BULGARIAN ACADEMY OF SCIENCES

CYBERNETICS AND INFORMATION TECHNOLOGIES • Volume **13**, No 3

Sofia • 2013 Print ISSN: 1311-9702; Online ISSN: 1314-4081
DOI: 10.2478/cait-2013-0025

A Large Block Cipher Involving Key Dependent Permutation, Interlacing and Iteration

V. U. K. Sastry[1], *N. Ravi Shankar*[2], *S. Durga Bhavani*[3]

[1] *School of Computer Science and Informatics, Sreenidhi Institute of Science and Technology, Hyderabad, India*
[2] *Department of Computer Science and Engineering, Keshav Memorial Institute of Technology, Hyderabad, India*
[3] *School of Information Technology, Jawaharlal Nehru Technological University Hyderabad, Hyderabad, India*

Emails: vuksastry@rediffmail.com ravishankar.nanduri@gmail.com sdurga.bhavani@gmail.com

Abstract: *In this paper we have developed a block cipher, wherein the size of the key matrix is 384 bits and the size of the plain text is as large as we choose. The permutation, the interlacing and the iteration introduced in this analysis are found to cause diffusion and confusion efficiently. Hence, the strength of the cipher proves to be remarkable.*

Keywords: *Modular arithmetic inverse, interlacing, decomposition, permutation, inverse permutation.*

1. Introduction

The classical Hill cipher [1, 2], is the first cipher, which has demonstrated the application of algebraic transformations in the area of cryptology. It is also the first block cipher developed in the literature of cryptography. Lester Hill's cipher proved to be unsecure against the known plain text attacks [3]. Though Hill introduced his algorithm in 1929, not much work was reported till the last decade. In the last ten years, several researchers have focused their attention on the classical Hill cipher and proposed many modifications [4-27] to make it stronger and resistant to various cryptanalytic attacks. Some were successful and some were not. One of the most significant aspects of Hill cipher is the ability of the cipher to dissipate the statistical characteristics of the plain text, and exhibit a very good diffusion property.

In this paper our objective is to offer a modification of Hill cipher by introducing a key dependent permutation, interlacing at binary bit level to the plain text in an iterative manner. These additional operations that we introduced will not allow a direct relationship to be established between the plain text and the cipher text, as it can be done in the case of the classical Hill cipher. Since Hill cipher's primary operation is a modular matrix multiplication, the plain text is arranged in the form of a matrix of size $n\times m$, such that n is equivalent to the number of columns of the key matrix, and m can be as long as we choose. Thus, if we have a square matrix K, of size $n\times n$, and a plain text matrix of size $n\times m$, matrix multiplication can be accomplished. This also gives us the flexibility of taking the entire plain text as a single block. Thus, theoretically, there will be no limit on the size of the plain text block that can be encrypted as a single unit.

In this paper we have taken 128 ASCII characters as the set of plain text characters to be encrypted. The elements of the key matrix are also in the range from 0 to 127. We take mod 128, instead of mod 26, as it was done in the case of the classical Hill cipher.

In Section 2 of this paper, we introduce the development of the cipher. In Section 3 we present the algorithms for encryption and decryption. Then in Section 4 we illustrate the cipher with a couple of examples. Subsequently we discuss the crypt analysis and avalanche effect in Sections 5 and 6. Finally, we present the computations and conclusions in Section 7.

2. Development of the cipher

Consider a plain text. When using the ASCII code, we write the plain text in the form of a matrix $P = [P_{ij}]$, $i = 1, \ldots, n$, $j = 1, \ldots, m$, in a column wise manner (pad if needed).

Let $K=[K_{ij}]$, $i = 1, \ldots, n$, $j = 1, \ldots, n$, be the key matrix. The elements in the key matrix are between 1 and n^2 in some permuted order.

Let $C=[C_{ij}]$ represents the cipher text corresponding to the plain text P. As in Hill cipher, the relations for encryption and decryption can be written as

(1) $$C=KP \bmod 128$$

and

(2) $$P=K^{-1}C \bmod 128.$$

where K^{-1} is the modular arithmetic inverse of K.

Let us now introduce the process of permutation and interlacing. On writing each element of the matrix $[P_{ij}]$ in terms of binary bits, we have

$$[P_{ij}]=[b_{il}^{j}],\ i = 1, \ldots, n,\ \ j = 1, \ldots, m,\ \ l=1, \ldots, 7.$$

Thus, each column of $[P_{ij}]$ is represented as a matrix of size $n\times 7$, and hence we have m such matrices. Let us now take $7n$ numbers (ranging from 1 to $7n$), in the order in which they appear in the key matrix and form a subkey.

