Comparison of a Proposed Algorithm and Hill cipher Algorithm in Cryptography

Kwasi Baah Gyamfi[1], Kwame Owusu Bempah[2]
[1]Mathematics Department, Kwame Nkrumah University of Science and Technology, Ghana
[2]Mathematics Department, University of Education, Winneba, Ghana

Abstract - The Hill cipher algorithm only encrypts messages in the form of document and can only decrypts the same message provided the matrix used as key is non-singular. In this paper, we propose an algorithm for decryption of documents to be possible for both singular and non -singular matrices as involutary key alongside giving practical examples by using two by two and three by three involutary keys for singular and non singular matrices to illustrate our result when encrypting and decrypting documents.

keywords: Singular Matrix, Non- Singular Matrix, Involutary Key

1 Introduction

Modular arithmetic is an aspect of algebra and has diverse applications in mathematics and one crucial application is in the field of cryptography which is the study of mathematical techniques to change important messages and informations to unreadable one. Cryptography deals with information which comprises of confidentiality, security, data integrity and authentication[1] etc. There are two types of cryptography namely symmetric and asymmetric cryptography. In symmetric cryptography, the same key is used for both encryption and decryption whiles in asymmetric, different keys are used. In all the aspects of cryptography, they employ techniques which results in ciphers or ciphertext. Some of the great mathematicians that introduced algorithms for encryption and decryption generating ciphers include Hill cipher, Vigenere cipher, Affine-Hill Ciphers. The Hill cipher algorithm $C = VR$, is a very powerful technique used by cryptographers to encrypts documents using $n \times n$ invertible matrix as key but the only draw-back was when generating the plaintext message for a singular matrix used as key since decryption is dependent on the matrix being invertible which is the decryption aspect for the algorithm[3]-[5]. In 2018, Yangyang and Chengzhe made valuable contribution by improving on the Hill cipher algorithm and published in their journal "The improved Hill Encryption algorithm". This algorithm was solely on video encryption . In 2017, there was another improvement on the Hill cipher algorithm which was published by J.Zou and T.weng entitled "A new image encryption instant communication method" and was based on matrix transformation which was focused solely on image encryption. This paper therefore focuses and makes an improvement on the Hill cipher algorithm by proposing an algorithm which uses either singular or non-singular matrices as keys in the area of encryption and decryption of documents in the form of messages.

http://dx.doi.org/10.29322/IJSRP.10.12.2020.p10837

2 Preliminaries

This section discusses the concept of equivalence in modular arithmetic where we look at congruence relation looking at some definitions, proposition, theorems and some examples that will enable us to understand modular arithmetic in cryptography

Definition 2.1 For equivalence in modular arithmetic, the idea of congruence relation where $r \in N_o$ is positive with $r > 0$ and e and f are integers. Then we say that e is congruent to f modulo r if $r|(e-f)$ and it is written as $e \equiv f(modr)$

Example 2.1 7 and 79 can be said to be congruent in mod 4 because $4|(79-7)$. This can be seen by noting that $79 \equiv 7$

Theorem 2.1 For positive integers e, f, g, h and r, if $e \equiv f(modr)$ and also $g \equiv h(modr)$, then $(i)e+g \equiv f+h(modr)$ and $(ii)eg \equiv fh(modr)$

Proof(i) when $e \equiv f(modr)$, then it can be written as $r|(e-f)$ which also means $(e-f) = pr$.this gives $e = f+pr$. then it also means $g \equiv h(modr)$ can be written as $g = h+tr$ where $p, t \in Z$ are positive integers.we than write $e+g \equiv f+h(modr)$ as $(e+g)-(f+h)modr$, then from the results we produce $f+pr+h+tr-f-h = r(p+t)$ and since $p, t \in Z$, then it implies $e+g \equiv f+h(modr)$(ii) also from the above, eg≡ $fh(modr)$can also be written as $eg-fhmodr$. then we have $(f+pr)(h+tr)-fh = fh+ftr+prh+ptr^2-fh$ we get r(ft+ph+ptr) but $ft+ph+ptr \in Z$ meaning $eg \equiv fh(modr)$

