American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-6, Issue-6, pp-212-217
www.ajer.org
Research Paper Open Access

Encrypt and Decrypt Messages Using Invertible Matrices Modulo 27.

Abdulaziz B.M.Hamed[1,3] and Ibrahim O.A. Albudawe[2,3]

([1] *Department of Mathematics and Statistics,Faculty of Science, Yobe State University Damaturu, Nigeria)*
([2]*Department of Mathematics, Faculty of Sciences , Aljouf University, Saudi Arabia)*
([3]*Department of Mathematics, Faculty of Education, West Kordofan University Elnohud, Sudan)*

ABSTRACT: *The study addressed the problem of cryptographic messages using invertible matrices (modulo 27) instate of Hill Cipher method. The messages has been encrypted and decrypted perfectly using secret key matrices along with congruence modulo, relative prime and inverse multiplication (modulo27) relations corresponding to English alphabetic letter + space. The numeric negative integer equivalents of English capital Letters has been generated .*
Keyword: *Cryptography, Congruence, Decrypt, Encrypt, Invertible matrices, Multiplication.*

I. INTRODUCTION

Cryptology is defined as the science of making communication incomprehensible to all people except those who have right to read and understand it[1]. Also defines cryptography as the study of mathematical techniques related to aspect of information security such as confidentiality, data integrity, entry authentication and data origin authentication [7,8].

Cryptography, the art of encryption and decryption , plays a major part in cellular communications, such as e-commerce, computer password, pay- TV, sending emails, ATM card, security, transmitting funds, and digital signatures. Nowadays, cryptography is considered as a branch of computer science as well as mathematics. At present time cryptography is usually classified into two major categories, symmetric and asymmetric. In symmetric cryptography , the sender and receiver both use the same key for encryption and decryption while in asymmetric cryptography, two different key are used. Both of these cryptosystem have their own advantage and disadvantages.[2].

Cryptography system was invented in 1929 by an American mathematician, Lester S. Hill. The idea of Hill Cipher, assigning a numerical value to each letter of the words, in English Language we have 26 alphabets, therefore Hill work on modulo 26, for more information see [1,2]. The study of cryptology consist of two parts: cryptography, concerns with the secrecy system and its design and cryptanalysis concerns with the breaking of the secrecy system above. Most of us associate cryptography with the military war and secret agents. indeed these areas have seen extensive use of cryptography but not limited [1].

II. MATHEMATICAL BACKGROUND:

In this section we present, an important mathematical relationships , definitions and theorems in order to study how to send and receive our messages perfect and secretly.

2.1 Definition : The greatest common divisor of two integers a and b is the greatest integer that divides both a and b, and denote by $\gcd(a,b)$[3].

2.2 Definition: Let m be a positive integer, we say that a is congruent to $b(\mathrm{mod}m)$ if $m|(a-b)$, where a and b are integer $i.e\, a = b + km$ and $k \in \mathbb{Z}$.

If a is congruent to $b(\mathrm{mod}m)$, we write $a \equiv b(\mathrm{mod}m)$. If $m \nmid (a-b)$, then we write $a \not\equiv b(\mathrm{mod}m)$. Equivalently $a \equiv b(\mathrm{mod}m)$, if and only if $a = b + my$ for some $y \in \mathbb{Z}$. The relation $a \equiv b(\mathrm{mod}m)$ is called congruence relation or simply a congruence , where the number m is called the modulus of congruence[4].

2.3.Theorem: Let $m \geq 0$. We say that the numbers a and b are congruent modulo m, denoted $a \equiv b(\mathrm{mod}m)$ if a and b leave the same reminder when divided by m. The number m is the modulus of congruence. The notation $a \not\equiv b(\mathrm{mod}m)$ means that they are not congruent [6].

2.4.1.Lemma: The number a and b are congruent modulo m if and only if $m|(a-b)$ and also if and only if $m|(b-a)$ [6].

Proof: Write $a = mq_a + r_a$ and $b = mq_b + r_b$ for some q_a, q_b, r_a and r_b with $0 \le r_a, r_b \le m$.

Subtracting gives $a - b = m(q_a - q_b) + (r_a - r_b)$. Observe that the restrictions on the remainders imply that $-m \le r_a - r_b \le m$ and so $r_a - r_b$ is not a multiple of m unless $r_a - r_b = 0$.

If a and b are congruent modulo m then $r_a = r_b$ which implies that $a - b = m(q_a - q_b)$ so $a - b$ is a multiple of m .The multiplication in reverse.

