T.C.

NEVŞEHİR HACI BEKTAŞ VELİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

KRİPTOGRAFİ, STEGANOGRAFİ VE KODLAMA TEORİSİNİN GRUP TEORİSİ İLE İLİŞKİSİNİN İNCELENMESİ VE BAZI UYGULAMALARIN GELİŞTİRİLMESİ

Tezi Hazırlayan

Mehmet KALKAN

Tez Danışmanı

Doç. Dr. ZARİFE ZARARSIZ

Matematik Anabilim Dalı

Doktora Tezi

Şubat 2021

NEVŞEHİR

T.C.

NEVŞEHİR HACI BEKTAŞ VELİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

KRİPTOGRAFİ, STEGANOGRAFİ VE KODLAMA TEORİSİNİN GRUP TEORİSİ İLE İLİŞKİSİNİN İNCELENMESİ VE BAZI UYGULAMALARIN GELİŞTİRİLMESİ

Tezi Hazırlayan

Mehmet KALKAN

Tez Danışmanı

Doç. Dr. ZARİFE ZARARSIZ

Matematik Anabilim Dalı

Doktora Tezi

Şubat 2021

NEVŞEHİR

Doç. Dr. Zarife ZARARSIZ danışmanlığında Mehmet KALKAN tarafından hazırlanan "Kriptografi, Steganografi ve Kodlama Teorisinin Grup Teorisi ile İlişkisinin İncelenmesi ve Bazı Uygulamaların Geliştirilmesi" başlıklı bu çalışma jürimiz tarafından Nevşehir Hacı Bektaş Veli Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalında Doktora Tezi olarak kabul edilmiştir.

JÜRİ

Başkan : (Prof. Dr. Fatma KARİPCİN)

Üye : (Doç. Dr. Zarife ZARARSIZ)

Üye : (Dr. Öğr. Üyesi Hatice TOPCU)

Üye : (Dr. Öğr. Üyesi Ziyattin TAŞ)

Üye : (Dr. Öğr. Üyesi Maya ALTINOK)

ONAY :

Bu tezin kabulü Enstitü Yönetim Kurulunun ... /… / 2021 tarih ve 2021 / … sayılı kararı ile onaylanmıştır.

… / … / 2021

Prof. Dr. Şahlan ÖZTÜRK

Enstitü Müdürü

TEZ BİLDİRİM SAYFASI

Tez yazım kurallarına uygun olarak hazırlanan bu çalışmada yer alan bütün bilgilerin bilimsel ve akademik kurallar çerçevesinde elde edilerek sunulduğunu ve bana ait olmayan her türlü ifade ve bilginin kaynağına eksiksiz atıf yapıldığını bildiririm.

Mehmet KALKAN

TEŞEKKÜR

Desteği, tecrübesi ve bilgisiyle bana rol model olan çok kıymetli danışmanım Doç. Dr. Zarife ZARARSIZ'a, önceki çalışmalarımda desteğini eksik etmeyen değerli Prof. Dr. Hacı AKTAŞ'a, bir ömür boyu desteğini eksik etmeyen aileme, sabır ve desteğini sakınmayan eşim ve çocuklarıma sonsuz teşekkürlerimi sunarım.

KRİPTOGRAFİ, STEGANOGRAFİ VE KODLAMA TEORİSİNİN GRUP TEORİSİ İLE İLİŞKİSİNİN İNCELENMESİ VE BAZI UYGULAMALARIN GELİŞTİRİLMESİ

(Doktora Tezi)

Mehmet KALKAN

NEVŞEHİR HACI BEKTAŞ VELİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

Şubat 2021

ÖZET

Bu tezin amacı: kriptografi, steganografi ve kodlama teorisinin grup teorisi ile ilişkisinin incelenmesi; esnek küme ve esnek gruplar kullanılarak esnek kriptografi, esnek steganografi ve esnek kod tabanlı yapılar oluşturmaktır.

Tez çalışması dört bölümden oluşmaktadır.

Tezin birinci bölümünde temel tanımlar, teoremler, kavramsal bilgiler toplanarak daha önce yapılmış olan çalışmalar incelenmiştir. Grup teorisi, kodlama teorisi, steganografi, esnek küme, esnek kriptografi ile esnek kodlama teorisinin temel özelliklerine yer verilmiştir.

İkinci bölümde steganografinin matematiksel yapısı tanımlanmıştır. Ayrıca steganografinin özellikleri ve kriptografi ile ilişkisi incelenerek melez bir yapı olan kristografi algoritması incelenerek esnek kristografi algoritması oluşturulmuştur.

Üçüncü bölümde kodlama teorisi ile ilgili cebirsel çalışmalar ve cebirsel kodlar incelenmiştir. Bu bölümde esnek küme üzerinde tanımlanmış olan cebirsel yapılar kullanan esnek kod türleri incelenmiştir. Kod tabanlı kriptografi protokolü olan McEliece kriptografi sistemi üzerine esnek McEliece kriptografi sistemi tanımlanmıştır.

Son bölümde ise grup tabanlı kriptografik algoritmalar ile esnek kriptografi incelenmiş ve bu kapsamda esnek kriptografi anahtar değişim protokolleri tasarlanmıştır.

Anahtar kelimeler: Esnek gruplar, esnek kodlama teorisi, kristografi, esnek kriptografi, grup kriptografi.

Tez Danışmanı: Doç. Dr. Zarife ZARARSIZ

Sayfa Adedi: 146

EXAMINATION OF THE RELATIONSHIP OF GROUP THEORY AND CRYPTOGRAPHY, STEGANOGRAPHY, CODING THEORY AND DEVELOPMENT OF SOME APPLICATIONS

(Phd. Thesis)

Mehmet KALKAN

NEVŞEHİR HACI BEKTAŞ VELİ UNİVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

February 2021

ABSTRACT

The aim of this thesis is to analyze the relationship between cryptography, steganography and coding theory with group theory. Soft cryptography, soft steganography and soft code based structures are created by using soft sets and soft groups.

The thesis consists of four parts.

In the first part of the thesis, basic definitions, theorems and conceptual information are collected and previous studies have been analyzed. The basic features and definitions of group theory, coding theory, steganography, soft sets, soft cryptography and soft coding theory are given.

In the second chapter, the mathematical structure of steganography is defined. In addition, by examining the properties of steganography and its relationship with cryptography, the crystography algorithm, which is a hybrid structure, was analyzed and a soft crystography algorithm was created.

In the third chapter, algebraic studies on coding theory and algebraic codes are determined. In this section, soft code types are analyzed by using algebraic structures defined on soft sets. Soft McEliece was defined on the McEliece cryptography system, which is a code-based cryptography protocol.

In the last part, group-based cryptographic algorithms and soft cryptography are analyzed and new soft sets applications are designed on key exchange protocols.

Keywords: Soft groups, soft coding theory, crystography, soft cryptography, group cryptography.

Thesis Supervisor: Assoc. Prof. Dr. Zarife ZARARSIZ

Page Number: 146

İÇİNDEKİLER

BÖLÜM 4

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

RESİMLER LİSTESİ

SİMGE ve KISALTMALAR LİSTESİ

AES : Advanced Encryption Standard (Gelişmiş şifreleme standardı)

DES : Data Encryption Standard (Veri şifreleme standardı)

RSA : Rivest-Shamir-Adleman

FPGA : Field Programmable Gate Array (Alanda programlanabilir kapı dizisi)

SCA : Side-Channel Analysis (Yan kanal analizi)

TA : Timing Analysis (Zaman analizi)

PA : Power Analysis (Güç analizi)

SPA : Single Power Analysis (Tek güç analizi)

DPA : Differential Power Analysis (Diferansiyel güç analizi)

ECC : Elliptic Curve Cryptography (Eliptik eğri kriptografi)

EMA : Electromagnetic Analysis (Elektromanyetik analiz)

SEMA : Single Electromagnetic Analysis (Tekli elektromanyetik analiz)

DEMA : Differential Electromagnetic Analysis (Diferansiyel Elektromanyetik analiz)

NIST : National Institute of Standards and Technology (Ulusal Standartlar ve Teknoloji Enstitüsü)

FIPS : Federal Information Processing Standards (Federal Bilgi İşleme Standartları)

$G\mathbb{F}$: Galois Cismi

DHP : Diffie-Helman problem (D-H problemi)

MSP : The membership search problem (Üyelik arama problemi)

CSP : Conjugacy search problem (Eşlenik arama problemi)

FSP : The factorization search problem (Çarpanlara ayırma arama problemi)

WP : The word problem (Kelime problemi)

DSP : The decomposition search problem (Ayrışma arama problemi)

GFP : Generalized factor problem (Genelleştirilmiş faktör problemi)

KEP : Key exchange problem (Anahtar değişim problemi)

DLP : Discrete logarithm problem (Ayrık logaritma problemi)

IP : The isomorphism problem (İzomorfizm problemi)

$\mathbb{N}$: Doğal sayılar kümesi

$\mathbb{Z}$: Tam sayılar kümesi

$\mathbb{Q}$: Rasyonel sayılar kümesi

$\mathbb{R}$: Reel sayılar kümesi

$\mathbb{C}$: Karmaşık sayılar kümesi

$C^{\perp}$: C kodunun duali

$|C|$: C kodunun eleman sayısı

G^{T} : G üreteç matrisinin transpozu

$w(a)$: Bir a sözcüğünün ağırlığı

$Ham(r, 2)$: İkili Hamming kodu

$G\mathbb{F}(q)$: Mertebesi $q = p^{k}$ olan Galois cismi

$\mathbb{F}_{q^m}$: q^m elemanlı sonlu cisim

$\mathbb{F}_{q}$: $\mathbb{F}_q$ üzerinde n boyutlu vektör uzayı

$\mathbb{F}_{q}^{k\times n}$: $\mathbb{F}_q$ üzerinde $k \times n$ boyutlu matrisler kümesi

m : Açık metin

c : Şifreli metin

e : Hata vektörü

n : Kod uzunluğu

k : Kod boyutu

d : Kod uzaklığı

(n, k, d) : Uzunluğu n, boyutu k, minimum uzaklığı d olan lineer kod

BÖLÜM 1

AMAÇ ve KAPSAM

1.1. Giriş

Bu tezin amacı: Kriptografi, steganografi ve kodlama teorisinin grup teorisi ile ilişkisinin incelenmesi; esnek küme ve esnek gruplar ile mevcut kodlama teorisi, kriptografi ve steganografi sistemlerini birleştirerek bu sistemlere katkı sunulmasıdır.

Tez çalışması dört bölümden oluşmaktadır.

Birinci bölümünde tez konusu için literatür taraması yapılmış, konu ile ilgili temel tanımlar, teoremler, kavramsal bilgiler toplanarak daha önce yapılmış olan çalışmalar incelenmiştir. Grup teorisi, kodlama teorisi, steganografi, esnek küme, esnek kriptografi ve esnek kodlama teorisi temel özellikleri verilmiştir.

İkinci bölümde steganografinin matematiksel yapısı tanımlanarak ve genel özellikleri, kriptografi ile ilişkisi incelenerek melez bir yapı olan esnek kristografi algoritması oluşturulmuştur.

Üçüncü bölümde kodlama teorisi ile ilgili cebirsel çalışmalar, cebirsel kodlar, esnek cebirsel kodlar ve McEliece kod tabanlı kriptografi incelenmiştir. Kod tabanlı esnek kriptografi tanımlaması yapılmıştır.

Son bölümde ise grup tabanlı kriptografik algoritmalar ile esnek kriptografi incelenmiş ve bu kapsamda yeni esnek kriptografik uygulamalar tasarlanmıştır.

1.2. Temel Kavramlar

Bu çalışmada, mevcut cebirsel yapılar kullanılarak oluşturulan esnek cebirsel yapılar incelenmiştir. Ayrıca, esnek kodlama metotları, esnek kristografi ve esnek kriptografi üzerinde çalışılmıştır.

Molodtsov [12] 1999 yılında belirsizlik kavramı ile başa çıkmak için bir matematiksel araç olarak esnek küme tanımını vermiştir. Bu kavram karar verme problemleri, istatistik, olasılık, kriptografi, kodlama teorisi, cebirsel uygulamalar ve sağlık bilimleri gibi bilimin birçok alanında kullanılmıştır. Esnek küme kavramı üzerine ilk cebirsel yapı Aktaş, H. ve Çağman, N. tarafından "Soft Sets and Soft Groups" isimli makaleleri ile 2007 yılında tanımlanmıştır [20]. Bu çalışmadan sonra araştırmacılar tarafından birçok esnek cebirsel yapı tanımı yapılmış ve cebirsel özellikleri incelenmiştir [6, 21-25].

Ayrıca gruplar, sonlu halkalar, esnek sonlu cisimler, vektör uzayları gibi cebirsel yapılar kullanılarak birçok kod türü ve hata düzeltme kodları geliştirilmiştir [39-40, 42, 44-47].

Kodlama teorisinin konusunu iletişimde dijital olarak kodlanmış verilerin kullanımı esnasında meydana gelen problemler ve bu problemlerin çözümleri oluşturmaktadır. 1948 yılında Claude E. Shannon tarafından yayımlanan "Haberleşmenin Matematiksel Teorisi" isimli makale bilgi ve kodlama teorisinin başlangıç noktası olarak kabul edilir [1]. Shannon bu makalesinde transfer edilen veride bozulmanın meydana gelme olasılığı olan bir iletişim kanalı için kanal kapasitesini tanımlamış ve bu kapasitenin altında herhangi bir güvenirlik düzeyinde iletişim sağlanmasının mümkün olduğunu olasılık kuramına ait metotlar kullanarak ispatlamıştır. Fakat ne Shannon'un ispatı ne de daha sonra ortaya konulan yeni ispatlar mükemmel kodlama sisteminin tasarlanması için yeterli olmamış, Shannon'un teoreminde bahsedilen şifreleme metodu henüz bulunamamıştır. Kodlama teorisyenleri bu teoriyi temel alarak gürültü kanalları boyunca veri iletimi ve bozulan mesajı düzeltme gibi konularla ilgilenmiş; doğru iletim oranı yüksek, zaman ve enerji tasarrufu sağlayan şifreleme yöntemlerini elde etmeyi hedeflemişlerdir. Amaçları iletişim sisteminde kaynaktan gönderilen mesajı doğruluğu yüksek bir olasılıkla iletmektir. Mesajı göndermek için alfabe olarak adlandırılan sonlu kod kümeler kullanılır. Kod kümesi olarak genellikle sonlu bir cisim ya da halka alınır. İletilecek mesaj oluşabilecek hatalardan korunmak üzere şifrelenir. Şifrelenen bu mesaj, kod kümesinin elemanları olan

"kod kelimeleri" dir. Kod kelimeleri kanala gönderilir. Bu gönderim esnasında bazı terimleri değişmiş yani hata oluşmuş olabilir. Sistem kod kelimelerinde hata olup olmadığını kontrol eder, hata varsa düzeltir ve orijinal mesajı elde edip alıcıya gönderir. İki kod kelimesinin farklı olduğu bit sayısı Hamming uzaklığı olarak ifade edilir. Kodun Hamming uzaklığı olarak da adlandırılan bir kodun minimum uzaklığı ne kadar büyük olursa kod o kadar çok hata düzeltebileceğinden, minimum uzaklığı büyük olan kodların elde edilmesi önemlidir [2].

Mesajların kodlanması için gerekli olan sembollerin tümünün kümesine kod alfabesi denir ve bu alfabe kullanılarak oluşturulan bütün kod kelimelerinin oluşturduğu kümeye ise kod denir [3]. Örneğin, $C = \{00, 01, 10, 11\}$ kodunun kod kelimeleri sırasıyla 00, 01, 10 ve 11, kod alfabesi ise $\{0,1\}$ dir. Kodlar da kendi içinde lineer kodlar, Hamming kodlar, genelleştirilmiş Reed-Solomon kodları, değiştirme kodları, devirli kodlar, Golay kodları, Reed-Muller kodları vb. olarak çeşitlenmektedir.

Kodlama teorisi, ilk ortaya atıldığı yıllarda akademik çevrede pek ilgi görmese de 1970'lerin ortalarında haberleşme sistemlerinin alt yapısında kullanılmaya başlanmıştır [11]. Bu teori, matematik, istatistik, bilgisayar, şifreleme ve haberleşme alanlarında haberleşme karmaşıklığını en az seviyeye indirmek ve kaynakların etkin biçimde temsil edilmesini sağlamak amacıyla kullanılmaktadır. Kodlama, iletişim alanında kaynakların, kanalların, alıcıların bilgi karakteristiklerini incelemek, bilginin iletimini optimize etmek ve iletimin güvenirliliğini sağlamak amacıyla kullanılmaktadır. Bilginin iletimi için vericiden gönderilen mesaj sözcüğünün gönderildiği kanaldan, gönderenden veya mesajı alandan kaynaklanan hatalar oluşabilir. Bu hatalardan dolayı mesaj sözcüğü bozulmaya uğrar ve alıcıya gönderilen mesajdan farklı bir mesaj sözcüğü iletilebilir. Bu durum haberleşme sisteminin hatalı mesaj göndermesi olarak adlandırılır. Kodlama teorisinin amacı da bu hatalı mesajları düzelterek doğru mesaj aktarımını en iyi duruma getirmektir.

Özlü [125] tarafından yapılan çalışmada esnek cebirsel kodlar tanımlayabilmek için literatürde mevcut olan [35]-[46] çalışmalardan yararlanmıştır. Bu çalışmada esnek grup tanımı kullanılarak bazı sonlu cisimler üzerinde esnek polinom kodları tanımlanmıştır. Buna ek olarak, esnek hata düzeltme kodları Aktaş ve Özlü [124] tarafından literatüre kazandırılmıştır.

Belirsizlik kavramını ilk defa Heisenberg tarafından 1920'lerde ortaya atılmıştır. Matematik, fizik, ekonomi, mühendislik, çevre bilimi gibi birçok bilim dalında klasik mantık kaynaklı görülen belirsizlik problemleri mevcuttur. Belirsizlik kavramı uzun yıllardan beri matematikçiler, mantıkçılar ve filozofların uğraş alanı olmuştur. Dolayısıyla belirsizlik problemlerinin çözümüne ulaşabilmek, bilgisayar ve yapay zeka alanında çalışan bilim insanları için de çok önemli olmuştur. Klasik mantığın tanımlayamadığı belirsiz kavramların matematiksel olarak ifade edilebilmesinin öneminden dolayı bilim adamları tarafından her geçen gün yeni teoriler ortaya koymaktadır. Bilinen en önemli teoriler; Fuzzy (bulanık) kümeler, yaklaşımlı kümeler, esnek küme, olasılık ve istatistik olmuştur [12], [14], [53], [106], [126], [127].

Ekonomi, mühendislik ve çevre bilimi ile ilgili bazı problemlerde birden fazla değişken olduğu için bu problemlerin klasik yöntemlerle çözümünün mümkün olmadığı durumlar ortaya çıkabilmektedir. Bu alanlarda ortaya çıkan belirsizlikler çok çeşitli tiplerde olabileceğinden klasik metotlar yetersiz kalmaktadır. Belirsizliği tanımlama ve modellemenin önemini ünlü fizikçi Einstein şu şekilde ifade etmiştir. "Matematiğin kavramları kesin oldukları sürece gerçeği yansıtmazlar, gerçeği yansıttıkları sürece de kesin değildirler" [10]. Klasik mantığın tanımlayamadığı belirsiz kavramların matematiksel olarak ifade edilebilmesine imkân tanıyan bulanık küme teorisi, klasik olasılık teorisinin bir alternatifi olarak görülmektedir. Bulanık küme teorisi ile belirsizlik kavramı matematiksel olarak tanımlanmış ve görüntü işleme, robotik, denetim mühendisliği, bilgisayar mühendisliği, bilgi işlem, vb. günlük hayatımıza kadar giren konularda yararlı uygulamalarda bulunulmuştur. 1982 yılında Pawlak [14] tarafından ortaya atılan yaklaşımlı küme teorisi ise evrenin alt kümelerinin, evrenin parçalanışının denklik sınıfları yardımıyla ifade edilebilmesi ihtiyacından ortaya çıkmıştır. Yaklaşımlı küme teorisi klasik küme teorisinin bir genişlemesidir. Yaklaşımlı küme teorisi, klasik küme kuramının aksine, bir kümenin tanımlanması için başlangıçta evrenin elemanları hakkında bazı bilgilere gereksinim olduğu varsayımına dayanan yaklaşımdır. Ancak bu teori de istenen düzeyde belirsizlik problemine çözüm getirememiştir. Bu belirsizlikleri ortadan kaldırmak için Molodtsov tarafından 1999 [12] yılında yayımlanan çalışma ile ilk kez esnek küme tanımını aşağıdaki şekilde verilmiştir.

Tanım 1.2.1. [12] U evrensel küme ve E de parametrelerin bir kümesi olsun. $P(U)$, U'nun kuvvet kümesi ve $A \subset E$ olmak üzere $F: A \to P(U)$ ile verilen bir dönüşüm ise (F, A) sıralı ikilisi U üzerinde esnek küme olarak adlandırılır.

Esnek küme teorisi, Molodtsov tarafından belirsizlikle başa çıkmak için bir matematiksel araç olarak ortaya atılmıştır. Molodtsov tarafından sürekli türevlenebilir fonksiyonlar, oyun teorisi, işlem araştırmaları, Riemann integrasyonu, Perron integrasyonu, olasılık, ölçüm teorisi vb. alanlarda esnek küme teorisini kullanılarak başarılı çalışmalar yapılmıştır. Ayrıca, Molodtsov yaklaşımlı nesne kavramını formülize etmiş ve "Esnek Küme Teorisi" isimli bir kitap yayımlamıştır [13]. Maji ve arkadaşları yaklaşımlı küme teorisi yardımıyla bir karar verme probleminde esnek kümenin bir uygulamasını sunmuşlardır [14],[27]. Ayrıca, bu çalışmalarında esnek küme teorisinde ihtiyaç duyulan birleşim ve kesişim gibi bazı temel kavramları tarif etmişlerdir. Xiao ve arkadaşları [15] tarafından esnek küme temelli iş rekabet kapasitesi için yapay bir hesaplama metodu üzerine çalışmalar yapılmıştır. Yang ve arkadaşları [16] tarafından yayımlanan makalede esnek ve yaklaşımlı küme tarifleri klinik teşhisin karar analizi indüksiyonuna uygulanmıştır. Chen ve arkadaşları [17] ile Kong ve arkadaşları [18] esnek kümede parametre indirgemesi üzerinde çalışmalar yapmışlardır. Ayrıca Mushrif ve arkadaşları [19] esnek küme temelli sınıflandırmalar üzerine çalışmalar yapılmıştır.

Aktaş ve Çağman [20] esnek grupların tanımını vermiş ve esnek grupların bazı temel özelliklerini elde etmişlerdir. Jun [21] esnek BCK\BCI-cebirleri ve esnek alt cebir kavramlarını ortaya atarak onların bazı özelliklerini incelemiştir. Jun ve Park [22] esnek kümeyi BCK\BCI-cebirlerine uygulayarak BCK\BCI-cebirlerinde esnek kümenin cebirsel özelliklerini araştırmıştır. Park ve arkadaşlarının [23] esnek WS-cebirleri üzerine bir çalışması yayımlanmıştır.] Esnek küme teorisini kullanılarak esnek halka tanımı Feng ve arkadaşları tarafından verilmiştir [24]. Sun ve arkadaşları [25] esnek modül tanımını vermiş ve Molodtsov'un esnek küme tanımını kullanarak esnek modüllerin önemli görülen bazı özelliklerini inşa etmişlerdir.

Zou ve Xiou [26] çalışmalarında, esnek kümedeki eşleme fonksiyonlarının değer alanları özelliğini kullanılmışlardır. Bu özelliğin kullanılması ile asimetrik verilerin gerçek durumunu yansıtmak için esnek kümenin veri analizi yaklaşımlarını belirleme aşamasında tercih edilebilir olduğu gösterilmiştir. Maji ve arkadaşları [27], bulanık esnek

kümeyi tanımlamış ve pek çok araştırmacının bulanık esnek küme üzerine çalışmasına öncülük etmişlerdir. Aktaş ve Çağman ise esnek kümeyi, bulanık küme ve yaklaşımlı küme kavramlarıyla karşılaştırmışlardır [20]. Aslam ve Qurashi [46] ise esnek alt grup, normal esnek grup, devirli esnek grup ve esnek homomorfizma kavramlarını tanımlamışlardır. Roy ve Maji [28] bir karar verme probleminde bulanık esnek kümenin uygulaması konusunda çalışmalar yapmışlardır. Yang ve arkadaşları [29] bulanık esnek kümede indirgemeyi tanımlayarak, bulanık esnek küme yardımıyla karar verme probleminin analizi yapmışlardır. Majumdar ve Samanta [30] da bulanık esnek kümede benzerlik ölçümünü ortaya atmışlardır. Kong ve arkadaşları [31] ile Xiou ve arkadaşları [32], bulanık esnek küme üzerine dayalı bazı yaklaşımları konu alan bir çalışma yapmışlardır.

Molodstov ve arkadaşları [33] tarafından, esnek küme teorisine dayalı bir analiz geliştirilerek, esnek sayı, esnek türev, esnek integral gibi kavramlar formülize edilmiştir. Bu analiz, Konkov ve arkadaşları [34] tarafından optimizasyon teorisi ile ilgili problemlere uygulanmıştır. Günümüz çalışmalarında da, esnek küme teorisi ve onun uygulamaları üzerine yapılan çalışmalar hızla gelişmektedir. Esnek küme teorisinin kriptografiye uygulanması yeni çalışılan bir alandır [128,142-144,160-163].

Kriptografi Yunanca'da gizli anlamındaki kryptós ve yazmak anlamına gelen graphein kelimelerinin birleşiminden oluşur. Kriptografi, üçüncü şahıslar veya kamu tarafından özel mesajların okumasını engelleyen protokoller bütünüdür. Modern kriptografi matematik, bilgisayar bilimleri, elektrik mühendisliği , iletişim bilimi ve fiziğin kesiştiği bilim alanıdır. Kriptografi uygulamaları arasında elektronik ticaret, kredi kartı gibi çip tabanlı ödeme kartları, dijital para birimleri , bilgisayar parolaları, blok zincir uygulamaları, elektronik kapılar ve askeri iletişim kanalları yer alır [120].

Kriptografinin tarihsel gelişiminin kronolojik örnekleri aşağıda verilmiştir [120];

- MÖ 1900 dolaylarında Mısırlı bir kâtibin yazdığı kitabelerde kullandığı standart dışı hiyeroglif işaretler ilk kriptografik işaretler olarak ele alınmaktadır.
- MÖ 60-50 Julius Caesar (MÖ 100-44) normal alfabedeki harflerin yerini üç karakter sağa kaydırarak yer değiştirme ile oluşturduğu şifreleme yöntemi, devlet yönetimi haberleşme sisteminde kullanılmıştır.

- 725-790 Abu Abd al-Rahman al-Khalil ibn Ahmad ibn Amr ibn Tammam al Farahidi al-Zadi al Yahmadi'nin kriptografi hakkında bir kitap yazdığı ancak bu kitabın kaybolduğu bilinmektedir.
- 1000-1200 yıllarında Gaznelilerden günümüze kalan bazı dokümanlarda şifrelenmiş metinlere rastlanmıştır. Bu metinlerde, yüksek mevki sahibi devlet görevlileri yeni görev yerlerine giderken şahsa özel şifreleme bilgileri verilmiştir.
- İlk olarak Giovan Battista Bellaso tarafından 1553'te tanımlanan Vigenère şifresi, Blaise de Vigenère'den esinlenerek adlandırılmıştır.
- 1623'te Sir Francis Bacon tarafından 5-bit ikili kodlamayla karakter tipi değişikliğine dayanan steganografi tanımlanmıştır.
- 1854'te Charles Wheatstone playfair şifresini tasarlamıştır.
- 1790 yılında strip cipher makinesi Thomas Jefferson tarafından geliştirilmiştir. ABD donanmasınca II. Dünya Savaşı'nda kullanılan M-138-A ise strip cipher makinesi baz alınarak tasarlanmıştır.
- 1917'de Joseph Mauborgne ve Gilbert Vernam mükemmel şifreleme sistemi olan tek kullanımlık şifre anlamındaki one time pad sistemini tasarlamışlardır.
- 1920 ve 1930 yılları arasında FBI bünyesinde içki kaçakçılarının gizli haberleşmelerini çözebilmesi için bir araştırma ofisi kurulmuştur.
- 1940'lı yıllarda Japonya'da Purple makinesi inşa edilmiştir.
- William F. Friedman, Riverbank laboratuvarını kurarak ABD güvenlik birimleri için kriptografik analiz çalışmaları yapmıştır. Bu çalışmalar sonucunda II. Dünya Savaşı'nda Japon ordusunun kullandığı Purple makinesinin şifreleme sistemi kırılmıştır.
- II. Dünya Savaşı'nda Almanlar Arthur Scherbius tarafından icat edilmiş olan Enigma makinesini kullanmışlardır. Bu makine Alan Turing ve ekibi tarafından çözülmüştür.
- 1970'lerde Horst Feistel, Lucifer algoritmasını geliştirmiştir.
- 1976'da DES (Data Encryption Standard) algoritması, ABD tarafından Federal "Information Processing Standard" veri tasarımı standardı olarak açıklanmıştır.
- 1976'da Whitfield Diffie ve Martin Hellman, açık anahtar kriptografi sistemini anlattıkları makale yayımlanmıştır.

- 1978'de Ronald L. Rivest, Adi Shamir ve Leonard M. Adleman tarafından RSA algoritması geliştirilmiştir.
- 1985'te Neal Koblitz ve Victor S. Miller birbirlerinden bağımsız yaptıkları çalışmalarında eliptik eğri kriptografik (ECC) sistemlerini geliştirmişlerdir.
- 1990'da Xuejia Lai ve James Massey, IDEA algoritmasını tasarlamışlardır.
- 1991'de Phil Zimmerman, PGP sistemini geliştirmiştir.
- 1995'te SHA-1 özet algoritması NIST tarafından özet algoritma standardı olarak yayımlanmıştır.
- 1997'de ABD'nin NIST Kurumu DES algoritmasının yerini alacak yeni bir simetrik algoritma için yarışma yapmıştır.
- 2001'de NIST'in yarışmasını kazanan Belçikalı Joan Daemen ve Vincent Rijmen tarafından AES (Advanced Encryption Standard) algoritması geliştirilmiştir.

Kriptografi, Gizlilik (privacy / confidentiality), Kimlik Denetimi (authentication / identification), Bütünlük (integrity), Reddedilemezlik (non-repudation) ve Erişim Kontrolü (access control) gibi bilgi güvenliği kavramlarını sağlamak için bir bilginin istenmeyen taraflarca okunamayacak bir hale dönüştürülmesinde kullanılan matematiksel yöntemler bütünüdür. Kriptografi, anahtarsız, gizli anahtarlı ve açık anahtarlı olmak üzere üç ana grupta incelenebilir. Bununla beraber kuantum bilgisayarlarının tasarlanması ile kuantum kriptografiden de söz edilebilir. Ancak günümüzde kuantum bilgisayar sistemleri çok yüksek maliyet gerektirdiğinden klasik bilgisayar sistemleri ile kuantum kriptografi çalışma alanı çok sınırlıdır [120].

Braid gruplar, devirli gruplar veya bazı sonlu cebirsel grupların kriptografi algoritmalarında kullanılmasıyla elde edilen kriptografik sistemlere grup bazlı kriptografi denir. Grup teorisi birçok kriptografi algoritmaları ve kriptografik anahtar değişim protokollerinde kullanılabilmektedir. Örneğin Diffie-Hellman anahtar değişimi protokolünde sonlu devirli grup kullanılır. Bununla birlikte Magyarik-Wagner açık anahtar protokolü, Anshel-Anshel-Goldfeld anahtar değişimi ve Ko-Lee ve arkadaşlarının anahtar değişim protokolü gibi örnekler incelenebilir [52, 54]. Ayrıca Thompson's grup, matris gruplar, küçük sadeleştirme grupları, solvable gruplar, Artin gruplar üzerinde de kriptografik çalışmalar yapılmıştır [61].

Kriptografinin yanında gizli iletişimi sağlayan bir diğer sistem steganografidir. Steganografi, Yunanca'da "gizlenmiş yazı" anlamına gelir ve veri gizleme bilimine verilen isimdir. Gizli veriyi içeren bir veriyi gören bir kimsenin gördüğü şeyin içinde önemli bir bilgi olduğunu fark edemiyor olması steganografinin şifreleme bilimi kriptografiye göre en büyük avantajıdır. Kriptografi ve steganografi herhangi bir veriyi gizlemek veya korumak için kullanılan yöntemlerdir. Steganografi verileri olduğu gibi, hiçbir değişiklik yapmadan varlığını gizleyebilirken, kriptografi verileri rastgele dizilmiş harf ve rakamlarla anlamsız hale getirilmiş bir metne dönüştürmektedir. Bu da üçüncü tarafların dikkatini çekmektedir. Bu bakımdan steganografi belirgin bir farklılık göstermektedir. Steganografi, hem şifreleme öncesi eski dönemde hem de sonrasında üçüncü tarafların dikkatini çekmemesinin oluşturduğu avantajdan dolayı kullanılmıştır [97].

Steganografinin tarihsel gelişimi göz önüne alındığında aşağıdaki örnekler verilebilir;

- Eski dönemlerde Yunanistan'da, insanlar mesajları tahtaya yazdıktan sonra üzerini mumla kaplamışlardır. Böylece bu tahta cisim kullanılmamış bir tablete benzetilmiştir. Ancak mum eritildikten sonra içindeki gizli mesaj açığa çıkarılmıştır.
- Herodot'un anlattığı bir hikâyede "Pers saldırısının öncesinde saçları tıraşlanan bir kölenin kafasına iletilmek istenen uyarı mesajı yazılmış ve saçlarının uzaması sayesinde saklanmıştır. Bu sayede mesaj dikkat çekmeden gerekli yere ulaştırılmıştır. Köle hedefe ulaştığında da kölenin saçları tekrar tıraşlanarak uyarı okunabilmiştir." denmiştir.
- II. Dünya Savaşı sırasında New York'ta görev yapan Japon ajanı Velvalee Dickinson oyuncak bebek pazarlamacısı kılığında saklanmaktaydı. Bu ajan, Amerikan ordusundan elde ettiği istihbaratı bebek siparişi içeren mektupların içine saklayarak Güney Amerika'daki ilgili adreslere göndermiştir.
- 1960 sonrasında mor ötesi boya ile yazı yazabilen sprey ve kalemler moda olmuştur. Bu boya ile yazılan yazılar, sadece bir mor ötesi ışıkla görülebilmiştir.
- Ron Howard'ın efsane bir sinema yapıtı olan Akıl Oyunları (A Beautiful Mind) filminde, John Nash gazete ve dergilerde gizli mesajlar aramaktaydı [97].

