Cumhuriyet Science Journal
CSJ

e-ISSN: 2587-246X
ISSN: 2587-2680

Cumhuriyet Sci. J., Vol.40-1(2019) 69-78

AES Encryption and A Cryptosystem Obtained with Soft Set II

Emin AYGÜN

Erciyes University, Faculty of Sciences, Department of Mathematics, Kayseri, TURKEY

Received: 18.04.2018; Accepted: 05.12.2018 *http://dx.doi.org/10.17776/csj.416395*

Abstract. In this paper, a new cryptographic algorithm was created with the soft sets, symmetric groups, soft matrices representing soft sets, and AES. In 1999, by Molodtsov proposed soft set theory as a new mathematical tool to deal with uncertainties. This theory which has been applied to many fields which contain uncertainties received much attention since proposed. The inverse product and characteristic product defined on soft matrices was used in soft encryption and soft decryption. In order to make the encryption more secure, symmetric groups included in the algorithm.

***Keywords*:** Soft Set, AES, Inverse Product, Characteristic Product.

AES Şifreleme ve Esnek Kümeler Yardımıyla Elde Edilen Kriptosistem II

Özet. Bu çalışmada, esnek kümeler, esnek kümeleri temsil eden esnek matrisler, simetrik gruplar ve AES ile yeni bir şifreleme algoritması oluşturulmuştur.1999'da Molodtsov tarafından esnek küme teorisi belirsizlikleri ortadan kaldırabilmek için yeni bir matematiksel yöntem olarak kullanılmaya başlandı. Belirsizlikleri içeren birçok alana uygulan bu teori önerildiğinden bu yana çok dikkat çekmiştir. Esnek matrisler üzerinde tanımlanan invers çarpım ve karakteristik çarpım esnek şifrelemede ve esnek deşifrelemede kullanılmıştır. Şifrelemenin daha güvenli olması için simetrik gruplar algoritmaya dahil edilmiştir.

***Anahtar Kelimeler*:** Esnek Küme, AES, İnvers Çarpım, Karakteristik Çarpım.

1. INTRODUCTION

The soft set theory introduced by Molodtsov[1] is seen as an effective mathematical tool as composed to other existing methods that were used to deal with uncertainties. The advantage of soft set theory over other theories is that researchers can select any parameters when they needed, since it does not impose any restriction while defining an object.

By using soft set theory Molodtsov worked in many fields such as Riemann integration, game theory, continuous differentiable functions, probability theory and measure theory[1-3].

Roy et. al. [4] investigated soft set theory for decision making problems. Many researches studied on soft set theory. For exampleFeng et al. [5] defined various concepts such as intersection, union, difference on soft sets. Sezgin and Atagün [6] introduced intersection, extended intersection, limited union, and limited difference on soft sets and examined the relationship with others. Aktaş and Çağman[7] compared soft sets with related concept of fuzzy sets and rough sets. In addition to, they introduced concept of soft group that has been launched in many new works. They also defined concepts of soft subgroup, normal soft subgroup and soft homomorphism on soft groups. Atagün and

* Corresponding author. *Email address:* *eaygun@erciyes.edu.tr*

Sezgin [8] worked on ring, field and soft algebraic modul. Sezgin and Atagün [9] defined soft near-ring. Atagun and Aygun proved that the set of all soft sets over a universe U is an abelian group under the each operations and called "the inverse group of soft sets" and "the characteristic group of soft sets" [10].

AES(Advanced Encryption Standard) is a subset of the Rijndael block cipher developed by two Belgian cryptographers, Vincent Rijmen and Joan Daemen, who submitted a proposal to NIST during the AES selection process. Rijndael is a family of ciphers with different key and block sizes [11]. AES which still maintains its reliability today, is used for security in the computing world. Today, fast and small size product are required in techonology's preferred features. Therefore, AES and speed need to have as few memories as possible. In our study [12], we did this with the charahteristic product. In this paper, a new cryptographic algorithmusing the inverse product is proposed for soft sets, soft matrices, symmetric groups and using the row shift method in AES cryptosystem.