We now focus our attention on the matrix corresponding to the first column of $[P_{ij}]$ (the size of this matrix is $n\times 7$). The elements of this are permuted by using the subkey (of size $7n$) above mentioned. Then, the aforementioned procedure is applied for the matrices corresponding to all other columns of $[P_{ij}]$.

Thus we get a new matrix, which includes all the permuted matrices, of size $n\times 7m$ and denoted by $[e_{ij}]$. This $[e_{ij}]$ is divided into two equal halves, wherein each half contains $7m/2$ columns, if m is an even number. Otherwise, it will be divided into two parts, wherein the left part contains $(7m+1)/2$ columns and the right one is having $(7m-1)/2$ columns.

Then we place the first column of the right half next to the first column of the left half. The second column of the right half next to the second column of the left half, and so on, till we exhaust all the columns of the right half. This completes the process of interlacing.

The reverse processes of interlacing and permutation are denoted as decomposition and inverse permutation respectively. These two are utilized in decryption.

In this cipher, we adopt an iterative procedure, which consists of 16 rounds. The procedures of encryption and decryption are depicted in the diagram shown in Fig. 1.

3. Algorithms

The algorithms describing encryption, decryption, modular arithmetic inverse, permutation, interlace, inverse permutation and decomposition, are given below.

3.1. Algorithm for encryption

1. read n, N, K, P;
2. $P^0 = P$;
3. $P^1 = KP^0 \bmod 128$;
4. for i=2 to N{
   Permute();
   interlace();
   $P^i = KP^{i-1} \bmod 128$;
   }
5. $C = P^N$;
6. write C;

3.2. Algorithm for decryption

1. read n, N, K, C;
2. find modinverse (K);
3. $P^N = C$;
4. for i=N to 2{
   $P^{i-1} = K^{-1}P^i \bmod 128$;
   decompose();
   invpermute();
   }
5. $P^0 = K^{-1}P^1 \bmod 128$;
6. P=P^0;
7. write P;

3.3. Algorithm for modinverse

```
1. read n,K;
2. find K_ij,Δ;
/* K_ij are the cofactors of the elements of K, and Δ is the determinant of K */
3. find d such that (dΔ)mod128=1;
/* d is the multiplicative inverse of Δ */
4. K^–1=(K_ji d)mod128;
```

3.4. Algorithm for permute

```
1. convert P^i into binary bits;
2. construct [e_ij], i=1 to n, j=1 to 7m;
3. generate subkey;
4. for l=0 to (m–1){
k=1;
    for i=1 to n{
            for j=(7l+1) to (7l+7){
temp[subkey[k]]=e_ij
 k++;
            }
    }
    k=1;
    for i=1 to n{
            for j=(7l+1) to (7l+7){
                    e_ij=temp[k];
                    k++;
            }
    }
}
```

3.5. Algorithm for invpermute

```
1. convert P^i into binarybits;
2. construct [e_ij], i=1 to 8, j=1 to 14;
3. generate subkey;
4. for l=0 to (m–1){
    k=1;
    for i=1 to n{
            for j=(7l+1) to (7l+7){
temp[k]=e_ij
k++;
            }
    }
    k=1;
    for i=1 to n{
            for j=(7l+1) to (7l+7){
e_ij=temp[subkey[k]];
```

```
k++;
            }
        }
    }
```

3.6 Algorithm for interlace

```
1. l=1;
2. convert P into binary bits;
3. for i=1 to n{
   for j=1 to 7{
               temp(l) = b_ij;
               temp(l+1) = d_ij;
               l=l+2;
            }
   }
4. l=1;
5. for i=1 to n{
            for j=1 to 7{
               b_ij=temp(l);
               d_ij=temp(l+n*7);
               l=l+1 ;
            }
   }
```

3.7. Algorithm for decomposition

```
1. l=1;
2. convert P into binary bits;
3. for i = 1 to n{
            for j=1 to 7{
               temp(l)=b_ij;
               temp(l+n*7)=d_ij;
   l = l + 1 ;
            }
   }
4. l=1;
5. for i = 1 to n{
            for j = 1 to 7{
               b_ij = temp(l);
               d_ij = temp(l+1);
               l = l + 2 ;
            }
   }
6. convert binary bits to decimal numbers.
```

