Yüksek Lisans Tezi

Büşra KILIÇ

Matematik

2015

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

ESNEK MATRİS ÇARPIMI VE ESNEK KRİPTOSİSTEM

Hazırlayan
Büşra KILIÇ

Danışman
Yrd. Doç. Dr. Emin AYGÜN

Yüksek Lisans Tezi

Temmuz 2015
KAYSERİ

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

ESNEK MATRİS ÇARPIMI VE ESNEK KRİPTOSİSTEM

Hazırlayan

Büşra KILIÇ

Danışman

Yrd. Doç. Dr. Emin AYGÜN

Temmuz 2015

KAYSERİ

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

Büşra KILIÇ

“ESNEK MATRİS ÇARPIMI VE ESNEK KRİPTOSİSTEM” adlı Yüksek Lisans tezi, Erciyes Üniversitesi Lisansüstü Tez Önerisi ve Tez Yazma Yönergesi’ ne uygun olarak hazırlanmıştır.

Tezi Hazırlayan
Büşra KILIÇ

Danışman
Yrd. Doç. Dr. Emin AYGÜN

Matematik ABD Başkanı
Prof. Dr. İlhan ÖZTÜRK

Yrd. Doç. Dr. Emin AYGÜN danışmanlığında **Büşra KILIÇ** tarafından hazırlanan **"Esnek Matris Çarpımı ve Esnek Kriptosistem"** adlı bu çalışma, jürimiz tarafından Erciyes Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalında **Yüksek Lisans** tezi olarak kabul edilmiştir.

15 /07 /2015

JÜRİ:

Danışman : Yrd. Doç. Dr. Emin AYGÜN

Üye : Doç. Dr. Hacı Aktaş

Üye : Doç. Dr. Akın Osman Atagün

ONAY:

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

/ /

Prof. Dr. Kâzım KEŞLİOĞLU

Enstitü Müdürü

TEŞEKKÜR

Bu tez çalışması boyunca tecrübesi ve bilgi birikimiyle yoluma ışık tutan, desteğini ve yardımlarını esirgemeyen değerli hocalarım Yrd. Doç. Dr. Emin AYGÜN' e ve Doç. Dr. Akın Osman ATAGÜN' e teşekkürü bir borç bilirim.

Ayrıca öğrenim hayatım boyunca sabır göstererek beni daima destekleyen aileme en içten teşekkürlerimi sunarım.

Büşra KILIÇ

Kayseri, Temmuz 2015

ESNEK MATRİS ÇARPIMI VE ESNEK KRİPTOSİSTEM

Büşra KILIÇ
Erciyes Üniversitesi, Fen Bilimleri Enstitüsü
Yüksek Lisans Tezi, Temmuz 2015
Tez Danışmanı: Yrd. Doç. Dr. Emin AYGÜN

ÖZET

Bu tez dört bölümden oluşmaktadır.

Birinci bölümde, esnek kümeyi ve esnek kümeleri temsil eden esnek matrisleri tanımlayacağız. Bu temsil, bilgisayar hafızasında esnek kümeyi saklamak için kullanışlıdır. Kriptosistem ile ilgili tanımlar vereceğiz.

İkinci bölümde, esnek matrislerin invers çarpımını ve karakteristik çarpımını tanımlayacağız ve özelliklerini vereceğiz.

Üçüncü bölümde, esnek kümelere ve esnek matrislere dayanan yeni bir şifreleme algoritması vereceğiz. Esnek şifreleme ve esnek deşifrelemeyi tanımlayacağız.

Dördüncü bölümde, esnek şifreleme ve esnek deşifreleme örnekleri vereceğiz.

Anahtar Kelimeler: Esnek küme, esnek matris, kriptosistem, invers çarpım, karakteristik çarpım, esnek şifreleme, esnek deşifreleme.

SOFT MATRIX PRODUCT AND SOFT CRYPTOSYSTEM

Büşra KILIÇ
Erciyes University, Graduate School of Natural and Applied Sciences
M. Sc. Thesis, July 2015
Thesis Supervisor: Assist. Prof. Dr. Emin AYGÜN

ABSTRACT

This thesis consists of four chapters.

In the first chapter, we define soft set and soft matrices which are representative of the soft sets. This style of representation is useful for storing a soft set in computer memory. We give definitions of with related cryptosystem.

In the second chapter, we define inverse product, characteristic product of soft matrices and give their properties.

In the third chapter, we suggest a new encryption scheme which are based on soft sets and soft matrices. We define soft encryption and soft decryption.

In the fourth chapter, we give examples of soft encryption and soft decryption.

Keywords: Soft set, soft matrix, inverse product, cryptosystem, characteristic product, soft encryption, soft decryption.

İÇİNDEKİLER

ESNEK MATRİS ÇARPIMI VE ESNEK KRİPTOSİSTEM

TABLOLAR LİSTESİ

KISALTMALAR VE SEMBOLLER

U : Evrensel küme

$P(U)$: U 'nun kuvvet kümesi

E : Parametreler kümesi

(f_A, E) : Esnek küme

f_A : (f_A, E) esnek kümesinin yaklaşım fonksiyonu

$f_A(e)$: e yaklaşımlı değer veya e yaklaşımlı küme

$\tilde{\subseteq}$: Esnek altküme

Φ : Boş esnek küme

$(f_{\tilde{A}}, E)$: Mutlak esnek küme

(f_A^c, E) : Esnek küme tümleyeni

R_A : Bağıntı formu

X_{R_A} : R_A' nın karakteristik fonksiyonu

$\left[a_{ij}\right]_{m\times n}$: $m\times n$ tipindeki esnek matris

$SM_{m\times n}$: U üzerindeki bütün $m\times n$ tipindeki esnek matrislerin kümesi

$\left[\tilde{a}_{ij}\right]$: $A-$evrensel esnek matris

$\tilde{\subset}$: Öz esnek altküme

$\tilde{\cup}$: Esnek matris birleşimi

$\tilde{\cap}$: Esnek matris kesişimi

$[a_{ij}]^c$: Esnek matris tümleyeni

$\wedge$: Ve – çarpımı

$\vee$: Veya- çarpımı

$\overline{\wedge}$: Ve- Tümleyen- çarpımı

$\overline{\vee}$: Veya- Tümleyen- çarpımı

$\cdot_i$: Esnek matrislerde invers çarpım

$\cdot_c$: Esnek matrislerde karakteristik çarpım

GİRİŞ

Ekonomi, mühendislik ve çevre bilimindeki karmaşık problemlerde çeşitli belirsizlik tiplerinin var olmasından dolayı, bu problemleri çözmek için, klasik metotları başarılı bir şekilde kullanamayız. Belirsizlikle başa çıkmak için matematiksel bir araç olarak göz önüne alabileceğimiz, olasılık teorisi, bulanık kümeler teorisi, aralık matematiği, yaklaşımlı kümeler teorisi ve esnek kümeler teorisi gibi teoriler geliştirildi. Her bir teorinin güçlü olduğu uygulamalar bulunmaktadır. Bu teorilerden arasından en göze çarpanlardan birisi, Zadeh' in [1] bulanık kümeler teorisidir. Bu teori hızla gelişmesine rağmen bazı yapısal zorluklara sahiptir. Bir bulanık küme onun üyelik fonksiyonu yoluyla tanımlanır. Molodtsov' a [2] göre üyelik fonksiyonun doğasının fazlasıyla bireysel olmasından dolayı, her bir durum için bir üyelik fonksiyonu inşa etme zorluğuyla karşılaşılır. Bu nedenle, üyelik fonksiyonu inşasından bağımsız bir kümeler teorisine ihtiyaç vardır.

Esnek kümeler teorisi, Molodtsov [2] tarafından belirsizlikle başa çıkmak için bir matematiksel araç olarak ortaya atılmıştır. Molodtsov [2] sürekli diferansiyellenebilir fonksiyonlar, oyun teorisi, işlem araştırmaları, Riemann integrasyonu, Perron integrasyonu, olasılık, ölçüm teorisi vb. alanlarda esnek küme teorisini kullanarak, başarılı çalışmalar yaptı.

Maji ve arkadaşları [3,4] ve Pawlak' ın [5] yaklaşımlı küme teorisi yardımıyla, bir karar verme probleminde esnek kümelerin bir uygulamasını sundu ve esnek kümelerde bazı işlemleri tanımladı. Xiao ve arkadaşları [6] esnek küme temelli iş rekabet kapasitesi için yapay bir hesaplama metodu üzerine bir çalışma yaptı. Yang ve arkadaşları [7] esnek kümelere ve yaklaşımlı kümelere dayalı klinik teşhisin karar analizi ve indüksiyon başlıklı bir çalışma yaptı. Chen ve arkadaşları [8,9] ile Kong ve arkadaşları [10] esnek kümelerde parametre indirgemesi üzerine çalışmalar yaptı. Xiao ve arkadaşları [11] ile

Pei ve Miao [12] esnek tabanlı bilgi sistemleri üzerine çalışmalar sundular. Mushrif ve arkadaşları [13] esnek küme temelli sınıflandırmalar üzerine bir çalışma yaptı.

Esnek kümelerin cebirsel özellikleri bazı yazarlar tarafından çalışılmaktadır. Aktaş ve Çağman [14], esnek grupların yeni bir tanımını vererek bazı temel özelliklerini elde etti. Jun [15] esnek BCK/BCI- cebirleri ve esnek altcebir kavramlarını ortaya atarak, onların bazı temel özelliklerini türetti. Jun ve Park [16] esnek kümeleri BCK/BCI- cebirlerine uygulayarak, BCK/BCI- cebirlerinde esnek kümelerin cebirsel özelliklerini tartıştı. Park ve arkadaşları [17] esnek WS- cebirleri üzerine bir çalışma yaptı. Feng ve arkadaşları [18] esnek küme teorisini kullanarak esnek yarı halka çalışmasını başlattı ve değişik ilişki özelliklerini açıkladı. Sun ve arkadaşları [19] esnek modüllerin tanımını verdi. Ayrıca modülleri ve Molodtsov' un esnek küme tanımını kullanarak bazı temel özellikleri inşa etti.

Zou ve Xiao [20] eksik bilgi adı altında esnek kümelerin veri analizi yaklaşımını ortaya koydu. Bu yaklaşımlar esnek kümelerde eksik verilerin mevcut durumlarını yansıtmak için tercih edilebilir.

