A NOVEL BLOCK CIPHER INVOLVING KEYS IN A KEY BUNCH MATRIX AS POWERS OF THE PLAINTEXT ELEMENTS

K. Anup Kumar[1], V.U.K Sastry[2]

[1]Associate Professor, [2]Director R & D, CSE Department, SNIST, A.P, India

Abstract

In this analysis, we have developed an asymmetric block cipher which is involving a key bunch matrix A (= [a_{ij}]) in the process of encryption, and B (= [b_{ij}]) in the process of decryption. The keys a_{ij} are used as powers of the plaintext elements, and the keys b_{ij} are used as the powers of the ciphertext elements. Here, we have made use of Euler's totient function and Euler's theorem in the development of the cipher. The cryptanalysis clearly shows that the strength of the cipher is quite significant.

Keywords: *Encryption, Decryption, Key, Plaintext, Cipher text and Cryptanalysis.*

----------***----------

1. INTRODUCTION

The literature of Cryptography [1] is replete with a number of block ciphers, in which majority of ciphers are symmetric and a few are asymmetric. The popular symmetric ciphers are Hill cipher [2], Feistel cipher [3], Data Encryption Standard (DES) [4], Advanced Encryption Standard (AES) [5] and several variants of these ciphers. The well known asymmetric cipher is RSA [6] developed by Ron Rivest et al.

In a recent investigation, Sastry and Sirisha [7] have developed a block cipher in which the encryption is carried out by a key bunch matrix E (= [e_{ij}]), and the decryption is done by using another key bunch matrix D (= [d_{ij}]) which is obtained by using the relation

$$(e_{ij} x d_{ij}) \bmod 256 = 1, \qquad (1.1)$$

in which both e_{ij} and d_{ij} are odd integers lying in the interval [1,255]. Here it is to be noted that the encryption key and the decryption key are different though they are related in a particular way. In all the ciphers, developed basing upon the cipher under consideration, the keys in the key bunch matrix are used as multiplicands of the plaintext elements.

In RSA, we have two keys -- one key called public key and another one called private key. The encryption is carried out by using the public key of the receiver and the decryption (at the receiver's end) is done by using his own private key. Here it is to be noted that, the public key {e, n} and the private key {d, n}, in which, n is the product of two distinct prime numbers *p* and *q*, and *e* and *d* are two positive integers governed by the relation

$$ed \bmod \Phi(n) = 1 \qquad (1.2)$$

Where,

$$\Phi(n) = (p-1)(q-1). \qquad (1.3)$$

In the RSA, both e and d are used as exponents, one in the process of encryption and the other one in the process of decryption.

In the present investigation our objective is to develop a block cipher, wherein, we use the keys in a key bunch matrix, say A = [a_{ij}], as powers of the plaintext elements (P = [p_{ij}]) in the process of encryption, and the corresponding keys (B=[b_{ij}]) are used as powers of the ciphertext elements, C=[c_{ij}], in the process of decryption.

The basic concepts utilized in the development of the cipher under consideration can be summarized [1] as follows. When n is a prime number, the number of integers less than n can be obtained in the form of the Euler's totient function [1] given by

$$\Phi(n) = n-1. \qquad (1.4)$$

On the other hand, when n is the product of two prime numbers, say p and q then

$$\Phi(n) = \Phi(pq) = (p-1)(q-1). \qquad (1.5)$$

The Euler's theorem well known in the literature of Cryptography is given by

$$a^{\Phi(n)} \bmod n = 1. \qquad (1.6)$$

On using this theorem, we readily prove that

$$p^{k\Phi(n)+1} \bmod n = p \bmod n \qquad (1.7)$$

Let us now take the basic equations of a block cipher in the form

$$C = P^e \bmod n \quad (1.8)$$

and

$$P = C^d \bmod n. \quad (1.9)$$

From (1.8) and (1.9), we get

$$P = P^{ed} \bmod n. \quad (1.10)$$

$$\text{On writing } ed = k\Phi(n)+1, \quad (1.11)$$

we find that (1.8) and (1.9) are valid relations of the cipher in view of (1.7). From (1.11), we find that

$$ed \bmod \Phi(n) = 1 \quad (1.12).$$

In the light of the above discussion, the basic equations governing the cipher are given by (1.8), (1.9) and (1.12).