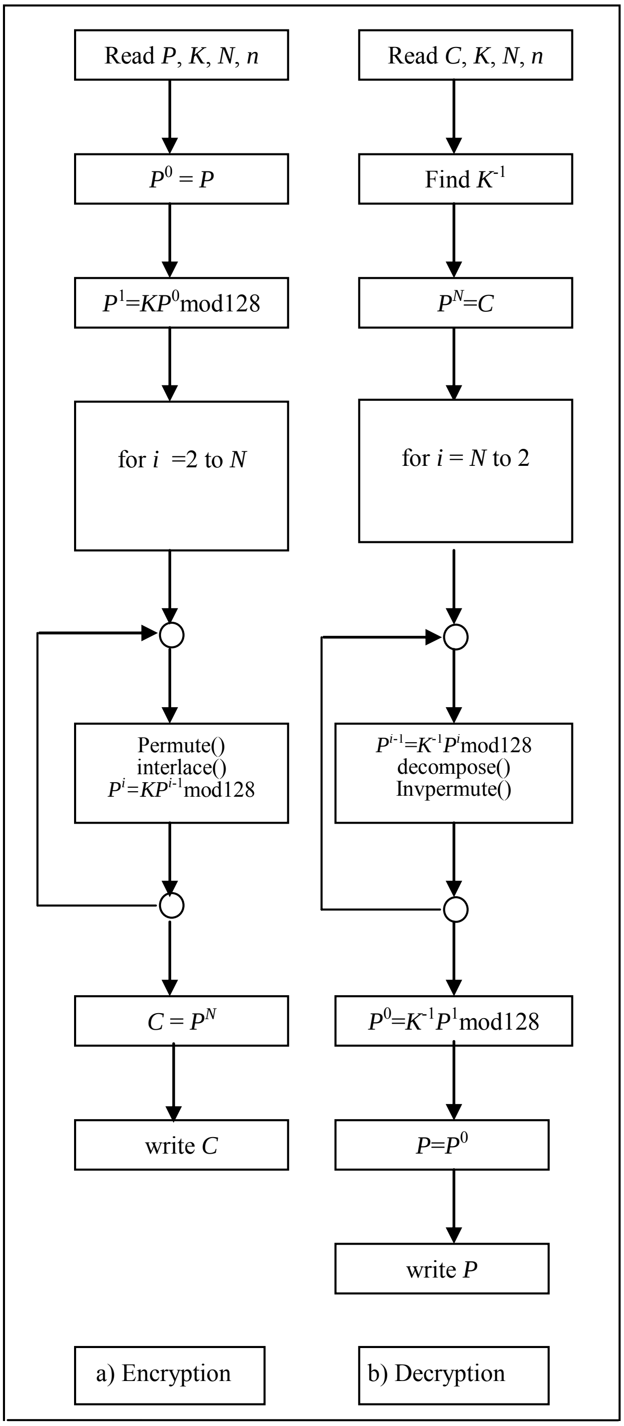

Fig. 1. Schematic diagram of the cipher

In this analysis, N denotes the number of iterations and it is taken as 16.

4. Illustration of the cipher

Let us consider the plain text given below:

(3) "**I am quite sure to assert that all the terrorists entered in to the jungle. Let us burn the forest without any lapse of time. Peace cannot be restored unless we do this immediately. Wish you best of luck**".

Let us focus our attention on the first sixty four characters of the above plain text given by

(4) "**I am quite sure to assert that all the terrorists entered in tob** ".

By using ASCII code, these characters can be represented as a matrix of size 8×8 and it assumes the form

(5)
$$P^0=\begin{bmatrix} 73 & 32 & 97 & 109 & 32 & 113 & 117 & 105 \\ 116 & 101 & 32 & 115 & 117 & 114 & 101 & 32 \\ 116 & 111 & 32 & 97 & 115 & 115 & 101 & 114 \\ 116 & 32 & 116 & 104 & 97 & 116 & 32 & 97 \\ 108 & 108 & 32 & 116 & 104 & 101 & 32 & 116 \\ 101 & 114 & 114 & 111 & 114 & 105 & 115 & 116 \\ 115 & 32 & 101 & 110 & 116 & 101 & 114 & 101 \\ 100 & 32 & 105 & 110 & 32 & 116 & 111 & 32 \end{bmatrix}.$$