2. PRELIMINARIES

Definition 2.1. Let U be a universal set, $P(U)$ be power set of U, E be a parameter set and $A \subseteq E$. Then, $f_A : E \to P(U)$ defined as follows:

$$(f_A, E) = \{(e, f_A(e)) : e \in E,\ f_A(e) \in P(U) \mid e \notin A \text{ ise } f_A(e) = \varnothing\}$$

The pair (f_A, E) is called soft set on U [13]. Where, f_A is approximate function of (f_A, E) and $f_A(e)$ is called ε-approach set. (f_A, E) can be represented as (F, A) or F_A. Moreover, (f_A, E) can be written as $(f_A, E) = \{f_A(e) | e \in A\}$[2].

Definition 2.2. Let (f_A, E) be a soft set on U.

i_1) If for all $e \in A$, $(f_A, E) = \emptyset$, then (f_A, E) is called empty soft set and it is denoted by $(f_A, E) = \Phi$.

i_2) If for all $e \in A$, $(f_A, E) = U$, then (f_A, E) is called absolute soft set and it is shown as $(f_A, E) = (f_{\tilde{A}}, E)$ [1].

Definition 2.3. Let (f_A, E) be a soft set on U .The complement of (f_A, E) denoted by $(f_A, E)^c$, $\forall e \in E$, $f^c{}_A(e) = U / f_A(e)$ [1].

Proposition 2.4. Let (f_A, E) be a soft set on U. Then,

i_1) $(f^c{}_A, E)^c = (f_A, E)$,

i_2) $\Phi^c = (f_E, E)$ [2].

Definition 2.5. The algorithm that uses the same key for encryption and decryption is called secret keyed algorithm [14].

Definition 2.6. The algorithms in which different keys are used for the encryption and decryption operations, decryption key can't be obtained from encryption key are called open keyed algorithm [14].

Definition 2.7. (Advanced Encryption Standard **)** The AES encryption algorithm is a block encryption algorithm that encrypts 128-bit data blocks with 128, 192 or 256-bit key operations. The information of

128 bits in size is separated into (4x4) square matrices and included in the encryption algorithm. The obtained matrix is named as “state” and every row of this matrix is named as “word” [14].

Definition 2.8. (Loop Structure)
Once state matrix is established, algorithm come into operation. The length of key determines the number of loops. The process of using columns is not needed in the final loops, a coded block is obtained by doing addition with the type key. The inverse of these sub-operation is used to solve encrypted text. In loops of state matrix, the four operations, given in [14] are used.

Definition 2.8.1. (Bit Changing)
Matrix named as state matrix will have a change in its elements. These changes are made according the previously calculated S-box. In S-box, the elements of the state matrices can be 16x16 matrix since they are based on the hexadecimal basis [14].

Definition 2.8.2. (Row Shifting)
This operation is done on new state matrix. The first row of the matrix remains fixed, the second, third and fourth rows are shifted by 1, 2 and 3 rows to the loft respectively [14].

Definition 2.8.3. (Column Shuffling)
The shuffling of columns is achieved by matrix multiplication of each column of the state matrix obtained by shifting rows in previous stage equation

$$a(x) = \{03\}\, x^3 + \{01\}\, x^2 + \{01\}\, x + \{02\}$$

independently. The new column is replaced by the old column [14].

Definition2.8.4. (Adding Loop Key)
According to AES algorithm, the key material is added at th end of each loop. This is the key index originally generated by the key generation block [14].

Definition 2.9.
The AES decryption algorithm is an algorithm used for decrypting the encrypted text. Similar steps used to decrypt the encrypted text, but operations are inversed. The conversions applied to encrypt the text are translated in the opposite direction and start in the inverse order of encryption [14].

Definition 2.9.1. (Inverse Row Shifting)
The state matrix is shifting to the right rather than to the left as applied in encryption. The second, third and fourth row are shifted by 1, 2 and 3 rows to the right respectively [14].