In the present paper, our interest is to develop a block cipher wherein n is a prime number. Thus in view of the relation (1.4), equation (1.12) assumes the form,

$$ed \bmod (n-1) = 1 \quad (1.13)$$

In this analysis, we take n=257 as 257 is the nearest prime number which encompasses all the EBCIDIC codes, which are lying in [0-255].

In what follows we present the details of the organization of this paper. In Section 2, we deal with the development of the cipher. In this we display the flowcharts and the algorithms describing the cipher. In Section 3, we present an illustration of the cipher and examine the avalanche effect. Section 4 is devoted to the study of the cryptanalysis. Finally in Section 5, we mention the computations carried out in this analysis and draw conclusions.

2. DEVELOPMENT OF THE CIPHER

Consider a plaintext. On using the EBCIDIC code, this can be written in the form of a matrix P given by

$$P = [p_{ij}], \quad i= 1 \text{ to } m, j = 1 \text{ to } m \quad (2.1)$$

in which each p_{ij} is an integer lying in [1-255].

Let

$$A = [a_{ij}], \quad i= 1 \text{ to } m, j = 1 \text{ to } m \quad (2.2)$$

be the encryption key bunch matrix,

and

$$B = [b_{ij}], \quad i= 1 \text{ to } m, j = 1 \text{ to } m \quad (2.3)$$

be the decryption key bunch matrix.

Here a_{ij} and b_{ij} are governed by the relation

$$(a_{ij} x b_{ij}) \bmod 256 = 1 \quad (2.4)$$

as we have taken n=257.

The basic equations governing the cipher can be written in the form,

$$C = [c_{ij}] = [p_{ij}^{aij}] \bmod 257 \quad (2.5)$$

and

$$P = [p_{ij}] = [c_{ij}^{bij}] \bmod 257. \quad (2.6)$$

The flowcharts and the algorithms concerned to the encryption and the decryption can be presented as shown below.

