RESEARCH ARTICLE OPEN ACCESS

Cryptographic Technique Used Lower and Upper Triangular Decomposition Method

B. KumaraswamyAchary, K. Rama Krishna Prasad, V. Vasu
Department of Mathematics, S.V. University, Tirupati

Abstract:
In this paper, the main cryptographic technique we will use affine cipher used for encryption and also decryption by using one of the linear algebra technique lower and upper triangular technique

Key words: Affine cipher, encryption, decryption, lower and upper triangular decomposition.

I. Introduction:

An encryption scheme or cryptosystem is a tuple (P, C, K, E, D) with the following properties.

- P is a set. It is called the plaintext space. Its elements are called plaintext.
- C is a set. It is called the cipher text space. Its elements are called cipher text.
- K is a set. It is called the key space. Its elements are called keys.

Factorization method:

This method is based on the fact that every matrix A can be expressed as the product of a lower triangular matrix and an upper triangular matrix provided al the principals minors of a are non-singular.i.e.

If A=[a$_{ij}$] then

$$a_{11} \neq 0 \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} \neq 0, \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{32} \end{vmatrix} \neq 0 etc$$

Also such a factorization if it exists, is unique. Now consider the equations.

$$a_{11}x_1 + a_{12}x_2 + a_{13}x_3 = b_1$$

$$a_{21}x_1 + a_{22}x_2 + a_{23}x_3 = b_2$$

$$a_{31}x_1 + a_{32}x_2 + a_{33}x_3 = b_3$$

Which can be written as AX=B where

$$A = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix}, X = \begin{vmatrix} x_1 \\ x_2 \\ x_3 \end{vmatrix}, B = \begin{vmatrix} b_1 \\ b_2 \\ b_3 \end{vmatrix}$$

Let A= LU

Where $L = \begin{vmatrix} 1 & 0 & 0 \\ l_{21} & 1 & 0 \\ l_{31} & l_{32} & 1 \end{vmatrix}$ and $U = \begin{vmatrix} u_{11} & u_{12} & u_{13} \\ 0 & u_{22} & u_{23} \\ 0 & 0 & u_{33} \end{vmatrix}$

Then (1) becomes LUX=B

Writing UX=V$_1$

(3) Becomes LV=B which is equivalent to the equations

V$_1$=b$_1$:l$_2$V$_1$+V$_2$=b$_2$:l$_{31}$v$_1$+l$_{32}$v$_2$+v$_3$=b$_3$

Solving these for V$_1$, V$_2$, V$_3$ we know V$_1$ then

(4) Becomes

U$_{11}$X$_1$+U$_{12}$X$_2$+U$_{13}$X$_3$=V$_{11}$U$_{22}$X$_2$+U$_{23}$X$_3$=V$_{21}$

$U_{33}X_3=V_3$

From which x_3,x_2 and x_1 can be found by back-substitution. To compute matrices L and U, we write (2) as

$$\begin{vmatrix} 1 & 0 & 0 \\ l_{21} & 1 & 0 \\ l_{31} & l_{32} & 0 \end{vmatrix} \begin{vmatrix} u_{11} & u_{12} & u_{13} \\ 0 & u_{22} & u_{23} \\ 0 & 0 & u_{33} \end{vmatrix} = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix}$$

Multiplying the matrices on the left and equating corresponding elements from both sides, we obtain

i) $U_{11}=a_{ll}$, $u_{12}=a_{12}$, $u_{13}=a_{13}$.

ii) $L_{21}u_{11}=a_{21}$ (or) $l_{21}=a_{21}/a_{11}$.

$L_{31}u_{11}=a_{31}$ (or) $l_{31}=a_{31}/a_{ll}$.

iii) $L_{21}u_{21}+u_{22}=a_{22}$ (or) $u_{22}=a_{22}-a_{21}/a_{ll}\ a_{12}$.

$L_{21}u_{13}+u_{23}=a_{23}$ (or) $u_{23}=a_{23}-a_{21}/a_{11}a_{13}$.

iv) $L_{31}u_{13}+l_{32}u_{22}=a_{32}$ (or) $l_{32}=1/u_{22}\ [a_{32}-a_{31}/a_{11}\ a_{12}]$

v) $L_{31}u_{13}+l_{33}u_{23}=a_{33}$ (or) which gives u_{33}.

Thus we compute the elements of L and U in the following set order.

i) First row of U.

ii) First row of L.

iii) Second row of U_1

iv) Second row of L_1

v) Third row of U_1

This procedure can easily be generalized.