The key matrix K is given by

(6)
$$K=\begin{bmatrix} 53 & 62 & 24 & 33 & 49 & 18 & 17 & 43 \\ 45 & 12 & 63 & 29 & 60 & 35 & 58 & 11 \\ 8 & 41 & 46 & 30 & 48 & 32 & 5 & 51 \\ 47 & 9 & 38 & 42 & 2 & 59 & 27 & 61 \\ 57 & 20 & 6 & 31 & 16 & 26 & 22 & 25 \\ 56 & 37 & 13 & 52 & 3 & 54 & 15 & 21 \\ 36 & 40 & 44 & 10 & 19 & 39 & 55 & 4 \\ 14 & 1 & 23 & 50 & 34 & 0 & 7 & 28 \end{bmatrix}.$$

On using the key matrix K and the plain text P, we apply (1) and obtain the modified P, denoted by P^1, as

(7)
$$P^1=\begin{bmatrix} 62 & 78 & 69 & 53 & 63 & 37 & 52 & 31 \\ 110 & 83 & 12 & 55 & 4 & 11 & 26 & 78 \\ 87 & 95 & 36 & 33 & 41 & 49 & 114 & 91 \\ 79 & 69 & 105 & 81 & 107 & 35 & 0 & 40 \\ 61 & 50 & 104 & 87 & 97 & 75 & 0 & 34 \\ 51 & 12 & 124 & 66 & 36 & 93 & 61 & 117 \\ 8 & 94 & 65 & 103 & 88 & 1 & 119 & 33 \\ 115 & 22 & 117 & 98 & 120 & 122 & 32 & 57 \end{bmatrix}.$$

By applying the process of permutation, described in Section 2, we get the transformed P^1 as

$$P^1 = \begin{bmatrix} 59 & 71 & 123 & 37 & 57 & 33 & 12 & 24 \\ 119 & 112 & 20 & 127 & 21 & 97 & 40 & 44 \\ 29 & 62 & 116 & 68 & 31 & 101 & 102 & 92 \\ 63 & 67 & 112 & 30 & 88 & 120 & 88 & 80 \\ 66 & 36 & 88 & 58 & 31 & 25 & 50 & 71 \\ 102 & 21 & 72 & 49 & 12 & 91 & 66 & 90 \\ 15 & 31 & 48 & 114 & 50 & 35 & 21 & 47 \\ 114 & 117 & 46 & 9 & 96 & 42 & 19 & 122 \end{bmatrix}. \tag{8}$$

On applying the interlacing process (see Section 2) on P^1, we obtain

$$P^1 = \begin{bmatrix} 31 & 75 & 72 & 43 & 66 & 93 & 18 & 97 \\ 85 & 90 & 18 & 98 & 79 & 4 & 53 & 29 \\ 86 & 59 & 124 & 1 & 80 & 120 & 38 & 103 \\ 12 & 96 & 93 & 122 & 97 & 4 & 54 & 70 \\ 7 & 119 & 61 & 57 & 11 & 46 & 13 & 47 \\ 124 & 52 & 98 & 112 & 22 & 17 & 92 & 93 \\ 55 & 106 & 106 & 74 & 124 & 8 & 92 & 102 \\ 118 & 64 & 39 & 40 & 19 & 45 & 43 & 70 \end{bmatrix}. \tag{9}$$

After carrying out all the sixteen rounds, we get the cipher text in the form

$$C = \begin{bmatrix} 110 & 15 & 113 & 48 & 54 & 62 & 44 & 82 \\ 58 & 83 & 32 & 47 & 113 & 25 & 101 & 73 \\ 76 & 60 & 98 & 34 & 80 & 27 & 97 & 48 \\ 73 & 107 & 109 & 27 & 106 & 68 & 90 & 74 \\ 9 & 54 & 4 & 52 & 26 & 87 & 64 & 107 \\ 121 & 15 & 126 & 14 & 23 & 108 & 54 & 2 \\ 94 & 26 & 109 & 81 & 117 & 64 & 85 & 29 \\ 84 & 94 & 115 & 69 & 35 & 121 & 117 & 115 \end{bmatrix}. \tag{10}$$

The modular arithmetic inverse of K, denoted by K^{-1}, is given by

$$K^{-1} = \begin{bmatrix} 27 & 40 & 53 & 3 & 117 & 48 & 25 & 2 \\ 41 & 60 & 17 & 92 & 5 & 21 & 106 & 81 \\ 57 & 39 & 116 & 118 & 18 & 0 & 37 & 116 \\ 94 & 97 & 52 & 27 & 94 & 102 & 104 & 19 \\ 63 & 123 & 117 & 0 & 98 & 9 & 97 & 32 \\ 61 & 50 & 54 & 60 & 101 & 12 & 69 & 56 \\ 64 & 41 & 57 & 22 & 73 & 75 & 49 & 122 \\ 71 & 61 & 17 & 32 & 42 & 88 & 81 & 113 \end{bmatrix}. \tag{11}$$