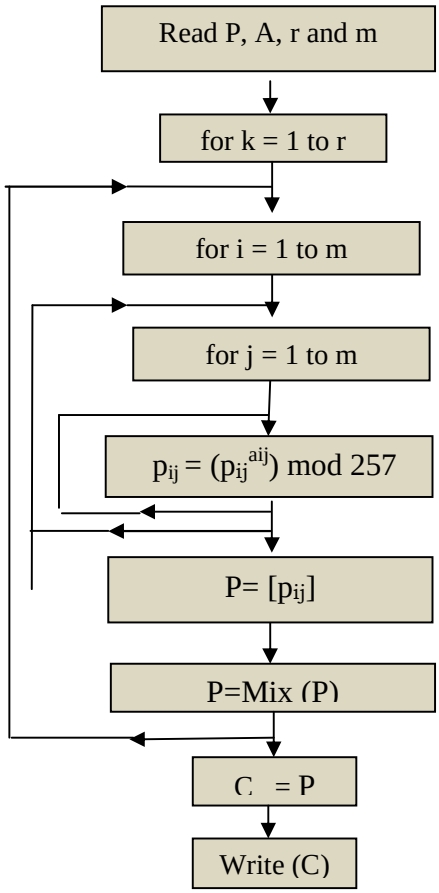

Fig 1 The process of Encryption

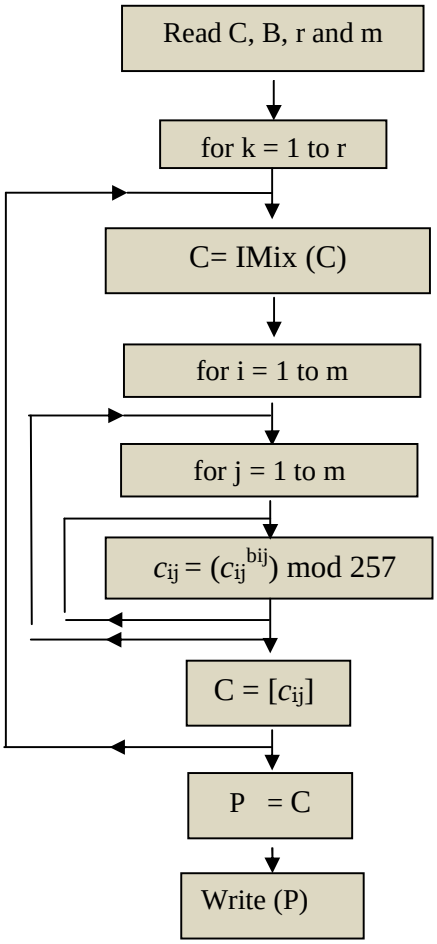

Fig 2 The process of Decryption

2.1 Algorithm for Encryption

1. Read P, n, A, r and m
2. for (k = 1 to r)
   begin

   for (i = 1 to m)
   begin

   for (j = 1 to m)
   begin
   $p_{ij} = (p_{ij}^{aij})$ mod 257
   end
   end
   P = [p_{ij}]
   P = Mix(P)
   end
3. C = P
4. Write (C)

2.2 Algorithm for Decryption

1. Read C, n, B, r and m

2. for (k = 1 to r)
   begin

   C = IMix (C)

   for (i = 1 to m)
   begin

   for (j = 1 to m)
   begin
   $c_{ij} = (c_{ij}^{bij})$ mod 257
   end
   end
   C = [c_{ij}]
   end
3. P = C
4. Write (P)

In this analysis, r represents the number of rounds in the iteration process. Here we have taken r=16. The function Mix ( ) which is used in each round of the iteration process can be explained as follows.

Let P = [p_{ij}], i = 1 to m, and j = 1 to m be the plaintext at a particular round of the iteration process. Let us suppose that there are 's' elements in the matrix P which are having their values as 256. Then the (m^2 – s) elements of P, which are not equal to 256, can be written in the form of a matrix having 8 rows and (m^2-s) columns. On writing the binary bits in each column as a decimal number we get (m^2-s) decimal numbers. These numbers can be placed, in a row wise manner, in all the other places, one after another, excluding the places wherein 256 is present, we get, a new matrix P of size mxm. Thus mixing is done in a perfect manner.

3. ILLUSTRATION OF THE CIPHER

Consider the plaintext given below

Respected uncle,
I am very much delighted to inform you that the Andhra Pradesh is now getting partitioned into two parts. The Hyderabad which was ruled earlier by our own people, now clubbed with another nine districts, is going to be carved as Telangana, and the rest of the thirteen districts are going to be branded as Seemandhra. This bifurcation is similar to the disintegration as Pakistan and India which we had just before Independence. We cannot forget the instance in which Pakistan was divided into two segments, and the role played by India in that bifurcation. This division of Andhra Pradesh is certainly going to help our community. With regards, Your Mohammad. (3.1)

Consider the string of the first 16 characters of the plaintext (3.1) given by

Respected uncle,
On using the EBCIDIC code we get

$$P = \begin{bmatrix} 082 & 101 & 115 & 112 \\ 101 & 099 & 116 & 101 \\ 100 & 032 & 117 & 110 \\ 099 & 108 & 101 & 044 \end{bmatrix} \quad (3.2)$$

Let us now choose the encryption key bunch matrix A in the form

$$A = \begin{bmatrix} 021 & 057 & 171 & 039 \\ 101 & 067 & 089 & 223 \\ 067 & 157 & 171 & 001 \\ 037 & 203 & 233 & 017 \end{bmatrix} \quad (3.4)$$

On using the relation (2.4), the decryption key bunch matrix B can be obtained in the form

$$B = \begin{bmatrix} 061 & 009 & 003 & 051 \\ 109 & 107 & 233 & 031 \\ 107 & 181 & 003 & 001 \\ 173 & 227 & 089 & 241 \end{bmatrix} \quad (3.5)$$

On applying the encryption algorithm the ciphertext C can be obtained as

$$C = \begin{bmatrix} 011 & 049 & 137 & 225 \\ 237 & 042 & 153 & 007 \\ 115 & 036 & 177 & 086 \\ 059 & 123 & 231 & 136 \end{bmatrix} \quad (3.6)$$

On using the decryption algorithm, given in Section 2, we get back the original plaintext P.

Now let us study the avalanche effect.

