{pmatrix} 44 & 3 \\ 32 & 32 \end{pmatrix}\begin{pmatrix} 12 & 10 \\ 36 & 35 \end{pmatrix}$$

$$= \begin{pmatrix} 48 & 6 \\ 17 & 19 \end{pmatrix}$$

5) Şimdi $\mathbb{Z}_{49}$' dan rastgele bir μ elemanını, $\mu = 5$ seçelim ve 49 moduna göre tersini, μ^{-1}=10 olarak buluruz.

6) Şifreli metni hesaplayalım.

$C = (C_1, C_2)$

$C_1 = \mu^{-1}\vartheta(\sigma(N^{-1})) = 10\begin{pmatrix} 48 & 6 \\ 17 & 19 \end{pmatrix} = \begin{pmatrix} 39 & 11 \\ 23 & 43 \end{pmatrix}$

$C_2 = \mu m\, \vartheta(\rho(N)) = 5\begin{pmatrix} 9 & 1 \\ 5 & 2 \end{pmatrix}\begin{pmatrix} 2 & 3 \\ 1 & 10 \end{pmatrix} = \begin{pmatrix} 45 & 5 \\ 25 & 10 \end{pmatrix}\begin{pmatrix} 2 & 3 \\ 1 & 10 \end{pmatrix}$

$$= \begin{pmatrix} 46 & 38 \\ 11 & 28 \end{pmatrix}$$

Deşifreleme

Düz metni elde etmek amacıyla aşağıdaki adımları yapalım.

1) Özel anahtarı kullanarak, D matrisini hesaplayalım.

$D = x\delta^{-1}(C_1) = (IJ^{-1})^{-1}C_1(IJ^{-1})$

$J^{-1} = \begin{pmatrix} 22 & 7 \\ 35 & 43 \end{pmatrix}$, $IJ^{-1} = \begin{pmatrix} 28 & 36 \\ 12 & 3 \end{pmatrix}\begin{pmatrix} 22 & 7 \\ 35 & 43 \end{pmatrix} = \begin{pmatrix} 14 & 29 \\ 26 & 17 \end{pmatrix}$

$(IJ^{-1})^{-1} = \begin{pmatrix} 5 & 3 \\ 1 & 7 \end{pmatrix}$

$D = \begin{pmatrix} 5 & 3 \\ 1 & 7 \end{pmatrix}\begin{pmatrix} 39 & 11 \\ 23 & 43 \end{pmatrix}\begin{pmatrix} 14 & 29 \\ 26 & 17 \end{pmatrix}$

$= \begin{pmatrix} 19 & 37 \\ 4 & 18 \end{pmatrix}\begin{pmatrix} 14 & 29 \\ 26 & 17 \end{pmatrix}$

$= \begin{pmatrix} 3 & 4 \\ 34 & 30 \end{pmatrix}$

2) Aşağıdaki matris işlemlerini hesaplayarak sonunda düz metni elde ederiz.

$$m=C_2D=\begin{pmatrix}46 & 38\\ 11 & 28\end{pmatrix}\begin{pmatrix}3 & 4\\ 34 & 30\end{pmatrix}$$

$$=\begin{pmatrix}9 & 1\\ 5 & 2\end{pmatrix}$$

Örnek 3.3.5.

Anahtar Üretimi

Anahtar üretmek için aşağıdaki adımları gerçekleştirelim.

1) Bir asal sayı p=5 seçelim, $n=p^2$=25 olur.

2) Rastgele bir matris $D=\begin{pmatrix}7 & 2\\ 4 & 3\end{pmatrix}\in GL(2,\mathbb{Z}_{25})$ alalım.

3) Matrisleri hesaplayalım.

$$I=D^2=\begin{pmatrix}7 & 20\\ 15 & 17\end{pmatrix},\quad J=D^3=\begin{pmatrix}4 & 24\\ 23 & 6\end{pmatrix}$$

$$I^2=\begin{pmatrix}24 & 5\\ 10 & 14\end{pmatrix},\quad J^2=\begin{pmatrix}18 & 15\\ 5 & 13\end{pmatrix}$$

$$I^2J=\begin{pmatrix}24 & 5\\ 10 & 14\end{pmatrix}\begin{pmatrix}4 & 24\\ 23 & 6\end{pmatrix}=\begin{pmatrix}11 & 6\\ 12 & 24\end{pmatrix}$$

$$IJ^2=\begin{pmatrix}7 & 20\\ 15 & 17\end{pmatrix}\begin{pmatrix}18 & 15\\ 5 & 13\end{pmatrix}=\begin{pmatrix}1 & 15\\ 5 & 21\end{pmatrix}$$