Yukardaki örneklerde de görüldüğü üzere steganografi, bir açık iletişim kanalı üzerinden gizli bilgi iletişimini sağlayan bir araçtır. Steganografi, düz metin, resim, ses veya video dosyasının içinde kullanıcıya gizlenmiş veriyi güvenli bir yolla iletmesine imkân tanımaktadır. Gizlenecek veride yapısal olarak herhangi bir değişiklik yapılmadan ve farklı bir veriye dönüştürülmeden olduğu gibi gizlenerek gönderilmektedir. Gönderilecek veri tamamen gizlenmekte ve böylece, gizlenen veri yetkisiz kişilerden korunabilmektedir. Steganografi bu yönüyle kriptografiden farklılık arz etmektedir [56-60].

Hem kriptografi hem de steganografi güvenli iletişimi sağlamaktadır. Ancak farklı algoritma ve yöntemlerle kullanılmaktadırlar. Bu iki sistemin bir arada kullanılmasıyla daha güvenli algoritmalar elde edilebilmiştir. Steganografi ve kriptografinin kombinasyonundan elde edilen hibrit sistemler kristografi olarak tanımlanmıştır. Bu konuda yapılan çalışmalar incelendiğinde, hemen hemen çalışmaların hepsinde kriptografi sisteminin algoritma yapısını güçlendirmeye yönelik olmadığı görülmektedir. Bu kristografi sistemlerinde, gizlenecek veri önce DES, AES, RSA, vb. kriptografi algoritmalarından birisi kullanılarak şifreli metine dönüştürülür. Daha sonra bu şifreli metin bir steganografi sistemi (örtüsü) içine gömülerek herkese açık bir internet ortamında güvenle gönderilebilmektedir. Bu çalışmaların, verinin daha güvenli saklanarak transferine yönelik olduğu görülmüştür [62-69].

Kriptografi ve steganografi sistemlerinin temelinde kodlama sisteminin gücü de yatmaktadır.

Çalışmanın ikinci bölümünde mevcut kriptografik sistemler ile steganografiyi birbirinden bağımsız kullanmak yerine birleştirerek yeni bir esnek kristografi algoritması tasarlanmıştır.

Bu çalışmada ayrıca son yıllarda daha çok önem kazanan grup teorisinin esnek küme ile olan ilişkisi, esnek gruplar yardımıyla elde edilen yeni kod sistemleri ve esnek yapılarla kriptografi sistemlerinde iyileştirme çalışmaları yapılmıştır.

1.3. Grup Teorisi

Tanım 1.3.1. [115] G boş olmayan bir küme ve G üzerinde tanımlı bir $\cdot$ işlemi olmak üzere, aşağıdaki şartları sağlayan $(G,\cdot)$ ikilisine grup denir:

i. $\forall\, a,b \in G$ için $a \cdot b \in G$ kapalılık özelliği sağlanmalıdır,
ii. $\forall\, a,b,c \in G$ için $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ birleşme özelliği sağlanmalıdır,
iii. G'nin öyle bir e elemanı vardır ki, G'deki herhangi bir a için $a \cdot e = e \cdot a$ olacak şekilde G'de bu özelliği sağlayan tek e birim elemanı vardır,
iv. G'deki her a elemanı için öyle bir $b \in G$ elemanı vardır ki; $a \cdot b = b \cdot a = e$ eşitliği sağlanıyorsa b elemanına a elemanının tersi adı verilir ve $b = a^{-1}$ ile gösterilir.

Sadece i. ve ii. özelliklerine sağlayan $(G,\cdot)$'ye yarı grup denir. Tanımda çarpımsal notasyon kullanılmıştır. $\cdot$ notasyonuna "grup çarpması" denir. Burada, $\forall\, a \in G$ elemanının tersi $b = a^{-1} \in G$ dir. Çarpımsal notasyonunun yerine toplamsal notasyon kullanılması halinde $a \cdot b$ yerine $a + b$ yazılır. Bu durumda $\forall\, a \in G$ elemanın tersi $b = -a \in G$ şeklinde ifade edilebilir.

Grup teorisi uygulamalarının kimya, fizik, kuantum kuramı, bilgisayar bilimleri gibi çok geniş uygulama alanları ve önemi vardır. Aşağıda grup teorisi için bazı önemli uygulama alanları verilmiştir [116];

i. Rubik küpünün çözümünün elde edilmesinde grup teorisi, geometri ve algoritma kullanılır.
ii. Polinomların köklerinin simetrileri gruplar kullanılarak bulunurken Galois teorisinden yararlanılır.
iii. Kriptografide birçok anahtar değişim protokolü sonlu kümeleri baz alır.
iv. Diferansiyel denklemlerin çözümlerinde ve simetrilerinde Lie grupları kullanılır.
v. Kimya biliminde, kristal yapıların sınıflandırılmasında grup teorisinden yararlanılır.

vi. Fizik biliminde ise, Noether teoremi ve fiziksel sistemlerin simetrileri ile o sistemin koruma kanunu arasında bir ilişki kurulmakta ve sistemlerin simetrileri çoğunlukla simetrik gruplar kullanılarak ifade edilmektedir.

Tanım 1.3.2. [114] G boş olmayan bir küme ve $(G,\cdot)$ bir grup olsun. G'deki her a,b elemanı için

$$a \cdot b = b \cdot a$$

eşitliğini sağlıyorsa, $(G,\cdot)$ grubuna değişmeli grup veya abelyen grup denir.

Sonuç 1.3.3 [118] G boş olmayan bir küme ve $(G,\cdot)$ değişmeli bir grup ise iki elemanın çarpımının tersi

$$(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$$

ile gösterilir.

İspat: G boş olmayan bir küme ve $(G,\cdot)$ değişmeli bir grup olsun. $\forall\, a,b \in G$ ve birim eleman $e \in G$ olsun. O halde

$$(a \cdot b) \cdot (a \cdot b)^{-1} = (a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = (a \cdot b) \cdot b^{-1} \cdot a^{-1} = a \cdot (b \cdot b^{-1}) \cdot a^{-1}$$

$$= a \cdot (e) \cdot a^{-1} = (a \cdot e) \cdot a^{-1} = a \cdot a^{-1} = e \text{ olur.}$$

Not: Eğer işlem yapılan grup değişmeli değil ise $a^{-1} \cdot b^{-1} \neq b^{-1} \cdot a^{-1}$

Sonuç 1.3.4. [118] G boş olmayan bir küme ve $(G,\cdot)$ bir grup, $\forall\, a_i \in G\ ve\ i = 1,2,\dots,n$ olsun. O halde

$$(a_1 \cdot a_2 \cdot \dots \cdot a_n)^{-1} = a_n^{-1} \cdot a_{n-1}^{-1} \cdot \dots \cdot a_1^{-1}.$$

Örnek 1.3.5. [117] $(\mathbb{C}\backslash\{0\},\cdot)$, $(\mathbb{Q}\backslash\{0\},\cdot), (\backslash\{0\},\cdot)$ çarpma işlemi üzerinde değişmeli gruplardır. Bu çarpımsal gruplarda "$e = 1$" birim elemandır.

Örnek 1.3.6. [112] $(\mathbb{Z},+)$, $(\mathbb{Q},+), (\mathbb{R},+)$ toplama işlemi üzerinde değişmeli gruplardır. Bu toplamsal gruplarda "$e = 0$" birim elemandır.

Örnek 1.3.7. [118] $M_2(\mathbb{R})$, girdileri reel sayı olan 2×2 lik matrisler kümesi olsun., $\forall\, a,b,c,d \in \mathbb{R}$ ve $\forall \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{R})$ için,

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

olduğundan bu grubun birim elemanı $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ dır.

$\forall \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{R})$ için,

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix} = \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix} + \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

olduğundan $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{R})$ matrisinin toplama işlemine göre tersi $\begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$ dir.

- $\forall \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \begin{bmatrix} k & l \\ m & n \end{bmatrix}, \begin{bmatrix} x & y \\ z & t \end{bmatrix} \in M_2(\mathbb{R})$ için

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \left(\begin{bmatrix} k & l \\ m & n \end{bmatrix} + \begin{bmatrix} x & y \\ z & t \end{bmatrix} \right) = \begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} k+x & l+y \\ m+z & n+t \end{bmatrix}$$

$$= \begin{bmatrix} a+k+x & b+l+y \\ c+m+z & d+n+t \end{bmatrix}$$

$$= \begin{bmatrix} a+k & b+l \\ c+m & d+n \end{bmatrix} + \begin{bmatrix} x & y \\ z & t \end{bmatrix}$$

$$= \left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} k & l \\ m & n \end{bmatrix} \right) + \begin{bmatrix} x & y \\ z & t \end{bmatrix}$$

- $\forall \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \begin{bmatrix} k & l \\ m & n \end{bmatrix} \in M_2(\mathbb{R})$ için

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} k & l \\ m & n \end{bmatrix} = \begin{bmatrix} a+k & b+l \\ c+m & d+n \end{bmatrix} = \begin{bmatrix} k+a & l+b \\ m+c & n+d \end{bmatrix} = \begin{bmatrix} k & l \\ m & n \end{bmatrix} + \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

olduğundan $M_2(\mathbb{R})$ matrisleri toplama işlemine göre değişmeli bir gruptur.

Ancak, $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ elemanının çarpma işlemine göre tersi olmadığından $M_2(\mathbb{R})$ matrisleri çarpma işlemine göre bir grup değildir.

Teorem 1.3.8. [118] G boş olmayan bir küme ve $(G,\cdot)$ bir grup olsun.

i) G'nin birim elemanı tektir.

ii) Her elemanın tersi tektir.

iii) $\forall\, a \in G$ için $(a^{-1})^{-1} = a$ dır.

İspat: $\forall\, a, b, c, e, e' \in G$ için

i) G'nin birim elemanları e, e' olsun. $e \in G$ birim eleman olduğundan $e \cdot e' = e'$ olur. Aynı şekilde $e' \in G$ de birim eleman olduğundan $e \cdot e' = e$ olur öyleyse $e = e'$.

ii) $a \in G$ olsun. $b\ ve\ c$ elemanları da a nın tersleri olsun. Yani $a \cdot b = b \cdot a = e\ ve\ a \cdot c = c \cdot a = e$ olur. Öyle ise $c = c \cdot e = c \cdot (a \cdot b) = (c \cdot a) \cdot b = e \cdot b =$b olur. Buradan da $a = b$ elde edilir.

iii) $b = a^{-1}\ ve\ c = a$ olsun. $b \cdot c = c \cdot b = e$ olduğundan b aynı zamanda c nin tersi olur. Yani $c = b^{-1} = (a^{-1})^{-1} = a$ elde edilir.

Not: Teorem 1.3.8 de toplamsal notasyon kullanılması halinde iii) – $(-a) = a$ olur.

Lemma 1.3.9. [111] G boş olmayan bir küme, $(G,\cdot)$ bir grup ve $x, y, z \in G$ olsun.

Eğer $z \cdot x = z \cdot y$ ise $x = y$ olur.

İspat: $t = z^{-1} \in G$ olsun. $z \cdot x = z \cdot y$ ise

$t \cdot (z \cdot x) = t \cdot (z \cdot y)$ ve $(t \cdot z) \cdot x = (t \cdot z) \cdot y$ elde edilir.

Burada $t \cdot z = e$ ve $z \cdot t = e$ olduğundan

$$e \cdot x = e \cdot y$$

İse

$$x = y$$

olur.

Cebirsel işlemler için sadeleştirme özelliği önemlidir. Ancak her zaman sadeleştirme yapılamaz. 2×2 'lik bir karesel $M_2(\mathbb{Z})$ matrisi ele alınırsa, matris çarpımında sadeleştirmenin her zaman yapılamayacağı görülür.

Tanım 1.3.10. [118] $M_2(\mathbb{R})$ matrisinde çarpma işlemi aşağıdaki şekilde tanımlansın. $\forall a, b, c, d, e, f, g, h \in \mathbb{R}$ için

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{bmatrix}.$$

$M_2(\mathbb{R})$ matrisi çarpma işlemine göre birleşme özelliğine sahiptir. Öyleyse yarı gruptur. Birim elemanı ise $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ dır. O halde $M_2(\mathbb{R})$ matrisi çarpma işlemi ile bir monoid oluşturur. Ancak aşağıdaki örnekte görüleceği üzere sadeleştirme özelliğine sahip değildir.

$M_2(\mathbb{Z})$ matrisinde ise $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 5 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ ve $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 8 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ buradan

$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 5 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 8 \\ 0 & 0 \end{bmatrix}$ elde edilir.

$\begin{bmatrix} 0 & 5 \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & 8 \\ 0 & 0 \end{bmatrix}$ olduğundan $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ matrisi sadeleştirilemez.

Örnek 1.3.11. [118] n bir pozitif tam sayı ve $\mathbb{R}$ reel sayılar kümesi olsun. Girdileri reel sayı olan $n \times n$ lik matrisler kümesi $\mathbb{R}^{nxn}$ ile gösterilsin. O halde her $n \geq 1$ için $GL(n, \mathbb{R}) = \{A \in \mathbb{R}^{nxn} : detA \neq 0\}$ kümesi, matrislerde çarpma işlemine göre bir gruptur.

Matrislerde değişme özelliği olmadığından $GL(n, \mathbb{R})$ değişmeli olmayan bir gruptur. Bu gruba n. dereceden genel lineer grup denir.

Tanım 1.3.12. [113] G boş olmayan bir küme ve $(G, \cdot)$ bir grup olsun. $(G, \cdot)$ grubu sonlu sayıda elemana sahip ise $(G, \cdot)$ ikilisine bir sonlu grup denir, aksi halde sonsuz grup adı verilir. $(G, \cdot)$'nin elman sayısı yani kardinalitesine $(G, \cdot)$'nin mertebesi denir ve $o(G)$ veya $|G|$ ile gösterilir.

Tanım 1.3.13. [118] $(G,\cdot)$ bir grup olsun. Bir $a \in G$ elemanının kuvvetleri; $\forall\, k \in \mathbb{Z}^+$ için

- $a^0 = e$,
- $a^1 = a$,
- $a^{k+1} = a^k \cdot a$,
- $a^{-k} = (a^{-1})^k$ şeklinde tanımlanır.

Tanım 1.3.14. [118] $(G,+)$ bir toplamsal grup olsun. $a \in G$ elemanının tam sayı katları $\forall\, k \in \mathbb{Z}^+$ için,

- $0 \cdot a = 0$,
- $1 \cdot a = a$,
- $(k+1) \cdot a = k \cdot a + a$,
- $(-k) \cdot a = k \cdot (-a)$ şeklinde tanımlanır.

Not: Çalışmamız boyunca $(G,\cdot)$ grubu için sadece G ve $k \cdot a$ çarpımı içinde ka kısaltmaları kullanılacaktır.

Teorem 1.3.15. [118] G çarpımsal bir grup ve $a, b \in G$ olsun. O zaman $\forall\, m, n \in \mathbb{Z}^+$için

i) $a^m a^n = a^{m+n}$ (toplamsal gruplarda $ma + na = (m+n)a$) dir.

ii) $(a^m)^n = a^{m+n}$ (toplamsal gruplarda $m(na) = (mn)a$) dir.

iii) Eğer G bir değişmeli grup ise o zaman $(ab)^n = a^n b^n$ (toplamsal gruplarda $n(a+b) = na + nb$) dir.

İspat: $\forall a, b \in G$ ve $\forall\, m, n \in \mathbb{Z}^+$ için,

i) $a^m a^n = \underbrace{aa\ldots a}_{m\ tane}\underbrace{aa\ldots a}_{n\ tane} = \underbrace{aa\ldots a}_{m+n\ tane} = a^{m+n}$ olur

ii) $(a^m)^n = \underbrace{a^m a^m \ldots a^m}_{n\ tane} = \underbrace{\underbrace{aa\ldots a}_{m\ tane}\underbrace{aa\ldots a}_{m\ tane}\ldots\underbrace{aa\ldots a}_{m\ tane}}_{n\ tane} = \underbrace{aa\ldots a}_{m+n\ tane} = a^{m+n}$ olur.

iii) $n = 1$ için $(ab)^1 = a^1 b^1 = ab$

$n = k$ için $(ab)^k = a^k b^k$ olsun. O zaman

$n = k+1$ için

$$(ab)^{k+1} = (ab)^k(ab)^1 = (a^k b^k)(ab) = a^k(b^k a)b$$
$$= a^k(ab^k)b = (a^k a)(b^k b) = a^{k+1}b^{k+1}$$

olduğundan $(ab)^n = a^n b^n$ dir.

Tanım 1.3.16. [118] G bir grup ve $a \in G$ olsun. $a^n = e$ olacak şekilde bir en küçük n doğal sayısı varsa bu doğal sayıya a nın derecesi denir. $|a| = n$ ile gösterilir.

Eğer böyle bir n doğal sayısı mevcut değil ise o zaman $|a| = \infty$ gösterimi kullanılır.

Tanım 1.3.17. [118] $(G,*)$ ve (H,Δ) birer grup olsun. Eğer

i) $H \subseteq G$,

ii) $\forall\, a,b \in H \; için \; a \,\Delta\, b = a * b \; ise$

o zaman H'ya G'nin bir altgrubu denir ve $H \leq G$ ile gösterilir. Eğer $H \leq G$ ve $H \neq G$ şartları sağlanıyorsa H 'ye G'nin bir öz altgrubu denir ve $H < G$ şeklinde gösterilir.

Tanım 1.3.18. [118] G bir grup ve e ∈ G birim elemanı olmak üzere {e} altgrubuna G grubunun aşikâr altgrubu denir.

Tanım 1.3.19. [118] G bir grup ve $\emptyset \neq A \subseteq G$ olsun. Bu durumda

$$\langle A\rangle = \{a_1 a_2 \dots a_n : \forall\, 1 \leq i \leq n \; için \; a_i \in A \; veya \; a_i^{-1} \in A\}$$

kümesine A tarafından üretilen küme denir. Özel olarak $\emptyset$ tarafından üretilen küme

$$\langle \emptyset \rangle = \{e_G\}$$

ile gösterilir.

Tanım 1.3.20. [118] G bir grup ve $a_1, \dots, a_n \in G$ olsun. Eğer $G = \langle a_1, \dots, a_n\rangle$ ise o zaman $a_1, \dots, a_n$ elemanlarına G'nin üreteçleri denir.

Tanım 1.3.21. [118] G bir grup ve $a \in G$ olsun. G grubunun $H := \{a^n : n \in \mathbb{Z}\}$ altgrubuna G grubunun a elemanı tarafından üretilen devirli altgrubu denir. $G = \langle a\rangle$ şeklinde gösterilir.

Özel olarak $G = \langle a \rangle$ olacak şekilde bir $a \in G$ varsa o zaman G'ye a elemanı tarafından üretilen devirli grup denir.

Eğer G bir toplamsal grup ise o zaman $\langle a \rangle = \{na : n \in \mathbb{Z}\}$ ile gösterilir.

Örnek 1.3.22. $A = \{1, -1, i, -i\}$ çarpma işlemi ile bir grup olsun; Öyleyse

- $\langle 1 \rangle = \{1\}$,
- $\langle -1 \rangle = \{1, -1\}$,
- $\langle i \rangle = \{1, -1, i, -i\}$,
- $\langle -i \rangle = \{1, -1, i, -i\}$

ve $\langle i \rangle = \langle -i \rangle = A$ olur. Dolayısıyla A çarpma işlemi ile devirli bir gruptur.

Ayrıca $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}, \}$ $(n \geq 1)$ olmak üzere $\forall \bar{x}, \bar{y} \in \mathbb{Z}_n$ için $\bar{x} \oplus \bar{y} = \overline{x + y}$ işlemi altında $(\mathbb{Z}_n, \oplus)$ bir değişmeli gruptur. Bu grubun birimi ise $\bar{0}$ dır.

Örnek 1.3.23. **[**118] $G = \left\{ \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} : n \in \mathbb{Z} \right\}$ kümesi matrislerin bilinen çarpma işlemine göre bir grup belirtir. Ayrıca $G = \langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \rangle$ olduğundan G devirli bir gruptur.

Tanım 1.3.24. [118] G bir grup ve $a \in G$ olsun. Eğer $G = \langle a \rangle$ ise o zaman a elemanına G grubunun bir üreteci denir.

Teorem 1.3.25. [119] G bir grup ve $G = \langle a \rangle$ ise o zaman G grubunun bir diğer üreteci a^{-1} dır.

İspat: $|a| = n$ ve $a^n = e$ olsun. $(a^{-1})^n = (a^n)^{-1} = e^{-1} = e$ olur. Şimdi $k < n$ olsun.

$$(a^{-1})^k = e \rightarrow (a^k)^{-1} = e$$

$$\rightarrow a^k = e^{-1} = e$$

Bu durum $|a| = n$ olması durumu ile çelişir. O halde $|a^{-1}| = n$ yani

$$G = \langle a^{-1} \rangle$$

olur.

Teorem 1.3.26. [118] G bir grup ve $a \in G$ olsun. Eğer $\forall\, k \in \mathbb{Z}^+$ için $a^k \neq e$ ise o zaman $\langle a \rangle$ sonsuz bir gruptur.

İspat: $a^k = e$ olsun. O zaman

$$a^i = a^k$$

olacak şekilde bir $a^i = e$ vardır.

Öyleyse $a^i = a^k$ da eşitliğin her iki tarafı a^{-k} ile çarpılırsa

$$a^{i-k} = a^{k-k} = a^0 = e$$

elde edilir.

Burada $i - k > 0$ olduğundan $\langle a \rangle$ sonlu bir gruptur. Bu bir çelişki oluşturacağından $\langle a \rangle$ sonsuz bir gruptur.

Sonuç 1.3.27. [118] G bir grup ve $a \in G$ olsun. Eğer G sonlu ise $a^k = e$ olacak biçimde $k \in \mathbb{Z}^+$ vardır.

Bir grupta eğer $|a| = \infty$ ise

$$\langle a \rangle = \{\dots, a^{-3}, a^{-2}, a^{-1}, e, a^1, a^2, \dots\}.$$

Eğer $|a| = n$ sonlu ise o zaman a elemanının negatif kuvveti pozitif bir kuvvetine eşit olacağından dolayı

$$\langle a \rangle = \{e, a^1, a^2, \dots, a^{n-1}\}$$

olur.

Tanım 1.3.28. [118] G bir grup, $a \in G$ olsun. Eğer $\langle a \rangle$ sonlu devirli bir grup ise o zaman $\langle a \rangle$ altgrubunun eleman sayısına a nın mertebesi denir. $o(a)$ veya $|a|$ ile gösterilir.

Eğer $\langle a \rangle$ sonsuz bir grup ise o zaman da a elemanının mertebesi sonsuzdur denir.

Örnek 1.3.29. **[**118] $\mathbb{Z}_8$ toplamsal grubu için $\langle \bar{2} \rangle = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}\}$ altgrubunun mertebesi 4 olduğu için $o(\bar{2}) = 4$ olur.

Tanım 1.3.30. [145] G ve H birer yarı grup olsun. $\forall\, a, b \in G$ için

$$f(ab) = f(a)f(b)$$

sağlayan $f: G \longrightarrow H$ fonksiyonuna bir homomorfizma denir.

Eğer f bire-bir ise bir monomorfizm, örten ise bir epimorfizm, bire-bir ve örten ise bir izomorfizm denir.

$f: G \longrightarrow H$ bir izomorfizm ise $G \cong H$ ile gösterilir.

$f: G \longrightarrow G$ homomorfizmasına bir endomorfizm denir. Bu durumda, f bire-bir örten olursa f ye otomorfizm denir.

Tanım 1.3.31. [145] G ve H birer grup olsun. $\forall\, a, b \in G$ için

$$f(ab) = f(a)f(b)$$

koşulunu sağlayan $f: G \longrightarrow H$ fonksiyonuna bir grup homomorfizma denir. Bu durumda f fonksiyonu için aşağıdaki özellikler sağlanır:

i. $f(e_G) = e_H$
ii. $f(a^{-1}) = (f(a))^{-1}$.

1.4. Halka Teorisi

Tanım 1.4.1. [118] $(G,+)$ değişmeli bir grup ve G üzerinde "$\cdot$" çarpma işlemi tanımlı olsun. Bu durumda G grubu çarpma işleminin birleşme özelliğine sahip ve G grubunda çarpma işlemi toplama işlemi üzerine soldan ve sağdan dağılma özelliğine sahip ise $(G,+,\cdot)$ üçlüsüne bir halka denir.

$\forall\, x \in G$ için $e \cdot x = x \cdot e$ olacak şekilde bir $e \in G$ var ise G halkasına birimli halka denir.

$\forall\, x, y \in G$ için $y \cdot x = x \cdot y$ ise G halkasına değişmeli halka denir.

Tanım 1.4.2. [118] $(G,+,\cdot)$ bir halka olsun.

$$C(G) = \{a \in R \mid \forall\, b \in G \; için \; ab = ba\}$$

kümesine halkanın merkezi adı verilir. Burada

$$C(G) = G$$

özelliğini sağlanıyor ise, $(G,+,\cdot)$ halkası değişmeli halkadır.

Örnek 1.4.3. [123] $\mathbb{Z}$ tam sayılar kümesi, $\mathbb{Q}$ rasyonel sayılar kümesi, $\mathbb{R}$ reel sayılar kümesi ve $\mathbb{C}$ karmaşık sayılar kümesi bilinen toplama ve çarpma işlemlerine göre birer birimli ve değişmeli halkadır.

Örnek 1.4.4. [123] Bilinen matris toplaması ve matris çarpması işlemlerine göre 2×2 tipindeki reel matrislerin kümesi bir halkadır.

Teorem 1.4.5. [118] G bir halka olsun. $\forall\, a \in G$ için

$$0_R \times a \;=\; a \times 0_R \;=\; 0_R \text{ dır.}$$

İspat: $0_R + 0_R = 0_R$ olduğundan

$$a \times 0_R + a \times 0_R = a \times (0_R + 0_R) = a \times 0_R$$

olur. Bunun sonucunda

$$(a \times 0_R + a \times 0_R) + (-a \times 0_R) = a \times 0_R + (-a \times 0_R) = 0_R$$

olur. Öyleyse

$$a \times 0_R + 0_R = 0_R$$

ve buradan

$$a \times 0_R = 0_R$$

elde edilir.

Benzer şekilde

$$0_R \times a + 0_R \times a = (0_R + 0_R) \times a = 0_R \times a$$

olur.

$(0_R \times a + 0_R \times a) + (0_R \times (-a)) = 0_R \times a + (0_R \times (-a)) = 0_R\big(a + (-a)\big) = 0_R$

öyleyse

$$0_R \times a + 0_R = 0_R$$

elde edilir ve buradan

$$0_R \times a = 0_R$$

sonucu elde edilir.

Teorem 1.4.6. [118] G bir halka ve $\forall\, x, y, z \in G$ olmak üzere

i. $(-x)y = -(xy)$
ii. $x(-y) = -(xy)$
iii. $(-x)(-y) = xy$
iv. $x(y - z) = xy - xz$
v. $(x - y)z = xz - yz$

özellikleri sağlanır.

Tanım 1.4.7. [118] G bir halka ve $\emptyset \neq S \subseteq G$ olsun. Eğer S kümesi G'nin işlemlerine göre halka şartlarını sağlarsa S'ye G'nin bir alt halkası adı verilir.

Uyarı 1.4.8. [118] Değişmeli bir halkanın her alt halkası değişmelidir fakat birimli bir halkanın bir alt halkası birimli olmak zorunda değildir.

Ayrıca $a \times b$ bilinen çarpma işlemi ab ile ifade edilecektir.

Örnek 1.4.9. [118] G bir halka olmak üzere $\{0\}$ ve G kümeleri G'nin alt halkalarıdır.

Örnek 1.4.10. [118] $n \in \mathbb{Z}$ olmak üzere $nZ = \{nx | x \in \mathbb{Z}\}$ kümesi $\mathbb{Z}$'nin bir alt halkasıdır. Tek tam sayılar kümesi toplamaya göre kapalı olmadığından $\mathbb{Z}$'nin bir alt halkası değildir.

Teorem 1.4.11 [118] G bir halka olsun. $\emptyset \neq S \subseteq G$ alt kümesinin G'nin bir alt halkasıdır ancak ve ancak $\forall\, x, y \in S$ için $x - y, xy \in S$ olmasıdır.

Örnek 1.4.12. [118] $M_2(\mathbb{Z})$ nin boş kümeden farklı $S = \left\{ \begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix} : x, y \in \mathbb{Z} \right\}$ alt kümesi ve $\forall \begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix}, \begin{bmatrix} z & 0 \\ 0 & t \end{bmatrix} \in S$ için,

i. $\begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix} - \begin{bmatrix} z & 0 \\ 0 & t \end{bmatrix} = \begin{bmatrix} x - z & 0 \\ 0 & y - t \end{bmatrix} \in S$

ii. $\begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix} \begin{bmatrix} z & 0 \\ 0 & t \end{bmatrix} = \begin{bmatrix} xz & 0 \\ 0 & yt \end{bmatrix} \in S$

ise S kümesi $M_2(\mathbb{Z})$'nin bir alt halkasıdır.

1.5. Cisim Teorisi

Tanım 1.5.1. [123] $F \neq \emptyset$ kümesi üzerinde $(+)$ toplama ve $(\times)$ çarpma ikili işlemleri tanımlansın. $(+)$ işleminin birim elemanını 0_F ile gösterilsin. Eğer aşağıdaki şartlar sağlanıyorsa $(F, +, \times)$ cebirsel yapısına bir cisim denir.

i. $(F, +)$ bir değişmeli gruptur,
ii. $(F/0_F, \times)$ bir değişmeli gruptur,
iii. $(\times)$ işleminin $(+)$ üzerine dağılma özelliği vardır.

Örnek 1.5.2. Toplama ve çarpma işlemlerine göre $\mathbb{Q}, \mathbb{R}$ ve $\mathbb{C}$ kümeleri birer cisimdir.

Tanım 1.5.3. [123] Sonlu cisim sonlu sayıda elemana sahip bir cisimdir. Sonlu cismin düzenini belirleyen sahip olduğu eleman sayısıdır. Eleman sayısı eşit olan tüm sonlu cisimler eş yapılıdır ve aynı matematiksel yapıyı gösterirler yani yalnızca elemanlarının gösteriş biçiminde farklılıklar vardır.

Tanım 1.5.4. [118] F bir cisim ve E kümesi F'nin bir alt halkası olsun. Eğer E kümesi e F cisminin işlemlerine göre bir cisim oluyorsa E kümesine F'nin bir alt cismi denir.

Örnek 1.5.5. $\mathbb{Q}$, $\mathbb{R}$'nin alt cismi ve $\mathbb{R}$ de $\mathbb{C}$'nin alt cismidir.

Teorem 1.5.6. [118] F bir cisim ve $\emptyset \neq E \subseteq F$ olsun. E kümesine F cisminin bir alt cismidir ancak ve ancak aşağıdaki üç koşul sağlanıyorsa;

i. $|E| \geq 2$.
ii. $\forall\, a, b \in E$ için $a - b,\ ab \in E$ olmalıdır.
iii. Sıfırdan farklı $\forall\, c \in E$ için $c^{-1} \in E$ dir.

Tanım 1.5.7. [123] p bir asal sayı olsun. p sayıda elemana sahip bir küme

$$Z_p = \{0,1,2, \dots, p-1\}$$

üzerinde $mod\, p$ toplama ve $mod\, p$ çarpma işlemlerinin tanımlanmasıyla, p sayıda elemana sahip bir sonlu cisim elde edilir. Bu sonlu cisim $GF(p)$ olarak adlandırılır.

Burada p , $GF(p)$ 'nin karakteristiği adını alırken $GF(p)$ de Galois cismi olarak adlandırılır.

Tanım 1.5.8. [123] $GF(p)$ bir Galois cismi olmak üzere, $q = p^n$ elemanlı bir $GF(p^n)$ cismi oluşturulsun. Bu cisme $GF(p)$'nin p karakteristiğine sahip genişletilmiş cismi denir.

Tanım 1.5.9. [123] Galois cisimlerinde karakteristiğin $p = 2$ alınması sonucunda elde edilen $GF(2^n)$ cismine ikili sonlu cisim denir. $GF(2^n)$ cisminin elemanları, $\{0,1\}$ bitlerinin kombinasyonları ile gösterilir.

Örneğin dört bitlik sistemde onluk sayı sisteminin rakamlarını ifade etmek için, 0000, 0001, 0010, 0011, 0100, 0101, 0110, 0111, 1000, 1001 kullanılmaktadır. Görüldüğü üzere bu gösterim $\{0 = (0000)_2,\ 1 = (0001)_2, 2 = (0010)_2, 3 = (0011)_2, 4 = (0100)_2, 5 = (0101)_2, 6 = (0110)_2, 7 = (0111)_2, 8 = (1000)_2, 9 = (1001)_2\}$ onluk taban sistemindeki bir rakamın ikilik taban sistemindeki karşılıklarını ifade etmektedir.

Bu kullanım $GF(2^n)$ üzerinde tanımlanan matematiksel işlemlerin sonuçlandırılmasını oldukça kolaylaştırmaktadır. Bu nedenle hem yazılım ve donanım uygulamalarında hem de kriptografik algoritmalarında yaygın olarak $GF(2^n)$ kullanılmaktadır. Bu tip cisimlerin, ikili sonlu cisimler olarak adlandırılmasının nedeni $GF(2^n)$ Galois cisminin elemanlarının yan yana yazılmış bitler, yani $\{0,1\}$ ile gösterilebilmesinden kaynaklanmaktadır.

Ayrıca hata düzelten kodların tasarımında ve kriptografide $GF(2^n)$ üzerinde oluşturulan polinomlar ve bu polinomlar arasındaki matematiksel işlemler büyük önem taşımaktadır.

Tanım 1.5.10. [123] Aynı cismin iki elemanının toplanması ya da çıkarılması işlemi standart polinomların toplama ve çıkarma işlemi gibidir.

Sonlu cisim aritmetiğinde cismin elemanları $\{0,1\}$ katsayılarına sahip polinomlar olarak temsil edilebildiğinden toplama işlemi katsayılarının basitçe $(mod\ 2)$ aritmetiğine göre toplanır. Bu toplama Bole cebrinde xor toplamı da denir. Bu işlem aşağıdaki dört durumdan birini sonuçlandırır.

i. $0\ xor\ 0 = 0,$
ii. $0\ xor\ 1 = 1,$

iii. $1\ xor\ 0 = 1,$

iv. $1\ xor\ 1 = 0.$

xor işlemi bir yönüyle ikilik taban sistemindeki sayıların toplama işleminden farklıdır. Örneğin ikilik taban sisteminde $3 + 6$ toplama işlemi aşağıdaki şekilde yapılırken

$$3+6 = (0011)_2 + (0110)_2 = (1001)_2 = 9$$

bu iki sayıya xor işlemi uygulandığında ise,

$$(0011)\ xor\ (0110) = (0101)$$

onluk sayı tabanında 5 sayısına karşılık gelen sonuca ulaşılır.