If $a - b$ is a multiple of m then in the equation $a - b = m(q_a - q_b) + (r_a - r_b)$, this implies that $r_a - r_b = 0$ by above observation. Therefore, then $r_a = r_b$. The $a - b$ statement is proved similarly.

2.5. Definition: Linear (Congruence's), A equation of the form $ax \equiv b(\text{mod } m)$, where a ,b,and m are integers and x is a variable is call a linear congruence [3].

2.6. Definition: Two numbers a and b are relatively prime if their prime factorization have no factors in common, such that $\gcd(a, b) = 1$.

2.7 Theorem: Let $m \ge 2$ be an integer, a an number such that $1 \le a \le m - 1$. Then a has a multiplicative inverse modulo m if a and m are relatively prime, such that $\gcd(a, m) = 1$.

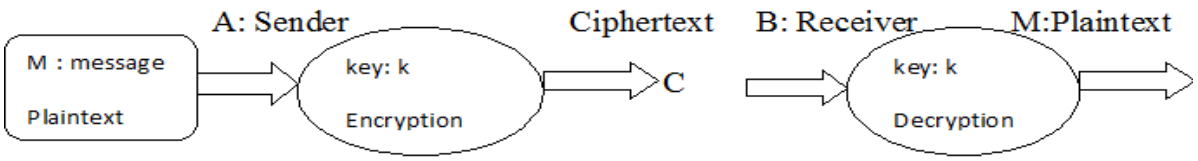
2.8.Theorem: Let $m \ge 2$. If a and m are relative prime then there exist a unique integer a^* such that $a.a^* \equiv 1(\text{mod}m)$ and $0 \le a^* \le m$ [6].

Proof: Assume that $\gcd(a, m) = 1$. By applying Bezouts lemma gives an s and t such that $as + mt = 1$. Hence $as - 1 = m(-t)$, that is $m|(as - 1)$ and so $as \equiv 1(\text{mod}m)$. Let $a^* \equiv s(\text{mod}m)$, so that $a.a^* \equiv 1(\text{mod}m)$.

To show the uniqueness, assume that $ac \equiv 1(\text{mod}m)$and $0 < c < m$. Then $ac \equiv a.a^*(\text{mod}m)$. Multiply both side of this congruence on the left by c and use the fact that $ca \equiv 1(\text{mod}m)$ to obtain $c \equiv a^*(\text{mod}m)$. This implies that $c = a^*$.

2.9 Definition: Inverse of an integer a to modulo m is a^{-1} such that $a * a^{-1} \equiv 1(\text{mod}m)$, where $a^{-1}$is called inverse of a.

The diagram I. Displaying general encryption and decryption process



In this paper, we assume that the words of the message should be separated from each other depending on the letter requirements, therefore we going to modify the Hill Cipher method modulo 26 [2] by method modulo 27 (26 English alphabets + space) and adopt the corresponding numerical values. Using the idea of matrix multiplication and multiplicative inverse, these matrix must be invertible (nonsingular) in order to get the inverse.

By using the standard modulo 27 alphabets in order to drive the following relationship between letters and numbers, these number are relatively prime to 27 such that $\gcd(a, 27) = 1$, where $2 \ge a \ge 27$. The table for alphabets and its corresponding positive and negative integers value.

To encrypt a message (plaintext), we break the message into two consecutive letter when we use 2×2 matrix , three consecutive letter for 3×3 matrix and four consecutive letter for 4×4 matrix modulo 27 (modified method). Also we convert the character into corresponding numerical vector values and multiplying the key matrix with the numerical vector matrices of characters modulo 27, we get column matrices of integer numbers which transform into corresponding characters to extract the analogous ciphertext.

To decrypt ciphertext in to plaintext, we use the same process as in encryption above in conjunction with inverse of matrices in state of given matrices. Eventually, we rewrite the characters in connection.

Table I. Illustrating English Alphabetic letters and its corresponding numerical integer value modulo 27.