Example 2.1 if 7≡37 mod5 and 9≡29 mod5, then(i) 7+9≡37+29 mod5 and (ii)7(9)≡37(29) mod5

Definition 2.2 For all $[e] \in Z_r$ and $[f] \in Z_r$ or if $([e][f]) \in Z_r$, then we can define addition mod r as $[e]_r + [f]_r = [e+f]_r$

Theorem 2.2 Addition and multiplication mod r satisfy the commutative and associative laws and multiplication distributes over addition

Proof For integers $[e], [f], [g] \in Z_r$, then for commutativity,
$[e] +_r [f] = [f +_r e]$. Since $\forall e, f \in Z_r$,we have $e+f = f+e$, then $[e] +_r [f] = [e+f] = [f+e] = [f +_r e]$.
Also for associativity,
$[e] +_r ([f] +_r [g]) = ([e +_r f]) +_r [g]$. Since $\forall e, f, g \in Z_r$, then we have,$e+f+g = (e+f)+g$, then $[e] +_r ([f] +_r [g]) = ([e +_r f]) +_r [g] = ([e] + ([f+g])_r)_r = [e]+([f+g]))_r = (([e+f])+[g])_r$. This produces the associative law for ordinary sums giving us $(([e +_r f]) + g)_r = ([e] +_r [f]) +_r [g]$

http://dx.doi.org/10.29322/IJSRP.10.12.2020.p10837

Example 2.2 (i)$[(4+15mod5)]mod5 = [(15+4mod5)]mod5$ (ii)$[3+(6+17mod6)]mod6 = [(3+6mod6)+17]mod6$

3 Main Result

In this section, we propose an algorithm for encrypting and decrypting documents or messages using the Hill cipher algorithm as foundation.

3.1 Overview of Hill cipher Algorithm

The encryption and decryption process of the Hill cipher algorithm are given as $C = VRmodm$ and $R = CV^{-1}modm$ respectively.
where V is a symmetric key which is chosen randomly in any invertible $n \times n$ matrix
R are numerical values of the letters of the English alphabet, C is the ciphertext produced which are also numerical values and m is the number of the letters of the English alphabet which is 26

3.2 Propose algorithm

Since the above Hill cipher algorithm only encrypt and decrypts documents for any $n \times n$ non-singular matrices chosen as key only, then there should be an improvement on this algorithm for either singular or non-singular matrices chosen as keys where the algorithm can be encrypted as

$$C = V + Imodm$$

and also decrypted as

$$I = C - Vmodm$$

where,

- V is an $n \times n$ singular or non-singular matrix chosen as key
- I is identity matrix for the $n \times n$ matrix chosen as key which is always replaced by numerical values of the letters of the alphabet
- C is ciphertext which are also numerical values of the letters of the alphabet
- m is numerical values of the letters of the English Alphabet which would be encrypted in modulo 27 to bring about clear distinction between the numerical value 0 and the spaces in between letters

Table 3.3 Letters of the English Alphabet and their numerical values in mod 27

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

http://dx.doi.org/10.29322/IJSRP.10.12.2020.p10837

where "sc" represents space in between letters

3.3.1 Encryption process of the propose algorithm

For this process, we will be converting documents in the form of plaintext messages into their ciphertext using the procedure below

step 1. Get any key of $n \times n$ matrix V being singular or non-singular. The size of the matrix is dependent on the grouping of the plaintext letters. This means any 2×2 matrix would be grouped into two letters each and 3×3 matrix chosen as key would also be grouped into three letters each.

step 2. Convert the letters in the plaintext message into their corresponding numerical values using table 3.3

step 3. Replace The first column of the identity matrix as plaintext letters of the message which will form I.
In order to make the algorithm more secured,we replace the columns of the identity matrix by the letters of the plaintext message to be encrypted

step 4. Add V to I to get the ciphertext matrix C

step 5. Convert each element in the matrix into their corresponding letters to form the ciphertext

