

Polynomial Representation of Vernam Cipher

Emin Aygün ^{1,a,*}, İncinur Yılmaz ^{1,b}

¹ Department of Mathematics, Faculty of Science, Erciyes University, Kayseri, Türkiye.

² Department of Mathematics, Faculty of Science, Erciyes University, Kayseri, Türkiye.

*Corresponding author

Research Article

History

Received: 11/01/2024

Accepted: 24/06/2024





This article is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License (CC BY-NC 4.0)

ABSTRACT


Storing information or data has been one of the basic needs of humans for many years and these needs have led to the existence of some systems throughout the years. In this paper, soft sets represented by polynomials will be encrypted and decrypted in line with their representations. We are going to use the Rijndael Algorithm for soft sets and then encrypt and decrypt the data in accordance with its algorithm. The Rijndael algorithm is an algorithm which carries out the cyclic process according to the keys it has. At the end of each loop, the key is renewed and is applied to the data. These data are firstly shown in strings. While enumerating, it starts with zero index and ends with one less than string length.

Keywords: Soft sets, Encryption, Decryption, Vernam cipher, Stream cipher.

 eaaygun@erciyes.edu.tr

 <https://orcid.org/0000-0003-3503-0552>

 incinur.yilmaz@hotmail.com

 <https://orcid.org/0000-0001-6481-8918>

Introduction

Since people need some information to send data in secret, cryptography has been a practical tool over the centuries. Thus, only the planned receiver of the data can understand it. Besides, cryptosystems have two different types: The first one is a symmetric cryptosystem which uses only one key during the encryption and decryption process while the second one is, an asymmetric cryptosystem which uses two different keys throughout the process [1,2]. A key is employed for encrypting data, while its counterparts are utilized to decrypt the encrypted information.

The symmetric cryptosystem has two different ciphers stream ciphers and block ciphers. It is not hard to distinguish. The most important difference between block and stream cipher is that while we deal with bits at a time in stream ciphers, in block ciphers, we deal with blocks all the time [3].

In this article, we examine a stream cipher known as Vernam Cipher and also application on a soft set dealing with uncertain objects to avoid some difficulties. The concept of encrypting soft set emerges from the security issues of the objects that the soft set deals with. However, we have three traditional theories dealing with uncertainties and solving complex problems in engineering, environment, economies, and others:

The first one is the theory of probability, the second is the theory of fuzzy sets [4,5] and the last one is interval mathematics [6]. Because of the assorted uncertainties of these problems, one cannot successfully use them. Additionally, each theory has its own difficulty in itself. Accordingly, these theories are not sufficient for describing a tiny change of date information and therefore

they are not reliable and adequate. They also somewhat contradict aims and other difficulties.

Materials and Methods

Definition 1.

Let U be a universal set, E is the parameters' set, and $P(U)$ is the power set of U and $A \subseteq E$. Assume that there is a soft set over universal set $(U: f_A: E \rightarrow P(U))$ such that if $e_j \notin A$ then $f_A(e_j)$ is defined F_A as \emptyset so $F_A = \{(e_j, f_A(e_j)) : e_j \in E, f_A(e_j) \in P(U)\}$.

Here, f_A is called the approximation function of the F_A [7].

Definition 2.

Let $U = \{u_1, u_2, u_3, \dots, u_n\}$ be a universal set, $E = \{e_1, e_2, e_3, \dots, e_m\}$ parameters' set, $A \subseteq E$ and F_A be a soft set over U .

$$R_A = \{(u_i, e_j) : e_j \in A, u_i \in F(e_j)\} \subseteq U \times E$$

is called the relation form of F_A . In this case, the characteristic function of the R_A relation form is defined by

$$X_{R_A}: U \times E \rightarrow \{0,1\}, A_{R_A}(u_i, e_j) = \begin{cases} 1, & (u_i, e_j) \in R_A \\ 0, & (u_i, e_j) \notin R_A \end{cases}$$

R_A can be described with the following table, where $U = \{u_1, u_2, u_3, \dots, u_n\}$ is a universal set, $E = \{e_1, e_2, e_3, \dots, e_m\}$ is the set of parameters and $A \subseteq E$:

R_A	e_1	e_2	...	e_m
u_1	$X_{R_A}(u_1, e_1)$	$X_{R_A}(u_1, e_2)$...	$X_{R_A}(u_1, e_m)$
u_2	$X_{R_A}(u_2, e_1)$	$X_{R_A}(u_2, e_2)$...	$X_{R_A}(u_2, e_m)$
\vdots	\vdots	\vdots	\ddots	\vdots
u_n	$X_{R_A}(u_n, e_1)$	$X_{R_A}(u_n, e_2)$...	$X_{R_A}(u_n, e_m)$

[8].

