Erciyes Üniversitesi
Fen Bilimleri Enstitüsü Dergisi
Cilt 35, Sayı 1, 2019

Erciyes University
Journal of Institue Of Science and Technology
Volume 35, Issue 1, 2019

AES Şifreleme ve Esnek Kümeler Yardımıyla Elde Edilen Yeni Bir Kriptosistem

Emin AYGÜN

Erciyes Üniversitesi Fen Bilimleri Fakültesi Matematik Bölümü / KAYSERİ

(Alınış / Received: 13.01.2019, Kabul / Accepted: 28.01.2019, Online Yayınlanma / Published Online: 30.04.2019)

Anahtar Kelimeler
Esnek kümeler,
İnvers ve Karakteristik çarpım,
Esnek şifreleme ve deşifreleme,
AES şifreleme

Özet: Molodtsov tarafından ortaya atılan esnek küme teorisi, belirsizlikle başa çıkmak için etkili bir matematiksel araç olarak görülmektedir. Bu teori, bilgi sistemleri, karar verme problemleri, optimizasyon teorisi, cebirsel yapılar ve matematiksel analiz gibi belirsizlik içeren birçok alana uygulandı. Bu çalışmada esnek matrisler üzerinde invers çarpım ve karakteristik çarpım olarak adlandırılan iki yeni işlem tanımlayacağız. Yeni kriptosistem metodunu esnek matrislerin invers çarpımı ve karakteristik çarpımını kullanarak ortaya koyacağız. Esnek şifrelemeyi ,esnek deşifrelemeyi tanımlayacağız ve AES şifreleme ile mukayese edeceğiz.

AES Encryption and A New Cryptosystem Obteined With Soft Set

Keywords
Soft Sets,
İnverse production and characteristic production,
Soft encryption and soft decryption,
AES encrption

Abstract: Soft set theory, proposed by Molodtsov, has been regarded as an effective mathematical tool to deal with uncertainties. This theory has been applied to many fields such as information systems, decision making problems, optimization theory, algebraic structure and basic mathematics analysis, etc. which contain uncertainties.In this work, we define two new operations on the set of soft matrices,called inverse production and characteristic production .We introduce soft cryptosystem as a new cryptosystem method by using inverse production and characteristic production of soft matrices.We define soft encyption, soft dencryption and we will compare with AES encyption.

1. Giriş

Esnek kümeler teorisi, Molodtsov [1] tarafından belirsizlikle başa çıkmak için bir matematiksel araç olarak ortaya atıldı. Molodtsov [1], sürekli diferansiyellenebilir fonksiyonlar, oyun teorisi, işlem araştırmaları, Riemann integrasyonu, Perron integrasyonu, olasılık, ölçüm teorisi vb. alanlarda esnek küme teorisini kullanarak, başarılı çalışmalar yaptı. Ayrıca, yazar yaklaşık nesne kavramını formüle etti ve esnek küme teorisi isimli bir kitap yayımladı. Maji ve arkadaşları [2] karar verme problemleri için esnek küme teorisini araştırdılar. Teorik olarak, esnek kümeler üzerine çeşitli işlemler tanımladılar. Ali ve arkadaşları [3] esnek kümelerin bazı kavramlarını verdiler. Maji ve ark. ve Pawlak' ın yaklaşımlı küme teorisi yardımıyla, bir karar verme probleminde esnek kümelerin bir uygulamasını sundu ve esnek kümelerde bazı işlemleri tanımladı. Xiao ve ark. esnek küme temelli iş rekabet kapasitesi için yapay bir hesaplama metodu üzerine bir çalışma yaptı. Yang ve ark. esnek kümelere ve yaklaşımlı kümelere dayalı klinik teşhisin karar analizi ve indüksiyon başlıklı bir çalışma yaptı. Xiao ve ark. ile Pei ve Miao esnek tabanlı bilgi sistemleri üzerine çalışmalar sundular. Mushrif ve ark. esnek küme temelli sınıflandırmalar üzerine bir çalışma yaptı. Esnek kümelerin cebirsel özellikleri bazı yazarlar tarafından çalışılmaktadır. Sezgin ve Atagün [4] esnek küme üzerinde kesişim, genişletilmiş kesişim, kısıtlanmış birleşim, kısıtlanmış farkı tanımladılar ve her birinin kendi arasındaki bağlantılarını gösterdiler. Aktaş ve Çağman [5] esnek kümeleri, bulanık kümeler ve yaklaşımlı kümelerin ilgili kavramlarıyla karşılaştırdılar, ayrıca pek çok yeni çalışmanın önünü açan "Esnek Grup Teorisi"ni literatüre kazandırdılar. Esnek grup yapısı üzerinde esnek altgrup,normal esnek altgrup, esnek homomorfizm gibi cebirsel yapılar tanımladılar. Acar ve diğerleri [6] esnek