4) Rastgele bir $N\in GL(2,\mathbb{Z}_{25})$ seçelim.

$$N=\begin{pmatrix}7 & 8\\ 3 & 4\end{pmatrix},\quad N^{-1}=\begin{pmatrix}1 & 23\\ 18 & 8\end{pmatrix}$$

5) $M_2(\mathbb{Z}_{25})$ halkasında aşağıdaki otomorfizmaları tanımlayalım.

$$x:V\to I^{-1}VI,\qquad \delta:V\to J^{-1}VJ,\qquad \forall\, V\in M_2(\mathbb{Z}_{25})$$

$$\rho=x^2\delta,\qquad \sigma=x\delta^2$$

$$\rho:V\to (I^2J)^{-1}V(I^2J),\qquad \sigma:V\to (IJ^2)^{-1}V(IJ^2)$$

6) Aşağıdaki matrisleri hesaplayalım.

$$IJ = \begin{pmatrix} 13 & 13 \\ 1 & 12 \end{pmatrix}$$

$$(I^2J)^{-1} = \begin{pmatrix} 22 & 7 \\ 14 & 8 \end{pmatrix},\ (IJ^2)^{-1} = \begin{pmatrix} 1 & 10 \\ 20 & 6 \end{pmatrix}$$

$$\rho(N) = \begin{pmatrix} 22 & 7 \\ 14 & 8 \end{pmatrix}\begin{pmatrix} 7 & 8 \\ 3 & 4 \end{pmatrix}\begin{pmatrix} 11 & 6 \\ 12 & 24 \end{pmatrix} = \begin{pmatrix} 0 & 4 \\ 22 & 19 \end{pmatrix}\begin{pmatrix} 11 & 6 \\ 12 & 24 \end{pmatrix}$$

$$= \begin{pmatrix} 23 & 21 \\ 20 & 13 \end{pmatrix}$$

$$\sigma(N^{-1}) = \begin{pmatrix} 1 & 10 \\ 20 & 6 \end{pmatrix}\begin{pmatrix} 1 & 23 \\ 18 & 8 \end{pmatrix}\begin{pmatrix} 1 & 15 \\ 5 & 21 \end{pmatrix} = \begin{pmatrix} 6 & 3 \\ 3 & 8 \end{pmatrix}\begin{pmatrix} 1 & 15 \\ 5 & 21 \end{pmatrix}$$

$$= \begin{pmatrix} 21 & 3 \\ 18 & 13 \end{pmatrix}$$

7) Genel anahtarımız,

$$\left(n = 25, \rho(N) = \begin{pmatrix} 23 & 21 \\ 20 & 13 \end{pmatrix}, \sigma(N^{-1}) = \begin{pmatrix} 21 & 3 \\ 18 & 13 \end{pmatrix},\ IJ = \begin{pmatrix} 13 & 13 \\ 1 & 12 \end{pmatrix}\right)$$

ve özel anahtarımız $\left(I = \begin{pmatrix} 7 & 20 \\ 15 & 17 \end{pmatrix}, J = \begin{pmatrix} 4 & 24 \\ 23 & 6 \end{pmatrix}\right)$ olur.

Şifreleme

Aşağıdaki adımları gerçekleştirelim.

1) $M_2(\mathbb{Z}_{25})$ da açık metinleri temsil eden bir matris m olsun.

$$m = \begin{pmatrix} 11 & 4 \\ 13 & 7 \end{pmatrix} \in M_2(\mathbb{Z}_{25})$$

2) Rastgele bir k tamsayısı için k=3 seçelim ve matrisleri hesaplayalım.

$X=(IJ)^3 = \begin{pmatrix} 16 & 16 \\ 7 & 9 \end{pmatrix}$, $X^{-1} = \begin{pmatrix} 12 & 12 \\ 24 & 13 \end{pmatrix}$

3) $M_2(\mathbb{Z}_{25})$ halkası üzerinde ϑ otomorfizmasını tanımlayalım.

$\vartheta: V \to X^{-1}VX, \quad \forall V \in M_2(\mathbb{Z}_{25})$ için.

4) Matrisleri hesaplayalım.