Definition 2.9.2.(Inverse Byte Changing)
In the encryption process, S- box has been used to change the byte. Similarly, S-box is also used for decryption. However, this S-box is the inverse of the S-box used for encryption [14].

Definition 2.9.3. (Inverse Coloumn Changing)
Every coloumn is multiplied with the equation $a^{-1}(x) = \{0B\}x^3 + \{0D\}x^2 + \{09\}x + \{0E\}$ and replaced with the old column [14].

Definition 2.9.4. (Adding Loop Key)
The loop key has a symmetrical structure and the opposite of the loop key is itself. The AES algorithm uses the same key to encrypt and decrypt the text [14].

Definition 2.10. The one-to-one and onto function defined on a non-empty set A is called permutation. It is a group with respect to composition of functions, and named as permutation group. It is shown as S_n [16].

3. SOFT MATRICES

Definition 3.1. Let (f_A, E) be a soft set on U. The subset $R_A = \{(u,e) : e \in A, u \in f_A(e)\}$ of $U \times E$ is called relation form of (f_A, E).

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

where R_A is called characteristic function [15].

If $a_{ij} = X_{R_A}(u_i, e_j)$,

$[a_{ij}] = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix}$ is called soft matrix of (f_A,E) on U. The all soft matrix of U are denoted by SM_{mxn}.

Example 3.2. Let U={ u_1 ,u_2, u_3, u_4, u_5} be the universal set, E={ e_1 , e_2 , e_3 , e_4 } be parameter set, A= { e_1 , e_3 , e_4} and (f_A, E) = { $(e_1, \{u_2, u_4\})$,$(e_3, \{u_1, u_3, u_5\})$,$(e_4\ U)$ }. The relation form of (f_A , E) R_A = { (u_2, e_1) , (u_4, e_1) ,(u_1, e_3),(u_3, e_3), (u_5, e_3) (u_1, e_4) , (u_2, e_4) , (u_3, e_4) , (u_4, e_4) , (u_5, e_4) }. Then soft matrix

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

Definition 3.3. Let $[a_{ij}] \in SM_{mxn}$.

i_1) If a_{ij}= 0 for all i and j, $[a_{ij}]$ is called zero soft matrix and it is shown with [0].

i_2) If a_{ij}= 1 for all j $\in I_A$= {j: $e_j \in$ A} and i , $[a_{ij}]$ is called A-universal soft matrix and it is shown with $[\tilde{a}_{ij}]$.

i_3) If a_{ij} = 1 for all i and j , $[a_{ij}]$ is called universal soft matrix and it is shown with [1]. [10]

Definition 3.4. Let $[a_{ij}]$, $[b_{ij}] \in SM_{m \times n}$. Then "$\cdot_i$" inverse product of $[a_{ij}]$ and $[b_{ij}]$ is

$[a_{ij}] \cdot_i [b_{ij}] = [c_{ij}]$, for each i, j

it is defined as $c_{ij} = \begin{cases} 1, & a_{ij} \neq b_{ij} \\ 0, & a_{ij} = b_{ij} \end{cases}$ [10].

Definition 3.5. Let $[a_{ij}], [b_{ij}] \in SM_{m\times n}$. Then "$\cdot_c$" characteristic product of $[a_{ij}]$ and $[b_{ij}]$ is $[a_{ij}] \cdot_c [b_{ij}] = [c_{ij}]$, for each i, j

it is defined as $c_{ij} = \begin{cases} 1, & a_{ij} = b_{ij} \\ 0, & a_{ij} \neq b_{ij} \end{cases}$ [10].

4. SOFT ENCRYPTION

The numbers corresponding to the letters in the alphabet for the cryptosystem are as follows:

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

The 5-bit counterpart of each letter in binary system:

A	B	C	…	Ş	Ü
00000	00001	00010	…	00100	11111

Due to binary system 6 letters are added to obtain 32: Ç,Ğ,İ,Ö,S,Ü.