halkaları, Atagün ve Sezgin [7] esnek yakın halkaları tanımladılar. Sezgin ve Atagün [8] halka, cisim ve modülün esnek cebirsel yapısıyla ilgili çalıştılar.Bu çalışmada, Molodtsov'un [1] esnek küme tanımı kullanılarak esnek matrisler üzerinde invers çarpım ve karakteristik çarpım tanımlanmıştır. Yeni esnek şifreleme ve esnek deşifreleme metodu verilmiştir. AES şifreleme hakkında bilgi verilmiştir.

2. Materyal ve Metot

Esnek kümeler yardımıyla elde edilecek olan şifreleme yöntemini oluşturmak için bu bölümde, temel bilgi niteliğinde olan ve çalışmanın diğer kısımlarında sıkça kullanılan yapılar verilecektir.

Tanım 2.1.

[1] U evrensel küme ve E parametrelerin bir kümesi olsun. P(U), U 'nun kuvvet kümesi ve $A \subset E$ olarak gösterilsin. Bir (F, A) sıralı ikilisi U üzerinde esnek küme olarak adlandırılır. Burada F, $F: A \rightarrow P(U)$ ile verilen bir dönüşümdür.

Tanım 2.2.

(f_A,E) ikilisi U üzerinde bir esnek küme olsun. Bu durumda UxE'nin R_A={ (u,e) : e ∈ A, u ∈ f_A (e) } alt kümesine (f_A,E) ikilisinin bağıntı formu denir. R_A'nın karakteristik fonksiyonu

$$X_{R_A}: UxE \rightarrow \{0,1\}$$

$$(u,e) \rightarrow X_{R_A}(u,e)=\begin{cases} 1, (u,e) \in X_{R_A} \\ 0, (u,e) \notin X_{R_A} \end{cases} \quad (1)$$

ile verilir. Eğer $a_{ij}=X_{R_A}(u_i, e_j)$ alınırsa,

$[a_{ij}]=\begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix}$ matrisine U üzerinde (f_A,E) esnek kümesinin esnek matrisi denir. U üzerindeki tüm esnek matrislerin kümesi SM_{mxn} ile gösterilir. [7]

Tanım 2.3.

$[a_{ij}] \in SM_{mxn}$ olsun.

i_1) Her i ve j için a_{ij}= 0 ise, $[a_{ij}]$ ya sıfır esnek matris denir ve [0] ile gösterilir.
i_2) Her $j \in I_A$= {j: $e_j \in A$} ve i için a_{ij}= 1 ise, $[a_{ij}]$ ya A-evrensel esnek matris denir ve $[\tilde{a}_{ij}]$ ile gösterilir.
i_3) Her i ve j için a_{ij} = 1 ise , $[a_{ij}]$ ya evrensel esnek matris denir ve [1] ile gösterilir.

Tanım 2.4.