Affine cipher:

The encryption process:

In fact, we can summarizethe encryption which is the process of converting plaintext into cipher text in the following steps.

a. Choose an (mxm) matrix A=LU which is invertible, where 'm' have may be depends on the length of the message that needs to be encrypted.

b. Change each plain text to its numerical values, by using the table below.

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

c. Form the (mx1) column vector P, having these numerical values as its entries.

d. Get each ciphertext vector C by multiplying A=LU with P and connect each entry of the ciphertext vector to its letter in the alphabet where L is lower triangular matrix and U is upper triangular matrix.

The encryption algorithm of this method is C=LUP mod N.

Where C is the column vector of the numerical values of ciphertext, P is the column vector of the numerical values of the plaintext, LU AN (mxm) matrix, is the key of the algorithm (this matrix must be invertible because are need the inverse of this matrix for the decryption process) and N is the number of letters of the alphabet used in the cryptography the decryption process:

The decryption which is the process of converting the cipher text into plaintext could also be summarized in the following steps:

a. Get the inverse of the matrix LU: say $(LU)^{-1}$.

b. Change each ciphertext to its numerical values.

c. Put each ciphertext in (mx1) column vector say C.

d. Get each plaintext vector by multiplying $(LU)^{-1}$ with C, and connect each plaintext vector to its letter in the alphabet. The decryption algorithm of this method is P≡ $(LU)^{-1}$ mod N. where $(LU)^{-1}$ is the inverse of the matrix LU.

In general, if A= LU

Where $L=\begin{bmatrix}1 & 0 & 0\\ l_{21} & 1 & 0\\ l_{31} & l_{32} & 1\end{bmatrix} U=\begin{bmatrix}u_{11} & u_{12} & u_{13}\\ 0 & u_{22} & u_{23}\\ 0 & 0 & u_{33}\end{bmatrix}$

And $P=\begin{bmatrix}P_{11}\\ \dots\\ P_{u1}\end{bmatrix}$ then in the encryption process, we get C= LUP mod N.

$$\Rightarrow\begin{bmatrix}C_{11}\\ \dots\\ C_{u1}\end{bmatrix}=\begin{bmatrix}1 & 0 & 0\\ l_{21} & 1 & 0\\ l_{31} & l_{32} & 1\end{bmatrix}\begin{bmatrix}u_{11} & u_{12} & u_{13}\\ 0 & u_{22} & u_{23}\\ 0 & 0 & u_{33}\end{bmatrix}\begin{bmatrix}p_{11}\\ \dots\\ p_{nn}\end{bmatrix}$$

Here when the size of the matrix A increases, or in other words when increases we will have the following advantages.

1. The cryptography process will be more complex and more difficult to decode.
2. The number of column vectors will decreases and we can encode any message consisting for example of 7 letters by using A(7x7) matrix in only one step. But there is one problem here, that is, it's not easy to get the inverse of the matrix used in the encryption process as n increases.

Below, we give several other ways of using affine cipher technique for encryption.

We can use the affine cipher technique to make the hill cipher more complex encryption algorithm here is given as

C=LUP+B (mod N)

$$\begin{pmatrix}c_{11}\\ \dots\\ c_{n1}\end{pmatrix}=\begin{pmatrix}1 & 0 & 0\\ l_{21} & 1 & 0\\ l_{31} & l_{32} & 1\end{pmatrix}\begin{pmatrix}u_{11} & u_{12} & u_{13}\\ 0 & u_{22} & u_{23}\\ 0 & 0 & u_{33}\end{pmatrix}+\begin{pmatrix}b_{11} & \dots & b_{1n}\\ \dots & \dots & \dots\\ b_{n1} & \dots. & b_{nn}\end{pmatrix}$$

Where A=LU is an invertible matrix and B is a column vector like the vectors C and P.

For the decryption

$P=LU^{-1}C-LU^{-1}B= LU^{-1}(C-B)$ (mod N)

Example 1: Encode the message (welcome) by using affine cipher algorithm where the matrix is

$$A=\begin{pmatrix}4 & 1\\ 2 & 3\end{pmatrix}$$

Sol: First use the table below to convert letters in the message to their numerical values.

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

Put also number O for the space between words. Group the plaintext letters into pairs and add O to fill out the last pairs.