We then produce the algorithm

$$V + I = C$$

based on the technique where 2×2 and 3×3 singular or non- singular matrix keys we choose; produces the following respectively

$$\begin{bmatrix} V_{11} & V_{12} \\ V_{21} & V_{22} \end{bmatrix} + \begin{bmatrix} I_{11} & 0 \\ I_{21} & 1 \end{bmatrix} = \begin{bmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{bmatrix}$$

and

$$\begin{bmatrix} V_{11} & V_{12} & V_{13} \\ V_{21} & V_{22} & V_{23} \\ V_{31} & V_{32} & V_{33} \end{bmatrix} + \begin{bmatrix} I_{11} & 0 & 0 \\ I_{21} & 1 & 0 \\ I_{31} & 0 & 1 \end{bmatrix} = \begin{bmatrix} C_{11} & C_{12} & C_{13} \\ C_{21} & C_{22} & C_{23} \\ C_{31} & C_{32} & C_{33} \end{bmatrix}$$

where I_{11},I_{21} and I_{31} are replacement of the letters in the message by their numerical values

3.3.2 Decryption Process of the Propose algorithm

step 1. Get the key for the matrix which is a singular or non-singular matrix

step 2. Convert the letters from the ciphertext C to each of their corresponding numerical values

step 3. Subtract V from C to get the matrix I. It would be vividly seen that, in getting I, the plaintext letters would be seen including the elements of the identity matrix.

http://dx.doi.org/10.29322/IJSRP.10.12.2020.p10837

step 4. Convert the elements seen in the plaintext letters of the matrix I to get the plaintext message.

We also produce the decryption algorithm from the techniques above as

$$C - V = I$$

where 2×2 and 3×3 singular or non-singular matrix as key can be given as

$$\begin{bmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{bmatrix} - \begin{bmatrix} V_{11} & V_{12} \\ V_{21} & V_{22} \end{bmatrix} = \begin{bmatrix} I_{11} & 0 & 0 \\ I_{21} & 1 & 0 \\ I_{31} & 0 & 1 \end{bmatrix}$$

and

$$\begin{bmatrix} C_{11} & C_{12} & C_{13} \\ C_{21} & C_{22} & C_{23} \\ C_{31} & C_{32} & C_{33} \end{bmatrix} - \begin{bmatrix} V_{11} & V_{12} & V_{13} \\ V_{21} & V_{22} & V_{23} \\ V_{31} & V_{32} & V_{33} \end{bmatrix} = \begin{bmatrix} I_{11} & 0 & 0 \\ I_{21} & 1 & 0 \\ I_{31} & 0 & 1 \end{bmatrix}$$

where I_{11},I_{21} and I_{31} are replacement of the letters in the message by their numerical values.

3.3.3 Practical example for 2×2 singular matrix on the propose algorithm

We are going to encrypt and decrypt informations in the form of messages on the proposed algorithm but with a 2×2 singular matrix as a key. Lets suppose Abenaa want to send a very confidential message entitled "I AM BLESSED" to kofi in London using the key V= $\begin{bmatrix} -8 & 16 \\ -2 & 4 \end{bmatrix}$

Abenaa will first of all convert every letter in the plaintext message into their numerical values using table 3.3 giving,
I→9, sc→0 A→0, M→14,sc→0 B→2, L→12, E→5, S→19, S→19, E→5, D→4
Abenaa will now group the message into two letters each since the size of the matrix is dependent on the grouping and I is the identity matrix with replacement of the first column of the identity matrix as numerical values of the plaintext message or letters. She now encrypts to get the ciphertext using $V + I = C$ as follows

$$\begin{bmatrix} -8 & 16 \\ -2 & 4 \end{bmatrix} + \begin{bmatrix} 9 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 16 \\ -2 & 5 \end{bmatrix} = \begin{bmatrix} 1 & 16 \\ 25 & 5 \end{bmatrix} mod 27$$

