A Composite key using Division Algorithm and Matrix Inversion in Symmetric Key Encryption

Shriram B. Patil
Nirmala Memorial Foundation College of Commerce and Science, Thakur Complex, Kandivali (East),
Mumbai 400101.

Abstract

In communication system no one should hack or modify the sent information with malicious intentions. One can obtain security in transformation using cryptography techniques. Many of the variants of algorithm such as stream cipher or block cipher use symmetric and public keys. Stream cipher technique involves encryption and decryption of one byte at a time. Block cipher techniques encrypts block of text at a time. The usual size in block cipher is 64, 128 or 256 bits where as in stream cipher it is 8 bits. In this paper, an invertible matrix (block cipher) is composed with division algorithm (stream cipher) based symmetric key encryption algorithm designed in DASKEA [5]. The sent message is encrypted twiceusing composition of stream and block cipher. This increases complexity of decrypting original message. The algorithm is based on matrix equation Ax = b, where A is square integer matrix of size n, defined over Z, the set of integers and is invertible over Z , x is a message vector. Matrix A acts on message x to get encrypted message b. The decrypted message is obtained by acting A^{-1}on message b and gives back original message x. Message is divided into group g of n characters. If the message length is not multiple of n then message is padded with some special character which is not used as a character in message so that length is multiple of n. Each character is mapped onto unique integer. Group is taken as column vector g of integers. Matrix A acts on g and then encode it as A.g = b, a process of block cipher. On each element of b, encryption procedure defined in DASKEA [5] is applied, a process of stream cipher. The message is encrypted as E, a combination of block and stream cipher. Reverse process of decryption in DASKEY and then followed by matrix inversion gives original message.

Key words - *Division algorithm, Cryptography, Symmetric key, Secret key, Asymmetric key, Public key, Stream cipher, Block cipher, Encryption, Decryption, Integer matrix, Inverse of matrix.*

I. MATHEMATICAL PRELIMINARIES

A. Factorial and Combination

If n is non negative integer then factorial of n denoted by n! is defined as

n! = 1 if n=0
= n(n-1)...3.2.1 if n $\geq$ 1.
Note That 0! = 1! = 1, 5! = 5.4.3.2.1=120.

Combination :nCr is the number of combinations of n objects taken r at a time.
Note that n C 0 = 1
5 C 3 = 5! / (3!(5-3)!) = 1.2.3.4.5 / (1.2.3.(1.2)) = 5.4.3 / 1.2.3 = 10
For n $\geq$1, n C r is product of r numbers starting from n in decreasing order divided by factorial r. i.e.
n C r = n.(n-1).(n-2) ... (n-r+1) / r!
For example, 11 C 5 = (11.10.9.8.7) / (1.2.3.4.5) = 462

B. Function

Let A, B, C be any three sets.
A function I: A->A is identity function on A if
I(x) = x for all x in A.
Let f: A -> B and g: B -> C be functions then the function gof: A -> C is a composite of two functions f and g defined by gof(x) = g(f(x), x Ɛ A.

A function f: A -> B is said to be invertible if there exists a function g: B -> A such that
fog = gof = I where I is identity function
Let f: A -> B and g: B -> C be invertible functions then the composite function gof: A -> C is invertible and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$

C. Integer matrix and matrix equation

Matrix is called integer matrix if all its entries are integers.
Identity matrix has main diagonal elements 1 and all other elements 0.

For example $I = \begin{pmatrix} 10 & 0 & \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

is identity matrix oforder 3.
Row vector $x_1,x_2,...x_n$ will be represented by
($x_1,x_2,...x_n$) and Column vector $x_1,x_2,...x_n$ will be represented by [$x_1,x_2,...x_n$].

A square integer matrix A is said to be invertible or non singular if there exists integer matrix B such that
A B = I = B A where I is identity matrix.

The inverse of an integer matrix is an integer matrix if and only if the determinant of the matrix is ±1.

Consider a matrix equation
A x = b ………………………… (1)
where A is n x n integer non singular matrix , x and b are column vectors having n elements.
The solution of matrix equation (1) is given by
x = A^{-1} b. …………………………… (2)
Here A^{-1} is integer matrix.

Division Algorithm: Given any two non negativeintegers m and n there exists unique integers q and r such that
n = qm + r , 0 ≤ r < m
For example, for n = 5088, m = 91, q = 55 and r =83.

