Science Forum (Journal of Pure and Applied Sciences)

journal homepage: https://atbu.edu.ng/science-forum/

# Construction of cryptographic scheme of finite field using logical operators on rhotrices

Domven Lohcwat[1], Enoch Suleiman[2], Samaila Markus[3], Dauda Gulibur Yakubu[1]*

[1] *Department of Mathematical Sciences, Abubakar Tafawa Balewa University, Bauchi, Nigeria*
[2] *Department of Mathematics, Federal University Gashua, Yobe State, Nigeria*
[3] *Department of Mathematical Sciences, University of Maiduguri, Borno State, Nigeria*

## ABSTRACT

Cryptography is the study of mathematical techniques for information security. The security of information to maintain its confidentiality, integrity, and availability has become a major issue today. Since security is the main concern in data communication, encryption algorithm carries an important part of it. The art or science encompasses the principles and methods of transforming an intelligible message into unintelligible, and then retransforming the message back into its original form for more security. The sequence of numbers generated by a Linear Feed Back Shift Register or its XNOR counterpart is used especially in military cryptography. In this study, we encode and decode messages using rhotrices and logical operators on Galois finite field. The application of rhotrices in cryptographic systems using logical operators on Galois finite field prove to be one of the most secured and constructive method that prevent public or third parties from reading or getting access to data transmission over an insecure channel.

## ARTICLE INFO

***Artcle history:***
Received 20 April 2022
Received in revised form
14 November 2022
Accepted 14 November
2022 Published 05 July 2023
Available online 05 July 2023

## KEYWORDS

Finite field
Logical XNOR operator
Plain text
Cipher text
Key rhotrix
**AMS (2010) Mathematics Subject Classification:** 12E20, 03B35, 68U15.

## 1. Introduction

Finite field, named after Evariste Galois, refers to a field in which there exist finitely many elements. It is particularly useful in translating computer data as they are represented in binary forms. That is, computer data consists of a combination of two numbers 0 and 1, which are the components in Galois field whose number of elements are two {0,1}.

### *1.1. Finite fields*

Let $F$ be a non-empty set. Then $F$ is called a *Field* if F is an abelian group under addition and multiplication. If the number of elements in $F$ is finite then the field is finite. The positive integers are stored in computer as $n$-bit words where $n$ is usually $8,16,32,64,$ and so on. Therefore the range of integers is $0$ to $2^n-1$. The Galois field $GF(p)$ with set $Z_p$ where $P$ is the largest prime number less than $2^n$ whereas $GF(2^n)$ is a finite field having ($2^n$) elements. The elements in this field are $n$-bit words, see Hun and Yen (2003) and Hell and Johnson (2009).

### *1.2. Logical operators*

An XNOR gate is a digital logical gate that performs a logical operation on one or more logic inputs and produces a single logic output. Several researchers

* **Corresponding author** Dauda Gulibur Yakubu, ✉ dgyakubu@atbu.edu.ng ✉ Department of Mathematical Sciences, Abubakar Tafawa Balewa University, Bauchi, Nigeria.

© 2023 Faculty of Science, ATBU Bauchi. All rights reserved

used the application of logical XNOR operation in cryptography, for example, see Stakhov (2007). The sequence of numbers generated by a Linear Feed Back Shift Register or its XNOR counterpart is used especially in military cryptography. In this research, we use rhotrices and logical XNOR operations on Galois finite field $GF(2^n)$ for encryption and decryption of messages.

Note: The finite field $GF(2^3)$ has 8 elements which are $\{0,1,g,g^2,g^3,g^4,g^5,g^6\}$ using the irreducible polynomial $f(x) = X^3+X+1$, which means that $g^3 + g + 1 = 0$ or $g^3 = g + 1$. Other powers of $g$ can be calculated accordingly. The following shows good examples of some values of $g$:

| | |
|---|---|
| 0 | 000 |
| 1 | 001 |
| $g$ | 010 |
| $g^2$ | 100 |
| $g^3 = g + 1$ | 011 |
| $g^4 = g^2 + g$ | 110 |
| $g^5 = g^3 + g + 1$ | 111 |
| $g^6 = g^2 + 1$ | 101 |