Definition 3.

Let $[a_{ij}], [b_{ij}] \in S_{m \times n}$. The inverse product of the soft matrices $[a_{ij}]$ and $[b_{ij}]$ are defined by $[a_{ij}] \cdot_i [b_{ij}] = [c_{ij}]$ where

$$c_{i,j} = \begin{cases} 1, & \text{if } a_{i,j} \neq b_{i,j} \\ 0, & \text{if } a_{i,j} = b_{i,j} \end{cases}$$

[9].

Definition 4.

The numerical equivalences of the letters are given in the following:

LETTERS	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
NUMBERS	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				

Thus, A starts from 0, and the letter Ü becomes 31. If the letters were matched with the binary system, it would be as follows:

LETTERS	A	B	C	D	E	...	Ş	Ü
BINARY	00000	00001	00010	00011	00100	...	11110	11111
SYSTEM								

Because we want the binary system to be 32 bits, we add six more letters such as Ç, Ğ, İ, Ö, Ş, Ü. If desired, different characters can be added to this alphabet and the number can be increased to 64 bits [9].

Definition 5.

A stream cipher which sends plaintext string P_1, P_2, P_3, \dots , using the key stream S_1, S_2, S_3, \dots , to a ciphertext C_1, C_2, C_3, \dots , where $C_i = E_{S_i}(P_i)$. The corresponding decryption function is $D_{d_i}(C_i) = P_i$. Also, d is a decryption key corresponding to the encrypting key S_i [10].

If the similarities between encryption and decryption algorithms are wanted to be proven, it has to be proven that the decryption function produces the plaintext bit P_i again. The ciphertext bit C_i is calculated using the encryption algorithm $C_i \equiv S_i + P_i \pmod{2}$ as follows:

$$\begin{aligned} D_{S_i(C_i)} &\equiv C_i + S_i \pmod{2} \\ &\equiv (x_i + S_i) + S_i \pmod{2} \\ &\equiv x_i + S_i + S_i \pmod{2} \\ &\equiv x_i + 2S_i \pmod{2} \\ &\equiv x_i + 0 \pmod{2} \\ &\equiv x_i \pmod{2} \end{aligned} \quad [10].$$

Definition 6.

Vernam Cipher, due to Gilbert Vernam in 1917, to encrypt and decrypt telegraph messages automatically is the simplest cipher. In the Vernam Cipher, the key stream is represented by bit string $S_1, S_2, S_3, \dots, S_m$, with the same length as the plaintext message, which is also a bit string, $P_1, P_2, P_3, \dots, P_m$ [11]. Plaintext bits are encrypted using the encryption algorithm given below:

$$C_i \equiv E_{S_i}(P_i) \equiv S_i + P_i \pmod{2}$$

Thus, the decryption algorithm of Vernam Cipher is,

$$D_{S_i(C_i)} \equiv C_i + S_i \pmod{2}$$

Polynomial Representation of Vernam Cipher

Definition 7.

A stream cipher which sends plaintext string $P_1(x), P_2(x), P_3(x), \dots$, using the key stream $S_1(x), S_2(x), S_3(x), \dots$, to a ciphertext $C_1(x), C_2(x), C_3(x), \dots$ where $C_i(x) = E_{S_i(x)}(P_i(x))$. The corresponding decryption function is

$$D_{d_i(x)}(C_i(x)) = P_i(x)$$

Also, $d(x)$ is a decryption key corresponding to the encrypting key $S_i(x)$ [12].

Definition 8.