D. Construction of invertible integer matrix

We shall use the construction of integer matrix as given in Ericsen [6].
Let (i,j) th entry of a matrix A be A(i, j). For an arbitrary nonnegative integer n ,
Define A(i,j) = (n+j-1) C (i-1)

Example 1. Let n=11,
A(1,1) = (11+1-1) C (1-1) = 11 C 0 = 1
A(1,2) = (11+2-1) C (1-1) = 12 C 0 = 1
A(1,3) = (11+3-1) C (1-1) = 13 C 0 = 1
A(2,1) = (11+1-1) C (2-1) = 11 C 1 = 11
A(2,2) = (11+2-1) C (2-1) = 12 C 1 = 12
A(2,3) = (11+3-1) C (2-1) = 13 C 1 = 13
A(3,1) = (11+1-1) C (3-1) = 11 C 2
= 11.10/1.2 = 55
A(3,2) = (11+2-1) C (3-1) = 12 C 2 = 12.11 /1.2 = 66
A(3,3) = (11+3-1) C (3-1) = 13 C 2 = 13.12 /1.2 = 78

$$A = \begin{pmatrix} 1 & 11 \\ 111213 & \\ 55 & 6678 \end{pmatrix} \text{ and } A^{-1} = \begin{pmatrix} 78 & -12 & 1 \\ -143 & 23 & -2 \\ 66 & -11 & 1 \end{pmatrix}$$

II. INTRODUCTION

In a communication system the secrecy of data is very important between sender and receiver. The data to be transmitted over communication channel can be in text, audio, image, video or audio-visual form. The data in communication system must be known to sender and receiver only. The security requirements such as Authentication, Privacy, Integrity and Non-repudiationcan be addressed through cryptography which will protect data from theft or alteration and for user authentication.
The following terminologies are commonly used in the context of Cryptography.

The data transmitted between sender and receiver be readable and uninterpretable over channel. The original data (M) sent by sender is in human readable plain text form. On the transmission medium it is changed to uninterpretable or encrypted form called a cipher text (C).

A sequence of bits called key (K) is used to configure cipher text. The process of converting plain text into cipher text is called encryption (E) and the inverse process of converting cipher text into plain original text is called decryption process (D).If the same key is used at sender and receiver end it is called symmetric or secret key otherwise it is called asymmetric key. Asymmetric key used for encrypting text is called a public key and at receiver end to decrypt cipher text is called a private key.Thus,

Original E:EncryptMD: Decrypt C
Message -------------→ Cypher Text---------→ M
M C

Cryptography is making of secret codes, Cryptanalysis is breaking of secret codes and Cryptology is making and breaking of secret codes. Cipher/Cryptosystem is a function forencryptingand decrypting data.The literature on cryptography can be found in [1],[2],[3]and [4].If single key is used for both encryption and decryption it is called Secret Key Cryptography or Symmetric Key Cryptography (SKC). If two distinct keys are used for encryption and decryption it is called Public Key Cryptography (PKC). Hash Functions uses a mathematical transformation to irreversibly "encrypt" information.

In a secret key cryptography, a single key is used for both encryption and decryption. Secret key cryptography schemes are either stream ciphers or block ciphers. Stream ciphers operate on a single bit (byte or computer word) at a time and implement some form of feedback mechanism so that the key is constantly changing whereas in block cipher scheme it encrypts one block of data at a time using the same key on each block. In general, the same plaintext block will encrypt to different cipher text in a stream cipher.

A. Block and Stream ciphers

A block cipher converts block of plain text into encrypted text. This concept is explained in [7] by

Menezes. It uses a fixed size of 64 bits, 128 bits and 256 bits at one time. DES [Data Encryption Standard], Triple DES, AES [Advanced Encryption Standard], IDEA [International Data Encryption Algorithm] and Blowfish are some of the commonly used encryption algorithms that fall under block cipher type[9].

A stream cipher converts 1 bit or 8 bits of plaintext into cipher text at a time. Pseudorandom bits is the key, it is unpredictable and is never reused. **RC4** [Rivest Cipher 4] is the most widely used technique for stream ciphers

B. Attacks

The purpose of attack is to discover the key used in the process of ciphering and deciphering. A Survey article by Gustavo Banegas [9] discusses attacks in stream cipher. The attacks discussed are mainly Exhaustive Search, Algebraic, Correlation, Fault, Distinguishing,Chosen-IV, Slide, Cube, Time-Memory Trade-off and Guess & Determine.

