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

# TAM (FULLY) HOMOMORFİK KRİPTOSİSTEMLER

**Hazırlayan**
**Gülhanım YALÇINKAYA**

**Danışman**
**Dr. Öğr. Üyesi Emin AYGÜN**

**Yüksel Lisans Tezi**

**Temmuz 2018**
**KAYSERİ**

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

# TAM (FULLY) HOMOMORFİK KRİPTOSİSTEMLER

**(Yüksel Lisans Tezi)**

**Hazırlayan**
**Gülhanım YALÇINKAYA**

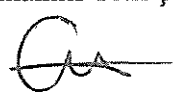
**Danışman**
**Dr. Öğr. Üyesi Emin AYGÜN**

**Temmuz 2018**
**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.

Gülhanım YALÇINKAYA



# YÖNERGEYE UYGUNLUK

**"Tam(Fully) Homomorfik Kriptosistemler"** adlı Yüksek Lisans tezi, Erciyes Üniversitesi Lisansüstü Tez Önerisi ve Tez Yazma Yönergesi'ne uygun olarak hazırlanmıştır.

Tezi Hazırlayan

Gülhanım YALÇINKAYA

Danışman

Dr. Öğr. Üyesi Emin AYGÜN

Prof. Dr. Hüseyin ALTINDİŞ

ABD Başkanı

Dr. Öğr. Üyesi Emin AYGÜN danışmanlığında **Gülhanım YALÇINKAYA** tarafından hazırlanan **"Tam(Fully) Homomorfik Kriptosistemler"** adlı bu çalışma, jürimiz tarafından Erciyes Üniversitesi Fen Bilimleri Enstitüsü **Matematik** Anabilim Dalında **Yüksek Lisans** tezi olarak kabul edilmiştir.

06/ 07 / 2018

**JÜRİ:**

Başkan : Doç.Dr. Abdulcabbar SÖNMEZ .....

Üye : Dr. Öğr. Üyesi Funda TAŞDEMİR .....

Üye : Dr. Öğr. Üyesi EminAYGÜN .....

ONAY:

Bu tezin kabulü, Enstitü Yönetim Kurulunun 17/07/2018 tarih ve 2018/30-50 sayılı kararı ile onaylanmıştır.

17/07/2018

Prof. Dr. Mehmet AKKURT
Enstitü Müdürü

# TEŞEKKÜR

Çalışmalarım boyunca farklı bakış açıları ve bilimsel katkılarıyla beni aydınlatan, yakın ilgi ve yardımlarını esirgemeyen ve bu günlere gelmemde en büyük katkı sahibi sayın hocam Dr. Öğr. Üyesi Emin AYGÜN' e teşekkürü bir borç bilirim.

Ayrıca; çalışmalarım süresince sabır göstererek beni daima destekleyen aileme en içten teşekkürlerimi sunarım.

Gülhanım YALÇINKAYA

Kayseri, Temmuz 2018

**FULLY(TAM) HOMOMORFİK KRİPTOSİSTEMLER**

**Gülhanım YALÇINKAYA**

**Erciyes Üniversitesi, Fen Bilimleri Enstitüsü**
**Yüksek Lisans Tezi, Temmuz 2018**
**Danışman: Dr. Öğr. Üyesi Emin AYGÜN**

# ÖZET

Bu tez üç bölümden oluşmaktadır. Birinci bölümde temel tanım ve teoremler ile daha sonra kullanılacak bazı önbilgiler verildi.

İkinci bölümde Ceasar, RSA, El-Gamal gibi çok bilinen şifreleme metodları açıklandı, bu metodların homomorfik özellikleri incelendi ve bu metodlar örneklendirildi.

Üçüncü bölümde tam(fully) homomorfik şifreleme şeması detaylı bir şekilde açıklandı ve örneklendirilmesi yapıldı.

**Anahtar Kelimeler:** Homomorfik Şifreleme, DLP, Matris, Çin kalan Teoremi

**FULLY HOMMOMORPHIC CRYPTOSYSTEMS**

**Gülhanım YALÇINKAYA**

**Erciyes University, Graduate School of Natural and Applied Sciences**
**M.Sc. Thesis, July 2018**
**Supervisor: Dr. Emin AYGÜN**

## ABSTRACT

This thesis consists of three chapters. In the first chapter the fundamental notions and theorems and the preliminaries which will be used later has been expressed.

In the second chapter, we have explained and sampled homomorphic properties of some known schemes like Ceasar, RSA, El-Gamal.

In the third chapter, the fully homomorphic crypto system scheme is explained in detail and exemplified.

**Keywords:** Homomorphic Encryption, DLP, Matrix, Chinese Remainder Theorem.

# İÇİNDEKİLER

## TAM (FULLY) HOMOMORFİK KRİPTOSİSTEMLER

# ŞEKİLLER LİSTESİ

# KISALTMALAR VE SİMGELER

| **Sembol** | | **Anlamı** |
|---|---|---|
| FHE | : | Full Homomorfik Kriptosistem |
| CKT | : | Çin Kalan Teoremi |
| DLP | : | Discrete Logaritma Problemi |
| DES | : | Data Encryption Standart |
| NIST | : | National Institute of Standarts and Technology |
| ECC | : | Eliptic Eğri Kriptosistemler |
| SHA | : | Secure Hash Algorithm |
| AES | : | Advanced Encryption Standart |
| IBM | : | International Business Machines |
| FIPS | : | Federal Information Processing Standart |
| $\left(\frac{a}{p}\right)$ | : | Legendre Sembolü |
| R | : | Rezidü |
| N | : | Rezidü Değil |
| $(a, m)$ | : | $a$ sayısı ile $m$ sayısının en büyük ortak böleni |
| $[a, m]$ | : | $a$ sayısı ile $m$ sayısının en küçük ortak katı |
| $ord_{m^a} = t$ | : | $a$ nın $m$ modülüne göre mertebesi $t$ dir |
| $\phi$ | : | Eulerin Fi Fonksiyonu |
| $(\,)_{11}$ | : | matrisin 1. satır ve 1. sütunundaki elemanlar |

# GİRİŞ

Kriptografi, Yunanca gizli anlamına gelen kryptos ve yazı anlamına gelen graphein kelimelerinden türetilmiştir. Kriptoloji ise Yunanca kryptos logos kelimelerinden türetilmiştir. Kryptos gizli saklı logos ise neden sonuç ilişkisi kurma anlamına gelmektedir.

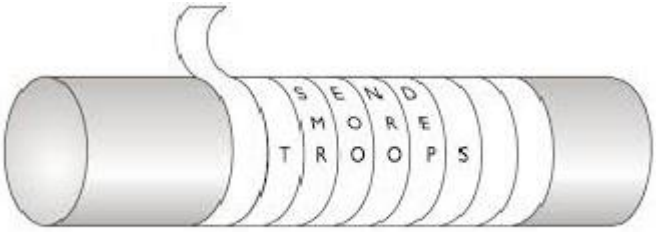
Şifreleme bir bilgiyi istenmeyen şahıslardan korumak amacıyla bir takım yöntemler kullanarak anlaşılmaz hale getirme işlemidir. Deşifreleme ise şifrelenmiş bilgiden alınmak istenen bilgiyi elde etme işlemidir.

Eski çağlardan beri insanlar bilginin güvenliğini sağlamak için çeşitli şifreleme yöntemleri kullanmışlardır. M.Ö.1900'lü yıllarda Mısırlıların yazdığı hiyeroglifler bilinen en eski şifreleme örnekleridir. Mısır'da Menet Khufu kasabasında bulunan hiyeroglifler bilinen ilk yazılı kriptografik belgelerdir.

M.Ö.1500'lü yıllarda Mezopotamya'daki çivi yazılarının bazılarının okunamadığı görülmüştür. Bunların şifrelenmiş ifadeler olduğu anlaşılmıştır. Daha sonra yapılan kriptolojik analizler sonrasında okunamayan metinlerden birinin, çömlek yapımı için geliştirilmiş olan bir birleşimin şifreli olarak kaydını içerdiği anlaşılmıştır.

M.Ö.590 dolaylarında Jeremiah'ın kitabındaki İbranice yazılarda Atbash şifreleme metodu kullanılmıştır. Atbash ters alfabe kullanılarak yapılan basit yerine koyma şifreleme metodudur.

M.Ö.487'de Spartalılar Scytale adı verilen bir şifreleme tekniği kulalanmışlardır. Tahta bir çubuk etrafına şerit şeklinde deri ya da parşömen sarılarak oluşturulmuş tekniktir. Askeri alanda kullanılan ilk şifreleme yöntemidir [1].




Şekil 1. Scytale Şifreleme

M.Ö.300'de Hindistan'da Kautilya tarafından yazılan Arthashastra kitabında istihbarat bilgilerine ulaşılmasını sağlayan çeşitli kriptanaliz metodlarını tavsiye eder.

M.Ö.100-44 yıllarında Julius Caesar düz metindeki her harfin alfabede kendinden sonraki 3. harfle yer değiştirmesi sonucu oluşan Caesar şifreleme metodunu bulmuştur. Caesar bu metodu devlet haberleşmelerinde kullanmıştır.

725-790 Abu Abd al-Rahman al-Khalil ibn Ahmad ibn Amr ibn Tammam al Farahidi al-Zadi al Yahmadi(daha çok Al Farahidi olarak bilinir), kriptografi üzerine Kitab al Mu'amma adlı kitabı yazdı. Kitapta Bizans imparatoru için Yunanca yazılmış şifreli metni nasıl çözdüğü anlatılmaktadır. Kitap kayıp durumdadır.

1000-1200 Gazneliler' den kalan bazı dokümanlarda şifreli metinler bulunmuştur. Bir tarihçinin dönemle ilgili araştırmalarına göre yüksek makamlardaki devlet görevlilerine yeni görev yerlerine giderken kişiye özel şifreleme bilgileri (belki şifreleme anahtarları) veriliyordu.

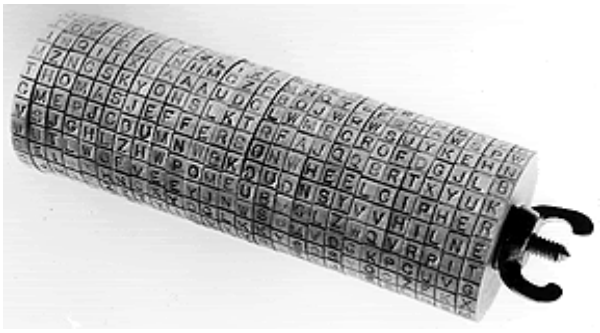
1404-1472 Leone Battista Alberti Caesar şifrelemenin kullanımını basitleştiren eşmerkezli iki diskten oluşan bir alet geliştirdi. Alberti Diski adı verilen bu alet yardımıyla içteki çember sabit dıştaki çember onun etrafında dönebilir şekilde her harfin istenilen miktarda ötelenmesi kolaylıkla yapılabiliyordu.