In Vernam encryption, the keystream $S_1(x), S_2(x), S_3(x), \dots, S_m(x)$ is a polynomial sequence $P_1(x), P_2(x), P_3(x), \dots, P_m(x)$ with the same number of terms as the plaintext message. Plaintext strings are encrypted according to the following encryption algorithm:

$$C_i(x) \equiv E_{S_i(x)}(P_i(x)) \equiv P_i(x) + S_i(x) \pmod{2}$$

Thus, the decryption algorithm of Vernam Cipher is,

$$D_{S_i(x)}(C_i(x)) \equiv C_i(x) + S_i(x) \pmod{2}$$

For the similarities between encryption and decryption algorithms, one has to prove that the decryption function produces the plaintext bit $P_i(x)$ again. As ciphertext bit $C_i(x)$ is calculated by using the encryption algorithm $C_i(x) \equiv S_i(x) + P_i(x) \pmod{2}$ as following:

$$D_{S_i(x)}(C_i(x)) \equiv C_i(x) + S_i(x) \pmod{2}$$

$$\equiv (X_i(x) + S_i(x)) + S_i(x) \pmod{2}$$

$$\equiv X_i(x) + S_i(x) + S_i(x) \pmod{2}$$

$$\equiv X_i(x) + 2S_i(x) \pmod{2}$$

$$C_i(x) \equiv S_i(x) + P_i(x) \pmod{2}$$

$$C_i(x) \equiv [(x^{18} + x^{11} + x^{10} + x^7) + (x^{18} + x^{17} + x^9 + x^6 + x^5 + x^2 + x + 1)] \pmod{2}$$

$$C_i(x) \equiv [2x^{18} + x^{17} + x^{11} + x^{10} + x^9 + x^7 + x^6 + x^5 + x^2 + x + 1] \pmod{2}$$

$$C_i(x) \equiv (x^{17} + x^{11} + x^{10} + x^9 + x^7 + x^6 + x^5 + x^2 + x + 1)$$

$$C_i(x) \equiv 00100\ 00011\ 10111\ 00111$$

As a result of the above steps, the ciphertext "EDXH" is obtained. Here note that the process has been made with the coefficients of the polynomials.

Example 2.

Let's decrypt the ciphertext "EDXH" as a polynomial using the Vernam Encryption Algorithm with the keyword "IDEA". The equivalence of "EDXH" in the binary system is 00100 00011 10111 00111 and the polynomial representation of the "EDXH" is $C_i(x) = x^{17} + x^{11} + x^{10} + x^9 + x^7 + x^6 + x^5 + x^2 + x + 1$. The equivalence of "IDEA" in the binary system is 01000 00011 00100 0000. Since the polynomial representation of the "IDEA" is $S_i(x) = x^{18} + x^{11} + x^{10} + x^7$ we use the decryption algorithm $P_i(x) \equiv C_i(x) + S_i(x) \pmod{2}$. Then,

$$P_i(x) \equiv C_i(x) + S_i(x) \pmod{2}$$

$$P_i(x) \equiv [(x^{17} + x^{11} + x^{10} + x^9 + x^7 + x^6 + x^5 + x^2 + x + 1) + (x^{18} + x^{11} + x^{10} + x^7)] \pmod{2}$$

$$P_i(x) \equiv (x^{18} + x^{17} + 2x^{11} + 2x^{10} + x^9 + 2x^7 + x^6 + x^5 + x^2 + x + 1) \pmod{2}$$

$$P_i(x) \equiv (x^{18} + x^{17} + x^9 + x^6 + x^5 + x^2 + x + 1)$$

$$P_i(x) = 01100\ 00000\ 10011\ 00111$$

As a result of the above steps, the plaintext "MATH" is obtained.

Suggestion For a New Cryptosystem

$[p_{ij}]_{m \times m}$ is the plaintext matrix, $[s_{ij}]_{m \times m}$ is the key matrix and they are two square matrices. The transposes of these matrices are $[p_{ij}]_{m \times m}^T$ and $[s_{ij}]_{m \times m}^T$;

Definition 9. Encryption procedure is obtained by

$$[p_{ij}]_{m \times m}^T \cdot [s_{ij}]_{m \times m}^T = [c_{ij}]_{m \times m}^T$$

By transposing the matrix $[c_{ij}]_{m \times m}^T$, the original ciphertext matrix $[c_{ij}]_{m \times m}$ is obtained. The encrypted matrix given to the receiver is $[c_{ij}]_{m \times m}$.

Definition 10. The decryption procedure is similar to the encryption procedure.

$$[c_{ij}]_{m \times m}^T \cdot [s_{ij}]_{m \times m}^T = [p_{ij}]_{m \times m}^T$$

The transpose of the plaintext matrix $[p_{ij}]_{m \times m}^T$ is obtained. By transposing the matrix $[p_{ij}]_{m \times m}^T$, the original plaintext matrix $[p_{ij}]_{m \times m}$ is obtained. Here, the decrypted version of the encrypted matrix given to the receiver is $[p_{ij}]_{m \times m}$.

Definition 11.