Alphabets	A	B	C	D	E	F	G	H	I	J	K	L	M	Space
Numbers	1, -26	2, -25	3, -24	4, -23	5, -22	6, -21	7, -20	8, -19	9, -18	10, -17	11, -16	12, -15	13, -14	
Alphabets	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
Numbers	14, -13	15, -12	16, -11	17, -10	18, -9	19, -8	20, -7	21, -6	22, -5	23, -4	24, -3	25, -2	26, -1	27 0

Table II. demonstrating the inverse of element modulo 27 which satisfies $a * a^{-1} \equiv 1 (\text{mod } m)$

Number	2	4	5	7	8	10	11	13	14
Inverse	14	7	11	4	17	19	5	25	2
Number	16	17	19	20	22	23	25	26	
Inverse	22	8	10	23	16	20	13	26	

III. METHOD IMPLEMENTATION

3.1 . Matrix 2×2 modulo 27 Method

Suppose we given nonsingular matrix $B = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}$ as an encryption key, such that B^{-1} exists and a message "**HELP ME PLEASE** ".

To encrypt the message using 2×2 matrix modulo 27. First we have assign each character to a single numerical value such that, $A = 1, B = 2 \dots \dots \dots Z = 26$ and space $= 0$, second break the message (plaintext) into Digraph and convert them into column vector matrix as $\begin{bmatrix} p_1 \\ p_2 \end{bmatrix}$. The substitution of ciphertext letter into plaintext letter position lead us to the following linear systems.

$C_1 = (b_{11}P_1 + b_{12}P_2) mod 27$

$C_2 = (b_{21}P_1 + b_{22}P_2) mod 27$

or we can expressed as matrices multiplication

$$\begin{bmatrix} C_1 \\ C_2 \end{bmatrix} = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} \begin{bmatrix} p_1 \\ p_2 \end{bmatrix} \Rightarrow C = BP$$

Where P and C are column vectors of length 2, representing the plaintext and ciphertext respectively and B is a 2×2 matrix, which must be known for both Sender and Receiver.

EXAMPLE:

Use the key matrix B=$\begin{bmatrix} 3 & 5 \\ 1 & 6 \end{bmatrix}$, encrypt the message " **HELP ME PLEASE** ".

Solution: First break the plaintext (message)into two consecutive letters

HE LP _M E_ PL EA SE

convert the character into corresponding numerical vector values

HE $= \begin{bmatrix} 8 \\ 5 \end{bmatrix}$, LP=$\begin{bmatrix} 12 \\ 16 \end{bmatrix}$, _M=$\begin{pmatrix} 0 \\ 13 \end{pmatrix}$, E_=$\begin{bmatrix} 5 \\ 0 \end{bmatrix}$, PL=$\begin{bmatrix} 12 \\ 16 \end{bmatrix}$, EA=$\begin{bmatrix} 5 \\ 1 \end{bmatrix}$, SE=$\begin{bmatrix} 19 \\ 5 \end{bmatrix}$

$C = B.P = \begin{bmatrix} 3 & 5 \\ 1 & 6 \end{bmatrix} \begin{bmatrix} 8 \\ 5 \end{bmatrix} \text{mod} 27 = \begin{bmatrix} 22 \\ 11 \end{bmatrix}, HE \Rightarrow \text{VK}$

$\begin{bmatrix} 3 & 5 \\ 1 & 6 \end{bmatrix} \begin{bmatrix} 12 \\ 16 \end{bmatrix} \text{mod} 27 = \begin{bmatrix} 8 \\ 0 \end{bmatrix}$, LP $\Rightarrow H\_$, $\begin{bmatrix} 3 & 5 \\ 1 & 6 \end{bmatrix} \begin{bmatrix} 0 \\ 13 \end{bmatrix} \text{mod} 27 = \begin{bmatrix} 11 \\ 24 \end{bmatrix}$, _M $\Rightarrow KX$

$\begin{bmatrix} 3 & 5 \\ 1 & 6 \end{bmatrix} \begin{bmatrix} 5 \\ 0 \end{bmatrix} \text{mod} 27 = \begin{bmatrix} 15 \\ 5 \end{bmatrix}$, E_ $\Rightarrow$ OE, $\begin{bmatrix} 3 & 5 \\ 1 & 6 \end{bmatrix} \begin{bmatrix} 16 \\ 12 \end{bmatrix} \text{mod} 27 = \begin{bmatrix} 0 \\ 7 \end{bmatrix}$, PL $\Rightarrow \_G$

$\begin{bmatrix} 3 & 5 \\ 1 & 6 \end{bmatrix} \begin{bmatrix} 5 \\ 1 \end{bmatrix} \text{mod} 27 = \begin{bmatrix} 20 \\ 11 \end{bmatrix}$, EA $\Rightarrow TK$, $\begin{bmatrix} 3 & 5 \\ 1 & 6 \end{bmatrix} \begin{bmatrix} 19 \\ 5 \end{bmatrix} \text{mod} 27 = \begin{bmatrix} 1 \\ 22 \end{bmatrix}$, SE $\Rightarrow$ AV

