On The Hill Cipher Algorithm from Encryption Algorithms

Osman AKDAG

Ahirli Sehit Samet Butun Secondary School

Fikri KOKEN

Necmettin Erbakan University

Introduction

From the past to the present, security problems have been addressed in the communication exchange between people or units with the developing technology. As various communication systems have developed in different fields, this problem has brought different problems and difficulties. Encryption and decryption methods applied by the sender and receiver have gained importance to securely transmit the information sent over these communication systems from the sender to the receiver. One of these methods of providing secure communication is encryption with matrices.

Overview of Encryption Algorithms

One of the greatest needs today is that "information is stored accurately and securely and used by relevant people when and where necessary". In this context, we come across "Crypto", that is, "Encryption". Cryptography is the science of sending a secret message to another person, group, or device in such a way that only the recipient can read the message. An undesired person on any communication channel can interrupt the message transmission and receive the message, so it is always assumed that the communication channels are insecure. Encryption is a system that has been used since ancient times. Caesar is the first known source to use encryption in history (Konheim, 1981; Stinson, 2002; Trappe, 2005; Sinkov, 2009).

Now let's give a few definitions that we will use in the chapter.

Plaintext: In cryptography, messages are unencrypted. Understandable original text.

Ciphertext: It is the text converted from plaintext with any encryption.

Key: It is the critical information used by the cipher that only the sender and receiver know.

Encryption: It is the process of rendering plain text incomprehensible, transforming it into ciphertext.

Decryption: It is the process of making the cipher text understandable again.

Public key: In a public key encryption system, it is the key that is used only for encrypting the message and not for decryption.

Cryptanalysis: It is the illegal analysis that aims to reach the original data without information and key by examining the inputs or outputs of a cryptographic system. It is also called a code-breaking.

Cryptanalyst: Practitioners of cryptanalysis are called.

Cryptographic Algorithm: It is a set of mathematical operations used in encryption and decryption operations.

Symmetric Algorithms: These are algorithms in which a (same) key is used in encryption and decryption operations. Also called secret key algorithms.

Asymmetric Algorithms: These are the algorithms in which separate keys are used in encryption and decryption processes, and the decryption key cannot be obtained from the encryption key. Also called public key algorithms.

Entity: A person or tool that uses, accepts, or sends information.

Sender: A person who legitimately sends information in any communication.

Receiver: It is the person who receives the information in communication.

Adversary: It is a harmful person who tries to break the security in the communication between the parties, not the receiver or the sender.

Attack: A successful or unsuccessful attempt to crack part or all of a cryptosystem.

Channel: Person or tool that helps move information from one person to another.

For the adversary not to learn the contents of the secret message, symbolically, the sender named A encrypts the message called plain text and sends the encrypted message called ciphertext to the other party, symbolically named B.

Encryption: It is used for the safe transmission of data and information to the desired persons under all circumstances. The basic algorithms that we use while performing the encryption process constitute the cryptosystem, which are the basic building blocks of the cryptosystem.

In cryptography, encryption algorithms generate keys in the form of a series of bits that are used to encrypt or decrypt a piece of information. How these keys are used makes the difference between symmetric and asymmetric encryption.

Encryption algorithms are generally divided into two categories: symmetric and asymmetric encryption. The main difference between these two encryption methods is that while a single key is used in the symmetric encryption algorithm, two different but re-

lated keys are used in asymmetric encryption. Such a difference, although seemingly simple, determines the functional differences between the two encryption techniques and the way they are used.

Features of Encryption Systems

Encryption systems used to transmit and store information securely should have the following features. (Stinson, 2002; Trappe, 2005; Sinkov, 2009).

Security degree: It is defined as the number of transaction attacks against the system to obtain information until full results are obtained with the best method. The security rating of a typical system, also called the transaction element, requires more transactions than the highest number of transaction attacks.

Functionality: Encryption systems should be able to process different types of information securely within the system. The functions of this encryption system, which is based on providing security, should be integrated with each other.

Transaction methods: During the implementation of the encryption system, the basic transaction processes may occur in different ways with different inputs. This shows the typical characteristic difference in processing methods.

Performance: It is expressed in the number of bits that the encryption algorithm used in the encryption system can encrypt in one second.

Ease of implementation: A software or hardware environment of different complexity may be required for the implementation of processes within encryption systems. The degree of complexity in these environments is a factor that affects processing power. The applicability of an encryption system in constrained and difficult situations is important.