By applying K^{-1} on the cipher text C, from (2) we get

$$(12)\qquad P^N=\begin{bmatrix} 100 & 126 & 123 & 26 & 13 & 10 & 38 & 94 \\ 24 & 22 & 54 & 51 & 116 & 93 & 102 & 44 \\ 50 & 36 & 84 & 84 & 114 & 99 & 108 & 16 \\ 113 & 70 & 2 & 99 & 106 & 90 & 90 & 58 \\ 125 & 75 & 28 & 38 & 29 & 22 & 107 & 22 \\ 29 & 25 & 106 & 55 & 47 & 101 & 13 & 12 \\ 6 & 42 & 73 & 60 & 63 & 57 & 27 & 49 \\ 100 & 8 & 81 & 19 & 27 & 1 & 16 & 65 \end{bmatrix}.$$

On applying the decomposition algorithm (see Sections 2 and 3), the transformed P^N assumes the form

$$(13)\qquad P^N=\begin{bmatrix} 87 & 107 & 33 & 53 & 78 & 116 & 38 & 85 \\ 36 & 112 & 105 & 5 & 82 & 14 & 74 & 25 \\ 123 & 53 & 58 & 69 & 105 & 34 & 37 & 119 \\ 23 & 78 & 82 & 105 & 16 & 38 & 64 & 5 \\ 27 & 19 & 114 & 86 & 32 & 94 & 79 & 82 \\ 101 & 80 & 67 & 103 & 89 & 100 & 124 & 52 \\ 57 & 73 & 28 & 26 & 38 & 118 & 123 & 34 \\ 62 & 44 & 40 & 32 & 117 & 53 & 49 & 9 \end{bmatrix}.$$

We now apply the inverse permutation algorithm described in Section 3 on the P^N above obtained and get the new P^N as

$$(14)\qquad P^N=\begin{bmatrix} 83 & 116 & 18 & 52 & 75 & 81 & 21 & 21 \\ 79 & 74 & 91 & 77 & 57 & 44 & 104 & 0 \\ 54 & 52 & 96 & 41 & 71 & 107 & 31 & 33 \\ 15 & 83 & 1 & 15 & 98 & 24 & 50 & 79 \\ 116 & 54 & 49 & 9 & 2 & 92 & 66 & 39 \\ 90 & 108 & 77 & 7 & 40 & 10 & 14 & 74 \\ 91 & 0 & 112 & 75 & 7 & 126 & 110 & 63 \\ 60 & 94 & 115 & 81 & 54 & 85 & 91 & 5 \end{bmatrix}.$$

After carrying out all the sixteen rounds, we get the deciphered text in the form

$$(15)\qquad P=\begin{bmatrix} 73 & 32 & 97 & 109 & 32 & 113 & 117 & 105 \\ 116 & 101 & 32 & 115 & 117 & 114 & 101 & 32 \\ 116 & 111 & 32 & 97 & 115 & 115 & 101 & 114 \\ 116 & 32 & 116 & 104 & 97 & 116 & 32 & 97 \\ 108 & 108 & 32 & 116 & 104 & 101 & 32 & 116 \\ 101 & 114 & 114 & 111 & 114 & 105 & 115 & 116 \\ 115 & 32 & 101 & 110 & 116 & 101 & 114 & 101 \\ 100 & 32 & 105 & 110 & 32 & 116 & 111 & 32 \end{bmatrix}$$

that is the same as the plain text given in (5).

Let us now consider another example, wherein we have taken the complete plain text given by (3). This plain text is containing 207 characters. To represent this in the form of a matrix consisting of n rows and m columns, where $n = 8$ and m is having an appropriate value, depending on the number of characters, we add one more character ($ is added here) to the plain text. With this padding, the plain text is represented in the form of ASCII codes. For convenience of space, we present the transpose of the plaintext matrix as shown in (16):