Çağman ve Enginoğlu [21] esnek matris teorisini tanımladılar Atagün ve Sezgin [22] esnek küme işlemleri üzerine çalıştılar. Sezgin, Atagün ve Aygün [23] esnek yakın-halkalar ve idealist esnek yakın-halkalar ile ilgili çalışmalar yaptılar.

Maji ve arkadaşları [24] bulanık esnek kümeleri tanımladı. Daha sonra pek çok araştırmacı bulanık esnek kümeler üzerine çalışmalar yaptı. Aktaş ve Çağman [14] esnek kümeleri, bulanık kümeler ve yaklaşımlı kümelerin ilgili kavramlarıyla karşılaştırdı. Roy ve Maji [25] bir karar verme probleminde bulanık esnek kümelerin bir uygulaması üzerinde bazı sonuçlar ortaya koydu. Yang ve arkadaşları [26] bulanık esnek kümelerde indirgemeyi tanımlayarak, bulanık esnek kümeler yoluyla bir karar verme problemini analiz etti. Majumdar ve Samantha [27] bulanık esnek kümelerde benzerlik ölçümünü ortaya koydu. Kong ve arkadaşları [28] ile Xiao ve arkadaşları [29] bulanık esnek küme üzerine dayalı bazı yaklaşımları konu alan bir çalışma yaptı.

Molodtsov ve arkadaşları [30] tarafından esnek küme teorisi üzerine dayalı bir analiz geliştirerek, esnek sayı, esnek türev, esnek integral gibi kavramlar formüle edildi. Bu

analiz, Kovkov ve arkadaşları [31] tarafından optimizasyon teorisi ile ilgili problemlere uygulandı. Şu anda esnek küme teorisi ve onun uygulamaları üzerine yapılan çalışmalar hızla gelişmektedir. Esnek küme üzerindeki farklı işlemlerin temel analizi Ali ve arkadaşları [32] tarafından açıklandı. Çağman ve Enginoğlu [33], Molodtsov'un [2] esnek kümelerindeki işlemleri, farklı yeni sonuçlar elde etmek için daha fonksiyonel yaparak yeniden tanımladı. Bu yeni tanımları kullanarak esnek karar verme metotlarını yaptılar.

Diğer taraftan, iletilmek istenen veri açık ağlar üzerinden iletildiğinde veri istenmeyen kişiler tarafından dinlenme veya değiştirilme tehdidi altındadır. Söz konusu veri şifrelenmemiş düz metindir. Şifreleme düz bir metnin içeriğini, istenmeyen şahıslar tarafından okunmasını engellemek için iletiyi bir takım yöntemlerle okunamayacak hale getirme işlemidir. Bu işlem sonucunda düz metin şifrelenmiş olur ve böylelikle bilginin içeriği başkaları tarafından anlaşılamayacak hale gelir. Şifreleme işlemi sonucu oluşan metine şifreli metin denir. Deşifreleme ise şifrelemenin tam tersi olup, şifreli metnin düz metne çevrilmesi işlemidir.

Kriptanaliz ise bazı teknikler kullanılarak ele geçen şifrelenmiş metinden şifrelenmemiş metni bulma yöntemidir. Kriptanaliz ile uğraşanlara ise kriptanalist denir. İyi bir kriptanalist aynı zamanda kriptografi konusunda da iyi olmalıdır, çünkü şifrelerin nasıl tasarlanabileceğini bilmeyen biri nasıl çözüleceği konusunda fikir de yürütemez. Kriptanalistlerin başarısı kriptografları yeni ve daha güvenli sistemler tasarlamaya zorlamıştır. Kriptoloji, matematiğin hem şifre bilimini(kriptografi), hem de şifre analizini(kriptanaliz) kapsayan bir dalıdır. Kriptoloji, kişiler arası veya özel devlet kurumları arasındaki mesajlaşmalardan, sistemlerin oluşumunda ve işleyişindeki güvenlik boşluklarına kadar her türlü dalla alakalıdır. Kriptoloji ile ilgilenen bilim adamlarına kriptolog denir.

Kriptografi, çeşitli iletilerin, bilgilerin herkese açık ortamlarda iletilirken istenmeyen kişiler tarafından kullanılmasını veya değiştirilmesini önlemek amaçlı kullanılır. Kriptografi, bilgiyi güvenli bir şekilde sadece istenilen kişiye ulaştırmak amacıyla uzun süredir kullanılmaktadır. Tarihin bilinen ilk şifreleme yöntemi yer değiştirme ve harf değiştirme yöntemidir. Bu yöntemlerden ilki bir yazıdaki harflerin yerlerini değiştirerek, ikincisi ise harfleri başka harflerle değiştirerek gerçekleştirilir.

Şifreleme amaçlı kullanılan algoritmanın güvenliği bu algoritmanın saklı tutulması ile sağlanıyorsa bu bir sınırlandırılmış algoritmadır. Bu tür algoritmalar günümüz şartlarına pek uymamaktadır. Algoritmanın güvenliği sadece gizli tutulmasıyla sağlandığından istenmeyen bir durumda algoritmanın açığa çıkması ile kullanılan tüm sistemin değiştirilmesi gerekir. Günümüzde bu sorun açık algoritma, gizli anahtar tekniği ile giderilmektedir. Günümüzde kullanılan şifreleme algoritmaları artık gizli değildir. Bilginin güvenliği algoritmanın gizlenmesi ile değil, iletiyi şifrelemek amaçlı kullanılan anahtarın saklı tutulması ile sağlanır. Kullanılan anahtar çok çeşitli değerler alabilir ve yalnızca bu anahtara sahip kişiler istenilen bilgiye ulaşabilir. Şifreleme sistemlerinde kullanılan anahtarların özgün olması ve kendini tekrarlamaması istenir.

Kriptografik sistemler önceleri askeri amaçlı kullanıldıysa da gelişen teknoloji ile birlikte ortaya çıkan güvenlik açığını kapatmak ve bilginin güvenilir bir şekilde taşınmasını sağlamak amacıyla sivil yaşamda da yerini almıştır.

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

İletişim tekniklerindeki gelişmeler bilgiyi saklama ve iletme açısından işleri zorlaştırmakta, yeni teknikler geliştirmek için insanları zorlamaktadır. Telefon görüşmeleri uydudan yansımakta; internet üzerinden yapılan her işlem de binlerce bilgisayarlardan geçmektedir. Haberleşme ve bilişimin genel sorunu bilgi güvenliğidir. Özellikle son yıllarda artan internet üzerinden yapılan sanal alışverişler, bireysel bankacılık işlemleri ve e-posta trafiği interneti daha güvenli bir ortam olmaya zorlamaktadır. İnternet üzerindeki ticari işlemler, yılda milyar dolarları aşmaktadır. Rakamlar bu kadar yüksek olunca kriptografik güvenlik yöntemlerinin kullanımı zorunlu hale gelmiştir. İnternet üzerinde ise tam güvenliği sağlamak olanaksızdır. İnternet altyapısında ve haberleşme araç gereçlerinde teknolojiyi belirleyenler, haberleşme ve güvenlik konularında da en avantajlı ülkelerdir. Çünkü köprünün başını tutan kimin geçeceğine de karar verir. O halde sorun, bilgi ve haberleşme güvenliğinin

yüksek oranda sağlanmasının nasıl gerçekleşeceğidir. Bunu sağlayacak olan da şifrebilimdir. Tüm bunlar, günümüzde teknolojinin gelişmesiyle ortaya çıkan güvenlik problemlerinin çözülmesinin ve eski çağlardaki kodlamadan yola çıkan ve günümüzde disiplinlerarası bir bilim haline gelmiş kriptografinin ne denli önemli olduğunu göstermektedir.

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

Bu tez çalışmasının, ilk bölümünde esnek kümeyi ve esnek matrisleri tanımlayacağız, esnek matrisle ilgili özellikleri, esnek matrislerin çarpımını ve kriptosistemle ilgili tanımları vereceğiz. İkinci bölümünde, esnek matrislerin invers çarpımını, karakteristik çarpımını ve ilgili özelliklerini tanımlayacağız. Üçüncü bölümünde, esnek şifreleme ve esnek deşifrelemeyi tanımlayacağız. Son bölümünde, bu yöntemlerin başarılı olduğunu gösteren örnekler vereceğiz.

BÖLÜM 1

TEMEL TANIMLAR VE TEOREMLER

Bu bölümde, esnek kümeyi ve esnek kümeleri temsil eden esnek matrisleri tanımlayacağız. Bu temsil, bilgisayar hafızasında bir esnek kümeyi saklamak için kullanışlıdır. İşlemler kullanışlı matrisler ile temsil edilebilecektir. Esnek matrislerin çarpım tanımlarını ve son olarak da kriptosistemle ilgili tanımları vereceğiz.

1.1. Esnek Kümeler

Tanım 1.1.1. U bir evrensel küme, $P(U)$ U'nun kuvvet kümesi, E parametreler kümesi ve $A \subseteq E$ olsun. Bu durumda $f_A: E \to P(U)$ olmak üzere

$$(f_A, E) = \left\{\left(e, f_A(e)\right) : e \in E, f_A(e) \in P(U) | e \notin A \; ise \; f_A(e) = \emptyset\right\}$$

şeklinde tanımlanan (f_A, E) ikilisine U üzerinde bir esnek küme denir. Burada, f_A'ya (f_A, E) esnek kümesinin yaklaşım fonksiyonu denir. $f_A(e)$'ye e yaklaşımlı değer veya e yaklaşımlı küme denir. (f_A, E) esnek kümesi (F, A) veya F_A şeklinde de gösterilebilir. Ayrıca (f_A, E) esnek kümesi $(f_A, E) = \{f_A(e) | e \in A\}$ olarak da ifade edilebilir [2].

Örnek 1.1.2. $U = \{u_1, u_2, u_3, u_4, u_5\}$ bir evrensel küme, $E = \{e_1, e_2, e_3, e_4, e_5\}$ parametreler kümesi olsun. $A = \{e_1, e_3, e_4\}$ ise, $f_A(e_1) = \{u_1, u_2\}$, $f_A(e_3) = \{u_2, u_4\}$ ve $f_A(e_4) = \{u_3, u_4, u_5\}$ olsun. U üzerinde (f_A, E) esnek kümesi ise $(f_A, E) = \{(e_1, \{u_1, u_2\}), (e_3, \{u_2, u_4\}), (e_4, \{u_3, u_4, u_5\})\}$ şeklindedir.