Örnek 1.5.11. $a = (1000111)$ ve $b = (1110101)$ olsun. O zaman

$$a\ xor\ b\ =\ 0110010$$

olarak elde edilir. Polinomsal olarak göstermek gerekirse

$$a = x^6 + x^2 + x^1 + 1$$

ve

$$b = x^6 + x^5 + x^4 + x^2 + 1$$

olur. Burada iki adet x^6 toplamında katsayıları 1 olduğundan $1\ xor\ 1 = 0$ elde edilir. Bunun sonucunda x^6 teriminin katsayısı sıfır olacaktır. Dolayısıyla

$$a + b = x^5 + x^4 + x^1$$

elde edilir.

Ancak $a = (1000111)_2$ ve $b = (1110101)_2$ ikilik taban sistemindeki iki sayının toplamı olarak,

$$a + b = (1000111)_2 + (1110101)_2 = (11111100)_2$$

elde edilirdi. Bu sonucun temsil ettiği polinomda

$$a + b = x^7 + x^6 + x^5 + x^4 + x^3 + x^2$$

olur.

Tanım 1.5.12. [123] Sonlu cisim aritmetiğinde çarpma işlemi, polinomların birbirleri ile aritmetik çarpımı şeklindedir. Ancak çarpma sonucunda sonlu cismin derecesinden daha yüksek dereceli elemanlar elde edilebilir. Dolayısıyla bu elemanları sonlu cismin derecesinden küçük olacak biçimde cismi oluşturan indirgenemez polinom aracılığı ile indirgemek gerekir. O halde bu işleme indirgenemez polinoma göre indirgeme (mod alma) işlemi denir.

Örnek 1.5.13. [123] $a = 1011$ ve $b = 0111$ ve indirgenemez polinom olarak

$$x^4 + x^1 + 1$$

seçilsin. Bu durumda,

$$\begin{aligned} a \cdot b &= (x^4 + x + 1) \cdot (x^2 + x^1 + 1) && , x^1 = x \\ &= x^6 + x^5 + x^4 + x^3 + x^2 + x + x^2 + x + 1 && \vdots \\ &= x^6 + x^5 + x^4 + x^3 + 1 && , x^4 = x + 1 \\ &= x^3 + x^2 + x^2 + x + x + 1 + x^3 + 1 && , x^5 = x^2 + x \\ &= 0 && , x^6 = x^3 + x^2 \end{aligned}$$

elde edilecektir.

Tanım 1.5.14. [123] n bitlik iki polinomun çarpımının kalanı seçilen indirgenemez polinoma göre 1'e eşit ise o zaman bu iki polinom birbirinin seçilmiş indirgenemez polinoma göre tersidir denir.

$$a \in GF(2^n) \text{ ve } a = \beta^i$$

olmak üzere a elemanının çarpma işlemine göre tersi,

$$a^{-1} = \beta^{(-i) mod (2^n - 1)}$$

dir.

$GF(2^n)$ de indirgenemez bir polinomun tersini bulmak için tablo oluşturmak da mümkündür. Bu tablo aşağıda Tablo 1.1. de verildiği gibidir.

Tablo 1.1. $GF(2^4)$ için elemanların tersi ve polinom gösterimi

β^0	(0001)	1	Tersi	β^{15}	(0001)	1
β^1	(0011)	$x+1$	Tersi	β^{14}	(1010)	x^3+x
β^2	(0101)	x^2+1	Tersi	β^{13}	(0110)	x^2+x
β^3	(1111)	x^3+x^2+x+1	Tersi	β^{12}	(0010)	x
β^4	(1110)	x^3+x^2+x	Tersi	β^{11}	(1011)	x^3+x+1
β^5	(1101)	x^3+x^2+1	Tersi	β^{10}	(1100)	x^3+x^2
β^6	(1000)	x^3	Tersi	β^9	(0100)	x^2
β^7	(0111)	x^2+x+1	Tersi	β^8	(1001)	x^3+1
β^8	(1001)	x^3+1	Tersi	β^7	(0111)	x^2+x+1
β^9	(0100)	x^2	Tersi	β^6	(1000)	x^3
β^{10}	(1100)	x^3+x^2	Tersi	β^5	(1101)	x^3+x^2+1
β^{11}	(1011)	x^3+x+1	Tersi	β^4	(1110)	x^3+x^2+x
β^{12}	(0010)	x	Tersi	β^3	(1111)	x^3+x^2+x+1
β^{13}	(0110)	x^2+x	Tersi	β^2	(0101)	x^2+1
β^{14}	(1010)	x^3+x	Tersi	β^1	(0011)	$x+1$
β^{15}	(0001)	1	Tersi	β^0	(0001)	1

Tanım 1.5.15. [123] $GF(2)$ cismi üzerinde oluşturulan n. dereceden $p(x)$ polinomu n' den daha küçük dereceli polinomlara bölünemiyor ise $p(x)$ polinomuna $GF(2)$ üzerinde indirgenemez denir.

Tanım 1.5.16. [123] $GF(2)$ üzerinde indirgenemez bir $p(x)$ polinomunun böldüğü x^n+1 polinomu için $n=2m-1$ ise $p(x)$ ilkel bir polinomdur.

Teorem 1.5.17. [123] $f(x), GF(2)$ üzerinde tanımlı bir polinom ve $\beta \in GF(2^m)$ olmak üzere, eğer $f(x)$ polinumunun bir kökü β ise o zaman $i \geq 0$ için β^{2^i} de $f(x)$ polinomunun bir köküdür.

Tanım 1.5.18. [123] Eğer $F(x)$ polinomu, $F(\beta) = 0$ koşulunu sağlayan minimum dereceli polinom ise o zaman $F(x)$'e, β'nın minimal polinomu denir.

Tablo 1.2. $GF(2^4)$ nin elemanlarının minimal polinomları

Eleman	Minimal Polinom
0	x
1	$x+1$
$\alpha^1, \alpha^2, \alpha^4, \alpha^8$	$x^4 + x + 1$
$\alpha^3, \alpha^6, \alpha^9, \alpha^{12}$	$x^4 + x^3 + x^2 + x + 1$
α^5, α^{10}	$x^2 + x + 1$
$\alpha^7, \alpha^{11}, \alpha^{13}, \alpha^{14}$	$x^4 + x^3 + x + 1$

1.6. Sayılar Teorisi

Tanım 1.6.1. [123] Eğer $\forall\, x, y \in \mathbb{Z}$ için $x = y \cdot m$ olacak şekilde bir $m \in \mathbb{Z}$ sayısı varsa y sayısı x sayısını böler denir ve $y|x$ ile gösterilir.

Örnek 1.6.2 $140 = 7 \cdot 20$ olduğundan $7|140$ olur.

Lemma 1.6.3. [123] $\forall\, x, y, z \in \mathbb{Z}$ için aşağıdakiler sağlanır.

i. $x|x$ (Her tam sayı kendisini böler.)
ii. $x|y$ ve $y|z$ ise $x|z$ olur.
iii. Eğer $x|y$ ve $x|z$ ise, $\forall a, b \in \mathbb{Z}$ için $x|(ay + bz)$ olur.
iv. Eğer $x|y$ ve $y|x$ ise $x = \mp y$ olur.

Tanım 1.6.4. (Bölme algoritması) [123] x ve y tam sayıları $y \geq 1$ koşulunu sağlaması şartıyla, x tam sayısının y tam sayısına bölümü q tam sayısı gibi bir bölüm ve r tam sayısı gibi bir kalan verir. Bu işlem aşağıda gösterildiği gibidir.

$$x = qy + r, \;\; 0 \leq r < y$$

burada q ve r tektir. Bu bölme işlemi

$$x = r \; (mod\; y)$$

ile de ifade edilebilir.

Tanım 1.6.5. [123] x ve y sıfırdan farklı birer tam sayı olsun. x ve y tam sayılarının en büyük ortak böleni, hem x sayısını hem de y tam sayısını bölen en büyük m tam sayısıdır. Kısaca $gcd(x, y) = m$ ile gösterilir.

Teorem 1.6.6. [123] x ve y tam sayılarının her ikisi de birlikte sıfır olmayacak şekilde alınsınlar, $gcd(x, y) = ax + by$ eşitliğini sağlayan a ve b tam sayılar her zaman vardır.

Tanım 1.6.7. [123] Bir ve kendisinden başka hiçbir böleni olmayan birden büyük pozitif tam sayılara asal sayı denir.

Örnek 1.6.8. $\{2,3,5,7,11,13,17,19\}$ kümesinin her bir elemanı bir asal sayıdır.

Tanım 1.6.9. [123] $\forall\, x, y \in \mathbb{Z}^+$ sayıları için $gcd(x, y) = 1$ ise, bu iki sayıya aralarında asal sayılardır denir. $gcd(x, y) = 1$ yerine kısaca $(x, y) = 1$ yazılabilir.

Ayrıca $1 = ax + by$ olacak şekilde a ve b tam sayılar her zaman vardır.

Tanım 1.6.10. (Aritmetiğin esas teoremi) [123] $2 \leq n \in \mathbb{Z}$ şartının sağlayan her n pozitif tam sayısı, asal sayıların çarpımları şeklinde tek olarak yazılır.

Yani, $e_1, e_2, \dots, e_k \in \mathbb{Z}^+$ ve birbirinden farklı $p_1, p_2, \dots, p_k$ birer asal sayı olsun. O zaman

$$n = {p_1}^{e_1}, {p_2}^{e_2}, \dots, {p_k}^{e_k}$$

elde edilir.

Örnek 1.6.11. $3000 = 2^3 3^1 5^3$.

Teorem 1.6.12 [145] $G = \langle a \rangle$ ve $|G| = n$ verilsin. $b \in G$, $a^s = b$ ve $(n, s) = d$ olsun. Öyleyse $H = \langle b \rangle$ için

$$|H| = n/d$$

olur.

Teorem 1.6.13. (Fermat Teoremi**)** [145] $n \in \mathbb{Z}$ bir tam sayı ve $p \in \mathbb{N}$ bir asal sayı olsun;

$$\begin{aligned} p \nmid a &\Longrightarrow p | a^{p-1} - 1 \\ &\Longrightarrow a^{p-1} \equiv 1 \ (mod\ p) \\ &\Longrightarrow a^p \equiv a \ (mod\ p). \end{aligned}$$

Teorem 1.6.14. (Euler teoremi**)** [145] Bir a pozitif tam sayısı ve n doğal sayısı için;

$$\begin{aligned} (a, n) = 1 &\Longrightarrow n | a^{\Phi(n)} - 1 \\ &\Longrightarrow n | a^{\Phi(n)} \equiv 1 (mod\ n) \end{aligned}$$

Tanım 1.6.15. (Euler Φ fonksiyonu**)** [145] Herhangi bir $n \in \mathbb{Z}^+$ için $1 \leq a \leq n$ ve $(a, n) = 1$ için $a \in \mathbb{Z}$ sayılarının sayısına Euler Φ fonksiyonu denir. Φ(n) ile gösterilir.

Euler Φ fonksiyonunun özellikleri aşağıda verildiği gibidir [145]:

$p \in \mathbb{Z}$ bir asal sayı olsun. Öyleyse Euler Φ fonksiyonu aşağıdaki özellikleri sağlar;

E₁ : $\Phi(\mathrm{p}) = \mathrm{p} - 1 = \mathrm{p}\left(1 - \frac{1}{p}\right)$,

E₂ : $r \in \mathbb{N}$ için $\Phi(\mathrm{p}^r) = \mathrm{p}^r - \mathrm{p}^{r-1} = \mathrm{p}^r\left(1 - \frac{1}{p}\right)$,

E₃ : $(m, n) = 1 \Longrightarrow \Phi(\mathrm{mn}) = \Phi(\mathrm{m})\Phi(\mathrm{n})$,

E₄ : $m = p_1^{r_1} p_2^{r_2} p_3^{r_3} \dots p_k^{r_k}$, öyle ki p_i ler asal sayı ve $r_i \in \mathbb{Z}^+$, $1 \leq i \leq k$, ise

$$\Phi(\mathrm{m}) = \Phi\left(p_1^{r_1} p_2^{r_2} p_3^{r_3} \dots p_k^{r_k}\right)$$

$$= \Phi\left(p_1^{r_1}\right)\Phi\left(p_2^{r_2}\right)\Phi\left(p_3^{r_3}\right) \dots \Phi\left(p_k^{r_k}\right)$$

$$= p_1^{r_1} p_2^{r_2} p_3^{r_3} \dots p_k^{r_k}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\left(1 - \frac{1}{p_3}\right) \dots \left(1 - \frac{1}{p_k}\right)$$

$$= m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\left(1 - \frac{1}{p_3}\right) \dots \left(1 - \frac{1}{p_k}\right).$$

1.7. Esnek Cebirsel Yapılar

Tanım 1.7.1. [133] U evrensel küme ve E parametre kümesi olsun. $F,\ E$ Kümesinden U kümesinin kuvvet kümelerine tanımlı bir dönüşüm olmak üzere (F,E) ikilisine U üzerinde esnek küme denir.

Tanım 1.7.2 [132] U üzerinde $A,B,C \in E$ ve $\mathrm{F},G,H \in U$ olmak üzere (F,E) ve (G,B) esnek kümelerinin birleşimi (H,C) şeklinde tanımlanır.
Burada $C = A \cup B$ ve $e \in C$ için $H(e)$ aşağıdaki şekilde tanımlanır;

$$H(e) = \begin{cases} F(e), & e \in A - B\ ise, \\ G(e), & e \in B - A\ ise, \\ F(e) \cup G(e), & e \in A \cap B\ ise, \end{cases}$$

ancak

$$(F,A)\ \tilde{\cup}\ (G,B) = (H,C)$$

biçiminde gösterilir.

Tanım 1.7.3 [132] U üzerinde $A,B,C \in E$ ve $\mathrm{F},G,H \in U$ olmak üzere (F,A) ve (G,B) esnek kümelerinin kesişimi (H,C) şeklinde tanımlanır. Burada $C = A \cap B$ ve $e \in C$ için $H(e)$ şu şekilde tanımlanır;

$$H(e) = \begin{cases} F(e) \\ G(e) \end{cases}$$

ancak

$$(F,A)\ \tilde{\cap}\ (G,B) = (H,C)$$

biçiminde gösterilir.

Tanım 1.7.4 [134] (F,A) kümesi G üzerinde bir esnek küme olmak ve $\forall\ x \in A$ için

$$F(x) < G$$

ise (F,A) kümesine G üzerinde bir esnek grup denir.

Örnek 1.7.5. [135] $G = A = S_3 = \{e, (12), (13), (23), (123), (132)\}$ ve

$F: S_3 \to S_3$ fonksiyonunun değer kümesi

$$F(x) = \{y \in G: xRy \leftrightarrow y = x^n, n \in N\}$$

olarak tanımlansın. (F, A) kümesinin alt kümeleri

$$F(x): x \in A$$

şeklinde parametrize edilir. Burada;

$$F(e) = \{e\}, F(12) = \{e, (12)\}, F(13) = \{e, (13)\},$$

$$F(23) = \{e, (23)\}, F(123) = F(132) = \{e, (123), (132)\}$$

elde edilir.

Tanım 1.7.6 [132] G bir esnek grup olsun. Eğer $\forall\, x \in A$ ve birim eleman $e \in G$ olmak üzere,

$$F(x) = \{e\}$$

ise (F, A)'ya G'de birim esnek grup denir.

Tanım 1. 7.7 [132] G bir esnek grup olsun. $\forall\, x \in A$ için

$$F(x) = G$$

ise (F, A)'ya G'de mutlak esnek grup denir.

Tanım 1.7.8 [132] (F, A) ve (H, K) kümeleri G üzerinde iki esnek grup olsun. Aşağıdaki iki koşulu sağlayan (H, K)'ya (F, A)'nin esnek bir alt grubudur denir.

$$(H, K) \cong (F, A)$$

şeklinde yazılır ve aşağıdaki iki özelliği sağlar;

i. $K \subset A$,

ii. $H(x)$, $F(x)$'nin esnek alt grubudur, $\forall\, x \in K$ *için*.

Tanım 1.7.9 [132] (F, A) ve (H, B) sırasıyla G ve K üzerinde iki esnek grup olsun, $f: G \to K$ ve $g: A \to B$ iki fonksiyon olsun. Öyleyse aşağıda belirtilen koşulların yerine getirilmesi durumunda (f, g) ikilisine esnek homomorfizm denir.

i. $f: G \to K$ bir homomorfizmdir,
ii. g, A ile B arasındaki bir eşlemedir,
iii. $f\big(F(x)\big) = H\big(g(x)\big),\ \forall\, x \in A$ için.

Burada (F, A), (H, B)'ye esnek homomorfiktir denir ve

$$(F, A) \sim (H, B)$$

şeklinde gösterilir.

Tanım 1.7.10. [132] (F, A) ve (H, B) sırasıyla G ve K üzerinde iki esnek grup olsun. (F, A) ve (H, B) esnek gruplarının çarpımı $\forall\, (x, y) \in A \times B$ için

$$U(x, y) = F(x) \times H(y)$$

iken

$$(F, A) \times (H, B) = (U, A \times B)$$

şeklinde tanımlanır.

Tanım 1.7.11. [136] Eğer $F: A \to U$ bir örten fonksiyon ise (F, A) ikilisine U üzerinde örten esnek küme denir.

Bundan sonra, G bir esnek grubu belirtirken, (F, A) esnek kümesi de örten esnek küme olacaktır. $F(a)$ elemanı ise (F, A) esnek kümesinin $(a, F\,(a))$ elemanının yerine kullanılacaktır.

Tanım 1.7.12. [136] (F, A), G üzerinde bir esnek küme ve $\forall\, x \in A$ için $F(x) \in (F, A)$ olsun. O halde

$$F(x)^n = \{a^n : a \in F(x), n \in \mathbb{Z}\}$$

$F(x)$'in n – kuvveti olarak adlandırılır.

Teorem 1.7.13. [136] $(F,A),G$ üzerinde bir esnek küme olsun. $x,y \in A$ için, $F(x),F(y) \in (F,A)$ olsun. Ardından, $her\ n \in \mathbb{Z}$ için,

i. $(F(x) \cap F(y))^n \subseteq F(x)^n \cap F(y)^n, \quad her\ n \in \mathbb{Z}\ için,$

ii. $(F(x) \cup F(y))^n = F(x)^n \cup F(y)^n, \quad her\ n \in \mathbb{Z}\ için,$

iii. $(F(x) \times F(y))^n = F(x)^n \times F(y)^n, \quad her\ n \in \mathbb{Z}\ için.$

Tanım 1.7.14. [136] $(F,A),G$ üzerinde bir esnek küme ve $F\ (x) \in (F,A)$ olsun. Eğer $F(x)n = \{e\}$ olacak şekilde bir n pozitif tam sayı varsa, o zaman en küçük pozitif n tam sayısına $F(x)$'in mertebesi olarak adlandırılır.

Eğer böyle bir n yoksa $F(x)$ sonsuz mertebeye sahip olur. $F(x)$'in mertebesi $|F(x)|$ ile gösterilir.

Teorem 1.7.15. [136] G sonlu bir grup ve (F,A), G üzerinde esnek bir grup olsun. Öyleyse, (F,A)'nın elemanlarının mertebeleri de sonludur.

Teorem 1.7.16. [136] $(F,A),G$ sonlu grubu üzerinde bir esnek küme ve $\forall\ x \in A$ için $F(x) \in (F,A)$ olsun. Öyleyse, $F(x)$'in mertebesi, $F(x)$ elemanlarının mertebelerinin en küçük katıdır.

Teorem 1.7.17. [136] Gsonlu bir grup, $(F,A)\ da\ G$ üzerinde esnek bir grup ve $F\ (x)$, $F(y)$ de (F,A)'nın elemanları olsun. Öyleyse, $\forall\ x,y \in A$ için, aşağıdaki üç koşul sağlanır:

i. $|F(x) \cap F(y)| \leq OBEB(|F(x)|,|F(y)|) \quad \forall\ x,y \in A\ için,$

ii. $|F(x) \cup F(y)| = OKEK(|F(x)|,|F(y)|) \quad \forall\ x,y \in A\ için,$

iii. $|F(x) \times F(y)| = |F(x)||F(y)| \quad \forall\ x,y \in A\ için.$

Tanım 1.7.18. [136] G bir grup ve (F,A) da G üzerinde bir esnek küme olsun. Öyleyse

$$(F,A)^n = \{F(x)^n : x \in A, n \in \mathbb{Z}\}$$

F kümesine n. kuvvette esnek küme denir.

Teorem 1.7.19. [136] $(F,A)\ ve\ (E,B), G$ üzerinde iki esnek küme olsun. O halde,

i. $((F,A) \vee (E,B))^n = (F,A)^n \vee (E,B)^n$,

ii. $Eğer\ A \subseteq B\ ve\ \forall a \in A$,

ise $F(a)$ ve $E(a)$ özdeş yaklaşımlardır ve

$$((F,A)\ \wedge\ (E,B))^n \subseteq (F,A)^n \wedge (E,B)^n$$

dır.

Teorem 1.7.20. [136] $(F,A), G$ sonlu grubu üzerinde tanım bir esnek grup ve $F(x) \in (F,A)$ olsun. Öyleyse aşağıdakiler sağlanır.

i. $F(x)$'in mertebesi (F,A)'nın mertebesini böler. Özellikle, $F(x)^{|(F,A)|} = \{e\}$.

ii. (F,A)'nın mertebesi G'nin mertebesini böler.

Teorem 1.7.21. [136] G sonlu bir grup olsun. $(F,A)\ ve\ (E,B)\ ise\ G$ üzerinde iki esnek grup olsun. Öyleyse;

$$|(F,A) \wedge (E,B)| \leq |F,A| ve\ |(F,A) \wedge (E,B)| \leq |E,B|$$

elde edilir.

Tanım 1.7.22. [137] $*$ işlemi altındaki bir G grubuna, $G = \{an: n \in \mathbb{Z}\} = \langle a \rangle$, devirli grup, a elemanına da devirli grubun üreteci denir.

$*$ çarpma işlemi ise,

$$\langle a \rangle = \{a^n : n\ \in \mathbb{Z}\}$$

$*$ toplama işlemi ise o zaman

$$\langle a \rangle = \{na : n\ \in \mathbb{Z}\}$$

olur.

Örnek 1.7.23. [137] $G = \{1, -1, i, -i\}$, üreteçleri $i, -i$ ile çarpma işlemi altında devirli bir gruptur.

Örnek 1.7.24. [137] $\mathbb{Z}$, üreteçleri $-1,1$ olan sonsuz bir devirli gruptur. Özellikle, G grubunun mertebesi $o(G) = n$ dir.

Bu örnekte G devirli grubunun üreteçleri sayısı, $\varphi(n)$'dir. $\varphi(n), n$'den daha küçük olan ve n ile aralarında asal olan pozitif tam sayıların sayısı olarak tanımlanan Euler totient fonksiyonudur. Dolayısıyla eğer n bir asal sayı olursa, G devirli grubunun tüm elemanları birer üreteç olurlar.

Tanım 1.7.25. [136] G bir grup ve $(F, A), G$ üzerinde bir esnek grup, X ise $P(G)$'nin bir elemanı olsun.

$$\{(a, \langle x \rangle) : F(a) = \langle x \rangle, \qquad x \in X\}$$

kümesine, (F, A)'nın bir esnek alt kümesi denir ve $\langle X \rangle$ ile gösterilir.

Eğer $(F, A) = \langle X \rangle \, ise, (F, A)$ esnek grubuna X tarafından üretilen devirli esnek grup denir.

Sonuç 1.7.26. [136] Eğer G bir devirli esnek grup ise o zaman (F, A) grubu G üzerinde devirli bir esnek gruptur, dolayısıyla tüm devirli grupların alt grupları da devirlidir. Ancak bunun tersi her zaman doğru değildir.

Örnek 1.7.27. [136] $G = S_3$ simetrik grup ve $A = \{e, (12), (13), (23), (123)\}$ parametre kümesi olsun. Eğer G üzerine (F, A) esnek kümesi, $\forall\, x \in A$ için

$$F(x) = \{y \in G : y = xn, \qquad n \in \mathbb{Z}\}$$

şeklinde inşa edilirse, G devirli grup olmasa bile (F, A)'ya G üzerinde esnek devirli grup denir.

Teorem 1.7.28. [136] G grubu için aşağıdaki özellikler sağlanır.

Eğer (F, A), X tarafından üretilen sonlu bir devirli esnek grup ve
$|F, A| = OKEK(|x_i|)$, burada $x_i \in X$ ise,

i. (F, A), X tarafından üretilen sonsuz bir sonsuz devirli grup ise, $|(F, A)| = |X|$.

ii. (F, A) bir birim esnek grubu ise, $\{e\}$ tarafından üretilen devirli esnek gruptur.

iii. $(F, A), G$'de tanımlanan bir mutlak esnek grup olsun. (F, A), bir devirli esnek gruptur ancak ve ancak G devirli bir grup ise.

iv. $(F, A), G$ üzerinde esnek bir grup olsun. G'nin mertebesi asal ise, (F, A) devirli esnek bir gruptur.

v. Devirli esnek bir grubun esnek bir alt grubu da devirli esnek bir gruptur.

Teorem 1.7.29. [136] $(F, A), G$ grubu üzerinde ve (H, B) grubu da K grubu üzerinde tanımlı esnek gruplar olsun. (f, g): $(F, A) \to (H, B)$ esnek bir homomorfizm olsun. Eğer (F, A), G üzerinde devirli bir esnek grup ise $(f(F), (A))$ da K üzerinde devirli bir esnek grup olur.

Teorem 1.7.30. [136] (F, A) ve (H, B) esnek grupları sırasıyla G ve K esnek grupları üzerinde iki izomorfik grup olsun. Eğer (F, A) devirli bir esnek grup ise, (H, B) devirli bir esnek gruptur.

Teorem 1.7.31. [136] Eğer G esnek grubu üzerinde iki devirli esnek grup (F, A) ve (H, B) ise,

$$(F, A) \wedge (H, B)$$

de G üzerinde devirli bir esnek gruptur.

Teorem 1.7.32. [136] Grup (F, A) ve (H, B), G üzerinde iki devirli esnek grup ve $A \cap B = \emptyset$ olsun. O zaman

$$(F, A) \,\tilde{\cup}\, (H, B)$$

de G üzerinde devirli bir esnek gruptur.

Teorem 1.7.33. [136] (F, A) ve (H, B) sırasıyla sonlu m ve n mertebeli G ve K grupları üzerinde tanımlı iki devirli esnek grubu olsun. m ve n aralarında asal ise

$$(F, A) \times (H, B)$$

devirli esnek bir gruptur.

Lemma 1.7.34. [137] Eğer (F, A) esnek grubu bir G eliptik eğrisin toplamsal grubu ve $y^2 = x^3 + ax + b$ ise (F, A) bir devirli esnek gruptur.

Örnek 1.7.35. [137] F_{23}'te $y^2 = x^3 + 5x + 4$ eliptik eğrisinin 19 çözümü vardır.

$$(F, A) = \{(0,2), (0,21), (3,0), (5,4), (5,19), (8,2), (8,21), (13,19), (13,14), (14,9), (14,14), (15,2), (15,21), (19,9), (19,14), (20,10)\ ), (20,13), (21,3), (21,20)\}$$

ise G, üreteci $P = (8,2)$ olan bir devirli gruptur.

Burada;

$$1P = P, 2P = (19,14), 3P = (20,10), 4P = (21,20), 5P = (0,2), 6P = (15,21),$$

$$7P = (13,14), 8P = (5,19), 9P = (14,9), 10P = (3,0), 11P = (14,14),$$

$$12P = (5,4), 13P = (13,9), 14P = (15,2), 15P = (0,21), 16P = (21,3),$$

$$17P = (20,13), 18P = (19,9), 19P = (8,21).$$

Bu örnekte $o(F, A) = 20$ olduğundan, $\varphi(20) = 8$ dır. Bu nedenle bu devirli grup için sekiz üreteç vardır. Diğer üreteçler ise

$$(8,2), (8,21), (13,9), (13,14), (14,9), (14,14), (20,10), (20,13)$$

şeklindedir.

BÖLÜM 2

KRİSTOGRAFİ

2.1. Kristografi

Kriptografi ve steganografi herhangi bir veriyi gizlemek veya korumak için kullanılan yöntemlerdir. Steganografide veriler olduğu gibi, hiçbir değişiklik yapılmadan herhangi bir örtü nesnesine gizlenir. Kriptografide ise veriler rastgele dizilmiş karakterlerle anlamsız hale getirilmiş bir metne dönüştürülmektedir. Kriptografi, gizlenmek istenen bir verinin istenmeyen taraflarca okunamayacak bir hale dönüştürülmesinde kullanılan matematiksel yöntemler bütünüdür.

Kriptografi; anahtarsız, gizli anahtarlı ve açık anahtarlı olmak üzere üç ana grupta incelenebilir. Genel özellikleri ve bazı örnekleri aşağıda verilmiştir [91-105];

- **Anahtarsız Kriptografi** (MD5, SHA-1, RIPEMD-160, …)

  i. Girdilerdeki değişiklik karşısında kelebek etkisi davranışı sergiler.
  ii. Sistem çok gizli bir güvenlik sistemi ile korunur.

- **Gizli Anahtarlı (Simetrik) Kriptografi** (Sezar, Vigenere, DES, 3DES, RC5, Blowfish, IDEA, SAFER, AES, …)

  i. Anahtar boyutu küçüktür.
  ii. Açık anahtarlı kriptografi sistemlerine göre daha hızlı şifreleme yapabilir.
  iii. Anahtar üretim hızı yüksektir ancak anahtar değişimi ve dağıtımı ciddi bir problemdir.
  iv. Sistemin güvenliği gizli anahtar ve sistemin gizliğine bağlıdır.

- **Açık Anahtarlı (Asimetrik) Kriptografi** (Diffie-Hellman, RSA, ElGamal, Paillier, Blum-Goldwasser, Goldwasser-Micali, Okamoto-Uchiyama,)

  i. Göndericinin ve alıcının ayrı ayrı gizli anahtarları ve ortak açık anahtarları vardır.
  ii. Her kullanıcının sadece kendi gizli anahtarını gizli tutması yeterlidir.

iii. Anahtar değiş tokuşu güvensiz kanallar üzerinde bile güvenli bir şekilde yapılabilir.
iv. Tek yönlü fonksiyon kullanır.
v. Gönderilecek her alıcı için ayrı anahtar üretmek gerekir.
vi. Gizli anahtarlı kriptografi sistemlerine göre daha yavaştırlar.

Ayrıca günümüz teknolojisinde kullanım alanları sınırlı olmakla birlikte kuantum bilgisayarlarının tasarlanması ile birlikte kuantum kriptografi sistemleri de tanımlanmıştır.

Dahası, açık ve kapalı anahtar sistemlerinin avantajlı yönlerini bir arada kullanabilen hibrit sistemler de bulunmaktadır. Hibrit sistemlerde kriptolama için simetrik anahtarlar kullanılırken, bu anahtarların iki taraf arasında taşınması için asimetrik kriptografi yöntemleri kullanılmaktadır [99].

Kriptografi, gizli bir dilde veya daha önce kişilerin kendi aralarında kararlaştırıp tasarladıkları özel dilde mektup yazmaya benzer. İnsanlar ona ulaşabilir, okuyabilir, ancak ne anlama geldiğini anlamaz. Bununla birlikte, bu mesajın varlığı, mektubu gören herkes için açıktır. Eğer yetkisiz birisi gizli dili bilir veya çözerse, gizli mesaj kolayca anlayabilir.

Aynı durumda steganografi kullanılacak olsaydı, mektubu, mektubun hedeflenen alıcısına hediye olarak gönderilecek çift katlı bir mendilin iç kısmına yazılarak mendil dikilir ve hediye kutusu içine saklanarak gönderilirdi. Mesajı bilmeyenler için, hediye kutusunda mendilden başka bir şey yokmuş gibi görünürdü. Ancak hedeflenen alıcı neyi arayacağını bildiğinden mendil içindeki saklı mesajı bulabilmektedir.

Benzer şekilde, Alice ve Bob adlı iki kullanıcı internet üzerinden bir fotoğraf gibi medya dosyalarını kriptografi ile değiş tokuş etmek istedikleri varsayılsın. Alice elindeki resmin her bir pikselini uygun bir kriptografi algoritması ile kodlayarak harf, rakam ve diğer yazı karakterlerine dönüştürülerek kapalı bir metin elde eder. Daha sonra bu kapalı (gizli) metni herkese açık bir internet ortamında Bob'a gönderir.

Ancak Alice steganografi kullanmak isterse, resmin yapısında bir değişiklik yapmadan uygun bir stego-sistem ile resmi bir nokta kadar küçültür. Bob'a gönderdiği mailin içindeki metnin ilk cümlesinin noktası olarak kullanıp gönderir. Ya da Bob'a gönderdiği farklı bir

resim içine gömülmüş bir nokta olarak gönderir [110]. Bu örnek Resim 2.1. ve Resim 2.2. de görülebilir.

Yukarıda verilen örneklerde anlaşılacağı gibi çok farklı steganografi metotları kullanılabilmektedir.

Bu bölümde ilk aşamada steganografi ve grup teorisinin ilişkisi üzerinde durulmuş ancak bu alanda mevcut kayda değer çalışmalar olmadığı gibi steganografinin yapısı gereği grup teori ile bir ilişki kurulmayacağı sonucuna varılmıştır. Daha sonra steganografinin kriptografi ile ilişkisi üzerinde durulmuş ve bu alanda bir hayli bilimsel çalışmanın olduğu gözlemlenmiştir. Bu alanda yapılan çalışmalarda iki bilim dalının aynı anda kullanılarak melez (hibrit) güvenlik sistemleri oluşturulmuş ve bu sistemler sayesinde güvenli bir şekilde veri transferinin gerçekleştirilmesine imkân tanınmıştır. Ancak kullanılan sistemleri incelediğimizde; transfer edilmek istenen veri mevcut kripto sistemler kullanılarak şifreli metin elde edilmekte daha sonra elde edilen bu kapalı metin stego örtü (metin, ses, video vb.,) içine gizlenmektedir. Kriptografi steganografinin melezlenmesi ile elde edilen ve kristografi olarak adlandırılan bu yeni sistem ile gönderilmek istenen gizli veri güvensiz açık kanallarda bile transfer edilebilmektedir.