Şekil 2. Alberti Diski

1586 yılında Blaise de Vigenere, Caesar kriptosisteminin bir türevi olan Vigenere şifreleme metodunu geliştirdi. Bu şifreleme metodunda açık metin ve şifreli metin için otomatik anahtarlama yönteminde bahsedilmiştir. Vigenere şifresi 1800'lü yılların ortalarına kadar kırılması imkansız olarak nitelendirildi. Charles Babbage, bu şifreyi kırmayı başardı ve 1864 yılında "Gizli Yazma ve Şifre Çözme Sanatı " adlı kitabında bu yöntemi yayınladı.

1623' de Sir Francis Bacon, stenografi buldu. Stenografi, alfabenin harfleri, noktalama işaretleri, kelimeleri yerine semboller ve kısaltmalar kullanan çabuk yazma sistemidir. Yazılar yakın, küçük ve dar yazıldığı için bu adı almıştır. Stenografi, meclis oturumlarında, mahkeme duruşmalarında, iş görüşmelerinde oldukça yaygın bir şekilde kullanılmaktadır.

1790' da Pensilvanya Üniversitesi' nde matematikçi olan Thomas Jefferson, Wheel (tekerlek) şifresini icat etti. Jefferson'ın cihazı her birinde alfabenin harflerinin yazılı olduğu 36 diskten oluşuyordu.



Şekil 3. Jefferson Tekerleği

1854'de Charles Wheatstone arkadaşı Lyon Playfair'in adını koyduğu playfair şifresini bulmuştur. Playfair şifreleme oldukça basit uygulanan bir blok şifreleme yöntemidir. $5 \times 5$ boyutunda bir matris alınarak şifreleme yapılır.

1861' de Friedrich W. Kasiski, tekrar eden harf gruplarını kullanan çok alfabeli şifrenin ilk genel çözümünü veren bir kitap yayınladı. Böylelikle yıllarca güçlü kabul edilen çok alfabeli şifre artık zayıf olarak kabul edilmiştir.

1876' da Rutherford Hayes ve Samuel Tilden' in aday oldukları Amerika Birleşik Devletleri başkanlık seçimlerinde 4 eyaletin seçim sonuçlarında anlaşmazlık yaşanmıştır. Tilden taraftarlarının birbirine gönderdikleri şifreli mesajlar ortaya çıkartılmış, kriptoanalistlerin yaptıkları incelemeler sonunda, gerçek mesajdaki kelimeler yerine farklı kelimeler kullanılarak bir bilgi gizleme tekniği uygulandığı anlaşılmıştır.

Alman ajanı Fritz Nebel tarafından I. Dünya savaşı sırasında geliştirilen iki şifreleme algoritması bulunur. Bunlar ADFGX ve ADFGVX olarak geçmektedir. Almanların Fransa saldırısı sırasında Fransız Geoges Painvin tarafından kırılarak alman birliğinin konumunun bulunması ve bu yüzden alman saldırısının başarısızlığı 1918 yılında yaşanan tarihi olaylardır.

1917 de 1. Dünya Savaşı sırasında Gilbert Vernam Almanların çözemeyeceği bir şifreleme metodu icat etmekle görevlendirilmişti ve bunun sonucu olarak önce akış şifrelemeyi icat etmiş ve sonrasında Joseph Mauborgne ile mükemmel şifreleme tekniği olan one-time pad (tek kullanımlık bloknot) şifreleme metodunu bulmuşlardır.

1920-1930‘da William Frederick Friedman, Riverbank Laboratuarlarını kurarak ABD için kriptoanaliz yaptı ve Japonlar’ ın 2. Dünya Savaşı sırasında Purple Machine şifreleme sistemini çözdü.

1923 başında Alman donanmasının kullanmaya başladığı Enigma şifreleme cihazı, 1930’lu yılların ortasında, ordunun temel bilgi güvenliği cihazı olarak tescil edildi. Alman ordusu muhabere birimlerindeki görevliler gönderilecek olan mesajı Enigma cihazının tuş takımı üzerinden yazıyor, mesaj cihaz içerisinde şifreleniyor ve elde edilen şifreli mesaj telsiz operatörü tarafından mors kodu kullanılarak, radyo dalgaları ile karşı tarafa gönderiliyordu. Enigma, mekanik ayarlarla yönlendirilen elektronik bir cihazdı 1918 yılında Arthur Scherbius tarafından ticari uygulamalarda kullanılmak üzere geliştirilmiş ve ilk olarak bankalar arasındaki haberleşmede kullanılmıştı. Alman ordusunun Enigma’yı kullanma kararı sonrasında, İkinci Dünya Savaşı süresince toplam yüzbin kadar Enigma kripto cihazı üretilmiştir. Enigma kripto cihazı, 21. yüzyıla kadar en yüksek miktarda üretilen kripto cihazı olma özelliğini korumuştur. Enigma cihazı matematikçi olan Alan Turing ve ekibi tarafından çözüldü.

1933’ de Japonlar mesajları şifrelemek için Purple makinasını icat ettiler. Bu makine alfabedeki harflerin yerini değiştirmek için rotorları kullanmıştır. Cihaz iki daktilo ve 25 karakterli alfabetik denetim santraline sahip bir elektrikli rotor sisteminden oluşmaktaydı.

1952’ de ABD’de Resmi olarak Ulusal Güvenlik Teşkilatı (NSA) kuruldu. Kriptoloji üzerine uzman bir teşkilattır.

1970’de Horst Feistel (IBM) DES’in temelini oluşturan Lucifer algoritmasını geliştirdi. Lucifer algoritmasındaki en önemli problem anahtar uzunluğunun orjinalde 128 bit olmasıydı. Daha sonra bazı düzenlemeler yapılarak anahtar uzunluğu 56 bite düşürülmüştür.

1976’ da Açık Anahtarlı Kriptografi doğdu. Whitfield Diffie ve Martin Hellman açık anahtarlı kriptografiyi anlatan New Direction in Crytography (Kriptografi’de Yeni Yönler ) kitabını yayınladı.

1976’ da DES (Data Encryption Standard), ABD tarafından FIPS 46 (Federal Information Processing Standard) standardı olarak açıklandı. Bu şifreleme yönteminde şifrelenecek metin parçalara bölünür ve her bir şifre ayrı ayrı şifrelenir.

1978’ de RSA Algoritmasını, Ronald L. Rivest, Adi Shamir ve Leonard M. Adleman önerdi. Şifreleme yönteminin adı bu üç kişinin soy isimlerinin baş harflerinden oluşur. RSA şifreleme metodunun güvenliği büyük sayıların çarpanlarının hesaplanmasının zorluğuna dayanır.

1985’ de Mısırlı bir matematikçi olan Taher El-Gamal tarafından El-Gamal Şifreleme Metodu bulundu. 1985 yılında. El-Gamal açık anahtarlı şifreleme metodunun güvenliği ayrık logaritma probleminin (DLP) zorluğuna dayanmaktadır.

1985’ de Neal Koblitz ve Victor S. Miller ayrı yaptıkları çalışmalarda (ECC) eliptik eğri kriptografik sistemlerini buldu. Eliptik eğri şifreleme metodunun mantığı gönderilecek mesajın iki boyutlu uzaydaki noktalara dönüştürülmesidir. Aynı zamanda dönüştürülen noktalardan da orjinal metne ulaşılması sağlanır.

1990’ da Xuejia Lai ve James Massey tarafından bir blok şifreleme olan IDEA algoritmasını tasarlanmıştır. Bilinen en güçlü algoritmalardandır. İlk öncelerini PES adıyla anılan bu algoritma geçirdiği revizyonlar ertesinde şu andaki halini almıştır.

1991’ de Phil Zimmerman PGP (Pretty Good Privacy) sistemini geliştirdi ve yayınladı. PGP’ nin amacı sadece dosya ve e-maillerin korunmasıdır. PGP nin Dünya’daki en yaygın e-mail şifreleme protokolü olduğu söylenebilir.

1995’ de SHA-1(Secure Hash Algorithm) özet algoritması NIST (National Institute of Standards and Technology) tarafından standart olarak yayınlandı. Uzaktan erişim uygulamaları, e-posta güvenliği uygulamaları, bilgisayar ağlarının özel uygulamaları gibi bir çok alanda kullanılır.

1997’ de ABD’nin NIST (National Institute of Standards and Technology) kurumu DES(Data Encryption Standard)’ in yerini alacak bir simetrik algoritma için yarışma açtı.

2001’ de NIST’in yarışmasını kazanan Belçikalı Joan Daemen ve Vincent Rijmen’e ait Rijndael algoritması, AES (Advanced Encryption Standard) adıyla standard haline getirildi. AES algoritmasında giriş, çıkış ve matrisler 128 bitliktir. Matris 4 satır, 4 sütun $(4 \times 4)$, 16 bölmeden oluşur. Bu matrise ‘durum’ denmektedir. Durumun her bölmesine bir baytlık veri düşer. Her satırda 32 bitlik bir kelimeyi meydana getirir. AES algoritması, 128 bit veri bloklarını 128, 192 veya 256 bit anahtar seçenekleri ile şifreleyen bir blok şifre algoritmasıdır [2], [3], [4], [5], [6], [7].

Günümüzde ise ticaretin ve bankacılığın elektronik ortamda yapılmaya başlanılmasından dolayı kriptolojinin önemi daha da artmıştır. Elektronik bankacılığın kullanımının artması, elektronik posta kullanımının yaygınlaşması ve cep telefonunun insan hayatındaki önemi göz önüne alındığında bilgi güvenliğinin önemi daha iyi anlaşılmaktadır.

Kriptografi artık şifreleme ve deşifrelemeden çok daha fazlasını içermektedir. Özellikle göndermek istenilen bilgilere isim eklemek zorunda olunduğunda, bu ismin gerçekliğini ve güvenliğini sağlamak amacıyla kimlik denetimi yapılmaktadır. Bunun için de sayısal (dijital) imza geliştirilmiştir. Sayısal imza kimlik saptama, yetki verme ve onaylama işlerini yapacak bir şekilde kişiye özel olarak hazırlanır. Sayısal imza, yazının içeriğine ve imzalayanın gizli anahtarına bağlı bir kriptografik yöntemle atıldığı için sayısal imzanın doğrulanmasında imzayı atanın açık anahtarı kullanılır.

Son zamanlarda ise, bilgiyi şifreleme ve deşifrelemenin yanı sıra şifreli bilgi üzerinde işlemler yapmaya imkan sağlayan şifreleme sistemleri geliştirilmeye çalışılmaktadır. Şifreli bilgiler üzerinde işlemler yapmaya izin veren kriptosistemlere homomorfik kriptosistemler denir.

1978 yılında Rivest, Adleman ve Dertouzos şifreli bilgiler üzerinde işlem yapma çalışmalarına başlamıştır [8]. 1978 yılından bu yana çeşitli çalışmalar yapılmıştır. Bazı kriptosistemler tek bir işleme göre homomorfiktir. RSA ve El-Gamal şifreleme metodları sadece çarpma işlemine göre homomorfiktir [9]. 1982 yılında S. Goldwasser ve S. Micali tarafından yapılan Goldwasser-Micali kriptosistemi toplamaya göre homomorfiktir [10], [11]. Bu sistemin genellemesi olan 1999 yılında P.Pailer tarafından yapılan Pailer kriptosistemi de toplamaya göre homomorfiktir. Ancak bu iki sistem için

toplamaya göre homomorfiklikten kasıt, iki şifreli metnin çarpımının deşifresinin açık metinlerin toplamını vermesidir.