$\vartheta\,(\rho(N))=X^{-1}\rho(N)X = \begin{pmatrix} 12 & 12 \\ 24 & 13 \end{pmatrix}\begin{pmatrix} 23 & 21 \\ 20 & 13 \end{pmatrix}\begin{pmatrix} 16 & 16 \\ 7 & 9 \end{pmatrix}$

$= \begin{pmatrix} 16 & 8 \\ 12 & 23 \end{pmatrix}\begin{pmatrix} 16 & 16 \\ 7 & 9 \end{pmatrix}$

$= \begin{pmatrix} 12 & 3 \\ 3 & 24 \end{pmatrix}$

$\vartheta\,(\sigma(N^{-1}))=X^{-1}\,\sigma(N^{-1})X= \begin{pmatrix} 12 & 12 \\ 24 & 13 \end{pmatrix}\begin{pmatrix} 21 & 3 \\ 18 & 13 \end{pmatrix}\begin{pmatrix} 16 & 16 \\ 7 & 9 \end{pmatrix}$

$= \begin{pmatrix} 18 & 17 \\ 13 & 16 \end{pmatrix}\begin{pmatrix} 16 & 16 \\ 7 & 9 \end{pmatrix}$

$= \begin{pmatrix} 7 & 16 \\ 20 & 2 \end{pmatrix}$

5) Şimdi $\mathbb{Z}_{25}$' dan rastgele bir μ elemanını, $\mu = 7$ seçelim ve 25 moduna göre tersini, μ^{-1}=18 olarak buluruz.

6) Şifreli metni hesaplayalım.

$C = (C_1, C_2)$

$C_1=\mu^{-1}\vartheta\,(\sigma(N^{-1}))=18\begin{pmatrix} 7 & 16 \\ 20 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 13 \\ 10 & 11 \end{pmatrix}$

$C_2= \mu m\,\vartheta(\rho(N))=7\begin{pmatrix} 11 & 4 \\ 13 & 7 \end{pmatrix}\begin{pmatrix} 12 & 3 \\ 3 & 24 \end{pmatrix}= \begin{pmatrix} 2 & 3 \\ 16 & 24 \end{pmatrix}\begin{pmatrix} 12 & 3 \\ 3 & 24 \end{pmatrix}$

$= \begin{pmatrix} 8 & 3 \\ 14 & 24 \end{pmatrix}$

Deşifreleme

Düz metni elde etmek amacıyla aşağıdaki adımları yapalım.

1) Özel anahtarı kullanarak, D matrisini hesaplayalım.

$D= x\delta^{-1}(C_1) = (IJ^{-1})^{-1}C_1(IJ^{-1})$

$J^{-1}= \begin{pmatrix}23 & 8\\ 16 & 7\end{pmatrix}$, $IJ^{-1}=\begin{pmatrix}7 & 20\\ 15 & 17\end{pmatrix}\begin{pmatrix}23 & 8\\ 16 & 7\end{pmatrix}=\begin{pmatrix}6 & 21\\ 17 & 14\end{pmatrix}$

$(IJ^{-1})^{-1}=\begin{pmatrix}7 & 2\\ 4 & 3\end{pmatrix}$

$D =\begin{pmatrix}7 & 2\\ 4 & 3\end{pmatrix}\begin{pmatrix}1 & 13\\ 10 & 11\end{pmatrix}\begin{pmatrix}6 & 21\\ 17 & 14\end{pmatrix}$

$=\begin{pmatrix}2 & 13\\ 9 & 10\end{pmatrix}\begin{pmatrix}6 & 21\\ 17 & 14\end{pmatrix}$

$=\begin{pmatrix}8 & 24\\ 24 & 4\end{pmatrix}$

2) Aşağıdaki matris işlemlerini hesaplayarak sonunda düz metni elde ederiz.

$m=C_2D =\begin{pmatrix}8 & 3\\ 14 & 24\end{pmatrix}\begin{pmatrix}8 & 24\\ 24 & 4\end{pmatrix}$

$=\begin{pmatrix}11 & 4\\ 13 & 7\end{pmatrix}$

Uyarı : 25 moduna göre işlem yaptığımızda, harflerden oluşan bir metni veya mesajı şifrelemek istersek, kullandığımız alfabenin de 25 harfi geçmemesi gerekecektir.

3.4. Sonuç

Bu şifreleme yönteminde daha az hesaplamalı ve daha güvenli kriptosistemler incelendi. İki farklı açık anahtarlı kriptosistemlerin algoritmasını verdik ve her ikisini de sayısal örnekleri kullanarak şifreleme tekniklerini test ettik. Her iki sistemde güvenlik yönünden daha hızlı ve dengelidir. Açık anahtarlı kriptosistemlerin kullanılmasının en önemli nedeni, anahtarın simetrik şifreler için protokolleri değiştirmesidir. Bu değişim farklı uygulamalarda daha basit ve verimli olmaktadır.