On replacing 82, the first row first column element of the matrix P by 83 we get a one bit change in the plaintext. On using this modified plaintext, the key given by (3.4), and the encryption algorithm, given in Section 2, we get the ciphertext C in the form

$$C = \begin{bmatrix} 085 & 068 & 132 & 236 \\ 239 & 093 & 149 & 020 \\ 115 & 142 & 133 & 146 \\ 005 & 068 & 244 & 116 \end{bmatrix} \quad (3.7)$$

On comparing (3.6) and (3.7), after converting them into their binary form, we notice that these two ciphertexts differ by 58 bits out of 128 bits. This shows that the cipher is expected to be a strong one.

Now let us consider a one bit change in the key A. This is achieved by replacing the first row second column element of A by 56. On using this modified key, the original plaintext and the encryption algorithm, we get the corresponding ciphertext C given by

$$C = \begin{bmatrix} 073 & 157 & 180 & 120 \\ 006 & 255 & 023 & 208 \\ 040 & 153 & 162 & 075 \\ 114 & 219 & 124 & 094 \end{bmatrix} \quad (3.8)$$

On comparing (3.8) and (3.6), brought into their binary form, we find that these two ciphertexts differ by 69 bits out of 128 bits. From this also, we conclude that this cipher is a potential one.

4. CRYPTANALYSIS

In the development of every cipher cryptanalysis plays a predominant role in deciding whether a cipher is having sufficient strength or not. The basic attacks that are available in the literature of the Cryptography are

1. Ciphertext only attack (Brute force attack)
2. Known Plaintext attack
3. Chosen plaintext attack
4. Chosen ciphertext attack

Usually, every cipher is designed so that it cannot be broken, atleast, by the first two attacks [1]. The first two attacks are thoroughly studied by offering analytical proofs. However, the strength of the last two attacks is also to be decided by applying all possible intuitive approaches.

Let us now consider, the ciphertext only attack (Brute force attack). In the case of this attack the ciphertext is known. Keeping this ciphertext in view we have to determine the key which leads to a sensible plaintext.

In the key bunch matrix A=[a_{ij}], each aij is an odd integer lying in the interval [1-255] as its value. Thus there are 128 possible values for aij. In the matrix used in this analysis, as we have m^2 elements the size of the key space is

m^2 $7m^2$ $0.7m^2$ $2.1\ m^2$

$128 = 2 = \left(2^{10}\right) \approx 10.$

On assuming that the time required for the computation of this cipher with one value of the key in the key space is 10^{-7} seconds, the time required for the computation with all possible keys in the key space is approximately equal to

$2.1\ m^2$ -7 $2.1m^2\text{-}15$

$$\frac{10 \quad x \quad 10}{365x24x60x60} = 3.12x\ 10 \quad \text{years.}$$

In this analysis as we have taken m=4, the time required for this cipher is

$3.12 \times 10^{18.6}$ years.

As this number is very large, we cannot break the cipher by the ciphertext only attack.

Now consider the known plaintext attack. To proceed with this we know the pairs of plaintext and ciphertext, as many as we require. If we assume that we are carrying out only one round of the iteration process, that is if take r = 1, the basic equations involved in the cipher are

$$p_{ij} = (p_{ij}^{aij}) \bmod 257, \quad (4.1)$$

$$P = [p_{ij}], \quad (4.2)$$

$$P = \text{Mix}(P), \quad (4.3)$$

$$C = P. \quad (4.4)$$

Here we know the p_{ij}, occurring in the right hand side of (4.1), and the C present in the left hand side of (4.4). As this C is known, we know the P occurring on the left hand side of (4.3). On using the IMix ( ), we readily obtain the pij which is occurring on the right hand side of (4.2). Thus we know the p_{ij} which is on the left hand side of (4.1). As we know the p_{ij} which is on the right hand side of (4.1) the key A (= $[a_{ij}]$) can be determined by making attempts with all the possible values of aij. Thus this cipher can be broken by the known plaintext attack when r=1.