Representing data as a vector in a Galois field allows mathematical operations to scramble data easily and effectively. Cryptography is the art and science encompassing the principles and methods of transforming an intelligible message (plaintext) into one that is unintelligible (cipher text) and then retransforming the message back to its original form. In modern times, cryptography is considered to be a branch of both mathematics and computer science, and is affiliated closely with information theory, computer security, and engineering. Although in the past, cryptography referred only to the encryption and decryption of messages using secret keys. Nowadays, cryptography generally being classified into two categories namely: the symmetric and the asymmetric. Conventional encryption is referred to as symmetric encryption or single key encryption. The Hill cipher algorithm in Galois field $GF(2^m)$ using polynomial is one of the symmetric key algorithms that have several advantages in data encryption. Galois field is used for one of the error-detecting code. But the inverse of the key matrix used for decryption of the cipher text does not always exist. If the key matrix is not invertible, then encrypted text cannot be decrypted. In the self-invertible matrix generation method, the key matrix used for the encryption is self-invertible. So at the time of decryption we need not to find the inverse of the key matrix.

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process the data. The word cryptography is derived from the Greek *kryptos*, meaning hidden. The origin of cryptographic system is dated back to 2000 BC, see Biggs (2008) with the Egyptian practice of hieroglyphics. These consisted of complex pictograms, the full meaning of which was only known to the elite who were very few by then. Egyptian practice of hieroglyphics, includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit.

The first known use of a modern cipher was by Julius Caesar (100 BC to 44 BC) who did not trust his messengers when communicating with his governors and officers, see Biggs (2008). For this reason, he created a system in which each character in his messages was replaced by a character three positions ahead of it in the Roman alphabet.

Modern cryptography is defined as the science of transforming communications so that only the intended recipient can understand them. Certain aspects of cryptography are indeed quite mathematical in nature, though it is also used to protect information in computing systems. It is closely related to the disciplines of cryptology and cryptanalysis. It is used everywhere and by billions of people worldwide on a daily basis, to protect data at rest and data in motion. Cryptographic systems are integral part of standard protocols, most notably the Transport Layer Security protocol, making it relatively easy to incorporate strong encryption into a wide range of applications, Dan and Shou (2015). However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as clear text) into cipher text (a process called encryption), then back again (known as decryption).

In recent times, cryptography has been used by the world's best mathematicians and computer scientists, for example, see Hill (1929, 1931) and the references therein. Because governments do not wish certain entities in and out of their countries to have access to ways to receive and send hidden information that may be a threat to national interests, cryptography has been subject to various restrictions in many countries, ranging from limitations of the usage and export of software to the public dissemination of mathematical concepts that could be used to develop cryptosystems.

However, the internet has allowed the spread of powerful programs and, more importantly, the underlying techniques of cryptography, so that today many of the most advanced cryptosystems and ideas are now in the public domain.

Sharma and Rehan (2013) modified the Hill cipher cryptography which is a symmetric key substitution algorithm, and is vulnerable to known plaintext attack. The presented paper provides two fold securities to the existing Hill cipher by using the elements of finite fields and logical operators. Two different keys were used in the proposed algorithm. The first key is taken as a non-singular matrix and the second key is obtained with the help of elements of finite fields. The elements of finite fields were used in binary and polynomial form during encryption and decryption of the message. In the paper, they provided an algorithm that is very difficult to alter. The sender and the receiver shares the secret key $K_1$, where $K_1$ is $(n-1)$-by- $(n-1)$ non-singular matrix and $n$ is a positive integer. The sender then converts the plaintext into pre-assigned numerical values and calculates $S_1 = K_1 P \ mod\ (2n-1)$; $S_1$ is the first cipher text, $P$ is the plain text. Then the sender converts $S_1$ into binary string of $n$-bits which gives the matrix $M$ in their paper and chooses a random matrix $A$ of order $(n-1)$ -by- $(n-1)$. The sender performs $XNOR$ operations with randomly selected rows/columns of $A$ with each row of matrix $M$ and gets a matrix $MXNOR$. According to the authors, the sender converts the entries of $MXNOR$ into the elements of $GF(2^n)$ and multiplies each entry with $g^n$ and calculates $K_2$, whose entries is 1 if $g$ has the power greater than $\left(2^n-1\right)$ otherwise $0$ and shares it with the receiver of the message. The receiver then reduces the powers of the entries to $mod\ \left(2^n-1\right)$ and gets the matrix $M_4$. After writing it into binary form, the receiver converts the same in numerical values and then into text to get the final cipher text $S_2$. This method of enciphering and deciphering is very complicated and difficult to alter or break.