W	E	L	C	O	M	E		T	O	
25	7	14	5	17	15	7	0	22	17	0

$$A=\begin{bmatrix}4 & 1\\ 2 & 3\end{bmatrix}=\begin{bmatrix}1 & 0\\ l_{21} & 1\end{bmatrix}\begin{bmatrix}U_{11} & U_{12}\\ 0 & U_{22}\end{bmatrix}=\begin{bmatrix}U_{11} & U_{12}\\ l_{21}U_{11} & l_{21}U_{12}+U_{22}\end{bmatrix}$$

U_{11}=4 V_{12}=1, $L_{21}U_{12}+U_{22}$=3
$L_{21}U_{11}$=2 ½ 1+V_{22}=3
L_{21}=2/4=1/2 V_{22}=3-1/2=5/2

$$L=\begin{bmatrix}1 & 0\\ 1/2 & 0\end{bmatrix},\ U=\begin{bmatrix}4 & 1\\ 0 & 5/2\end{bmatrix}$$

$$C=LUB(\mathrm{mod}\,26)$$

$$C_1=\begin{bmatrix}1 & 0\\ 1/2 & 0\end{bmatrix}\begin{bmatrix}4 & 1\\ 0 & 5/2\end{bmatrix}\begin{bmatrix}25\\ 7\end{bmatrix}=\begin{bmatrix}3\\ 19\end{bmatrix}(\mathrm{mod}\,26)$$

$$C_2=\begin{bmatrix}1 & 0\\ 1/2 & 0\end{bmatrix}\begin{bmatrix}4 & 1\\ 0 & 5/2\end{bmatrix}\begin{bmatrix}14\\ 5\end{bmatrix}=\begin{bmatrix}9\\ 17\end{bmatrix}(\mathrm{mod}\,26)$$

$$C_3=\begin{bmatrix}1 & 0\\ 1/2 & 0\end{bmatrix}\begin{bmatrix}4 & 1\\ 0 & 5/2\end{bmatrix}\begin{bmatrix}17\\ 15\end{bmatrix}=\begin{bmatrix}5\\ 1\end{bmatrix}(\mathrm{mod}\,26)$$

$$C_4=\begin{bmatrix}1 & 0\\ 1/2 & 0\end{bmatrix}\begin{bmatrix}4 & 1\\ 0 & 5/2\end{bmatrix}\begin{bmatrix}7\\ 0\end{bmatrix}=\begin{bmatrix}2\\ 14\end{bmatrix}(\mathrm{mod}\,26)$$

$$C_5=\begin{bmatrix}1 & 0\\ 1/2 & 0\end{bmatrix}\begin{bmatrix}4 & 1\\ 0 & 5/2\end{bmatrix}\begin{bmatrix}22\\ 17\end{bmatrix}=\begin{bmatrix}1\\ 17\end{bmatrix}(\mathrm{mod}\,26)$$

Now the message becomes

3	19	9	17	5	1	2	14	1	17
A	W	G	O	C	Y	Z	L	Y	O

Example 2: Encoding the message (Application of Mathematics)

$$a=\begin{pmatrix}3 & 2 & 7\\ 2 & 3 & 1\\ 3 & 4 & 1\end{pmatrix}$$

Let $A=UL=\begin{pmatrix}1 & 0 & 0\\ l_{21} & 1 & 0\\ l_{31} & l_{32} & 1\end{pmatrix}\begin{pmatrix}u_{11} & u_{12} & u_{13}\\ 0 & u_{22} & u_{23}\\ 0 & 0 & u_{33}\end{pmatrix}$

$$\Rightarrow\begin{bmatrix}3 & 2 & 7\\ 2 & 3 & 1\\ 3 & 4 & 1\end{bmatrix}=\begin{bmatrix}1 & 0 & 0\\ l_{21} & 1 & 0\\ l_{31} & l_{32} & 1\end{bmatrix}\begin{bmatrix}u_{11} & u_{12} & u_{13}\\ 0 & u_{22} & u_{23}\\ 0 & 0 & u_{33}\end{bmatrix}$$

So that

(i) U_{11}=3, U_{12}= 2, U_{13}=7
(ii) $L_{21}U_{11}$=2, $L_{31}U_{11}$=3, L_{21}=2/3
L_{31}=1
(iii) $L_{21}U_{12}+U_{22}$=3, $L_{21}U_{13}+U_{23}$=1
V_{22}=5/3 U_{23}=11/3
(iv) $L_{31}U_{12}+L_{32}U_{22}$=4
L_{32}=6/5
(v) $L_{31}U_{13}+L_{32}U_{23}+U_{33}$=1
U_{33}=-8/5

Thus $A = LV = \begin{bmatrix} 1 & 0 & 0 \\ 2/3 & 1 & 0 \\ 1 & 6/5 & 1 \end{bmatrix}\begin{bmatrix} 3 & 2 & 7 \\ 0 & 5/3 & -11/3 \\ 0 & 0 & -8/5 \end{bmatrix}$