Then the message " **HELP ME PLEASE**" has been encrypted to " **VKH KXOE GTKAV**"

To decrypt the message "**VKH KXOE GTKAV**" to the original one, we use the inverse of key matrix, such that ,

$$B^{-1} = \frac{1}{b_{11}b_{22} - b_{12}b_{21}} \begin{bmatrix} b_{22} & -b_{12} \\ -b_{21} & b_{11} \end{bmatrix} = \frac{1}{13} \begin{bmatrix} 6 & -5 \\ -1 & 3 \end{bmatrix} mod 27 = 25 \begin{bmatrix} 6 & -5 \\ -1 & 3 \end{bmatrix} mod 27$$

$= \begin{bmatrix} 15 & -17 \\ -25 & 21 \end{bmatrix} \Rightarrow \begin{bmatrix} 15 & 10 \\ 2 & 21 \end{bmatrix}$ so $B^{-1} = \begin{bmatrix} 15 & 10 \\ 2 & 21 \end{bmatrix}$

Now multiplying the inverse matrix with column vector matrices which generated from matrix operations $B.P\ (mod27)$. Thus

$\begin{bmatrix} 15 & 10 \\ 2 & 21 \end{bmatrix}\begin{bmatrix} 22 \\ 11 \end{bmatrix} \text{mod}27 = \begin{bmatrix} 8 \\ 5 \end{bmatrix} \Rightarrow HE$, $\begin{bmatrix} 15 & 10 \\ 2 & 21 \end{bmatrix}\begin{bmatrix} 8 \\ 0 \end{bmatrix} \text{mod}27 = \begin{bmatrix} 12 \\ 16 \end{bmatrix} \Rightarrow LP$

$\begin{bmatrix} 15 & 10 \\ 2 & 21 \end{bmatrix}\begin{bmatrix} 11 \\ 24 \end{bmatrix} \text{mod}27 = \begin{bmatrix} 0 \\ 13 \end{bmatrix} \Rightarrow \_M$, $\begin{bmatrix} 15 & 10 \\ 2 & 21 \end{bmatrix}\begin{bmatrix} 15 \\ 5 \end{bmatrix} \text{mod}27 = \begin{bmatrix} 5 \\ 0 \end{bmatrix} \Rightarrow E\_$

$\begin{bmatrix} 15 & 10 \\ 2 & 21 \end{bmatrix}\begin{bmatrix} 0 \\ 7 \end{bmatrix} \text{mod}27 = \begin{bmatrix} 16 \\ 12 \end{bmatrix} \Rightarrow PL$, $\begin{bmatrix} 15 & 10 \\ 2 & 21 \end{bmatrix}\begin{bmatrix} 20 \\ 11 \end{bmatrix} \text{mod}27 = \begin{bmatrix} 5 \\ 1 \end{bmatrix} \Rightarrow EA$

$\begin{bmatrix} 15 & 10 \\ 2 & 21 \end{bmatrix}\begin{bmatrix} 1 \\ 22 \end{bmatrix} \text{mod}27 = \begin{bmatrix} 19 \\ 5 \end{bmatrix} \Rightarrow SE.$

Then the decrypted message is " **HELP ME PLEASE** ".

3.2. Matrix 3×3 Method

Suppose we given key matrix $B = \begin{bmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{bmatrix}$, where B is invertible matrix such that B^{-1} exists.

In this approach the plaintext split into three successive vector column of letters as $\begin{bmatrix} p_1 \\ p_2 \\ p_3 \end{bmatrix}$ and multiplying with the key matrix to generate the following linear systems :

$$C_1 = p_1 b_{11} + p_2 b_{12} + p_3 b_{13}$$
$$C_2 = p_1 b_{21} + p_2 b_{22} + p_3 b_{23}$$
$$C_3 = p_1 b_{31} + p_2 b_{32} + p_3 b_{33}$$

or we can expressed as matrices multiplication

$$\begin{bmatrix} C_1 \\ C_2 \\ C_3 \end{bmatrix} = \begin{bmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{bmatrix}\begin{bmatrix} p_1 \\ p_2 \\ p_3 \end{bmatrix} \Rightarrow C = BP$$

Where P and C are column vectors of length 3, representing the plaintext and Ciphertext respectively and B is a 3×3 matrix, which is known for both Sender and Receiver.