Most of the attacks are on either block cipher or stream cipher but not on both. Hence design of algorithm which uses both ciphers is a solution to increase complexity in deciphering the text. The keys used for block and stream cipher is very large and hence finding a key from such infinite set is very difficult. One may consider finite fields say Z_p, p is prime, the residue classes of integers modulo p or Galois field for ciphering text.

In this paper we shall consider arbitrary integer invertible square matrix of size n for block cipher. Each column of the matrix is a block of text of length n. If integer is 16 bits long, we can encrypt block of n integers into 16n bits long. If the matrix is chosen where n = 4, block cipher is 64 bits long. For n=4,8,16 we obtain standard block ciphers of length 64, 128 or 256 bits. However no restriction is puton the value of n. If long integers are used, we take integer as 4 bytes long.

III. DIVISION ALGORITHM BASED SYMMETRIC KEY ENCRYPTION ALGORITHM

In this section, Division Algorithm based Symmetric Key Encryption AlgorithmDASKEA [5] isexplainedwith an example. .

A. Encryption Procedure :

String DAEncrypt(n, k, m :n, k and m arepositive integers)

Example 2 :Using Decimal Number System

Encryptionprocedure :

```
String DAEncrypt(n,k,m: n,k,m are integers)
Let y and z be string.
Let z = DAEncrypt (910,91,2)
1 .Here n=910, k=91and m = 2.
2.  Applying Division Algorithm to n and k, we
     obtain two integers q and r such that $n = q * k + r$,
where $0 \leq r < k$.
910=10*91+0
     Here q=10, and r = 0.
4.  Consider each q and r as m=2 digit number
     q = 10 and r = 00  are2 digit numbers as string
5.  Form new number string y
     y = {digits in r} concatenate  {digits in q}
     y =”0010”
6.   y is a cipher text
7. Return y
```

Decryption procedure:

```
Integer DADecrypt(String y, k, m :  k, m are positive integers)
Let pand z be integer and
p = DADecrypt("0010",91,2)
Here y="0010", k=91 and m =2.
1. Let q1 and r1 be respectively the last and first  m
digits in y. Hence, q1 = "10", r1 = "00"
   Convert q1, r1 into integers q and r to get  q=10
and r =0
2. Let  $z = q * k + r = 10*91+0 = 910$
3. Return z
```

B. Encryption and Decryption using Integer MatrixEquation [EDIME]

Suppose plain textT is to be transmitted from sender S to receiver R. Assume that text contains alphanumeric and some special characters.

We define set of digits

D = {0,1,2,3,4,5,6,7,8,9 } ,

alphabets α = { A,B,C,D,E,F,G,H,I,J,K,L,M,N,O,P,Q,R,S,T,U,V,W,X, Y,Z, a,b,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u,v,w,x,y,z} and some special characterset

S ={~,!, @, #, $, %, &, *, ? } for forming a message and let $\sum = D \cup \alpha \cup S$.

Total number of characters that can be used for message will be 71 i.e. 10 digits, 52 alphabets and9 special characters.These characters will be coded as given in table 1.

Char	0	1	2	3	4	5
Code	0	1	2	3	4	5
Char	6	7	8	9	A	B
Code	6	7	8	9	10	11
Char	C	D	E	F	G	H
Code	12	13	14	15	16	17
Char	I	J	K	L	M	N

Code	18	19	20	21	22	23
Char	O	P	Q	R	S	T
Code	24	25	26	27	28	29
Char	U	V	W	X	Y	Z
Code	30	31	32	33	34	35
Char	*	a	b	c	d	e
Code	36	37	38	39	40	41
Char	f	g	h	i	j	k
Code	42	43	44	45	46	47
Char	l	m	n	o	p	q
Code	48	49	50	51	52	53
Char	r	s	t	u	v	w
Code	54	55	56	57	58	59
Char	x	y	z	!	@`	#
Code	60	61	62	63	64	65
Char	$	%	^	&	~	?
Code	66	67	68	69	70	71

Table 1

C. EDIME Algorithm:

This algorithm uses block cipher technique. Suppose a message s is to be sent over communication channel using character set ∑. Let A be invertible integer matrix so that inverse of A i.e. A^{-1} is also an integer matrix. The message s will be converted into integer code y using Table 1. y is encrypted by matrix A. Let Ay = b. Therefore b is block cipher text or encrypted message. Encrypted message b is received by receiver. Thus sender sends message s and is block ciphered as or encrypted as b. At the receiver end b will be decrypted by A^{-1} to obtain original message s.
This means if ·A s = b then s = A^{-1}b.
Diagrametically,