Tanım 1.1.3. U üzerinde (f_A, E) ve (g_B, E)esnek kümeleri için,

i. $A \subseteq B$ ve
ii. $\forall\, e \in A$ için $f_A(e) = g_B(e)$

ise (f_A, E), (g_B, E)' nin esnek alt kümesidir denir ve $(f_A, E) \tilde{\subseteq} (g_B, E)$ şeklinde gösterilir [4].

Tanım 1.1.4. Eğer U üzerinde (f_A, E), (g_B, E)' nin esnek alt kümesi ve (g_B, E)' de (f_A, E)'nin esnek alt kümesi ise bu durumda (g_B, E) ve (f_A, E), U üzerinde esnek eşittir denir [4].

Tanım 1.1.5. (f_A, E), U üzerinde bir esnek küme olsun.

i. $\forall e \in E$ için $f_A(e) = \emptyset$ ise bu durumda (f_A, E) esnek kümesine boş esnek küme denir ve $(f_A, E) = \Phi$ şeklinde gösterilir.
ii. $\forall e \in E$ için $f_A(e) = U$ ise bu durumda (f_A, E)' ye mutlak esnek küme denir ve $(f_A, E) = (f_{\tilde{A}}, E)$ şeklinde gösterilir [4].

Önerme 1.1.6. (f_A, E), (f_B, E) ve (f_C, E), U üzerinde esnek kümeler olsun. Bu durumda,

i. $(f_A, E) \tilde{\subseteq} (f_E, E)$,
ii. $\Phi \tilde{\subseteq} (f_A, E)$,
iii. $(f_A, E) \tilde{\subseteq} (f_A, E)$,
iv. $(f_A, E) \tilde{\subseteq} (f_B, E)$ ve $(f_B, E) \tilde{\subseteq} (f_C, E)$ ise $(f_A, E) \tilde{\subseteq} (f_C, E)$' dir [4].

Tanım 1.1.7. (f_A, E), U üzerinde bir esnek küme olsun. (f_A, E)' nin tümleyeni olan, $\forall e \in E$ için yaklaşım fonksiyonu ile tanımlanır [4].

Önerme 1.1.8. (f_A, E), U üzerinde bir esnek küme olsun. Bu durumda,

i. $(f^c{}_A, E)^c = (f_A, E)$,
ii. $\Phi^c = (f_E, E)$' dir [4].

1.2. Esnek Matrisler

Tanım 1.2.1. (f_A, E), U üzerinde bir esnek küme olsun.
$R_A = \{(u, e): e \in A, u \in f_A(e)\}$ şeklinde tanımlanan $U \times E$' nin alt kümesine (f_A, E)' nin bir bağıntı formu denir.

$$X_{R_A}: U \times E \to \{0,1\}, \quad X_{R_A}(u,e) = \begin{cases} 1, & (u,e) \in R_A \; ise \\ 0, & (u,e) \notin R_A \; ise \end{cases}$$

ile tanımlanan fonksiyona R_A' nın karakteristik fonsiyonu denir.

Eğer $U = \{u_1, u_2, \dots, u_m\}$, $E = \{e_1, e_2, \dots, e_n\}$ ve $A \subseteq E$ ise, bu durumda R_A,

Tablo 1.1. Bağıntı formunun karakteristik fonksiyon yoluyla temsili

R_A	e_1	e_2	…	e_n
u_1	$X_{R_A}(u_1, e_1)$	$X_{R_A}(u_1, e_2)$	…	$X_{R_A}(u_1, e_n)$
u_2	$X_{R_A}(u_2, e_1)$	$X_{R_A}(u_2, e_2)$	…	$X_{R_A}(u_2, e_n)$
⋮	⋮	⋮	⋱	⋮
u_m	$X_{R_A}(u_m, e_1)$	$X_{R_A}(u_m, e_2)$	…	$X_{R_A}(u_m, e_n)$

şeklinde ifade edilebilir. Eğer $a_{ij} = X_{R_A}(u_i, e_j)$ dersek, bu durumda U üzerindeki (f_A, E) esnek kümesi

$$[a_{ij}]_{m \times n} = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}$$

$m \times n$ tipindeki bir matrisle temsil edilebilir ve buna**.** (f_A, E)' nin esnek matrisi denir. Bu tanıma göre bir (f_A, E) esnek kümesi $[a_{ij}]_{m\times n}$ matrisi tarafından tek türlü belirtilir. Bunun anlamı bir (f_A, E) esnek kümesi $[a_{ij}]_{m\times n}$ matrisine eşittir. Sonuç olarak, herhangi bir esnek kümeyi onun esnek matrisi ile temsil edebiliriz. U üzerindeki bütün $m \times n$ tipindeki matrislerin kümesini $SM_{m\times n}$ sembolü ile göstereceğiz ve $[a_{ij}] \in SM_{m\times n}$ ifadesi $i = 1,2, \dots, m$ ve $j = 1,2, \dots, n$ için $[a_{ij}]'$ nin $m \times n$ tipinde bir matris olduğunu gösterdiğinden, $[a_{ij}]_{m\times n}{}'$ nin yerine $[a_{ij}]'$ yi kullanacağız [33].

Örnek 1.2.2. $U = \{u_1, u_2, u_3, u_4, u_5\}$ bir evrensel küme ve $E = \{e_1, e_2, e_3, e_4\}$ tüm parametrelerin kümesi olsun. $A = \{e_1, e_2, e_4\}$ ise, $f_A(e_1) = \{u_2, u_3, u_4\}$, $f_A(e_2) = \{u_1, u_3, u_5\}$ ve $f_A(e_4) = \{u_2, u_4, u_5\}$ olsun. U üzerinde (f_A, E) esnek kümesi ise $(f_A, E) = \{(e_1, \{u_2, u_3, u_4\}), (e_2, \{u_1, u_3, u_5\}), (e_4, \{u_2, u_4, u_5\})\}$ olur ve $(f_A, E)'$ nin bağıntı formu

$R_A = \{(u_2, e_1), (u_3, e_1), (u_4, e_1), (u_1, e_2), (u_3, e_2), (u_5, e_2), (u_2, e_4), (u_4, e_4), (u_5, e_4)\}$

olur. Sonuç olarak $[a_{ij}]$ esnek matrisi

$$[a_{ij}] = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

şeklinde olur.

Tanım 1.2. 3. $[a_{ij}] \in SM_{m\times n}$ olsun.

i. Her $i \; ve \; j$ için $a_{ij} = 0$ ise, $[a_{ij}]$' ye sıfır esnek matris denir ve [0] ile gösterilir.

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

iii. Her $i \; ve \; j$ için $a_{ij} = 1$ ise, $[a_{ij}]$' ye evrensel esnek matris denir ve [1] ile gösterilir [33].

Örnek 1.2.4. $U = \{u_1, u_2, u_3, u_4, u_5\}$ bir evrensel küme ve $E = \{e_1, e_2, e_3, e_4\}$ tüm parametrelerin kümesi ve $[a_{ij}], [b_{ij}], [c_{ij}] \in SM_{5\times4}$ olsun.

Eğer $A = \{e_1, e_4\}$ ve $f_A(e_1) = \emptyset$, $f_A(e_4) = \emptyset$ ise bu durumda $[a_{ij}] = 0$‘ dır ve

$$[0] = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

şeklindedir.

Eğer $B = \{e_2, e_3\}$ ve $f_B(e_2) = U$, $f_B(e_3) = U$ ise bu durumda $[b_{ij}] = [\tilde{b}_{ij}]$‘ dir ve

$$[\tilde{b}_{ij}] = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$

şeklindedir.

Eğer $C = E$ ve $t$üm $e_i \in C'ler$ $için$ $f_C(e_i) = U$ ise $[c_{ij}] = [1]$‘ dir ve

$$[1] = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

şeklindedir.

Tanım 1.2.5. $[a_{ij}], [b_{ij}] \in SM_{m\times n}$ olsun. Bu durumda,

i. Her i ve j için $a_{ij} \leq b_{ij}$ ise, $[a_{ij}]$’ ye $[b_{ij}]$’ nin esnek altmatrisi denir ve $[a_{ij}] \tilde{\subseteq} [b_{ij}]$ ile gösterilir.

ii. Her $i\ ve\ j$ için $a_{ij} \leq b_{ij}$ ve en az bir terimi için $a_{ij} < b_{ij}$ ise $[a_{ij}]$' ye $[b_{ij}]$' nin öz esnek altmatrisi denir ve $[a_{ij}] \tilde{\subset} [b_{ij}]$ ile gösterilir.

iii. Her $i\ ve\ j$ için $a_{ij} = b_{ij}$ ise $[a_{ij}]$ ve $[b_{ij}]$ esnek eşit matristir denir ve $[a_{ij}]$=$[b_{ij}]$ ile gösterilir [33].

Örnek 1.2.6. $[a_{ij}] = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}, [b_{ij}] = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$ olsun. Bu durumda her $i\ ve\ j$ için $a_{ij} \leq b_{ij}$ olduğundan $[a_{ij}] \tilde{\subseteq} [b_{ij}]$' dir.

$$[a_{ij}] = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}, [b_{ij}] = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

olsun. Bu durumda $a_{42} < b_{42}$ ve her $i\ ve\ j$ için $a_{ij} \leq b_{ij}$ olduğundan $[a_{ij}] \tilde{\subset} [b_{ij}]$ şeklindedir.

Tanım 1.2.7. $[a_{ij}], [b_{ij}] \in SM_{m\times n}$ olsun. Bu durumda,

i. Her $i\ ve\ j$ için $[a_{ij}] \tilde{\cup} [b_{ij}] = [c_{ij}]$, $c_{ij} = max\{a_{ij}, b_{ij}\}$ şeklinde tanımlanan $[c_{ij}]$' ye $[a_{ij}]$ ve $[b_{ij}]$' nin birleşimi denir.

ii. Her $i\ ve\ j$ için $[a_{ij}] \tilde{\cap} [b_{ij}] = [c_{ij}]$, $c_{ij} = min\{a_{ij}, b_{ij}\}$ şeklinde tanımlanan $[c_{ij}]$' ye $[a_{ij}]$ ve $[b_{ij}]$' nin kesişimi denir.

iii. Her $i\ ve\ j$ için $c_{ij} = 1 - a_{ij}$ ise $[c_{ij}]$' ye $[a_{ij}]$' nin tümleyeni denir ve $[c_{ij}] = [a_{ij}]^c$ şeklinde gösterilir [33].