Definition 4.1. While any $S \in SM_{5X5}$ soft matrix is arranged according to any $\pi \in S_5$ permutation group, the elements in each row of the soft matrix are displaced according to the given π. Obtained matrix will be shown with S_π. This paper, soft matrix will be shown with S, message with M,ciphertext with C.

Example 4.2. Let $S = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \end{bmatrix}$ and π =(13542). The elements of each row of soft matrix are displaced according to $1 \to 3 \to 5 \to 4 \to 2 \to 1$ to arrange soft matrix according to π permutation. The first row arranged is 00111. If the same operation applied to each row

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

matrix is obtained.

Theorem 4.3. Let $S, M, C \in SM_{5x5}$ and $\pi \in S_5$. Then,

$i_1)$ $S_\pi \cdot_i M = C$

$i_2)$ $S_\pi \cdot_c M = C$

$i_3)$ $(S_\pi \cdot_i M) \cdot_c S_\pi = C$

Proof: Theorem 4.3. Soft Encryption Algorithm with i_1)

1. Any soft set is taken.
2. A soft matrix is obtained which corresponds to the soft set.
3. The message is divide into blocks and found counterpart in binary system.
4. The first row of the soft matrix remains fix, the second, third and fourth row is shifted by 1, 2 and 3 rows to the left respectively.
5. Each row of the soft matrix is rearrange according to π and S_π key is obtained.
6. Makes "$\cdot_i$" product S_π and message.
7. Each row of the matrix which obtained letter and sends to receiver.

The other matters of the theorem can be done in similar way only changing the type of product.

Theorem 4.4. Let $S, M, C \in SM_{5x5}$ and $\pi \in S_5$. Different decryption methods are given as follows according to Theorem 4.3.

$i_1)\ C \cdot_i S_\pi = M$

$i_2)\ C \cdot_c S_\pi = M$

$i_3)\ S_\pi \cdot_i (C \cdot_c S_\pi) = M$

Proof: Theorem 4.4. Soft Decryption Algorithm with i_1)

1. The soft set used for encryption is taken.
2. The soft matrix corresponding to the soft set is obtained.
3. Ciphertext is divided into blocks and found corresponding in the binary system.
4. The first row of the soft matrix remains fix, the second, third and fourth row is shifted by 1, 2 and 3 rows to the left respectively.
5. Each row of the soft matrix is rearrange according to π and S_π key is obtained.
6. Makes "$\cdot_i$" product S_π and ciphertext.
7. Each row of the matrix which obtained letter and the message is decrypted.

The other matters of the theorem can be done in similar way only changing the type of product.

5. APPLICATION OF SOFT ENCRYPTION AND DECRYPTION

Example 5.1. Soft Encryption

1) Let (f_A ,E) = { (e_1 , {u_1 , u_3, u_5}) ,(e_3 , {u_2 , u_4 , u_5}) , (e_5 , {u_3 , u_4}) } be soft set on U Let " SOFT ENCRYPTION " is the message.

2) The soft matrix corresponding to the soft set:

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

3) The message is divided into blocks. SOFTE / NCRYP / TIONA
Found counterpart in binary system and each row create a matrix. Here, to the last of the message is appended with a letter to complete the block.

SOFTE - 10010 , 01110 , 00101 , 10011 , 00100

$$M_1 = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

NCRYP - 01101, 00010, 10001, 11000, 01111

$$M_2 = \begin{bmatrix} 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

TIONA - 10011, 01000, 01110, 01101, 00000

$$M_3 = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

4) Other rows obtained the first row of the soft matrix are shifted as defined in the algorithm.

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

5) Let $\pi = (14235) \in S_5$. Soft matrix is arranged according to π.

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

6) $S_\pi \cdot_i M_1 = C_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix}$

Similarly, $C_2 = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}$, $C_3 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \end{bmatrix}$ is obtained.

7) Turns from soft matrix of message the letter. the ciphertext is obtaind as

" QCNHIPOZMDREGZM" and is sent to receiver.