$[a_{ij}]$, $[b_{ij}] \in SM_{mxn}$ olsun. $[a_{ij}]$ ve $[b_{ij}]$ nin invers çarpımı "$\cdot_i$" ile gösterilir. $[a_{ij}] \cdot_i [b_{ij}]= [c_{ij}]$ olmak üzere

$$c_{ij} = \begin{cases} 1, & a_{ij} \neq b_{ij} \\ 0, & a_{ij} = b_{ij} \end{cases} \quad (2)$$

şeklinde tanımlanır.

Tanım 2.5.

$[a_{ij}]$, $[b_{ij}]$ $\in SM_{mxn}$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

$$c_{ij}=\begin{cases}1, & a_{ij}=b_{ij}\\ 0, & a_{ij}\neq b_{ij}\end{cases} \tag{3}$$

şeklinde tanımlanır.

Tanım 2.6.

Herhangi bir $S \in SM_{5X5}$ esnek matrisi herhangi bir $\pi \in S_5$ permütasyon grubuna göre düzenlenirken esnek matrisin her bir satırındaki elemanlar π 'de verilen sıraya göre yer değiştitir.

Örnek 2.6.

$$S=\begin{bmatrix}1&1&0&1&1\\1&0&1&1&0\\0&1&1&1&1\\0&1&0&0&1\\0&0&0&1&1\end{bmatrix}$$ esnek matrisini alalım.

π =(12543) olsun. S esnek matrisinin her satırını π'e göre düzenleyelim. π de verilen sıralamayı dikkate alırsak $1 \to 2 \to 5 \to 4 \to 3 \to 1$ şeklindedir. O halde ilk satır düzenlenirken elemanlar bu sıralamaya göre yer değiştirecektir. İlk satırın düzenlenmiş hali 01111 olur. Her bir satıra bu işlem uygulanırsa

$$S_\pi=\begin{bmatrix}0&1&1&1&1\\1&1&1&0&0\\1&0&1&1&1\\0&0&0&1&1\\0&0&1&1&0\end{bmatrix}$$ elde edilir

Tanım 2.7.

Aes şifreleme algoritması, 128 bit veri bloklarını 128, 192 veya 256 bit anahtar seçenekleri ile şifreleyen bir blok şifre algoritmasıdır. 128 bit uzunluğunda olan veri, (4x4)' lük matrislerle bölünerek algoritmaya dahil olur. Bu matrise "durum" denilir ve her bir satırı kelime olarak adlandırılır. AES şifrelerken kullanacağı algoritmada anahtarın uzunluğuna göre döngü sayısının atamasını yapar. Bu döngüsel işlemin artmasıyla veri daha çok güvenilir hale gelir. Fakat aynı zamanda yapılacak olan döngüsel işlemlerin de artmasıyla hem işlem sayısı artar hem de bellek alanı artar. Özellikle 256 bit anahtar kullanımlarında döngüsel artım olduğu için algoritma hızı düşer.

Döngü Yapısı

Durum matrisinin oluşumuyla algoritma yürürlüğe girer. Döngü sayısı anahtar uzunluğuna göre değişir. Sadece son döngüde sütun karıştırma işlemi yapılmaz, tur anahtarı ile toplama işlemi yapılır ve şifrelenmiş blok elde edilir Şifrelenmiş veriyi çözerken de bu alt işlemlerin tersi uygulanır. Döngüler durum matrislerinde 4 işlem gerçekleştirir.

1. Bayt Değiştirme

Değişiklik değerleri önceden hesaplanmış S-Kutusuna göre yapılır. S-Kutusu, durum matrisinin elemanları onaltılık tabana göre oluştuğu için 16x16 boyutunda bir matristir denebilir.

2. Satır Kaydırma

Satır kaydırma işlemi yeni durum matrisi üzerinde yapılır. Bu işlemde matrisin ilk satırı aynı kalırken, ikinci satır 1 bayt, üçüncü satır 2 bayt, dördüncü satır ise 3 bayt sola ötelenir.

3. Sütun Karıştırma

Sütunları karıştırma işlemi, satır kaydırmadan elde edilen durum matrisinin her bir sütununu birbirinden bağımsız şekilde $a(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}$ denklemiyle matris çarpımına tabi tutar.