Tanım 1.2.8. $[a_{ij}], [b_{ij}] \in SM_{m\times n}$ olsun. Bu durumda her $i\ ve\ j$ için $[a_{ij}] \tilde{\cap} [b_{ij}] = [0]$ ise $[a_{ij}]$ ve $[b_{ij}]$ ayrıktır denir [33].

Örnek 1.2.9. $[a_{ij}] = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}, [b_{ij}] = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ olsun. Bu durumda

$$[a_{ij}] \tilde{\cup} [b_{ij}] = [c_{ij}] = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}, [a_{ij}] \tilde{\cap} [b_{ij}] = [c_{ij}] = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

$$[a_{ij}]^c = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

şeklindedir.

Önerme 1.2.10. $[a_{ij}], [b_{ij}], [c_{ij}] \in SM_{m\times n}$ olsun. Bu durumda,

i. $[a_{ij}] \tilde{\cap} [a_{ij}] = [a_{ij}]$,

ii. $[a_{ij}] \tilde{\cap} [0] = [0]$,

iii. $[a_{ij}] \tilde{\cap} [1] = [a_{ij}]$,

iv. $[a_{ij}] \tilde{\cap} [a_{ij}]^c = [0]$,

v. $[a_{ij}] \tilde{\cap} [b_{ij}] = [b_{ij}] \tilde{\cap} [a_{ij}]$,

vi. $([a_{ij}] \tilde{\cap} [b_{ij}]) \tilde{\cap} [c_{ij}] = [a_{ij}] \tilde{\cap} ([b_{ij}] \tilde{\cap} [c_{ij}])$ [33].

Önerme 1.2.11. $[a_{ij}], [b_{ij}] \in SM_{m\times n}$ olsun. Bu durumda aşağıdaki De Morgan' s yasaları geçerlidir.

i. $([a_{ij}] \tilde{\cup} [b_{ij}])^c = [a_{ij}]^c \tilde{\cap} [b_{ij}]^c$,

ii. $([a_{ij}] \tilde{\cap} [b_{ij}])^c = [a_{ij}]^c \tilde{\cup} [b_{ij}]^c$ [33].

1.3. Esnek Matrislerin Çarpımı

Bu kısımda, dört çeşit esnek matris çarpımını tanımlayacağız.

Tanım 1.3.1. $[a_{ij}], [b_{ij}] \in SM_{m\times n}$ olsun. Bu durumda $[a_{ij}]$ ve $[b_{ik}]$' nin Ve- çarpımı $\wedge: SM_{m\times n} \times SM_{m\times n} \to SM_{m\times n^2}$, $[a_{ij}] \wedge [b_{ik}] = [c_{ip}]$ burada $c_{ip} = min\{a_{ij}, b_{ik}\}, p = n(j-1)+k$ şeklinde tanımlanır [33].

Tanım 1.3.2. $[a_{ij}], [b_{ij}] \in SM_{m\times n}$ olsun. Bu durumda $[a_{ij}]$ ve $[b_{ik}]$' nin Veya-çarpımı $\vee: SM_{m\times n} \times SM_{m\times n} \to SM_{m\times n^2}$, $[a_{ij}] \vee [b_{ik}] = [c_{ip}]$ burada $c_{ip} = max\{a_{ij}, b_{ik}\}, p = n(j-1)+k$ şeklinde tanımlanır [33].

Tanım 1.3.3. $[a_{ij}], [b_{ij}] \in SM_{m\times n}$ olsun. Bu durumda $[a_{ij}]$ ve $[b_{ik}]$' nin Ve-Tümleyen-çarpımı $\overline{\wedge}: SM_{m\times n} \times SM_{m\times n} \to SM_{m\times n^2}$, $[a_{ij}] \overline{\wedge} [b_{ik}] = [c_{ip}]$ burada $c_{ip} = min\{a_{ij}, 1-b_{ik}\}$, $p = n(j-1)+k$ şeklinde tanımlanır [33].

Tanım 1.3.4. $[a_{ij}], [b_{ij}] \in SM_{m\times n}$ olsun. Bu durumda $[a_{ij}]$ ve $[b_{ik}]$' nin Veya-Tümleyen- çarpımı $\overline{\vee}: SM_{m\times n} \times SM_{m\times n} \to SM_{m\times n^2}$, $[a_{ij}] \overline{\vee} [b_{ik}] = [c_{ip}]$ burada $c_{ip} = max\{a_{ij}, 1-b_{ik}\}$, $p = n(j-1)+k$ şeklinde tanımlanır [33].

Örnek 1.3.5. $[a_{ij}], [b_{ik}] \in SM_{m\times n}$

$$[a_{ij}] = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}, [b_{ik}] = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

olsun. Bu durumda

$$[a_{ij}] \wedge [b_{ik}] = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

şeklinde olur. Benzer şekilde $[a_{ij}] \vee [b_{ik}], [a_{ij}] \overline{\wedge} [b_{ik}]$ ve $[a_{ij}] \overline{\vee} [b_{ik}]$ kolaylıkla bulunabilir.

Önerme 1.3.6. $[a_{ij}], [b_{ik}] \in SM_{m\times n}$ olsun. Bu durumda aşağıdaki ifadeler doğrudur.

i. $\left([a_{ij}] \vee [b_{ik}]\right)^c = [a_{ij}]^c \wedge [b_{ik}]^c$,

ii. $\left([a_{ij}] \wedge [b_{ik}]\right)^c = [a_{ij}]^c \vee [b_{ik}]^c$,

iii. $\left([a_{ij}] \bar{\vee} [b_{ik}]\right)^c = [a_{ij}]^c \bar{\wedge} [b_{ik}]^c$,

iv. $\left([a_{ij}] \bar{\wedge} [b_{ik}]\right)^c = [a_{ij}]^c \bar{\vee} [b_{ik}]^c$ [33].

1.4. Kriptosistem İle İlgili Tanımlar

Tanım 1.4.1. Açık anahtar, açık anahtarlı kriptografide herkes tarafından erişilebilen anahtardır. Sadece eşi olan özel anahtara sahip kişi tarafından açılması istenen verileri şifrelemek için kullanılır. Bir açık anahtar sisteminde sadece mesajın şifrelenmesinde kullanılır [41].

Tanım 1.4.2. Açık anahtarlı algoritmalar, **ş**ifrelemenin ve deşifrelemenin farklı anahtarlar yardımıyla yapıldığı kriptografik algoritmalardır. Deşifreleme anahtarının şifreleme anahtarından elde edilemediği algoritmalardır. Açık anahtar ve onun eşi olan özel anahtar ile bir anahtar çifti oluşturur. Çift anahtarlı kriptografi veya asimetrik algoritmalar da denir [41].

Tanım 1.4.3. Açık metin, metinlerin şifrelenmemiş, normal, okunabilir halleridir. Düz metin de denir [41].

Tanım 1.4.4. Alıcı, haberleşmede bilgiyi alan kişidir [41].

Tanım 1.4.5. Anahtar, **v**erileri şifrelemek veya deşifrelemek için kullanılan algoritmanın bilinmeyen kısmını oluşturan parçadır (sayı, kelime veya herhangi bir sayısal veri parçası) [41].

Tanım 1.4.6. Anahtar üretimi**,** kriptografide her kullanıcının açık/gizli anahtarın, kullanılan kriptografik yönteme bağlı matematiksel işlemlerle hazırlanmasıdır [41].

Tanım 1.4.7. Bilgi bütünlüğü**,** bilginin saklanması veya açık/kapalı iletişim ağlarından iletimi sırasında içerik açısından herhangi bir değişime uğratılmamış olması, özgün halinde korunmasıdır [41].

Tanım 1.4.8. Bilgi güvenliği, bilginin kime ait olduğu belirlenmiş, bütünlüğü korunmuş ve gizliliği sağlanmış olarak iletimi ve saklanmasıdır [41].

Tanım 1.4.9. Gizlilik, iletişim kuran iki taraf arasındaki yazışmaların üçüncü kişilerden gizli tutulması veya bir kişiye ait bilgilerin kendisi dışındaki herkesten gizli tutulmasıdır[41].

Tanım 1.4.10. Gönderici, bir haberleşmede bilgiyi meşru olarak gönderen kişidir [41].

Tanım 1.4.11. Kanal, bilginin bir kullanıcıdan diğerine iletimi için gereken fiziksel iletişim ortamıdır. Örneğin bilgisayar bağlantısı, telefon kablosu, radyolink ve uydu üzerinden diğer kullanıcıya ulaşan bağlantının tümüdür [41].

Tanım 1.4.12. Kimlik belirleme, herhangi bir servisi almak isteyen birinin, gerçekten de kendi iddia ettiği kişi olduğunun belirlenmesidir [41].

Tanım 1.4.13. Kod, bilginin kısaltılarak kayıt edildiği ya da tanımlandığı karakter dizisidir. Bilgisayarın tanıyacağı formda özel semboller kullanılarak bilginin gösterilmesi ya da tanımlanmasıdır [41].

Tanım 1.4.14. Kriptanaliz, bir kriptografik sistemin girdi veya çıktılarını inceleyerek, bilgi ve anahtar olmaksızın orijinal verilere ulaşmayı amaçlayan analizdir [41].

Tanım 1.4.15. Kriptanalist, kriptanalizin uygulamacılarına denir [41].

Tanım 1.4.16. Kriptografi, kodunu yalnız alıcısının açabileceği şekilde düzenlenen, mesajların içeriğini gizleme ve mesajı tekrar eski orijinal haline geri dönüştürme prensipleri ve yöntemlerini içeren gizli dönüşümler bilimidir [41].

Tanım 1.4.17. Kriptografik algoritma, şifreleme ve deşifreleme işlemlerinde kullanılan matematiksel işlemlerin bütünüdür [41].

Tanım 1.4.18. Kriptoloji, çözülebilmesi çok zor matematik problemlerini inceleyen kriptografi ile bu problemleri çözmeyi hedefleyen ve saldırıları belirleyen kriptanalizi içeren bilim dalıdır (kriptoloji = kriptografi + kriptanaliz) [41].

Tanım 1.4.19. Gizli anahtar, hem şifreleme hem de deşifreleme işlemlerinde kullanılan anahtardır [41].

Tanım 1.4.20. Saldırgan, taraflar arasındaki haberleşmede mesajı alan veya gönderen kişi olmayıp güvenliği kırmaya çalışan zararlı kimsedir [41].