Yukarıda ki kriptosistemlerin hiç birisi her iki işleme göre homomorfik olma özelliğini sağlamamaktadır. Her iki işleme göre homomorfik özelliği sağlayan kriptosistemlere tam(fully) homomorfik kriptosistemler denir. Yani tam(fully) homomofik kriptosistemlerde şifremetinler üzerinde toplama ve çarpma işlemleri istenildiği kadar yapıldığında bile, şifremetinlerin deşifresi orijinal metni vermektedir.

2005 yılında D. Boneh, E-J. Goh ve K. Nissim, tarafından yapılan kriptosistemde şifreli metinler üzerinde bir tek çarpma ve sınırsız sayıda toplama yapılabildiğinden bu kriptosistem kısmi homomorfiktir [12].

2009 yılında Dan Boneh' in doktora öğrencisi Craig Gentry, kendisinin doktora tezinde, o zamana kadar bilinen ilk tam(fully) homomorfik kriptosistemi yapmayı başarmıştır. Şifremetinler üzerinde iki işlemi birden yapmaya sınırlı sayıda izin veren şemalara Somewhat Homomorfik şemalar adı verilir. Gentry de önce somewhat homomorfik şema ile başlamış, daha sonra Bootstrapping adını verdiği bir teknikle şemasını tam(fully) homomorfik şekle dönüştürmüştür [13], [14], [15].

2010 yılında Van Dijk, Halevi ve Vaikuntanathan, tam sayılar kullanılarak yapılan, hem gizli anahtarlı hem de açık anahtarlı somewhat homomorfik bir şemayı yine Gentry' nin bootstrap teknikleri ile tam(fully) homomorfik şekle dönüştürmüştür.

2011 yılında Chunsheng tarafından yapılan çalışmada matrisler kullanılmıştır. Yapılan çalışmada matrislerin yanı sıra latisler de kullanılmıştır [18]

2012 ve 2013 yıllarında yapılan çalışmalardaki kriptosistemlerde matrisler kullanılmıştır. Bu sistemin güvenliği çarpanlara ayırmanın zorluğuna dayanmaktadır. Bu kriptosistem, çarpanlara ayırmanın zorluğuna dayanan ilk tam(fully) homomorfik kriptosistemdir.

Homomorfik kriptosistemler elektronik oylama (e-seçim) ve bulut bilişim (Cloud Computing) de yaygın bir şekilde kullanılmaktadır. e-seçim sistemi 1991' de ilk olarak Belçika' da iki bölgede iki farklı sistemle başlatıldı. Bu sistemin uygulamaları Hindistan ve Kanada da yapılmıştır [19]. Elektronik oylamayı bir örnekle açıklayalım:

10 kişi 2 aday için, her iki adaya 1 ile 100 arasında puanlar versin.1. aday için verilen gerçek puanlar $a_1, a_2, a_3, \ldots, a_{10}$ ve 2. aday için verilen gerçek puanlar $b_1, b_2, b_3, \ldots, b_{10}$ olsun. Her bir oyun şifrelenmiş halleri de sırasıyla $p_1, p_2, p_3, \ldots, p_{10}$ ve $q_1, q_2, q_3, \ldots, q_{10}$ olsun. 1. aday için verilen şifreli puanların toplamı olan $p_1 + p_2 + p_3 + \cdots + p_{10} = G$ toplamının deşifrelenmesi orijinal puanların toplamı olan $a_1 + a_2 + a_3 + \cdots + a_{10} = Y$ toplamını veriyorsa, bu takdirde seçimi yöneten kişi oy verenlerin 1. adaya kaç puan verdiğini bilmeden, sadece şifreli puanların toplamı olan $G$ toplamını deşifre ederek 1. aday için gerçek puan toplamına ulaşabilir. Aynı şekilde 2. aday içinde gerekli işlemler yapılarak gerçek puan toplamları kıyaslanır ve seçimin galibi belirlenir. Burada homomorfik şifreleme kullanılarak oy verenlerin hangi adaya kaç puan verdiği bilinmeden seçim tamamlanmış olur.

Bulut bilişim (Cloud Computing), çevrim içi bilgi dağıtımı amacıyla kullanılan ve çeşitli hesaplama kaynaklarından oluşan internet tabanlı bir teknolojidir. Bulut bilişim, gerek düşük maliyetli kullanım olanakları sağlaması, gerekse büyük hesaplama olanakları sunması açısından sıklıkla tercih edilmektedir. Bulut bilişimde gizlilik ve güvenliğin sağlanması için homomorfik kriptosistemlere ihtiyaç duyulur.

# 1. BÖLÜM

# KRİPTOLOJİDE KULLANILACAK TEMEL TANIM VE TEOREMLER

Bu bölümde kriptolojide kullanılacak bazı tanımlar ve şifreleme yapmakta bize fayda sağlayacak bazı teoremler verilmiştir. Bu bölümde yararlanılan kaynaklar [2], [19], [20], [21], [22], [23] dir.

## 1.1. Temel Tanım ve Teoremler

**Tanım 1.1.1.** Gizlilik, kimlik denetimi, bütünlük gibi bilgi güvenliğini sağlamak için kullanılan matematiksel yöntemler bütününe kriptografi (cryptography) denir.

**Tanım 1.1.2.** Şifrelenmiş metinleri çözümlemeyi ve yapılan saldırıları belirlemeye yarayan kriptoloji dalına kriptoanaliz (cryptanalysis) denir.

**Tanım 1.1.3.** Gizlilik sistemlerinin bağlı olduğu bilim dalına kriptoloji (cryptology) denir. ( Kriptoloji = Kriptografi + Kriptoanaliz )

**Tanım 1.1.4.** Bir bilgiyi şifrelemek ya da deşifrelemek için kullanılan algoritmanın parçasına anahtar (key) denir.

**Tanım 1.1.5.** Bilginin şifrelendiği algoritmada kullanılan ve herkes tarafından ulaşılabilir olan anahtara açık anahtar (public key) denir. Sadece özel anahtara sahip kişilerin göndermiş olduğu şifreli metinleri çözmek ve ya özel anahtara sahip kişi tarafından açılması istenen verileri şifrelemek için kullanılır.

**Tanım 1.1.6.** Açık anahtar kullanılarak şifrelenmiş bilgilerin deşifresi için kullanılan ve sadece kullanıcının kendisine ait olan anahtara gizli-özel anahtar (private key) denir.

**Tanım 1.1.7.** Düz metni şifreli metne dönüştürme, anlaşılmaz hale getirme işlemine şifreleme (encryption) denir.

**Tanım 1.1.8.** Şifrelenmiş metni çözüp düz metin haline getirme işlemine deşifreleme (decryption) denir.

**Tanım 1.1.9.** Bilginin şifrelenmemiş orijinal hallerine düz metin-açık metin (plaintext) denir.

**Tanım 1.1.10.** Bilginin şifrelenerek anlaşılmaz hale getirilmiş şekline şifreli metin (ciphertext) denir.

**Tanım 1.1.11.** Şifreleme ve deşifreleme işleminde kullanılan matematiksel işlemlerin tamamına kriptografik algoritma denir.

**Tanım 1.1.12.** Şifreleme ve deşifreleme işlemlerinde aynı anahtarın kullanıldığı algoritmalara simetrik algoritmalar denir. Gizli anahtarlı algoritmalar olarakta adlandırılır.

**Tanım 1.1.13.** Şifreleme ve deşifreleme işlemlerinde farklı anahtarın kullanıldığı algoritmalara asimetrik algoritmalar denir. Açık anahtarlı algoritmalar olarakta adlandırılır.

**Tanım 1.1.14.** Şifrelenmiş bir metnin ya da mesajın şifresini kırmak için yapılan hamlelere saldırı (attack) denir.

**Tanım 1.1.15.** Şifrelenmiş metin ya da mesajın şifresini kırmaya çalışan kişiye saldırgan (attacker) denir.

**Tanım 1.1.16.** Şifrelenmiş bir metnin gizli olan şifrelerini öğrenmek amacıyla yapılan bütün işlemlere şifre kırma (crack) denir.

**Tanım 1.1.17.** Bir mesajlaşmada bilgiyi deşifre etmek için alan kişiye alıcı, bilgiyi şifreleyip gönderen kişiye ise gönderici denir.

**Tanım 1.1.18.** $(G,+)$ 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

$$f(a+b) = f(a) * f(b)$$

oluyor ise $f$ ' ye bir grup homomorfizması denir.

**Örnek 1.1.1.** $G = (\mathbb{Z}, +)$ ve n $\in \mathbb{Z}$ olsun. $f : G \to G$ dönüşümü $\forall\, x \in \mathbb{Z}$ için $f(x) = nx$ şeklinde tanımlansın. $f$ bir grup homomorfizmasıdır, çünkü

$$f(x+y) = n(x+y) = nx + ny = f(x) + f(y).$$

**Örnek 1.1.2.** $G = (\mathbb{R}, +)$ ve $H = (\mathbb{R}^+, .)$ olsun. $f : G \to H$, $f(x) = e^x$ şeklinde tanımlansın. $\forall\, x, y \in \mathbb{R}$ için

$$f(x+y) = e^{x+y} = e^x . e^y = f(x).f(y)$$

olup $f$ bir grup homomorfizmasıdır.

**Tanım 1.1.19.** Şifreli bilgiler üzerinde işlemler yapmaya izin veren kriptosistemlere homomorfik kriptosistemler denir.