Information Security and Encryption

In order to talk about information security in general; basic elements, such as confidentiality, integrity, identity identification and verification, non-repudiation and continuity, must be found or created by cryptosystems.

Confidentiality can be expressed as ensuring that information is accessible only to those who have been authorized to access it. Confidentiality, which is the most basic step of security, is provided by encryption algorithms or approaches. It is known that it is difficult to have detailed information about any attack carried out with a passive attack. Therefore, since incoming and outgoing messages between two people may fall into the hands of attackers without being aware of it, the element of confidentiality is a must.

Messages sent or received are converted to a different format using an encryption algorithm. A secure environment is provided as the attackers cannot decrypt the hidden

messages that have been converted to different formats.

Integrity can be expressed as ensuring or recruitment that the content of a document or message is not changed. Integrity is one of the indispensable elements for any secure communication, and summarization algorithms are used to ensure this.

To ensure the integrity of a message, a summary of the sent message is taken and this digest is sent to the other party along with the message. The other party, on the other hand, extracts the summary of the received message and compares this summary with the summary sent to it.

Symmetric Encryption

On the basis of symmetric encryption algorithms, data is encrypted with a single secret key, and data is decrypted with the same key. That is, if the encryption is done with a secret key that is securely agreed upon by the communicating A and B in advance, this system is called symmetric encryption. Since the encryption and decryption keys are kept secret by A and B, only persons A and B with the secret key can encrypt or decrypt the message. As long as the keys remain secret, no one can understand or easily decipher the message, so A and B can communicate freely between them. These encryption methods work in mathematically uncomplicated transactions and work very fast, but the text must be delivered to the other user securely in the key as well as sending it to the user. Although often used concurrently with asymmetric encryption to solve the problem of securely transferring keys, symmetric encryption schemes remain an essential element of modern computer security (Konheim, 1981; Stinson, 2002; Trappe, 2005; Sinkov, 2009). Thanks to its speed, simplicity and security, symmetric encryption is frequently used in a wide range of applications, from securing internet traffic to protecting data stored on cloud servers.

Figure 1. Symmetric Encryption

After defining the symmetric encryption algorithms, we can specify the general features, advantages and disadvantages of these algorithms in the following:

Advantages of Symmetric Encryption Algorithms:

- Symmetric encryption is quite fast.
- They can work with hardware.

- They offer a high level of security while being fast and simple.
- Its keys are quite short and consist of simple mathematical operations.
- They can be used as intermediaries in the creation of stronger passwords.

Disadvantages of Symmetric Encryption Algorithms:

- Keys are difficult to store and deliver to parties and involve security risks.
- Large networks need too many switches, not scalable. A system with x users has $\lceil x(x-1)/2 \rceil$ keys.
- It does not provide integrity. The person who got the key may have changed the data.
- It does not provide authentication. Data can be encrypted by anyone with the same key.

Asymmetric Encryption

Asymmetric Encryption Algorithms are called public key cryptography. Unlike the symmetric encryption algorithm, there are two different keys in the asymmetric encryption algorithm, the public and private keys. The encryption key is called the public key, and the decryption key is called the private key. The key used for decryption is different from the keys used for encryption. For this reason, a text encrypted with a user's public key can only be decrypted with the private key of that user. In addition, in asymmetric encryptions, the person can send the text by first encrypting it with his private key and then with the public key of the other person. In this case, the user who receives the text opens the text with his private key and the sender's public key, both securely reaching the text and authenticating the sender of the text.

In the following example, person A encrypts the text with B's public key to send any text that only person B can see. Only person B can decrypt this text with his private key.

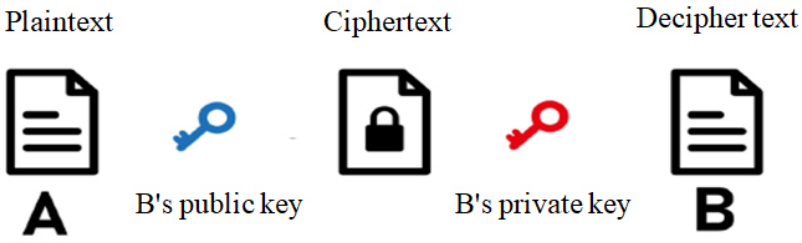

Figure 2. The first example of asymmetric encryption

In the following, we see the use of asymmetric encryption for authentication purposes.