$$
\begin{bmatrix}
73 & 32 & 97 & 109 & 32 & 113 & 117 & 105 \\
116 & 101 & 32 & 115 & 117 & 114 & 101 & 32 \\
116 & 111 & 32 & 97 & 115 & 115 & 101 & 114 \\
116 & 32 & 116 & 104 & 97 & 116 & 32 & 97 \\
108 & 108 & 32 & 116 & 104 & 101 & 32 & 116 \\
101 & 114 & 114 & 111 & 114 & 105 & 115 & 116 \\
115 & 32 & 101 & 110 & 116 & 101 & 114 & 101 \\
100 & 32 & 105 & 110 & 32 & 116 & 111 & 32 \\
116 & 104 & 101 & 32 & 106 & 117 & 110 & 103 \\
108 & 101 & 46 & 32 & 32 & 76 & 101 & 116 \\
32 & 117 & 115 & 32 & 98 & 117 & 114 & 110 \\
32 & 116 & 104 & 101 & 32 & 102 & 111 & 114 \\
101 & 115 & 116 & 32 & 119 & 105 & 116 & 104 \\
111 & 117 & 116 & 32 & 97 & 110 & 121 & 32 \\
108 & 97 & 112 & 115 & 101 & 32 & 111 & 102 \\
32 & 116 & 105 & 109 & 101 & 46 & 32 & 32 \\
80 & 101 & 97 & 99 & 101 & 32 & 99 & 97 \\
110 & 110 & 111 & 116 & 32 & 98 & 101 & 32 \\
114 & 101 & 115 & 116 & 111 & 114 & 101 & 100 \\
32 & 117 & 110 & 108 & 101 & 115 & 115 & 32 \\
119 & 101 & 32 & 100 & 111 & 32 & 116 & 104 \\
105 & 115 & 32 & 105 & 109 & 109 & 101 & 100 \\
105 & 97 & 116 & 101 & 108 & 121 & 46 & 32 \\
32 & 87 & 105 & 115 & 104 & 32 & 121 & 111 \\
117 & 32 & 98 & 101 & 115 & 116 & 32 & 111 \\
102 & 32 & 108 & 117 & 99 & 107 & 46 & 36
\end{bmatrix}. \tag{16}
$$

Here we perform interlacing and permutation as described in Section 2. Then, on adopting the process of encryption, we get the cipher text in hexadecimal notation, as shown below:

(17) F45CE2BBB263629C83A3DF35B015BB4574DD1A8C45A5CFD0C93D 6107DE4C2025E6D342505CD0206BC8FC8E55134C2F48DD61EC68739A4F0C 60CA5886728398191B858BB5E47B241D3A4E76D4FC0CFEBCAA749F72B672 D8EE12922F3276FD80FAFBB80ADA008D154E92C5942BAB7989A4C19CF0D FB37F761A6B9EB5DB2B4E89034162B3CF4A8410DD3A00435.

On using the process of decryption, we readily find that this cipher text can be brought into the form of the original plain text.

5. Cryptanalysis

Let us first consider the brute force attack. In the illustration of the cipher, we have taken an 8x8 matrix. Thus, the number of elements in the key matrix is 64. We take the numbers from 1 to 64 in a permuted order. There are 64! such permutations. One needs to check all these permutations to arrive at the correct key matrix. On the other hand, some researchers have estimated the key space of the Hill cipher [28, 29]. As per that, there will be 157, 248 possible invertible matrices for a 2×2 matrix for which a modular arithmetic (mod 26) exists. For a 3×3 matrix, the number is 1,634,038,189,056. A 4×4 matrix will have 12,303,585,972,327,392,870,400 possible invertible matrices. As we notice, the number grows by many orders with the increase in the order of the matrix. In our present cipher, we have taken the key matrix as 8×8 and a mod 128 is considered. With this, the exhaustive key space search will not be practical.

We now take the plain text attack. The Hill cipher exhibits vulnerability against the known plain text attack, as the cipher causes a direct relationship, such as
$X=KY$ mod 128.

If we can find Y^{-1}, the modular arithmetic inverse for Y, we can find K by applying

$$XY^{-1} \bmod 128 = KYY^{-1} \bmod 128 = K.$$

But in the present cipher, the relationship between the plain text and cipher text is not as simple as the one in the classical Hill cipher. The key dependent permutation and the interlacing at each step of the iteration prevent such direct relationship from being established, making it difficult to break the cipher using the known plain text attack. In the same aspect we say that no special choice of the plain text or the cipher text will help the crypt analyst in breaking the cipher using the chosen plain text/chosen cipher text attack.

6. Avalanche effect

Avalanche effect is a necessary condition for all modern block ciphers. It demonstrates the diffusion property of the block cipher. We have tested our cipher for a large number of plain texts and verified the avalanche effect. We are illustrating one case as an example.