EXAMPLE:

Use the key matrix $A = \begin{bmatrix} 2 & 5 & 3 \\ 3 & 1 & 2 \\ 1 & 2 & 1 \end{bmatrix}$ encrypt the message HELP ME PLEASE.

Solution: First break the plaintext (message)into three successive letters as

HEL P_M E_P LEA SE_

By converting the character to corresponding numerical vector values, such that

HEL$\equiv \begin{bmatrix} 8 \\ 5 \\ 12 \end{bmatrix}$, P_M$\equiv \begin{bmatrix} 16 \\ 0 \\ 13 \end{bmatrix}$, E_P $\equiv \begin{bmatrix} 5 \\ 0 \\ 16 \end{bmatrix}$, LEA $\equiv \begin{bmatrix} 12 \\ 5 \\ 1 \end{bmatrix}$ and SE $\equiv \begin{bmatrix} 19 \\ 5 \\ 0 \end{bmatrix}$

By multiplying the key matrix by column vectors matrices (plaintext) in order to get the corresponding numerical vectors value, which can convert to corresponding ciphertext.

$\begin{bmatrix} 2 & 5 & 3 \\ 3 & 1 & 2 \\ 1 & 2 & 1 \end{bmatrix}\begin{bmatrix} 8 \\ 5 \\ 12 \end{bmatrix} mod27 \equiv \begin{bmatrix} 23 \\ 26 \\ 3 \end{bmatrix} \Rightarrow$ WZC,

$\begin{bmatrix} 2 & 5 & 3 \\ 3 & 1 & 2 \\ 1 & 2 & 1 \end{bmatrix}\begin{bmatrix} 16 \\ 0 \\ 13 \end{bmatrix} mod27 \equiv \begin{bmatrix} 17 \\ 20 \\ 2 \end{bmatrix} \Rightarrow$QTB

$\begin{bmatrix} 2 & 5 & 3 \\ 3 & 1 & 2 \\ 1 & 2 & 1 \end{bmatrix}\begin{bmatrix} 5 \\ 0 \\ 16 \end{bmatrix} mod27 \equiv \begin{bmatrix} 4 \\ 20 \\ 21 \end{bmatrix} \Rightarrow$ DTU ,

$\begin{bmatrix} 2 & 5 & 3 \\ 3 & 1 & 2 \\ 1 & 2 & 1 \end{bmatrix}\begin{bmatrix} 12 \\ 5 \\ 1 \end{bmatrix} mod27 \equiv \begin{bmatrix} 25 \\ 16 \\ 23 \end{bmatrix} \Rightarrow$ YPW ,

$$\begin{bmatrix}2&5&3\\3&1&2\\1&2&1\end{bmatrix}\begin{bmatrix}19\\5\\0\end{bmatrix} mod 27 \equiv \begin{bmatrix}9\\8\\2\end{bmatrix} \Rightarrow \text{IHB}$$

Then the message HELP ME PLEASE has been encrypted to WZCQTBDTUYPWIHB.

To decrypt the encrypted message, we need to get the inverse of the key matrix A

$$A^{-1} = \frac{1}{4}\begin{bmatrix}-3&1&7\\-1&-1&5\\5&1&-13\end{bmatrix} mod 27 \equiv 7\begin{bmatrix}-3&1&7\\-1&-1&5\\5&1&-13\end{bmatrix} mod 27 \equiv \begin{bmatrix}-21&7&22\\-7&-7&8\\8&7&-10\end{bmatrix} mod 27 \equiv \begin{bmatrix}6&7&22\\20&20&8\\8&7&17\end{bmatrix}$$

Then $\begin{bmatrix}6&7&22\\20&20&8\\8&7&17\end{bmatrix}\begin{bmatrix}W\\Z\\C\end{bmatrix} mod\ 27 \equiv \begin{bmatrix}6&7&22\\20&20&8\\8&7&17\end{bmatrix}\begin{bmatrix}23\\26\\3\end{bmatrix} mod\ 27 \equiv \begin{bmatrix}8\\5\\12\end{bmatrix} \Rightarrow$ HEL

$$\begin{bmatrix}6&7&22\\20&20&8\\8&7&17\end{bmatrix}\begin{bmatrix}Q\\T\\B\end{bmatrix} mod\ 27 \equiv \begin{bmatrix}6&7&22\\20&20&8\\8&7&17\end{bmatrix}\begin{bmatrix}17\\20\\2\end{bmatrix} mod\ 27 \equiv \begin{bmatrix}16\\0\\13\end{bmatrix} \Rightarrow \text{P\_M}$$