4. Döngü Anahtarını Ekleme

AES algoritmasında her döngünün sonunda anahtar materyali eklenir. Bu anahtar, başlangıçta anahtar üretim bloğu tarafından üretilen anahtar dizisidir.

Tanım 2.8.

Aes deşifreleme algoritması, şifeli metni çözmek için uygulanan algoritmadır. Şifreli metni çözmek için uygulanan adımlar şifreleme işlemi için kullanılan adımların benzeridir fakat tersi şeklinde uygulanır. Şifrelemek için uygulan dönüşümler tersine çevrilir ve şifreleme sırasının tersinden başlanır.

1. Ters Satır Kaydırma

Durum matrisi sola değil sağa doğru kaydırılır. İkinci satır bir bayt, üçüncü satır iki bayt, dördüncü satır üç bayt sağa doğru kaydırılır.

2. Ters Bayt Değiştirme

Şifre çözme işleminde de yine aynı şekilde bir S-kutusu kullanılır. Bu S-Kutusu aynı S-Kutusu değildir ve şifreleme için kullanılan kutunu tersidir.

3. Ters Sütun Değiştirme

Her sütun $a^{-1}(x) = \{0B\}x^3 + \{0D\}x^2 + \{09\}x + \{0E\}$ denklemi ile çarpılır ve elde edilen yeni sütun eskisinin yerine yazılır.

4. Döngü Anahtarını Ekleme

Döngü anahtarını eklemenin tersi yine kendisidir. AES algoritması şifreleme ve şifreyi çözmede aynı anahtarı kullanan simetrik yapıya sahiptir.

3. Bulgular

Bu bölümde esnek şifreleme ve esnek deşifreleme algoritmaları verilip elde edilen yeni şifreleme yönteminin uygulaması yapılacaktır. Esnek kümeler, esnek matrisler ve keyfi olarak alınan $\pi \in S_5$ e bağlı olarak yeni şifreleme yöntemini ileri süreceğiz.

Harfler A B C D E F G H I J K L M N O P Q R S T U V W X Y Z Ç Ğ İ Ö Ş Ü

Numaralar 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31

Harflerin ikili sistemde karşılıkları ;

Harfler	A	B	C	D	...	Ş	Ü
İkili sistem	00000	00001	00010	00011		11110	11111

şeklindedir.

Esnek matris S ile, mesaj M ve şifreli metin C ile ifade edilecektir. Esnek matrisin her bir satırı π'e göre düzenlenerek elde edilen esnek matris S_π ile gösterilecektir.

Teorem 3.1. S,M, C ∈ S_{mxn} ve π ∈ S_5 olsun. Aşağıda farklı şifreleme yöntemleri verilmiştir.

$i)$ $S_\pi \cdot_i M = C$

$ii)$ $S_\pi \cdot_c M = C$

$iii)$ $(S_\pi \cdot_i M) \cdot_c S_\pi = C$

Teorem 3.1. i) ile esnek şifreleme algoritması

1. Herhangi bir esnek küme alınır.
2. Esnek kümeye karşılık gelen esnek matris elde edilir.
3. Mesaj bloklara bölünür ve ikili sistemde karşılıkları bulunur.
4. Esnek matrisin her bir satırı alınan π'e göre tekrar düzenlenir S_π elde edilir.
5. $S_{\boldsymbol{\pi}}$ ile mesajın invers çarpımı yapılır.
6. Elde edilen matristen her satırın harf karşılığı bulunup alıcıya gönderilir.

Örnek 3.1. Esnek küme $(f_A,E)=\{(e_1,\{u_1,u_2\}),(e_2,\{u_2,u_3,u_4,\}),(e_4,\{u_1,u_5\}),\ (e_5,\{u_3,u_4\})\}$ olsun. Şifrelenmek istenilen mesaj YENİ ŞİFRELEME olsun. Esnek kümeye karşılık gelen matris

$$S=\begin{bmatrix}1&0&0&1&0\\0&1&0&0&0\\0&1&0&0&1\\0&1&0&0&1\\0&0&0&1&0\end{bmatrix}$$ olur.