Application of Mathematics
3 18 18 14 11 3 22 11 17 16 178 15 3 22 10 7 15 3 22 11 5 2 1
C=LUP mod M

$$C_1 = \begin{bmatrix} 1 & 0 & 0 \\ 2/3 & 1 & 0 \\ 1 & 6/5 & 1 \end{bmatrix}\begin{bmatrix} 3 & 2 & 7 \\ 0 & 5/3 & -11/3 \\ 0 & 0 & -8/5 \end{bmatrix}\begin{bmatrix} 3 \\ 18 \\ 18 \end{bmatrix} = \begin{bmatrix} 15 \\ 0 \\ 21 \end{bmatrix} \pmod{26}$$

$$C_2 = \begin{bmatrix} 1 & 0 & 0 \\ 2/3 & 1 & 0 \\ 1 & 6/5 & 1 \end{bmatrix}\begin{bmatrix} 3 & 2 & 7 \\ 0 & 5/3 & -11/3 \\ 0 & 0 & -8/5 \end{bmatrix}\begin{bmatrix} 14 \\ 11 \\ 5 \end{bmatrix} = \begin{bmatrix} 21 \\ 14 \\ 13 \end{bmatrix} \pmod{26}$$

$$C_3 = \begin{bmatrix} 1 & 0 & 0 \\ 2/3 & 1 & 0 \\ 1 & 6/5 & 1 \end{bmatrix}\begin{bmatrix} 3 & 2 & 7 \\ 0 & 5/3 & -11/3 \\ 0 & 0 & -8/5 \end{bmatrix}\begin{bmatrix} 3 \\ 22 \\ 11 \end{bmatrix} = \begin{bmatrix} 0 \\ 5 \\ 4 \end{bmatrix} \pmod{26}$$

$$C_4 = \begin{bmatrix} 1 & 0 & 0 \\ 2/3 & 1 & 0 \\ 1 & 6/5 & 1 \end{bmatrix}\begin{bmatrix} 3 & 2 & 7 \\ 0 & 5/3 & -11/3 \\ 0 & 0 & -8/5 \end{bmatrix}\begin{bmatrix} 17 \\ 16 \\ 17 \end{bmatrix} = \begin{bmatrix} 20 \\ 21 \\ 2 \end{bmatrix} \pmod{26}$$

$$C_5 = \begin{bmatrix} 1 & 0 & 0 \\ 2/3 & 1 & 0 \\ 1 & 6/5 & 1 \end{bmatrix}\begin{bmatrix} 3 & 2 & 7 \\ 0 & 5/3 & -11/3 \\ 0 & 0 & -8/5 \end{bmatrix}\begin{bmatrix} 8 \\ 15 \\ 3 \end{bmatrix} = \begin{bmatrix} 23 \\ 12 \\ 9 \end{bmatrix} \pmod{26}$$

$$C_6 = \begin{bmatrix} 1 & 0 & 0 \\ 2/3 & 1 & 0 \\ 1 & 6/5 & 1 \end{bmatrix}\begin{bmatrix} 3 & 2 & 7 \\ 0 & 5/3 & -11/3 \\ 0 & 0 & -8/5 \end{bmatrix}\begin{bmatrix} 22 \\ 10 \\ 7 \end{bmatrix} = \begin{bmatrix} 5 \\ 3 \\ 9 \end{bmatrix} \pmod{26}$$

$$C_7 = \begin{bmatrix} 1 & 0 & 0 \\ 2/3 & 1 & 0 \\ 1 & 6/5 & 1 \end{bmatrix}\begin{bmatrix} 3 & 2 & 7 \\ 0 & 5/3 & -11/3 \\ 0 & 0 & -8/5 \end{bmatrix}\begin{bmatrix} 15 \\ 3 \\ 22 \end{bmatrix} = \begin{bmatrix} 23 \\ 9 \\ 1 \end{bmatrix} \pmod{26}$$

$$C_8 = \begin{bmatrix} 1 & 0 & 0 \\ 2/3 & 1 & 0 \\ 1 & 6/5 & 1 \end{bmatrix}\begin{bmatrix} 3 & 2 & 7 \\ 0 & 5/3 & -11/3 \\ 0 & 0 & -8/5 \end{bmatrix}\begin{bmatrix} 11 \\ 5 \\ 21 \end{bmatrix} = \begin{bmatrix} 8 \\ 20 \\ 22 \end{bmatrix} \pmod{26}$$