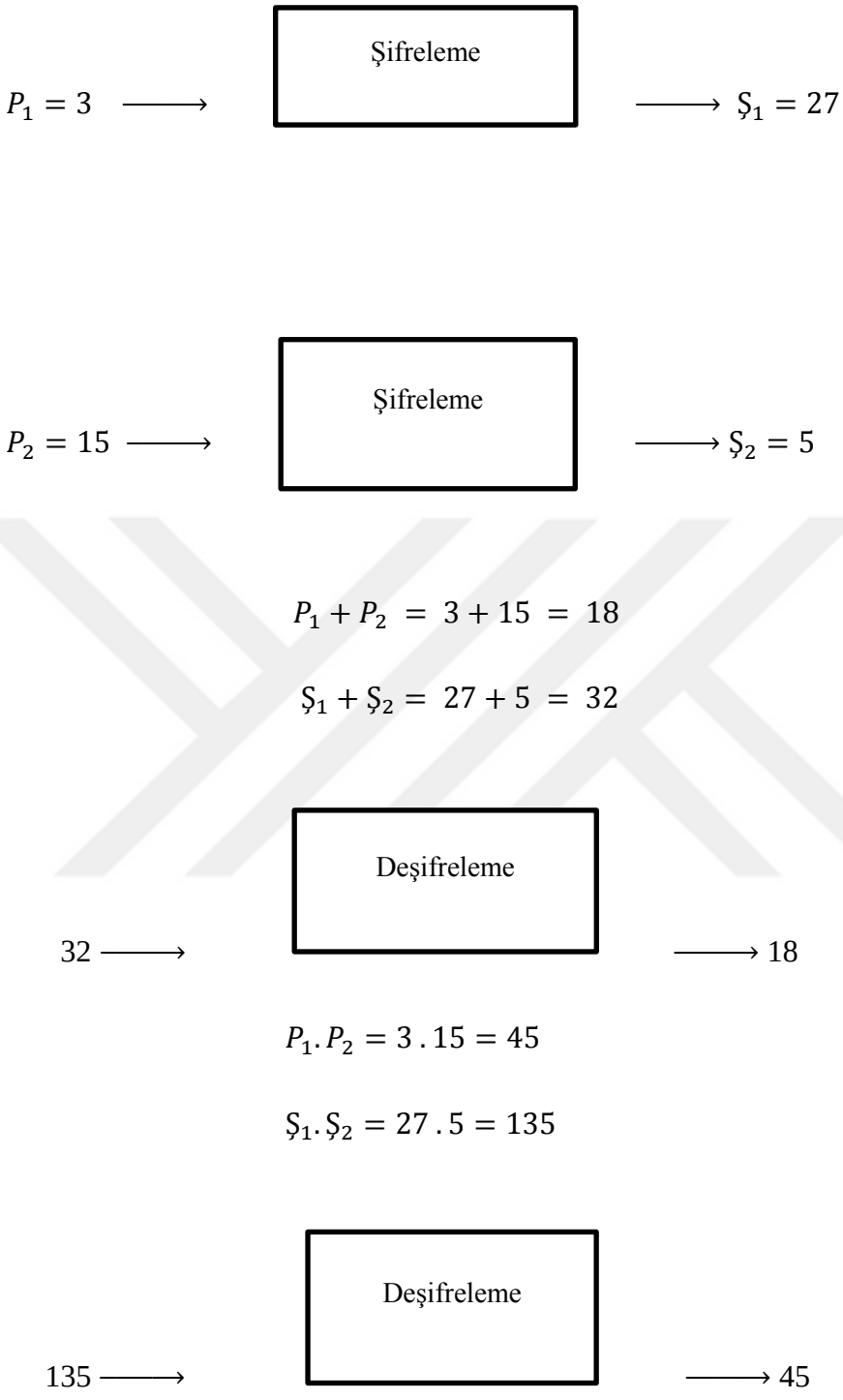
$P_1$ ve $P_2$ mesajlarının şifreleme fonksiyonu ile şifrelenmiş halleri $Ş_1$ ve $Ş_2$ olsun. $Ş_1 + Ş_2$ 'yi şifreleme fonksiyonunun tersi ile deşifrelediğimizde $P_1 + P_2$' yi veriyorsa veya $Ş_1 . Ş_2$ ' yi şifreleme fonksiyonunun tersiyle deşifrelediğimizde $P_1 . P_2$' yi veriyorsa bu şifrelemeye homomorfik şifreleme denir.

**Tanım 1.1.20.** Bir kriptosistem toplama işlemine göre homomorfik ise bu kriptosisteme toplamsal homomorfik denir.

**Tanım 1.1.21.** Bir kriptosistem çarpma işlemine göre homomorfik ise bu kriptosisteme çarpımsal homomorfik denir.

**Tanım 1.1.22.** Bir kriptosistem hem çarpımsal homomorfik hem de çarpımsal homomorfik ise bu kriptosisteme tam(fully) homomorfik kriptosistem (FHE) denir [24], [25], [26], [27].

Şimdide tam(fully) homomorfik şifrelemeyi şekil üzerinde gösterelim.




Şekil 1.1. Tam (Fully) Homomorfik Şifreleme

Şekilde görüldüğü gibi $P_1 = 3$ açık metninin şifrelenmiş hali $Ş_1 = 27$ ve $P_2 = 15$ açık metninin şifrelenmiş hali $Ş_2 = 5$ olsun. Bu durumda açık metinlerin toplamı $P_1 + P_2 = 18$, şifreli metinlerin toplamı $Ş_1 + Ş_2 = 32$ olur. 32 değerinin aynı sistemde deşifre edilmesi ile 18 değerini elde edebiliyorsak bu kriptosistem toplamsal homomorfiktir.

Benzer şekilde açık metinlerin çarpımı $P_1 . P_2 = 45$, şifreli metinlerin çarpımı $Ş_1 . Ş_2 = 135$ olur. 135 değerinin aynı sistemde deşifre edilmesi ile 45 değerini elde edebiliyorsak bu kriptosistem çarpımsal homomorfiktir. Bu özelliği her iki işlem de sağlıyorsa buna tam(fully) homomorfik kriptosistem denir.

**Teorem 1.1.1.** $n \geq 2$ olan her tam sayı ya asaldır ya da asalların çarpımı şeklinde çarpanların sıra değişikliği hariç tek türlü yazılır. **(Aritmetiğin Temel Teoremi )**

**Tanım 1.1.23.** $m > 0$ olan bir tam sayı ve $m|a - b$ ise $a$ tam sayısı $b$ tam sayısına $m$ modülüne göre kongrüenttir (denktir) denir ve $a \equiv b \pmod{m}$ şeklinde yazılır. Eğer $a$, $m$ modülüne göre $b$ ye kongrüent (denk) değil ise yani $m \nmid a - b$ ise $a \not\equiv b \pmod{m}$ şeklinde gösterilir.

**Tanım 1.1.24.** $n \geq 1$ olmak üzere $n'$ yi geçmeyen ve $n$ ile aralarında asal olan pozitif tam sayıların sayısını veren fonksiyona Eulerin $\phi$ fonksiyonu denir ve $\phi(n)$ ile gösterilir.

**Teorem 1.1.2. (Euler Teoremi)**

$(a, m) = 1$ olmak üzere $a^{\phi(m)} \equiv 1 (\mathrm{mod}\, m)$ dir.

**Örnek 1.1.3.** $a = 5, m = 7$ olsun.$(5, 7) = 1$ olduğundan $5^{\phi(7)} \equiv 1\ (7)$ olmalıdır.$\phi(7) = 6$ olduğundan $5^6 \equiv 1\ (7)$ tir.

**Teorem 1.1.3. (Fermat Teoremi)**

$p$ asal $p \nmid a$ olmak üzere $a^{p-1} \equiv 1 (\ \mathrm{mod}\ p)$ dir.

**Örnek 1.1.4**. $p = 3, a = 8$ olsun. $3 \nmid 8$ olduğundan $8^{3-1} \equiv 1\ (3)$ olmalıdır.$8^2 \equiv 1\ (3)$ olduğu basit bir hesapla görülmektedir.

**Tanım 1.1.25.** $p$ bir tek asal ve$(p, a) = 1$ olsun. Eğer $x^2 \equiv a(p)$ kongrüansı çözülebilir ise $a$ ya $p$ modülüne göre kuadratik rezidü (karesel kalan) denir ve R ile gösterilir. $x^2 \equiv a(p)$ kongrüansı çözülemez ise $a$ ya $p$ modülüne göre kuadratik olmayan rezidü denir ve N ile gösterilir.

**Örnek 1.1.5.** $p = 5$ modülüne göre kuadratik ve kuadratik olmayan rezidüleri bulalım**.**

$$1^2 \equiv 1\ (5),\quad 2^2 \equiv 4\ (5),\quad 3^2 \equiv 4\ (5),\quad 4^2 \equiv 1(5)$$

olduğundan 1 ve 4 sayıları 5 modülüne göre kuadratik rezidülerdir. 2 ve 3 sayıları 5 modülüne göre kuadratik olmayan rezidülerdir.

**Teorem 1.1.4.** $p$ bir tek asal olmak üzere $p$' nin R ve N lerinin sayısı birbirine eşit olup her biri $\frac{p-1}{2}$ tanedir.

**Tanım 1.1.26. (Legendre Sembolü).**

$p$ bir tek asal ve $a$ da $p$ ile bölünemeyen bir tam sayı olsun. $(\frac{a}{p})$ şeklinde gösterilen Legendre sembolü;

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & aRp \\ -1, & aNp \end{cases}$$

olarak tanımlanır.

**Örnek 1.1.6.** $p = 5$ ve $a = 1, 2, 3, 4$ için $(\frac{a}{5})$ Legendre Sembolü

$$\left(\frac{1}{5}\right) = \left(\frac{4}{5}\right) = 1$$

$$\left(\frac{2}{5}\right) = \left(\frac{3}{5}\right) = -1$$

**Teorem 1.1.5.** $p$ bir tek asal ve$a$ da $(p, a) = 1$ olan bir tam sayı ise

$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$ dir.

**Tanım 1.1.27.** $a$ ve $m$ aralarında asal tam sayılar olsun. $a^t \equiv 1\ (m)$ olacak şekilde en küçük $t$ tam sayısına $a$ nın $m$ modülüne ait üssü ya da $a$ nın $m$ modülüne göre mertebesi denir. $Ord_{m^a} = t$ şeklinde gösterilir.

**Örnek 1.1.7.** 2 nin 5 modülüne göre mertebesini bulalım.

$2 \equiv 2\ (5),\ 2^2 \equiv 4\ (5),\ 2^3 \equiv 3\ (5),\ 2^4 \equiv 1(5)$ olup 2 nin 5 modülüne göre mertebesi 4 tür. Yani $Ord_{5^2} = 4$ olur.

**Tanım 1.1.28.** $Ord_{m^a} = \phi(m)$ ise yani $a$, $m$ modülüne göre $\phi(m)$ üssüne ait ise $a$ ya $m$ nin ilkel kökü denir.

**Örnek 1.1.8.** $Ord_{5^2} = 4$ olduğunu örnek 1.1.7. de gördük. $\phi(5) = 4$ olduğunu göz önüne alırsak $Ord_{5^2} = 4 = \phi(5)$ olur ki bu da bize 2 nin 5 modülüne göre bir ilkel kök olduğunu gösterir.

**Teorem 1.1.6.** $m$, ilkel kökü olan bir tam sayı olsun. k pozitif bir tamsayı ve $(m, a) = 1$

olmak üzere $x^k \equiv a(\mathrm{mod}\, m)$ kongrüansının çözülebilir olması için gerek ve yeter şart $a^{\frac{\phi(m)}{d}} \equiv 1\ (m)$ olmasıdır. Üstelik $d$ tane birbirine kongrüent olmayan çözüm vardır. Burada $d = (k, \phi(m))$ dir.

**Örnek 1.1.9.** 5 in 13 modülüne göre 4. kuvvetten rezidü olup olmadığına bakalım.

$x^4 \equiv 5\ (13)$ kongrüansının çözülüp çözülemez olduğuna bakalım.

$5^{\frac{12}{(4,12)}} = 5^3 \equiv 8\ (13)$ olduğundan 5, 13 modülüne göre 4. kuvvetten rezidü değildir.