Mesaj bloklara bölünür. YENİŞ-İFREL-EMEAA ikili sistemdeki karşılıkları hesaplanır ve her blok bir matris oluşturur. Burada bloğun tamamlanması için son kısma mesajı bozmayan harf eklenmiştir.

YENİŞ- 11000, 00100, 01101, 11100, 11110

$$M=\begin{bmatrix}1&1&0&0&0\\0&0&1&0&0\\0&1&1&0&1\\1&1&1&0&0\\1&1&1&1&0\end{bmatrix}$$

π =(13542) ∈ S_5 alalım. Esnek matrisin her bir satırı π'e göre düzenlenir. 1→ 3 → 5 → 4 → 2 → 1 oldğundan esnek matrisin satırındaki birinci eleman üçüncü elemanın yerine, üçüncü eleman beşinci eleman yerine, beşinci eleman dördüncü eleman yerine, dördüncü elaman ikinci elemanın yerine ve ikinci elemanda birinci elemanın yerine yazılır. Bu düzenlemeye göre her bir satır oluşturulur.

$$S_\pi = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix}$$ elde edilir.

$$S_\pi \cdot_i \mathrm{M} = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \end{bmatrix} = \mathrm{C}$$

Mesajın şifrelenmiş bloğu UUÜOW olur. Mesajın diğer blokları da benzer işlemlerle bulunur.

Şifreli metin: UUÜOW-QVDWD-IİWSI bulunur ve alıcıya gönderilir.

Teorem 3.2. S,M, C ∈ S_{mxn} ve π ∈ S_5 olsun. Aşağıda Teorem 3.1. e göre farklı deşifreleme yöntemleri verilmiştir.

$i)$ $\mathrm{C} \cdot_i S_\pi = \mathrm{M}$

$ii)$ $\mathrm{C} \cdot_c S_\pi = \mathrm{M}$

$iii)$ $S_\pi \cdot_i (\mathrm{C} \cdot_c S_\pi)$

Teorem 4.1. i) ile esnek deşifreleme algoritması

1. Şifrelemede kullanılan esnek küme alınır.

2. Esnek kümeye karşılık gelen esnek matris elde edilir.

3. Şifreli metin bloklara bölünür ve ikili sistemde karşılıkları bulunur.

4. Esnek matrisin her bir satırı alınan π' e göre tekrar düzenlenir S_π elde edilir.

5. Şifreli metin ile S_π'nin invers çarpımı yapılır.

6. Elde edilen matrisin her satırının harf karşılığı bulunur ve mesaj deşifrelenmiş olur.

Örnek 4.1. Örnek 3.2. deki esnek kümeyi ve mesajı alalım.

(f_A,E)={(e_1,{u_1,u_2}),(e_2,{u_2, u_3, u_4,}), (e_4,{u_1, u_5}), (e_5,{u_3, u_4})} olsun. Esnek kümeye karşılık gelen matris

$$\mathrm{S} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Şifreli metin UUÜOW- QVDWD- İİWSI bloklara bölünür ve ikili sistemdeki karşılıkları bulunur.

$$C=\begin{bmatrix}1&0&1&0&0\\1&0&1&0&0\\1&1&1&1&1\\0&1&1&1&0\\1&0&1&1&0\end{bmatrix}-\begin{bmatrix}1&0&0&0&0\\1&0&1&0&1\\0&0&0&1&1\\1&0&1&1&0\\0&0&0&1&1\end{bmatrix}-\begin{bmatrix}0&1&0&0&0\\1&1&1&0&0\\1&0&1&1&0\\1&0&0&1&0\\0&1&0&0&0\end{bmatrix}$$ elde edilir.