$$\begin{bmatrix} -8 & 16 \\ -2 & 4 \end{bmatrix} + \begin{bmatrix} 1 & 1 \\ 0 & 13 \end{bmatrix} = \begin{bmatrix} -7 & 17 \\ -2 & 17 \end{bmatrix} = \begin{bmatrix} 20 & 17 \\ 25 & 17 \end{bmatrix} mod 27$$

$$\begin{bmatrix} -8 & 16 \\ -2 & 4 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 19 & 16 \\ 0 & 5 \end{bmatrix} mod 27$$

http://dx.doi.org/10.29322/IJSRP.10.12.2020.p10837

$$\begin{bmatrix} -8 & 16 \\ -2 & 4 \end{bmatrix} + \begin{bmatrix} 1 & 12 \\ 0 & 5 \end{bmatrix} = \begin{bmatrix} 20 & 1 \\ 25 & 9 \end{bmatrix} mod 27$$

$$\begin{bmatrix} -8 & 16 \\ -2 & 4 \end{bmatrix} + \begin{bmatrix} 19 & 0 \\ 19 & 1 \end{bmatrix} = \begin{bmatrix} 11 & 16 \\ 17 & 5 \end{bmatrix} mod 27$$

Abenaa will then convert every elements in the matrix operation gotten into their letters to get the ciphertext which is the hidden message as "$AYFETYQQSPETYAIKQPETYUH$". Abenaa then sends the ciphertext and the key V to kofi. Kofi receives the message and decrypt it using the algorithm $C - V = I$
where he converts the ciphertext letters into their nuemerical values using table 3.3 which produces

$$\begin{bmatrix} 1 & 16 \\ 25 & 5 \end{bmatrix} - \begin{bmatrix} -8 & 16 \\ -2 & 4 \end{bmatrix} = \begin{bmatrix} 9 & 0 \\ 0 & 1 \end{bmatrix} mod 27$$

$$\begin{bmatrix} 20 & 17 \\ 25 & 17 \end{bmatrix} - \begin{bmatrix} -8 & 16 \\ -2 & 4 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 13 \end{bmatrix} mod 27$$

$$\begin{bmatrix} 19 & 16 \\ 0 & 5 \end{bmatrix} - \begin{bmatrix} -8 & 16 \\ -2 & 4 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 2 & 1 \end{bmatrix} mod 27$$

$$\begin{bmatrix} 20 & 1 \\ 25 & 9 \end{bmatrix} - \begin{bmatrix} -8 & 16 \\ -2 & 4 \end{bmatrix} = \begin{bmatrix} 1 & 12 \\ 0 & 5 \end{bmatrix} mod 27$$

$$\begin{bmatrix} 11 & 16 \\ 17 & 5 \end{bmatrix} - \begin{bmatrix} -8 & 16 \\ -2 & 4 \end{bmatrix} = \begin{bmatrix} 19 & 0 \\ 19 & 1 \end{bmatrix} mod 27$$

$$\begin{bmatrix} 20 & 21 \\ 25 & 8 \end{bmatrix} - \begin{bmatrix} -8 & 16 \\ -2 & 4 \end{bmatrix} = \begin{bmatrix} 1 & 5 \\ 0 & 4 \end{bmatrix} mod 27$$