3.5. Tartışma ve Öneriler

Genel Lineer Grupları kullanarak yapılan Kriptosistem, güvenli ve başarılı olarak değerlendirilebilir. Bu kriptosistemi kırmak için yapılan saldırıların başarılı olma olasılığı çok azdır. Çünkü bu şifrelemede kullanılan ikili matris çarpımlarının kapalı varyasyon değerleri değişmektedir. Matris çarpımlarının değerleri değiştiği için ortaya çıkan çok fazla çözümden hangisinin doğru olduğunu tespit etmek imkansız hale gelir. Ayrıca tek kullanımlık anahtarların kullanılması da sistemin güvenliğini arttırmaktadır.
Bu çalışmanın devamında farklı boyutlardaki matrislerle ifade edilebilecek her türlü bilgilerin şifrelenmesi sağlanabilir.

KAYNAKLAR

1. Altındiş, H. 2011. Sayılar Teorisi ve Uygulamaları, Lazer Ofset, Ankara, 308 s.
2. Karabaş, C. 2010.Özel Lineer Gruplar ve Mor Kriptosistem. Erciyes Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, Kayseri, 62s.
3. Khan, M. 2015.Construction And Applications Of Cryptographically Secure Chaotic Nonlinear Component For Blocak Ciphers, Pakistan, 252s.
4. Öztürkmenoğlu, Ş.C. 2016.Matrislerle Şifreleme Üzerine. Muğla Sıtkı Koçman Üniversitesi Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, Muğla, 64s.
5. Yeşilbaş, E. 2016.Cebirsel Kriptoloji Yöntemleri ve Bazı Uygulamaları. Recep Tayyip Erdoğan Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, Rize, 78s.
6. Hassanpour, A.A. 2015.Asal Sayıların Şifreleme Teorisindeki Uygulamaları. Atatürk Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, Erzurum, 85s.
7. Lüy, E. 2012.Abelyan Olmayan Sonlu Gruplar Kullanılarak Elde Edilen Açık Anahtar Kriptosistem Üzerine. Erciyes Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, Kayseri, 61s.
8. Kart, C. 1985. Matris Metodları ve Lineer Dönüşümler. Ankara Üniversitesi Fen Fakültesi Yayınları, Ankara, 322 s.
9. Sezer, M. 1990. Lineer Cebir ve Analitik Geometri. Dokuz Eylül Üniversitesi, İzmir, 61s.
10. Çeşmeci, M.Ü.,2009.Elektronik Çağ Öncesi Dönem Kriptoloji Tarihi. **Tubitak Uekae Dergisi 1:**20-32.
11. Soyalıç, S. 2005.KriptografikHash Fonksiyonları ve Uygulamaları. Erciyes Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, Kayseri 92s.
12. Okumuş, İ. 2012. RSA Kriptosisteminin Hızını Etkileyen Faktörler. Atatürk Üniversitesi, Fen Bilimleri Enstitüsü, Doktora Tezi, Erzurum 68 s.
13. Taşçı, D. 2007. Soyut Cebir. Alp Yayınevi, Ankara, 671 s.
14. Koblitz, N.,1994. A Course in Number Teory and Cryptografy, Springer-Verlag, Yer, New York, 235 pp.
15. Kara, O., 2009. Kriptografinin Yapıtaşları Kriptografik Algoritmalar ve Protokoller. **Bilim Teknik, 500:**34-50

16. Çimen, C. , Akleylek, S., Akyıldız, E., 2007. Şifrelerin Matematiği: Kriptografi, ODTÜ Bilim ve Toplum Kitapları Dizisi, Ankara, 131 s.
17. Kara, O. 2009. II. Dünya Savaşından Günümüze Kriptoloji: Enigma'dan AES'E Şifreleme. **Bilim Teknik, 500:**28-34
18. Çimer, C. , Akleylek, S., Akyıldız, E., 2009. Şifrelerin Matematiği: Kriptografi, 4. Baskı, Orta Doğu Teknik Üniversitesi, Toplum Bilim Merkezi, Ankara, 131 s.
19. **http://en.wikipedia.org/wiki/Scytale (25 Ocak 2016)**
20. **http://en.wikipedia.org/wiki/Jefferson_disk (30 Ocak 2016)**
21. **http://e-bergi.com/y/enigma (23 Nisan 2016)**

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı Soyadı : Murat KORKMAZ
Baba Adı : İsmail
Anne Adı : Ayşe
Doğum Yeri : Sarız / KAYSERİ
Doğum Tarihi : 10.01.1988

EĞİTİM

Derece	**Kurum**	**Mezuniyet Tarihi**
Lisans	Erciyes Üniversitesi Fen Fakültesi Matematik Bölümü	2010
Ortaöğrenim	Kocasinan Atatürk Lisesi, Kayseri	2005