Esnek matrisin her bir satırı $\pi=(13542)$'e göre düzenlenir.

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

$$C\cdot_i S_\pi = M=\begin{bmatrix}1&1&0&0&0\\0&0&1&0&0\\0&1&1&0&1\\1&1&1&0&0\\1&1&1&1&0\end{bmatrix}-\begin{bmatrix}1&1&1&0&0\\0&0&1&0&1\\1&0&0&0&1\\0&0&1&0&0\\0&1&0&1&1\end{bmatrix}-\begin{bmatrix}0&0&1&0&0\\0&1&1&0&0\\0&0&1&0&0\\0&0&0&0&0\\0&0&0&0&0\end{bmatrix}$$ elde edilir.

Her matrisin harf karşılıkları bulunur. YENİŞ-İFREL-EMEAA. Mesaj YENİ ŞİFRELEME deşifrelenmiş olur. Benzer şekilde diğer teoremler de kullanılarak şifreleme ve deşifreleme uygulanabilir.

4. Tartışma ve Sonuç

Elde edilen bulgulara göre esnek küme yardımıyla oluşturulan şifreleme algoritması güvenilir ve hızlıdır. Aes şifreleme algoritmasında kullanılan anahtarın uzunluğuna göre döngü sayısı arttığından işlem sayısı ve bellek alanı da artar. Şifrelemede güvenilirlik önemlidir ancak şifreleme hızı da kullanışlılığı etkiler. Aes şifreleme güvenli olmasına rağmen farklı anahtar uzunluklarının kullanılması algoritma hızını düşürür.

Teşekkür

Bu çalışma, Proje Numarası: FYL-2017-7109 olan "Esnek Kümeler Yardımıyla Elde Edilen Yeni Bir Kriptosistem" isimli Yüksek Lisans Tez Projesi ile Erciyes Üniversitesi Bilimsel Araştırma Projeleri Koordinasyon Birimince Desteklenmiştir

Kaynakça

[1] Molodtsov, D. 1999. Soft Set Theory-Firrst Results, Computers and Mathematics with Applications, 37 (1) (1999), 19-31.

[2] Maji, P. K., Bismas, R., Roy, A.R. 2003. Soft Set Theory, Computers and Mathematics with Applications, 45(1) (2003), 550-562

[3] Ali, M.I., Feng, F., Liu, X., Min, W.K., Shabir, M. 2009. On Some New Operations in Soft Set Theory, Comput. Math Appl. 57(9) (2009), 1547-1553

[4] Sezgin A., Atagün A.O. 2011. On Operations of Soft Sets Comput. Math. Appl. , 61(5) (2011) 1457-1467.

[5] Aktaş, H., Çağman, N. 2007. Soft Sets and Soft Groups, Information Sciences, 177(1) (2007), 2726- 2735.

[6] Acar U., Koyuncu F. and Tanay B. 2010. Soft Sets and Soft Rings, Comput. Math. Appl. 59 (2010), 3458-3463.

[7] Sezgin. A., Atagün A.O., Aygün E., 2011. A Note On Soft Near-Rings and Idealistic Soft Near-Rings, Filomat, 25(1) (2011), 53-68

[8] Atagün A.O. and Sezgin A. 2011. Soft Substructures of Rings, Fıelds and Modules, Comput. Math. Appl., 61 (3) (2011) 592-601.

[9] D.Molodtsov, 2004. The Theory of Soft Sets, URRS Puplishers. , Moscow, 2004, (in Russian)

[10] D. Stinson. 1995. Cyrptography: Theory and Practice , CRC Press, New Jersey 573s.

[11] C.F. Yang , A note on soft set theory. 2008. Computers and Matematics with Aplications. 2003. 56 (2008), 1899-1900. [Comput. Math. Appl. 45 (4-5) (2003), 555-562]

[12] Atagün A.O., Aygün E. 2016. Groups of Soft sets. Journal of Intelligent & Fuzzy Systems 30 (2016) 729–733