It can be seen that, the letters of the plaintext message are gotten including the identity elements. The numerical values representing the letters of the message are then converted to thier plaintext letters using table 3.3 leaving the identity elements which we get,
9→I, 0→sc,1→A 13→M,0→sc 2→B, 12→L, 5→E, 19→S, 19→S, 5→E, 4→D
This gives "I AM BLESSED" which is the plaintext message encrypted by Abenaa

http://dx.doi.org/10.29322/IJSRP.10.12.2020.p10837

3.3.4 Practical example for 2×2 non- singular matrix on the propose algorithm

In this example, we will be using a 2×2 non-singular matrix V= $\begin{bmatrix} 6 & 3 \\ 4 & 5 \end{bmatrix}$ as a key for the algorithm to encrypt the same confdential message "I AM BLESSED". Abenaa who is the sender will still change all the letters in the plaintext message into their numerical values producing, I→9, sc→0 A→0, M→14,sc→0 B→2, L→12, E→5, S→19, S→19, E→5, D→4
She then groups the message into two letters and replaces the first column of the identity elements by the numerical values of the plaintext letters for I. She then encrypts the message using the algorithm $V + I = C$ as,

$$\begin{bmatrix} 6 & 3 \\ 4 & 5 \end{bmatrix} + \begin{bmatrix} 9 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 15 & 3 \\ 4 & 6 \end{bmatrix} mod 27$$

$$\begin{bmatrix} 6 & 3 \\ 4 & 5 \end{bmatrix} + \begin{bmatrix} 1 & 1 \\ 0 & 13 \end{bmatrix} = \begin{bmatrix} 7 & 4 \\ 4 & 8 \end{bmatrix} mod 27$$

$$\begin{bmatrix} 6 & 3 \\ 4 & 5 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 6 & 3 \\ 6 & 6 \end{bmatrix} mod 27$$

$$\begin{bmatrix} 6 & 3 \\ 4 & 5 \end{bmatrix} + \begin{bmatrix} 1 & 12 \\ 0 & 15 \end{bmatrix} = \begin{bmatrix} 7 & 15 \\ 4 & 10 \end{bmatrix} mod 27$$

$$\begin{bmatrix} 6 & 3 \\ 4 & 5 \end{bmatrix} + \begin{bmatrix} 19 & 0 \\ 19 & 1 \end{bmatrix} = \begin{bmatrix} 25 & 3 \\ 23 & 6 \end{bmatrix} mod 27$$

$$\begin{bmatrix} 6 & 3 \\ 4 & 5 \end{bmatrix} + \begin{bmatrix} 1 & 5 \\ 0 & 4 \end{bmatrix} = \begin{bmatrix} 7 & 8 \\ 4 & 9 \end{bmatrix} mod 27$$

Abenaa still converts the elements of each matrix above into their letters using table 3.3 to form the hidden message which is the ciphertext as "ODCFGDDRF-FCFGDOJYWCFGDHI" and then sends to kofi. Kofi receives the message and then decrypts by converting every letter in the ciphertext into their corresponding numerical values producing $C - V = I$ which gives,

$$\begin{bmatrix} 15 & 3 \\ 4 & 6 \end{bmatrix} - \begin{bmatrix} 6 & 3 \\ 4 & 5 \end{bmatrix} = \begin{bmatrix} 9 & 0 \\ 0 & 1 \end{bmatrix} mod 27$$

$$\begin{bmatrix} 7 & 4 \\ 4 & 18 \end{bmatrix} - \begin{bmatrix} 6 & 3 \\ 4 & 5 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 13 \end{bmatrix} mod 27$$

http://dx.doi.org/10.29322/IJSRP.10.12.2020.p10837

$$\begin{bmatrix} 6 & 3 \\ 6 & 6 \end{bmatrix} - \begin{bmatrix} 6 & 3 \\ 4 & 5 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 2 & 1 \end{bmatrix} mod 27$$

$$\begin{bmatrix} 7 & 15 \\ 4 & 10 \end{bmatrix} - \begin{bmatrix} 6 & 3 \\ 4 & 5 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 12 & 5 \end{bmatrix} mod 27$$

$$\begin{bmatrix} 25 & 3 \\ 23 & 6 \end{bmatrix} - \begin{bmatrix} 6 & 3 \\ 4 & 5 \end{bmatrix} = \begin{bmatrix} 19 & 0 \\ 19 & 1 \end{bmatrix} mod 27$$

$$\begin{bmatrix} 7 & 8 \\ 4 & 9 \end{bmatrix} - \begin{bmatrix} 6 & 3 \\ 4 & 5 \end{bmatrix} = \begin{bmatrix} 1 & 5 \\ 0 & 4 \end{bmatrix} mod 27$$