Tanım 1.4.21. Saldırı, bir kriptosistemin bir kısmını veya tamamını kırmak için yapılan başarılı veya başarısız teşebbüstür [41].

Tanım 1.4.22. Sayısal imza, elektronik ortamdaki yazışmalara eklenen, yazıyı gönderenin kimliğini ve gönderilen yazının iletimi sırasında bozulmadığını kanıtlamaya yarayan bölümdür. Sayısal imza, yazının içeriğine ve imzalayanın gizli anahtarına bağlı bir kriptografik yöntemle atıldığı için, sayısal imzanın doğrulanmasında, imzayı atanın açık anahtarı kullanılır [41].

Tanım 1.4.23. Simetrik algoritmalar, şifreleme ve deşifreleme işlemlerinde aynı anahtarın kullanıldığı algoritmalardır. Tek anahtarlı kriptografi veya gizli anahtarlı algoritmalar da denir [41].

Tanım 1.4.24. Şifre çözme, şifrelenmiş veriyi çözüp eski haline getirme işlemidir [41].

Tanım 1.4.25. Şifre kırma, **e**lektronik ortamda kullanılan şifreleri öğrenmek amacıyla yapılan işlemdir. Genellikle art niyetli kişilerce, çıkar amaçlı uygulandığı için yasadışı olarak kabul edilmektedir [41].

Tanım 1.4.26. Şifreleme, açık metni anlaşılmaz hale getirme, şifreli metne dönüştürme sürecidir. Amaç; veriyi, gerekli anahtar olmadan çözülebilmesi imkânsıza mümkün olduğunca yakın şekilde kodlamaktır [41].

Tanım 1.4.27. Şifreli metin**,** metinlerin şifrelenerek anlaşılamaz hale getirilmiş biçimleridir [41].

Tanım 1.4.28. Kriptosistem, bir mesajın yetkili kişi(ler) dışında okunmasını engelleyecek matematiksel dönüşümlerdir [41].

Diğer taraftan, kriptosistem için alfabenin harfleri aşağıdaki gibi numaralarla eşleştirilir:

Tablo 1.2. Alfabenin sayısal değerleri

$HARFLER$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
$NUMARALAR$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17

S	T	U	V	W	X	Y	Z	Ç	Ğ	İ	Ö	Ş	Ü
18	19	20	21	22	23	24	25	26	27	28	29	30	31

Böylece A, 0’ dan başlamış olup, Ü’ nün de harf numarası 31 oldu. Eğer harfler ikili sistemle eşleştirilmesi aşağıdaki gibidir:

Tablo 1.3. Alfabenin ikili sistemde sayısal değerleri

$HARFLER$	A	B	C	D	E	⋯	Ş	Ü
İ$KİLİ$ $SİSTEM$	00000	00001	00010	00011	00100	⋯	11110	11111

İkili sistemden dolayı ve 32 bit olmasını istediğimizden dolayı Ç, Ğ, İ, Ö, Ş, Ü gibi beş harf daha ekledik. Bu alfabeye farklı karakterler eklenerek 64 bite de çıkarılabilir.

2. BÖLÜM

ESNEK MATRİS ÇARPIMLARI

Bu bölümde, esnek matrislerin invers çarpımını, karakteristik çarpımını tanımlayacağız ve özelliklerini vereceğiz.

2.1. Esnek Matrislerin İnvers Çarpımları

Tanım 2.1.1. $[a_{ij}], [b_{ij}] \in SM_{m\times n}$ olsun. Bu durumda $[a_{ij}]$ ve $[b_{ij}]$' nin "$\cdot_i$" invers çarpımı $[a_{ij}] \cdot_i [b_{ij}] = [c_{ij}]$, burada her i, j için $c_{ij} = \begin{cases} 1, & a_{ij} \neq b_{ij} \; ise \\ 0, & a_{ij} = b_{ij} \; ise \end{cases}$ şeklinde tanımlanır [35].

Örnek 2.1.2. $U = \{u_1, u_2, u_3, u_4\}$ bir evrensel küme ve $E = \{e_1, e_2, e_3\}$ parametrelerin kümesi, $A = \{e_1, e_2\}$ ve $B = \{e_2, e_3\}$ olsun. $(f_A, E) = \{(e_1, \{u_1, u_3\}), (e_2, \{u_2, u_3, u_4\})\}$, $(f_B, E) = \{(e_2, \{u_1, u_2, u_3\}), (e_3, \{u_2, u_4\})\}$ esnek kümeler ve

$$[a_{ij}] = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}, [b_{ij}] = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

bu esnek kümelere karşılık gelen esnek matrisler olsun.

Bu esnek matrislerin invers çarpımları,

$$[a_{ij}] \cdot_i [b_{ij}] = [c_{ij}] = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix} \in SM_{4\times 3}$$

şeklindedir. $[a_{ij}]$ ve $[b_{ij}]$ matrislerinin elemanlarında tüm durumlar dikkate alınarak, elemanlarda " $\cdot_i$ " çarpımı yaparak aşağıdaki ispatları vereceğiz.

Önerme 2.1.3. " $\cdot_i$ " çarpımı $SM_{m\times n}$' de bir birleşmeli işlemdir [35].

İspat. $[a_{ij}],[b_{ij}],[c_{ij}] \in SM_{m\times n}$ olsun. $[a_{ij}] \cdot_i ([b_{ij}] \cdot_i [c_{ij}]) = ([a_{ij}] \cdot_i [b_{ij}]) \cdot_i [c_{ij}]$ olmak üzere sekiz ihtimal olup bunlar aşağıdaki şekilde gösterilmiştir.

$$0 \cdot_i (0 \cdot_i 0) = (0 \cdot_i 0) \cdot_i 0 = 0,$$
$$0 \cdot_i (0 \cdot_i 1) = (0 \cdot_i 0) \cdot_i 1 = 1,$$
$$0 \cdot_i (1 \cdot_i 0) = (0 \cdot_i 1) \cdot_i 0 = 1,$$
$$0 \cdot_i (1 \cdot_i 1) = (0 \cdot_i 1) \cdot_i 1 = 0,$$
$$1 \cdot_i (0 \cdot_i 0) = (1 \cdot_i 0) \cdot_i 0 = 1,$$
$$1 \cdot_i (1 \cdot_i 0) = (1 \cdot_i 1) \cdot_i 0 = 0,$$
$$1 \cdot_i (0 \cdot_i 1) = (1 \cdot_i 0) \cdot_i 1 = 0,$$
$$1 \cdot_i (1 \cdot_i 1) = (1 \cdot_i 1) \cdot_i 1 = 1$$

olup ispat tamamlanır.

Önerme 2.1.4. $[a_{ij}],[b_{ij}] \in SM_{m\times n}$ olsun. Bu durumda,

- **i.** $[a_{ij}] \cdot_i [0] = [0] \cdot_i [a_{ij}] = [a_{ij}]$,
- **ii.** $[a_{ij}] \cdot_i [a_{ij}] = [0]$,
- **iii.** $[a_{ij}] \cdot_i [a_{ij}]^c = [1]$,
- **iv.** $[a_{ij}] \cdot_i [a_{ij}] \cdot_i [a_{ij}] = [a_{ij}]$,
- **v.** $[a_{ij}] \cdot_i [b_{ij}] = [b_{ij}] \cdot_i [a_{ij}]$,
- **vi.** $[a_{ij}]^c \cdot_i [b_{ij}]^c = [a_{ij}] \cdot_i [b_{ij}]$

şeklindedir [35].

İspat. i. İlk önce eşitliğin sol tarafını alalım. $[a_{ij}] \cdot_i [0] = [c_{ij}]$ olsun. Tanım 2.1.1. 'den her i,j için $c_{ij} = \begin{cases} 1, & a_{ij} \neq 0 \; ise \\ 0, & a_{ij} = 0 \; ise \end{cases}$ şeklindedir. Dolayısıyla her i,j için $[a_{ij}] = [0]$ ise $[c_{ij}] = [0], [a_{ij}] = [1]$ ise $[c_{ij}] = [1]$' dir. Bu da $[a_{ij}] = [c_{ij}]$ demektir, yani $[a_{ij}] \cdot_i [0] = [a_{ij}]$ şeklindedir.

Şimdi eşitliğin sağ tarafına bakalım. $[0] \cdot_i [a_{ij}] = [c_{ij}]$ olsun. Benzer şekilde her i, j için $[a_{ij}] = [0]$ ise $[c_{ij}] = [0], [a_{ij}] = [1]$ ise $[c_{ij}] = [1]$' dir. Bu da $[a_{ij}] = [c_{ij}]$ demektir, yani $[a_{ij}] \cdot_i [0] = [a_{ij}]$ şeklindedir. $[a_{ij}] \cdot_i [0] = [0] \cdot_i [a_{ij}] = [a_{ij}]$ olup ispat tamamlanmış olur.

Diğerleri de benzer şekilde ispatlanabilir.

Teorem 2.1.5. $SM_{m\times n}$ kümesi " $\cdot_i$ " işlemi ile bir değişmeli gruptur [35].

İspat. Önerme 2.1.3. ve Önerme 2.1.4.' den " $\cdot_i$ " işlemi altında $(SM_{m\times n}, \cdot_i)$ değişmeli, kapalı, birleşmeli, [0] matrisi etkisiz elemanı ve $[a_{ij}], [a_{ij}]$' nin ters elemanı olduğunu elde ederiz.

Teorem 2.1.6. $(SM_{m\times n}, \cdot_i, \widetilde{\cap})$ birimli bir değişmeli halkadır [35].

İspat: i. Teorem 2.1.5' ten, $(SM_{m\times n}, \cdot_i)$ bir değişmeli gruptur.

ii. Önerme 1.2.10' dan, $(SM_{m\times n}, \widetilde{\cap})$ bir yarıgruptur.

iii. $[a_{ij}], [b_{ij}], [c_{ij}] \in SM_{m\times n}$ olsun.