Lakshmi et al. (2011) studied cryptographic methods of sending messages in disguised form so that only the intended recipients can remove the disguise and read the massage. According to the authors with widespread availability of computer technology, the rapid growth of wireless communications secured exchange of information has become a challenging task. The most basic of the modules in modern cryptography is that of a primitive, which may be regarded as a cryptographic building block which performs one or more desired functions, and may be combined with others to form a cryptographic protocol. They went on to say that the most well-known and perhaps the simplest primitive of encryption, which allows parties to achieve confidential data transmission over an insecure channel is by encrypting information. In the same paper, they proposed a cryptographic technique using elements of a finite field and logical operators based on the inverse property. To test the efficacy of the proposed scheme the cryptanalysis was performed, which they found to be better than most of the encryption techniques in the literature.

Yakubu et al. (2018, 2022) introduced some methods of storing and transmitting data in a particular form so that only those for whom it is intended can read and process the data using rhotrices. The new method of sending secret messages which is very difficult to alter or break either in motion or at rest was proved to be one of the best methods of sending secret information in the present computer age. The use of rhotrix to encode and decode messages which were respectively called the encoding rhotrix and decoding rhotrix plays very important role in cryptography. Applications of rhotrices to polyalphabetic cipher systems proved to be one of the most secured and constructive method of analyzing protocols, prevent public or third parties called adversaries from reading or hearing the message.

It is the goal of this note to convey a new secured and practical application of rhotrices in cryptographic system using logical operators on Galois finite field to send secret message to a receiver without being altered by an adversary.

## 2. Basic Properties of Rhotrix

The algebra and analysis of rhotrix have been studied by many authors in the past few years in the field of mathematics and computer science where researchers show interest in the theory and analysis of rhotrix properties. Ajibade (2003) introduced the concept of rhotrix as mathematical arrays that are in some ways between two-by-two-dimensional matrices and three-by-three dimensional matrices. Ajibade's work was an extension of ideas discussed in a paper by Atanassov and Shannon (1998). He based his work on three-dimensional rhotrix and established the relationships between rhotrices and their hearts, and also the relationship between rhotrices and matrices. The dimension of rhotrices according to Ajibade can be increase in size retaining all its properties, that is, the operations of addition (+) and multiplication ($\circ$) on rhotrices, identity element, inverse of a rhotrix and spanning/linear combination of rhotrices. Ajibade defined the object by $R$ and refer to as a rhotrix due to the rhomboidal nature of its entries and is given by

$$R = \left\{ \left\langle \begin{matrix} & a & \\ b & & d \\ & e & \end{matrix} \right\rangle : a,b,c,d,e \in \Re \right\}, \qquad (1)$$

where $\Re$ is the set of real numbers. The initial algebra and analysis of rhotrices were presented by using only two-by-two-dimensional matrices and three-by-three-dimensional matrices. The author suggested and defined the heart of the rhotrix $R$ by $h(R)$ and designated as,

$$R = \left\langle \begin{matrix} & a & \\ b & h(R) & d \\ & e & \end{matrix} \right\rangle. \quad (2)$$

Addition (+) and multiplication ($\circ$) of two rhotrices can easily be performed in a similar manner like that of matrices. According to Ajibade (2003), extension is possible in various ways.

Sani (2004) proposed an alternative method of multiplication of rhotrices. The author suggested that, since rhotrices lie somewhere between two-by-two and three-by-three dimension matrices, multiplication of rhotrix can also be defined similar to matrix multiplication, where the row-column multiplication method of matrices can be used except for the hearts which are multiplied directly. The definition of rhotrix determinant and transpose showed that all the properties of determinants and transpose for matrices are applicable (holds) on rhotrices. He also showed that there is an isomorphism between invertible rhotrices and invertible matrices. The row-column multiplication method as an alternative multiplication for rhotrices has the advantages of relating rhotrices to two-by-two matrices through an isomorphism. Sani (2007) presented a method of row-column multiplication of rhotrices of higher dimension. This was an extension of his earlier work on row-column multiplication for base level rhotrices of dimension three. He showed that using row-column multiplication, one obtains a direct relationship between invertible rhotrices of dimension *n* and invertible $t-by-t$ matrices where $t=(n+1)/2$ using an isomorphism between the two groups. Such relationship exists between invertible *n*-dimensional rhotrices and invertible $(t-1)$-by-$(t-1)$ matrices. Based on the idea of the isomorphic theory he came up with the following group theorem:

**Theorem 1:** Sani (2007) *The group of all invertible n-dimensional rhotrices is isomorphic to the group of t×t real non-singular matrices where* $t=(n+1)/2$.