Since person A can decrypt the ciphertext with B's public key, he understands that the text came from person B.

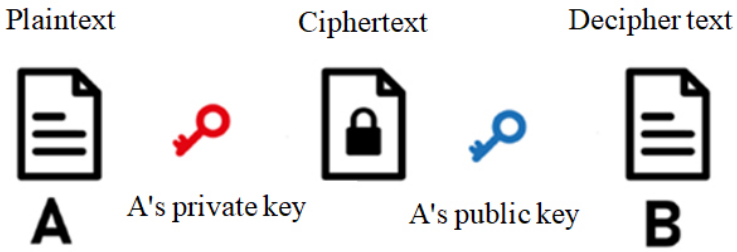

Figure 3. The second example of asymmetric encryption

In the below third example, person B could not decrypt the ciphertext of person C because he used A's public key. Because only C's public key can decrypt the text encrypted with C's private key.

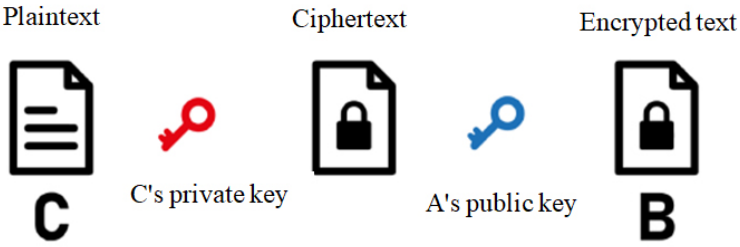

Figure 4. The third example of asymmetric encryption

After defining the asymmetric encryption algorithms, we can specify the general features, advantages and disadvantages of these algorithms in the following.

Advantages of Asymmetric Encryption Algorithms:

1. Passwords are relatively harder to crack.

2. Authentication is a secure way to enforce integrity and confidentiality principles.

3. Since two keys are used in encryption, it cannot be denied with a digital signature.

Disadvantages of Asymmetric Encryption Algorithms:

1. It is much slower than symmetric encryption.

2. It causes more CPU consumption in the system.

In the rest of the report, we will talk about the Hill Encryption algorithm, which is a symmetric encryption method.

Encryption of Hill Cryptography Algorithm

In this part, we present a method of encoding and decoding messages.

Before we start the encryption process, we need to define a square matrix that we will use as the key. Let's call the size of our matrix . We can adjust the size of the square matrix to whatever size we want $K=\left[k_{ij}\right]_n$.

In the second step, we will split the text we want to encrypt into n-length pieces $T=\left[t_{1j}\right]_n$. At this stage, we run into a problem: not every text can be divided into equal parts. Let's calculate the complexity by denoting the text length as M and the key matrix width as n. First, we're going to split our text into n chunks of length, so we'll have M/n chunks. M may not be exactly divisible by n, so we will add values to M as a multiple of n. Then, we can represent our piece count as $\lceil M/n \rceil$. In order to eliminate this problem, we can fill in the remaining gaps with a value that we have determined (Anton,2019).

Then we have to convert the parts of the text we want to encrypt into numbers. We can do this with the values $k, p \in Z$, we set ourselves, or with values in the ASCII Table (Stinson, 2002; Trappe, 2005; Sinkov, 2009).

Table 1. Alphabetic characters and ASCII values

A	B	C	D	E	F	G	H	I	J	K	L
k	k+1	k+2	k+3	k+4	k+5	k+6	k+7	k+8	k+9	k+10	k+11
65	66	67	68	69	70	71	72	73	74	75	76

M	N	O	P	Q	R	S	T	U	V	W
k+12	k+13	k+14	k+15	k+16	k+17	k+18	k+19	k+20	k+21	k+22
77	78	79	80	81	82	83	84	85	86	87

X	Y	Z	.	,	!	…	;	?
k+23	k+24	k+25	k+26	k+27	k+28	…	k+p-1	k+p
88	89	90	46	44	33	…	59	63

Then we will multiply each of these parts $T^{(m)}=\left[t_{1j}\right]_n$, $m=1,2,...,\lceil M/n \rceil$ with our key matrix $K=\left[k_{ij}\right]_n$, that is, we will do matrix multiplication $D^{(m)}=\left[d_{1j}\right]_n$;

$$D^{(m)}=T^{(m)}K, \qquad m=1,2,...,\lceil M/n \rceil$$

$$\left[d_{1j}\right]_n=\sum_{l=1}^{n} t_{1l}\,k_{lj}\,.$$

For each piece, we're going to do matrix multiplication, so we're going to multiply a n x 1 wide array by an n x n wide matrix. We can represent the number of operations here with 1 x n x n, that is, with n^2. If we were to repeat the matrix multiplication for each piece, we would have to perform $\lceil M/n \rceil n^2$ times. We can also denote the complexity as $M\,n$ if we accept M as a multiple of n (Anton,2019).