$([a_{ij}] \widetilde{\cap} [c_{ij}]) \cdot_i ([b_{ij}] \widetilde{\cap} [c_{ij}]) = ([a_{ij}] \cdot_i [b_{ij}]) \widetilde{\cap} [c_{ij}]$ olmak üzere sekiz ihtimal olup sağdan dağılma özelliği aşağıdaki gibidir:

$$(0 \widetilde{\cap} 0) \cdot_i (0 \widetilde{\cap} 0) = (0 \cdot_i 0) \widetilde{\cap} 0 = 0,$$
$$(0 \widetilde{\cap} 1) \cdot_i (0 \widetilde{\cap} 1) = (0 \cdot_i 0) \widetilde{\cap} 1 = 0,$$
$$(0 \widetilde{\cap} 1) \cdot_i (1 \widetilde{\cap} 1) = (0 \cdot_i 1) \widetilde{\cap} 1 = 1,$$
$$(1 \widetilde{\cap} 1) \cdot_i (1 \widetilde{\cap} 1) = (1 \cdot_i 1) \widetilde{\cap} 1 = 0,$$
$$(0 \widetilde{\cap} 0) \cdot_i (1 \widetilde{\cap} 0) = (0 \cdot_i 1) \widetilde{\cap} 0 = 0,$$
$$(1 \widetilde{\cap} 0) \cdot_i (1 \widetilde{\cap} 0) = (1 \cdot_i 1) \widetilde{\cap} 0 = 0,$$
$$(1 \widetilde{\cap} 1) \cdot_i (0 \widetilde{\cap} 1) = (1 \cdot_i 0) \widetilde{\cap} 1 = 1,$$
$$(1 \widetilde{\cap} 0) \cdot_i (0 \widetilde{\cap} 0) = (1 \cdot_i 0) \widetilde{\cap} 0 = 0.$$

Soldan dağılma özelliği de benzer şekildedir.

iv. Önerme 1.2.10' dan, $(SM_{m\times n},\widetilde{\cap})$ yarıgrubu değişmelidir ve birim elemana sahiptir. Dolayısıyla $(SM_{m\times n},\cdot_i,\widetilde{\cap})$ birimli bir değişmeli halkadır.

2.2. Esnek Matrislerin Karakteristik Çarpımı

Tanım 2.2.1. . $[a_{ij}],[b_{ij}] \in SM_{m\times n}$ olsun. Bu durumda $[a_{ij}]$ ve $[b_{ij}]$' nin "$\cdot_c$" karakteristik çarpımı $[a_{ij}] \cdot_c [b_{ij}] = [c_{ij}]$, burada her i,j için $c_{ij} = \begin{cases} 1, & a_{ij} = b_{ij}\ ise \\ 0, & a_{ij} \neq b_{ij}\ ise \end{cases}$ şeklinde tanımlanır [35].

şeklindedir.

Örnek 2.2.2. . $U = \{u_1,u_2,u_3,u_4\}$ bir evrensel küme ve $E = \{e_1,e_2,e_3\}$ parametrelerin kümesi, $A = \{e_2,e_3\}$ ve $B = \{e_1,e_3\}$ olsun. $(f_A,E) = \{(e_2,\{u_2,u_3\}),(e_3,\{u_1,u_4\})\}$, $(f_B,E) = \{(e_1,\{u_1,u_3\}),(e_3,\{u_2,u_4\})\}$ esnek kümeler ve

$$[a_{ij}] = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, [b_{ij}] = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

bu esnek kümelere karşılık gelen esnek matrisler olsun.

Bu esnek matrislerin karakteristik çarpımları,

$$[a_{ij}] \cdot_c [b_{ij}] = [c_{ij}] = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix} \in SM_{4\times 3}$$

şeklindedir.

Önerme 2.2.3. $[a_{ij}],[b_{ij}] \in SM_{m\times n}$ olsun. Bu durumda,

- **i.** " $\cdot_c$ " çarpımı $SM_{m\times n}$' de bir birleşmeli işlemdir.
- **ii.** $[a_{ij}] \cdot_c [1] = [a_{ij}]$,
- **iii.** $[a_{ij}] \cdot_c [0] = [a_{ij}]^c$,
- **iv.** $[a_{ij}] \cdot_c [a_{ij}] = [1]$,

v. $[a_{ij}] \cdot_c [a_{ij}]^c = [0]$,
vi. $[a_{ij}] \cdot_c [b_{ij}] = [b_{ij}] \cdot_c [a_{ij}]$,
vii. $[a_{ij}]^c \cdot_c [b_{ij}]^c = [a_{ij}] \cdot_c [b_{ij}]$

şeklindedir [35].

İspat. i. $[a_{ij}], [b_{ij}], [c_{ij}] \in SM_{m\times n}$ olsun. $[a_{ij}] \cdot_c ([b_{ij}] \cdot_c [c_{ij}]) = ([a_{ij}] \cdot_c [b_{ij}]) \cdot_c [c_{ij}]$ olmak üzere sekiz ihtimal olup bunlar aşağıdaki şekilde gösterilmiştir.

$$0 \cdot_c (0 \cdot_c 0) = (0 \cdot_c 0) \cdot_c 0 = 0,$$
$$0 \cdot_c (0 \cdot_c 1) = (0 \cdot_c 0) \cdot_c 1 = 1,$$
$$0 \cdot_c (1 \cdot_c 0) = (0 \cdot_c 1) \cdot_c 0 = 1,$$
$$0 \cdot_c (1 \cdot_c 1) = (0 \cdot_c 1) \cdot_c 1 = 0,$$
$$1 \cdot_c (0 \cdot_c 0) = (1 \cdot_c 0) \cdot_c 0 = 1,$$
$$1 \cdot_c (1 \cdot_c 0) = (1 \cdot_c 1) \cdot_c 0 = 0,$$
$$1 \cdot_c (0 \cdot_c 1) = (1 \cdot_c 0) \cdot_c 1 = 0,$$
$$1 \cdot_c (1 \cdot_c 1) = (1 \cdot_c 1) \cdot_c 1 = 1$$

olup " $\cdot_c$ " çarpımı $SM_{m\times n}$'de bir birleşmeli işlemdir.

ii. İlk olarak eşitliğin sol tarafına bakalım. $[a_{ij}] \cdot_c [1] = [c_{ij}]$ olsun. Tanım 2.2.1. 'den her i, j için $c_{ij} = \begin{cases} 1, & a_{ij} = 1 \; ise \\ 0, & a_{ij} \neq 1 \; ise \end{cases}$ şeklindedir. Dolayısıyla her i, j için $[a_{ij}] = [0]$ ise $[c_{ij}] = [0], [a_{ij}] = [1]$ ise $[c_{ij}] = [1]$' dir. Bu da $[a_{ij}] = [c_{ij}]$ demektir, yani $[a_{ij}] \cdot_c [1] = [a_{ij}]$ şeklindedir.

Şimdi eşitliğin sağ tarafına bakalım. $[1] \cdot_c [a_{ij}] = [c_{ij}]$ olsun. Benzer şekilde her i, j için $[a_{ij}] = [0]$ ise $[c_{ij}] = [0], [a_{ij}] = [1]$ ise $[c_{ij}] = [1]$' dir. Bu da $[a_{ij}] = [c_{ij}]$ demektir, yani $[a_{ij}] \cdot_c [1] = [a_{ij}]$ şeklindedir. $[a_{ij}] \cdot_c [1] = [1] \cdot_c [a_{ij}] = [a_{ij}]$ olup ispat tamamlanmış olur.

Diğerleri de benzer şekilde ispatlanabilir.

Önerme 2.2.4. $[a_{ij}], [b_{ij}] \in SM_{m\times n}$ olsun. Bu durumda, aşağıdaki *De Morgan's yasaları* geçerlidir [35].

i. $([a_{ij}] \cdot_i [b_{ij}])^c = [a_{ij}]^c \cdot_c [b_{ij}]^c$,

ii. $([a_{ij}] \cdot_c [b_{ij}])^c = [a_{ij}]^c \cdot_i [b_{ij}]^c$.

İspat. i. $[a_{ij}], [b_{ij}] \in SM_{m\times n}$ olsun. $([a_{ij}] \cdot_i [b_{ij}])^c = [a_{ij}]^c \cdot_c [b_{ij}]^c$ için dört ihtimal bulunup bunlar aşağıdaki gibidir:

$$(0 \cdot_i 0)^c = 0^c \cdot_c 0^c = 1,$$
$$(0 \cdot_i 1)^c = 0^c \cdot_c 1^c = 0,$$
$$(1 \cdot_i 0)^c = 1^c \cdot_c 0^c = 0,$$
$$(1 \cdot_i 1)^c = 1^c \cdot_c 1^c = 1$$

elde edilir. İspatın geri kalanı benzer şekildedir.

Önerme 2.2.4' te, invers çarpım ve karakteristik çarpım için De Morgan's yasalarını gösterdik. Şimdi Önerme 2.2.5'te invers çarpım ve karakteristik çarpım için $SM_{m\times n}$'de De Morgan's tipinin nasıl olduğunu göstereceğiz.

Önerme 2.2.5. $[a_{ij}] = A, [b_{ij}] = B \; ve \; [c_{ij}] = C \in SM_{m\times n}$ olsun. Bu durumda,

i. $(A \cdot_i B) \cdot_c C = A^c \cdot_c (B \cdot_i C^c)$,
ii. $(A \cdot_c B) \cdot_i C = A^c \cdot_i (B \cdot_c C^c)$,
iii. $A \cdot_i (B \cdot_c C) = (A^c \cdot_c B) \cdot_i C^c$,
iv. $A \cdot_c (B \cdot_i C) = (A^c \cdot_i B) \cdot_c C^c$

şeklindedir [35].

İspat. i. Önerme 2.1.4 ve Önerme 2.2.3' ten,

$$\begin{aligned}(A \cdot_i B) \cdot_c C &= (A^c \cdot_c B^c) \cdot_c C \\ &= A^c \cdot_c (B^c \cdot_c C) \\ &= A^c \cdot_c (B \cdot_i C^c)\end{aligned}$$

şeklindedir. Böylece, ispat tamamlanmış olur. İspatın geri kalanı benzer şekildedir.

Şimdi, Önerme 2.2.5.' in (i.) şıkkına bir örnek vereceğiz.

Örnek 2.2.6. $A, B, C \in SM_{4\times 5}$ ve

$A = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$ ve $C = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \end{pmatrix}$ olsun.

Böylece,

$$(A \cdot_i B) \cdot_c C = A^c \cdot_c (B \cdot_i C^c) = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$'dir.

3. BÖLÜM

ESNEK KRİPTOSİSTEM

Bu bölümde, esnek kümelere ve esnek matrislere dayanan yeni bir şifreleme algoritması vereceğiz. Esnek şifreleme ve esnek deşifrelemeyi tanımlayacağız. Bu bölüm boyunca, S ile esnek matrisi, M ile mesajı, C ile de şifreli metni göstereceğiz.