A generalization of the row-column multiplication for n-dimensional rhotrices is also possible. That is, given n-dimensional rhotrices $R_n=\langle a_{ij}, c_{lk}\rangle$ and $Q_n=\langle b_{ij}, d_{lk}\rangle$ the multiplication of $R_n$ and $Q_n$ is defined as follows:

$$R_n \circ Q_n = \langle a_{i_1 j_1}, c_{l_1 k_1}\rangle \circ \langle b_{i_2 j_2}, d_{l_2 k_2}\rangle = \left\langle \sum_{i_2 j_1=1}^{t} (a_{i_1 j_1} b_{i_2 j_2}), \sum_{l_2 k_1=1}^{t-1} (c_{l_1 k_1} d_{l_2 k_2}) \right\rangle, \; t=(n+1)/2. \quad (3)$$

Rhotrix vectors (either row vectors or column vectors) can be represented in *t* different ways where $t=(n+1)/2$. This is different compared to vectors in matrices that can be represented in a unique way. The method of converting a rhotrix to a special matrix called "coupled matrix" was also suggested by Sani (2008). This idea can be used to solve systems of $n\times n$ and $(n-1)\times(n-1)$ matrix problems simultaneously. In general, we have

$$R_n^{T/2} = \langle a_{ij}, c_{lk}\rangle^{T/2} = \left[ a_{ij}, c_{lk} \right] = \left[ Ac \right]_n, \quad (4)$$

which is a coupled matrix, coupling a $t\times t$ matrix with a $(t-1)\times(t-1)$ matrix, where $t=(n+1)/2$.

**Theorem 2:** Sani (2008) *if a coupled matrix* $\left[Ac\right]_n$ *is completed with zeros, then its determinant is the product of the determinants of the matrices* $\left[A\right]_{t\times t}$ *and* $\left[c\right]_{(t-1)\times(t-1)}$ *where* $t=(n+1)/2$.

**Theorem 3:** *Freshman's Dream Theorem (Fraleigh, 1993, Julio 1984). For every prime P and every positive integer n, there exists a finite field F with* $P^n$ *elements. Furthermore, any field of order* $P^n$ *is isomorphic to the splitting field* $x^{P^n}-x$ *over* $Z_p$.

**Table 1.** Numerical values for the English Alphabet letters and some symbols.

| | A | B | C | D | E | F | G |
|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| H | I | J | K | L | M | N | O |
| 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| P | Q | R | S | T | U | V | W |
| 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |
| X | Y | Z | [ | \ | ] | ^ | @ |
| 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |

**Theorem 4:** *The inverse of a given rhotrix say K is unique* (Yakubu et al., 2022).

## 3. Enciphering and Deciphering of Secret Messages

Modern cryptography is heavily based on mathematical theory and computer science practice. Cryptographic algorithms are designed around the computational hardness assumptions, making such algorithms hard to break in practice by an adversary. These schemes are therefore termed computationally secured and theoretically advances, for example encryption using rhotrices instead of matrices. The encoding rhotrices probably cannot be broken even with unlimited computing power but these schemes are more difficult to implement than the best theoretical breakable but computationally secured mechanisms. Here we illustrate the application of rhotrices with finite field of cryptographic method of encoding and decoding secret messages using logical operators.

### *3.1. Illustration*

We shall now consider some messages to be sent on the insecure channel for illustration purposes.

Example 1. Use the rhotrix $R_5$ below, to construct a cipher text for the plain text "AGE."

$$R_5 = \left\langle \begin{array}{ccccc} & & 6 & & \\ & 5 & 1 & 1 & \\ 4 & 3 & 3 & 0 & 3 \\ & 2 & 7 & 5 & \\ & & 1 & & \end{array} \right\rangle.$$

Solution. We convert the plain text AGE into numerical values and write it in 4-bit binary string as:

$$M_1 = \left\langle \begin{array}{ccccc} & & 0001 & & \\ & 0000 & 0000 & 0111 & \\ 0000 & 0000 & 0000 & 0000 & 0101 \\ & 0000 & 0000 & 0000 & \\ & & 0000 & & \end{array} \right\rangle.$$

We select all the columns from the rhotrix $R_5$ and convert them to 4-bit binary numbers and perform logical XNOR operation with each row of the rhotix $M_1$ to obtain $M_{XNOR}$ as follows:

$$M_{XNOR} = \left\langle \begin{array}{ccccc} & & 1000 & & \\ & 1110 & 1111 & 1101 & \\ 1100 & 1111 & 1100 & 1100 & 11110 \\ & 1010 & 1000 & 1101 & \\ & & 1110 & & \end{array} \right\rangle.$$