It can be seen above that, the elements of the plaintext letters are gotten in addition to the elements of the identity.The numerical values which represents the plaintext letters in the message are then converted leaving the identity elements which produces
9→I, 0→sc,1→A 13→M,0→sc 2→B, 12→L, 5→E, 19→S, 19→S, 5→E, 4→D
which represents "I AM BLESSED" which is the message that was sent by Abenaa

3.3.5 Practical Example for 3×3 non- singular matrix on the propose algorithm

In this example, we will be encrypting and decrypting documents using the algorithm in the form of messages sent by Linda entitled "DO NOT OPEN" to Thomas as receiver with the non- singular matrix key V= $\begin{bmatrix} 3 & 1 & 1 \\ 4 & 3 & 2 \\ 2 & 8 & 4 \end{bmatrix}$
Linda will encrypts the message by converting the letters in the plaintext message into their numerical values using table 3.3 and also replaces the columns of the elements of the identity matrix by the numerical values of the plaintext letters to form I. Now we have,
D→4,O→14,sc→0 N→13, O→14, T→19,sc→0 O→14, P→15, E→4, N→13
Now lets get the ciphertext using the encryption algorithm $V + I = C$ as

$$\begin{bmatrix} 3 & 1 & 1 \\ 4 & 3 & 2 \\ 2 & 8 & 4 \end{bmatrix} + \begin{bmatrix} 4 & 0 & 0 \\ 15 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 7 & 1 & 1 \\ 19 & 4 & 2 \\ 2 & 8 & 5 \end{bmatrix} mod 27$$

$$\begin{bmatrix} 3 & 1 & 1 \\ 4 & 3 & 2 \\ 2 & 8 & 4 \end{bmatrix} + \begin{bmatrix} 1 & 15 & 0 \\ 0 & 18 & 0 \\ 0 & 19 & 1 \end{bmatrix} = \begin{bmatrix} 4 & 15 & 1 \\ 4 & 18 & 2 \\ 2 & 0 & 5 \end{bmatrix} mod 27$$

http://dx.doi.org/10.29322/IJSRP.10.12.2020.p10837

$$\begin{bmatrix} 3 & 1 & 1 \\ 4 & 3 & 2 \\ 2 & 8 & 4 \end{bmatrix} + \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 15 \\ 0 & 0 & 16 \end{bmatrix} = \begin{bmatrix} 4 & 1 & 1 \\ 4 & 4 & 17 \\ 2 & 8 & 20 \end{bmatrix} mod 27$$

$$\begin{bmatrix} 3 & 1 & 1 \\ 4 & 3 & 2 \\ 2 & 8 & 4 \end{bmatrix} + \begin{bmatrix} 5 & 0 & 0 \\ 14 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 8 & 1 & 1 \\ 18 & 4 & 2 \\ 2 & 8 & 5 \end{bmatrix} mod 27$$

Linda gets the ciphertext "GSBADHABEDDBORABEDDBADHAQTHRBADHABE" by converting the result of every elements in the operation into their letters using table 3.3. She then sends the ciphertext in addition with the key V to Thomas. Thomas decrypts the hidden message using the decryption algorithm $C - V = I$ which produces,

$$\begin{bmatrix} 7 & 1 & 1 \\ 19 & 4 & 2 \\ 2 & 8 & 5 \end{bmatrix} - \begin{bmatrix} 3 & 1 & 1 \\ 4 & 3 & 2 \\ 2 & 8 & 4 \end{bmatrix} = \begin{bmatrix} 4 & 0 & 0 \\ 15 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} mod 27$$