However, the multiplication results may not be within the range that we have determined for the number equivalents of the letters, so much larger numbers may come out. In order to eliminate this problem, we must take the mode of all the products we have obtained. Since we are using the English alphabet and some characters in Table 1, we have p characters, so we will take the mod of p;

$$D^{(m)} \equiv D^{(m')} \left(\text{mod } p\right),$$

$$d_{Ij} \equiv \left[d'_{Ij} \right]_n \left(mod\ p\right) .$$

Finally, we will add all the values we have obtained side by side in order and find out which letters the number values correspond to

$$D^{(1)} D^{(2)} \ldots D^{(\lceil M/n \rceil)}$$

Thus, we have encrypted the desired text as text characters $\lceil M/n \rceil n$ (Anton,2019).

For example, taking n as 2, we'll use any matrix $K = \left[k_{ij} \right]_2 = \left[i + j \right]_2$, $i, j = \{1, 2\}$,

$$K = \begin{bmatrix} 2 & 3 \\ 3 & 4 \end{bmatrix}. \qquad (1)$$

We want to encrypt the text "Turkish Youth! Your first duty is to preserve and to defend Turkish Independence and the Turkish Republic, forever.", since we take n as 2, only study a little part "Tu-rk-is-hY-ou-th-!" of the encrypt the text, the character "!" at the end remains single. In order to eliminate this problem, we will fill in the remaining gaps with a value that we have determined the end remains single. In our example, we can put the letter ! in the blanks.

"Tu-rk-is-hY-ou-th-!!"

Then we have to convert the parts of the text we want to encrypt into numbers. In our example, we will use the values that we determined ourselves for $k = 2$ and $p = 29$ in Table 1. So, the following table is established as

Table 2. The selected characters and values form Table 1

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
P	Q	R	S	T	U	V	W	X	Y	Z	.	,	!	
17	18	19	20	21	22	23	24	25	26	27	28	29	30	

We can do this with the values in Table 2.

Table 3. The vectors and plaintext

T u	r k	i s	h Y	o u	t h	! !
$[21 \quad 22]$	$[19 \quad 12]$	$[10 \quad 20]$	$[9 \quad 26]$	$[16 \quad 22]$	$[21 \quad 9]$	$[30 \quad 30]$

Then we will multiply each of these parts $T^{(m)} = \left[t_{1j}\right]_n$, $m = 1,2,...,7$ with the key matrix in (1). If the multiplication results may not be within the range that we have determined for the number equivalents of the letters, so much larger numbers may come out, then we must take the mod of 29 of all the products since we have obtained by using 29 characters in Table 2.

$$T^{(1)}K = [21 \quad 22]\begin{bmatrix} 2 & 3 \\ 3 & 4 \end{bmatrix} = [108 \quad 151] = D^{(1)}$$

$$[108 \quad 151] = [21 \quad 6](mod\ 29) \tag{2}$$

$$T^{(2)}K = [19 \quad 12]\begin{bmatrix} 2 & 3 \\ 3 & 4 \end{bmatrix} = [74 \quad 105] = D^{(2)}$$

$$[74 \quad 105] = [16 \quad 18](mod\ 29) \tag{3}$$

$$T^{(3)}K = [10 \quad 20]\begin{bmatrix} 2 & 3 \\ 3 & 4 \end{bmatrix} = [80 \quad 110] = D^{(3)}$$

$$[80 \quad 110] = [22 \quad 23](mod\ 29) \tag{4}$$

$$T^{(4)}K = [9 \quad 26]\begin{bmatrix} 2 & 3 \\ 3 & 4 \end{bmatrix} = [96 \quad 131] = D^{(4)}$$

$$[96 \quad 131] = [9 \quad 15](mod\ 29) \tag{5}$$

$$T^{(5)}K = [16 \quad 22]\begin{bmatrix} 2 & 3 \\ 3 & 4 \end{bmatrix} = [98 \quad 136] = D^{(5)}$$