E:EncryptionD:Decryption

$$s \xrightarrow{\qquad} Ax = b \xrightarrow{\qquad} s = A^{-1} b$$

Block cipher

String EDIME(String E, S,Encoding matrix A, n)
{E and Sare strings, A and A^{-1} arenxn integer matrices

```
    E = MEncrypt(String S, Matrix A,n)
  S = MDecrypt (String E, Matrix A^-1 )
   }
```

Example 3.
String MEncrypt(Strings, Matrix A,n)
Let t be string.
t = MEncrypt("ITS3*MOS*", Matrix A, 3)
1. Message s is "ITS3*MOS*"
2. Let A be 3x3 invertible integer matrix as defined abovein Ic.

$$A = \begin{pmatrix} 1 & 11 & \\ 11 & 12 & 13 \end{pmatrix} \quad A^{-1} = \begin{pmatrix} 78 & -12 & 1 \\ -143 & 23 & -2 \end{pmatrix}$$

55 6678 66 -11 1

3. Since A has 3 columns, we break the message into groups of 3 characters from left to right.
i.e. s will be broken as "ITS", "3*M", "OS*"
i.e. s ={s1,s2,s3}.
Each character is now replaced by codes defined in Table 1.With this
s1="ITS"="18 29 28",s2="3*M"
= "3 36 22" and s3="OS*" = "24 28 36".
Note that blank spacesare inserted for readability.
Let y1=[18 29 28], y2 = [3 36 22] and
y3 = [24 28 36] be integer column vectors obtained from s1,s2 and s3 respectively.
4. Each y1,y2,y3 will be encrypted by matrix A
The message "ITS" = "18 29 28" will be encrypted as Ay1

$$Ay1 = \begin{pmatrix} 11118 & 75 \\ 11121329 & \\ 55667828 & \end{pmatrix} = \begin{pmatrix} 910 & = \\ 5088 & \end{pmatrix} \begin{pmatrix} b1 \end{pmatrix}$$

Similarly we calculate b2 and b3.

$$A\ y2 = \begin{pmatrix} 1113 & 61 \\ 1112 & 13 \\ 5566 & 78 \end{pmatrix} \begin{pmatrix} 36 \\ 22 \end{pmatrix} = \begin{pmatrix} 751 \\ 4257 \end{pmatrix} = b2$$

$$A\ y3 = \begin{pmatrix} 11 & 124 \\ 111213 & 28 \\ 556678 & 36 \end{pmatrix} = \begin{pmatrix} 88 \\ 1068 \\ 5976 \end{pmatrix} = b3$$

Column vectors b1, b2 and b3 are block ciphers or encrypted messages for "ITS","3*M" and "OS*" respectively.

$$\text{Let } Y = (y1\ y2\ y3) = \begin{pmatrix} 18 & 324 \\ 29 & 3628 \\ 28 & 2236 \end{pmatrix}$$

$$\text{and } B = (b1,b2,b3) = \begin{pmatrix} 75 & 61 & 88 \\ 910 & 751 & 1068 \\ 5088 & 4257 & 5976 \end{pmatrix}$$

It can be verified that AY = B.

5. We can write encrypted message from matrix B by taking transpose of each column and then writing it as a string in linear form. Therefore encrypted message is

E = "75 910 5088 61 751 4257 88 1068 5976".

Encryption of s= "ITS3*MOS*" is
E = "75 910 5088 61 751 4257 88 1068 5976"
6. Return E

Example 4: String MDecrypt(String E, Matrix B : B is inverse of A)
String T = MDecrypt("75 910 5088 61 751 4257 88 1068 5976", Matrix A^{-1})
The string E is returned from MEncrypt algorithm from example 3.
E = "75 910 5088 61 751 4257 88 1068 5976".
Form column vector of group of 3 elements from E, convert them into integers and call it as b1,b2 and b3.
Let B = (b1,b2,b3) whereb1=[75 910 5088],
b2= [61 751 4257] andb3 = [88 1068 5976]

1. Calculate V= $A^{-1}B$

$$= \begin{pmatrix} 78 & -121 \\ -143 & 23 \\ 66 & -11 \end{pmatrix} \begin{pmatrix} 756188\,18 \\ -29107511068 \\ 1508842575976 \end{pmatrix} = \begin{pmatrix} 3 & 24 & \\ 29 & 36 & 28 \\ 28 & 22 & 36 \end{pmatrix}$$

Let v_1^T = (18 29 28), v_2^T = (3 36 22) and $v_3{}^T$ = (24 28 336).
Let V = (18 29 28 3 36 22 24 28 36).
2. Refer to Table 1 and replace each of code in V with character , we shall get original message
S = "ITS3*MOS*"
3. Return S.