Şimdi, kriptografi ve steganografi sistemlerinin tanımları ve genel özellikleri verilecektir.

Tanım 2.1.1 [120] P: Açık yazıların (metinlerin) sonlu bir kümesi,

C: Kapalı yazıların sonlu bir kümesi,

K: Anahtar uzayı, olası anahtarların sonlu bir kümesi,

E: Kapama (şifreleme) fonksiyonlarının sonlu bir kümesi,

D: Açma (deşifreleme) fonksiyonlarının sonlu bir kümesi olsun.

$\forall\, k \in K$ için bir kapama fonksiyonu $e_k \in E$ ve buna karşılık gelen açma fonksiyonu $d_k \in D$ olsun öyle ki, $e_k: P \to C$ ve $d_k: C \to P$ fonksiyonları,

$$\forall\, x \in P \text{ için } d_k\,(e_k(x)) = x$$

özelliğini sağlıyorsa (P, C, K, E, D) beşlisine bir kriptografik sistem denir.

Tanım 2.1.2 [91-105] Steganografi, bir açık iletişim kanalı üzerinden gizli bilgi iletişimini sağlayan bir araçtır.

Steganografi, düz metin, resim, ses veya video dosyasının içinde kullanıcıya gizlenmiş bilgiyi iletmesine imkân tanır. Gizlenecek metinde herhangi bir değişiklik yapılması gerekmemektedir. Böylece, gizlenecek veri diğer insanlara içeriğini vermeden korunabilir. Steganografi bu yönüyle kriptografiden farklılık arz etmektedir.

Örnek 2.1.3 [97,98] Benim için futbolda önemli olan centilmenlik ve dostluktur. Hedefim illaki kazanmak falan değildir. Ben sadece kendi reklamını düşünen kişiliğe sahip olsam başka olurdu. Ben net birisiyim arkadaş! Takımım kazanırsa malzemecisine kadar mutlu oluruz. Ben de sporcu varlığımı geliştiririm. Hakemlere baskı uygulamak sportmenliğe yakışmaz. Fair-play için mücadele gerekirse onu da yaparım. Medyayı da bağrıma basmışım, spor uğruna gülmüşüm ve ağlamışım, kafam rahat!

Aşağıdaki şekilde yazılıp satır atlanarak sadece sarı renkli cümleler okunduğunda;

"Benim için futbolda önemli olan centilmenlik
ve dostluktur. Hedefim illaki kazanmak
falan değildir. Ben sadece kendi reklamını düşünen
kişiliğe sahip olsam başka olurdu. Ben net
birisiyim arkadaş! Takımım kazanırsa mal-
zemecisine kadar mutlu oluruz. Ben de sporcu
varlığımı geliştiririm. Hakemlere baskı uygulamak
sportmenliğe yakışmaz. Fair-play için mücadele
gerekirse onu da yaparım. Medyayı da bağ-
rıma basmışım, spor uğruna gülmüşüm ve ağ-
lamışım, kafam rahat!"

ise çok farklı bir anlam ifade edebilmektedir. Bu örnekte de açıkça anlaşılacağı üzere steganografi, herkese açık kaynaklarda bile güvenli bir iletişim metodu oluşturabilmeye imkân tanımaktadır. Aşağıdaki tabloda (Tablo 2.1) günümüzde en çok kullanılan modern kristografi sistemlerinin isimleri ve genel özellikleri verilmiştir.

Tablo 2.1. Steganografi Araçları

Program	**Görüntü dosyaları**	**Ses dosyaları**	**Video dosyaları**	**Metin dosyaları**	**Diğer destek**	**Notlar**
Anubis	BMP, JPEG	-	-	-	Dosyanın sonuna eklenen veriler	Açık kaynak
BMP Secrets	BMP, JPEG, TIFF, GIF	-	-	-	-	-
Dark CryptTC	BMP, JPEG, TIFF, PNG, PSD, TGA, MNG	WAV	-	TXT, HTML, XML, ODT	EXE, DLL, NTFS akışları	RSD modu (RNG tabanlı rastgele veri dağıtımı), AES şifreleme desteklenir
DeepSound	BMP	Ses CD'si, APEetiketi FLAC, MP3,WAV WMA	-	-	-	AES 256 bit şifreleme
ImageSpyer G2	BMP, TIFF	-	-	-	-	RSD algoritması uygulandı, Total Commander eklentisi
iWatermark	JPEG	-	-	-	-	Mac, Win, iOS ve Android için JPEG fotoğraflarda gizlenmiş steganografik filigran
MP3Stego	-	MP3	-	-	-	Açık kaynak
Mr. Crypto	BMP, PNG, TIFF	-	-	-	-	Arayüz;AES, TripleDES şifreleme. Veri gizlemek için LSB kullanır.
OpenPuff	BMP, JPEG, PNG, TGA	MP3,WAV	3GP, MP4, MPEG-1, MPEG2, VOB, SWF, FLV	PDF	-	Açık kaynak, 256 bit çoklu şifreleme, Taşıyıcı zincirleri, Çok katmanlı gizleme
OpenStego	BMP, PNG	-	-	-	-	Açık kaynak
OutGuess	JPEG, PNM	-	-	-	-	Ücretsiz yazılım
Outguess-rebirth	JPEG, PNM	-	-	-	-	Taşınabilir ücretsiz Windows (Linux için Outguess'e dayalı)
PHP-Class StreamSteganography	PNG	-	-	-	-	-

Program	Görüntü dosyaları	Ses dosyaları	Video dosyaları	Metin dosyaları	Diğer destek	Notlar
QuickStego / QuickCrypto	BMP, JPEG, GIF	-	-	-	-	Windows XP, Vista, 7
Red JPEG	JPEG	-	-	-	-	Total Commander için XT, LZMA sıkıştırma, PRNG tabanlı maskeleme ve dağıtım
S-Tools	BMP, GIF	WAV	-	-		Kullanılmayan disket alanı
Steg	BMP, PNG, JPEG, GIF	-	-	-	-	Simetrik ve asimetrik anahtar şifreleme, Win / Linux / Mac üzerinde çalışır
StegaMail	BMP, PNG	-	-	-	-	56 bit şifreleme, zLib sıkıştırma
SteganographicLabora-tory (VSL)	BMP, PNG, JPEG, TIFF	-	-	-	-	Açık kaynak
Steganography Studio	BMP, PNG, GIF	-	-	-	-	Farklı gizleme yöntemleri (LSB, LSB Eşleştirme, SLSB), Açık kaynak
Steganography Online Codec	BMP, PNG, JPEG, GIF	-	-	-	-	PBKDF2 anahtar türetme ile AES CBC 256 bit şifreleme kullanan ücretsiz çevrimiçi araçtır
SteganPEG	JPEG	-	-	-	-	Windows XP, Vista, 7
StegFS	-	-	-	-		Linux için steganografik dosya sistemi
Steghide	JPEG, BMP	WAV, AU	-	-	-	Açık kaynak (GNU Genel Kamu Lisansı)
Stegonaut	-	MP3	-	-	-	Açık kaynak, AES 256 bit şifreleme
StegoShare	BMP, JPEG, PNG, GIF, TIFF	-	-	-	-	Açık kaynak
stegano-rs	PNG	WAV	-	-	-	Açık kaynak (GNU GPLv3)

Tanım 2.1.4 Steganografik sistem c gizli mesajını, k anahtarını kullanarak m örtü cismine gizleyen bir mekanizmadır. m mesajını taşıyan stego nesne s elde edilir. F gömme fonksiyonu ve G çıkarma fonksiyonu iken (F, G) çiftine stego sistem denir.

Burada;

$$s = F(C; m, k)$$

ve

$$m = G(s, k)$$

dir [91-105].

M olası tüm mesajları kümesi olsun, o zaman stego sistemin gömme kapasitesi

$$\log_2 M$$

olur.

Tanım 2.1.5 [97] Bir kullanıcının bir görüntü veya video gibi bir taşıyıcı dosyaya gizli verileri yerleştirmesine ve daha sonra bu verileri çıkarmasına olanak tanıyan araçlara steganografi yazılım aracı denir.

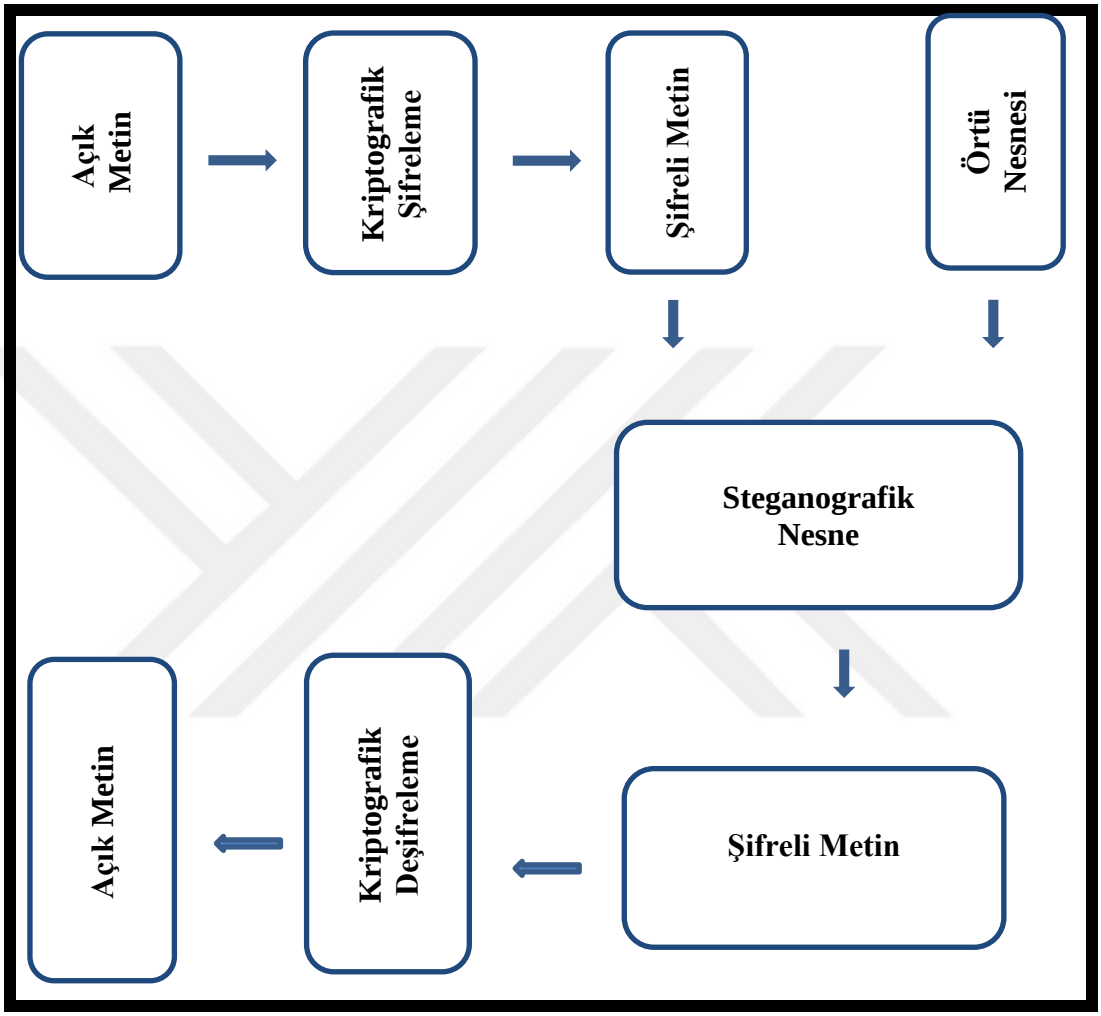
Modern steganografi çeşitli araçlar kullanmaktadır. Bu araçlar ve hangi dosya formatlarının gizlenmesinde kullanıldıkları Tablo 2.1.'de verilmiştir [97].

Steganografi ve kriptografinin kombinasyonunu kristografi olarak tanımlanmıştır. Bu konuda yapılan temel çalışmalar aşağıda verilmiştir.

F. Borges ve arkadaşları yaptıkları çalışmalarında aşırı güvenlik gerektiren durumlarda kullanılmak üzere steganografi ve kriptografinin birlikte kullanıldığı ve stegano-kriptografi diye adlandırdıkları bir model kullanmışlardır. Bu modelde Diffie-Hellman, RSA ve kriptografi sistemlerini irrasyonel sayılar ile kullanmışlardır. Bununla birlikte resim ve video gibi görsel araçlar kullanılarak bu enkript edilmiş veriyi (kapalı metini) gönderebilmek için DCT katsayılarında steganografi kullanılmıştır [104].

M. H. Rajyaguru'ya göre kristografi, kriptografi ve steganografinin kombinasyonudur. Rajyaguru kristografiyi şifreli veriyi başka bir dijital verinin içine gizleyen bir iletişim sistemi olarak tanımlamaktadır. Birçok farklı taşıyıcı dosya formatları stego-örtü olarak kullanılabilir. Ancak internet üzerinde frekansı nedeniyle dijital görüntüler en popüler olanlarıdır. Görüntülerde özel verileri gizlemek için oldukça fazla çeşitlilikte steganografi metotları mevcuttur. Bu metotların bazıları diğerlerine göre daha karmaşıktır ve hepsinin

ayrı ayrı güçlü ve zayıf noktaları vardır. Rajyaguru bu makalede kristografik metotlarla ilgili sorunları çözmeye çalışmıştır. Her bir mesaj için hızla değiştirilebilen mesaj anahtarı oluşturulmuş ve o anahtar ile mesaj güvenlik altına almaya çalışılmıştır [62].



Şekil 2.1. Kristografi Sistemi

A.J. Raphael, Dr. V Sundaram, "Dijital haberleşme günümüzde savunma sisteminin önemli bir parçası haline gelmiştir. Dijital haberleşme uygulamaların birçoğu internet tabanlıdır ve bu iletişimin gizli yapılmış olması önem arz etmektedir. Açık bir kanal üzerinden iletilen verinin güvenliği günümüz modern toplumlarının en temel sorunu haline gelmiştir. Bu nedenle gizlilik ihlali, veri bütünlüğünün bozulması, yetkisiz erişim ve kullanıma karşı korunmak için yüksek maliyetli ve profesyonel güvenlik sistemlerinin kullanılması gerekmektedir. Bu durum veri gizlemedeki istikrarsız büyümenin bir sonucu olarak ortaya çıkmıştır. Kriptografi ve steganografi veri güvenliğini sağlamak için kullanılan iki popüler yöntemdir. Steganografi mesajın kendisini gizlerken kriptografi

mesajın mevcut şeklini değiştirir ve anlamsız görünen bir veriye dönüştürür. Kriptografi sistemleri veriyi önce anlamsız bir forma dönüştürerek kapalı veriyi elde eder. Daha sonra bu şifrelenmiş veri herkese açık iletişim sistemleri üzerinden iletilir. Steganografide ise veri bir görüntü dosyasına gömülerek (gizlenerek) iletilir." [66] demiştir

Raphael ve Sundaram, bu çalışmalarında internet gibi açık bir kanal üzerinden gerçekleştirilen iletişimin güvenliğini artırmak için kriptografi ve steganografi yöntemlerinin birleştirilmesiyle elde edilen güçlü bir metot üzerinde durmuştur [66].

Raphael ve Sundaram'ın oluşturdukları kristografi sistemi yukarıda Şekil 2.1. de görülebilmektedir [66].

Brifcani A. [107], çalışmasında kriptografi ve steganografi algoritmalarına dayanmakta olan iki aşamalı (stego-tabanlı-kripto) tersinir tekniğini tasarlamıştır. Birinci aşamada veri güvenliğini artırmak için RSA şifreleme algoritması kullanılarak kriptolu mesaj elde edilir. İkinci aşamada ise steganografi algoritması olarak IWT (Tam sayıları tam sayılara eşleyen dalgacık dönüşümleri, orijinal görüntünün mükemmel bir şekilde yeniden yapılandırılmasını sağlayan transformasyon) tabanlı kaldırma şeması kullanılarak kriptolu veri olduğu gibi örtü nesnesinin içine gizlenir. RSA algoritmasında sistemin güvenliğini artırmak için 14 basamaklı olan bir anahtar kullanılmıştır. Gizli mesajın yük ve dayanıklılık kapasitesini artırmak için veri, IWT katsayılarının arasına düşük, orta ve yüksek frekans alt bantlarında gizlenir. Bu tekniğin kullanılması sayesinde;

i. Sezilmezlik, parazit oranı (PSNR) değerlerinin tepe sinyali artırılarak geliştirilmiştir.
ii. Güvenlik, açık anahtarlı kriptografi algoritması kullanılarak geliştirilmiştir.
iii. Kapasite, gömülü verinin, IWT'nin düşük, orta ve yüksek frekans alt bantlarının katsayılarıyla geliştirilmiştir.

S. A. Laskar ve K. Hemachandran, yüksek performanslı JPEG steganografi ile birlikte yerine koyma kripto metodolojini tasarlamışlardır. Bu yaklaşım frekans alanında kullanılan DCT (farklı frekanslarda salınan kosinüs fonksiyonlarının toplamı cinsinden sonlu bir veri noktaları dizisini ifade eder) tekniğini kullanarak görüntünün içine kriptolu veriyi gizlemektedir. Yaptıkları deney sonuçları göstermektedir ki, kriptolu verinin görsel bir örtü nesnesinin içine yerleştirilmeden önce örtü nesnesinin görsel ve istatistiksel

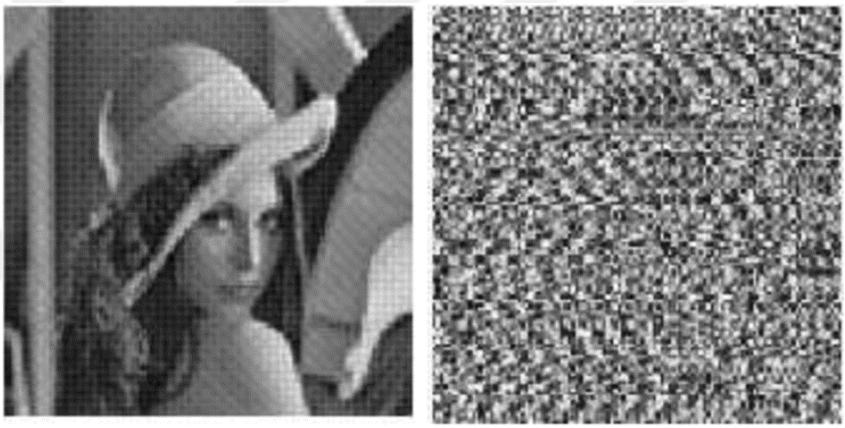
değerleri ile yerleştirildikten sonraki değerleri birbirine benzemelidir. Böylece gizli mesajın tespit edilme tehlikesi minimize edilmiş ve gizli iletişimin sağlanmasına imkân tanınmış olur. Kullandıkları yönteminin etkinliği MSE (hataların karelerinin ortalamasını, yani tahmini değerler ile gerçek değer arasındaki ortalama kare farkını ölçer) ve PSNR (bir sinyalin olası maksimum gücü ile temsilinin doğruluğunu etkileyen bozulma gürültüsü gücü arasındaki oran için bir mühendislik terimidir) ile hesaplayarak elde etmişlerdir. Bu yöntemle gizli mesaj görüntü dosyasına gömülürken, görüntünün kalitesinde görünür bir bozulma veya bulanıklığın oluşmasına imkan verilmemektedir. Dolayısıyla tasarlanan bu metot, kullanıcıya internet ağı üzerinde güvenli bir şekilde veri transfer etmesine imkân tanımakta ve saldırılara karşı yüksek hacimli gizleme (gömme) gerektiren dayanıklı uygulamalar için de kullanılabilmesine imkan tanımaktadır. Steganografi yönteminin daha güvenli olabilmesi için şu üç aşamayı çalışmalarında kullanmışlardır;

i. Gizlenmesi gereken mesaj önce sıkıştırılmıştır. (Winzip programları ile yapılan işlem gibi)
ii. Sıkıştırılan mesaj kriptografi sistemi ile enkript edilmiştir. (yani kapalı veri elde edilir.)
iii. Elde edilen kapalı veri gizleme (stego) örtüsüne gömülerek gönderilmiştir [108].

A.R. Aparajita, ise çalışmasında; “Steganografi, gizlenen şey tek bir görüntü dosyası olsa bile veriyi gizleme ile ilgilenir. Ancak bu veri gizlenmeden önce kriptolanması gerekir. Birçok farklı dosya formatları veriyi gizlemek için kullanılır ancak internet üzerindeki frekanslar nedeniyle en yaygın olarak dijital dosyalar kullanılmaktadır. Kendine has güçlü ve zayıf yönleri olan çeşitli steganografi araçları vardır.” demiştir. Aparajita’nın bu çalışmasında çeşitli steganografi araçları kullanarak bir resim dosyasına özel verileri gizlemeyi incelemiş ve sonuç olarak kriptografi ve steganografi arasındaki temel farklara değinilmiştir [105].

Bu iki sistem arasındaki farklılık steganografi işlemi uygulanan Resim 2.1. [105] ile kriptografi işlemi uygulanan Resim 2.2. [160] incelendiğinde bariz bir bir şekilde görülebilir.

Resim 2.1. Stego Örtü Olarak Kullanılan Resim



Resim 2.2. a Resminin Şifrelenmeden Öncesi ve Sonrası

A. B. Mansoor ve arkadaşları, AES ve DES kriptografi algoritmalarını kullanarak açık metinden kapalı metini elde ettikten sonra hem açık hem de kapalı metini model tabanlı steganografi ve F5 steganografi tekniğini kullanarak görüntü dosyasına gömmüşlerdir. Özellikle DWT (Veri analizinde, verinin farklı çözünürlüklerde incelenmesine olanak sağladığı için özellikle görüntü işleme alanında kullanılan dönüşümdür.) ve DCT (Veri sıkıştırılmasında çokça kullanılan bir matematiksel dönüşümdür. Örneğin jpeg resimlerin sıkıştırılmasında kullanılır.) etki alanları da ayıklanarak steganalize için yüksek dereceden istatistikleri kullanılmıştır. Daha sonra bir FLD (Veri setinin mevcut hali bileşenleri ayırmak için çok elverişli olmadığında veriyi daha kolay ayrılabilir hale getirmekte kullanılır.) sınıflandırıcı oluşturmuşlardır. Deneyler sonunda elde ettikleri sonuç; model tabanlı steganografinin F5 steganografi den daha güvenli olduğu sonucuna olmuştur [100].

Kriptografi çalışmalarında ASCII kodu kullanılmaktadır. ASCII kod tablosu Tablo 2.2. de verilmiştir.

Her ne kadar ASCII kodları klavyedeki tüm karakterler için oluşturulsa da, çalışmamızda yapılacak işlemlerin geçişlerinin daha basit yollarla görülebilmesi ve sözel metin örnekleri üzerine çalışabilmek için Türkçe harflerin sayısal değerlerle eşleştiren bir tablo oluşturulmuştur (Tablo 2.2.). Bu tabloda her harfe karşılık $mod\ 29$'a göre bir sayısal değer verilmiştir.

Tablo 2.2. ASCII Kodu Eşleştirme Tablosu

32	(space)	48	0	64	@	80	P	96	`	112	p
33	!	49	1	65	A	81	Q	97	a	113	q
34	"	50	2	66	B	82	R	98	b	114	r
35	#	51	3	67	C	83	S	99	c	115	s
36	$	52	4	68	D	84	T	100	d	116	t
37	%	53	5	69	E	85	U	101	e	117	u
38	&	54	6	70	F	86	V	102	f	118	v
39	'	55	7	71	G	87	W	103	g	119	w
40	(	56	8	72	H	88	X	104	h	120	x
41	)	57	9	73	I	89	Y	105	i	121	y
42	*	58	:	74	J	90	Z	106	j	122	z
43	+	59	;	75	K	91	[	107	k	123	{
44	,	60	<	76	L	92	\	108	l	124	|
45	-	61	=	77	M	93	]	109	m	125	}
46	.	62	>	78	N	94	^	110	n	126	~
47	/	63	?	79	O	95	_	111	o		

Tablo 2.3. de elde edilen harflerin sayısal değerleri için ikilik tabanda dört bitlik eşleştirme tablosu olan Tablo 2.4. oluşturulmuştur.

Tablo 2.3. Türkçe Alfabesi Sayısal Değer Eşleştirme Tablosu

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

Tüm sayısal verilerde ki her bir karakter onluk sistemdeki rakamlara denk geldiğinden bu tabloda 0,1,2,3,4,5,6,7,8,9 rakamlarının ikilik tabandaki değerlerinden meydana getirilmiştir.

Tablo 2.4. Rakamların İkilik Taban Değerleri

0	1	2	3	4	5	6	7	8	9
0000	0001	0010	0011	0100	0101	0110	0111	1000	1001

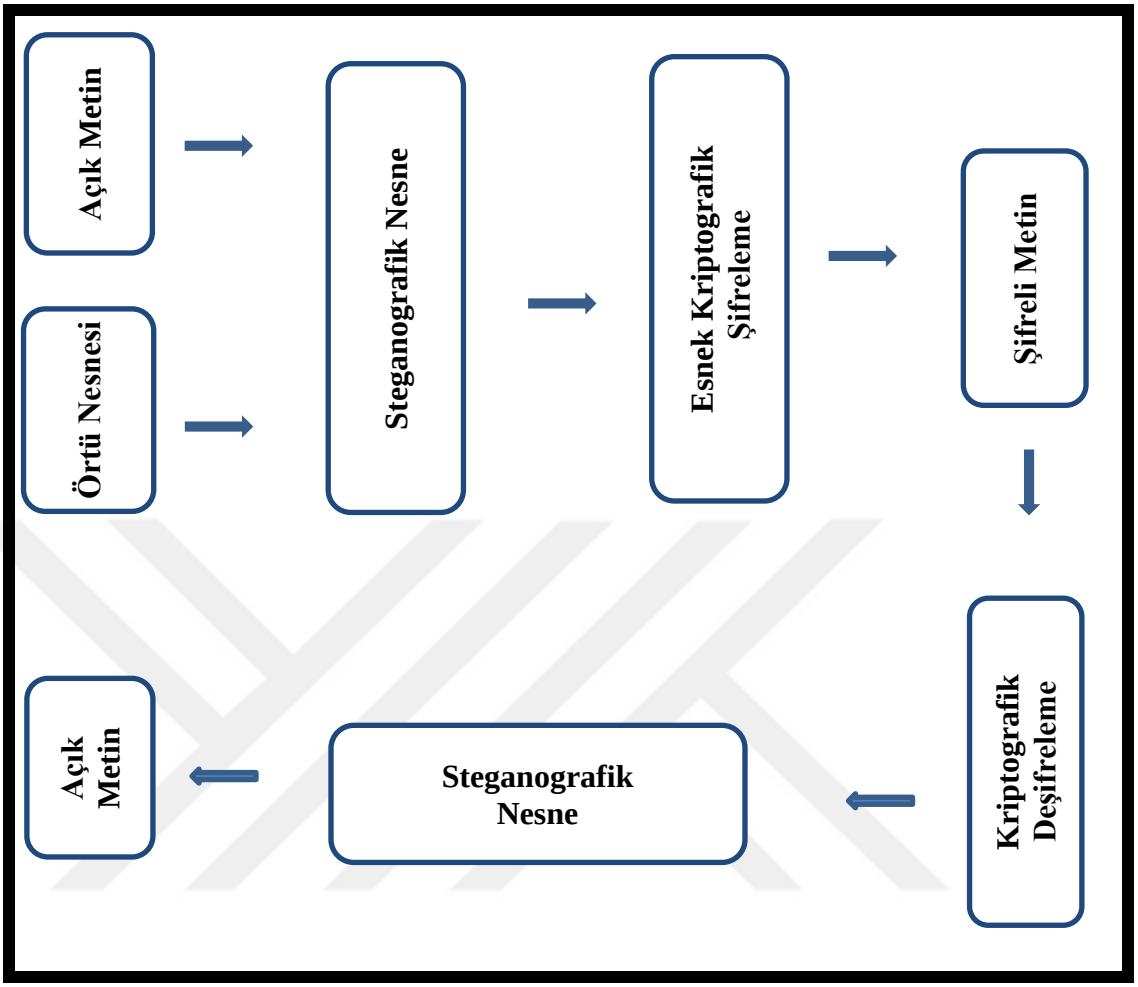
Bu anlamda tez çalışması kapsamında oluşturulan esnek kristografi algoritma şu şekilde tasarlanmıştır;

- Önce gönderilmek istenen veri sayısal veriye dönüştürülür. Dönüştürme için alfabedeki her bir harfe karşılık $0, 1, 2, \dots, 28$ $(mod 29)$ sayılarından biri ile eşleştirme tablosu oluşturularak (Tablo 2.3.) kullanılır.
- Daha sonra bir stego örtü seçilir. Örneğin tek doğal sayıların küçükten büyüğe doğru sıralanması gibi.
- Gönderilmek istenen metinin her bir harfine karşılık Tablo 2.3. kullanılarak sayısal veri elde edilir. Elde edilen sayısal değerlerin her biri belirlenen kurala göre stego örtünün içine yerleştirilerek örtülü sayısal metin elde edilir.
- Daha sonra bu örtülü metin esnek küme tarafından belirlenen kriptografi algoritması (DES, AES, RSA vb,) kullanılarak şifreli metne dönüştürülür. Şifreli metin elde edildikten sonra açık bir iletişim kanalı aracılığı ile transfer edilir.

Bu çalışma sonucunda oluşturulan esnek kristografi sistemi aşağıda verilen Şekil 2.2. de gösterilmiştir.

Tanım 2.1.6 Açık metinden elde edilen sayı dizisinde bit değerlerinden seçilecek yerleştirilme aralığı ve kaydırılacak bit sayılarının kaç tane olduğunu belirleyen değere fet değeri denir.

Bu değer sistemde kullanılacak bit sayısından küçük olmalıdır. 8 bitlik sistemin dikkate alınması durumunda $0 < fet < 8$ kullanılır. Bu durumda anahtar uzunluğu $2^8 = 128$ karakterden oluşacaktır.



Şekil 2.2. Esnek Kristografi Sistemi

4 bitlik sistemin kullanılması durumunda $0 < fet < 4$ kullanılır. Anahtar uzunluğu ise $2^4 = 16$ karakterden oluşacaktır. 16 karakterli anahtar tablosu Tablo 2.5. te her sütunda istenen karakter yazılarak belirlenir.

Tablo 2.5. Anahtar Dönüşüm Tablosu

0000	0001	0010	0011	0100	0101	0110	0111
1000	1001	1010	1011	1100	1101	1110	1111

Tablo 2.5**.** kullanılarak elde edilen sayısal veri kristografik veri elde edilir.

Tanım 2.1.7 fet steganografi algoritma komut sistemi aşağıdaki özellikleri taşıyan sistemdir:

1. Sistemde kaç bitlik değer kullanılacağını belirlenir,
2. Uygun uzunlukta dönüşüm anahtarı belirlenerek Tablo 2.5.'e yazılır,
3. fet değeri belirlenir, ($0 < fet < bit$ sayısı),
4. Stego örtü olarak bir sayı dizi belirlenir (örneğin ilk 500 ardışık pozitif tek sayınının küçükten büyüğe doğru art arda dizerek oluşturulacak sayı dizisi gibi),
5. Stego örtünün baştan fet değeri kadar rakamı silinir,
6. Türkçe alfabesindeki her harfe karşılık rastgele farklı bir sayı belirlenir (Tablo 2.3.),
7. Açık metindeki harflerin karşılıklarını Tablo 2.3.'ten belirlenir,
8. Belirlenen sayılar stego-örtü sayı dizisinden elde edilen sayının basamaklar arasına açık metinden şu şekilde yerleştirilir;

   8a. İlk sayı 1. basamaktan hemen sonra, diğer sayılarda sırasıyla fet değeri olarak belirlenen sayı kadar basamak atlayarak birer birer yerleştir,

9. Stego-örtünün içine son değer yerleştirildikten sonra, stego örtü sayı dizisinin fazla kalan kısmı silinir,
10. Elde edilen sayı dizisindeki her bir rakamı ikili sayı sisteminde kullanılacak uygun bit değerine dönüştürülür (Tablo 2.4.),
11. Sıfır ve birlerden oluşan yeni sayı dizisini belirlenir,
12. Sayı dizisini fet değeri kadar bitten oluşan gruplara ayrılır, (örneğin, $fet = 5$ ise $10011, 011001$ gibi),
13. Sağ ve sol iki bloğa sırasıyla önce sol bloğa ilk beş bit, sonra sağ bloğa ikinci beş bitlik değerleri sıralayarak yeni bir sayı dizisi oluşturulur,

14. Bitlerin yer değiştirmesiyle elde edilen yeni (sol blok + sağ blok) sayı dizisindeki her bir harfe denk gelen bit değerlerini Tablo 2.5.'deki anahtar dönüşüm tablosundan belirlenir,

15. Elde edilen şifreli metini (kapalı metin) yazılır,

16. Elde edilen şifreli metin internet gibi bir ortamda transfer edilir.

Tanım 2.1.8 U şifrelenecek açık metinlerin evrensel kümesi ve E kriptografik sistemlerinin parametre kümesi olsun. $F: E \rightarrow P(U)$ bir dönüşüm ve (F, E) ikilisi U üzerinde esnek küme olmak üzere,

$A = \{e_1, e_2, e_3, \dots, e_n\}$, E de boş olmayan sonlu bir alt küme ve $U = \{h_1, h_2, h_3, \dots, h_m\}$ olsun. Aşağıdaki koşulları sağlayan (F, A)'ya esnek kristografi denir.

Esnek kristografi sisteminde stego-örtü olarak herhangi bir sayı dizisinin istenen kadar basamağı seçilir. Bu örtü içine açık metin gizlenerek stego-metin elde edilir. Bu stego-metin esnek fonksiyon ile belirlenen kriptografi algoritması kullanılarak gizli metne dönüştürülür. $fet = 3$ alınsın;

1. Sistemde dört bitlik değer kullanılır,
2. Uygun uzunlukta ($2^4 = 16$) dönüşüm anahtarı belirlenir (Tablo 2.5.),
3. Stego örtü olarak bir sayı dizi belirlenir (π sayısının virgülden sonrasındaki istenen kadar basamağı gibi),
4. Bu sayı dizisin baştan fet değeri kadar rakam örtü sayı dizisinden silinir,
5. Türkçe alfabesindeki her harfe karşılık $mod29$'a göre bir sayı verilir (Tablo 2.3.),
6. Açık metindeki harflerin karşılıkları (Tablo 2.3.)'ten belirlenir,
7. Belirlenen sayıları, stego örtü sayı dizisinden elde edilen sayının basamakları arasına açık metinden şu şekilde yerleştirilir,
8. İlk sayı 1. basamaktan hemen sonra, diğer sayılarda sırasıyla fet değeri olarak belirlenen sayı kadar basamak atlayarak birer birer yerleştirilir,
9. Elde edilen stego metin esnek fonksiyonun belirlediği kriptografik algoritmadan (AES, DES, RSA, …) geçirilerek şifreli metin elde edilir,

10. Elde edilen şifreli metin internet gibi güvensiz bir ortamda rahatlıkla transfer edilebilir.

Örnek 2.1.8 U evrensel küme ve E parametre kümesi olsun, $F: E \rightarrow P(U)$ bir dönüşüm olmak üzere (F, E) ikilisi U üzerinde esnek küme olmak üzere,

$A = \{e_1, e_2, e_3, e_4, e_5, e_6\}$, E de bir alt küme ve $U = \{h_1, h_2, h_3, \dots, h_{16}\}$ olsun.

