WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Use of alternate form of matrix multiplication in hill cipher algorithm

Raju W. Asole

Department of Mathematics, Late ku. Durga K. Banmeru science college Lonar, Dist- Buldhana.
Email- rajasole111@gmail.com

ABSTRACT :

The world is moving fast toward digitalisation, for this we need more strong security to restrict attacker and as we know there are some algorithms that are useful in digital security, one of them is hill cipher. Hill cipher is oldest algorithm which used matrices to encrypt the plain text but attacker can be decrypt plain text. For this we used alternate operation on matrix multiplication of order 3 rather than usual multiplication of matrices in hill cipher encryption/ decryption procedure. So in this paper we use 3*3 matrix multiplication in hill cipher algorithm, which is different than usual matrix multiplication.

Keywords : Hill cipher, new operation on matrix, encryption, decryption.

Introduction

In today's world confidential data must have to make secure and for this we use a cryptography methods. These methods ensure that our data will be safe but sometimes attackers can attacks our data and get each and every details, which is very harmful and we will loss our security. So sharing information must have been safe, for this cryptography plays a crucial role. In cryptography there are some principals, methods and algorithms which are transferring information into unintelligible information called as encryption method and then transferring that information back to intelligible information called as decryption method. One of them is Hill cipher which is invented by S. Hill in 1929, that encrypt plaintext by dividing it into blocks and transforming them using a matrix based algorithm. Here we need a matrix called as key matrix which is an invertible matrix. Sometimes choose matrix is not a invertible matrix and then decryption of plain text in hill cipher fails, but using this new introduced matrix multiplication, matrix always have inverse, so one of the problem of matrix multiplication is automatically resolved , also the hill cipher was vulnerable to know a plaintext attack since hill cipher make a linear equation of cipher text and we know linear equations can be solve easily and for this we use 3*3 matrix for plaintext rather than column matrix and another way of matrix multiplication. So in this paper we used new matrix multiplication that helpful to make massage encryption in different way and used key matrix always have inverse, hence decryption always possible.

Hill cipher

Hill cipher was developed by S. Hill which convert a plaintext into a cipher text by assigning a numbers to alphabets and use it into matrix, the assigning of numbers to alphabets is as follows :

a	b	c	d	e	f	g	h	i	J
0	1	2	3	4	5	6	7	8	9
K	l	m	n	o	p	q	r	s	T
10	11	12	13	14	15	16	17	18	19
U	v	w	x	y	z				
20	21	22	23	24	25				

Table no. 1

After assigning numbers to alphabets, Hill cipher used them in matrix and multiplied them using multiplication with mod26 (modulo 26).
The encryption and decryption of Hill cipher is as follows :
Encryption:

$$C=KPmod26$$

Where, C is cipher text, K is a key matrix (must have invertible) and P is a plain text (written in column vectors).
Decryption:

$$P=K^{-1}Cmod26$$

Where, K^{-1} is an inverse of matrix K.

Main Result

In above, Hill cipher uses usual matrix multiplication with mod 26 but sometimes we can get plaintext attacks, also one should have to notice that key matrix must have be invertible. So, to overcome this problems we use new type of matrix multiplication with modulo operation. So here first we introduced new operation on matrix multiplication of matrices with order 3.

New operation

$$let\ A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}\ and\ B = \begin{bmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{bmatrix}$$

So implies that,

$$AB = \begin{bmatrix} a_{11} + b_{11} + a_{12}b_{21} & a_{12} + b_{12} & a_{13} + b_{13} + a_{12}b_{23} \\ a_{21} + b_{21} & a_{22} + b_{22} & a_{23} + b_{23} \\ a_{31} + b_{31} + a_{32}b_{21} & a_{32} + b_{32} & a_{33} + b_{33} + a_{32}b_{23} \end{bmatrix}$$

Also inverse of matrix is given as follows :

$$A^{-1} = \begin{bmatrix} -a_{11} + a_{12}a_{21} & -a_{12} & -a_{13} + a_{12}a_{23} \\ -a_{21} & -a_{22} & -a_{23} \\ -a_{31} + a_{21}a_{32} & -a_{32} & -a_{33} + a_{23}a_{32} \end{bmatrix}$$

Propose method

Here we used a key matrix of order 3 and also plain text matrix is of order 3, also we assigning numbers to alphabets with inserting some dummy alphabets that can used during encryption and decryption methods. Before defining rules for encryption and decryption method we make a table of alphabets with some dummy letters α, β, μ, and π such that we can assign them numbers.

a	b	c	d	e	f	g	h	i	α
0	1	2	3	4	5	6	7	8	9
j	k	l	m	n	o	p	q	r	β
10	11	12	13	14	15	16	17	18	19
s	t	u	v	w	x	y	z	μ	π
20	21	22	23	24	25	26	27	28	29

Table no. 2

Here dummy letters can be place anywhere at 30 positions and can be use at space of sentences.
Now we define some rules for encryption and decryption-

ENCRYPTION:

1. First we add some dummy letters at a position of space in sentence.
2. Make a 3*3 matrix P of first 9 alphabets including dummy letters, if word has not a 9 alphabets then add dummy letters at remaining positions.
3. Assigns numbers to alphabets from table no. 2.
4. Choose any key matrix K of order 3.
5. Find matrix C, using

   C=KPmod30

   Where the matrix multiplication of K and P is should be defined as above.