$$\begin{bmatrix} 4 & 15 & 1 \\ 4 & 18 & 2 \\ 2 & 0 & 5 \end{bmatrix} - \begin{bmatrix} 3 & 1 & 1 \\ 4 & 3 & 2 \\ 2 & 8 & 4 \end{bmatrix} = \begin{bmatrix} 1 & 14 & 0 \\ 0 & 15 & 0 \\ 0 & 19 & 1 \end{bmatrix} mod 27$$

$$\begin{bmatrix} 4 & 1 & 1 \\ 4 & 4 & 2 \\ 2 & 8 & 5 \end{bmatrix} - \begin{bmatrix} 3 & 1 & 1 \\ 4 & 3 & 2 \\ 2 & 8 & 4 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 15 \\ 0 & 0 & 16 \end{bmatrix} mod 27$$

$$\begin{bmatrix} 8 & 1 & 1 \\ 18 & 4 & 2 \\ 2 & 8 & 5 \end{bmatrix} - \begin{bmatrix} 3 & 1 & 1 \\ 4 & 3 & 2 \\ 2 & 8 & 4 \end{bmatrix} = \begin{bmatrix} 5 & 0 & 0 \\ 14 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} mod 27$$

Thomas then convert each element in the operation into their plaintext letters using table 3.3 leaving the elements of the identity which produces,
4→D,15→O,0→sc 14→N, 15→O, 19→T,0→sc 15→O, 16→P, 5→E, 14→N, 0→sc
and reveals the plaintext message "DO NOT OPEN" which was sent by Linda.

3.3.6 Practical Example for 3×3 singular matrix on the propose algorithm

In this example, we will consider a 3×3 singular matrix key V= $\begin{bmatrix} 2 & 1 & 1 \\ 2 & 4 & 6 \\ 1 & 2 & 3 \end{bmatrix}$ where Linda still sends the confidential message "DO NOT OPEN" to Thomas

http://dx.doi.org/10.29322/IJSRP.10.12.2020.p10837

in London. She groups the letters of the message into three letters and converts them into their numerical values using table 3.3 as
D→4,O→14,sc→0 N→13, O→14, T→19,sc→0 O→14, P→15, E→4, N→13
she gets the ciphertext using the encryption algorithm $V + I = C$ as

$$\begin{bmatrix} 2 & 1 & 1 \\ 2 & 4 & 6 \\ 1 & 2 & 3 \end{bmatrix} + \begin{bmatrix} 4 & 0 & 0 \\ 15 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 6 & 1 & 1 \\ 17 & 5 & 6 \\ 1 & 2 & 4 \end{bmatrix} mod 27$$

$$\begin{bmatrix} 2 & 1 & 1 \\ 2 & 4 & 6 \\ 1 & 2 & 3 \end{bmatrix} + \begin{bmatrix} 1 & 14 & 0 \\ 0 & 15 & 0 \\ 0 & 19 & 1 \end{bmatrix} = \begin{bmatrix} 3 & 15 & 1 \\ 2 & 19 & 6 \\ 1 & 21 & 4 \end{bmatrix} mod 27$$

$$\begin{bmatrix} 2 & 1 & 1 \\ 2 & 4 & 6 \\ 1 & 2 & 3 \end{bmatrix} + \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 15 \\ 0 & 0 & 16 \end{bmatrix} = \begin{bmatrix} 3 & 1 & 1 \\ 2 & 5 & 21 \\ 1 & 2 & 19 \end{bmatrix} mod 27$$

$$\begin{bmatrix} 2 & 1 & 1 \\ 2 & 4 & 6 \\ 1 & 2 & 3 \end{bmatrix} + \begin{bmatrix} 5 & 0 & 0 \\ 14 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 7 & 1 & 1 \\ 16 & 5 & 6 \\ 1 & 2 & 4 \end{bmatrix} mod 27$$