The new message becomes

15	0	21	21	14	13	0
M	X	S	S	L	K	K
5	4	20	21	2	23	12
C	B	R	S	Z	U	J
9	5	3	9	23	9	1
G	C	A	G	Y	G	Y
8	20	22				
F	R	T				

Example 3: Decode the message SNOITAUQE RAENIL by using Caesar cipher algorithm and the inverse of the matrix

$$A=\begin{bmatrix}3 & -2 & -1\\ -4 & 1 & -1\\ 2 & 0 & 1\end{bmatrix}$$

Solution:

21	16	17	14	22	3	23	
S	N	O	I	T	A	U	
19	7	20	3	7	16	11	14
W	E	R	A	E	N	I	L

$$A=LU=\begin{bmatrix}1 & 0 & 0\\ l_{21} & 1 & 0\\ l_{31} & l_{32} & 1\end{bmatrix}\begin{bmatrix}u_{11} & u_{12} & u_{13}\\ 0 & u_{22} & u_{23}\\ 0 & 0 & u_{33}\end{bmatrix}$$

So that

i. $U_{11}=3$, $U_{12}= -2$, $U_{13}=-1$

ii. $L_{21}U_{11}=-4$, $L_{21}U_{12}+U_{22}=1$, $L_{21}U_{13}+U_{23}=-1$
$L_{21}=-4/3$ $U_{22}=-5/3$ $U_{23}=-7/3$

iii. $L_{31}U_{11}=2$ $L_{31}U_{12}+L_{32}U_{22}=0$
$L_{31}=2/3$ $2/3-2+5/3L_{33}=0$
$L_{32}=-4/5$

iv. $L_{31}U_{13}+L_{32}U_{23}+U_{33}=1$
$2/3(-1)+-4(-7/5)+U_{33}=1$
$-2/3+28/5+U_{33}=1$
$U_{33}=-69/5$

$$L=\begin{bmatrix}1 & 0 & 0\\ -4/3 & 1 & 0\\ 2/3 & -4/5 & 1\end{bmatrix}U=\begin{bmatrix}3 & -2 & -1\\ 0 & -5/3 & -7/3\\ 0 & 0 & -59/15\end{bmatrix}$$

P= $(LU)^{-1}$ mod26

$$P_1=\begin{pmatrix}1 & 2 & 3\\ 2 & 5 & 7\\ -2 & -4 & -5\end{pmatrix}\begin{pmatrix}21\\ 16\\ 17\end{pmatrix}=\begin{pmatrix}0\\ 7\\ -9\end{pmatrix}\mathrm{mod}\,26=\begin{pmatrix}0\\ 7\\ 17\end{pmatrix}$$

$$P_2=\begin{pmatrix}1 & 2 & 3\\ 2 & 5 & 7\\ -2 & -4 & -5\end{pmatrix}\begin{pmatrix}14\\ 22\\ 3\end{pmatrix}=\begin{pmatrix}15\\ 3\\ -1\end{pmatrix}\mathrm{mod}\,26=\begin{pmatrix}15\\ 3\\ 25\end{pmatrix}$$

$$P_3=\begin{pmatrix}1 & 2 & 3\\ 2 & 5 & 7\\ -2 & -4 & -5\end{pmatrix}\begin{pmatrix}23\\ 19\\ 7\end{pmatrix}=\begin{pmatrix}4\\ 8\\ -1\end{pmatrix}\mathrm{mod}\,26=\begin{pmatrix}4\\ 8\\ 25\end{pmatrix}$$

$$P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 5 & 7 \\ -2 & -4 & -5 \end{pmatrix} \begin{pmatrix} 20 \\ 3 \\ 7 \end{pmatrix} = \begin{pmatrix} 21 \\ 24 \\ -9 \end{pmatrix} \bmod 26 = \begin{pmatrix} 21 \\ 24 \\ 17 \end{pmatrix}$$

$$P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 5 & 7 \\ -2 & -4 & -5 \end{pmatrix} \begin{pmatrix} 16 \\ 11 \\ 14 \end{pmatrix} = \begin{pmatrix} 2 \\ 3 \\ -16 \end{pmatrix} \bmod 26 = \begin{pmatrix} 2 \\ 3 \\ 10 \end{pmatrix}$$

The remaining values are

0	7	17	15	3	25
A	E	O	M	A	W
4	8	25	21	24	17
B	F	W	J	V	O
2	3	10			
Z	A	H			

The new message

AEOMAW BFW SVO ZAH

References:

[1] Charles C. Pinter A Book of Abstract algebra second edition
[2] Higher engineering mathematic khanna publishers by Dr. B.S. Grewal 40th edition
[3] Joseph A Gallian contemporary abstract algebra sixth edition 2006
[4] P.B. Bhattachary SK Jain S.R. Nagpaul First course in Linear Algebra 1983