$$[98 \quad 136] = [11 \quad 20](mod\ 29) \tag{6}$$

$$T^{(6)}K = [21 \quad 9]\begin{bmatrix} 2 & 3 \\ 3 & 4 \end{bmatrix} = [69 \quad 99] = D^{(6)}$$

$$[69 \quad 99] = [11 \quad 12](mod\ 29) \tag{7}$$

$$T^{(7)}K = [30 \quad 30]\begin{bmatrix} 2 & 3 \\ 3 & 4 \end{bmatrix} = [150 \quad 210] = D^{(7)}$$

$$[150 \quad 210] = [5 \quad 7](mod\ 29) \tag{8}$$

Finally, we consider all the values in (2)-(8), obtain side by side in order, and find out which letters the number values in the matrix $D^{(m')}$ correspond from Table 2.

Table 4. The vectors and ciphertext in Table 3

[21 6]	[16 18]	[22 23]	[9 15]	[11 20]	[11 12]	[5 7]
T E	O Q	U V	H N	J S	J K	D F

Thus, the word "Turkish Youth!" have been encrypted as "TEOQUVHNJSJKDF" in Table 4.

The Decryption of The Hill Cryptography Algorithm

Let's understand the logic of the decryption process: The decryption process also includes the same encryption steps, basically again matrix multiplication and mode calculation (Anton,2019; Bedasa, Bedada and Mulatu, 2020).

Let's denote the parts of the text we want to encrypt with $T^{(m)} = \left[t_{1j}\right]_n$, $m = 1,2,...,\lceil M/n \rceil$, the key matrix as $K = \left[k_{ij}\right]_n$, and the parts of the encrypted version with $D^{(m)} \equiv D^{(m')} \left(\mathrm{mod}\ p\right)$.

Accordingly, what we do, simply it can be shown as

$$D^{(m')} \equiv T^{(m)}\ K\ (mod\ p), \quad m = 1,2,...,\lceil M/n \rceil.$$

We know that the product of a matrix by its inverse is the unit matrix: $K\ K^{-1} = K^{-1}\ K = I$. According to this, we find that

$$D^{(m')}\ K^{-1} = T^{(m)}\ K\ K^{-1},$$

$$T^{(m)} \equiv D^{(m')} K^{-1} (mod\ p).$$

Here we understand that we need the inverse of the key matrix in order to decipher the encrypted text, we have to find the inverse of the key matrix, but not every matrix can be found. The condition for finding the inverse of the matrix is that the determinant of the matrix is nonzero. For this reason, we cannot use every matrix as a key.

First of all, we know that there are many methods to find the inverses of matrices whose determinant is nonzero. So, the determinant of our key matrix has to be non-zero, if $det(K) \neq 0$, then we have a matrix K^{-1}.

Methods such as adjugate matrix, the eigen decomposition, the Gaussian elimination and the Cholesky decomposition can be used to find the inverse of the matrix, we have studied the inverse of key matrix K with the adjugate matrix method;

$$K^{-1} = \frac{1}{det(K)} Adj(K) \tag{9}$$

where $det(K)$ is the determinant of K, $Adj(K)$ is the matrix transpose of cofactors. However, when we find the inverse in (9), the matrix elements can be fractional, which can cause calculation problems and miscalculations (Anton,2019).

For this reason, the inverse of the key matrix should be found with additional operations in the adjugate matrix method used for the Hill encryption algorithm. Firstly, in order to obtain integer values in the inverse matrix, we have to express the adjugate matrix method differently. We well know that $det(K) = 1 / det(K^{-1})$, an inverse matrix in (9) is

$$K^{-1} = det(K^{-1}) Adj(K) \tag{10}$$

In that case, we get the formula $det(K^{-1})$, we have to solve the following equation

$$det(K) det(K^{-1}) \equiv 1 (mod\ p). \tag{11}$$

The determinant of the key matrix and the mode value (for our example, the mode value 29) must be prime between them. Otherwise, incorrect results may be obtained during decoding. For this reason, the matrices that we can choose as keys are limited.