6. Replace numbers from matrix C into alphabets and make a sentence of this matrix called as cipher text.
7. Repeat all 6 steps for remaining alphabets.

DECRYPTION:

1. Find an inverse of key matrix K using as defined above, denoted as K^{-1}.
2. Make 3*3 matrix C of first 9 letters including dummy letters.
3. Assigns numbers to letters in matrix C from table no. 2.
4. Find matrix P, using

   $P=K^{-1}C\text{mod}30$

   Where the matrix multiplication of K^{-1} and C is should be defined as above.
5. Replace entries of matrix P from to numbers to alphabets and make a sentence back of this matrix.
6. Remove dummy letters from this sentence and get plaintext back.
7. Repeat above steps for remaining cipher text.

We understand this procedure by taking numeric example.

Example: we apply this algorithm on plaintext ‘my new operation’.

Encryption -

1. We put α, β at position of space, so plaintext become ‘ myαnewβoperation’
2. Now choose first 9 alphabets and make a plaintext matrix.

   That is,

$$P = \begin{bmatrix} m & y & \alpha \\ n & e & w \\ \beta & o & p \end{bmatrix}$$

3. Assign numbers for each alphabets to above matrix P from table no. 2 :

$$P = \begin{bmatrix} 13 & 26 & 9 \\ 14 & 4 & 24 \\ 19 & 15 & 16 \end{bmatrix}$$

4. Now we take private key matrix $K = \begin{bmatrix} 5 & 7 & 2 \\ 8 & 1 & 4 \\ 9 & 6 & 5 \end{bmatrix}$

5. Here both P and K matrix available so our aim is now, finding a matrix C, later can be convert into ciphertext using, C=KPmod30

   So,

$$C = \begin{bmatrix} 5 & 7 & 2 \\ 8 & 1 & 4 \\ 9 & 6 & 5 \end{bmatrix} \begin{bmatrix} 13 & 26 & 9 \\ 14 & 4 & 24 \\ 19 & 15 & 16 \end{bmatrix} mod30$$

$$C = \begin{bmatrix} 5+7+7*14 & 7+26 & 9+2+7*24 \\ 8+14 & 4+1 & 4+24 \\ 9+19+6*14 & 6+15 & 5+16+6*24 \end{bmatrix} mod30$$

$$C = \begin{bmatrix} 26 & 3 & 29 \\ 22 & 5 & 28 \\ 22 & 21 & 15 \end{bmatrix}$$

6. Converting above matrix C from numbers to alphabets using table no. 2 :

$$C=\begin{bmatrix} y & d & \pi \\ u & f & \mu \\ u & t & o \end{bmatrix}$$

So we write this matrix in the form,

C=ydπufμuto ....1)

7. Successfully we convert plaintext into ciphertext but still there remains some plaintext so repeating all this steps for remaining plaintext.

Here the remaining plaintext is 'eration', but this is only seven alphabets so we add two dummy letters α and β at the end.

This implies that,

$$C=\begin{bmatrix} 5 & 7 & 2 \\ 8 & 1 & 4 \\ 9 & 6 & 5 \end{bmatrix}\begin{bmatrix} 4 & 18 & 0 \\ 21 & 8 & 15 \\ 14 & 9 & 19 \end{bmatrix} mod30$$

$$C=\begin{bmatrix} 6 & 25 & 17 \\ 29 & 9 & 19 \\ 29 & 15 & 24 \end{bmatrix}=\begin{bmatrix} g & x & q \\ \pi & \alpha & \beta \\ \pi & o & w \end{bmatrix}$$

And hence we write this matrix in the following form,

C=gxqπαβπow ....2)

From 1) and 2) we see that, ciphertext from plaintext 'my new operation' is YDπUFμUTOGXQπαβπOW.