We convert the above entries into elements of $GF\left(2^4\right)$ in their basis form such that $g^4 + g + 1 = 0$, or $g^4 = g + 1$ and so on so that we have:

$$M_2 = \left\langle \begin{array}{ccccc} & & g^3 & & \\ & g^{11} & g^{11} & g^{13} & \\ g^6 & g^{12} & g^6 & g^6 & g^{11} \\ & g^9 & g^3 & g^{13} & \\ & & g^{11} & & \end{array} \right\rangle.$$

Now multiply $M_2$ by $g^4$ to get:

$$M_3 = \left\langle \begin{array}{ccccc} & & g^7 & & \\ & g^{15} & g^{15} & g^{17} & \\ g^{10} & g^{16} & g^{10} & g^{10} & g^{15} \\ & g^{13} & g^7 & g^{17} & \\ & & g^{15} & & \end{array} \right\rangle.$$

$M_3$ is reduced to mod 15 giving $M_4$ as

$$M_4 = \left\langle \begin{array}{ccccc} & & g^7 & & \\ & g^0 & g^0 & g^2 & \\ g^{10} & g^1 & g^{10} & g^{10} & g^0 \\ & g^{13} & g^7 & g^2 & \\ & & g^0 & & \end{array} \right\rangle.$$

We find $K_0$ such that if power of g in $M_3$ is less than 15, the entry in the key is taken as 0 or 1 otherwise.

$$K_0 = \left\langle \begin{array}{ccccc} & & 0 & & \\ & 0 & 0 & 1 & \\ 0 & 1 & 0 & 0 & 0 \\ & 0 & 0 & 1 & \\ & & 0 & & \end{array} \right\rangle.$$

$M_4$ is converted to 4-bit binary elements which gives $C_5$ as

$$C_5 = \left\langle \begin{array}{ccccc} & & 1011 & & \\ & 0001 & 0001 & 0100 & \\ 0111 & 0010 & 0111 & 0111 & 0001 \\ & 1101 & 1011 & 0100 & \\ & & 0001 & & \end{array} \right\rangle.$$

Now all the binary elements of the rhotrix $C_5$ are coded to the text characters using ASCII code which is called the first cipher text **KDAAGAGDBKGMA.**

The cipher text **KDAAGAGDBKGMA** is sent to the receiver through the public channel.

Example 2. The message **KDAAGAGDBKGMA** is converted to text character into 4-bit string using ASCII code and write this in form of a $5\times5$ rhotrix.

$$C_5 = \left\langle \begin{array}{ccccc} & & 1011 & & \\ & 0001 & 0001 & 0100 & \\ 0111 & 0010 & 0111 & 0111 & 0001 \\ & 1101 & 1011 & 0100 & \\ & & 0001 & & \end{array} \right\rangle.$$

Decrypt the message **KDAAGAGDBKGMA** encrypted in example 1 above.

Solution. Now convert the above 4-bit binary elements into element of $GF\left(2^4\right)$ to get $D_1$ as,

$$D_1 = \left\langle \begin{array}{ccccc} & & g^7 & & \\ & g^0 & g^0 & g^2 & \\ g^{10} & g^1 & g^{10} & g^{10} & g^0 \\ & g^{13} & g^7 & g^2 & \\ & & g^0 & & \end{array} \right\rangle$$

We then multiply the key by $15$ and on adding $D_1$ we get

$$D_2 = K_0 + D_1 = \left\langle \begin{array}{ccccc} & & g^7 & & \\ & g^{15} & g^{15} & g^{17} & \\ g^{10} & g^{16} & g^{10} & g^{10} & g^{15} \\ & g^{13} & g^7 & g^{17} & \\ & & g^{15} & & \end{array} \right\rangle.$$

Multiply $D_2$ by $g^{-4}$ to get

$$D_3 = g^{-4}\times D_2 = \left\langle \begin{array}{ccccc} & & g^3 & & \\ & g^{11} & g^{11} & g^{13} & \\ g^6 & g^{12} & g^6 & g^6 & g^{11} \\ & g^9 & g^3 & g^{13} & \\ & & g^{11} & & \end{array} \right\rangle.$$

We now convert the above entries into 4-bit binary elements to get

$$D_4 = \left\langle \begin{array}{ccccc} & & 1000 & & \\ & 1110 & 1110 & 1101 & \\ 1100 & 1111 & 1100 & 1100 & 1110 \\ & 1010 & 1000 & 1101 & \\ & & 1110 & & \end{array} \right\rangle.$$

We recall that all the columns from the rhotrix $R_5$ and perform logical XNOR operation between each rows of $D_4$ to obtain $M_1$.