IV. ENCRYPTION AND DECRYPTION PROCEDURE BASED ON COMPOSITION OFINTEGER MATRIX ANDDIVISION ALGORITHM

In this section we present main algorithm for encryption and decryption.
Let A and A^{-1} be nxn invertible integer matrices.Let s be original message containing some or all of characters defined in Table1. If total no of characters in sare not multiple of n then append s with appropriate number of* characters.The main algorithm consists of application of EDIME and DASKEA algorithm to string s in a composed manner and then apply decryption procedure defined in DASKEA and then followed by decrypt procedure defined in EDIME. We may consider EDIME as function f for block cipher, DASKEA as function gfor stream cipher and form composite map gof acting on string s. i.e. gof(s) = g(f(s))= E. Here gof is combination of block and stream cipher.
Using(gof) $^{-1}$= (f^{-1} o g^{-1}), we obtain
(f^{-1} o g^{-1})(E) = s

Encrypt by EDIME Encrypt by DASKEA
s----- f------>b =Ax ------ g --------->Y
---------------- gof ----------------------------->

Decrypt by Decrypt by

(i,j)	z_{ij}	Remainder r in 2 digit format	Quotient q in 2 digit format	Encryption rq
(1,1)	z_{11}	r_{11}	q_{11}	$r_{11}q_{11}$
(1,2)	z_{12}	r_{12}	q_{12}	$r_{12}q_{12}$
	..	..	..	..
(m,n)	z_{mn}	r_{mn}	q_{mn}	$r_{mn}q_{mn}$

DASKEA EDIME
Y ------ g^{-1} --------→ A^{-1} Y ----- f^{-1} ----→ s
----------------- g^{-1} of^{-1} ----------------------→

A. . Encryption procedure :

String Encrypt (String s, Encoding matrix A, n)

Let s be the message to be transmitted over network. If the number of characters in s i.e. |s| is not multiple of n, we append * at the end of string so that s contains mn characters, m is positive integer.
1. Let s be any string of characters from Σ.
2. Let A be nxn invertible integer matrix.
3. Refer to Table 1 and write integer code for each of the character in string s. Let this messageof integer code be Y.
4. Now apply MEncrypt algorithm to Y.
From Y, group in n elements and form column vectors of integers y_1, y_2, y_3, ...y_m
Calculate b_1=A y_1, b_2=A y_2, ... and b_m= Ay_m
Each column has n integers and if each integer is stored as long using 4 bytes, then every
block of text will be 4n bytes long. For m groups of text it will be 4mn bytes long.
5. Let Z be the coded message obtained from b_1^T, b_2^T, b_3^T ... b_m^T. The message is written as row vector.
6.Let Z =[$z_{i,j}$] , $1 \le i \le n$, $1 \le j \le m$
Z = (b_1^T b_2^T b_3^T ...b_m^T).
7 . To each element $z_{i,j}$of Z apply DAEncryptwith suitable values of k and m.
By division algorithm $z_{ij} = q_{ij}.k + r_{ij}$.
It will be encrypted as digits in r_{ij} followed by digitsin q_{ij}. $r_{ij}$and q_{ij} will be written as mdigit string.
By applying division algorithm to remaining elements we obtain

Table 2. Encryption using Division
For each element we apply stream cipher. The feedback byte is not considered.
8.The encrypted message is derived from 5 th columnrqof the above table

E = “$r_{11}q_{11}$ $r_{12}q_{12}$ ... $r_{mn}q_{mn}$”
9. Return E

B. Decryption Procedure:

String Decrypt (String E, Matrix B, Integer k, Integer m)

Here E is the message returned by Encrypt, Matrix B is inverse of A, m and k are integers defined in Encrypt procedure.