$$\begin{bmatrix}6&7&22\\20&20&8\\8&7&17\end{bmatrix}\begin{bmatrix}D\\T\\U\end{bmatrix} mod\ 27 \equiv \begin{bmatrix}6&7&22\\20&20&8\\8&7&17\end{bmatrix}\begin{bmatrix}4\\20\\21\end{bmatrix} mod\ 27 \equiv \begin{bmatrix}5\\0\\16\end{bmatrix} \Rightarrow E\_P$$

$$\begin{bmatrix}6&7&22\\20&20&8\\8&7&17\end{bmatrix}\begin{bmatrix}Y\\P\\W\end{bmatrix} mod\ 27 \equiv \begin{bmatrix}6&7&22\\20&20&8\\8&7&17\end{bmatrix}\begin{bmatrix}25\\16\\23\end{bmatrix} mod\ 27 \equiv \begin{bmatrix}12\\5\\1\end{bmatrix} \Rightarrow \text{LEA}$$

$$\begin{bmatrix}6&7&22\\20&20&8\\8&7&17\end{bmatrix}\begin{bmatrix}I\\H\\B\end{bmatrix} mod\ 27 \equiv \begin{bmatrix}6&7&22\\20&20&8\\8&7&17\end{bmatrix}\begin{bmatrix}9\\8\\2\end{bmatrix} mod\ 27 \equiv \begin{bmatrix}19\\5\\0\end{bmatrix} \Rightarrow SE\_$$

Eventually the ciphertext " WZCQTBDTUYPWIHB " decrypted to plaintext (original message) "HELP ME PLEASE", using the inverse of key matrix.

3.3. Matrix 4×4 Method:

Suppose we given the matrix $B = \begin{bmatrix}b_{11}&b_{12}&b_{13}&b_{14}\\b_{21}&b_{22}&b_{23}&b_{24}\\b_{31}&b_{32}&b_{33}&b_{34}\\b_{41}&b_{42}&b_{43}&b_{44}\end{bmatrix}$ nonsingular matrix encryption key, such that B^{-1} exists, the same process as 2×2 matrix only we break the plaintext into four consecutive column vector of letters as $\begin{bmatrix}p_1\\p_2\\p_3\\p_4\end{bmatrix}$ and multiplying with the key matrix as follow:

$$\begin{bmatrix}C_1\\C_2\\C_3\\C_4\end{bmatrix} = \begin{bmatrix}b_{11}&b_{12}&b_{13}&b_{14}\\b_{21}&b_{22}&b_{23}&b_{24}\\b_{31}&b_{32}&b_{33}&b_{34}\\b_{41}&b_{42}&b_{43}&b_{44}\end{bmatrix}\begin{bmatrix}p_1\\p_2\\p_3\\p_4\end{bmatrix} \Rightarrow C = BP$$

Thus, we generate the following linear systems

$$C_1 = p_1 b_{11} + p_2 b_{12} + p_3 b_{13} + p_4 b_{14}$$
$$C_2 = p_1 b_{21} + p_2 b_{22} + p_3 b_{23} + p_4 b_{24}$$
$$C_3 = p_1 b_{31} + p_2 b_{32} + p_3 b_{33} + p_4 b_{34}$$
$$C_4 = p_1 b_{41} + p_2 b_{42} + p_3 b_{43} + p_4 b_{44}$$

Where P and C are column vectors of length 4, representing the Plaintext and Ciphertext respectively and B is a 4×4 matrix, must be known for both Sender and Receiver.

Example:

Use the key matrix $B = \begin{bmatrix}2&4&3&2\\3&6&5&2\\2&5&2&-3\\4&5&14&14\end{bmatrix}$ encrypt the message, "PLEASE CHECK YOUR EMAIL".