$h_1 =$ DES, $h_2 =$ AES, $h_3 =$ RSA, $h_4 =$ Sezar, $h_5 =$ Diffie-Helllman, $h_6 =$ fet sistem,

$h_7 = \pi$ sayısının virgülden sonraki ilk 1000000 basamağı olsun, $h_8 = \sqrt{5}$ sayının virgülden sonraki ilk 1000000 basamağı olsun, $h_9 =$ Fibonacci dizisinin ardışık yazılarak elde edilen 1113581321 ... sayısının ilk 1000000 rakamından oluşan kısmı olsun, $h_{10} = \sqrt{2}$ sayının virgülden sonraki ilk 1000000 basamağı olsun, $h_{11} =$ asal sayı dizisinin ardışık yazılarak elde edilen 23571113171923293137... sayısının ilk 1000000 rakamından oluşan kısmı olsun, $h_{12} =$ tek doğal sayı dizisinin ardışık yazılarak elde edilen 1357911131517... sayısının ilk 1000000 rakamından oluşan kısmı olsun, $h_{13} =$4 bitlik sistem kullan, $h_{14} = 8$ bitlik sistem kullan, $h_{15} = fet(3)$, $h_{16} =$ sistem dönüşüm anahtarı,

$e_1 =$ NEVŞEHİR, $e_2 =$ ÜNİVERSİTESİ, $e_3 =$ FEN, $e_4 =$ BİLİMLERİ, $e_5 =$ ENSTİTÜSÜ, $e_6 =$ MATEMATİK, olmak üzere

$$f(e_1) = \{h_6, h_7, h_{13}, h_{15}, h_{16}\} \in (F, A)$$

sistemine esnek kristografi denir.

Örnek 2.1.9. Yukarıdaki *Örnek 2.1.8* de belirlenen $f(e_1)$ esnek fonksiyonunda $e_1 =$ NEVŞEHİR kelimesi ve $\{h_6, h_7, h_{13}, h_{15}, h_{16}\}$ parametreleri kullanarak şifreli metne dönüştürme işlemini adım adım gerçekleştiriniz.

Düz metin : NEVŞEHİR
Stego Örtü : π
Esnek Sistem : Örnek 2.1.8 de verilen $f(e_1) = \{h_6, h_7, h_{13}, h_{15}, h_{16}\} \in (F, A)$
Kripto Anahtar : NEVŞHİRÜSTFBLMOG

Çözüm:

1. Steganografik örtü olarak seçilen π sayısı ondalık kısmının istenilen boyutta seçimi yapılır;

$$\pi = 3{,}14159265358979323846264338327950288419716939937510582097494459230781640628620899862803482534211706798214$$

2. $fet(3)$ kullanıldığından sayı dizisinin virgülden sonraki ilk üç rakamı (141) silinerek

$$592653589793238462643383279502884197169399375105820974944592307816406286208998628034825342117067982$$

stego-örtüsü elde edilir.

3. Tablo 2.3.'ten NEVŞEHİR düz metin sayısal metine dönüştürülerek Tablo 2.6. oluşturulur.

Tablo 2.6. Açık Metin mod 29 Değerleri

N	E	V	Ş	E	H	İ	R
16	5	26	22	5	9	11	20

4. N harfine karşılık gelen **16** sayısal verisi stego-örtünün ilk karakteri olan 5'in hemen sonrasına yerleştirilir,

$$5\mathbf{16}9265358979323846264338327950288419716939937510582097494459230$$

Diğer değerleri ise fet değerinin üç olması nedeniyle üçer basamak aralıklarla stego-örtüye yerleştirmeye devam edilir,

$$5\mathbf{16}926\mathbf{5}535\mathbf{26}897\mathbf{22}932\mathbf{5}384\mathbf{9}626\mathbf{11}433\mathbf{20}$$

5. Elde edilen bu steganografik veriyi Tablo 2.5 kullanılarak ikilik taban sitemine çevrilir,

$$1010001011010010010011001010101001101010010011010001001011100100010100100110010010100111000010010010110001001100001000101000011001100100000$$

6. Elde edilen bu sayısal veri dizisini $fet = 3$ olduğundan 3 bitlik gruplara ayırılır,

010 **100** 010 **110** 100 **100** 100 **110** 010 **101** 010 **011** 010 **100** 100 **110** 100 **010** 010 **111** 001 **000** 101 **001** 001 **100** 100 **101** 001 **110** 000 **100** 100 **101** 100 **010** 011 **000** 010 **001** 010 **000** 110 **011** 001 **000** 00

7. $1.,3.,5.,\ldots$, gibi tekli sıradaki veriler arka arkaya sol kolon, $2.,4.,6.,\ldots$, çift sıradaki kırmızı verileri sağ kolon olarak sol kolonun arkasına sırasıyla dizilir,

010010100100010010010100100010001101001100001000100100011010010
110001001001101001101010111001100101110000011001011101001010100
00001000011000

8. Bu sayı dizisindeki her bir dört bite karşılık gelen harfi aşağıdaki anahtar tablodan bulunur (Tablo 2.7.),
9. Elde edilen esnek kristografik metin;

$$HFHHTHSSMVNSTEF\text{İ}ST\text{Ş}HM\text{İ}LLBS\text{Ş}VOT\text{İ}NVES$$

elde edilir.

Tablo 2.7. Anahtar Dönüşüm Tablosu

0000	0001	0010	0011	0100	0101	0110	0111
N	E	V	Ş	H	İ	R	Ü
1000	1001	1010	1011	1100	1101	1110	1111
S	T	F	B	L	M	O	G

Esnek yapıların kullanılması ile edilen bu sistem, kullanıcılara kişileştirilmiş kristografi algoritması sunmaktadır. Ayrıca, mevcut kriptografi ve steganografi algoritmalarını kullanılması büyük avantaj sağlamaktadır. Esnek fonksiyon sayesinde kullanılacak kriptografik algoritma seçenekleri kullanıcının değiştireceği bir parametre ile anında değiştirilebilecektir.

2.2. Kristografi Algoritmasının C# ile Tasarımı

Elde edilen esnek kristografi örneğinin C# dili yazım kodu aşağıda yazıldığı şekliyle tasarlanmıştır [129].

```
namespace esnekkristografi
{
   partial class Form1
   {      /// <summary>
      /// Required designer variable.
      /// </summary>
      private System.ComponentModel.IContainer components = null;
      /// <summary>
      /// Clean up any resources being used.
      /// </summary>
      /// <param name="disposing">true if managed resources should be disposed; otherwise, false.</param>
      protected override void Dispose(bool disposing)
      {
         if (disposing && (components != null))
         {
            components.Dispose();
         }
         base.Dispose(disposing);
      }
      #region Windows Form Designer generated code
      /// <summary>
      /// Required method for Designer support - do not modify
      /// the contents of this method with the code editor.
```

```
        /// </summary>
        private void InitializeComponent()
        {
            this.richTextBox1 = new System.Windows.Forms.RichTextBox();
            this.richTextBox2 = new System.Windows.Forms.RichTextBox();
            this.button1 = new System.Windows.Forms.Button();
            this.label1 = new System.Windows.Forms.Label();
            this.label2 = new System.Windows.Forms.Label();
            this.SuspendLayout();
            //
            // richTextBox1
            //
            this.richTextBox1.BackColor = System.Drawing.SystemColors.ButtonFace;
            this.richTextBox1.Location = new System.Drawing.Point(12, 36);
            this.richTextBox1.Name = "richTextBox1";
            this.richTextBox1.Size = new System.Drawing.Size(355, 69);
            this.richTextBox1.TabIndex = 0;
            this.richTextBox1.Text = "";
            this.richTextBox1.KeyPress += new
System.Windows.Forms.KeyPressEventHandler(this.richTextBox1_KeyPress);
            //
            // richTextBox2
            //
            this.richTextBox2.BackColor = System.Drawing.SystemColors.ButtonFace;
            this.richTextBox2.Location = new System.Drawing.Point(12, 135);
            this.richTextBox2.Name = "richTextBox2";
            this.richTextBox2.Size = new System.Drawing.Size(355, 310);
            this.richTextBox2.TabIndex = 0;
            this.richTextBox2.Text = "";
```

```
            //
            // button1
            //
            this.button1.Location = new System.Drawing.Point(12, 464);
            this.button1.Name = "button1";
            this.button1.Size = new System.Drawing.Size(355, 53);
            this.button1.TabIndex = 1;
            this.button1.Text = "DÖNÜŞTÜR";
            this.button1.UseVisualStyleBackColor = true;
            this.button1.Click += new System.EventHandler(this.button1_Click);
            //
            // label1
            //
            this.label1.AutoSize = true;
            this.label1.Font = new System.Drawing.Font("Microsoft Sans Serif", 9.841726F,
System.Drawing.FontStyle.Regular, System.Drawing.GraphicsUnit.Point, ((byte)(162)));
            this.label1.Location = new System.Drawing.Point(12, 9);
            this.label1.Name = "label1";
            this.label1.Size = new System.Drawing.Size(57, 24);
            this.label1.TabIndex = 2;
            this.label1.Text = "GİRİŞ";
            //
            // label2
            //
            this.label2.AutoSize = true;
            this.label2.Font = new System.Drawing.Font("Microsoft Sans Serif", 9.841726F,
System.Drawing.FontStyle.Regular, System.Drawing.GraphicsUnit.Point, ((byte)(162)));
            this.label2.Location = new System.Drawing.Point(12, 108);
            this.label2.Name = "label2";
            this.label2.Size = new System.Drawing.Size(55, 24);
```

```
            this.label2.TabIndex = 3;
            this.label2.Text = "ÇIKIŞ";
            //
            // Form1
            //
            this.AutoScaleDimensions = new System.Drawing.SizeF(8F, 16F);
            this.AutoScaleMode = System.Windows.Forms.AutoScaleMode.Font;
            this.BackColor = System.Drawing.SystemColors.ControlDarkDark;
            this.ClientSize = new System.Drawing.Size(388, 543);
            this.Controls.Add(this.label2);
            this.Controls.Add(this.label1);
            this.Controls.Add(this.button1);
            this.Controls.Add(this.richTextBox2);
            this.Controls.Add(this.richTextBox1);
            this.Name = "Form1";
            this.Text = "Form1";
            this.ResumeLayout(false);
            this.PerformLayout();
        }
        #endregion
        private System.Windows.Forms.RichTextBox richTextBox1;
        private System.Windows.Forms.RichTextBox richTextBox2;
        private System.Windows.Forms.Button button1;
        private System.Windows.Forms.Label label1;
        private System.Windows.Forms.Label label2;
    }
}
using System;
using System.Collections.Generic;
```

```
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Windows.Forms;
using System.Collections;
namespace esnekkristografi
{
   public partial class Form1 : Form
   {
      public Form1()
      {
         InitializeComponent();
      }
            private void richTextBox1_KeyPress(object sender, KeyPressEventArgs e)
      {
                  if (char.IsDigit(e.KeyChar))// rakam tuşları kilitlendi
         {
            e.Handled = true;
         }
         if(char.IsWhiteSpace(e.KeyChar))  // boşluk tuşu kiliitlendi
         {
            e.Handled = true;
         }
         if(char.IsSymbol(e.KeyChar))     /// semboller kilitlendi
         {              e.Handled = true;
         }
         if (char.IsPunctuation(e.KeyChar))    // noktalama kilitlendi
```

```
{            e.Handled = true;
}
    }
private void button1_Click(object sender, EventArgs e)
{
   string girilenMetin = richTextBox1.Text;
   richTextBox2.Clear();
   if (girilenMetin.Length == 0)
   {
      MessageBox.Show("Giriş Yapın");
   }
   // tablonun oluşturulması ve metindeki harflerle değiştirilmesi
   else
   {
      // metinin harfleri diziye dönüştürülüyor
      string[] metinDizisi = girilenMetin.Select(c => c.ToString()).ToArray();
            // dizi değerleri sayıya dönüşüyor
      metinDizisi = metinDizisi.Select(s => s.Replace("a", "0")).ToArray();
      metinDizisi = metinDizisi.Select(s => s.Replace("b", "1")).ToArray();
      metinDizisi = metinDizisi.Select(s => s.Replace("c", "2")).ToArray();
      metinDizisi = metinDizisi.Select(s => s.Replace("ç", "3")).ToArray();
      metinDizisi = metinDizisi.Select(s => s.Replace("d", "4")).ToArray();
      metinDizisi = metinDizisi.Select(s => s.Replace("e", "5")).ToArray();
      metinDizisi = metinDizisi.Select(s => s.Replace("f", "6")).ToArray();
      metinDizisi = metinDizisi.Select(s => s.Replace("g", "7")).ToArray();
      metinDizisi = metinDizisi.Select(s => s.Replace("ğ", "8")).ToArray();
      metinDizisi = metinDizisi.Select(s => s.Replace("h", "9")).ToArray();
      metinDizisi = metinDizisi.Select(s => s.Replace("ı", "10")).ToArray();
      metinDizisi = metinDizisi.Select(s => s.Replace("i", "11")).ToArray();
```

```
            metinDizisi = metinDizisi.Select(s => s.Replace("j", "12")).ToArray();
            metinDizisi = metinDizisi.Select(s => s.Replace("k", "13")).ToArray();
            metinDizisi = metinDizisi.Select(s => s.Replace("l", "14")).ToArray();
            metinDizisi = metinDizisi.Select(s => s.Replace("m", "15")).ToArray();
            metinDizisi = metinDizisi.Select(s => s.Replace("n", "16")).ToArray();
            metinDizisi = metinDizisi.Select(s => s.Replace("o", "17")).ToArray();
            metinDizisi = metinDizisi.Select(s => s.Replace("ö", "18")).ToArray();
            metinDizisi = metinDizisi.Select(s => s.Replace("p", "19")).ToArray();
            metinDizisi = metinDizisi.Select(s => s.Replace("r", "20")).ToArray();
            metinDizisi = metinDizisi.Select(s => s.Replace("s", "21")).ToArray();
            metinDizisi = metinDizisi.Select(s => s.Replace("ş", "22")).ToArray();
            metinDizisi = metinDizisi.Select(s => s.Replace("t", "23")).ToArray();
            metinDizisi = metinDizisi.Select(s => s.Replace("u", "24")).ToArray();
            metinDizisi = metinDizisi.Select(s => s.Replace("ü", "25")).ToArray();
            metinDizisi = metinDizisi.Select(s => s.Replace("v", "26")).ToArray();
            metinDizisi = metinDizisi.Select(s => s.Replace("y", "27")).ToArray();
            metinDizisi = metinDizisi.Select(s => s.Replace("z", "28")).ToArray();
            //double pi = Math.PI;
            //string piSayisi = pi.ToString();  // c# kendi pi sayısını sadece 15 hane almıştır
            // bu yüzden kendi 𝑝𝑖 sayısı yazılır
            Random rnd = new Random();
            int fetDegeri = rnd.Next(2,10);  // fet deger aralığını fazla bulunuyorsa azaltılabilir,
            string piSayisi =
"3.14159265358979323846264338327950288419716939937510582097494459230781640628
620899862803482534211706798214808651328230664709384460955058223172535940812
848111745028410270193852110555964462294895493038196442881097566593344612847 5
648233786783165271201909145648566923460348610454326648213393607260249141273 7
245870066063155881748815209209628292540917153643678925903600113305305488204 6
652138414695194151160943305727036575959195309218611738193261179310511854807 4
462379962749567351885752724891227938183011949129833673362440656643086021394 9
```

463952247371907021798609437027705392171762931767523846748184676694051320005681271452635608277857713427577896091736371787214684409012249534301465495853710507922796892589235420199561121290219608640344181598136297747713099605187072113499999983729780499510597317328160963185950244594553469083026425223082533446850352619311881710100031378387528865875332083814206171776691473035982534904287554687311595628638823537875937519577818577805321712268066130019278766111959092164201989380952572010654858632788659361533818279682303019520353018529689955773622599413891249721775283479131515574857242454150695950829533116861727855889075098381754637464939319255060400927701671139009848824012858361603563707660104710181942955596198946767837449448255379774726847104047534646208046684259069491293313677028989152104752162056966024058038150193511253382430035587640247496473263914199272604269922796782354781636009341721641219924586315030286182974555706749838505494588586926995690927210797509302955321165344987202755960236480665499119881834797753566369807426542527862551818417574672890977727938000816470600161452491921732172147723501414419735685481613611573525521334757418494684385233239073941433345477624168625189835694855620992192221842725502542568876717904946016534668049886272327917860857843838279679766814541009538837863609506800642251252051173929848960841284886269456042419652850222106611863067442786220391949450471237137869609563643719172874677646575739624138908658326459958133904780275900994657640789512694683983525957098258226205224894077267194782684826014769909026401363944374553050682034962524517493996514314298091906592509372216964615157098583874105978859597729754989301617539284681382686838689427741559918559252459539594310499725246808459872736446958486538367362226260991246080512438843904512441365497627807977156914359977001296160894416948685558484063534220722258284886481584560285060168427394522674676788952521385225499546667278239864565961163548862305774564980355936345681743241125150760694794510965960940252288797108931456691368672287489405601015033086179286809208747609178249385890097149096759852613655497818931297848216829989487226588048575640142704775551323796414515237462343645428584447952658678210511413547357395231134271661021359695362314429524849371871101457654035902799344037420073105785390621983874478084784896833214457138687519435064302184531910484810053706146806749192781911979399520614196634287544406437451237181921799983910159195618146751426912397489409071864942319615679452080951465502252316038819301420937621378559566389377870830390697920773467221825625996615014215030680384477367

45492026054146659252014974428507325186660021324340881907104863317346496514539057962685610055081066587969981635747363840525714591028970641401109712062804390397595156771577004203378699360072305587631763594218731251471205329281918261861258673215791984148488291644706095752706957220917567116722910981690915280173506712748583222871835209353965725121083579151369882091444210067510334671103141267111369908658516398315019701651511685171437657618351556508849099898599823873455283316355076479185358932261854896321329330898570642046752590709154814165498594616371802709819943099244889575712828905923233260972997120844335732654893823911932597463667305836041428138830320382490375898524374417029132765618093773444030707469211201913020330380197621101100449293215160842444859637669838952286847831235526582131449576857262433441893039686426243410773226978028073189154411010446823252716201052652272111660396665573092547110557853763466820653109896526918620564769312570586356620185581007293606598764861179104533488503461136576867532494416680396265797877185560845529654126654085306143444318586769751456614068007002378776591344017127494704205622305389945613140711270004078547332699390814546646458807972708266830634328587856983052358089330657574067954571637752542021149557615814002501262285941302164715509792592309907965473761255176567513575178296664547791745011299614890304639947132962107340437518957359614589019389713111790429782856475032031986915140287080859904801094121472213179476477726224142548545403321571853061422881375850430633217518297986622371721591607716692547487389866549494501146540628433663937900397692656721463853067360965712091807638327166416274888800786925602902284721040317211860820419000422966171196377921337575114959501566049631862947265473642523081770367515906735023507283540567040386743513622224771589150495309844489333096340878076932599397805419341447377441842631298608099888687413260472156951623965864573021631598193195167353812974167729478672422924654366800980676928238280689964004824354037014163149658979409243237896907069779422362508221688957383798623001593776471651228935786015881617557829735233446042815126272037343146531977774160319906655418763979293344195215413418994854447345673831624993419131814809277771038638773431772075456545322077709212019051660962804909263601975988281613323166636528619326686336062735676303544776280350450777235547105859548702790814356240145171806246436267945612753181340783303362542327839449753824372058353114771199260638133467768796959703098339130771098704085913374641442822772634659470474587847787201927715280731767907707157213444730605700733492436935468

113835049316312840425121925651798069411352801314701304781643788518529092854520116583934196562134914341595625865865570552690496520985803385072242648293972858478316305777756068887644624824685792603953527734803048029005876075825104747091643961362676044925627420420832085661190625454337213153595845068772460290161876679524061634252257719542916299193064553779914037340432875262888963995879475729174642635745525407909145135711136941091193932519107602082520261879853188770584297259167781314969900901921169717372784768472686084900337702424291651300500516832336435038951702989392233451722013812806965011784408745196012122859937162313017114448464090389064495444006198690754851602632750529834918740786680881833851022833450850486082503930213321971551843063545500766828294930413776552793975175461395398468339363830474611996653858153842056853386218672523340283087112328278921250771262946322956398989893582116745627010218356462201349671518819097303811980049734072396103685406643193950979019069963955245300545058068550195673022921913933918568034490398205955100226353536192041994745538593810234395544959778377902374216172711172364343543947822181852862408514006660443325888569867054315470696574745855033232334210730154594051655379068662733379958511562578432298827372319898757141595781119635833005940873068121602876496286744604774649159950549737425626901049037781986835938146574126804925648798556145372347867330390468838343634655379498641927056387293174872332083760112302991136793862708943879936201629515413371424892830722012690147546684765357616477379467520049075715552781965362132392640616013635815590742202020318727760527721900556148425551879253034351398442532234157623361064250639049750086562710953591946589751413103482276930624743536325691607815478181152843667957061108615331504452127473924544945423682886061340841486377670096120715124914043027253860764823634143346235189757664521641376796903149501910857598442391986291642193994907236234646844117394032659184044378051333894525742399508296591228508555821572503107125701266830240292952522011872676756220415420516184163484756516999811614101002996078386909291603028840026910414079288621507842451670908700069928212066041837180653556725253256753286129104248776182582976515795984703562226293486003415872298053498965022629174878820273420922224533985626476691490556284250391275771028402799806636582548892648802545661017296702664076559042909945681506526530537182941270336931378517860904070866711496558343434769338578171138645587367812301458768712660348913909562009939361031029161615288138437909904231747336394804575931493140529763475748119356709110137751721028413

0803155902485309066920376719220332290943346768514221447737939375170344366199
1040337511173547191855046449026365512816228824462575916333039107225383742182
1408835086573917715096828874782656995995744906617583441375223970968340800535
5984917541738188399944697486762655165827658483588453142775687900290951702835
2971634456212964043523117600665101241200659755851276178583829204197484423608
0071930457618932349229279650198751872127267507981255470958904556357921221033
3466974992356302549478024901141952123828153091140790738602515227429958180724
7162591668545133312394804947079119153267343028244186041426363954800044800267
0496248201792896476697583183271314251702969234889627668440323260927524960357
9964692565049368183609003238092934595889706953653494060340216654437558900456
3288225054525564056448246515187547119621844396582533754388569094113031509526
1793780029741207665147939425902989695946995565761218656196733786236256125216
3208628692221032748892186543648022967807057656151446320469279068212073883778
1423356282360896320806822246801224826117718589638140918390367367222088832151
3755600372798394004152970028783076670944474560134556417254370906979396122571
4298946715435784687886144458123145935719849225284716050492212424701412147805
7345510500801908699603302763478708108175450119307141223390866393833952942578
6905076431006383519834389341596131854347546495569781038293097164651438407007
0736041123735998434522516105070270562352660127648483084076118301305279320542
7462865403603674532865105706587488225698157936789766974220575059683440869735
0201410206723585020072452256326513410559240190274216248439140359989535394590
9440704691209140938700126456001623742880210927645793106579229552498872758461
0126483699989225695968815920560010165525637568";

// pi sayının virgülden sonra fet degeri kadar silinir sonra girilen metinin harf sayısını fet degeri ile çarpıp bir çıkarır ve çıkan sonuç kadar çekilir

string islemeGirecekPiSayisi = piSayisi.Substring(2 + fetDegeri, (fetDegeri * girilenMetin.Length) - 1);

string[] piSayıDizisi = islemeGirecekPiSayisi.Select(c => c.ToString()).ToArray(); // pi sayı metini diziye dönüştü

ArrayList piSayıDizisiList = new ArrayList(); // dizi listeye dönüştürülüyor

piSayıDizisiList.AddRange(piSayıDizisi);

{

string[] metinDizisi = girilenMetin.Select(c => c.ToString()).ToArray();

```
                // dizi değerleri ikilik taban değerlerine dönştürülür
            metinDizisi = metinDizisi.Select(s => s.Replace("0", "0000")).ToArray();
            metinDizisi = metinDizisi.Select(s => s.Replace("1", "0001")).ToArray();
            metinDizisi = metinDizisi.Select(s => s.Replace("2", "0010")).ToArray();
            metinDizisi = metinDizisi.Select(s => s.Replace("3", "0011")).ToArray();
            metinDizisi = metinDizisi.Select(s => s.Replace("4", "0100")).ToArray();
            metinDizisi = metinDizisi.Select(s => s.Replace("5", "0101")).ToArray();
            metinDizisi = metinDizisi.Select(s => s.Replace("6", "0110")).ToArray();
            metinDizisi = metinDizisi.Select(s => s.Replace("7", "0111")).ToArray();
            metinDizisi = metinDizisi.Select(s => s.Replace("8", "1000")).ToArray();
            metinDizisi = metinDizisi.Select(s => s.Replace("9", "1001")).ToArray();
                    }
 for (int k = 1, i = 0; i < metinDizisi.Length; i++, k += fetDegeri+1) // pi sayısına harf kodları ilave edilir
 {
            piSayıDizisiList.Insert(k, metinDizisi[i]);
                    }
            piSayıDizisiList.Insert(0, fetDegeri.ToString());
            string[] piSayıDizisi2 = (string[])piSayıDizisiList.ToArray(typeof(string));
           // liste diziye dönüştürülür
            //
            //   dizi anahtar vasıtası ile harflere dönüştürülür
            piSayıDizisi2 = piSayıDizisi2.Select(x => x.Replace("0000", "N")).ToArray();
            piSayıDizisi2 = piSayıDizisi2.Select(x => x.Replace("0001", "E")).ToArray();
            piSayıDizisi2 = piSayıDizisi2.Select(x => x.Replace("0010", "V")).ToArray();
            piSayıDizisi2 = piSayıDizisi2.Select(x => x.Replace("0011", "Ş")).ToArray();
            piSayıDizisi2 = piSayıDizisi2.Select(x => x.Replace("0100", "H")).ToArray();
            piSayıDizisi2 = piSayıDizisi2.Select(x => x.Replace("0101", "İ")).ToArray();
            piSayıDizisi2 = piSayıDizisi2.Select(x => x.Replace("0110", "R")).ToArray();
```

```
            piSayıDizisi2 = piSayıDizisi2.Select(x => x.Replace("0111", "Ü")).ToArray();
            piSayıDizisi2 = piSayıDizisi2.Select(x => x.Replace("1000", "S")).ToArray();
            piSayıDizisi2 = piSayıDizisi2.Select(x => x.Replace("1001", "T")).ToArray();
            piSayıDizisi2 = piSayıDizisi2.Select(x => x.Replace("1010", "F")).ToArray();
            piSayıDizisi2 = piSayıDizisi2.Select(x => x.Replace("1011", "B")).ToArray();
            piSayıDizisi2 = piSayıDizisi2.Select(x => x.Replace("1100", "L")).ToArray();
            piSayıDizisi2 = piSayıDizisi2.Select(x => x.Replace("1101", "M")).ToArray();
            piSayıDizisi2 = piSayıDizisi2.Select(x => x.Replace("1110", "0")).ToArray();
            piSayıDizisi2 = piSayıDizisi2.Select(x => x.Replace("1111", "G")).ToArray();
            for (int i = 0; i < piSayıDizisi2.Length; ++i)
            {
               richTextBox2.Text += piSayıDizisi2[i].ToString(); ////  en sonda elde edilen dizi
metne dönüştürülür
               //if (i < piSayıDizisi2.Length)
               //    richTextBox2.Text += "";
            }
         }
      }
   }
}
```

2.3. Sonuç

Verilerin sayısal ortamda tutulması ile birlikte bilgi güvenliği günümüzün en önemli çalışma alanlarından biri haline gelmiştir. Kriptografi ve steganografi bilgi güvenliğinin en önemli çalışma alanlarındandır. Kriptografi, mevcut bilgiyi anlaşılmaz bir formata dönüştürdüğünden ortaya bir gizem çıkmaktadır. Bu durum oldukça dikkat çekmekte iken steganografide böyle bir durum söz konusu değildir. Dolayısıyla iki sistemin birleştirilmesiyle ortaya çıkacak olan kristografi sistemi birçok uygulama alanında bilgi güvenliğinin seviyesini artırmış olacaktır. Çünkü üçüncü kişi veya sistemler tarafından kriptografi sistemleri çözülerek açık metin elde edilebilir. Ancak elde edilecek metin steganografi örtüsünün içine gömülü olacağından gizli veri tamamen ele geçirilmiş olmayacaktır.

Bu bölümde kristografi sistemin programsal uygulanabilirliğini gösterebilmek amacıyla C# diliyle yazılmış bir sistem oluşturulmuştur. Bu sistemde 8 , 16 ve daha yüksek bitlik sistemlerle güvenlik seviyesi daha da arttırılmış olacaktır. fet değerinin küçük olması güvenliğin artırılmasını sağlanmış olacaktır. Sonuç olarak kullandığımız esnek steganografi yöntemini günümüzde hâlâ kullanılmakta olan modern kriptografi yöntemlerle kombine ederek çok daha güçlü ve daha kişileştirilebilir algoritmaların oluşturulabilmesine imkân tanıyacaktır. Bu yöntem DES, AES, RSA, vb. algoritmaları ile birleştirilebilir. Esnek kristografi ile ATM, kredi kartı, cep telefonu vb. şifre güvenlik programlarına uygulanarak güvenlik seviyelerinin yükseltmesine katkı sunulabilir.

Bu bölüm 2013 yılında gerçekleştirilen 26. ulusal matematik sempozyumunda “Mathematics and Security: Steganography and Cryptography" başlığı ile sunulmuştur. Ayrıca, 2014 yılında “An Application of the Crystography” başlığıyla ESCI ve Scopus indeksli, Journal of Mathematics and Computer Science dergisinde yayımlanmıştır.

BÖLÜM 3

KODLAMA TEORİSİ

3.1. Kodlama Teorisi

Son yıllarda, kuantum bilgisayarlarının yapım aşaması ve inşasında sürekli ilerleme kaydedilmiştir. Kuantum bilgisayarlarının ortaya çıkışı, mevcut tüm güvenlik sistemlerini yok edebilecek bir sürecin başlangıcı kabul edilmiştir. Bu tehlikenin farkında olan NIST, kuantum sonrası açık anahtar şifreleme algoritmalarının sunumu için 20 Aralık 2016 da "Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms" başlığı ile halka açık bir çağrı yayımlamıştır. Kasım 2017'ye kadar toplam 82 adayın çalışmaları NIST tarafından incelenmiştir. Aralık 2017'de NIST, bu adaylardan 69'unun hem başvuru koşullarını hem de asgari kabul kriterlerini karşıladığı ve standardizasyon sürecinin ilk turuna kabul edildiğini duyurulmuştur. İlk tur adayları için başvuru paketleri, halka açık inceleme ve yorum için https://www.nist.gov/pqcrypto adresinde çevrimiçi olarak yayımlanmıştır. Ocak 2019 yılında adayların kamuya açık geri bildirimlerine ve dâhili incelemelerine dayanarak NIST, standardizasyon sürecinin ikinci turuna geçmek için 26 algoritma seçmiştir. Bu 26 algoritmadan biri de yeniden tasarlanmış klasik McEliece algoritması olmuştur [130].

NIST post-kuantum kriptografi standardizasyon süreci ikinci tur durum raporunda, "Büyük ölçekli kuantum bilgisayarların kullanımı yaygınlaşırsa, güvenlik sistemlerinin temelinde yaygın olarak kullanılan birçok açık anahtarlı şifreleme sistemi ve dijital imza sistemlerinin güvenliğini tehdit edeceklerdir. Özellikle ayrık logaritmalar, çarpanlara ayırma ve eliptik eğri kriptografisine dayalı anahtar oluşturma şemaları ve dijital imzalar en ciddi şekilde etkilenenler olacaktır. Ancak blok şifre algoritmalı ve karma işlevler gibi simetrik kriptografik ilkeler daha az etkilenecektir. Bu probleme yanıt olarak kuantum sonrası kriptografi üzerine yoğun araştırmalar yapıldı. Bu bilimsel çalışmalar hem kuantum hem de klasik bilgisayarlara sahip düşmanlara karşı güvenli olacak şifreleme sistemleri üzerine yapılan çalışmalardır ve mevcut iletişim ağlarında ve protokollerinde büyük değişiklikler yapılmadan kullanılabilir. Bu hususlardan motive olan Ulusal Standartlar ve Teknoloji Enstitüsü (NIST), herkese açık, rekabete benzer bir süreç

aracılığıyla açık anahtarlı şifreleme algoritmalarını seçme sürecindedir," [130] şeklinde ifade etmişlerdir.

Ayrıca Taş ve Kiani'nin de belirtiği gibi, günümüz yeni dünya ekonomik sisteminin temelini oluşturan blok zincir tabanlı kripto para ödeme sistemleri oldukça popüler olmuştur. Güncel haliyle bitcoin fiyatı 40000 $'ı aşmış durumdadır ve kripto para işlem hacmi milyon dolarla ifade edilmektedir. Taş ve Kiani kripto para güvenlik sistemlerine yapılan saldırıları incelemişlerdir. Ulaştıkları sonuç "kriptografi algoritmaları incelenerek yeniden tasarlanmalı, ek protokollerle güçlendirilmeli ve blok zinciri sisteminin güvenli kalabilmesi için kuantum bilgisayarlara dayanıklı kriptografi algoritmalarının tasarlanması gerekmektedir." olmuştur [131].

Yeni açık anahtar şifreleme standartları, dijital imzalar, açık anahtar şifrelemesi ve anahtar oluşturma için bir veya daha fazla ek algoritma belirleyecektir. Yani mevcut sistemlerinde ek protokollerle geliştirilmesi gerekmektedir. Bu sebepler doğrultusunda çalışmamızda kodlama temelli McEliece kriptografi sistemine katkı sunmaya çalışılmıştır.