Finally, we found $det(K^{-1})$ If we multiply their values in (10) and take the mode of each value we find, we have found our inverse matrix

$$K^{-1} \equiv det(K^{-1}) Adj(K) (mod\ p) \tag{12}$$

Now we can perform the inverse matrix process for the matrix $K=\left[k_{ij}\right]_2=\left[i+j\right]_2$, $i,j=\{1,2\}$ given in (1). Firstly, this process follows the determinant and the adjugate matrix of the matrix K

$$det\left(K\right)=-1,\quad Adj\left(K\right)=\begin{bmatrix}4 & -3\\ -3 & 2\end{bmatrix}. \tag{13}$$

Next, we need to solve the equation given in (11), but, haven't need to calculate the value $det\left(K\right)=-1$, because its values are not fractional. Simply, this value can be written as

$$det\left(K^{-1}\right)\equiv -1\left(mod\ 29\right)\ \text{ or }\ det\left(K^{-1}\right)\equiv 28\left(mod\ 29\right).$$

Finally, the inverse expression in (12) is given as

$$K^{-1}\equiv\left(-1\right)\begin{bmatrix}4 & -3\\ -3 & 2\end{bmatrix}\left(mod\ 29\right)\ \text{ or }\ K^{-1}\equiv 28\begin{bmatrix}4 & -3\\ -3 & 2\end{bmatrix}\left(mod\ 29\right).$$

We calculated that

$$K^{-1}\equiv\begin{bmatrix}-4 & 3\\ 3 & -2\end{bmatrix}\left(mod\ 29\right)\ \text{ or }\ K^{-1}\equiv\begin{bmatrix}25 & 3\\ 3 & 27\end{bmatrix}\left(mod\ 29\right).$$

Now we can perform the decryption process. We'll split the ciphertext into 2-length chunks and find their numeric equivalents.

Table 5. The ciphertext and vectors in Table 4

T E	O Q	U V	H N	J S	J K	D F
$[21\quad 6]$	$[16\quad 18]$	$[22\quad 23]$	$[9\quad 15]$	$[11\quad 20]$	$[11\quad 12]$	$[5\quad 7]$

We will multiply each of the parts by the inverse of the key matrix and get the mode of each product.

$$D^{(1)}K^{-1}=\begin{bmatrix}21 & 6\end{bmatrix}\begin{bmatrix}-4 & 3\\ 3 & -2\end{bmatrix}=\begin{bmatrix}-66 & 51\end{bmatrix}=T^{(1)}$$

$$\begin{bmatrix}-66 & 51\end{bmatrix}\equiv\begin{bmatrix}21 & 22\end{bmatrix}\left(mod\ 29\right) \tag{14}$$

$$D^{(2)}K^{-1}=\begin{bmatrix}16 & 18\end{bmatrix}\begin{bmatrix}-4 & 3\\ 3 & -2\end{bmatrix}=\begin{bmatrix}-10 & 12\end{bmatrix}=T^{(2)}$$

$$\begin{bmatrix}-10 & 12\end{bmatrix}\equiv\begin{bmatrix}19 & 12\end{bmatrix}\left(mod\ 29\right) \tag{15}$$

$$D^{(3)}K^{-1}=\begin{bmatrix}22 & 23\end{bmatrix}\begin{bmatrix}-4 & 3\\ 3 & -2\end{bmatrix}=\begin{bmatrix}-19 & 20\end{bmatrix}=T^{(3)}$$

$$\begin{bmatrix}-19 & 20\end{bmatrix}\equiv\begin{bmatrix}10 & 20\end{bmatrix}(mod\ 29) \tag{16}$$

$$D^{(4)}K^{-1}=\begin{bmatrix}9 & 15\end{bmatrix}\begin{bmatrix}-4 & 3\\ 3 & -2\end{bmatrix}=\begin{bmatrix}9 & -3\end{bmatrix}=T^{(4)}$$

$$\begin{bmatrix}9 & -3\end{bmatrix}\equiv\begin{bmatrix}9 & 26\end{bmatrix}(mod\ 29) \tag{17}$$

$$D^{(5)}K^{-1}=\begin{bmatrix}11 & 20\end{bmatrix}\begin{bmatrix}-4 & 3\\ 3 & -2\end{bmatrix}=\begin{bmatrix}16 & -7\end{bmatrix}=T^{(5)}$$

$$\begin{bmatrix}16 & -7\end{bmatrix}\equiv\begin{bmatrix}16 & 22\end{bmatrix}(mod\ 29) \tag{18}$$

$$D^{(6)}K^{-1}=\begin{bmatrix}11 & 12\end{bmatrix}\begin{bmatrix}-4 & 3\\ 3 & -2\end{bmatrix}=\begin{bmatrix}-8 & 9\end{bmatrix}=T^{(6)}$$