Solution: The procedure as in the previous examples, but here we break the message into four consecutive character including space as follow:

PLEASE CHECK YOUR EMAIL⇒ PLEA SE_C HECK _YOU R_EM AIL_

$$\text{PLEA} \Rightarrow \begin{bmatrix}16\\12\\5\\1\end{bmatrix}, \begin{bmatrix}2&4&3&2\\3&6&5&2\\2&5&2&-3\\4&5&14&14\end{bmatrix}\begin{bmatrix}16\\12\\5\\1\end{bmatrix} \bmod 27 \equiv \begin{bmatrix}16\\12\\18\\19\end{bmatrix} \Rightarrow \text{PLRS}$$

$$\text{SE\_C} \Rightarrow \begin{bmatrix}19\\5\\0\\3\end{bmatrix}, \begin{bmatrix}2&4&3&2\\3&6&5&2\\2&5&2&-3\\4&5&14&14\end{bmatrix}\begin{bmatrix}19\\5\\0\\3\end{bmatrix} \bmod 27 \equiv \begin{bmatrix}10\\12\\0\\8\end{bmatrix} \Rightarrow \text{JL\_H}$$

$$\text{HECK} \Rightarrow \begin{bmatrix}8\\5\\3\\11\end{bmatrix}, \begin{bmatrix}2&4&3&2\\3&6&5&2\\2&5&2&-3\\4&5&14&14\end{bmatrix}\begin{bmatrix}8\\5\\3\\11\end{bmatrix} \bmod 27 \equiv \begin{bmatrix}13\\10\\14\\10\end{bmatrix} \Rightarrow \text{MJNJ}$$

$$\text{\_YOU} \Rightarrow \begin{bmatrix}0\\25\\15\\21\end{bmatrix}, \begin{bmatrix}2&4&3&2\\3&6&5&2\\2&5&2&-3\\4&5&14&14\end{bmatrix}\begin{bmatrix}0\\25\\15\\21\end{bmatrix} \bmod 27 \equiv \begin{bmatrix}25\\24\\11\\8\end{bmatrix} \Rightarrow \text{YXKH}$$

$$\text{R\_EM} \Rightarrow \begin{bmatrix}18\\0\\5\\13\end{bmatrix}, \begin{bmatrix}2&4&3&2\\3&6&5&2\\2&5&2&-3\\4&5&14&14\end{bmatrix}\begin{bmatrix}18\\0\\5\\13\end{bmatrix} \bmod 27 \equiv \begin{bmatrix}23\\24\\7\\0\end{bmatrix} \Rightarrow \text{WXG\_}$$

$$\text{AIL\_} \Rightarrow \begin{bmatrix}1\\9\\12\\0\end{bmatrix}, \begin{bmatrix}2&4&3&2\\3&6&5&2\\2&5&2&-3\\4&5&14&14\end{bmatrix}\begin{bmatrix}1\\9\\12\\0\end{bmatrix} \bmod 27 \equiv \begin{bmatrix}20\\9\\17\\1\end{bmatrix} \Rightarrow \text{TIQA}$$

Then the message "PLEASE CHECK YOUR EMAIL" encrypted to ciphertext as "PLRSJL HMJNJYXKHWXG TIQA"

To decrypt the encrypted message above, we need to obtain the inverse of the key matrix $\mathbf{B}$, such that $C = BP \Rightarrow P = B^{-1}C$

$$B^{-1} = \begin{bmatrix}-23&2&-2&-9\\10&-12&16&23\\1&-2&12&22\\2&-2&6&11\end{bmatrix} \bmod 27$$

$$\begin{bmatrix}-23&2&-2&-9\\10&-12&16&23\\1&-2&12&22\\2&-2&6&11\end{bmatrix}\begin{bmatrix}P\\L\\R\\S\end{bmatrix} \bmod 27 \Rightarrow \begin{bmatrix}-23&2&-2&-9\\10&-12&16&23\\1&-2&12&22\\2&-2&6&11\end{bmatrix}\begin{bmatrix}16\\12\\18\\19\end{bmatrix} \bmod 27 \equiv \begin{bmatrix}-11\\12\\5\\1\end{bmatrix} \Rightarrow \text{PLEA}$$

$$\begin{bmatrix}-23&2&-2&-9\\10&-12&16&23\\1&-2&12&22\\2&-2&6&11\end{bmatrix}\begin{bmatrix}J\\L\\\_\\H\end{bmatrix} \bmod 27 \Rightarrow \begin{bmatrix}-23&2&-2&-9\\10&-12&16&23\\1&-2&12&22\\2&-2&6&11\end{bmatrix}\begin{bmatrix}10\\12\\0\\8\end{bmatrix} \bmod 27 \equiv \begin{bmatrix}-8\\5\\0\\3\end{bmatrix} \Rightarrow SE\_C$$