**Teorem 1.1.7.** $(m, a) = 1, m > 0, Ord_{m^a} = t$ olmak üzere $a^i \equiv a^j\ (\mathrm{mod}\, m)$ olması için gerek ve yeter şart $i \equiv j\ (\mathrm{mod}\ t)$ olmasıdır. Burada $i$ ve $j$ pozitif tam sayılardır.

**Teorem 1.1.7. (Çin Kalan Teoremi)**

$m_1, m_2, \ldots, m_r$ ikişer ikişer aralarında asal olan pozitif tam sayılar olsun. Bu durumda;

$$x \equiv a_1\ (m_1)$$
$$x \equiv a_2\ (m_2)$$

$$\vdots$$

$$x \equiv a_r\ (m_r)$$

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

Çin Kalan Teoremi (ÇKT) kriptografide yaygın olarak kullanılmaktadır [28], [29], [30].

**Tanım 1.1.29.** (R, +, .) ve (S, +, .) iki halka ve $\theta : R \to S$ bir fonksiyon olsun. Eğer $\theta$ aşağıdaki şartları sağlıyorsa; yani

1. $\forall\, a, b \in R$ için $\theta(a + b) = \theta(a) + \theta(b)$,
2. $\forall\, a, b \in R$ için $\theta(a.b) = \theta(a).\theta(b)$

ise $\theta$ bir halka homomorfizması denir.

**Tanım 1.1.30.** H bir çarpımsal grup olsun. $h \in$ H için, $< h >$ de $h$ tarafından üretilen devirli bir alt grup olsun. $h \in$ H ve $a \in < h >$ için $h^x = a$ olacak şekilde $x$ değerini bulma problemine ayrık logaritma problemi (discrete logarithm problem) denir.

**Tanım 1.1.31.** Elektronik ortamdaki yazışmalara eklenen, yazıyı gönderenin kimliğini ve gönderilen yazının iletimi sırasında bozulmadığını kanıtlamaya yarayan bölüme sayısal imza (dijital imza) denir.

**Tanım 1.1.32.** Halkın yaptığı seçimin demokratik koşullar göz önünde bulundurularak ve sağlanarak, oyların elektronik aygıtlarla toplanıp değerlendirilmesi işlemine elektronik oy (e-voting) denir.

**Tanım 1.1.33.** Sahip olduğunuz tüm uygulama, program ve verilerinizin sanal bir sunucuda yani bulutta depolanması ve internette bağlı olduğunuz herhangi bir ortamda cihazlarınız aracılığıyla bu bilgilere, verilere, programlara kolayca ulaşım sağlayabileceğiniz hizmetler bütününe bulut bilişim (cloud computing) denir.

# 2. BÖLÜM

# BAZI ŞİFRELEME METODLARI VE HOMOMORFİK ÖZELLİKLERİ

Bu bölümde bazı şifreleme metodları verilmiş ve bunların homomorfik özellikleri incelenmiştir. Bu bölümde istifade edilen kaynaklar [2], [9], [10], [11], [31], [32], [33] dür.

## 2.1. Ceasar Şifreleme Metodu

Eski Roma İmparatoru Julius Ceasar tarafından kullanılmış, modüler aritmetiğe dayanan şifreleme metodudur. Herhangi bir açık metine

$$C \equiv P + 3 \,(mod 29)$$

bağıntısı kullanılarak şifreleme işlemi yapılır.

$$P \equiv C - 3 \,(mod 29)$$

bağıntısı kullanılarak deşifreleme işlemi yapılır.

Örneğin $P_1 = 7$ açıkmetni şifrelenirse $C_1 = 10$ ve $P_2 = 2$ açıkmetni şifrelenirse $C_2 = 5$ şifremetinleri elde edilir. Şifre metinleri deşifrelendiğinde ise $P_1 = 7$ ve $P_2 = 2$ açıkmetinleri elde edilir.

Ceasar şifreleme metodu toplama işlemi ve çarpma işlemine göre homomorfik değildir. $P_1$ ve $P_2$ açıkmetinleri verilsin ve bunların şifrelenmiş halleri $C_1$ ve $C_2$ olsun.

$C_1 + C_2 = P_1 + P_2 + 6$ olur değeri deşifre edilirse $P_1 + P_2 + 3$ elde edilir. Buradan da Ceasar şifreleme metodunun toplamsal homomorfik olmadığı görülmektedir.

Benzer şekilde $C_1\, x\, C_2 = (P_1 + 3)\, x\, (P_2 + 3) = P_1\, x\, P_2 + 3(P_1 + P_2) + 9$ olup bu ifadenin deşifresi $P_1\, x\, P_2 + 3(P_1 + P_2) + 6$ olur. Bu da $P_1\, x\, P_2$ değerinden farklı olduğundan Ceasar şifreleme metodu çarpma işlemine göre homomorfik değildir.

Yukarıdaki örneği bu özelliklere uygularsak $C_1 + C_2 = 10 + 5 = 5$ bu ifade deşifre edilirse $15 - 3 = 12$ elde edilir. $P_1 + P_2 = 7 + 2 = 9$ değeri deşifre ettiğimiz değere eşit olmadığından Ceasar şifreleme metodu toplamsal homomorfik değildir. Benzer şekilde $C_1\, x\, C_2 = 10\, x\, 5 = 50$ değeri deşifre edilirse $50 - 3 = 47$ elde edilir. 47 değeri $(mod 29)$ da 18 değerine denktir. Fakat 18 değeri $P_1\, x\, P_2 = 7\, x\, 2 = 14$ değerinden farklı olduğundan Ceasar şifreleme metodu çarpımsal homomorfik değildir.

### 2.2.RSA Şifreleme Metodu

RSA şifreleme metodu en pratik açık anahtarlı tasarım olarak kabul edilir. Algoritma 1978 ‘ de Ron Rivest, Adi Shamir ve Leonard Adleman tarafından bulunmuştur. Şifreleme yönteminin adı bu üç kişinin soy isimlerinin baş harflerinden oluşur. RSA şifreleme metodunun güvenliği büyük sayıların çarpanlarının hesaplanmasının zorluğuna dayanır. Anahtar oluşturma işlemi için asal sayılar kullanılarak daha güvenli bir yapı oluşturulmuştur. RSA hem mesaj şifreleme hem de elektronik imza amacıyla kullanılmaktadır.

**RSA Şifreleme Algoritması:**

**Anahtar Oluşturma : (A Şahsı )**

1) Birbirinden farklı $a$ ve $b$ asal sayıları seçilir.
2) $g = a\, x\, b$ ve $\emptyset(g) = (a-1)x(b-1)$ değerleri hesaplanır.
3) $(y, \emptyset(g)) = 1$ olacak şekilde, $1 < y < \emptyset(g)$ tamsayısı seçilir.
4) Genişletilmiş Euclidiean Algoritması kullanılarak $yh \equiv 1\, mod(\emptyset(g))$ olacak şekilde $1 < h < \emptyset(g)$ tamsayısı bulunur.

5) A şahsının açık anahtarı $\{y\ ,g\}$ ve özel anahtarı $\{h\ ,g\}$ elde edilir.

**Şifreleme : ( B Şahsı)**

1) A ‘ nın açık anahtarı $\{y\ ,g\}$ yi elde edilir.

2) P şifrelemede istenen mesajdaki harfler $[0\ ,g-1]$ aralığında sayısal denkliklere dönüştürülür.

3) $Ş \equiv P^{y}\ (mod\ g)$ hesaplanır.

4) Ş şifre metni A ‘ ya gönderir.

**Deşifre : ( A Şahsı)**

Özel anahtar $\{g\ ,h\}$ yi kullanarak $P \equiv Ş^{h}\ (mod\ g)$ ‘yi hesaplar ve P açık metnine ulaşır.

RSA Kriptosistemi çarpımsal homomorfik kriptosistemdir. Fakat toplamsal homomorfik kriptosistem değildir. $P_1\ ve\ P_2$ açıkmetinler ve bunlara karşılık gelen şifreli metinler $Ş_1\ ve\ Ş_2$ olsun. $Ş_1\ x\ Ş_2 = {P_1}^{y}\ x\ {P_2}^{y} = (P_1 x\ P_2)^{\ y}$ elde edilir. $(P_1 x P_2)^{y}$ değeri deşifre edilirse $(P_1 x P_2)^{yxh} \equiv P_1 x P_2\ (mod\ g)$ elde edilir. Bu da bize RSA Kriptosisteminin çarpma işlemine göre homomorfik olduğunu gösterir.

**Örnek 2.2.1.** RSA şifreleme sistemi ile B şahsı A şahsına KAÇ mesajını göndersin.

**Anahtar Oluşturma : (A Şahsı)**

1) $a = 47\ ve\ b = 61$ asal sayılarını seçsin.

2) $g = axb = 47x61 = 2867$ ve $\emptyset(g) = (a-1)(b-1) = 46x60 = 2760$ değerini hesaplar.

3) $(y\ ,\emptyset(g)) = 1$ olacak şekilde $1 < y < \emptyset(g)$ aralığında $y = 7$ değerini seçsin.

4) $yh \equiv 1\ (mod\ \emptyset(g))$ ve $1 < h < \emptyset(g)$ olacak şekilde $h = 1183$ değerini hesaplar.

5) A şahsının açık anahtarı $\{7, 2867\ \}$ ve özel anahtarı $\{1183, 2867\}$ olur.

**Şifreleme : ( B Şahsı )**

1) A ‘ nın açık anahtarı $\{7,\ 2867\}$ yi elde eder.

2) Şifrelemek istediği KAÇ mesajını sayısal denkliklere dönüştürür. $KAÇ = 1303$ elde edilir. $P_1 = 13\ ve\ \ P_2 = 3$ ‘ü ayrı ayrı şifreler.

3) $Ş_1 \equiv {P_1}^y (mod\ g)$ ‘ den $Ş_1 \equiv 13^7 \equiv 1355\ mod\ (2867)$ ve $Ş_2 \equiv {P_2}^y (modg)$ ‘ den $Ş_2 \equiv 3^7 \equiv 2187\ mod(2867)$ olarak hesaplar.

4) $Ş_1 = 1355\ ve\ Ş_2 = 2187$ şifre metinlerini A ‘ ya gönderir.

**Deşifre : (A Şahsı)**

$P_1 \equiv {Ş_1}^h\ (mod\ g)$ ‘ den $P_1 \equiv 1355^{1183} \equiv 13\ (mod 2867)$ ve $P_2 \equiv {Ş_2}^h\ (modg)$ ‘ den $P_2 \equiv 2187^{1183} \equiv 3\ (mod 2867)$ açık metinlerine ulaşır.

Yukarıdaki örneği kullanarak RSA Kriptosisteminin çarpımsal homomorfik olduğunu gösterelim.

$$Ş_1\ x\ Ş_2 = 1355x2187$$

$$\equiv 2963385\ (mod\ 2867)$$

$$\equiv 1774\ (mod\ 2867)$$

olup deşifre edilirse

$$1774^{1183} \equiv 39\ mod\ (2867\ )$$

elde edilir.$P_1 x P_2 = 13x3 = 39$ olduğundan RSA Kriptosistemi çarpımsal homomorfiktir.