Thus,

$$M_1 = \left\langle \begin{array}{ccccc} & & 0001 & & \\ & 0000 & 0000 & 0111 & \\ 0000 & 0000 & 0000 & 0000 & 0101 \\ & 0000 & 0000 & 0000 & \\ & & 0000 & & \end{array} \right\rangle.$$

All the elements of the rhotrix $M_1$ which are in 4-bit binary elements are converted to the text characters using the ASCII code to get the original message "AGE."

Example 3. Use the rhotrix $R_7$ below to construct a cipher text for the plain text "ATBU."

$$R_7 = \left\langle \begin{array}{ccccccc} & & & 3 & & & \\ & & 2 & 5 & 4 & & \\ & 5 & 1 & 3 & 6 & 2 & \\ 2 & 4 & 7 & 8 & 3 & 3 & 7 \\ & 3 & 1 & 3 & 5 & 2 & \\ & & 2 & 2 & 9 & & \\ & & & 3 & & & \end{array} \right\rangle.$$

Solution. We now convert the plain text ATBU into numerical values and write it into 5-bit binary string as;

$$M_1 = \left\langle \begin{array}{ccccccc} & & & 00001 & & & \\ & & 00000 & 00000 & 10100 & & \\ & 00000 & 00000 & 00000 & 00000 & 00010 & \\ 00000 & 00000 & 00000 & 00000 & 00000 & 00000 & 10101 \\ & 00000 & 00000 & 00000 & 00000 & & \\ & & 00000 & 00000 & & & \\ & & & 00000 & & & \end{array} \right\rangle.$$

We select all the columns from $R_7$ and convert them to 5-bit binary numbers and perform the logical XNOR operation with each of them using each row of the rhotrix $M_1$, to obtain $M_{XNOR}$ as follows,

$$M_{XNOR} = \left\langle \begin{array}{ccccccc} & & & 11101 & & & \\ & & 11011 & 11010 & 01001 & & \\ & 11101 & 11001 & 11100 & 11110 & 11000 & \\ 11000 & 11100 & 11100 & 10111 & 11000 & 11011 & 01000 \\ & 11101 & 11000 & 11100 & 11110 & 11100 & \\ & & 10110 & 11101 & 11101 & & \\ & & & 11100 & & & \end{array} \right\rangle.$$

We now convert the above entries into elements of $GF\left(2^5\right)$ in their basis form such that $(g^5 + g^2 + 1) = 0$, or $g^5 = g^2 + 1$ and we get

$$M_2 = \left\langle \begin{array}{ccccccc} & & & g^{14} & & & \\ & & g^{16} & g^{9} & g^{29} & & \\ & g^{14} & g^{25} & g^{13} & g^{24} & g^{21} & \\ g^{21} & g^{13} & g^{13} & g^{26} & g^{21} & g^{16} & g^{3} \\ & g^{14} & g^{21} & g^{13} & g^{24} & g^{13} & \\ & & g^{28} & g^{14} & g^{14} & & \\ & & & g^{13} & & & \end{array} \right\rangle.$$

Now multiply $M_2$ by $g^5$ to get:

$$M_3 = \left\langle \begin{array}{ccccccc} & & & g^{19} & & & \\ & & g^{21} & g^{14} & g^{34} & & \\ & g^{19} & g^{30} & g^{18} & g^{29} & g^{26} & \\ g^{26} & g^{18} & g^{18} & g^{31} & g^{26} & g^{21} & g^{8} \\ & g^{19} & g^{26} & g^{18} & g^{29} & g^{18} & \\ & & g^{31} & g^{19} & g^{19} & & \\ & & & g^{18} & & & \end{array} \right\rangle.$$

$M_3$ is reduced to mod $31$ giving $M_4$ as follows:

$$M_4 = \left\langle \begin{array}{ccccccc} & & & g^{19} & & & \\ & & g^{21} & g^{14} & g^{3} & & \\ & g^{19} & g^{30} & g^{18} & g^{29} & g^{26} & \\ g^{26} & g^{18} & g^{18} & g^{0} & g^{26} & g^{21} & g^{8} \\ & g^{19} & g^{26} & g^{18} & g^{29} & g^{18} & \\ & & g^{0} & g^{19} & g^{19} & & \\ & & & g^{18} & & & \end{array} \right\rangle.$$