McEliece [122], genel kod çözme probleminin zorluğunu kullanarak cebirsel kodlama teorisine dayalı bir şifreleme sistemi önermiştir. Her ne kadar bir kriptografik yapı konu edinilmiş olsa da McEliece kodlama temeli kripto sistemdir. Bu sistemin arkasındaki fikir yüzeysel olarak aşağıdaki gibi açıklanabilir:

İyi bir kod çözme algoritmasına sahip bir C kodu alınır. Bu kod görünür bir yapısı olmayan yeni bir C' koduna dönüştürülür. Gönderici, C' kodunu kullanarak mesajı gönderir. Artık C' kodunun görünür bir yapısı olmadığı için, rastgele bir doğrusal kod kadar iyidir ve yetkisiz kişilerce çözülemez. Sistemi yaratan için C kodundan C' koduna dönüşümü geri döndürebilir ve C çerçevesinde çalışılabilir. C' iyi bir kod çözücüsü olduğu için başarıyla kod çözülebilir. Sisteme dışardan sızmaya çalışan için ise sistemi C' den C 'ye çevirmenin bir yolu olmadığı için bu çözülemez.

Bu bölümde esnek küme ve esnek grupların McEliece kripto-sistemine uygulanabilirliği üzerinde durulmuştur.

Grup kodları, kodlama teorisinde kullanılan bir tür kod türüdür. G sonlu bir abelyan grup olsun. G^n bir alt grubu olan n lineer blok kodu grup kodu olarak tanımlanır.

Grup kodları özel üreteç matrisleri ile oluşturulabilir. Bu matrislerin elemanlarının doğrusal blok kodlarının üreteç matrislerine benzeyen kodun alfabesindeki semboller yerine grubun endomorfizmleri bulunmaktadır.

Tanım 3.1.1. [123] F_q, q dizili bir sonlu cisim olsun. $\emptyset \neq V$ kümesi, F_q da seçilen skaler ile çarpma ve toplama işlemleriyle aşağıdaki şartları sağlıyorsa F_q üzerinde bir vektör uzayıdır. $\forall\, u, v, w \in V$ ve $\forall\, \mu, \lambda \in F_q$ olsun,

i. $u + v \in V$,
ii. $(u + v) + w = u + (v + w)$,
iii. $\forall\, v \in V$ için $\exists\, 0 \in V$ öyle ki $0 + v = v = v + 0$,
iv. $\forall\, u \in V$ için $\exists\, (-u) \in V$ öyle ki $u + (-u) = 0 = (-u) + u$ için,
v. $u + v = v + u$,
vi. $\lambda\, v \in V$,
vii. $\lambda(v + u) = \lambda v + \lambda u$ ve $(\lambda + \mu)v = \lambda v + \mu v$,
viii. $(\lambda\mu)v = \lambda(\mu v)$.

Tanım 3.1.2. [123] F_q üzerinde bir vektör uzayı V olsun. $\alpha_1, \alpha_2, \dots, \alpha_k \in F_q$ birer skaler çarpan olmak üzere $v_1, v_2, \dots, v_k \in V$ vektörlerinin lineer kombinasyonu

$$w = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_k v_k$$

ile tanımlanan bir vektördür.

Tanım 3.1.3. [123] V, F_q üzerinde bir vektör uzayı olsun. $v_1, v_2, \dots, v_k \in V$ vektörü için

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_k v_k = 0 \implies \alpha_1 = \alpha_2 = \cdots = \alpha_k = 0$$

koşulunu sağlıyor ise lineer bağımsızdır denir.

Aksi durumda α_i'lerden en az bir tanesi sıfırdan farklı ise V lineer bağımlıdır denir.

Tanım 3.1.4. [123] V, F_q üzerinde bir vektör uzayı ve $\emptyset \neq S = \{v_1, v_2, \dots, v_k\} \in V$ olsun**.** Öyleyse S'nin spanı

$$\langle S \rangle = \{\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_k v_k : \alpha_k \in F_q\}$$

olarak tanımlanır. Eğer S boş küme ise

$$\langle S \rangle = \{0\}$$

ile tanımlanır.

Tanım 3.1.5. [123] V, F_q üzerinde bir vektör uzayı olsun. Lineer bağımsız bir $\emptyset \neq B \subset V$ için

$$V = \langle B \rangle$$

olacak şekilde $B = \{v_1, v_2, \dots, v_k\}$ 'ye V'nin bir tabanı denir.
Bir vektör uzayı için her tabandaki elemanların sayısına o vektör uzayının boyutu denir. Bununla beraber bir vektör uzayının tün tabanları aynı sayıda elemanlar içerir.

Tanım 3.1.6. [123] $v = v_1, v_2, \dots, v_n \in F_q^n$ ve $w = w_1, w_2, \dots, w_n \in F_q^n$ olsun.

i. $w.v = w_1 v_1 + w_2 v_2 + \cdots + w_n v_n \in F_q$ ya w ile v'nin skaler çarpımı denir.

ii. Eğer $v.w = 0$ ise bu iki vektör ortogonaldir.

iii. F_q^n'nin boştan farklı bir altkümesi S olsun. O halde

$$S^{\perp} = \{v \in F_q^n : \forall s \in S \; için \; v.s = 0\}$$

ile gösterilir ve S'nin ortogonal komplementi denir.

Tanım 3.1.7. [123] G, m elemanlı bir halka olsun.

$$G^n = \{u = (u_1, u_2, \dots, u_n), u \in G\}$$

olmak üzere G kümesinin s elemanlı C alt modülüne, n uzunluklu, s elemanlı bir lineer kod denir ve (n, s) −lineer kod şeklinde ifade edilir. C kodunun herhangi bir elemanına kod sözcüğü adı verilir.

Tanım 3.1.8. [123] $u, v \in G^n$ kümesinin iki elemanı olmak üzere u ve v arasındaki Hamming uzaklığı $d(u,v) = |\{ i : u \neq v\}|$ ile tanımlanır.

$$d: G^n \times G^n \to \mathbb{N}^+$$
$$(u,v) \to d(u,v)$$

ile tanımlanan bu dönüşüm aşağıdaki özellikleri sağlar;

i) $\forall\, u,v \in G^n \, için \, d(u,v) \geq 0 \, , d(u,v) = 0 \Leftrightarrow u = v$,

ii) $\forall\, u,v \in G^n \, için \, d(u,v) = d(v,u)$,

ii) $\forall\, u,v,t \in G^n \, için \, d(u,v) \leq d(u,t) + d(t,v)$.

Tanım 3.1.9. [123] C kodunun minimum uzaklığı

$$d = d(C) = \min_{\substack{u,v \in C \\ u \neq v}} d(u\, v)$$

dır. Uzunluğu n, eleman sayısı S, minimum uzaklığı d olan bir C lineer kodu kısaca $(n, S, d\,)-$lineer kod ile gösterilir.

Tanım 3.1.10. [123,147] $x \in F_q^n$ olmak üzere x vektörünün sıfırdan farklı bileşenlerinin sayısına x vektörünün ağırlığı denir ve $w(x)$ ile gösterilir. Hamming ağırlığı ise $wt(x)$ ile gösterilir. Ayrıca

$$wt(x) = d(C, 0)$$

dır.

C kodunun sıfırdan farklı tüm kod sözcükleri ağırlıklarının en küçüğüne C kodunun minimum ağırlığı denir. Minimum ağırlık $w(C)$ ile gösterilir.

Örnek 3.1.11. [123] $C = \{0001000, 0001110\, , 0111100, 0000000, 1111111\}$ olsun.
(0001000): Bu kodun sıfırdan farklı bir tane kod sözcüğü vardır. Dolayısıyla $w(0001000) = 1$ olur.
(0001110): Bu kodun sıfırdan farklı bir tane kod sözcüğü vardır. Dolayısıyla $w(0001110) = 3$ olur.

(0111100) Bu kodun sıfırdan farklı bir tane kod sözcüğü vardır. Dolayısıyla $w(0111100) = 4$ olur.
(0000000): Bu kodun sıfırdan farklı bir tane kod sözcüğü vardır. Dolayısıyla $w(0000000) = 0$ olur.
(1111111): Bu kodun sıfırdan farklı bir tane kod sözcüğü vardır. Dolayısıyla $w(1111111) = 7$ olur.
Öyleyse C konunu minimum ağırlık $w(C) = 1$ dir.

Önerme 3.1.12. $x, y \in F_q^n$ olmak üzere $d(x, y) = w(x - y)$.

Tanım 3.1.13. [123] p bir asal sayı, $n \in \mathbb{N}$ olmak üzere $q = p^n$ elemanlı cisme Galois cismi denir. $GF(q)$ veya F_q ile gösterilir.

Tanım 3.1.14. [123] $V(n, q) = F_q^n = \{x = (x, x, \dots, x): x \in F\}$ kümesi F_q üzerinde n boyutlu bir vektör uzayı olmak üzere, F_q^n in bir C alt uzayına bir lineer kod denir. C, F_q^n vektör uzayının k boyutlu bir alt uzayı ise C bir $[n, k]$-lineer koddur, d minimum uzaklığı da belirtilmek isteniyorsa C bir $[n, k, d]_q$-lineer koddur denir. C, bir $[n, k, d]_q$ -lineer kod ise kodun eleman sayısı q^k kodun oranı $\frac{n}{k}$ dır.

Tanım 3.1.15. [123] C bir lineer kod ise satırları C kodunun bir baz vektörlerinden oluşan $k \times n$ boyutlu G matrisine, C kodunun üreteç matrisi denir. Yani C kodunun kod kelimeleri, G matrisinin satırlarının lineer birleşimidir. Burada

$$C = \{xG | \, x \in V(k, q)\}$$

dır.

Tanım 3.1.16. [123] G üreteç matrisi, $k \times k$ mertebeli birim matris I_k ve A da $k \times (n - k)$ mertebeli bir matris olmak üzere $(I_k|A)$ şeklinde ki bir matrise denktir. G matrisinin bu formuna G matrisinin standart formu adı verilir.

Tanım 3.1.17. [123] C bir lineer $[n, k]$ −kod olsun. O zaman C lineer kodunun duali

$$C^{\perp} = \{y \in V(n, q) | \langle y, x \rangle = 0, \forall x \in C\}$$

dir. Burada $(C^{\perp})^{\perp} = C$ olur.

Tanım 3.1.18. [123] C bir kod ve $G = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix} = (I_2|A)$

üreteç matrisi de $G = (I_k|A)$ olmak üzere $GH^T = 0$ koşulunu sağlayan

$$H = (-A^T|I_k)$$

matrisine ise C kodunun kontrol matrisi denir.

Örnek 3.1.19. [123] $C = \{00000,10110,01011,11101\}$ olsun. Bu lineer kodun üreteç matrisi

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix} = (I_2|A)$$

standart formundadır.

Ayrıca $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ ve $A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ olsun. O zaman C kodunu kontrol matrisi ise, $H = (-A^T|I_{n-k})$ ile ifade edileceğinden

$$H = (-A^T|I_3)$$

olur. Buradan da $-A^{\perp} = A^{\perp}$ olacağından

$$H = (-A^T|I_3) = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

elde edilir. H kontrol matrisi $C^{\perp}$ kodunun üreteç matrisi olduğu için H matrisi satırlarının lineer toplamı $C^{\perp}$ kodunun elemanları olan kod kelimelerini verir. Buradan

$$C^{\perp} = \{00000,10100,11010,01001,11101,10011,00111\}$$

elde edilir.

Sonuç 3.1.20. [147] F_q cismi üzerindeki bir (n, k) lineer C kodunun duali, F_q cismi üzerinde bir $(n, n-k)$ lineer koddur.

Tanım3.1.21. [147] Herhangi bir (n,k) lineer C kodu için $C^{\perp}$'nin üreteç matrisine C kodunun eşlik denetim matrisi denir.

Tanım 3.1.22. [147] $H \in F_q^{(n-k)\times n}$ formundaki bir (n,k) lineer C kodu için

$$C = \{c \in F_q^n \,|\, Hc^T = 0\}$$

olur.

Tanım 3.1.23. [147] F_q üzerinde n uzunluğundaki herhangi bir C lineer kodu F_q^n cisminin bir alt uzayıdır.

Aşağıda kodlama teorisinde en çok kullanılan kod çeşitleri verilecektir.

Tanım 3.1.24. [147] (LRPC kodlar) F_{q^m} cismi üzerinde d ranklı, n uzunluğunda ve k boyutunda bir LRPC kod $(n-k)\times n$ boyutunda ve $H = (h_{i,j})$ eşlik denetim matrisine sahiptir. F_{q^m} cisminin H matrisinin elemanlarıyla üretilen alt vektör uzayının boyutu en fazla H matrisinin ağırlığı olan d kadardır ve $\{F_1, F_2, \dots, F_d\}$ ile gösterilir.

Örnek 3.1.25. [147] F_{2^4} cismi üzerinde $e = (0,0,\alpha,0,\alpha,0)$ hata vektörü olsun. e vektörünün bileşenlerinden oluşan 1 boyutlu E alt vektör uzayı ise $\{a\}$ bazı ile gösterilir.

Tanım 3.1.26. [147] (Koppa Kodlar) $\Gamma(L, g(z))$ Goppa kodu F_{q^m} cisim genişlemesi üzerinde t dereceli $g(z)$ Goppa polinomu ve F_{q^m} cisminin L altkümesi ile tanımlanır.

$$g(z) = g_1 z + g_2 z^2 + \cdots + g_t z^t = \sum_{i=0}^{t} g_i z^i$$

$$L = \{\alpha_1, \alpha_2, \dots, \alpha_n\} \subseteq F_{q^m}$$

$g(\alpha_i) \neq 0$ ve $\forall \alpha_i \in L$ için F_q üzerinde bir $c = c_1, c_2, \dots, c_n$ vektörü $R_c(z) = \sum_{i=0}^{t} \frac{c_i}{z-\alpha_i}$

ile tanımlanır. Burada

$$(z-\alpha_i)\cdot\frac{c_i}{z-\alpha_i} \equiv 1 \left(mod\ g(z)\right)$$

denkliğini sağlayan polinomlar tersinirdir.

Tanım 3.1.27. [148] (Hamming kodu) $r \geq 2$ olmak üzere uzunluğu $n = 2^r - 1$ ve eşlik denetim matrisi, sütunları F_2^r nin sıfırdan farklı vektörlerinden oluşan bir matris olan ikili koda bir ikili Hamming kodu denir. Bu kodu $Ham(r, 2)$ ile gösterilir.

Tanım 3.1.28. [148] (Golay Kodları) A matrisi 12×12 bir karesel matris ve $G = (I_{12}|A)$ olmak üzere üreteç matrisi G_{24} olan ikili doğrusal koda genişletilmiş ikili Golay kodu denir ve g ile gösterilir. Bu kodların uzunluğu 24 ve boyutları ise 12 dir.

Tanım 3.1.29. [148] (Reed-Muller Kodları) $\forall\, m \geq 1$ tam sayısı için aşağıdaki gibi özyineli (recursive) olarak tanımlanan ve $R(1, m)$ ile gösterilen kodlara Reed-Muller kodları denir.

i. $R(1,1) = F_2^2\ dir.$

ii. $m \geq 1$ için, $R(1, m+1) = \{(u, u) : u \in R(1, m)\} \cup \{(u, u+1) : u \in R(1, m)\}$ olur.

Tanım 3.1.30. [148] (Devirli Kodlar) $C \subseteq F_q^n$ için eğer $(a_0, \dots, a_{n-2}, a_{n-1}) \in C$ iken $(a_{n-1}, a_0, \dots, a_{n-2}) \in C$ oluyorsa C kümesine devirli kod denir. Eğer C lineer kodu devirli ise bu C koduna devirli kod denir.

Tanım 3.1.31. [148] (BCH kodlar) $\alpha \in F_q^n$ cisminin bir ilkel elemanı olmak üzere α^i elemanının F_q üzerinde minimal polinomu $M^i(x)$ ve $\delta \geq 2$ bir tam sayı olsun. Bir $a \in \mathbb{Z}$ için

$$g(x) = ekok(M^{(a)}(x), M^{(a+1)}(x), \dots, M^{(a+\delta+1)}(x))$$

polinomu tarafından üretilen $q-$lu devirli koda uzunluğu $n = q^m - 1$ ve tasarlanmış uzaklığı δ olan F_q üzerinde BCH (Binary Coded Hexadecimal) kod denir.

Tanım 3.1.32. [123] (Reed Solomon Kodlar) Reed Solomon (RS) kodları ikili olmayan sabit k ve n değerleri için minimum Hamming uzaklığa sahip kodlardır. Reed Solomon kodlar BCH kodlarının bir alt kümesidir.

3.2. Esnek Matris Tabanlı AES Algoritması

Esnek küme ve esnek grup gibi esnek cebirsel yapıların kriptografiye de uygulanabilir olduğu tezi ilk defa 2014 yılında Kalkan ve Zararsız tarafından ortaya atılmıştır. Daha sonra Aygün ve Kılıç tarafından "Soft Matrix Product and Soft Cyrptosystem" başlığıyla ilk kez esnek yapılar üzerine kriptografi sistemi tanımlanmıştır. Aygün "AES Şifreleme ve Esnek Küme Yardımıyla Elde Edilen Yeni Bir Kriptosistem" [143] adlı çalışması yayımlandı. Bu çalışmada esnek kriptografi sistemi esnek matrislerin ters (invers) çarpımı ve karakteristik çarpımını kullanarak tasarlanmıştır. Ayrıca esnek şifreleme ve esnek deşifreleme tanımlanarak AES şifreleme sistemi ile mukayese edilmiştir [144].

Rehman ve arkadaşları [162] ile Abdullah ve Amin [160], çalışmalarında görüntü şifrelemede kullanılan S-kutularını esnek fuzzy kümeler üzerine tanımlamışlardır. Razzaque ve arkadaşları [163] da şifrelemede kullanılan esnek fuzzy kümeler üzerine tanımlanmış olan S-kutularını istatistiki analize uyarlamıştır. Benzer bir çalışmada ise Khalaf [164] görüntü şifrelemede kullanılan esnek fuzzy kümeler üzerine tanımlanmış olan S-kutularını karar verme kriterlerinde kullanmıştır. Buna ek olarak Shah [161] da sezgisel fuzzy esnek kümlerinin karar verme kriterlerinde kullanılan blok şifrelemeye uyarlamıştır.

Rahman ve arkadaşları, FS (esnek bulanık) toplama operatörü kullanarak şifreleme algoritmalarında kullanılan S-kutucuklarının görüntü şifreleme uygulamasına uygunluğunu ve doğruluğunu analiz edebilmek için bulanık esnek küme teorisini kullanmışlardır [149].

Tanım 3.2.1. [142-144] U evrensel küme ve E parametrelerin bir kümesi, $P(U)$, U'nun kuvvet kümesi ve $A \subset E$ olsun. $f_A: A \to P(U)$ olmak üzere bir (f_A, A) sıralı ikilisi U üzerinde esnek küme olarak adlandırılır.

Öyleyse (f_A, E) ikilisi U üzerinde bir esnek küme olsun. Bu durumda $U \times E$'nin

$$R_A = \{(u, e): e \in A, u \in f_A(e)\}$$

alt kümesine (f_A, E) ikilisinin bağıntı formu denir.

R_A'nın karakteristik fonksiyonu X_{R_A} aşağıdaki şekilde tanımlanır,

$$X_{R_A}: U \times E \to \{0,1\}$$

$$(u,e) \to X_{R_A}(u,e) = \begin{cases} 1, & (u,e) \in X_{R_A} \text{ ise} \\ 0, & (u,e) \notin X_{R_A} \text{ ise} \end{cases}$$

Eğer $a_{ij} = X_{R_A}(u,e)$ olursa $[a_{ij}] = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix}$ matris U üzerinde (f_A, E) esnek kümesinin esnek matris denir.

U üzerindeki tüm esnek matrisler kümesi $SM_{m\times n}$ ile gösterilecektir.

Tanım 3.2.2. [142-144] $[a_{ij}] \in SM_{m\times n}$ olmak üzere;

i. $\forall\, i,j$ için $a_{ij} = 0$ ise $[a_{ij}]$ ye sıfır esnek matrisi denir ve $\begin{bmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{bmatrix} = [0]$ şeklinde gösterilir.

ii. $\forall\, i,j$ için $j \in I_A = \{j : e_j \in A\}$ ve $a_{ij} = 1$ ise $[a_{ij}]$ ye A-evrensel esnek matrisi denir ve $[\tilde{a}_{ij}]$ şeklinde gösterilir.

iii. $\forall\, i,j$ için $a_{ij} = 1$ ise $[a_{ij}]$ ye evrensel esnek matrisi denir ve $[a_{ij}]$ şeklinde gösterilir.

Tanım 3.2.3. [142-144] $[a_{ij}], [b_{ij}] \in SM_{m\times n}$ olsun. $[a_{ij}]$ ve $[b_{ij}]$ nin invers çarpımları "$\cdot_i$" sembolü ile gösterilir.

$[a_{ij}] \cdot_i [b_{ij}] = [c_{ij}]$ olmak üzere bu çarpımda $\forall\, i = 1,2,\dots,m$ ve $\forall\, j = 1,2,\dots,n$ için

$$c_{ij} = \begin{cases} 1, & a_{ij} \neq b_{ij} \text{ ise} \\ 0, & a_{ij} = b_{ij} \text{ ise} \end{cases}$$

olarak verilir.

Tanım 3.2.4. [142-144] $[a_{ij}], [b_{ij}] \in SM_{m\times n}$ olsun. $[a_{ij}]$ ve $[b_{ij}]$ nin karakteristik çarpımları "$\cdot_c$" sembolü ile gösterilir.

$[a_{ij}] \cdot_c [b_{ij}] = [c_{ij}]$ olmak üzere bu çarpımda $\forall\, i = 1,2,\dots,m$ ve $\forall\, j = 1,2,\dots,n$ için

$$c_{ij} = \begin{cases} 1, & a_{ij} = b_{ij} \text{ ise} \\ 0, & a_{ij} \neq b_{ij} \text{ ise} \end{cases}$$

ile gösterilir.

Tanım 3.2.5. [142-144] Herhangi bir esnek karesel matris $S \in SM_{5\times5}$ için bir $\pi \in S_5$ permütasyon grubuna göre düzenlenebilir. $\pi \in S_5$ esnek matrisin satırlarında bulunan her bir elemanı, verilen sıraya göre yer değiştirir.

Örnek 3.2.6. [142-144] $\pi = (12453)$ ve $S \in SM_{5\times5}$ matrisi aşağıdaki şekilde verilsin,

$$S = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}_{5\times5}$$

S esnek matrisinin her satırı $\pi = (12453)$'ye göre yeniden düzenlenir. Bu dizilim

$$1 \rightarrow 2 \rightarrow 4 \rightarrow 5 \rightarrow 3 \rightarrow 1$$

şeklinde olacaktır. Bu işlem kriptografik algoritmalarında satır kaydırma işlemi olarak da adlandırılır. Bu işlem ilk satıra uygulandığında ilk satır 011111'e dönüşür. Sırasıyla diğer satırlara kaydırma işlemi uygulandığında elde edilecek esnek matris S_π matrisidir.

$$S_\pi = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix}_{5\times5}$$

3.3. Kod Tabanlı McEliece Kriptografi Sistemi

Tanım 1.38 [122] M üreteç matrisi, $[n,k]$ doğrusal kod C'yi ve $\mathcal{E}$ ise C tarafından düzeltilebilir hataların sayısı olsun. McEliece kripto-sistemi aşağıdaki şekilde tanımlanır:

Açık Anahtar: $M' = SMP$

Gizli anahtar: (S, M, P) dir, burada $S \in GL_k(F_2)$ ve P ise $n \times n$ permütasyon matrisi alınsın,

Şifreleme:

k-bit'li açık metin $p \in F_q^k$ alınır. e bir rastgele hata vektörü ve $wt(e) \leq \mathcal{E}$ için

$c = pM' + e$ fonksiyonu ile elde edilen şifreli metindir.

Deşifreleme:

Alınan c şifreli metini aşağıda deşifreleme işlemine tabi tutularak düz metine geri döndürülür;

$$cP^{-1} = (pM' + e)P^{-1} = (pSMP + e)P^{-1} = pSM + e_2$$

elde edilir.

3.4. Kod Tabanlı Esnek McEliece Kriptografi Sistemi

Tanım 3.4.1. (Esnek McEliece Algoritması) Esnek McEliece kriptografi sistemi aşağıdaki parametreleri sağlayan sistemdir.

- $n \times k$ boyutlu üreteç matrisi G,
- $k \times k$ boyutlu tersinir esnek matrisi S_{π},
- $n \times n$ permütasyon matrisi P,
- $k = n - td$ boyutlu Goppa kodu $\Gamma(\alpha_1, \alpha_2, \dots, \alpha_n, g)$,
- n, k, t açık anahtar sistemi parametreleridir,
- $\alpha_1, \alpha_2, \dots, \alpha_n, g, P, S_{\pi}$ ise gizli anahtar sistemi parametreleri,
- Tesadüfi hata vektörü e,
- Esnek McEliece açık anahtarı $k \times n$ boyutlu $S_{\pi}GP$ matrisi olsun,

Şifreleme:

Esnek McEliece kriptografi sistemi k uzunluğundaki m mesajını şifrelerken $mS_{\pi}GP$ matrisini hesaplar. t ağırlığında ve n uzunluğuna sahip tesadüfi e hata vektörünü ekleyerek

$$c = mS_{\pi}GP + e$$

Goppa kod kelimesini elde ederek gönderir.

Deşifreleme:

Göndericiden gelene c şifreli metinini açık metine dönüştürmek için $c \cdot_i P^{-1}$ hesaplanır.

$$c = mS_{\pi}GP + e$$

kod kelimeleri $\cdot_i P^{-1}$ ile çarpılarak

$$c \cdot_i P^{-1} = (mK + e) \cdot_i P^{-1} = (mS_\pi GP + e) \cdot_i P^{-1}$$

$$= mS_\pi GP \cdot_i P^{-1} + e \cdot_i P^{-1} = mS_\pi G + e \cdot_i P^{-1}$$

elde edilir. Burada $e \cdot_i P^{-1}$ hata permütasyonunun maksimum ağırlığı t ve e nin ağırlığı ile aynıdır. Dolayısıyla bu hata Goppa kodu tarafından düzeltilebilir, yani sistem $e \cdot_i P^{-1}$ hata matrisini hesaplayarak düzeltir. $mS_\pi G$ esnek kod kelimesi Γ'nun bir elemanıdır. Burada Petterson kod çözme algoritması kullanılır. Yani $mS_\pi G = (mS_\pi)G$ kod kelimeleri $k - 1$ kez çözülerek mS_π elde edilir. Buradan da $mS_\pi \cdot_c S_\pi^{-1} = m$ elde edilir.

3.5. Sonuç

Quantum sonrası kriptografi çalışmaların gereksinimleri doğrultusunda çalışmamızda kodlama temelli McEliece kriptografi sistemi [122] ve esnek matris çarpımları [142] kullanılarak elde edilen esnek kriptografi sistemlerinin kombine edilmesi ile elde edilen esnek McEliece kriptografi sistemi oluşturulmuştur.

BÖLÜM 4

KRİPTOGRAFİ

4.1. Kriptografi

Kriptografinin en temel amaçlarından biri, birbirleri ile iletişim ağı kuran iki tarafın güvenli olmayan bir iletişim kanalı üzerinde güvenli bir şekilde iletişim kurabilmelerine olanak sağlamaktır. Geleneksel olarak, iki tarafın da önceden bir "gizli anahtarı" güvenli bir şekilde paylaşma yoluna ihtiyaç duyacağı ve daha sonra mesajlarını şifrelemek için bu gizli anahtarı kullanabileceği varsayılmıştır. 1976'da, Diffie ve Hellman [76] tarafından, sırlarını önceden paylaşmamış olan taraflar arasında bile güvensiz bir kanalda güvenli iletişimin yapılabileceğini gösteren bir makale yayımlandı. Oluşturdukları sistemin yapısı devirli gruplara, üstelleştirme ve ayrık logaritmalar arasındaki karmaşıklığın varsayılmış boşluğuna dayanıyordu. Bu çalışma sonrasında anahtar değişim protokollerinde Thompson grubu, matris grupları, sadeleştirme grupları, Braid grupları, Artin grupları, permütasyon grubu eşlemeleri, Grigorchuck grubu, sonlu grup eşlemeleri, polisiklik gruplar, devirli gruplar, çözülebilir gruplar vb. tabanlı güçlü kriptografi algoritmaları oluşturulmuştur. Daha detaylı bilgi için bu kaynaklar incelenebilir [42], [61], [70], [72-74], [77], [79], [80], [82], [113-117], [128], [137], [146]. Kriptografik algoritmalarının birbirlerine karşı güçlü ve zayıf yönleri vardır. Bilgi korumanın ve güvenli bir şekilde aktarmanın temelinde güvenli bir algoritmanın yanında anahtar değişim protokolleri de ciddi önem taşımaktadır. Ancak tüm bu sistemlerde çeşitli problemlerle karşılaşılmaktadır. Kriptografi sistemlerinde karşılaşılan en önemli problemler şunlardır:

- DHP: (Diffie-Helman problem)
- MSP: (The membership search problem)
- CSP: (Conjugacy search problem)
- FSP: (The factorization search problem)

- WP: (The word problem)
- DSP: (The decomposition search problem)
- GFP: (Generalized factor problem)
- KEP: (Key exchange problem)
- DLP: (Discrete logarithm problem)
- IP: (The isomorphism problem)

Bu ve benzeri problemlerin üstesinden gelebilmek için kriptografik algoritmalarda farklı yaklaşımlar ve yöntemler çalışılmıştır. Bu çalışmalardan biride grup tabanlı kriptografi algoritmaları ve grup tabanlı anahtar değişim protokolleri gelişimine esnek yapılarla katkı sunmaktır. Blackburn, Cid ve Mullan [4], RSA ve Diffie-Hellman algoritmalarında grup teorisinin kullanılmasında pratik bir sonuca ulaşılamayacağını ancak ilginç sonuçların ortaya çıkabileceğinden bahsetmişlerdir.

Günümüz kriptografi algoritmaları ve sistemleri, kuantum bilgisayarların varlığı ile birlikte ciddi bir tehlike ile karşı karşıya kalmıştır. En güçlü algoritmaya sahip RSA sistemini klasik bilgisayarlar ile 100 yıldan fazla sürecek bir çaba sonucunda ancak kırılabileceği varsayılırken, kuantum bilgisayarlar ile haftalar hatta günlerle ifade edilecek kadar kısa bir zamanda kırılabileceği varsayılmaktadır. Bu konunun oldukça endişe verici olması araştırmacıların hem açıklamalarına hem de çalışmalarına yansımıştır. Örneğin, Cook “Büyük kuantum bilgisayarlar pratik hale gelirse ve olduklarında, büyük astarların ürününü verimli bir şekilde hesaba katabilirler ve böylece RSA'yı kırabilirler. Ayrık logaritma ve eliptik ayrık logaritma problemlerini, Diffie-Hellman ve eliptik eğri şifreleme sistemlerini kırarak da çözebilirler. Şu anda ortak kullanımda olan tüm açık anahtarlı şifreleme sistemleri kırılacaktır. Kuantum bilgisayarlar yokken neden şimdi bunun için endişelenelim? Bunun nedeni; şifreleme yöntemlerini geliştirmenin, analiz etmenin, standartlaştırmanın ve devreye almanın oldukça uzun sürmesidir. Bir de ileriye dönük güvenlik sorunları var. Örneğin herhangi bir kişi gelecekte şifresini çözmek umuduyla şifrelenmiş mesajları saklayabilir. Bu, TLS üzerinden iletilen kedi fotoğrafları için önemli değil, ancak devlet

sırları için önemli olabilir; hükümetler, onlarca yıldır gizli tutmak istedikleri belgeleri şifreliyor olabilir. NIST, kuantuma dayanıklı şifreleme yöntemlerini geliştirmek ve standartlaştırmak için bir yarışmaya sponsorluk yapıyor [150].” demiştir.

Yeni anahtar değişim protokolleri ve şifreleme yöntemlerini geliştirmek, test etmek ve uygulamak yıllar almaktadır. Bu nedenle araştırmacılar, ihtiyaç duyulduğunda kuantuma dirençli şifreleme yöntemlerine yönelik çalışmalar hız kazanmıştır. “Post Quantum” başlığı ile google arama motoruna yazıldığında 258 milyon sonuç bulunmakta, yine Google akademik arama motorunda tarandığında ise 2290000 adet akademik çalışma sonucu bulunmaktadır. Bu sonuçlardan kuantum sonrası çalışmaların önemi ve gerekliliği ortaya çıkmaktadır.

Bu bağlamda esnek yapılar kullanılarak mevcut sistemlerini temel yapısı değiştirilmeden uygun parametre ve esnek fonksiyonlar kullanılarak kişiselleştirilebilir yapılar oluşturmak mümkün görülmektedir.

4.2. Grup Bazlı Kriptografi

Bu bölümde öncelikle grup tabanlı protokoller ve grup tabanlı kriptografik sistemlerin temel problemleri verilecektir. Daha sonra üzerinde esnek yapılar uygulanabilen anahtar değişim protokolleri incelenerek esnek anahtar değişim protokolleri inşa edilecektir.

Tanım 4.2.1. [75,173] Diffie-Hellman Anahtar Değişim Protokolü

Diffie ve Hellman anahtar değişim protokolü $G = \langle g \rangle$ sonlu devirli grup tabanlı çalışan bir protokoldür. Bu protokolde g ve grubun mertebesi p açıktan yayımlanır. Alice ve Bob rastgele $a, b \in [2, d-1]$ tam sayılarını ile g ve p kullanarak gizli iletişim anahtarlarını elde edecekleri protokol aşağıdaki şekilde verilmiştir;

i. Alice rastgele a tam sayısını seçer ve $g^a(mod\ p)$ 'yi hesaplayarak Bob'a gönderir,

ii. Aynı yöntemle Bob b'yi seçer $g^b(mod\ p)$'yi hesaplayarak Alice'ye gönderir,

iii. Alice $g^{ba}(mod\ p) = (g^b)^a(mod\ p)$'yi hesaplarken,

Bob $g^{ab}(mod\ p) = (g^a)^b(mod\ p)$'yi hesaplar.

iv. Dolayısıyla hem Alice hem de Bob

$$g^{ba}(mod\ p) = g^{ab}(mod\ p) = K \in G$$

ortak anahtarını elde ederler.