**Örnek 2.2.2.** RSA şifreleme sistemi ile B şahsı A şahsına GEL mesajını göndersin.

**Anahtar Oluşturma : (A Şahsı)**

1) $a = 13\ ve\ b = 29$ asal sayılarını seçsin.

2) $g = axb = 13x29 = 377$ ve $\emptyset(g) = (a-1)(b-1) = 12x28 = 336$ değerini hesaplar.

3) $(y, \emptyset(g)) = 1$ olacak şekilde $1 < y < \emptyset(g)$ aralığında $y = 11$ değerini seçsin.

4) $yh \equiv 1\ (mod\ \emptyset(g))$ ve $1 < h < \emptyset(g)$ olacak şekilde $h = 275$ değerini hesaplar.

5) A şahsının açık anahtarı $\{11, 377\}$ ve özel anahtarı {275, 377} olur.

**Şifreleme : ( B Şahsı )**

1) A ' nın açık anahtarı $\{11,\ 377\}$ yi elde eder.

2) Şifrelemek istediği GEL mesajını sayısal denkliklere dönüştürür. $GEL = 7514$ elde edilir. $P_1 = 75\ ve\ P_2 = 14$ 'ü ayrı ayrı şifreler.

3) $Ş_1 \equiv {P_1}^y (mod\ g)$ ' den $Ş_1 \equiv 75^{11} \equiv 186\ mod\ (377)$ ve $Ş_2 \equiv {P_2}^y (modg)$ ' den $Ş_2 \equiv 14^{11} \equiv 66\ mod(377)$ olarak hesaplar.

4) $Ş_1 = 186\ ve\ Ş_2 = 66$ şifre metinlerini A ' ya gönderir.

**Deşifre : (A Şahsı)**

${P_1} \equiv {Ş_1}^h\ (mod\ g)$ ' den ${P_1} \equiv 186^{275} \equiv 75\ (mod 377)$ ve ${P_2} \equiv {Ş_2}^h\ (modg)$ ' den ${P_2} \equiv 66^{275} \equiv 14\ (mod 377)$ açıkmetinlerine ulaşır.

Yukarıdaki örneği kullanarak RSA Kriptosisteminin çarpımsal homomorfik olduğunu gösterelim.

$$Ş_1\ x\ Ş_2 = 186x66$$

$$\equiv 12276\ (mod\ 377)$$

$$\equiv 212(mod\ 377)$$

olup deşifre edilirse

$$212^{275} \equiv 296\ (mod\ 377\ )$$

$$296 \equiv 1050(mod\ 377)$$

elde edilir. $P_1 x P_2 = 75 \times 14 = 1050$ olduğundan RSA Kriptosistemi çarpımsal homomorfiktir.

### 2.3.El-Gamal Şifreleme Metodu

1985 yılında Mısırlı bir matematikçi olan Taher El-Gamal tarafından bulunan açık anahtarlı şifreleme metodunun güvenliği ayrık logaritma probleminin (DLP) zorluğuna dayanmaktadır.

**El-Gamal Şifreleme Algoritması:**

**Anahtar Oluşumu: (A Şahsı)**

1) Rastgele bir $q$ asalı seçilir.
2) $mod\ (q)$ ' ya göre tamsayıların oluşturduğu çarpım grubu $\mathbb{Z}_q^*$ ve bu grubun bir üreteci $\alpha$ seçilir.
3) $1 \leq n \leq q-2$ olacak şekilde bir $n$ tamsayısı seçilir.
4) $\alpha^n \equiv b\ (mod\ q)$ değeri hesaplanır.
5) Açık anahtar $(q, \alpha, b)$ , gizli anahtar $n$ ' dir.

**Şifreleme : (B Şahsı)**

1) A 'nın açık anahtarı $(q, \alpha\ , b)$ 'yi elde eder.
2) $1 \leq k \leq q-2$ aralığında bir $k$ tamsayısı seçer
3) $\gamma \equiv \alpha^k\ (mod\ q)$ değerini hesaplar.
4) $\delta \equiv P.\, b^k (mod\ q)$ değerini hesaplar.
5) $Ş = (\gamma\ , \delta)$ karşı tarafa gönderir.

**Deşifreleme : ( A Şahsı)**

1) $n$ gizli anahtar yardımıyla $\gamma^{-n}\ (mod\ q)$ değerini hesaplar.

2) $\gamma^{-n}.\delta \equiv P\ (mod\ q)$ ‘ dan $P$ ‘yi bulur.

El-Gamal Kriptosistemi çarpımsal homomorfiktir. $Ş_1 = (\gamma_1, \delta_1)$ ve $Ş_2 = (\gamma_2, \delta_2)$ olsun.

$$Ş_1 \times Ş_2 = (\gamma_1, \delta_1).(\gamma_2, \delta_2) = (\gamma_1.\gamma_2\ , \delta_1.\delta_2)$$

$$= (\alpha^k.\alpha^k\ , P_1.\alpha^{nk}.P_2.\alpha^{nk}) = (\alpha^{2k}\ , P_1.P_2.\alpha^{2nk})$$

olup deşifresi ise $P_1 \times P_2$ ‘ ye eşittir. Bu da bize El-Gamal Kriptosisteminin çarpma işlemine göre homomorfik kriptosistem olduğunu gösterir.

**Örnek.2.3.1.** KAÇ mesajını El-Gamal şifreleme yöntemiyle şifreleyelim.

**Anahtar oluşturma : (A Şahsı)**

1) $q = 3301$ asal sayısını seçsin.

2) $mod(3301)$ ‘ e göre tamsayıların oluşturduğu $\mathbb{Z}_{3301}{}^*$ çarpım grubundan $\alpha = 3$ üreteci seçilsin.

3) $1 \leq n \leq q - 2$ olacak şekilde $n = 1505$ tamsayısı seçilir.

4) $\alpha^n \equiv b\ (mod\ q)$ değeri $3^{1505} \equiv 2860\ (mod 3301)$ olarak heasaplar.

5) Açık anahtar $(3301\ ,3\ ,2860)$ , gizli anahtar 1505 ‘ tir.

**Şifreleme : (B Şahsı)**

1) A nın açık anahtarı $(3301\ ,3\ ,2860)$ ‘ ı elde eder.

2) B şahsı KAÇ mesajını sayısal değerlerine çevirir. KAÇ $= 1303$ olarak bulur. $P_1 = 13\ ve\ P_2 = 3$ alarak ayrı ayrı şifreleme yapar.

3) $1 \leq k \leq q - 2$ aralığında $k = 495$ tamsayısını seçer.

4) $\gamma_1 \equiv \alpha^k\ (mod\ q)$ değerini $\gamma_1 \equiv 3^{495} \equiv 2847\ (mod 3301)$ olarak hesaplar.

5) $\delta_1 \equiv P_1.b^k(mod\ q)$ değerini $\delta_1 \equiv 13.2860^{495} \equiv 3288(mod3301)$ olarak hesaplar.

6) $Ş_1 = (2847\ , 3288)$ elde edilir.

   Aynı şekilde bu şifreleme işlemleri $P_2$ içinde yapılırsa $Ş_2 = (2847, 3298)$ elde edilir.

7) $Ş_1\ ve\ Ş_2$ şifreli mesajları A şahsına gönderir

**Deşifreleme : ( A Şahsı )**

**1)** $n = 1505$ gizli anahtarı ile ${\gamma_1}^{-n}$ $(modq)$ değerini $2847^{-1505} \equiv 3300(mod3301)$ olarak hesaplar.

**2)** ${\gamma_1}^{-n}.\delta_1 \equiv P_1\ (mod\ q)$ ' dan $3300.3288 \equiv 13\ mod(3301)$ $P_1 = 13$ ve ${\gamma_2}^{-n}.\delta_2 \equiv P_2\ (mod\ q)$ ' dan $3300.3298 \equiv 3\ (mod3301)$ $P_2 = 3$ açıkmetinlerini elde eder.

Yukarıdaki örneği kullanarak El-Gamal Şifreleme Metodunun çarpımsal homomorfik olduğunu göstereli.

$$Ş_1.Ş_2 = (2847\ , 3288).(2847\ , 3298)$$

$$= (2847.2847\ , 3288.3298)(mod3301)$$

$$= (1454\ , 39)$$

$$= Ş_3$$

elde edilir ve deşifresi ;

$$1454^{-1505}.39 \equiv 39\ (mod3301)$$

olur. $P_1\ ve\ P_2$ açık metinlerin çarpımı $13\ x\ 3\ =\ 39$ olup iki şifreli metnin çarpımının deşifresi açık metinlerin çarpımını verdiğinden El-Gamal şifreleme metodu çarpma işlemine göre homomorfik kriptosistemdir.

**Örnek.2.3.2.** GEL mesajını El-Gamal şifreleme yöntemiyle şifreleyelim.

**Anahtar oluşturma : ( A Şahsı)**

1) $q = 4001$ asal sayısını seçsin.
2) $mod(4001)$ ' e göre tamsayıların oluşturduğu $\mathbb{Z}_{4001}{}^{*}$ çarpım grubundan $\alpha = 5$ üreteci seçilsin.
3) $1 \leq n \leq q - 2$ olacak şekilde $n = 881$ tamsayısı seçilir.
4) $\alpha^n \equiv b \ (mod\ q)$ değeri $5^{881} \equiv 509 \ (mod\ 4001)$ olarak heasaplar.
5) Açık anahtar $(4001\ ,5\ ,509)$ , gizli anahtar 881 ' dir.

**Şifreleme : ( B Şahsı )**

1) A nın açık anahtarı $(4001, 5, 509)$ ' u elde eder.
2) B şahsı GEL mesajını sayısal değerlerine çevirir. $\text{GEL} = 7514$ olarak bulur. $P_1 = 75\ ve\ P_2 = 14$ alarak ayrı ayrı şifreleme yapar.
3) $1 \leq k \leq q - 2$ aralığında $k = 302$ tamsayısını seçer.
4) $\gamma_1 \equiv \alpha^k \ (mod\ q)$ değerini $\gamma_1 \equiv 5^{302} \equiv 3976 \ (mod 4001)$ olarak hesaplar.
5) $\delta_1 \equiv P_1 . b^k (mod\ q)$ değerini $\delta_1 \equiv 75.509^{302} \equiv 1782 (mod 4001)$ olarak hesaplar.
6) $Ş_1 = (3976, 1782)$ elde edilir.

   Aynı şekilde bu şifreleme işlemleri $P_2$ içinde yapılırsa $Ş_2 = (3976, 1773)$ elde edilir.
7) $Ş_1\ ve\ Ş_2$ şifreli mesajları A şahsına gönderir

**Deşifreleme : ( B Şahsı )**

**3)** $n = 881$ gizli anahtarı ile ${\gamma_1}^{-n}$ $(modq)$ değerini $3976^{-881} \equiv 1785(mod4001)$ olarak hesaplar.