$$\begin{bmatrix}-8 & 9\end{bmatrix}\equiv\begin{bmatrix}21 & 9\end{bmatrix}(mod\ 29) \tag{19}$$

$$D^{(7)}K^{-1}=\begin{bmatrix}5 & 7\end{bmatrix}\begin{bmatrix}-4 & 3\\ 3 & -2\end{bmatrix}=\begin{bmatrix}1 & 1\end{bmatrix}=T^{(7)}$$

$$\begin{bmatrix}1 & 1\end{bmatrix}\equiv\begin{bmatrix}30 & 30\end{bmatrix}(mod\ 29) \tag{20}$$

Finally, we will add all the values we have obtained side by side and find out which letters the number values correspond to.

Table 6. Decrypted text-vectors of ciphertext-vectors in Table 5

[21 22]	[19 12]	[10 20]	[9 26]	[16 22]	[21 9]	[30 30]
T U	R K	I S	H Y	O U	T H	! !

In Table 6, the word “TURKISHYOUTH!!” have been decrypted text “TEOQUVHNJSJKDF” in Table 5. Thus, we have regained the word “Turkish Youth!”. When the text we specify cannot be divided into equal parts by the width of the matrix, we add the text to the end of the text to meet the condition, for example, we encrypt the text “TURKISH YOUTH!” as “TURKISHYOUTH!!”. For some texts, this may cause misunderstandings for the recipient. For this reason, the algorithm is limited in terms of understanding.

Conclusion

Thanks to this study, information was obtained about encryption methods with matrices and how to decrypt the encrypted message. As explained in the above example, the system designed on encryption with matrices can be considered as a successful and reliable encryption method. Since one of the parameters that increase the reliability of the system

in such encryption systems is the use of any multidimensional key matrix, when long text encryption and decryption will be performed, the use of any key matrix of different sizes can be evaluated in terms of the security and speed of the system. A key matrix is required to decrypt an encrypted text. Key matrices can be found by performing crypto analysis with the help of any computer with detailed key search methods. Here, the size of the key matrix can be chosen high, so that the crypto analysis time can be long. However, using a multidimensional key matrix also causes delays in encryption and decryption processes. So it is clear that key matrix sizes are important in encryption.

References

Anton, H., Rorres, C. and Kaul, A. (2019) Elementary Linear Algebra Applications Version-Wiley.

Bedasa, M. F., Bedada, A. S. and Mulatu W. B. (2020) Data Encryption and Decryption by Using Hill Cipher Algorithm, Control Theory and Informatics, Vol.10, DOI: 10.7176/CTI/10-01.

Konheim, A. G. (1981). Cryptography, a Primer (New York: Wiley-Interscience.

Sinkov, A. (2009). Elementary Cryptanalysis, a Mathematical Approach (Mathematical Association of America.

Stinson D. R. (2002), Cryptography: Theory and Practice, 2nd Ed., Chapman & Hall/Crc, ISBN 1-58488-206-9.

Trappe, W. and Washington, L.C. (2005). Mathematics of Cryptography 17-51, Introduction to Cryptography: with Coding Theory, 2. Baskı, Pearson Prentice Hall, Washington, 577s.

About the Authors

Osman AKDAG is a Computer Teacher at Ahirli Sehit Samet Butun Secondary School in Konya, Turkey. He has a degree in Department of Computer Education and Instructional Technologies from Marmara University. His main areas of interest are robotic coding, educational content development and 3D design.

E-mail: fenosman@gmail.com, akdag-osman@hotmail.com, **Orcid:** 0000-0001-7705-972X

Fikri KOKEN is an Associate Professor of Computer Engineering at Necmettin Erbakan University in Konya, Turkey. He holds a Ph.D. from Mathematics Department at Selcuk University. His main areas of interest are Algebra and Number Theory, Matrix Theory and Applications.

E-mail: kokenfikri@gmail.com, fkoken@erbakan.edu.tr , **Orcid:** 0000-0002-8304-9525

Similarity Index

The similarity index obtained from the plagiarism software for this book chapter is %9.

To Cite This Chapter

Akdag, O. & Koken, F. (2022). On The Hill Cipher Algorithm From Encryption Algorithms, Y. Uzun. & R. Butuner (Eds.), *Current Studies in Artificial Intelligence, Virtual Reality and Augmented Reality* (pp. 120–134). ISRES Publishing.