By applying the encryption algorithm to the plain text given in (4), and using the key matrix K, the corresponding cipher text can be obtained as

(18) 11011100001111111000101100000111010101001101000000101111100110
0011110011000100100010100100111010111101101001101100010010110110000
0100011010011110010001111111111000011101011110001101011011011010001
1010100101111011100111000101011011001111100101100101001011100010011
0011100101100100110100000011011110000101100001101010100010010110101
0010100011010101011110000001101011001011111011000110110000001011101
01100000010101010011101010001111110011110101111 0011.

We now change the third character of the plaintext given in (4) from *a* to *c*. Then the modified plain text will be of the form

(19) "**I am quite sure to assert that all the terrorists entered in tob**".

It may be noted that the plain texts given in (4) and (19) differ by exactly one bit. The cipher text corresponding to the plain text given in (19) is

(20) 10011101100010100101111110110111000101000100110100110100100001
1101000010010011011010011001110001101010110111010111101100010011101
1100000010100000010000000101000100000000100110000100010110000100101
1000001001100111000100111011101100110010110001001010100110000110010
0011000100011111100100010100011110000000001101101010000110010111100
1011111010110001000100011011010001110101011101001110111101111011001
01101001110000111000110110011010010101000110000 1001.

We readily notice that the cipher texts given in (18) and (20) differ by 224 bits which is substantial.

Let us now change the key matrix element K_{25} form from 60 to 62. With this change, the original key and the modified key differ by one bit. By applying the modified key, the cipher text corresponding to the plain text given in (4) is obtained as

(21) 00001101111111101110100000011110001110100001110100101100010100
1000110110001110011110011000101100100001101100010101011101000010110
1000000001001110101001110010101011011001111110010001111001101100010
0111000111101100011100101110100010011101001110110010100100010001001
1111111010001110101110101111100011010110111000100101111110110111011
1001011001111101111101100110100101010101001010101000010110000111110
0011000000001000011000111000000100010111010000101 0010.

The cipher texts given in (18) and (21) differ by 234 bits, which is also very significant.

7. Computations and conclusions

In this paper we have extended the analysis of the modified Hill cipher by considering a plain text of any size. In this analysis we have illustrated the cipher by considering two cases. In the first one, the plain text is an 8×8 matrix and in the second one, it is of size 8×26.

The algorithms designed in this analysis are implemented in C language.

As the key size and the plain text size are significantly large, and as the iteration together with the permutation and the interlacing are effectively leading to diffusion and confusion, the cipher is resistant to crypt analytic attacks.

In the case of a complete plain text, which is taken in the form of a single block, the time required for encryption is 8.5×10^{-3} s and the time required for decryption is 13×10^{-3} s. These results indicate that the algorithm is quite efficient and it can be applied in any context for transmission of information. This analysis can be extended to the case, where we take multiple key matrices so that the process is further strengthened.