Tanım 4.2.2. Ko-Le Anahtar Değişim Protokolü

Bu protokolün en önemli özelliği, platform olarak kullandığı gruplardır. Ko ve arkadaşları, Braid gruplarını platform olarak kullanmışlardır. A ve B grupları B_n Braid grubunun birer alt grupları olmak üzere;

$$B_n = \left\langle \begin{matrix} \sigma^1, \sigma^2, \dots\dots, \sigma^{n-1}, \mid \sigma_i\sigma_j = \sigma_j\sigma_i \\ \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j \text{ for } |i-j| = 1 \end{matrix} \right\rangle$$

şeklinde verilir. Burada $s, t \in \mathbb{Z}$ için $s + t = n$ alınarak

$$A = \langle \sigma_1, \sigma_2, \ldots\ldots, \sigma_{s-1} \rangle$$

ve

$$B = \langle \sigma_{s+1}, \sigma_{s+2}, \ldots\ldots, \sigma_{s+t-1} \rangle$$

şeklinde tanımlanmıştır.

G abelyan olmayan bir grup, $g \in G$ de herkes tarafından bilinen bir eleman ve $A, B \leq G$ abelyan altgruplar olsun. Alice ve Bob'un üreteceği ortak gizli anahtar prosedürü aşağıda verildiği gibidir;

i. Alice $a \in A$'yı seçer ve $g^a = a^{-1}ga$ sayısını hesaplayarak Bob'a gönderir.

ii. Bob $b \in B$'yi seçerek $g^b = b^{-1}gb$ sayısını hesaplayarak Alice'e gönderir.

iii. Alice $K_a = (g^b)^a$ 'yı anahtar olarak oluştururken, Bob da $K_b = (g^a)^b$ 'yı oluşturur.

Buradan $ab = ba$ olduğundan, bu işlem soncunda

$$K = K_a = K_b$$

ortak gizli anahtarı oluşturulmuş olur [10-11], [152-153].

Braid gruplarının grup çarpma işlemi ile ters alma işlemlerini sağladığı avantajlardan dolayı platform olarak seçilirler. Ancak A, B birer sonlu küme olmadığından a ve b elemanlarının seçimi açık değildir.

Tanım 4.2.3. Stickel Anahtar Değişim Protokolü

$G = GL(n, F_q)$ ve $g \in G$ verilmiş olsun. Mertebeleri sırasıyla n_a ve n_b olan $a, b \in G$ için $ab \neq ba$ olsun. Burada G grubu ve a, b elemanları açıktan yayımlandığından herkes tarafından bilinmektedir. Gizli anahtar oluşturma prosedürü şu şekilde olacaktır [78], [173];

i. Alice $0 < l < n_a$ ve $0 < m < n_b$ olmak üzere l, m tam sayılarını tekdüze ve rastgele seçer,
ii. Alice $u = a^l g b^m$'yi hesaplayarak Bob'a gönderir,
iii. Bob ise $0 < r < n_a$ ve $0 < s < n_b$ olmak üzere r, s tam sayılarını tekdüze ve rastgele seçer,
iv. $v = a^r g b^s$'yi hesaplayarak Alice'e gönderir,
v. Alice $k_a = a^l v b^m = a^{l+r} g b^{m+s}$ hesaplar,
vi. Bob da $k_b = a^r u b^s = a^{l+r} g b^{m+s}$ hesaplar,
vii. Böylece paylaştıkları, $K = k_a = k_b$ ortak anahtarı oluşturulur.

Tanım 4.2.4. [84] $C = [c_{ij}]_{n\times n}$ bir n-kare matris olmak üzere elemanları

$$c_{ij} = c_{0,j-i} = c_{j-i}, \qquad j - i \equiv k \ (mod\ n)$$

şartını sağlayan $n \times n$ mertebeli C matrisine sirkülant matris denir.

$n\times n$ mertebeli sirkülant matris n elemanlı bir vektör ile temsil edilir ve bu vektör, matrisin ilk satırını oluşturur. Böylece takip eden satırlar önceki satırın son elemanını başa alarak devam eder. Bir sirkülant matrisin esas köşegeni üzerindeki elemanları ile esas köşegene paralel olan doğrultu üzerindeki elemanları aynıdır.

Tanım 4.2.5. $SL(d, q)$ Tabanlı El-Gamal

Mahalanobis sirkulant matrislerdeki ayrık logaritma problemini inceleyerek aşağıdaki anahtar değişim protokolünü tasarlamıştır;

Gizli anahtar: $t, s \in \mathbb{N}$ belirlenir.

Açık anahtar: $A \in SL(d, q)$ için A ve A^t açık anahtar olarak yayımlanır.

Şifreleme:

i. Bob keyfi bir $r \in \mathbb{N}$ seçerek göndereceği $v \in \mathbb{F}_q^d$ metini için A^s ve A^{ts} matrislerini hesaplar,

ii. $(A^s, A^{ts} v^T)$ şifreli metini elde edilir (burada v^T vektörü v vektörünün devriğidir).

Deşifreleme

Alice'in elinde m olduğundan $(A^s, A^{ts}v^T)$ şifreli metinini aldığında A^s'yi kullanarak A^{ts} ve A^{-ts}'yi elde eder. Daha sonra $A^{ts}v^T$ işlemi sonucunda şifreli metinden v açık metinini elde eder.

Ayrıca Mahalanobis, $SL(d,q)$ tabanlı El-Gamal şifreleme sisteminin sağlığı güvenliğin $SL(d,q)$ tabanlı Diffie-Hellman problemine eşdeğer olduğunu göstermiştir [84].

Aşağıda verilen problemler, esnek küme özellikleri kullanılarak çözülebilmelerine çalışılmış ancak doktora sonrası çalışlarda incelenmek üzere ertelenmiştir.

Tanım 4.2.6. Ayrık Logaritma Problemi

Ayrık Logaritma Problemi (DLP) şu şekilde ifade edilebilir:

$$G = \langle g \rangle$$

devirli bir grup olmak üzere, verilen herhangi bir $h \in G$ için,

$$g^x = h$$

olacak şekilde bir x bulunabilir mi [173]?

G devirli bir grup ve $\bar{x} =, y_1, y_n \dots, y_n$ kalan sınıfları birden fazla olduğundan $g^x = g^{y_i}$ elemanına denk fakat x eşit olmayan y_i'ler olacaktır. Dolayısıyla g^x kullanılarak doğru x elemanını bulmak bir problem teşkil etmektedir. Bu ayrık logaritma problemi kriptografiden sıklıkla karşılaşılan açık bir problemdir.

Tanım 4.2.7. Eşlenik Bulma Problemi

G değişmeli olmayan bir grup olsun. Verilen $g, h \in G$ için $\exists\ x \in G$ öyle ki

$$h = g^x$$

olacak şekilde x'e göre g'nin eşleniği $x^{-1}gx$ olacaktır. Verilen $g, h \in G$, için $y \in G$ öyle ki

$$\mathrm{h} = g^{y}$$

olacak şekilde bir $y \in G$ bulmaya eşlenik bulma problemi denir [72].

Tanım 4.2.8. Sözcük Bulma Problemi

G devirli grubunun üreteci olarak w verilsin; $w = 1 \in G$ vektörünün sonlu sayıda basamakta bulunup bulunamaması, sözcük problemi olarak ifade edilmektedir [75].

Tanım 4.2.9. İzomorfizma Problemi

G ve G' iki grup olsun. Bu iki grubun sonlu sayıda denemeyle birbirine izomorfik olup olmadığı izomorfizma problemi olarak ifade edilmektedir [76].

Tanım 4.2.10. Genelleştirilmiş Eşlenik Bulma Problemi

$x, y \in B_n$ verilsin öyle ki bazı $a \in LB_n$ için $y = a^{-1}xa$ olmak üzere $y = b^{-1}xb$ olan bir $b \in LB_n$ bulanabilir mi [81]?

Tanım 4.2.11. Diffie-Hellman Tipi Genelleştirilmiş Eşlenik Bulma Problemi

Verilen $\exists\ a \in LB_n$ ve $\exists\ b \in UB_n$ için $x, y_A, y_B \in \mathrm{B}_n$ öyle ki

$$y_A = a^{-1}xa$$

ve

$$y_B = b^{-1}xb$$

olsun. Bu durumda

$$b^{-1}y_A\, b = a^{-1}y_B\, a = a^{-1}b^{-1}xab$$

bulunabilir mi [81]?

Tanım 4.2.12. Çoklu Simultane Eşlenik Bulma Problemi

Verilen $\exists\ a \in B_n$ için $x_i, y_i \in B_N$, $1 \le i \le t$ $y_i = a^{-1}x_i a$ olsun. $\forall\ i$ için

$$y_i = b^{-1}x_i b$$

olacak şekilde $b \in B_n$ var mıdır [81]?

4.3. Esnek Kriptografi

Tanım 4.3.1 Eğer (F, A) esnek grubu bir G eliptik eğrisin toplamsal grubu ve

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

ise (F, A) bir devirli esnek gruptur.

Örnek 4.3.2. [137] F_{23}'te $y^2 = x^3 + 5x + 4$ eliptik eğrisinin 19 çözümü vardır.

$(F, A) = \{O, (0,2), (0,21), (3,0), (5,4), (5,19), (8,2), (8,21), (13,19), (13,14), (14,9), (14,14), (15,2), (15,21), (19,9), (19,14), (20,10)\ ), (20,13), (21,3), (21,20)\}$

ise G, üreteci $P = (8,2)$ olan bir devirli gruptur.

Tanım 4.3.3. GF uzayında p asal sayı olmak üzere,

$$A = GF(p) = \{GF(2), GF(3), GF(5), GF(7), GF(11)\}$$

ve E parametre kümesi olmak üzere $F(x) = E_p$ eliptik eğri olsun. Burada (F, A) ikilisine devirli esnek grup denir.

$GF(23)$ üzerinde

$$F(x) = E_{23}(5,4)$$

eliptik eğrisini alınmış olsun, o halde elde edilecek eliptik eğri kriptografi algoritması aşağıda verildiği şekilde tasarlanmıştır;

Şifreleme:

Alice ve Bob, (E, e_1, e_2) eliptik eğri üzerinde anlaşırlar.

Alice devirli grubun $F(e_1) = (8,21)$ üretecini ve $d = 4$'yi seçer.

Daha sonra $F(e_2) = d \times e_1 = (21,3)$ hesaplanır.

Bob tarafından $P = (8, 2)$ düz metinini seçilir. Daha sonra ise $r = 3$ gizli anahtar olarak seçilir.

Bob tarafından $C_1 = r \times F(e_1) = (20,13)$ve $C_2 = P + r \times Fp(e_2) = (14,9)$ noktaları hesaplayarak Alice'ye gönderilir.

Böylece Alice, C_1 ve C_2 şifreli metinleri elde etmiş olur.

Deşifreleme:

Alice tarafından $P = C_2 - (d \times C_1) = (14,9) - (5,19) = (14,9) + (5,4)$ hesaplanır. Burada $(5,4)$ noktası $(5,19)$ noktasının toplamsal tersi olduğundan Alice,

$$P = (8,2)$$

açık metni elde etmiş olacaktır [76], [152].

Qiu ve Xiong çalışmalarında şifreleme işleminde, $\langle e_1 \rangle$'in bir üreteç olması gerektiği, aksi takdirde şifreleme işleminin gerçekleşmeyeceği sonucuna varmışlarıdır [154].

Tanım 4.3.4. Esnek Diffie-Hellman Anahtar Değişim Protokolü:

$G = \mathbb{Z}_p$ ve p bir asal sayı olsun. (F, A) esnek kümesi $\mathbb{Z}_p$ üzerinde bir esnek grup, X ise $P(\mathbb{Z}_p)$'nin bir elemanı olsun.

$$\{(a_i, \langle x \rangle) : F(a_i) = \langle x \rangle, \qquad x \in X\}$$

kümesine, (F, A)'nın bir esnek alt kümesi denir ve $\langle X \rangle$ ile gösterilir.

$$(F, A) = \langle X \rangle$$

ise, (F, A) esnek grubuna X tarafından üretilen devirli esnek grup denir.

Alice ve Bob güvensiz bir iletişim kanalı üzerinde güvenli ve gizli bir iletişim kurmak isterler.

i. Alice rastgele $\langle x \rangle \in \mathbb{Z}_q$ seçer, $F(a) = gx$ değerini hesaplar ve Bob'a gönderir.
ii. Bob rasgele $\langle y \rangle \in \mathbb{Z}_q$ seçer, $F(b) = gy$ değerini hesaplar ve Alice'ye gönderir.
iii. Her iki taraf da paylaşılan anahtarı hesaplar ve sonuçta

$$k = gxy = bx = ay$$

ortak anahtar elde edilmiş olur [128].

Tanım 4.3.5. Esnek El Gamal Açık Anahtar Şifreleme Şeması

Esnek El Gamal açık anahtar şifreleme şeması aşağıdaki özellikleri sağlayan şemadır.

i. Alice, rastgele $\langle x \rangle \in \mathbb{Z}_q$ devirli esnek grubunu seçer, k ortak anahtarı olarak $F(a) = g^x$'yi yayımlar ve $\langle x \rangle$'i gizli anahtarı olarak tutar.
ii. Bir $m \in G = \mathbb{Z}_q$ mesajı göndermek için, Bob rastgele $\langle y \rangle \in \mathbb{Z}_q$ seçer.
iii. Bob, $F(b) = g^y$ ve $F(c) = m \cdot k = m \cdot g^{xy}$ hesaplayarak Alice'e gönderir.
iv. Alice $(F(b), F(c))$'yi aldıktan $\frac{F(c)}{F(b)}$ ve $\langle x \rangle$ gizli anahtarını kullanarak m açık metnini elde eder [128].

4.4. Post Kuantum Anahtar Değişim Algoritması

Kuantum teknolojilerindeki gelişmeler, bir kuantum bilgisayarla düşmanın saldırılarına dirençli yeni kriptografik ilkellerin geliştirilmesini zorunlu kılmıştır. İki katılımcı için çok fazla anahtar değişim protokolü seçeneği bulunmaktadır. 2000 yılında, anahtar derecesindeki kademeli artışa dayalı olarak, üç katılımcı için izojen temelli bir anahtar değişim protokolü planı önerildi [156]. Reza ve arkadaşları tarafından ise ağaç yapısı kullanarak bir grup katılımcı için birer anahtar oluşturmak için başka bir ilke önerildi. Önerilen anahtar değişim protokolü dört katılımcı için kullanılabilmekte ve şema matematiksel bir araç olarak eliptik eğrilerin izojenisini kullanmaktadır [157]. İzojeni temelli anahtar değişim protokolü sağladığı üstün güvenlik sistemi nedeniyle Tor ağı, ve Bitcoin tarafından kullanılmaktadır.

Tanım 4.4.1 Bir izojeni, örten ve sonlu bir çekirdeğe sahip olan cebirsel grupların (diğer bir deyişle grup çeşitlerinin) bir morfizmdir.

Tanım 4.4.2. Açık bir kanal üzerinden gizli verileri iletmede ikiden daha fazla katılımcı için ortak bir anahtar elde edilmesini sağlayan post kuantum Diffie-Hellman anahtar değişim protokolü aşağıdaki koşulları gerçekleyen protokoldür.

A, B ve C katılımcılarının paylaşılan bir anahtar almak için gerçekleştirdikleri işlem sırası aşağıdaki verilen sıra ile belirlenir:

1. Katılımcılar algoritmanın p ve g genel parametrelerini seçerler;

2. A, B ve C katılımcıları gizli anahtarlarını sırasıyla a, b ve c'yi üretirler;

3. A katılımcısı,

$$g^a \ (mod\ p)$$

işlemini hesaplar ve sonucu B katılımcısına gönderir;

4. B katılımcısı,

$$(g^a)^b \ (mod\ p) = g^{ab} \ (mod\ p)$$

işlemini hesaplar ve sonucu C katılımcısına gönderir;

5. C katılımcısı

$$(g^{ab})^c \ (mod\ p) = \ g^{abc} \ (mod\ p)$$

işlemini hesaplar ve paylaşılan bir gizli anahtar alır;

6. B katılımcısı,

$$g^b \ (mod\ p)$$

işlemini hesaplar ve sonucu C katılımcısına gönderir;

7. C katılımcısı,

$$(g^b)^c \ (mod\ p) = g^{bc} \ (mod\ p)$$

işlemini hesaplar ve sonucu A katılımcısına gönderir;

8. A katılımcısı, paylaşılan bir gizli anahtar olan

$$(g^{bc})^a \ (mod\ p) = \ g^{bca} \ (mod\ p) = \ g^{abc} \ (mod\ p)$$

işlemini hesaplar;

9. C katılımcısı,

$$g^c (mod\ p)$$

işlemini hesaplar ve sonucu A katılımcısına gönderir;

10. A katılımcısı

$$(g^c)^a (mod\ p) = g^{ca} (mod\ p)$$

işlemini hesaplar ve sonucu B katılımcısına gönderir;

11. B katılımcısı

$$(g^{ca})^b (mod\ p) \ = \ g^{cab} \ (mod\ p) = \ g^{abc} (mod\ p)$$

işlemini hesaplar ve ayrıca paylaşılan bir gizli anahtar elde etmiş olur.

Böylece, bir saldırgan iletilen mesajları herhangi bir aşamada durdurursa, yalnızca $g, g^a, g^b, g^c, g^{ab}, g^{ac}, g^{bc}$ değerlerini alabilecektir. Bu değerler kullanılarak klasik bilgisayarlardan gelen saldırılarla a, b, c gizli anahtarları hesaplayabilmek mümkün olmayacaktır.

Üç katılımcı için bir anahtar elde etme şeması, eliptik eğrilerin izojenliğine dayalı olarak geliştirilmiştir [156].

İlk parametre

$$p = l_A^{eA} * l_B^{eB} * l_C^{eC} * f \pm 1$$

burada l_A, l_B, l_C asallar ve f bir kofaktördür (eş çarpanıdır). E ise F_{p^2} üzerinde tanımlanan bir süper singuler eliptik eğridir. Yani $a, b, c \in \mathbb{R}$ ve $c \neq 0$ için

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

formundadır. Ayrıca j-invaryantı ise $c = 0$ için

$$j(E) = 1728\frac{4a^3}{4a^3 + 27b^2}$$

formülü ile hesaplanır. Burulma grupları (tüm elemanları sonlu mertebeye sahip olan grup) ve ilgili jeneratörler aşağıda verildiği şekliyle belirlenir:

$$E[l_A^{eA}] = \langle P_A, Q_A \rangle$$

$$E[l_B^{eB}] = \langle P_B, Q_B \rangle$$

$$E[l_C^{eC}] = \langle P_C, Q_C \rangle$$

Protokolün her bir tarafı kendi özel anahtarı olarak iki sayı üretir ve karşılık gelen izojenik çekirdeği ($\langle P_i, Q_i \rangle$) hesaplar. Ortaya çıkan eğri ve bu eğri üzerindeki diğer tarafların taban noktalarının eşlenmesi bir açık anahtardır.

A, B ve C katılımcılarının paylaşılan bir anahtar almak için gerçekleştirdikleri işlem sırası aşağıdaki şekildedir:

i. Katılımcı A, katılımcı B'ye, E_A'yı ve P_B, Q_B, P_C ve Q_C'yi E_A ile eşleme noktalarını içeren açık anahtarını gönderir. Katılımcı B, katılımcı A'dan veri aldığında, ortak anahtar Pub_{AB}'yi , E_{AB} eğrisini hesaplar ve P_C ve Q_C noktalarını EAB'ye eşler.

ii. Üye B, genel anahtarını ve hesaplanan Pub_{AB}'yi üye C'ye gönderir. Üye C, ortak anahtar B 'yi kullanarak paylaşılan gizli anahtar Pub_{BC}'yi hesaplayabilir.

iii. Pub_{BC} 'yi hesapladıktan sonra, katılımcı C ortak anahtarını ve oluşturulan Pub_{BC}'yi üye A'ya gönderir. Üye C, paylaşılan şifreyi ve B üyesine aktarım için Pub_{AC}'yi hesaplar.

iv. Üye A, oluşturulan Pub_{AC}'ı B üyesine gönderir. Üye B paylaşılan gizli anahtarı hesaplayabilir.

Ortak anahtar,

$$j(E_{ABC})$$

değişmezdir (invaryantır). Elde edilen tüm E_{ABC}, E_{BCA} ve E_{CAB}, eğrilerinin her biri

$$\frac{E}{\langle K_A, K_B, K_C \rangle}$$

'ye izomorftur ve bu nedenle aynı j-değişmezine sahiptir.

Bu sistemde katılımcılar arasında minimum mesaj yönlendirme sayısının 4 olduğu görülmektedir. Genel olarak transfer sayısı, n protokol katılımcılarının sayısı olduğundan $(2n-2)$ formülü kullanılarak hesaplanır.

Yukarıdaki tanımda (Tanım 4.4.2) verilen izojeni tabanlı anahtar değişim protokolü 3 katılımcının bulunduğu grupta kullanımı verilmiştir. Gruptaki kişi sayısının artması durumunda işlem yükü çarpan etkisi nedeniyle çok ciddi miktarda artmakta bu da verimsizliğe neden olabilmektedir. Bu nedenle alternatif yöntemlerin geliştirilmesi gerekmektedir. Bu sistemin esnek kümelerle birleştirilmesi mümkün görülmektedir.

4.5. Esnek Post Kuantum Anahtar Değişim Algoritması

Tanım 4.5.1. (Esnek Post Kuantum Anahtar Değişim Algoritması)

$$\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\} \text{ ve } \overline{1} = \{1,4,7, \dots, 3n-2\}$$

U anahtar değişim protokolü katılımcılarının evrensel kümesi ve E post kuantum anahtar değişim protokolünün parametre kümesi olsun, $F: E \rightarrow P(U)$ bir dönüşüm olmak üzere (F, E) ikilisi U üzerinde esnek küme olmak üzere, $i = \overline{1}$'in sırasıyla kalan sınıfının elemanları olmak üzere $A = (e_i)$, E de boş olmayan sonlu bir alt küme ve

$$U = (h_1, h_2, h_3, \dots, h_{3n})$$

olsun. Aşağıdaki koşulları sağlayan (F, A)'ya esnek post kuantum anahtar değişim protokolü denir.

$f(e_i) = \{h_i, h_{i+1}, h_{i+2}, p_i, g_i\} \in (F, A)$ olmak üzere,

$$f(e_1) = \{h_1, h_2, h_3, p_1, g_1\} \in (F, A)$$

$$f(e_4) = \{h_4, h_5, h_6, p_4, g_4\} \in (F, A)$$

$$\vdots$$

$$f(e_{3n-2}) = \{h_{3n-2}, h_{3n-1}, h_{3n}, p_{3n-2}, g_{3n-2}\} \in (F, A).$$

h_1, h_2 ve h_3 katılımcılarının paylaşılan ortak bir anahtar almak için gerçekleştirdikleri işlem sırası aşağıda verilmiştir:

1. $f(e_1)$ esnek fonksiyonu döngüye girecek katılımcıları ile p_1 ve g_1 sayılarını rastgele seçsin;

2. h_1, h_2, h_3 katılımcıları gizli anahtarlarını sırasıyla a, b ve c'yi üretirler;

3. h_1 katılımcısı,

$$g_1{}^a \ (mod\ p_1)$$

işlemini hesaplar ve sonucu h_2 katılımcısına gönderir;

4. h_2 katılımcısı,

$$({g_1}^a)^b \ (mod\ p_1) = {g_1}^{ab} \ (mod\ p_1)$$

işlemini hesaplar ve sonucu h_3 katılımcısına gönderir;

5. h_3 katılımcısı

$$({g_1}^{ab})^c \ (mod\ p_1) = \ {g_1}^{abc} \ (mod\ p_1)$$

işlemini hesaplar ve paylaşılan ortak gizli anahtarını almış olur;

6. h_2 katılımcısı,

$${g_1}^b \ (mod\ p_1)$$

işlemini hesaplar ve sonucu h_3 katılımcısına gönderir;

7. h_3 katılımcısı,

$$({g_1}^b)^c \ (mod\ p_1) = {g_1}^{bc} \ (mod\ p_1)$$

işlemini hesaplar ve sonucu h_1 katılımcısına gönderir;

8. h_1 katılımcısı, ve gizli anahtarını kullanarak paylaşılan bir gizli anahtar olan

$$({g_1}^{bc})^a \ (mod\ p_1) \ = \ {g_1}^{bca} \ (mod\ p_1) \ = \ {g_1}^{abc} \ (mod\ p_1)$$

işlemini hesaplar ve paylaşılan ortak gizli anahtarını almış olur;

9. h_3 katılımcısı,

$${g_1}^c (mod\ p_1)$$

işlemini hesaplar ve sonucu h_1 katılımcısına gönderir;

10. h_1 Katılımcısı

$$({g_1}^c)^a \ (mod\ p_1) = {g_1}^{ca} \ (mod\ p_1)$$

işlemini hesaplar ve sonucu h_2 katılımcısına gönderir;

11. h_2 Katılımcısı

$$({g_1}^{ca})^b \ (mod\ p_1) = \ {g_1}^{cab} (mod\ p_1) = \ {g_1}^{abc} \ (mod\ p_1)$$

işlemini hesaplar ve böylece her üç kişilik katılıcı grubu arasında paylaşılan ortak bir gizli anahtar elde edilmiş olur.

Ayrıca, bir saldırgan iletilen mesajları herhangi bir aşamada durdururursa, yalnızca $g_1, {g_1}^a, {g_1}^b, {g_1}^c, {g_1}^{ab}, {g_1}^{ac}, {g_1}^{bc}$ değerlerini alabilecektir. Bu değerler kullanılarak klasik bilgisayarlardan gelen saldırılarla a, b, c gizli anahtarları polinomsal zamanda hesaplayabilmek mümkün olmayacaktır.

Benzer şekilde

1. $f(e_4) = \{h_4, h_5, h_6, p_4, g_4\}$ esnek fonksiyonunun ürettiği $h_4, h_5, h_6,\ p_4$ ve g_4 sayılarını rastgele seçilerek h_4, h_5, h_6 katılımcıların her birine p_4 ve g_4 gönderilsin;

2. h_4, h_5, h_6 katılımcıları gizli anahtarlarını sırasıyla a_4, b_4, c_4'ü üretirler;

3. h_4 katılımcısı,

$$ {g_4}^{a_4} (mod\ p_4)$$

hesaplar ve sonucu h_5 katılımcısına gönderir;

4. h_5 katılımcısı,

$$({g_4}^{a_4})^{b_4} \ (mod\ p_1) = {g_4}^{a_4 b_4} \ (mod\ p_4)$$

hesaplar ve sonucu h_6 katılımcısına gönderir;

5. h_6 katılımcısı

$$({g_4}^{a_4 b_4})^{c_4} \ (mod\ p_1) = \ {g_4}^{a_4 b_4 c_4} \ (mod\ p_4)$$

hesaplar ve paylaşılan ortak gizli anahtarını almış olur;

6. h_5 katılımcısı,

$$ {g_4}^{b_4} \ (mod\ p_4)$$

hesaplar ve sonucu h_6 katılımcısına gönderir;

7. h_6 katılımcısı,

$$({g_4}^{b_4})^{c_4}\ (mod\ p_1) = {g_4}^{b_4 c_4}\ (mod\ p_4)$$

hesaplar ve sonucu h_4 katılımcısına gönderir;

8. h_4 katılımcısı, ve gizli anahtarını kullanarak paylaşılan bir gizli anahtar olan

$$({g_4}^{b_4 c_4})^{a_4}\ (mod\ p_4)\ =\ {g_4}^{b_4 c_4 a_4}\ (mod\ p_4)\ =\ {g_4}^{a_4 b_4 c_4}\ (mod\ p_4)$$

hesaplar ve paylaşılan ortak gizli anahtarını almış olur;

9. h_6 katılımcısı,

$${g_4}^{c_4}(mod\ p_4)$$

hesaplar ve sonucu h_4 katılımcısına gönderir;

10. h_4 katılımcısı

$$({g_4}^{c_4})^{a_4}\ (mod\ p_4) = {g_4}^{c_4 a_4}\ (mod\ p_4)$$

hesaplar ve sonucu h_5 katılımcısına gönderir;

11. h_5 katılımcısı

$$({g_4}^{c_4 a_4})^{b_4}\ (mod\ p_4) =\ {g_4}^{c_4 a_4 b_4}(mod\ p_4) =\ {g_4}^{a_4 b_4 c_4}\ (mod\ p_4)$$

hesaplar ve ayrıca her üç kişilik katılıcı grubu arasında paylaşılan ortak gizli anahtar elde edilmiş olur.

Bu döngünün $f(e_i)$ esnek fonksiyonu tarafından devam ettirilmesi ile istenen sayıda rastgele seçilmiş üç katılımcılı güvenlik çemberleri oluşturularak anahtar değişim protokolü en verimli sistemde çalıştırılmış olmaktadır. Ayrıca her bir a_i, b_i, c_i katılımcıların kendilerince seçilen gizli anahtarlar olsa da p_i ve g_i çiftlerinin her birisi $f(e_i)$ esnek fonksiyonu tarafından rastgele ve birbirinden farklı seçileceğinden gruplarca elde edilecek ortak gizli anahtarlarının çakışma ihtimali ortadan kaldırılmıştır.

Post kuantum Diffie-Helman anahtar değişim protokolü, Microsoft [155] tarafından yeni nesil kriptografi (CNG) ismi ile C# programlama dili altyapısında kullanılmak üzere System.Security.Cryptography sınıfı oluşturulmuştur. Microsoft tarafından geliştirilen

System.Security.Cryptography sınıfını kullanarak örnek verilerin nasıl şifrelendiğini ve şifresinin çözülmesini gösteren Gelişmiş Şifreleme Standardı (AES) C# uygulamalarının devralması gereken soyut temel sınıfı temsil etmektedir [154]. Bu sınıf içinde gerekli esnek kodlama tanımlamaları yapılarak System.Security.Cryptography sınıfına dahil edilmesi ile Aygün [142,144] tarafından geliştirilen "Esnek AES" kriptografi sistemine uyarlanabilir. Böyle bir çalışmanın prototipi olan esnek AES kriptografi tasarımının C# kodları EK-1'de verilmiştir.

Eliptik Eğri, Diffie-Hellman (ECDH) algoritmasının yeni nesil şifreleme sistemlerine uygulanmasını sağlar. Bu yeni nesil ECDiffieHellmanCng sınıfı C# ve diğer programlama dillerinde şifreleme işlemleri gerçekleştirmek için kullanılan kodları barındırmaktadır. EK-2'de, ECDiffieHellmanCng bir anahtar değişim algoritması oluşturmak için sınıfının nasıl kullanılacağını göstermektedir. Genel bir kanaldan gönderilebilecek ve alıcı tarafından şifresi çözülebilecek bir iletiyi şifrelemek için esnek AES anahtarın nasıl kullanılacağı da gösterilmektedir. Bu tasarımın C# kodları EK-2 de verilmiştir [155].

4.6. Sonuç ve Öneriler

Dördüncü bölümün Tanım 4.3.5.'e kadar olan kısmına 2014 yılında gerçekleştirilen KMD 2014 uluslararası matematik sempozyumunda "On the Group Based Cryptography" başlığıyla sunulmuştur. Ayrıca 2014 yılında "On the Group Based Cryptography" başlığıyla OCLC, CNKI, Google Scholar, CrossRef, Index of Copurnicus, World Cat, CQVIP, P. R. China, WanFang Data indekslerine sahip Journal of Mathematics and System Science isimli dergide yayımlanmıştır.

Esnek cebirsel yapılar ile kriptografi sistemlerinin yapısal algoritmaları değiştirilmeden esnek algoritma oluşturma çalışmaları yapılmıştır. Kriptografi sistemleri hem çok maliyetli hem de uzun süren çalışmalar sonucunda ortaya konmuş sistemlerdir. Günümüzde, yeni teknolojik gelişmeler karşısında gücünü kaybeden sistemlerden tamamen vazgeçilebilmektedir. Bu durum zaman ve para kaybına sebep olmaktadır. Bu esnek kombinasyonlar, kriptografi algoritma ve sistemlerinin tamamen kullanılmaz hale gelmesinin önüne geçecektir. Ayrıca esnek parametrelerin seçimi ile kullanıcılarda parametre değerlerinin değiştirebilme olanağına sahip olacaktır. O halde her sistem birbirinden bağımsız ek parametreler vasıtasıyla kişiselleştirilebilir sistemlere dönüştürülebilme imkanına sahip olacaktır. Örneğin günümüzde birçok banka sistemi kullanıcı adı ve şifre işlemlerinden sonra ek bir seçenek olarak daha önce banka tarafından belirlenmiş bir görsel resim seçimini sunmaktadır. Bu örnekte olduğu gibi esnek fonksiyon parametreleri bu imkânı her sistem kullanıcısına ek avantaj olarak sağlayabilecektir. Buna ek olarak kriptografi sisteminin gizli anahtarı istenmeyen kişilerce ele geçirilebilse bile her üç kullanıcının ayrı ayrı ikinci bağımsız gizli anahtar parametresi farklı olacağından sistem güvenliğini sağlamaya devam edecektir.

Esnek cebirsel yapılar kullanılarak çok güçlü, esnek ve kişiselleştirilebilir kriptografi algoritmaları elde edilebilir.

KAYNAKLAR

1. Shannon, C., "A Mathematical Theory of Communication", *Bell System Tech. J.*, Vol. 27, 379-423, 1948.
2. Çengellenmiş, Y., "Değerlendirme Teorisi ve Kodlama Teorisi Üzerine", *Trakya Üniversitesi Fen Bilimleri Enstitüsü, Doktora Tezi*, Edirne, 2005.
3. Topcu, H., "Self-Dual Kodlar ve İnşa Yöntemleri", *NEVÜ Fen Bilimleri Enstitüsü*", *Yüksek Lisans Tezi*, Nevşehir, 2012.
4. Keleş, E., "Soft Kümeler Üzerine*", Muğla Üniversitesi Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi*, Muğla, 2009.
5. Enginoğlu, S., *"*Esnek Kümeler ve Esnek Karar Verme Metotları*", Gaziosmanpaşa Üniversitesi Fen Bilimleri Enstitüsü", Yüksek Lisans Tezi*, Tokat, 2009.
6. İnan, E., "Soft Kümeler ve Bazı Cebirsel Yapılar*", Adıyaman Üniversitesi Fen Bilimleri Enstitüsü*", *Yüksek Lisans Tezi*, Adıyaman, 2011.
7. Aktaş, H. and Çakır, K., "Esnek Gruplar Üzerinde Bazı Cebirsel Uygulamalar", *Gaziosmanpaşa Journal of Scientific* Research 2, 35-40, 2013.
8. Liu, Y. and Xin, X., "General Fuzzy Soft Groups and Fuzzy Normal Soft Groups", *Annals of Fuzzy Mathematics and Informatics* Vol. 6, No. 2, pp.391-400, 2013.
9. Aktaş, H., Çitak, F., "Roughness in the Field of Quotients of an Integral Domain", *Annals of Fuzzy Mathematics and Informatics*, Vol. 4, No.1, 2012.
10. Atmaca, S., "Fuzzy, Rough ve Soft Kümeler ile Topolojileri Üzerine*", Cumhuriyet Üniversitesi Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi,* Sivas, 2010.
11. Yamalı, Ş., "Kodlaştırma Teorisi Üzerine", *Çanakkale On sekiz Mart Üniversitesi*, *Yüksek Lisans Tezi,* Çanakkale, 2010.
12. Molodtsov, D., "Soft set theory –first results", *Computers and Mathematics with Applications*, 37(1), 19-31, 1999.
13. Molodtsov, D., "The Theory of Soft Sets (in Russian)", *URSS Publishers*, Moscow, 2004.
14. Pawlak, Z., "Rough sets", *International Journal of Information and Computer Sciences*, 11(1), 341-356, 1982.