We choose $K_0$ so that if power of g in $M_3$ is less than $31$, the entry in the key rhotrix is taken as 0 or otherwise 1, that is, if power of $g$ exceed $31$.

$$K_0 = \left\langle \begin{array}{ccccccc} & & & 0 & & & \\ & & 0 & 0 & 1 & & \\ & 0 & 0 & 0 & 0 & 0 & \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ & 0 & 0 & 0 & 0 & 0 & \\ & & 0 & 0 & 0 & & \\ & & & 0 & & & \end{array} \right\rangle.$$

$M_4$ is converted to $5$-bit binary elements giving $C_7$ as

$$C_7 = \left\langle \begin{array}{ccccccc} & & & 00110 & & & \\ & & 11000 & 11101 & 01000 & & \\ & 00110 & 10010 & 00011 & 01001 & 10111 & \\ 10111 & 00011 & 00011 & 00001 & 10111 & 11000 & 01101 \\ & 00110 & 10111 & 00011 & 01001 & 00011 & \\ & & 00001 & 00110 & 00110 & & \\ & & & 00011 & & & \end{array} \right\rangle.$$

Thus, all the binary elements of the rhotrix $C_7$ are coded to the text characters using ASCII code which can be called the first cipher text **FHWM] IXXCWCRAIFCCFCWFWFAC**. This cipher text is sent to the receiver through the public channel.

Example 4. The message **FHWM] IXXCWCRAIFCCFCWFWFAC** is converted to text character into 5-bit string using ASCII code and write this in form of a $7 \times 7$ rhotrix.

$$C_7 = \left\langle \begin{array}{ccccccc} & & & 00110 & & & \\ & & 11000 & 11101 & 01000 & & \\ & 00110 & 10010 & 00011 & 01001 & 10111 & \\ 10111 & 00011 & 00011 & 00001 & 10111 & 11000 & 01101 \\ & 00110 & 10111 & 00011 & 01001 & 00011 & \\ & & 00001 & 00110 & 00110 & & \\ & & & 00011 & & & \end{array} \right\rangle.$$

Decrypt the message and transform it back to its original form.

**Solution**. We convert the above 5-bit binary elements to $GF\left(2^5\right)$

$$D_1 = \left\langle \begin{array}{ccccccc} & & & g^{19} & & & \\ & & g^{21} & g^{14} & g^{3} & & \\ & g^{19} & g^{30} & g^{18} & g^{29} & g^{26} & \\ g^{26} & g^{18} & g^{18} & g^{0} & g^{26} & g^{21} & g^{8} \\ & g^{19} & g^{26} & g^{18} & g^{29} & g^{18} & \\ & & g^{0} & g^{19} & g^{19} & & \\ & & & g^{18} & & & \end{array} \right\rangle.$$

Multiply the key with $31$ and on adding $D_1$ we get

$$D_2 = K + D_1 = \left\langle \begin{array}{ccccccc} & & & g^{19} & & & \\ & & g^{21} & g^{14} & g^{34} & & \\ & g^{19} & g^{30} & g^{18} & g^{29} & g^{26} & \\ g^{26} & g^{18} & g^{18} & g^{31} & g^{26} & g^{21} & g^{8} \\ & g^{19} & g^{26} & g^{18} & g^{29} & g^{18} & \\ & & g^{31} & g^{19} & g^{19} & & \\ & & & g^{18} & & & \end{array} \right\rangle.$$

We multiply $D_2$ by $g^{-5}$ to get

$$D_3 = g^{-5} \times D_2 = \left\langle \begin{array}{ccccccc} & & & g^{14} & & & \\ & & g^{16} & g^{9} & g^{29} & & \\ & g^{14} & g^{25} & g^{13} & g^{24} & g^{21} & \\ g^{21} & g^{13} & g^{13} & g^{26} & g^{21} & g^{16} & g^{3} \\ & g^{14} & g^{21} & g^{13} & g^{24} & g^{13} & \\ & & g^{28} & g^{14} & g^{14} & & \\ & & & g^{13} & & & \end{array} \right\rangle.$$

We then convert the above entries into 5-bit binary elements as follows: -

$$D_4 = \left\langle \begin{array}{ccccccc} & & & 11101 & & & \\ & & 11011 & 11010 & 01001 & & \\ & 11101 & 11001 & 11100 & 11110 & 11000 & \\ 11000 & 11100 & 11100 & 10111 & 11000 & 11011 & 01000 \\ & 11101 & 11000 & 11100 & 11110 & 11100 & \\ & & 10110 & 11101 & 11101 & & \\ & & & 11100 & & & \end{array} \right\rangle.$$