Let us consider the cipher when r = 2. In this case the basic equations governing the cipher are given by

$$p_{ij} = (p_{ij}^{aij}) \bmod 257, \quad (4.5)$$

$$P = [p_{ij}], \quad (4.6)$$

$$P = \text{Mix}(P), \quad (4.7)$$

$$p_{ij} = (p_{ij}^{aij}) \bmod 257, \quad (4.8)$$

$$P = [p_{ij}], \quad (4.9)$$

$$P = \text{Mix}(P), \quad (4.10)$$

$$C = P. \quad (4.11)$$

Here also we know the initial plaintext (p_{ij} occurring in the right hand side of (4.5)), and the ciphertext C in (4.11). On using this C and the IMix ( ) we can find the pij occurring in (4.9), this gives the pij which is on the left hand side of (4.8). From here, we cannot proceed further in the upward direction. Though p_{ij}, occurring on the right hand side of (4.5), is known to us, we are stuck up at this stage as the other quantities involved here are not known. In the light of the above facts the key A (= $[a_{ij}]$) cannot be determined by any means. Hence the cipher is unbreakable by the known plaintext attack when r is equal to 2. This implies that the strength of the cipher is quite significant as we have taken r=16.

Now let us explore what will happen in the case of the chosen plaintext attack and in the case of the chosen ciphertext attack. On inspecting the equations (4.5) to (4.11), and using our intuition in an effective manner, we readily notice that this cipher cannot be broken either by the chosen plaintext attack or by the choosen ciphertext attack.

From the above analysis, we firmly conclude that this cipher is a strong one, and it cannot be broken by any cryptanalytic attack.

5. COMPUTATIONS AND CONCLUSIONS

In this paper, we have developed an asymmetric block cipher in which we are having a key bunch matrix A (= $[a_{ij}]$) for encryption, and another key bunch matrix B (= $[b_{ij}]$) for decryption, wherein, these two matrices are connected by the relation

$$(a_{ij} \times b_{ij}) \bmod 256 = 1 . \quad (5.1)$$

In this analysis, we have used the keys in the key bunch matrix A as powers of the plaintext elements in the process of encryption, and the keys in the key bunch matrix B as powers of the ciphertext elements in the process of decryption.

Basing upon the algorithms, given in Section 2, we have written the programs for the encryption and the decryption in C language.

From the cryptanalysis carried out in this investigation, we have seen that the strength of the cipher is remarkable as the powers are playing a vital role, and the Mix ( ) function is supporting further very thoroughly.

REFERENENCES

[1]. William Stallings, Cryptography and Network Security, Principles and Practice, Third Edition, Pearson, 2003.
[2]. Jack Levine and Richard Chandler, “The Hill Cryptographic System with Unknown Cipher Alphabet, But Known Plaintext”, Cryptologia 13:1, pp. 1 – 28, Jan 1989.
[3]. Feistel H, “Cryptography and Computer Privacy”, Scientific American, Vol. 228, No. 5, pp. 15 – 23, 1973.
[4]. National Bureau of Standards NBS FIPS PUB 46, “Data Encryption Standard (DES)”, National Bureau Standards, US Department of Commerce, Jan 1977.
[5]. Daemen J and Rijmen V, “Rijndael, the Advanced Encryption Standard (AES)”, Dr. Dobbs’ Journal, Vol. 26, No. 3, pp. 137 – 139, Mar 2001.

[6]. Diffie,W. and Hellman, M. New directions in Cryptography, IEEE Transactions Information Theory IT – 22, (Nov, 1976) 644-654. people.csail.mit.edu/rivest/Rsapaper.pdf
[7]. V.U.K Sastry and K. Shirisha " A Novel Block Cipher Involving a Key Bunch Matrix" IJCA International Journal of computer Applications (0095-8887), Vol 55 No.16, October 2012.

BIOGRAPHIES:

Dr. V. U. K. Sastry is presently working as Professor in the Dept. of Computer Science and Engineering (CSE), Director (SCSI), Dean (R & D), SreeNidhi Institute of Science and Technology (SNIST), Hyderabad, India. He was Formerly Professor in IIT, Kharagpur, India and worked in IIT, Kharagpur during 1963 – 1998. He guided 12 PhDs, and published more than 90 research papers in various international journals. His research interests are Network Security & Cryptography, Image Processing, Data Mining and Genetic Algorithms.

Mr. K. Anup Kumar is presently working as an Associate Professor in the Department of Computer Science and Engineering, SNIST, Hyderabad India. He obtained his B.Tech (CSE) degree from JNTU Hyderabad and his M.Tech (CSE) from Osmania university, Hyderabad. He is now pursuing his PhD from JNTU, Hyderabad, India, under the supervision of Dr. V.U.K. Sastry in the area of Information Security and Cryptography. He has 12 years of teaching experience and his interest in research area includes Cryptography, Steganography and Parallel Processing Systems.