**4)** ${\gamma_1}^{-n}.\delta_1 \equiv P_1\ (mod\ q)$ ' dan $1785.1782 \equiv 75\ mod(4001)$ $P_1 = 75$ ve ${\gamma_2}^{-n}.\delta_2 \equiv P_2\ (mod\ q)$ ' dan $1785.1773 \equiv 14\ (mod4001)$ $P_2 = 14$ açık metinlerini elde eder.

Yukarıdaki örneği kullanarak El-Gamal Şifreleme Metodunun çarpımsal homomorfik olduğunu göstereli.

$$Ş_1.Ş_2 = (3976,\ 1782).(3976,\ 1773)$$

$$= (3976.3976\ , 1782.1773)(mod4001)$$

$$= (625, 2697)$$

$$= Ş_3$$

elde edilir ve deşifresi ;

$$625^{-881}.2697 \equiv 1050\ (mod4001)$$

olur. $P_1\ ve\ P_2$ açık metinlerin çarpımı $75\ x\ 14 = 1050$ olup iki şifreli metnin çarpımının deşifresi açık metinlerin çarpımını verdiğinden El-Gamal şifreleme metodu çarpma işlemine göre homomorfik kriptosistemdir.

Bu şifreleme metodlarının yanı sıra Pailler Şifreleme Metodu ve Goldwasser-Micali Şifreleme Metodu da mevcuttur. Güvenliği n. rezidü sınıflarını hesaplamanın zorluğuna dayanan Pailler şifreleme metodunda, şifreli metinlerin çarpımının deşifresi açık metinlerin toplamını vermektedir. Güvenliği verilen bir x sayısının N modunda kuadratik rezidü olup olmadığını belirlemenin zorluğuna dayanan Goldwasser-Micali şifreleme metodunda şifreli metinlerin çarpımının deşifresi açıkmetinlerin mod 2 de toplamını vermektedir.

# 3. BÖLÜM

# TAM (FULLY) HOMOMORFİK KRİPTOSİSTEMLER

Bu bölümde tam(fully) homomorfik şifreleme şeması ve bu şemanın homomorfik özellikleri incelenmiştir. Bu bölümde yararlanılan kaynaklar [9], [13], [16], [17], [18] dir.

## 3.1. Tam(Fully) Homomorfik Kriptosistem

Marten Van Dijk, Craig Gentry, Shai Halevi ve Vinod Vaikuntanathan tam (fully) homomorfik şifreleme algoritmasını sundular. 2011 yılında Vinod Vaikuntanathan, bir çalışmasında tam (fully) homomorfik şifreleme hakkında ana hatlarıyla bilgiler vermiştir. 2012 ve 2013 yıllarında yapılan çalışmalardaki kriptosistemlerde matrisler kullanılmakta ve sistemin güvenliği çarpanlara ayırmanın zorluğuna dayanmaktadır. Bu kriptosistem, çarpanlara ayırmanın zorluğuna dayanan ilk tam (fully) homomorfik kriptosistemdir.

**Anahtar Oluşturma: (A şahsı)**

1) $2m$ tane aralarında asal ve $1 \leq i \leq m$ olacak şekilde $p_i$ ve $q_i$ tek tam sayıları seçilir.

2) $f_i = p_i . q_i$ ve $N = \prod_{i=1}^{m} f_i$ değerleri hesaplanır.

3) $4x4$ tipinde tersinir bir $k \in m_4(\mathbb{Z}_N)$ matrisi seçilir.

4) $k$ matrisinin tersi $k^{-1}$ mod $N$ ye göre hesaplanır.

5) Anahtar $(f_i, N, k, k^{-1})$ dir.

**Şifreleme: (B şahsı)**

1) B şahsı A şahsının oluşturduğu anahtarı elde eder.

2) Rastgele bir $r \in \mathbb{Z}_N, r \neq x$ tam sayısı seçilir.

3) $X_{mx3}$ tipinde, her satırda x e eşit tek bir eleman içeren ve diğer iki elemanı $r$ olan bir matris elde edilir.

4) Çin Kalan Teoremini kullanarak $1 \leq j \leq 3$ için $x_j \equiv X_{ij} \bmod f_i,\ 1 \leq i \leq m$ kongrüansları çözülür.

5) Şifreli metin $Ş = k^{-1}.diag(x, x_1, x_2, x_3).k$ olarak bulunur.

**Deşifreleme: (A Şahsı)**

1) $x = (k.Ş.k^{-1})_{11}$ işlemi ile düz metin elde edilir.

**Örnek 3.1.1.** 571 mesajını tam(fully) homomorfik şifreleme yöntemini kullanarak şifreleyelim.

**Anahtar oluşturma: (A Şahsı)**

1) $m = 2$ olsun ve $p = (3, 7)$, $q = (11, 5)$ olsun.

2) $f_1 = 3x11 = 33$ ve $f_2 = 7x5 = 35$ olur ve $N = f_1 x f_2 = 33x35 = 1155$ elde edilir.

3) $4x4$ tipinde tersinir matris

$$k = \begin{pmatrix} 333 & 1009 & 1093 & 394 \\ 566 & 870 & 285 & 192 \\ 305 & 642 & 456 & 407 \\ 326 & 1103 & 363 & 837 \end{pmatrix} \pmod{1155}$$

olarak seçilsin.

4) $k$ matrisinin tersi

$$k^{-1} = \begin{pmatrix} 33 & 929 & 342 & 393 \\ 963 & 100 & 1113 & 161 \\ 202 & 88 & 1042 & 976 \\ 906 & 1051 & 944 & 441 \end{pmatrix} \text{mod}(1155)$$

olarak hesaplanır.

5) $(33,35,1155, \begin{pmatrix} 333 & 1009 & 1093 & 394 \\ 566 & 870 & 285 & 192 \\ 305 & 642 & 456 & 407 \\ 326 & 1103 & 363 & 837 \end{pmatrix}, \begin{pmatrix} 33 & 929 & 342 & 393 \\ 963 & 100 & 1113 & 161 \\ 202 & 88 & 1042 & 976 \\ 906 & 1051 & 944 & 441 \end{pmatrix})$

anahtarı B şahsına gönderir.

**Şifreleme : (B Şahsı)**

1) $r \neq x$ ve $r \in Z_{1155}$ olacak şekilde $x = 571$ ve $r = 155$ seçelim.

2) $m = 2$ olduğundan $mx3 = 2x3$ tipindeki matris

$$X = \begin{pmatrix} 155 & 571 & 155 \\ 155 & 155 & 571 \end{pmatrix}$$

şeklinde elde edilir.

3) Bu matris bize aşağıdaki kongrüansları vermektedir.

a) $x_1 \equiv 155 \pmod{33}$

$x_1 \equiv 155 \pmod{35}$

b) $x_2 \equiv 571 \pmod{33}$

$x_2 \equiv 155 \pmod{35}$

c) $x_3 \equiv 155 \pmod{33}$

$x_3 \equiv 571 \pmod{35}$

4) Bu kongrüanslar Çin Kalan Teoremi yardımıyla çözülürse;

$$x_1 \equiv 155\ (mod 1155)$$

$$x_2 \equiv 505\ (mod 1155)$$

$$x_3 \equiv 221\ (mod 1155)$$

çözümleri elde edilir.

5) $Ş = k^{-1}.diag(x, x_1, x_2, x_3).k$ olacak şekilde

$$\begin{pmatrix} 33 & 929 & 342 & 393 \\ 963 & 100 & 1113 & 161 \\ 202 & 88 & 1042 & 976 \\ 906 & 1051 & 944 & 441 \end{pmatrix}.\begin{pmatrix} 571 & 0 & 0 & 0 \\ 0 & 155 & 0 & 0 \\ 0 & 0 & 505 & 0 \\ 0 & 0 & 0 & 221 \end{pmatrix}.\begin{pmatrix} 333 & 1009 & 1093 & 394 \\ 566 & 870 & 285 & 192 \\ 305 & 642 & 456 & 407 \\ 326 & 1103 & 363 & 837 \end{pmatrix}$$

$$\equiv \begin{pmatrix} 227 & 531 & 243 & 693 \\ 405 & 230 & 537 & 24 \\ 1102 & 26 & 934 & 555 \\ 239 & 282 & 681 & 61 \end{pmatrix} (\text{mod}1155)$$ olarak bulunur.

B şahsı Ş mesajını A şahsına gönderir.

**Deşifreleme : (A Şahsı)**

$x = (k.Ş.k^{-1})_{11}$ işlemi yapılırsa

$$\begin{pmatrix} 333 & 1009 & 1093 & 394 \\ 566 & 870 & 285 & 192 \\ 305 & 642 & 456 & 407 \\ 326 & 1103 & 363 & 837 \end{pmatrix}.$$

$$\begin{pmatrix} 227 & 531 & 243 & 693 \\ 405 & 230 & 537 & 24 \\ 1102 & 26 & 934 & 555 \\ 239 & 282 & 681 & 61 \end{pmatrix}.\begin{pmatrix} 33 & 929 & 342 & 393 \\ 963 & 100 & 1113 & 161 \\ 202 & 88 & 1042 & 976 \\ 906 & 1051 & 944 & 441 \end{pmatrix}$$

$$\equiv \begin{pmatrix} 571 & 0 & 0 & 0 \\ 0 & 155 & 0 & 0 \\ 0 & 0 & 505 & 0 \\ 0 & 0 & 0 & 221 \end{pmatrix} \text{mod}1155$$

$x = 571$ açık metin elde edilir.

### 3.1.1. Verilen Şemanın Homomorfik Özelliğinin İncelenmesi

**Teorem 3.1.1.** Tam(fully) kriptosistemde deşifreleme doğru biçimde açıkmetni vermektedir.

**İspat:** $Ş(x,k)$ $x$ açık metninin $k$ anahtarı kullanılarak şifrelenmiş halini ve $P(x,k)$ de deşifrelenmiş haşini belirtsin. Herhangi bir $A$ matrisi için $A \text{ x } I = I \text{ x } A = A$ ve $k \text{ x } k^{-1} = k^{-1} \text{ x } k = I$ olduğundan verilmiş olan bir $Ş(x,k)$ şifre metni ile $k$ anahtarı için deşifreleme

$$\begin{aligned} P(x,k) &= (k \text{ x } Ş \text{ x } k^{-1})_{11} \\ &= (k \text{ x } k^{-1} \text{ x } diag(x, x_1, x_2, x_3) \text{ x } k \text{ x } k^{-1})_{11} \\ &= (diag(x, x_1, x_2, x_3))_{11} \\ &= x \end{aligned}$$

**Teorem 3.1.2.** Verilen şema tam(fully) homomorfik bir şemadır.

**İspat :** $Ş(x,k)$ ve $Ş(y,k)$ sırasıyla $x$ ve $y$ açık metinlerinin $k$ anahtarı kullanılarak şifrelenmiş halleri ve $P(x,k)$ de deşifrelenmiş hallerini belirtsin.

$$\begin{aligned} Ş(x,k) + Ş(y,k) &= k^{-1} \times diag(x, x_1, x_2, x_3) \times k + k^{-1} \times diag(y, y_1, y_2, y_3) \times k \\ &= k^{-1} \times (diag(x, x_1, x_2, x_3) + diag(y, y_1, y_2, y_3)) \times \text{k} \\ &= k^{-1} \times (\text{diag}(\text{x} + \text{y}, x_1 + y_1, x_2 + y_2, x_3 + y_3)) \times \text{k} \\ &= P(x + y, k) \end{aligned}$$

olup şemanın toplamsal homomorfik olduğu görülür.

$$\begin{aligned} Ş(x,k) \times Ş(y,k) &= k^{-1} \times diag(x, x_1, x_2, x_3) \times k \times k^{-1} \times diag(y, y_1, y_2, y_3) \times k \\ &= k^{-1} \times (diag(x, x_1, x_2, x_3) \times diag(y, y_1, y_2, y_3)) \times \text{k} \\ &= k^{-1} \times (\text{diag}(\text{x} \times \text{y}, x_1 \times y_1, x_2 \times y_2, x_3 \times y_3)) \times \text{k} \end{aligned}$$

$$= P(x \times y, k)$$

olup şemanın çarpımsal homomorfik olduğu görülür.şema hem toplamsal homomorfik hem de çarpımsal homomorfik olduğundan tam(fully) homomorfiktir.