Soft Decryption

1) The soft set used for encryption is taken.
(f_A ,E) = { (e_1 , {u_1 , u_3, u_5}) ,(e_3 , {u_2 , u_4 , u_5}) , (e_5 , {u_3 , u_4}) }

2) The soft matrix corresponding to the soft set:

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

3) The ciphertext is divided into blocks "QCNHI- POZMD- REGZM" soft matrices of the ciphertext respectively:

$$C_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix}, C_2 = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}, C_3 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \end{bmatrix}$$

4) Other rows except the first row of the soft matrix are shifted as defined in the algorithm.

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

5) $\pi = (14235) \in S_5$ was taken as. Soft matrix is arranged according to π.

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

6) $C \cdot_i S_\pi = M_1 = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}$, $M_2 = \begin{bmatrix} 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \end{bmatrix}$, $M_3 = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$

7) Turns from soft matrix of message the letter. SOFTE / NCRYP / TIONA the message is decrypted. “SOFT ENCRYPTION” obtains the message. Similarly, other theorems can be used for encryption and decryption.

6. CONCLUSION

In this paper, a new cryptographic algorithm was created based on the soft sets, symmetric groups and AES. Precise selection of universal set and soft set elements improves the security of encryption. The soft encryption created with $\pi \in S_5$ similarly can be applied for $\pi \in S_6$, S_7. Then, the size of the soft matrix changes. Furthermore, we can also do the operations in the rows instead of the columns.

Acknowledgements

This paper was supported by the BAP project, Project Number: FYL-2018-7999.

REFERENCES

[1]. Molodtsov, D., Soft set theory-first results, Computers and Mathematics with Applications, 37 (1999) 19–31.
[2]. Molodtsov, D. , The Theory of Soft Sets, URRS Puplishers. , Moscow, (in Russian) 2004.
[3]. Rivest, R. , Adleman, L. and Dertouzos, M., On data banks and privacy homomorphisms, In Foundations of Secure Computation, (1978) 169–180.
[4]. Roy, A.R. and Maji, P.K., A fuzzy soft set theoretic approach to decision making problem, Journal of Computational and Applied Mathematics , 203 (2007) 412–418.
[5]. Feng, F., Jun, Y. B. and Zhao X., Soft semirings, Computers and Mathematics with Applications, 56 (2008) 2621–2628.

[6]. Sezgin, A. and Atagün, A.O., On operations of soft sets, Computers and Mathematics with Applications, 61 (2011) 1457–1467.
[7]. Aktas H., Çagman N., Soft sets and soft groups, Inform. Sci. , 177 (2007) 2726-2735.
[8]. Atagün, A.O. and Sezgin, A., Soft substructures of rings, fields and modules, Comput. Math. Appl., 61 (3) (2011) 592-601.
[9]. Sezgin, A .Atagün, O. and Aygün, E., A note on soft near-rings and idealistic soft near-rings, Filomat, 25-1 (2011) 53–68.
[10]. Atagün, A.O. and Aygün, E., Groups of soft sets, Journal of Intelligent and Fuzzy Sys., 30 (2016) 729-733.
[11]. Miller, F.P., Vandome, A.V., McBrewster, J., Advanced Encryption Standard, Alpha Press, London, 243s. 2009.
[12]. Aygun, E. and Akbulut, S. AES Şifreleme ve Esnek Kümeler Yardımıyla Elde Edilen Yeni Bir Kriptosistem, Erciyes University Journal of the Institute of Science and Technology, 35-1 (2019)
[13]. Maji, P.K., Biswas , R. and Roy, A.R., Soft set theory. Computers & Mathematics with Applications, 45 (2003) 555-562.
[14]. Daeman, J., Rijmen, V. The design of Rijndael: AES: the Advanced Encryption Standard.Berlin Heidelberg: Springer-Verlag 128s, 2002.
[15]. Çağman, N. and Enginoğlu S., Soft matrix theory and its decions making, Computers and Mathemetics with Applications, 59 (2010) 3308-3314.
[16]. Stinson, D., Cyrptography: Theory and Practice , CRC Press, New Jersey 573s. 1995.