3.1. Esnek Şifreleme ve Deşifreleme

Teorem 3.1.1. . $S, M, C \in SM_{m\times n}$ olsun. Bu durumda,

i. $S \cdot_i M = C$,

ii. $S \cdot_c M = C$,

iii. $(S \cdot_i M) \cdot_c S = C$,

iv. $(S \cdot_c M) \cdot_i S = C^c$,

v. $S \cdot_i (M \cdot_c S) = C^c$,

vi. $S \cdot_c (M \cdot_i S) = C$

şeklindedir [35].

İspat. İnvers çarpım ve karakteristik çarpım tanımlarından kolayca elde edilir.

Ayşe, Ali' ye mesaj göndermek istiyor, fakat Ayşe' nin Ali' ye gönderdiği tüm bilgiler kötü niyetli Emel tarafından elde edilecek olması olasıdır. Gönderdiği mesajın sadece Ali' nin okuması için mesajı esnek şifreleme yöntemiyle şifreleyip yollayacaktır. Ali de esnek deşifreleme yaparak mesajı okuyacaktır.

Esnek şifreleme ve deşifreleme şeması aşağıdaki iki algoritma ile verilmiştir.

Teorem 3.1.1. (i.) ile esnek şifreleme algoritması:

1. Ayşe bir esnek küme alır.
2. Ayşe bu esnek kümenin, esnek matris karşılığını bulur.
3. Ayşe mesajı bloklara ayırır ve harfleri ikili sisteme çevirip, matrisin satırlarına sırasıyla her harfin ikili sistemdeki karşılığı yazılır.
4. Ayşe esnek matrisle mesajı $\cdot_i-$çarpımı yapar.
5. Ayşe matrisin her bir satırı ikili sisteme denk gelen harflere çevrilir ve Ali' ye yollar.

Teorem 3.1.1. (i.) ile esnek deşifreleme algoritması:

1. Ali esnek kümeyi ve esnek matrisi alır.
2. Ali şifreli metni bloklara ayırır ve harfleri ikili sisteme çevirip, matrisin satırlarına sırasıyla her harfin ikili sistemdeki karşılığı yazılır.
3. Ali esnek matrisle şifreli metni $\cdot_i-$çarpımı yapar.
4. Ali matrisin her bir satırı ikili sisteme denk gelen harflere çevrilir.
5. Ali mesajı elde eder.

Esnek kriptosistem şemasında, mesajı bloklara ayırmak zorunda değiliz. Ancak, mesajı bloklara ayırmak uzun mesajlar için daha da zor olabilir. Biz mesajı bloklar halinde ayıracağız.

Benzer şekilde, Teorem 3.1.1. (ii.)' ye karakteristik çarpım uygulanabilir.

Teorem 3.1.1. (iii.) ile esnek şifreleme algoritması:

1. Ayşe bir esnek küme alır ve esnek matris karşılığını bulur.
2. Ayşe mesajı bloklara ayırır ve harfleri ikili sisteme çevirip, matrisin satırlarına sırasıyla her harfin ikili sistemdeki karşılığı yazılır.
3. Ayşe esnek matrisle mesajı soldan $\cdot_i-$çarpımı yapar.
4. Ayşe soldan $\cdot_i-$çarpımı yapılan mesajı esnek matrisle sağdan $\cdot_c-$çarpımı yapar.

5. Ayşe matrisin her bir satırı ikili sisteme denk gelen harflere çevrilir ve Ali' ye yollar.

Teorem 3.1.1. (iii.) ile esnek deşifreleme algoritması:

1. Ali esnek kümeyi ve esnek matrisi alır.
2. Ali şifreli metni bloklara ayırır ve harfleri ikili sisteme çevirip, matrisin satırlarına sırasıyla her harfin ikili sistemdeki karşılığı yazılır.
3. Ali esnek matrisle şifreli metni sırasıyla, sağdan $\cdot_c-$çarpımı ve soldan $\cdot_i-$çarpımı yapar.
4. Ali matrisin her bir satırı ikili sisteme denk gelen harflere çevrilir.
5. Ali mesajı elde eder.

Bu sistem esnek kümelere ve esnek matrislere bağlıdır. Dolayısıyla, yukarıda belirtilen sistem, hızlı şifreleme ve deşifreleme sağlar. Saldırıları önlemek için, esnek kümelerin seçiminde dikkatli olmalıyız. Evrensel kümenin ve esnek kümelerin elemanlarını dikkatlice seçersek, şifreleme güvenliği artar. Ayrıca burada satırlarda yaptığımız işlemleri benzer şekilde sütunlarda da yapabiliriz.

4. BÖLÜM

UYGULAMALAR

4.1. Esnek Kriptosistem Uygulamaları

Teorem 3.1.1. (i.) ile esnek şifreleme algoritması:

Ayşe, Ali' ye bir mesaj göndermek istiyor. Mesaj *"ESNEK ŞİFRELEME"* olsun.

1. Ayşe
$(f_A, E) = \{(e_1, \{u_1, u_2, u_3\}), (e_2, \{u_1, u_4, u_5\}), (e_3, \{u_2, u_3\}), (e_4, \{u_4, u_5\}), (e_5, \{u_1, u_2, u_4\})\}$
esnek kümesini alır.

2. Ayşe esnek matris karşılığını bulur ve $S = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix}$' dir.

3. Ayşe mesajı bloklara ayırır : *"ESNEK – ŞİFRE – LEMEA"*. *"ESNEK"* için sırasıyla $E \rightarrow 00100$, $S \rightarrow 10010$, $N \rightarrow 01101$, $E \rightarrow 00100$, $K \rightarrow 01010$ elde edilir. Harflerin her birinin ikili sistemdeki karşılığı sırasıyla matrisin satırlarına yazılır. Diğerleri de benzer şekilde yapılır. Mesajın esnek matrisleri sırasıyla

$$M = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

elde edilir.

4. Ayşe esnek matrisle mesajı sırasıyla $\cdot_i-$çarpımı yapar.

$$\mathrm{M} \cdot_i S = C = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

5. Ayşe matrisin her bir satırı ikili sisteme denk gelen harflere çevrilir. İlk matrisin her bir satırı için 11101→ Ö, $00111 \rightarrow H$, $11001 \rightarrow Z$, 01111→ P, 00000→ A elde edilir. Diğer matrisler için de benzeri yapılır. Şifreli metin *"ÖHZPA – HJRÇO – SRYPK"* şeklindedir ve şifreli metni Ali' ye yollar.

Teorem 3.1.1. (i.) ile esnek deşifreleme algoritması:

1. Ali esnek kümeyi ve esnek matrisi alır. Esnek küme

$(f_A, E) = \{(e_1, \{u_1, u_2, u_3\}), (e_2, \{u_1, u_4, u_5\}), (e_3, \{u_2, u_3\}), (e_4, \{u_4, u_5\}), (e_5, \{u_1, u_2, u_4\})\}$

ve esnek matris $S = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix}$ şeklindedir.

2. Ali şifreli metni bloklara ayırır. *"ÖHZPA – HJRÇO – SRYPK"* ve *"ÖHZPA"* için sırasıyla *Ö*→11101, *H*→ 00111, *Z*→ 11001, *P*→01111, *A* →00000 elde edilir. Harflerin her birinin ikili sistemdeki karşılığı sırasıyla matrisin satırlarına yazılır. Diğerleri de benzer şekilde yapılır. Şifreli metnin esnek matris karşılığı sırasıyla aşağıdaki şekildeki gibidir:

$$C = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

3. Ali esnek matrisle şifreli metni $\cdot_i-$çarpımı yapar.

$$C \cdot_i S = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

4. Ali matrisin her bir satırı ikili sisteme denk gelen harflere çevrilir. İlk matrisin her bir satırı için sırasıyla 00100→ E, 10010→ S, 01101→ N, 00100→ E, 01010→ K elde edilir. Diğer matrisler için de benzer işlem yapıldığında *"ESNEK – ŞİFRE – LEMEA"* elde edilir.
5. Ali mesajı elde eder. *"ESNEK ŞİFRELEME"*.

Teorem 3.1.1. (iii.) ile esnek şifreleme algoritması:

Ayşe, Ali' ye yukarıdaki mesajı göndermek istiyor.

1. Ayşe yukarıdaki esnek kümeyi alır ve esnek matris karşılığını bulur.
2. Ayşe mesajı bloklara ayırır : *"ESNEK – ŞİFRE – LEMEA"*. *"ESNEK"* için sırasıyla E→00100, S→10010, N→01101, E→00100, K→01010 elde edilir. Harflerin her birinin ikili sistemdeki karşılığı sırasıyla matrisin satırlarına yazılır. Diğerleri de benzer şekilde yapılır. Mesajın esnek matrisleri sırasıyla

$$M = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$ ' dir.

3. Ayşe esnek matrisle mesajı soldan $\cdot_i-$çarpımı yapar.

$$S \cdot_i M = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

4. Ayşe soldan $\cdot_i-$çarpımı yapılan mesajı esnek matrisle sağdan $\cdot_c-$çarpımı yapar.

$$(S \cdot_i M) \cdot_c S = C = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

5. Ayşe matrisin her bir satırı ikili sisteme denk gelen harflere çevrilir. İlk matrisin her bir satırı için 11011→ Ğ, 01101 → N, 10010 → S, 11011→ Ğ, 10101→ V elde edilir. Diğer matrisler için de benzeri yapılır. Şifreli metin *"ĞNSĞV –BDÇQĞ–UĞTĞÜ"* şeklindedir ve şifreli metni Ali' ye yollar.

Teorem 3.1.1. (iii.) ile esnek deşifreleme algoritması:

1. Ali yukarıdaki gibi bir esnek küme alır ve karşılık gelen esnek matrisini bulur.

2. Ali şifreli metni bloklara ayırır. *"ĞNSĞV –BDÇQĞ–UĞTĞÜ"* ve *"ĞNSĞV"* için sırasıyla $\check{G}$→ 11011, N→ 01101, S→ 10010, $\check{G}$→11011, V → 10101 elde edilir. Harflerin her birinin ikili sistemdeki karşılığı sırasıyla matrisin satırlarına yazılır. Diğerleri de benzer şekilde yapılır. Şifreli metnin esnek matris karşılığı sırasıyla aşağıdaki şekildeki gibidir:

$$C = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

3. Ali esnek matrisle şifreli metni sırasıyla, sağdan $\cdot_c-$çarpımı ve soldan $\cdot_i-$çarpımı yapar.

$$\mathrm{C} \cdot_c \mathrm{S} = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix},$$

$$S \cdot_i (C \cdot_c S) = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

4. Ali matrisin her bir satırı ikili sisteme denk gelen harflere çevrilir. İlk matrisin her bir satırı için sırasıyla $00100\rightarrow E$, $10010\rightarrow S$, $01101\rightarrow N$, $00100\rightarrow E$, $01010\rightarrow K$ elde edilir. Diğer matrisler için de benzer işlem yapıldığında *"ESNEK – ŞİFRE – LEMEA"* elde edilir.
5. Ali mesajı elde eder. *"ESNEK ŞİFRELEME"*.