The Soft Encryption Algorithm is as follows:

Step 1: An arbitrary soft set is chosen.

Step 2: A soft set quadratic matrix is created using the selected soft set.

Step 3: The message is divided into blocks and each line is converted into a binary system.

Step 4: Each row of the soft matrix is rearranged according to the received π to obtain S_π .

Step 5: The characteristic multiplication of S_π and the message is made.

Step 6: The letter equivalent of each resulting line is found and sent to the recipient.

The Soft Decryption Algorithm is as follows:

Step 1: The encrypted message reaches the recipient.

Step 2: The receiver performs the characteristic multiplication of the encrypted message and S_π .

Step 3: The soft matrix is rearranged.

Step 4: The text equivalent of the matrix is found.

Step 5: The encrypted text is decrypted.

Example 3. Encrypt and decrypt the plaintext matrix $[p_{ij}]_{3 \times 3} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$ with the new encryption proposal using the

key matrix $[s_{ij}]_{3 \times 3} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix}$.

The transposes of the matrices are $[p_{ij}]_{3 \times 3}^T = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$ and $[s_{ij}]_{3 \times 3}^T = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}$.

If we apply the encryption procedure then $[p_{ij}]_{m \times m}^T \cdot_c [s_{ij}]_{m \times m}^T = [c_{ij}]_{m \times m}^T$, and therefore

$$\begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \cdot_c \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} = [c_{ij}]_{3 \times 3}^T$$

is obtained. If $[c_{ij}]_{m \times m}^T$ is transposed, then we have $[c_{ij}]_{3 \times 3} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$. (The matrix and its transpose coincided.)

If we apply the decryption procedure then $[c_{ij}]_{m \times m}^T \cdot_c [s_{ij}]_{m \times m}^T = [p_{ij}]_{m \times m}^T$, and therefore

$$\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} \cdot_c \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} = [p_{ij}]_{3 \times 3}^T$$

is obtained. If the $[p_{ij}]_{m \times m}^T$ is transposed, then we have $[p_{ij}]_{3 \times 3} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$.

In this way, a new encryption method is discovered.

Conclusion

According to these mathematical findings, we can encrypt and decrypt a soft set using the Vernam Encryption Algorithm as well as representing it as a polynomial. Additionally, as a result of our work, we found a new cryptosystem suggestion.

Conflict of interest

There are no conflicts of interest in this work.

References

- [1] Aktaş H., Çağman N., Soft Sets and Soft Groups, *Information Sciences*, 177 (2007) 2726-2735.
- [2] Aktaş H., Çağman N., Erratum to "Soft Sets and Soft Groups", *Information Sciences* 3 (2009), 338. *Information Sciences*, 177 (2007) 272-2735.
- [3] Atagün A.O., Sezgin A., Soft Substructures Of Rings, Fields and Modules, *Computers & Mathematics With Applications*, 61 (3) (2011) 592-601.
- [4] Zadeh L.A., Fuzzy Sets, *Information and Control*, 8 (1965) 338-353.
- [5] Zadeh L.A., Toward A Generalized Theory Of Uncertainty (GTU)-An Outline, *Information Sciences*, 172 (2005) 1-40.

- [6] Gorzalzany M.B., A Method Of Inference In Approximate Reasoning Based On Interval-Valued Fuzzy Sets, *Fuzzy Set and Systems*, 21 (1987) 1-17.
- [7] Dmitry M., Soft Sets Theory – First Results, *Computers & Mathematics With Applications*, 37 (1999) 19-31.
- [8] Atagün A.O., Kamacı H., Oktay O., Reduced Soft Matrices and Generalized Products With Applications In Decision Making, *Neural Computing and Applications*, 29 (2018) 445-456.
- [9] Aygün E., Soft Matrix Product and Soft Cryptosystem, *Filomath*, 32 (19) (2018) 6519-6530.
- [10] Hashim H.R., Husain A.M., Vernem Cipher Over A Soft Set, *Globakl Journal Of Mathematics*, 5 (2) (2015) 2395-4760.
- [11] Rosen K.H., Elementary Number Theory, and Its Applications. 5th Edn., United States of America, Boston, (2005) 363.
- [12] Aygün E., Yılmaz İ., Esnek Kümeler Ve Vernam Şifreleme Üzerine, 3. Başkent International Conference On Multidisciplinary Studies Full Text Book, 3. Başkent International Conference On Multidisciplinary Studies, Ankara, 2022, 1108-1115.