References

1. Hill, L. S. Cryptography in an Algebraic Alphabet. – American Mathematical Monthly, Vol. **36**, 1929, No 6, 306-312.
2. Hill, L. S. Concerning Certain Linear Transformation Apparatus of Cryptography. – American Mathematical Monthly, Vol. **38**, 1931, No 3, 135-154.
3. Stallings, W. Cryptography and Network Security Principles and Practices. 3rd Edition. New Jersey, Prentice Hall, 1999.
4. Sastry, V. U. K., N. Ravi Shankar. Modified Hill Cipher with Interlacing and Iteration. – Journal of Computer Science, Science Publications, Vol. **3**, 2007, No 11, 854-859.
5. Sastry, V. U. K., N. Ravi Shankar. Modified Hill Cipher for a Large Block of Plaintext with Interlacing and Iteration. – Journal of Computer Science, Science Publications, Vol. **4**, 2008, No 1, 15-20.
6. Sastry, V. U. K., N. Ravi Shankar, S. Durga Bhavani. A Modified Hill Cipher Involving Interweaving and Iteration. – International Journal of Network Security, Vol. **11**, 2010, No 1, 11-16.
7. Sastry, V. U. K., N. Ravi Shankar, S. Durga Bhavani. A Large Block Cipher Involving Interweaving and Iteration. – In: Proceedings of the International Conference on Advances and Emerging Trends in Computing Technologies (ICAET'10), 21-24 June 2010, Chennai, 328-333.
8. Sastry, V. U. K., N. Ravi Shankar, S. Durga Bhavani. A Modified Playfair Cipher Involving Interweaving and Iteration. – International Journal of Computer Theory and Engineering, Vol. **1**, December 2009, No 5, 594-598.
9. Sastry, V. U. K., N. Ravi Shankar, S. Durga Bhavani. A Modified Playfair Cipher for a Large Block of Plaintext. – International Journal of Computer Theory and Engineering, Vol. **1**, 2009, No 5, 590-594.
10. Sastry, V. U. K., N. Ravi Shankar, S. Durga Bhavani. A Generalized Playfair Cipher Involving Intertwining, Interweaving and Iteration. – International Journal of Networks and Mobile Technology, Vol. **1**, 2010, No 2, 45-53.
11. Sastry, V. U. K., N. Ravi Shankar, S. Durga Bhavani. A Blending of A Generalized Playfair Cipher and A Modified Hill Cipher. – International Journal of Networks and Mobile Technologies, Vol. **2**, 2011, No 1, 35-43.
12. Sastry, V. U. K., V. Janaki. On the Modular Arithmetic Inverse in the Cryptology of Hill Cipher. – In: Proceedings of North American Technology and Business Conference, September 2005, Montreal, Canada.
13. Levine, J., R. E. Hartwig. Applications of the Drazin Inverse to the Hill Cryptographic System. Part I. – Cryptologia, Vol. **4**, 1980, No 2, 71-85.
14. Levine, J., R. E. Hartwig. Applications of the Drazin Inverse to the Hill Cryptographic System. Part II. – Cryptologia, Vol. **4**, 1980, No 3, 150-168.
15. Levine, J., R. E. Hartwig. Applications of the Drazin Inverse to the Hill Cryptographic System. Part III. – Cryptologia, Vol. **5**, 1981, No 2, 67-77.
16. Levine, J., R. E. Hartwig. Applications of the Drazin Inverse to the Hill Cryptographic System. Part IV. – Cryptologia, Vol. **5**, 1981, No 4, 213-228.
17. Makar, B. H. Application of a Certain Class of Infinite Matrices to the Hill Cryptographic System. – Cryptologia, Vol. **7**, 1983, No 1, 63-78.
18. Levine, J., R. Chandler. The Hill Cryptographic System with Unknown Cipher Alphabet, But Known Plaintext. – Cryptologia, Vol. **13**, 1989, No 1, 1-28.
19. Kiele, W. A. A Tensor-Theoretic Enhancement to the Hill Cipher System. – Cryptologia, Vol. **14**, 1990, No 3, 225-233.
20. Thilaka, B., K. Rajalakshmi. An Extension of Hill Cipher Using Generalized Inverses and mth Residue modulo n. – Cryptologia, Vol. **29**, 2005, No 4, 267-276.
21. Saeednia, S. How to Make the Hill Cipher Secure. – Cryptologia, Vol. **24**, 2000, No 4, 353-360.

22. Y e h, Y. S., T. C. W u, C. C. C h a n g, W. C. Y a n g. A New Cryptosystem Using Matrix Transformation. – In: Proceedings of the 25th IEEE International Carnahan Conference on Security Technology, 1991, 131-138.
23. M a h m o u d, A. Y., A. G. C h e f r a n o v. Hill Cipher Modification Based on Eigenvalues HCM-EE. – In: Proceedings of the Second International Conference on Security of Information and Networks (SIN2009), Gazimagusa (TRNC) North Cyprus, A. Elci, M. Orgun, A. Chefranov, (Eds) ACM, New York, USA, 2009, 164-167.
24. M a h m o u d, A. Y., A. G. C h e f r a n o v. Hill Cipher Modification Based on Pseudo-Random Eigenvalues. – Fourth coming paper, to appear in Applied Mathematics & Information Sciences.
25. L i n, C. H., C. Y. L e e, C. Y. L e e. Comments on Saeednia's Improved Scheme for the Hill Cipher. – Journal of the Chinese Institute of Engineers, Vol. **27**, 2004, No 5, 743-746.
26. T o o r a n i, M., A. F a l a h a t i. A Secure Cryptosystem Based on Affine Transformation. – Journal of Security and Communication Networks, Vol. **4**, 2011, No 2, 207-215.
27. T o o r a n i, M., A. F a l a h a t i. A Secure Variant of the Hill Cipher. – In: Proceedings of the 14th IEEE Symposium on Computers and Communications (ISCC'09), July 2009, 313-316.
28. O v e r b e y, J., W. T r a v e s, J. W o j d y l o. On the Keyspace of the Hill Cipher. – Cryptologia, Vol. **29**, 2005, No 1, 59-72.
29. B a u e r, C., K. M i l l w a r d. Cracking Matrix Encryption Row by Row. – Cryptologia, Vol. **31**, 2007, 76-83.