Linda gets the hidden message as "FQAAEBAFDCBAOSUAFDCBAAEBAUSGPAAEBAFD" which she sends to Thomas in addition with the key V. Thomas also decrypts and converts the letters in the hidden message into numerical values and then uses the decryption algorithm $C - V = I$ which he gets

$$\begin{bmatrix} 6 & 1 & 1 \\ 17 & 5 & 6 \\ 1 & 2 & 3 \end{bmatrix} - \begin{bmatrix} 2 & 1 & 1 \\ 25 & 4 & 6 \\ 1 & 2 & 3 \end{bmatrix} = \begin{bmatrix} 4 & 0 & 0 \\ 15 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} mod 27$$

$$\begin{bmatrix} 3 & 15 & 1 \\ 2 & 19 & 6 \\ 1 & 21 & 4 \end{bmatrix} - \begin{bmatrix} 2 & 1 & 1 \\ 25 & 4 & 6 \\ 1 & 2 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 14 & 0 \\ 0 & 15 & 0 \\ 0 & 19 & 1 \end{bmatrix} mod 27$$

$$\begin{bmatrix} 3 & 1 & 1 \\ 2 & 5 & 21 \\ 1 & 2 & 19 \end{bmatrix} - \begin{bmatrix} 2 & 1 & 1 \\ 2 & 4 & 6 \\ 1 & 2 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 15 \\ 0 & 0 & 16 \end{bmatrix} mod 27$$

$$\begin{bmatrix} 7 & 1 & 1 \\ 16 & 5 & 6 \\ 1 & 2 & 4 \end{bmatrix} - \begin{bmatrix} 2 & 1 & 1 \\ 2 & 4 & 6 \\ 1 & 2 & 3 \end{bmatrix} = \begin{bmatrix} 5 & 0 & 0 \\ 14 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} mod 27$$

Thomas converts every elements in this operation into their plaintext letters

http://dx.doi.org/10.29322/IJSRP.10.12.2020.p10837

leaving the elements of the identity where we gets
4→D,15→O,0→sc 14→N, 15→O, 19→T,0→sc 15→O, 16→P, 5→E, 14→N, 0→sc
and produces "DO NOT OPEN" which is the message encrypted by Linda.

4 Conclusion

In a nutshell , an algorithm has been proposed with either singular or non-singular key matrix to be used to encrypt and also decrypt document with practical examples on the proposed algorithm. Comparing the two algorithms, the proposed algorithm can be encrypted and decrypted whether the key is either singular or non-singular matrix which is an improvement or an advantage over the Hill cipher algorithm

5 Recommendation

Studies have shown that, matrices with complex entries used as key becomes a challenged when carried out using the algorithm. So we therefore recommend that further studies should be carried out to involve complex matrices with either singular or non-singular key

REFERENCES

[1] Brassard,G.(1994).Modern cryptology:A Tutorial Lecture notes in Computer Science 325,..New york: springer-verlag [2] Beutelspacher,A.(1994).Cryptology. Washinton: The Mathematical Association of America

[3] Lester,S.H(1992). Cryptography in an algebraic alphabet. The American mathematical monthly, 36:306-312

[4] Nagpau, P.B.B.-S.K.S.R.(1983). First course in Linear Algebra

[5] Overbey, J. Traves, W.and Wojdylo, J.(2005). On the key space of the Hill cipher

[6] Ismail, I. A.,Amin, M., and Diab, H. (2006). How to repair the hill cipher. Journal of zhejiang university science A ; 7: 2022-2030.

[7] Matsui, M.(1993). Linear cryptanalysis method for DES Cipher. In advances in cryptography-Eurocrypt'93.springer-verlag

http://dx.doi.org/10.29322/IJSRP.10.12.2020.p10837

Authors

First Author- Kwasi Baah Gyamfi, Kwame Nkrumah University of Science and Technology, Ghana
kwasibaahgyamfi1@gmail.com
Second Author- Kwame Owusu Bempah, University of Education Winneba,Ghana
kwamooooo30@gmail.com

Corresponding Author-Kwame Owusu Bempah, kwameowusubempah@uew.edu.gh.com

http://dx.doi.org/10.29322/IJSRP.10.12.2020.p10837