Benzer şekilde, bu yeni kriptosistemin uygulaması Teorem 3.1.1. (ii.), (iv.), (v.) ve (vi)' ya da uygulanabilir.

32 bitte çalıştığımızdan dolayı sütun sayısı beşten fazla olamaz. Ancak 64 bite çıkarılırsa bir sütun daha eklenebilir.

4.2 Sonuç

Bu tez çalışmasında ilk olarak Molodstov' un esnek kümesini ve ilgili özelliklerini, Çağman ve Enginoğlu' nun esnek matrislerini, esnek matrislerle alakalı tanımlarını ve esnek matrislerin çarpımını inceledik. Kriptosistem ile ilgili bazı temel tanımları verdik. Şifreleme ve deşifreleme işlemlerinde kullanılan harflerin sayısal ve ikili sistemdeki karşılıklarını gösterdik.

Esnek matrislerde invers çarpım ve karakteristik çarpım olmak üzere iki özel çarpım tanımladık ve bu çarpımlar ile ilgili bazı tanımlar ve önermeler verdik. Daha sonra esnek kümelere ve esnek matrislere dayanan esnek çarpımları kullanılarak yeni bir şifreleme algoritması tanımladık. Şifrelemede önemli olan şifrelemenin ve deşifrelemenin hızlı bir şekilde yapılması ve aynı zamanda kırılmasının çok zor olması veya çok fazla zaman almasıdır. Esnek kriptosistemde mesajın üçüncü şahıslar tarafından ele geçirilmemesi için anahtarı ve uygulanan kriptografiyi sadece şifreleyen ve deşifreleme yapan kişiler tarafından bilinmesi gerektiğini gösterdik. Son olarak da kriptosistemin başarılı olduğuna dair örnekler verdik. Bu tez tamamen orijinal çalışmadan oluşmaktadır. Makale olarak düzenlenip dergiye gönderilmiştir.

KAYNAKLAR

1. Zadeh, L. A., 1965. Fuzzy sets. **Information and Control, 8** (1), 338–353.
2. Molodtsov, D., 1999. Soft set theory- first results. **Computers and Mathematics with Applications, 37**(1), 19-31.
3. Maji, P.K., Roy, A.R., Biswas, R., 2002. An application of soft sets in a decision making problem. **Computers and Mathematics with Applications, 44**(1), 1077-1083.
4. Maji, P. K., Bismas, R., Roy, A.R., 2003. Soft set theory. **Computers and Mathematics with Applications, 45**(1), 555-562.
5. Pawlak, Z., 1982. Rough sets. **International Journal of Information and Computer Sciences, 11**(1), 341-356.
6. Xiao, Z., Li, Y., Zhong, B. and Yang, X., 2003. Research on synthetically evaluating method for business competitive capacity based on soft set. **Statistical Research,** 52-54.
7. Yang, H., Qu, C., Li, N-C., 2004. The induction and decision analysis of clinical diagnosis based on rough sets and soft sets. **(Fangzhi Gaoxiao Jichukexue Xuebao Ed.), 17**(3), 208-212.
8. Chen, D-G., Tsang, E.C.C., Yeung, D.S., 2003. Some notes on the parameterization reduction of soft sets. **International Conference on Machine Learning and Cybernetics, 3**, 1442-1445.
9. Chen, D., Tsang, E.C.C., Yeung, D.S., Wang, X., 2005. Theparameterization reduction of soft sets and its applications. **Computers and Mathematics with Applications, 49**(1), 757-763.
10. Kong, Z., Gao, L., Wang, L. and Li, S., 2008. The normal parameter reduction of soft sets and its algoritm. **Computers and Mathematics with Applications, 56**(1), 3029-3037.
11. Xiao, Z., Chen, L., Zhong, B., Ye, S., 2005. Recognition for soft information based on the theory of soft sets. **In Proceedings of ICSSSM-05 (Ed: J. Chen), IEEE, 2**, 1104-1106.

12. Pei, D., Miao, D., 2005. From soft sets to information systems. **In: Proceedings of Granular Computing (Eds: X. Hu, Q. Liu, A. Skowron, T.Y. Lin, R.R. Yager, B.Zhang) IEEE, 2**, 617-621.
13. Mushrif, M.M., Sengupta, S., Ray, A.K., 2006. Texture classifcation using a novel, Soft-set theory based classifcation algorithm. **Lecture Notes In Computer Science, 3851,** 246-254.
14. Aktaş, H. and Çağman, N., 2007. Soft sets and soft groups. **Information Sciences, 177**(1), 2726-2735.
15. Jun, Y.B., 2008. Soft BCK/BCI-algebras **Computers and Mathematics with Applications, 56** (1), 1408-1413.
16. Jun, Y. B. and Park, C. H., 2008. Applications of soft sets in ideal theory of BCK/BCI-algebras. **Information Science, 178** (1)**,** 2466-2475.
17. Park, C.H., Jun, Y.B., Öztürk, M.A., 2008. Soft WS-algebras. **Commun. Korean Math. Soc, 23** (3), 313-324.
18. Feng, F., Jun, Y. B., Zhao, X., 2008. Soft semirings. **Computers and Mathematics with Applications, 56** (10), 2621-2628.
19. Sun, Q-M., Zhang, Z-L., Liu, J., 2008. Soft sets and soft modules, (In Guoyin Wang, Tian-rui Li, Jerzy W. Grzymala-Busse, Duoqian Miao, Andrzej Skowron, Yiyu Yao Eds): **Rough Sets and Knowledge Technology, RSKT, Proceedings, Springer,** 403-409.
20. Zou, Y., Xiao, Z., 2008. Data analysis approaches of soft sets under incomplete information. **Knowledge-Based Systems, 21** (1), 941-945.
21. Çağman, N., Enginoğlu, S., 2010. Soft matrix theory and its decision making. **Computers and Mathematics with Applications, 59,** 3308–3314.
22. Sezgin, A., Atagün, A.O., 2011. On operations of soft sets. **Computers and Mathematics with Applications, 61**, 1457–1467.
23. Sezgin, A., Atagün, A.O., Aygün, E., 2011. A note on soft near-rings and idealistic soft near-rings. **Filomat Vol. 25** (1), 53–68.
24. Maji, P.K., Biswas, R.andRoy, A.R., 2001. Fuzzy soft sets. **Journal of Fuzzy Mathematics, 9**(3), 589-602.
25. Roy, A.R., Maji, P.K., 2007. A fuzzy soft set theoretic approach to decision making problems. **Journal of Computational and Applied Mathematics, 203**(1), 412-418.

26. Yang, X., Yu, D.,Yang, J. and Wu, C., 2007. 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.

27. Majumdar, P., Samanta, S. K., 2008. Similarity measure of soft sets. **New Mathematics and Natural Computation, 4**(1), 1-12.

28. Kong,Z., Gao, L., Wang, L., 2009. Comment on "A fuzzy soft set theoretic approach to decision making problems". **Journal of Computational and Applied Mathematics, Volume 223**, 540–542.

29. Xiao, Z., Gong, K., Zou, Y., 2009. A combined forecasting approach based on fuzzy soft sets. **Computers and Mathematics with Applications, 228,** 326-333.

30. Molodtsov, D. A., Leonov V. Yu. and Kovkov D. V., 2006. Soft sets technique and its application. **Nechetkie Sistemy i Myagkie Vychisleniya, 1**(1), 8-39.

31. Kovkov, D. V., Kolbanov, V. M., Molodtsov, D. A., 2007. Soft sets theory-based optimization. **Journal of Computer and Systems Sciences International, 46** (6), 872-880.

32. Ali, M.I., Feng, F., Liu, X., Min, W.K., Shabir, M., 2009. On some new operations in soft set theory. **Computers and Mathematics with Applications, 57** (9), 1547–1553.

33. Çağman, N., Enginoğlu, S., 2010, Soft matrix theory and its decision making, **Computers and Mathematics with Applications, 59,** 3308–3314.

34. Altındiş, H., 1999. Sayılar Teorisi ve Uygulamaları, Erciyes Üniversitesi yayınları, Kayseri, 308s.

35. Aygün, E., Atagün, A.O., Kılıç, B., 2014. Soft matrix product and soft cyrptosystem. (İncelemede).

36. Elgamal, T. A., 1985. Public key cryptosystem and a signature scheme based on discrete logarithms , **Information Theory, IEEE Transactions on, vol.31**, 469-472.

37. Çimen, C. Akleylek, S. Akyıldız, E., 2007. Şifrelerin Matematiği: Kriptografi, ODTÜ Geliştirme Vakfı Yayıncılık, Ankara, 131s.

38. Babaoğlu, A. 2009. Kriptolojinin geçmişi: bir şifreleme algoritması kullanmadan önce son kullanım tarihine bakın!. **Bilim ve Teknik, 638**, 24.

39. Kara, O., 2009. Kriptografinin yapıtaşları kriptografik algoritmalar ve protokoller. **Bilim ve Teknik, 500**, 34.

40. Koblitz, N. A., 1948. Course in Number Teory and Cryptografy, -Second Addition Library of Congress Cataloging-in-Publication Data,,USA, 235pp.

41. Stinson, D., 2006. Cryptography: Theory and Practice-Third Edition, Chapman & Hall/CRC Taylor & Francis Group, USA, 611pp.

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı, Soyadı: Büşra KILIÇ

Uyruğu: Türkiye (TC)

Doğum Tarihi ve Yeri: 17 Mayıs 1990, Ankara

Medeni Durumu: Bekâr

email: busra.kilic17@gmail.com

EĞİTİM

Derece	**Kurum**	**Mezuniyet Tarihi**
Yüksek Lisans	EÜ Fen Bilimleri Enstitüsü	2015
Lisans	EÜ Fen Fakültesi Matematik	2012
Lise	Cumhuriyet Anadolu Lisesi, Ankara	2008