**Örnek 3.1.2.** Yukarıda tanımlanan şifreleme algoritmasının toplamaya ve çarpmaya göre homomorfik olduğunu gösterelim.

1) $m$=2, $p$={3,5}, $q$={7,11} seçelim.

2) Bu takdirde $f_1$=21 ve $f_2$=55 olur. $N$=1155 olur.

3) $k$ matrisimizi

$$k \equiv \begin{pmatrix} 366 & 826 & 315 & 660 \\ 224 & 398 & 457 & 165 \\ 1063 & 849 & 492 & 597 \\ 401 & 1083 & 114 & 496 \end{pmatrix} (\text{mod}1155)$$

seçelim.

4) k matrisimizin tersi

$$k^{-1} \equiv \begin{pmatrix} 1083 & 213 & 1 & 1053 \\ 1093 & 792 & 84 & 342 \\ 307 & 784 & 877 & 471 \\ 300 & 375 & 874 & 613 \end{pmatrix} (\text{mod}1155) \text{ olur.}$$

5 ve 12 mesajlarını yukarıdaki örnekteki gibi şifrelersek

$$Ş_5 \equiv \begin{pmatrix} 286 & 618 & 534 & 180 \\ 954 & 662 & 651 & 765 \\ 122 & 1131 & 428 & 450 \\ 825 & 285 & 1020 & 196 \end{pmatrix} (\text{mod}1155)$$

$$Ş_{12} \equiv \begin{pmatrix} 877 & 813 & 768 & 1122 \\ 60 & 1149 & 1152 & 33 \\ 507 & 245 & 304 & 759 \\ 472 & 531 & 828 & 150 \end{pmatrix} (\text{mod} 1155)$$

olur. Bu iki şifrelenmiş metnin toplamı olan

$$Ş_{5+12} \equiv \begin{pmatrix} 8 & 276 & 147 & 147 \\ 1014 & 656 & 648 & 798 \\ 629 & 229 & 732 & 54 \\ 142 & 816 & 693 & 346 \end{pmatrix} (\text{mod} 1155)$$

ifadesini deşifre edersek;

$$X=(k.Ş_{5+12}.k^{-1}) \equiv \begin{pmatrix} 17 & 0 & 0 & 0 \\ 0 & 408 & 0 & 0 \\ 0 & 0 & 1079 & 0 \\ 0 & 0 & 0 & 238 \end{pmatrix} (\text{mod} 1155)$$

ifadesinin birinci satır birinci sütunundaki ifade 17'dir. Orijinal metinlerimiz 5 ve 12 nin toplamı da 17 olduğu için şifrelememiz toplamaya göre homomorfiktir.

Bu iki şifrelenmiş metnin çarpımı olan

$$Ş_{5.12} \equiv \begin{pmatrix} 265 & 150 & 180 & 897 \\ 180 & 1005 & 450 & 933 \\ 185 & 775 & 500 & 609 \\ 82 & 816 & 933 & 360 \end{pmatrix} (\text{mod} 1155)$$

ifadesinin deşifrelenmiş hali;

$$X=(k.Ş_{5.12}.k^{-1}) \equiv \begin{pmatrix} 60 & 0 & 0 & 0 \\ 0 & 440 & 0 & 0 \\ 0 & 0 & 673 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} (\text{mod} 1155)$$

olup matrisinin birinci satır birinci sütunundaki değer 60'tır. Orijinal değerlerimiz olan 5 ve 12 nin çarpımı da 60 olduğu için şifrelememiş çarpımsal homomorfiktir.

Hem toplamaya göre hem de çarpmaya göre homomorfik olduğu için şifrelememiz tam(fully) homomorfik şifrelemedir.

# KAYNAKLAR


1. Lunde, P., 2010. ¸Sifreler Kitabı, NTV yayınları.

2. Altındiş, H., 2011. Sayılar Teorisi ve Uygulamaları, (3. Basım), Lazer Ofset,Ankara.

3. Babaoğlu, A., 2009. Kriptolojinin Geçmişi: Bir Şifreleme Algoritması Kullanmadan Önce Son Kullanım Tarihine Bakın!, **Bilim ve Teknik 500**.

4. Çeşmeci, M., 2009. Elektronik Çağ Öncesi Dönem Kriptololoji Tarihi, **Tübitak Uekae Dergisi**, **1**:20 – 32.

5. Çimen, C., Akleylek, S., ve Akyıldız, E., 2007. Şifrelerin Matematiği: Kriptografi, ODTÜ Bilim ve Toplum Kitapları Dizisi, Ankara, 131s.

6. Kaşkaloğlu, K., 2003. Geçmişten Günümüze Kriptoloji: Şifrelerin Bilimi, Technical report, Atılım Üniversitesi.

7. Kara, O., 2009. II. Dünya Savaşından Günümüze Kriptoloji: Enigma'dan AES'e Şifreleme, **Bilim Teknik, 500: 28-34.**

8. Rivest, R., Adleman, L., ve Dertouzos, M.L., 1978. On data banks and privacy homomorphisms, **Foundations of Secure Computation**.

9. Silverberg, A., 2013. Fully Homomorphıc Encryptıon for Mathematicıins, **sponsored by DARPA under agreement numbers FA8750-11-1-0248 and FA8750- 13-2-0054**.

10. Goldwasser, S. ve Micali, S., 1982. Probabilistic encryption and how to play mental poker keeping secret all partial information, **in proceedings of the 14th ACM Symposium on Theory of Computing**, 365–377.

11. Pailler, P., 1999. Public-Key Cryptosystems Based on Composite degree Residuosity Classes, **in Advances in Cryptology, Eurocrypt**, 223–238.

12. Boneh, D., Goh, E., ve Nissim, K., 2005. Evaluating 2-DNF formulas on chiphertexts, ˙In Theory of Cryptography, **Lecture Notes in Computational Science , Springer**, 325–341.

13. Gentry, C., 2009. A Fully Homomorphic Encryption Scheme, Ph.D. thesis, Stanford University.

14. Gentry, C., 2009. Fully Homomorphic Encryption Using Ideal Lattices, **In Procedings of STOC '09**, 169–178.

15. Gentry, C., 2010. Computing arbitrary functions of encrypted data, **Communications of the ACM**, 97–105.

16. Sharma, I., 2013. Fully Homomorphic Encryption Scheme with Symmetric Keys, Master's thesis, Rajasthan Technical University.

17. Gupta, C.P. ve Sharma, I., 2013. A Fully Homomorphic Encryption scheme with Symmetric Keys with Application to Private Data Processing in Clouds, Network of the Future (NOF), **Fourth International Conference on the Digital Object Identifier: 10.1109/NOF.2013.6724526, IEEE Conference Publıcatıons**, 1 – 4.

18. Chunsheng, G., 2011. Full Homomorfik Encryption Based on Approximate Matrix GCD, **http://eprint.iacr.org/2011/645.pdf**. (Şubat 2016)

19. Telciler, C. Elektronik Seçim Sistemi, **Pamukkale Üniversitesi**.

20. **http://www.timurdemir.com.tr/bulut-bilisim-cloud-computing-nedir**/( Aralık 2015)

21. Taşcı, D., 2007. Soyut Cebir, Alp Yayınevi.

22. Menezes, A.J., van Oorschot, P.C., ve Vanstone, S.A., 1996. Handbook of Applıed Cryptography.

23. McCURLEY, K.S., 1990. The Discrete Logarithm Problem, **Proceedings of Symposia in Applied Mathematics**, **42**.

24. Goluch, S., 2011. The development of homomorphic cryptography From RSA to Gentry's privacy homomorphism, Ph.D. thesis, Vienna University of Technology.

25. TEBAA, M., HAJJI, S.E., ve GHAZI, A.E., 2012. Homomorphic Encryption Applied to the Cloud Computing Security, **Proceedings of the World Congress on Engineering 2012WCE 2012, July 4 - 6, London, U.K.**, **1**.

26. Parmar, P.V., Padhar, S.B., Jhaveri, R.H., Patel, S.N., Bhatt, N.I., ve Jhaveri, R.H., April 2014. Survey of Various Homomorphic Encryption algorithms and Schemes, **International Journal of Computer Applications**.

27. Cao, X., Moore, C., O'Neill, M., Hanley, N., ve O'Sullivan, E., 2014. High-Speed Fully Homomorphic Encryption over the Integers, **Lecture Notes in Computational Science , Springer,**.

28. Hu, Y., 2013. Improving the Efficiency of Homomorphic Encryption Schemes, Ph.D. thesis,Worcester Polytechnic Institüte. 29. Hu, Y., Martin, W.J., ve Sunar, B., 2012. Enhanced Flexibility for Homomorphic Encryption Schemes via CRT, **Proceedings ACNS, Springer Verlag, LNCS,**.

29. Wu, C.H., Hong, J.H., ve Wu, C.W., 2001. RSA Cryptosystem Design Based on the Chinese Remainder Theorem, **IEEE**.

30. Yi, X., Paulet, R., ve Bertino, E., 2014. Homomorphic Encrption and Applications, Springer.

31. Rivest, R., Shamir, A., ve Adleman, L., 1978. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.

32. Gamal, T.E., July 1985. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, **IEEE Transactions on Information Theory, Vol. IT-31, No. 4,**.

# ÖZGEÇMİŞ

## KİŞİSEL BİLGİLER

Adı, Soyadı: Gülhanım YALÇINKAYA

Uyruğu: Türkiye (TC)

Doğum Tarihi ve Yeri: 10 Ocak 1990, Kayseri

Medeni Durumu: Bekar

Tel: +90 538 630 85 40

email: gulyalcinkaya@hotmail.com

## EĞİTİM

| Derece | Kurum | Mezuniyet Tarihi |
|---|---|---|
| Lisans | Erciyes Üniversitesi Fen Fakültesi Matematik Bölümü | 2013 |
| Lise | Sema Yazar Anadolu Lisesi, Kayseri | 2008 |

## YABANCI DİL

İngilizce