Recall all the columns from the rhotix $R_7$ and convert them to 5-bit binary elements and then perform a logical XNOR operation with $D_4$ to get $M_1$. Thus,

$$M_1 = \left\langle \begin{array}{ccccccc} & & & 00001 & & & \\ & & 00000 & 00000 & 10100 & & \\ & 00000 & 00000 & 00000 & 00000 & 00010 & \\ 00000 & 00000 & 00000 & 00000 & 00000 & 00000 & 10101 \\ & 00000 & 00000 & 00000 & 00000 & 00000 & \\ & & 00000 & 00000 & 00000 & & \\ & & & 00000 & & & \end{array} \right\rangle$$

All the elements of the rhotrix $M_1$ which are in 5-bit binary are converted to the text characters using ASCII code in Table 1 to get the original message "ATBU."

## 4. Conclusion

The new feature considered in this paper is the use of logical XNOR operation on Galois finite field, using rhotrices which extends some conventional methods of encryptions. We use the method of constructing practical cryptography of polyalphabetic cipher systems for which we can argue security under plausible assumptions in the research. In the construction systems we ensure both data secrecy (confidentiality) and data integrity, even against very aggressive attackers that can interact with the sender and receiver quite maliciously and arbitrarily. Such systems are said to provide authenticated encryption security or are simply said to be AE-secure. We presented many real-world settings where undetected cipher text tampering comprises both message secrecy and message integrity. This approach can reduce cipher text size and also improve security of the message to be transmitted to the intended receiver. We finally conclude by saying that to the best of our knowledge, this is the first time rhotrices are applied on Galois finite field $GF\left(2^n\right)$ using logical XNOR operation. Hence,

this research opens several possibilities for further investigation.

## References


Ajibade AO. The concept of rhotrix in mathematical enrichment. Int J Math Educ Sci Technol 2003; 34:175–9.

Atanassov KT, Shannon AG. Matrix-tertions and matrix noitrets: exercises in mathematical enrichment. Int J Math Educ Sci Technol 1998; 29:898–903.

Biggs N. An introduction to information communication and cryptography. Springer, 171 p, 2008.

Hun CC, Yen JC. A new cryptography systems and its VISI realization. J Syst Arch 2003; 49:355–67.

Dan B, Shou V. A graduate course in applied cryptography. Autoedición, pp 7–23, 2015.

Fraleigh JB. A first course in abstract algebra. Addison-Wesley Publishing Company, 453 p, 1993.

Hell M, Johnson T. Breaking the strem ciphers F-FCSR-H and F-FCSR-16 in real time. J Cryptol 2011; 24:427–45.

Hill LS. Cryptography in an algebraic alphabet. Am Math Mon 1929; 36(6):306–12.

Hill LS. Concerning certain linear transformation apparatus of cryptography. Am Math Mon 1931; 38(3):135–54.

Julio RB. Field extension and Galois theory. Addison-Wesley Publishing Company, 1984.

Lakshmi GN, Kumar BR, Suneetha C, Sekhar AC. A cryptographic scheme of finite fields using logical operators. Intern J Comput Applic 2011; 31(4):1–4.

Sani B. An alternative method for multiplication of rhotrices. Int J Math Educ Sci Technol 2004: 35:777–81.

Sani B. The row-column multiplication for high dimensional rhotrices. Int J Math Educ Sci Technol 2007; 38:657–62.

Sani B. Conversion of a rhotrix to a coupled matrix. Int J Math Educ Sci Technol 2008; 39:244–9.

Sharma PL, Rehan M. On security of Hill cipher using finite fields. Inter J Compu Applic 2013; 71(4):30–3.

Stakhov AP. The golden matrices and a new kind of Cryptography. Chaos Solit Fractals 2007; 32:1138–46.

Yakubu DG, Mathias LB, Lucy BG, Lohcwat D. Extension of Affine Hill cipher using rhotrices in the polyalphabetic cipher systems 2018. Abacus J Math Asso Niger 2018; 45(1):273–84.

Yakubu DG, Mathias LB, Lucy BG, Lohcwat D. A secured cryptographic technique using rhotrices in polygraphic cipher systems. Sci Forum J Pure Appl Sci 2022; 22(1):35–42.