15. Xiao, Z. ve Ark., "Research on Synthetically Evaluating Method for Business Competitive Capacity Based on Soft Set", *Statistical Research*, 52-54, 2003.
16. Yang, H. ve Ark., "The Induction and Decision Analysis of Clinical Diagnosis Based on Rough Sets and Soft Sets" (F*angzhi Gaoxiao Jichukexue Xuebao Ed.*), September, 17(3), 208-212, 2004.
17. Chen, D-G., Tsang, E.C.C., Yeung, D.S., "Some Notes on the Parameterization Reduction of Soft Sets", *International Conference on Machine Learning and Cybernetics*, 3, 1442-1445, 2003.
18. Kong, Z., Gao, L.,Wang, L. and Li, S., "The normal Parameter Reduction of Soft Sets and Its Algoritm", *Computers and Mathematics with Applications*, 56(1), 3029-3037, 2008.
19. Mushrif, M.M.ve Ark., "Texture Classification Using a Novel, Soft-Set Theory Based Classification, Algorithm", *Lecture Notes In Computer Science*, 3851 246-254, 2006.
20. Aktaş, H. and Çağman, N., "Soft Sets and Soft Groups", *Information Sciences*, 177(1), 2726-2735, 2007.
21. Jun, Y. B., "Soft BCK/BCI-Algebras", *Computers and Mathematics with Application*s, 56(1), 1408-1413, 2008.
22. Jun, Y. B. and Park, C. H., "Applications of Soft Sets in Ideal Theory of BCK/BCI-algebras", *Information Sciences*, 178(1) 2466-2475, 2008.
23. Park, C.H. ve Ark., "Soft WS-Algebras", *Commun. Korean Math. Soc*, 23(3), 313-324, 2008.
24. Feng, F., Jun, Y. B. and Zhao, X., "Soft Semi Rings", *Computers and Mathematics with Applications*, 56(10), 2621-2628, 2008.
25. Sun, Q-M. ve Ark., "Soft Sets and Soft Modules", *Rough Sets and Knowledge Technology Lecture Notes in Computer Science* Vol. 5009, pp 403-409, 2008.
26. Zou, Y. and Xiao, Z., "Data Analysis Approaches of Soft Sets Under Incomplete Information", *Knowledge-Based Systems*, 21(1), 941-945, 2008.
27. Maji, P.K. ve Ark., "Fuzzy Soft Sets", *Journal of Fuzzy Mathematics*, 9(3), 589-602, 2001.
28. Roy, A.R. and Maji, P.K., "A Fuzzy Soft Set Theoretic Approach to Decision-Making Problems", *Journal of Comp. and Applied Mathematics*, 203(1), 412-418, 2007.

29. Yang, X. et. all, "Generalization of Soft Set Theory: From Crisp to Fuzzy Case", *In Fuzzy Information and Engineering: Proceedings of ICFIE, (Bing-Yuan Cao Ed.), Advances in Soft Computing* 40, Springer, 345-355, 2007.
30. Majumdar, P. ve Samanta, S. K., "Similarity Measure of Soft Sets", *New Mathematics and Natural Computation*, 4(1), 1-12, 2008.
31. Kong, Z. ve Ark., "Comment on "A fuzzy soft set theoretic approach to decision making problems". *Journal of Comp. and Applied Mathematics,* 2008.
32. Xiao, Z., Gong, K. and Zou, Y., "A Combined Forecasting Approach Based on Fuzzy Soft Sets", *Computers and Mathematics with Applications,* 2009.
33. Molodtsov, D. A., Leonov, V. Y. and Kovkov, D. V., "Soft Sets Technique and Its Application", *Nechetkie Sistemy i Myagkie Vychisleniya,* 1(1), 8-39, 2006.
34. Kovkov, D. V., Kolbanov, V. M. and Molodtsov, D. A., "Soft Sets Theory-Based Optimization", *Journal of Computer and Systems Sciences International*, 46(6), 872-880, 2007.
35. Reed, S., Solomon, G., "Polynomial Codes Over Certain Finite Fields*", Journel of the Society for Industrial and Applied Mathematics*, Vol. 8, No. 2, 300-304, 1960.
36. Esmaeili, M., Esmaeili, M., "A Fibonacci-Polynomial Based Coding Method With Error Detection and Correction", C*omputers & Mathematics with Applications,* 60(10): 2738-2752, 2010.
37. Basu, M. and Prasad, B., "The Generalized Relations Among the Code Elements for Fibonacci Coding Theory", *Chaos Solitons Fractals 41*, no. 5, 2517-2525, 2009.
38. Calabi, L., "Note on Rank and Nullity in Coding Theory", *Information and Control* 4, 359-363, 1961.
39. Delsarte, PH., "Bilinear Forms over a Finite Field with Applications to Coding Theory", *Journal of comb. Theory,* Series A 25, 226-241, 1978.
40. Berlekamp E. R., "Coding Theory and The Mathieu Groups", *Information and Control 18*, 40-64, 1971.
41. MacWilliams, F.J., "Cyclotomic Numbers, Coding Theory and Orthogonal polynomials", *Discrete Mathematics 3*, 133- 151, 1972.
42. Van Gelder, I., Olteanu, G., "Finite Group Algebras of Nilpotent Groups: A Complete Set of Orthogonal Primitive Idempotents", *Finite Fields and Their Applications 17*, 157–165, 2011.

43. Ben-Arieh, D., Lee, S.E., Chang, P.T., "Theory and Methodology Fuzzy Part Coding for Group Technology", *European Journal of Opr. Research 92,* 637-648, 1996.
44. Bernal, J. J., del Río, Á., Simón, J. J., "Group Code Structures of Affine-İnvariant Codes", *Journal of Algebra 325*, 269–281, 2011.
45. Hachenberger, D., "On a Combinatorial Problem in Group Theory", *Journal of Combinatorial Theory*, Series A 64, 79-101, 1993.
46. Iiams, J. E., "On Difference Sets in Groups of Order $4p^2$", *Journal of Combinatorial Theory*, Series A 72, 256-276, 1995.
47. Aslam, M., Qurasi, S.M., "Some Contributions to Soft Groups", *Annals of Fuzzy Mathematics and Informatics*, Vol. 4, No. 1, pp. 177- 195, ISSN 2093–9310, 2012.
48. Fu, L., "Notes on the Soft Operations", *ARPN Journal of Systems and Software*, Vol. 1, No. 6, ISSN 2222-9833, 2011.
49. Xun, G. and Yang, S., "Investigations on Some Operations of Soft Sets", *World Academy of Science, Engineering and Technology 75*, 1113-1116, 2011.
50. Zhu P., Wen Q., "Operations on Soft Sets Revisited", arXiv: 1205. 2857 Vol. 1, 2012.
51. Razak, S.A., Mohamad, D., "A Soft Set Based on Group Decision Making with Criteria Weight", *World Academy of Science, Engineering and Technology 7*5, 574-579, 2011.
52. Rose, A.N.M., Mohd, H., Deris, M.M., "Solving Incomplete Inormation in Soft Set using Descimal Approach", In *Proceeding of ICCIT 2012 1st Taibah University International Conference on Computing and Information Technology*. University of Taibah, 225-230, 2012.
53. Zadeh, L.A., "Fuzzy Sets", *Inform and Control*, 8, 338-352, 1965.
54. Loeliger, H-A., and Mittelholzer, T.. "Convolutional Codes Over Groups" *Information Theory*, IEEE Transactions on 42.6, 1660-1686, 1996.
55. Arpasi, J.P., "On the Uncontrollability of Nonabelian Group Codes with Uncoded Group Z_p", *Hindawi Publishing Corporation Mathematical Problems in Engineering* Vol.Article, ID 783516, 2011.
56. Bhattacharyya, D., et al, "Text Steganography: A Novel Approach", *International Journal of Advanced Science and Technology*, Vol. 3, February, 2009.
57. Channalli, S., Jadhav, A., "Steganography An Art of Hiding Data", *International Journal on Computer Science and Eng*. Vol. 1(3), 137-141, 2009.

58. Hamid, N. et al, “Image Steganography Techniques: An Overview”, *IJCSS,* Vol. (6), Issue (3), 2012.
59. El-Emam, N.N., "Hiding a Large Amount of Data With High Security Using Steganography Algorithm." *Journal of Computer Science 3 (4)*: 223-232, 2007.
60. Challita, K. and Farhat, H., “Combining Steganography and Cryptography: New Directions”, *IJNCAA, 1(1),* 199-208, SDIWC, (ISSN 2220-9085), 2011.
61. Alexei, M., Vladimir, S., Alexander, U., “Group-Based Cryptography**”,** ISBN 978-3-7643-8826-3 *Birkhäuser Verlag*, *Basel Boston*, Berlin, 2008.
62. Rajyaguru, M. H., “Crystography-Combination of Cryptography and Steganography With Rapidly Changing Keys”, *IJETAE,* Vol. 2, Issue 10, 2012.
63. Mansoor, A.B., Khan, Z., Khan, S.A., “Crypto-Steg: A Hybrid Cryptology - Steganography Approach for Improved Data Security”, *Mehran University Research Journal of Engineering & Technology*, Vol. 31, No. 2, 2012.
64. Borges F., Portugal R., & Oliveira J., “Steganography with Public-Key Cryptography for Video Conference”, *National Laboratory of Scientific Computing - LNCC*, 25651-075, 2007.
65. Aparajita, A.R., “STEGNOGRAPHY-The Art of Hiding Information A Comparison from Cryptography”, *International Journal of Innovative Research in Science, Engineering and Technology*, 1308, Vol. 2, Issue 5, May 2013.
66. Raphael, A.J., Dr. Sundaram, V, “Cryptography and Steganography-A Survey”, ISSN: 2229-6093, Int. J. Comp. Tech. Appl., Vol. 2 (3), 626-630, 2011.
67. Brifcani, A.M.A., "Stego-Based-Crypto Technique for High Security Applications", *International Journal of Computer Theory and Engineering*, Vol. 2, No.6, December, 1793-8201, 2010.
68. Laskar, S. A. and Hemachandran, K., “Secure Data Transmission Using Steganography and Encryption Technique*”, International Journal on Cryptography and Information Security (IJCIS),* Vol. 2, No.3, September 2012.
69. Evgeny O. et al. “The Application of Cryptography and Steganography in the Integration of Seaport Security Subsystems”, *Zeszyty Naukowe Akademia Morska w* Szczecinie, 26(98) pp. 80-87, 2011.
70. Kaliski, Jr. ve Ark., “Is the Data Encryption Standard a Group?”, *Advances in Cryptology-EUROCRYPT'85*, Springer Berlin Heidelberg, 1998.

71. Campbell, K. W., & Wiener, M. J., “DES is not a Group”, *In Advances in Cryptology-CRYPTO'92*, (pp. 512-520), 1993.
72. Cid, C., Mullan, C., “Group Theory in Cryptography”, *Proceedings of Groups St Andrews 2009 in Bath Vol. 1*, Cambridge University Press, 133-149, 2011.
73. Myasnikov A., Shpilrain V., Ushako A., “Group-based Cryptography”, *Advanced Courses in Mathematics CRM* Barcelona, Birkhauser, Basel, 2008.
74. Hasapis, S. D., & Panagopoulos, D., “Some Aspects of Group-based Cryptography”, *Journal of Applied Mathematics & Bioinformatics*, Vol. 3, No. 1,2013,83-97 ISSN:1792-6602(print), 1792-6939 (online) Scien. press Ltd, 2013.
75. Rivest R., Shamir A., Adleman L., “A Method for Obtaining Ddigital Signatures and Pulic-Key Cryptosystems”, *Communications of the ACM*, 21, 120-126, 1978.
76. Diffie W., HellmanM ., “New Directions in Cryptography”, *IEEE Transaction on Information Theory*, 22, 644-654, 1976.
77. Ko, K.H. et all, “New Public-key Cryptosystem Using Braid Group”, *in Advances in Cryptology-CRYPTO 2000* (M. Bellare, ed.), Lecture Notes in Computer Science 1880, 166--183, 2000.
78. Stickel E., A New Method for Exchanging Secret Keys”, *in Proc. Third International Conference on Information Technology and Applications (ICITA '05)*, 426-430, IEEE Computer Society, Piscataway, 2005.
79. Nhut, N.T., “Group-based Public Key Cryptography”, *Ho Chi Minh City University of Natural Science*, M. Thesis, VNU-HCM, 2004.
80. Parvez, A., “Introduction to Braid Group Cryptography”, Documents from *www.cs.washington.edu*, 2006.
81. Dehornoy, P., “Braid-based Cryptography”, *Contemp. Mathematics* 360, 5-33. 2004.
82. Kahrobaei, D., Koupparis, C., Shpilrain, V., “Public Key Exchange Using Matrices Over Group Rings”, *Groups, Complexity, Cryptology* 5, 97-115, 2013.
83. Mahalanobis, A. "Are Matrices Useful in Public-Key Cryptography?", *International Mathematical Forum*, http://dx.doi.org/10.12988/imf.2013.310187, Vol. 8, no. 39, 1939 - 1953, 2013.
84. Mondal, S. and Pal M., "Soft Matrices" *Journal of Uncertain Systems*, Vol. 7, No.4, p.254-264, *Online at: www.jus.org.uk*, 2013.
85. Molodtsov, D., “Soft Set Theory-first Results”, *Computer and Mathematics with applications*, Vol. 37, pp.19-31, 1999.

86. Aktas, H., and N. Çağman, “Soft Set and Soft Groups”, *Information Sciences,* Vol. 177, pp.2726--2735, 2007.
87. Ali, M.I., et al., “On Some New Operations in Soft Set Theory”, *Computer and Mathematics with Applications,* Vol. 57, 1547-1553, 2009.
88. Yin, X., "Study on Soft Groups", *Journal of Computers*, Vol. 8, No. 4, 2013.
89. Basu, T.M., Mahapatra, N.K. and Mondal, S.K., "Matrices in Soft Set Theory and Their Applications in Decision Making Problems", *SAJM,* Vol. 2(2):126-143, ISSN 2251-1512, 2012.
90. İnternet: Wikipedia, “RSA”, *http://en.wikipedia.org/wiki/RSA_(cryptosystem),* 2020.
91. Bhattacharyya, D., et al, “Text Steganography: A Novel Approach”, *International Journal of Advanced Science and Technology*, Vol. 3, 2009.
92. Channalli, S., Jadhav, A., “Steganography An Art of Hiding Data”, *International Journal on Computer Science and Engineering”,* Vol. 1(3), 137-141, 2009.
93. Hamid, N. et al, “Image Steganography Techniques: An Overview”, *IJCSS*, Vol. (6), Issue (3), 2012.
94. El-Emam, N.N., “Hiding a Large Amount of Data With High Security Using Steganography Algorithm”, *Journal of Computer Science* 3 (4): 223-232, 2007.
95. Challita, K. and Farhat, H., “Combining Steganography and Cryptography: New Directions”, *IJNCAA,* 1(1): 199-208, 2011.
96. Çimen, C., Akleylek, S., & Akyıldız, E., “Şifrelerin matematiği: kriptografi*”, ODTÜ yayınları,* Ankara, 2008.
97. İnternet: Wikipedia, “Steganografi”, *http://tr.wikipedia.org/wiki/Steganografi*, https://en. wikipedia.org /wiki/Steganography_tools, 2020.
98. Can, B., “Steganografi: Bilgiyi Gizleme Bilimi”, http://www.birdunyabilgi.org /steganografi-bilgiyi-gizleme-biliminedir, 2013.
99. İnternet: “Tübitak”, http://www.kamusm.gov.tr/dosyalar/kitaplar/aaa/, 2013.
100. Mansoor, A.B., Khan, Z., Khan, S.A., “CRYPTO-STEG: A Hybrid Cryptology - Steganography Approach for Improved Data Security”, *Mehran University Research Journal of Engineering & Technology*, Vol. 31, No. 2, 2012.
101. Gorla, S., “Combination of Cryptography and Steganography for Secure Communication in Video File”, *California State University, Master Thesis,* Sacramento, 2009.

102. Challita, K., Farhat, H., "Combining Steganography and Cryptography: New Directions", *International Journal on New Computer Architectures and Their Applications (IJNCAA*) 1(1): 199-208, 2011.

103. Saran, N., "Kriptografideki Güncel Çalışmalar", *2. Mühendislik ve Teknoloji Sempozyumu, Çankaya Üniversitesi* / Ankara, 30 Nisan - 1 Mayıs, 2009.

104. Borges, F., Portugal, R., & Oliveira, J., "Steganography with Public-Key Cryptography for Video conference", *National Laboratory of Scientific Computing* - LNCC, 25651-075, Petr´opolis, RJ, 2010.

105. Aparajita, A.R., "STEGNOGRAPHY-The Art of Hiding Information A Comparison from Cryptography", *International Journal of Innovative Research in Science, Engineering and Technology*, Copyright to IJIRSET www.ijirset.com, 1308, Vol. 2, Issue 5, 2013.

106. Çağman, N., Karataş, S., "Bulanıklık ve Olasılık", *Mantık, Matematik ve Felsefe 4. Ulusal Sempozyumu*, 5–8 Eylül 2006, Kültür Üniversitesi, Foça-İzmir, 2006.

107. Brifcani, A., "Stego-Based-Crypto Technique for High Security Applications", *International Journal of Computer Theory and Engineering*, Vol. 2, No.6, December, 1793-8201, 2010.

108. Laskar, S. A., Hemachandran, K., "Secure Data Transmission Using Steganography and Encryption Technique" *International Journal on Cryptography and Information Security* (IJCIS), Vol. 2, No. 3, September 2012.

109. Evgeny O., et al. "The application of cryptography and steganography in the integration of seaport security subsystems Zastosowanie kryptografii i steganografii w integracji podsystemów bezpieczeństwa informacyjnego portów morskich", *Zeszyty Naukowe Akademia Morska w Szczecinie*, 26(98) pp. 80-87, 2011.

110. Lee M. C. and Lau C. Y., "Three Orders Mixture Algorithm of Audio Steganography Combining Cryptography", *Journal of Information Hiding and Multimedia Signal Processing*", ISSN 2073-4212 Ubiquitous International, Vol. 9, Number 4, July, 2018.

111. Artin, M., "Algebra", Prentice Hall, ISBN 978-0-13-468960-9, *Chapter 2 Contains an Uundergraduate-level Exposition of the Notions Covered in This Article*, 2008.

112. Devlin, K., “The Language of Mathematics: Making the Invisible Visible”, *Owl Books, ISBN 978-0-8050-7254-9, Chapter 5 provides a layman-accessible explanation of groups*, 2000.

113. Hall, G. G., “Applied Group Theory”, *American Elsevier Publishing Co., Inc.*, New York, MR 0219593, An Elementary Introduction, 1976.

114. Ledermann, W., (1973), “Introduction to Group Theory”, *New York: Barnes and Noble, OCLC* 795613, 1973.

115. Robinson, D., John, S., “A Course in the Theory of Groups”, *Berlin, New York: Springer-Verlag*, ISBN 978-0-387-94461-6, 1996.

116. İnternet: Wikipedia, “Group Theory”, https://en.wikipedia.org/wiki/Group (mathematics), 2020.

117. Savin, G. “Numbers, Groups and Cryptography”, *Department of Mathematics, Univ. of Utah*, Salt Lake City, 2009.

118. Halıcıoğlu, S., Üngör, B., “Cebir I”, Ankara Üniversitesi Açık ders platformu, https://acikders.ankara.edu.tr/course/view.php?id=1011, 2020.

119. Hungerford, T. W., “Abstract Algebra: an Introduction”, *Cleveland State University, Nelson Education*, 2012.

120. İnternet: Wikipedia, “Kriptografi”, https://tr.wikipedia.org/wiki/Kriptografi, https://en. wikipedia .org/wiki/Cryptography, 2020.

121. İnternet: Wikipedia, “List_of_Cryptographer”, https://en.wikipedia.org/wiki/List _ of_cryptographers, 2020.

122. McEliece, K., R. J., "A Public-Key Cryptosystem Based on Algebraic Coding Theory", *DSN Progress Report*. 44: 114–116, 1978.

123. Arda, D., “Kodlama Teorisinin Kriptografik Açıdan Incelenmesi”, *Doktora tezi, Trakya Üniversitesi*, Edirne, 2011.

124. Özlü Ş., & Aktaş, H., “Error Correcting Soft Codes for Odd Numbers Which are Equalor Less then $(\frac{n}{2}-1)$”, *Journal of New Theory*, (2), 94-104, 2015.

125. Özlü Ş., “Bazı Sonlu Cisimler Üzerinde Esnek Polinom Kodlar”, *Nevşehir Hacı Bektaş Veli Üniversitesi Fen Bilimleri Enstitüsü*, Dr. Tezi, 2015.

126. Zararsız, Z., & Şengönül, M., “The Application Domain of Cesaro Matrix on Some Sequence Spaces of Fuzzy Numbers”, *International Journal of Mathematical Analysis*, *9*(1), 1-14, 2015.

127. Şengönül, M., & Zararsız, Z., "Some Additions to the Fuzzy Convergent and Fuzzy Bounded Sequence Spaces of Fuzzy Numbers", *Abstract and Applied Analysis,* Vol. 2011, Hindawi, 2011.

128. Kalkan, M., Aktaş, H., "On the Group Based Cryptography", *Journal of Mathematics and System Science, 4*(11), 2014.

129. Aktas, H., Kalkan, M., "An Application of the Crystography", *JMCS, 11*(2), 147-158, 2014.

130. Alagic, G., ve Ark, "Status Report on the Second Round of the NIST Post-quantum Cryptography Standardization Process", *US Department of Commerce, NIST*, 2020.

131. Taş O., Kiani, F., "Blok Zinciri Teknolojisine Yapılan Saldırılar Üzerine bir İnceleme", *Bilişim Teknolojileri Dergisi*, *11*(4), 369-382, 2018.

132. Aktaş, H., Çağman, N., "Soft Set and Soft Groups", Information Science 177, 2726-2735, 2007.

133. Acar, U., Koyuncu, F. Tanay, B., "Soft Sets and Soft Rings", Computers and Mathematics with Applications 59, 3458-3463, 2010.

134. Aktaş H., Çakır K., "Esnek Gruplar Üzerinde Bazı Cebirsel Uygulamalar", *Gaziosmanpaşa Bilimsel Araştırma Dergisi*, (2), 35-40, 2013.

135. Babitha K.V., Sunil, J.J., "Soft Set Relations and Functions", *Computers and Mathematics with Applications*, 60, 1840-1849, 2010.

136. Aktaş, H., & Özlü, Ş., "Cyclic Soft Groups and Their Applications on Groups", *The Scientific World Journal*, *2014*.

137. Sekhar, A. C. ve Ark, "Cyclic groups of Elliptic Curves-A Implemenation to Cryptography", *International Journal of Advanced Research in Computer Science,* 2(5), Sept –Oct, 2011, 544-546, 2011.

138. Adams, S. S., "Introduction to Algebraic Coding Theory" , *Franklin W. Olin College: NSF CCLI,* January 11, 2008.

139. Jan, C.A., "Coding Theory", van der Lubbe., *Information Theory*. Cambridge Press, 1997.

140. ElGamal, T. "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", *In Advances in Cryptology* (CRYPTO 1984), Springer LNCS 196, 10–18, 1985.

141. Bowman, J. C., “Cryptographic Error-Correcting Codes”, *Math422 Coding Theory and Cyptogaphy*, University of Alerta, Canada, 2015.

142. Aygün, E., Kılıç, B, "Soft Matrix Product and Soft Cyrptosystem," *International Conference on Algebra and Number Theory* , Samsun, Turkey, 2014.

143. Aygün, E., “AES Şifreleme ve Esnek Kümeler Yardımıyla Elde Edilen Yeni Bir Kriptosistem”, *Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, Cilt 35, Sayı 1, 2019.

144. Aygün, E., “AES Encryption and A Cryptosystem Obtained with Soft Set II”, *Cumhuriyet Science Journal*, *40*(1), 69-78, 2019.

145. Denizler, I. H., “Soyut Cebir”, *Yüzüncü Yıl Üniversitesi,* 2015.

146. Z Bobrysheva, J. & Zapechnikov, S., “Post-quantum Group Key Agreement Scheme”, In *Biologically Inspired Cognitive Architectures Meeting* (pp. 49-55). Springer, Cham

147. Kara, S., “Kod Tabanlı Kuantum Sonrası Bazı Şifreleme Algoritmaları ve Anahtar Kapsülleme Mekanizmalarının İncelenmesi*”* Master's thesis, *TOBB ETÜ Fen Bilimleri Enstitüsü,* 2020.

148. Saraç, B., “Cebirsel Kodlama Teorisine Giriş*”, Lecture, Hacettepe Üniversitesi*, 2019.

149. Rehman, I., Razzaque, A., & Shah, T., “A Novel Approach to Analyze S-boxes in Image Encryption Using Fuzzy Soft Set Aggregation Operator”, *J. Multiple Valued Log. Soft Comput.*, *28*(4-5), 495-510, 2017.

150. Cook, J., “Mixing Error-correcting Codes and Cryptography”, *https://www. johndcook.com/blog/2019/03/23/code-based-cryptography/*, 2019.

151. Cook, J., “Isogeny Based Cryptography”, *https:// www.johndcook.com/blog /2019 /04/20/isogeny-based-cryptography/* , 2019.

152. Ko, H.K, et all, “New Public-key Cryptosystem Using Braid Group”, *in Advances in Cryptology - CRYPTO 2000”, (M. Bellare, ed.), Lecture Notes in Computer Science 1880*, 166-183, 2000.

153. Artin, T, “The Theory of Braids,” *Annals of Math.* 48, 101-126, 1947.

154. Qiu, F. Q., & Xiong, Q. Research on Elliptic Curve Cryptography. *In 8th International Conference on Computer Supported Cooperative Work in Design*, (Vol. 2, pp. 698-701). IEEE, 2004

155. Bobrysheva, J., & Zapechnikov, S., "Post-quantum Group Key Agreement Scheme", In *Biologically Inspired Cognitive Architectures Meeting* (pp. 49-55). Springer, Cham, 2020.

156. Keller, S. "Agreement of Symmetric Keys Using Discrete Logarithm Cryptography Major Steps of Key Agreement," *Integers, pp.* 1–24, 2000.

157. Reza, A., Jalali, A., Jao, D. and Soukharev, V.. "Practical Supersingular Isogeny Group Key Agreement." *IACR Cryptol. ePrint Arch*. 2019.

158. İnternet: Microsoft, "AES Sınıf, Gelişmiş Şifreleme Standardı", *https://docs.microsoft.com/tr/tr/dotnet/api/system.security.cryptography.aes?view=net-5.0&viewFallbackFrom= dotnet-plat-ext-5.0*, 2021.

159. İnternet: Microsoft, "Eliptik Eğri Diffie-Hellman (ECDH) Algoritması", *https://docs.microsoft.com/trtr/dotnet/api/system.security.cryptography.Ecdiffiehellmancng? view=dotnet-plat-ext-5*.0, 2021.

160. Abdullah, S., & Amin, N. U., "Analysis of S-box Image Encryption Based on Generalized Fuzzy Soft Expert Set", *Nonlinear Dynamics*, *79*(3), 1679-1692, 2015.

161. Shah, T., Medhit, S., & Farooq, G., "Intuitionistic Fuzzy Soft Set Decision Criterion for Selecting Appropriate Block Cipher", *3D Research, 6*(3), 1-15, 2015.

162. Rehman, I., Razzaque, A., & Shah, T, "A Novel Approach to Analyze S-boxes in Image Encryption Using Fuzzy Soft Set Aggregation Operator", *J. Multiple Valued Log. Soft Comput., 28*(4-5), 495-510, 2017.

163. Razzaque, A., at el., "Application of Fuzzy Soft Sets to Analyze the Statistical Strength of S-boxes", *International Journal of Advanced and Applied Sciences*, 8(3) 2021, Pages: 30-35, 2020.

164. Khalaf, M. M., "Optimal Alternative for Suitability of S-boxes to Image Encryption Based on m-polar Fuzzy Soft Set Decision-making Criterion", *Journal of the Egyptian Mathematical Society*, *28*(1), 1-25, 2020.

EKLER

EK-1

```
using System;
using System.IO;
using System.Security.Cryptography;
namespace SoftAes_Example
{
   class SoftAesExample
   {
      public static void Main()
      {
         string original = " AES Şifreleme ve Esnek Kümeler Yardımıyla Elde Edilen
Yeni Bir Kriptosistem!";
         using (Aes myAes = Aes.Create())
         {
            byte[] encrypted = EncryptStringToBytes_Aes(original, SoftAes.Key,
SoftAes.IV);
            string roundtrip = DecryptStringFromBytes_Aes(encrypted, SoftAes.Key,
SoftAes.IV);
            Console.WriteLine("Original:   {0}", original);
            Console.WriteLine("Round Trip: {0}", roundtrip);
         }
      }
      static byte[] EncryptStringToBytes_Aes(string plainText, byte[] Key, byte[] IV)
      {
         if (plainText == null || plainText.Length <= 0)
            throw new ArgumentNullException("plainText");
         if (Key == null || Key.Length <= 0)
            throw new ArgumentNullException("Key");
         if (IV == null || IV.Length <= 0)
            throw new ArgumentNullException("IV");
```

```
            byte[] encrypted;

            using (Aes aesAlg = Aes.Create())
            {
                aesAlg.Key = Key;
                aesAlg.IV = IV;
                ICryptoTransform encryptor = aesAlg.CreateEncryptor(aesAlg.Key,
aesAlg.IV);
                using (MemoryStream msEncrypt = new MemoryStream())
                {
                    using (CryptoStream csEncrypt = new CryptoStream(msEncrypt,
encryptor, CryptoStreamMode.Write))
                    {
                        using (StreamWriter swEncrypt = new StreamWriter(csEncrypt))
                        {
                            swEncrypt.Write(plainText);
                        }
                        encrypted = msEncrypt.ToArray();
                    }
                }
            }
            return encrypted;
        }
        static string DecryptStringFromBytes_Aes(byte[] cipherText, byte[] Key, byte[]
IV)
        {
            if (cipherText == null || cipherText.Length <= 0)
                throw new ArgumentNullException("cipherText");
            if (Key == null || Key.Length <= 0)
                throw new ArgumentNullException("Key");
            if (IV == null || IV.Length <= 0)
                throw new ArgumentNullException("IV");
            string plaintext = null;
```

```
            using (Aes aesAlg = Aes.Create())
            {
                aesAlg.Key = Key;
                aesAlg.IV = IV;
                ICryptoTransform decryptor = aesAlg.CreateDecryptor(aesAlg.Key,
aesAlg.IV);
                using (MemoryStream msDecrypt = new MemoryStream(cipherText))
                {
                    using (CryptoStream csDecrypt = new CryptoStream(msDecrypt,
decryptor, CryptoStreamMode.Read))
                    {
                        using (StreamReader srDecrypt = new StreamReader(csDecrypt))
                        {
                            plaintext = srDecrypt.ReadToEnd();
                        }
                    }
                }
            }
            return plaintext;
        }
    }
}
```

EK-2

```
using System;
using System.IO;
using System.Security.Cryptography;
using System.Text;
public class Alice
{
   public static byte[] alicePublicKey;
   public static void Main(string[] args)
   {
      using (ECDiffieHellmanCng alice = new ECDiffieHellmanCng())
      {
         alice.KeyDerivationFunction = ECDiffieHellmanKeyDerivationFunction.Hash;
         alice.HashAlgorithm = CngAlgorithm.Sha256;
         alicePublicKey = alice.PublicKey.ToByteArray();
         Bob bob = new Bob();
         CngKey k = CngKey.Import(bob.bobPublicKey,
CngKeyBlobFormat.EccPublicBlob);
         byte[] aliceKey = alice.DeriveKeyMaterial(CngKey.Import(bob.bobPublicKey,
CngKeyBlobFormat.EccPublicBlob));
         byte[] encryptedMessage = null;
         byte[] iv = null;
         Send(aliceKey, "Nevşehir Üniversitesi Fen Bilimleri Enstitüsü Matematik ABD
Esnek Diffie Helman  Tasarımı", out encryptedMessage, out iv);
         bob.Receive(encryptedMessage, iv);
      }
   }
   private static void Send(byte[] key, string secretMessage, out byte[]
encryptedMessage, out byte[] iv)
   {
      using (SoftAes aes = new AesCryptoServiceProvider())
      {
```

```
            aes.Key = key;
            iv = aes.IV;
            using (MemoryStream ciphertext = new MemoryStream())
            using (CryptoStream cs = new CryptoStream(ciphertext, aes.CreateEncryptor(),
CryptoStreamMode.Write))
            {
                byte[] plaintextMessage = Encoding.UTF8.GetBytes(secretMessage);
                cs.Write(plaintextMessage, 0, plaintextMessage.Length);
                cs.Close();
                encryptedMessage = ciphertext.ToArray();
            }
        }
    }
}
public class Bob
{
    public byte[] bobPublicKey;
    private byte[] bobKey;
    public Bob()
    {
        using (ECDiffieHellmanCng bob = new ECDiffieHellmanCng())
        {
            bob.KeyDerivationFunction = ECDiffieHellmanKeyDerivationFunction.Hash;
            bob.HashAlgorithm = CngAlgorithm.Sha256;
            bobPublicKey = bob.PublicKey.ToByteArray();
            bobKey = bob.DeriveKeyMaterial(CngKey.Import(Alice.alicePublicKey,
CngKeyBlobFormat.EccPublicBlob));
        }
    }
    public void Receive(byte[] encryptedMessage, byte[] iv)
    {
        using (SoftAes aes = new AesCryptoServiceProvider())
        {
```

```
            aes.Key = bobKey;
            aes.IV = iv;
            using (MemoryStream plaintext = new MemoryStream())
            {
                using (CryptoStream cs = new CryptoStream(plaintext,
aes.CreateDecryptor(), CryptoStreamMode.Write))
                {
                    cs.Write(encryptedMessage, 0, encryptedMessage.Length);
                    cs.Close();
                    string message = Encoding.UTF8.GetString(plaintext.ToArray());
                    Console.WriteLine(message);
                }
            }
        }
    }
}
```