1. Encrypted message E is partitioned into groups of length of 2m characters from left to right.
The groups are $r_{11}q_{11}$, $r_{12}q_{12}$, ... , $r_{mn}q_{mn}$
Each group is further divided into groups of m characters.
Consider $r_{11}q_{11}$. Left group is $r_{11}$and right group isq_{11}. Converting string q_{11} and r_{11} tointegers q and r we getquotient q andremainder r.
By Division algorithm, $z_{11} = k\,q + r$, $0 \leq r<k$
Repeating the above process for $r_{12}q_{12}$,... , $r_{mn}q_{mn}$ we obtain z_{12}, ..., z_{nm}.
2. Form the matrix
$Z = [\, z_{ij} \,] \quad 1 \leq i \leq n ,\ 1 \leq j \leq m$
3. Calculate BZ and call it V
$V = BZ = A^{-1}\, Z$
4. Write columns of V as row vector to getString C of integers.C =(v1 v2 ... v_m)
5. Refer to Table 1, write characters corresponding to each element of C to get original
message E = “$s_1s_2...s_{mn}$”
6. Return E

C . Main algorithm

Thus, main procedure is

procedure

EDIMCDA(String s, Int Matrix A, Int: n, k)

```
        {
        E =  Encrypt ( String s, Matrix A, n)
        s =Decrypt (String E, Matrix B, Integer k, Integer m)
        }
```

We shall illustrate this algorithm with an example.

Example 5:

Let “ITS3*MOS” be the message to be transmitted over network. The number of characters are 8 and not multiple of 3, hence we append * at the end of string. The resulting string is “ITS3*MOS*”

Encryption Procedure:

String Encrypt (Strings, Matrix A, n)
1. Let s = “ITS3*MOS*”.

2. Let A be 3x3 invertible integer matrix

1 11
A =111213 and its inverse -143 23 -2
55 6678

78 -12 1
-143 23 -2
A^{-1}=66 -11 1\`

3. Referring to code Table 1, we obtain integer codes for each character of string s

Char	I	T	S	3	*	M	O	S	*
Code	18	29	28	3	36	22	24	28	36

Let Y = "18 29 28 3 36 22 24 28 36"
4. From Y, group in 3 elements and form column vectors y1, y2 and y3
Calculate b1=Ay1, b2=Ay2 and b3 = Ay3.

18 3 24
Let y1 = 29 y2=36y3 = 28
28 22 36

Then
Ay1= 1 1 118 75= b1
1112 1329 = 910
55 66 78 28 5088

11 1 3 61
A y2 = 111213 36 = 751 = b2
556678 22 4257

1 11 24 88
A y3 = 111213 28 = 1068 = b3
556678 36 5976

5. Let Z be the coded message obtained from b1, b2 and b3. Let Z = (b_1^T b_2^T b_3^T ... b_m^T).

6. Let Z =[$z_{i,j}$] , $1 \leq i \leq n$, $1 \leq j \leq m$

75 61 88
Z = 910 751 1068
5088 4257 5976

6. To each element of Z apply Encryption process of DASKEA algorithm DAEncryptwith
k = 91 and m = 2. Here k is divisor and m is no of characters in string number.
The first element of ZisZ $_{11}$ = 75

By division algorithm 75 = 0.91 + 75. Here quotient q is 0 and remainder r is 75. It will be encrypted as digits in r followed by digits in q .
r and q will be written as m=2 digit string
i.e. "75" and "00".Thus 75 will be encrypted as “7500”
By applying division algorithm to remaining elements we obtain

Table 3. Encryption using Division

7. The encrypted message is derived from 5 th column of the above table3 by catenation
E = “750000108355630023087146880067116165”

8. Return E

D. Decryption Procedure

String Decrypt (String E, Matrix B, Int k, Int m)

Here E is the message returned by Encrypt, Matrix B is inverse of A, m and k are integers defined in Encrypt procedure.
Here
E=“750000108355630023087146880067116165”,
Matrix B is inverse of A,m = 2 and k = 91

1. Encrypted message E is partitioned into groups of 4 (i.e. 2m =2.2) characters from left to right.
The groups are “7500”, “0010”, “8355”, “ 6300”, “ 2308”, “7146”, “8800”, “6711”, “6165”
Each group is further divided into groups of two characters. Left group is r1and right group is q1. Thus, r1 =”75” and q1 = “00” and converting r1 and q1 into integers we get quotient q=0 and remainderr=75
By Division algorithm, z_{11} = k q + r = 91.0+75 = 75
From the second group, r_{21} = ”00”, q_{21}= ”10” and converting q_{21} and r_{21} to integers we get
q = 10 and r = 0
By Division algorithm, z_{21}=kq+r=91.10+0=910
From the third group, r_{31} = ”83”, q_{31} = ”55” and converting q_{31} and r_{31} to integers we get
q =55 and r = 83. By Division algorithm,
z_{31} = k q + r = 91 .55 + 83 = 5088
By repeating this process for rest of the groups we obtain z_{12} = 61,z_{22} = 751, z_{23} = 4257,
z_{13}=88, z_{23} = 1068 and z_{33} = 5976