Decryption –

1. For decryption we need inverse of key matrix so we Take a inverse of matrix K.

Since,

$$K=\begin{bmatrix} 5 & 7 & 2 \\ 8 & 1 & 4 \\ 9 & 6 & 5 \end{bmatrix}$$

$$K^{-1}=\begin{bmatrix} -5+7*8 & -7 & -2+7*4 \\ -8 & -1 & -4 \\ -9+8*6 & -6 & -5+6*4 \end{bmatrix}=\begin{bmatrix} 51 & -7 & 26 \\ -8 & -1 & -4 \\ 39 & -6 & 19 \end{bmatrix}$$

2. The ciphertext are,YDπUFμUTOGXQπαβπOW. Choosing first nine letters and make a matrix of this letters which is denoted as C.

That is,

$$C=\begin{bmatrix} y & d & \pi \\ u & f & \mu \\ u & t & o \end{bmatrix}$$

3. Now assigning numbers from table no. 2 to above matrix:

$$\mathrm{C}=\begin{bmatrix} 26 & 3 & 29 \\ 22 & 5 & 28 \\ 22 & 21 & 15 \end{bmatrix}$$

4. We have matrix C of ciphertext and inverse of key matrix so we find a matrix P using, $P=K^{-1}Cmod30$

This implies that,

$$P = \begin{bmatrix} 51 & -7 & 26 \\ -8 & -1 & -4 \\ 39 & -6 & 19 \end{bmatrix} \begin{bmatrix} 26 & 3 & 29 \\ 22 & 5 & 28 \\ 22 & 21 & 15 \end{bmatrix} mod30$$

$$P = \begin{bmatrix} 51 + 26 - 7 * 22 & -4 & 26 + 29 - 7 * 28 \\ 14 & 4 & 24 \\ 39 + 22 - 6 * 22 & 15 & 19 + 15 - 6 * 28 \end{bmatrix} mod30$$

$$P = \begin{bmatrix} 13 & 26 & 9 \\ 14 & 4 & 24 \\ 19 & 15 & 16 \end{bmatrix}$$

5. Hence we get a matrix P of plaintext. Assigning alphabets to this matrix P :

$$P = \begin{bmatrix} m & y & \alpha \\ n & e & w \\ \beta & o & p \end{bmatrix}$$

6. Writing this matrix P into the following form,

P= myαnewβop ....3)

7. Now we repeat these steps for remaining ciphertext.

The remaining ciphertext are gxqπαβπow, so we repeating all steps for this ciphertext.

$$P=K^{-1}Cmod30$$

$$P = \begin{bmatrix} 51 & -7 & 26 \\ -8 & -1 & -4 \\ 39 & -6 & 19 \end{bmatrix} \begin{bmatrix} 6 & 25 & 17 \\ 29 & 9 & 19 \\ 29 & 15 & 24 \end{bmatrix} mod30$$

$$P = \begin{bmatrix} 51 + 6 - 7 * 29 & -7 + 25 & 26 + 17 - 7 * 19 \\ -8 + 29 & -1 + 9 & -4 + 19 \\ 39 + 29 - 6 * 29 & -6 + 15 & 19 + 24 - 6 * 19 \end{bmatrix} mod30$$

$$P = \begin{bmatrix} 4 & 18 & 0 \\ 21 & 8 & 15 \\ 14 & 9 & 19 \end{bmatrix} = \begin{bmatrix} e & r & a \\ t & i & o \\ n & \alpha & \beta \end{bmatrix}$$

And hence we write this matrix in the form,

P= erationαβ ....4)

From 3) and 4) we get 'myαnewβoperationαβ', now after removing dummy letters which gives plaintext ‘my new operation’ back.

By taking above example we see that how can we convert plaintext into ciphertext and plaintext back from ciphertext.

Conclusion

In this research paper we used a new form of matrix multiplication of order 3 with module30, also we add some dummy letters between alphabets that can helpful to make more stronger encryption and decryption because we can add dummy letter anywhere from position 0 to 25 so if there are more dummy letters we have more possibilities to put them and hence this algorithm overcomes the attacks and problem of matrix inverse. Here we shown how we used different form of matrix multiplication but we can also used any another type of matrix multiplication secretly this can helpful to avoid attacks.

REFERENCES

1. Stallings, W. (2016). Cryptography and Network Security: Principles and Practice.
2. Christof Paar, Jan Pelzl (2009), Understanding Cryptography, Sringer.
3. Wenbo Mao (2003), Modern Cryptography: theory and practice, Prentice Hall.
4. J. Hoffstein, J. Pipher, J. Silverman (2008), an Introduction to Mathematical Cryptography, Sringer.
5. Katz, J., & Lindell, Y. (2020). Introduction to Modern Cryptography.
6. Bruce Schneier, (1996), Applied Cryptography: Protocols, Algorithm, and source code in C, John Wiley and sons.
7. R. W. Asole, (2025), Defines a New Operation on a Set of Matrices of Order 3 that forms a Group, IJARESM, Volume 13 Issue 4, April 2025.