$$\begin{bmatrix}-23&2&-2&-9\\10&-12&16&23\\1&-2&12&22\\2&-2&6&11\end{bmatrix}\begin{bmatrix}M\\J\\N\\J\end{bmatrix} \bmod 27 \Rightarrow \begin{bmatrix}-23&2&-2&-9\\10&-12&16&23\\1&-2&12&22\\2&-2&6&11\end{bmatrix}\begin{bmatrix}13\\10\\14\\10\end{bmatrix} \bmod 27 \equiv \begin{bmatrix}-19\\5\\3\\11\end{bmatrix} \Rightarrow \text{HECK}$$

$$\begin{bmatrix}-23&2&-2&-9\\10&-12&16&23\\1&-2&12&22\\2&-2&6&11\end{bmatrix}\begin{bmatrix}Y\\X\\K\\H\end{bmatrix} \bmod 27 \Rightarrow \begin{bmatrix}-23&2&-2&-9\\10&-12&16&23\\1&-2&12&22\\2&-2&6&11\end{bmatrix}\begin{bmatrix}25\\24\\11\\8\end{bmatrix} \bmod 27 \equiv \begin{bmatrix}0\\25\\15\\21\end{bmatrix} \Rightarrow \text{\_YOU}$$

$$\begin{bmatrix}-23&2&-2&-9\\10&-12&16&23\\1&-2&12&22\\2&-2&6&11\end{bmatrix}\begin{bmatrix}W\\X\\G\\\_\end{bmatrix} \bmod 27 \Rightarrow \begin{bmatrix}-23&2&-2&-9\\10&-12&16&23\\1&-2&12&22\\2&-2&6&11\end{bmatrix}\begin{bmatrix}23\\24\\7\\0\end{bmatrix} \bmod 27 \equiv \begin{bmatrix}-9\\0\\5\\13\end{bmatrix} \Rightarrow R\_EM$$

$$\begin{bmatrix}-23&2&-2&-9\\10&-12&16&23\\1&-2&12&22\\2&-2&6&11\end{bmatrix}\begin{bmatrix}T\\I\\Q\\A\end{bmatrix} \bmod 27 \Rightarrow \begin{bmatrix}-23&2&-2&-9\\10&-12&16&23\\1&-2&12&22\\2&-2&6&11\end{bmatrix}\begin{bmatrix}20\\9\\17\\1\end{bmatrix} \bmod 27 \equiv \begin{bmatrix}-26\\9\\12\\0\end{bmatrix} \Rightarrow \text{AIL\_}$$

Hence the decrypted ciphertext "PLRSJL HMJNJYXKHWXG TIQA" has encrypted to the original plaintext "PLEASE CHECK YOUR EMAIL"

IV. RESULTS

In this study we used invertible key matrices congruent modulo 27 instate of congruent modulo 26 method, which introduced by Hill Cipher in order to encrypt and decrypt messages. Mathematical relations have been logically implemented so as to keep the information secure from the other partners. Meanwhile it was found that , cryptography process using matrices is the strongest method among the other cryptography methods because it use mathematical techniques.

V. CONCLUSION

The study introduced cryptography of messages using nonsingular matrices modulo 27 as the key, which must be known for both Sender and Receiver. However, mathematical techniques have been applied. and the positive and negative numerical values equivalent to English Alphabetic have been generated.

The messages have been coded and decoded perfectly using 2×2 , 3×3 and 4×4 invertible matrices modulo 27. Eventually, the information could be sent and received safely using the method above.

The messages couldn't decrypt without key matrix and congruence relations.

REFERENCES

[1]. Stu Schwart. Cryptography for Beginners. Wissahickon High Ambler, Pa 19002,www.mastermathmentor.com

[2]. Neha Sharma,Sachin Chirgaiya. A Novel Approach to Hill Cipher. International Journal of Computer Applications, India , 2014.

[3]. Wissam Raji. An Introductory Course in Elementary Number Theory. Publisher Saylor Foundation 2016.

[4]. Victor Shoup, , A computational Introduction to Number Theory and Algebra, Cambridge University press. 2008.

[5]. P.Shanmugam and C.Loganathan. INVOLUNTORY MATRIX IN CRYPTOGRAPHY.IJRRAS volume 6, Issue 4, India, March 2011.

[6]. W. Edwin Clark. Elementary Number Theory. University of South Florida, Dec 2002.

[7]. Menzes A, Van Oorschot P and Vanstoe, S. Hand book of Applied Cryptography, CRC press, 1997.

[8]. Sani Isa and Abdulaziz B. M. Hamed. Cryptography Using Congruence Modulo Relations. American Journal of Engineering Research volume 6 issue -3, pp 156-160.