2. Form the matrix

$$Z = \begin{pmatrix} 75 & & 61 \quad 88 \\ 910 & 751 & 1068 \\ 5088 & 4257 & 5976 \end{pmatrix}$$

3. Calculate B.Z and call it V
$V = BZ = A^{-1} Z$

$$= -143 \begin{pmatrix} 78-12 & 17561 & \\ 23 & -2910 & 751 \\ 66\ -11 & 1\ 5088 & \end{pmatrix} \begin{pmatrix} 88 \\ 1068 \\ 4257\ 5976 \end{pmatrix}$$

$$= \begin{pmatrix} 18 & 3 & 24 \\ 29 & 36 & 28 \\ 28 & 22 & 36 \end{pmatrix}$$

4. The matrix V is linearised to get
C ="18 29 28 3 36 22 24 28 36" as row vector of integer codes.

5. Refer to Table 1, write characters corresponding to each element of C to get original message
x = “ITS3*MOS*” .

Note that blanks introduced for readability are ignored.

6. Return x

V. CONCLUSION

The algorithm uses composition of two invertible maps for block and stream cipher hence key space for both the maps when taken together becomes arbitrarily large space. Since block and stream cipher are used as composite, finding key to decipher the text is acomplex procedure.The uniqueness of quotient and remainder in division algorithm and uniqueness of integer inverse of matrix and the composition of two invertible maps satisfies the fact that enciphering and deciphering processes are inverses of each other. The examples presented here uses decimal numbers . Programs can be written using binary number system with choice of m larger than 4 and the characters can be represented with more than 8 bits. In block transfer for a square matrix of size 3 defined on long integer, we use 96 bits at a time for encryption which is unusual compared to use of 64 or 128 bits. The length of string is increased and because of composition of maps it will address the issue of secure transmission.

(i j)	Z_{ij}	Remainder r in 2 digit format	Quotient q in 2 digit format	Encryption rq
(1,1)	75	75	00	"7500"
(2,1)	910	00	10	"0010"
(3,1)	5088	83	55	"8355"
(1,2)	61	63	00	"6300"
(2,2)	751	23	08	"2308"
(3,2)	4257	71	46	"7146"
(1,3)	88	88	00	"8800"
(2,3)	1068	67	11	"6711"
(3,3)	5976	61	65	"6165"

Acknowledgement: Author wishes to thank the management of Nirmala Memorial Foundation College of Commerce and Science for their encouragement.

REFERENCES

[1] Andrew S Tanenbaum (2003), Computer Networks, 4 th Edition, Pearson Education Inc. and Dorling Kindersley Publishing Inc. , Delhi, ISBN:0-13-046002-8

[2] Gary K. (2012), "An Overview of Cryptography", www.garykessler.net

[3] William Stallings(2006), Cryptography and Network Security – Principles and Practice, 4 thEdition ,Pearson Education Inc. and Dorling Kindersley Publishing Inc., Delhi, ISBN–978–81–7758-774-6

[4] William Stallings(2008),Network Security Essentials – Applications and Standards, Pearson Education Inc. and Dorling Kindersley (India) Private Ltd. , Delhi, Third Edition, ISBN–978–81–317–1664–9.

[5] Shriram B. Patil (2013), A Division algorithm based symmetric key encryptionalgorithm [DASKEA], The IUP Journal of Computer Sciences, VolVII, No 3,pp 35-42

[6] EricksenW. S.(1980) Inverse Pairs of Matrices with Integer Elements, SIAM J.Numer. Anal. 1980, Vol 17, No 3, pp 474-477

[7] Alfred J. Menezes, Scott A. Vanstone, and Paul C. Van Oorschot. Handbook of Applied Cryptography. CRC Press, Inc., Boca Raton, FL, USA, 1stedition, 1996.

[8] https://www.jscape.com/blog/stream-cipher-vs-block-cipher

[9] https://eprint.iacr.org/2014/677.pdf