A Modified Hill Cipher Involving Interweaving and Iteration

V. Umakanta Sastry[1], N. Ravi Shankar[2], and S. Durga Bhavani[3]

(Corresponding author: V. Umakanta Sastry)

Director, SCSI, Dean (R&D), Sreenidhi Institute of Science and Technology, Hyderabad, India[1]

CSE Department, SNIST, Hyderabad, India[2]

SIT, JNT University, Hyderabad, India[3]

(Email: vuksastry@rediffmail.com)

(Received Nov. 24, 2008; revised and accepted May 4 & May 12, 2009)

Abstract

This paper deals with a modification of the Hill cipher. In this, we have introduced interweaving in each step of the iteration. The interweaving of the resulting plaintext, at each stage of the iteration, and the multiplication with the key matrix leads to confusion and diffusion. From the cryptanalysis performed in this investigation, we have found that the cipher is a strong one.

Keywords: Interweaving, inverse interweaving, modular arithmetic inverse

1 Introduction

In the literature of cryptography, it is well known that, confusion and diffusion play a vital role in the development of a cipher [3, 4, 5]. The transposition or permutation of characters in the plaintext is responsible for confusion, and the influence of each bit of the key on each plaintext bit causes diffusion.

The study of the classical Hill cipher [12], in which, a matrix containing numbers is used as a key in the encryption process, and the modular arithmetic inverse of the key is employed in the decryption process, has attracted the attention of several researchers [6, 7, 8, 9, 10, 11] in the recent years. In the Hill cipher, the basic steps of encryption and decryption are given by

$$C = PK \bmod 26,$$

and

$$P = K^{-1}C \bmod 26,$$

where P is the plaintext, K the key matrix, C the ciphertext and K^{-1} is the modular arithmetic inverse of K. Here, he has taken mod 26, as he focused his attention on the 26 characters of English alphabet.

Subsequently, Feistel [2] analyzed the general principles of block ciphers and lead to the development of Data Encryption Standard (DES). In this, the length of the key is 56 bits, and the length of the plaintext block is 64 bits. In DES, as the length of the key is only 56 bits, it is found that this cipher is breakable with a good deal of effort by brute force attack. In view of this fact, several variants, of DES, such as 2DES and 3DES came into existence. However, these are found to be relatively sluggish in software. In the light of this, at the end of the last century, Joan Daeman and Vincent Rijman developed an algorithm called Advanced Encryption Standard (AES). In this, the block length is 128-bit and the key length is 128, 192 or 256 bits. This cipher is found to be a strong one.

In a recent investigation [7, 10], we have used a new concept called interlacing, and modified the Hill cipher. In the process of interlacing, mixing of binary bits is carried out in a row wise manner, i.e., binary bits of the elements of each row are separately mixed. This process, included in each iteration, strengthens the cipher.

In the present paper, we modify the Hill cipher by introducing interweaving (transposition of the binary bits of the plaintext characters belonging to the neighboring rows and columns) and iteration. In this, the multiplication of the plaintext with the key matrix, the interweaving and the iteration cause a lot of diffusion and confusion. Here, our objective is to develop a strong block cipher, whose key length is significantly large.

In Section 2, we present the development of the cipher. We design the algorithms for encryption, decryption, modular arithmetic inverse, interweaving, and inverse interweaving in Section 3. In Section 4, we illustrate the cipher with an example. We discuss the cryptanalysis in Section 5, and mention the avalanche effect in Section 6. Finally, in Section 7, we draw conclusions from the computations carried out in this analysis.

2 Development of the Cipher

Consider a plaintext P of 2n characters. By using the ASCII code, let us represent P in the form of a matrix, given by

$$P = [P_{ij}], i = 1 \text{ to } n, \ j = 1 \text{ to } 2.$$

Let $K = [K_{ij}]$, $i = 1$ to n, $j = 1$ to n, be the key matrix, in which all the elements are less than 128. The process of encryption can be described by the following equations.

$$\begin{aligned} P_0 &= P, \\ P^i &= < KP^{i-1} \bmod 128 >, i = 1 \text{ to } N, \\ C &= KP^N \bmod 128. \end{aligned}$$

Here, <> denote interweaving of the resulting matrix in a column wise and a row wise manner and C is the ciphertext.

The process of decryption is governed by the relations

$$\begin{aligned} P_N &= K^{-1}C \bmod 128, \\ P^{i-1} &= > K^{-1}P^i \bmod 128 <, i = N \text{ to } 1, \\ P &= P^0. \end{aligned}$$

In this, >< denotes the reverse process of interweaving and K^{-1} is the modular arithmetic inverse of K.

The process of interweaving can be described as follows.

Let $[Q_{ij}]$, $i = 1$ to n, $j = 1$ to 2 be the transformed plaintext matrix obtained after performing the multiplication with the key matrix and taking mod 128. On converting each element of $[Q_{ij}]$ into binary form, we get a new matrix

$$[b_{il}], i = 1 \text{ to } n, \ l = 1 \text{ to } 14.$$

Thus we have $[b_{il}] = \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{114} \\ b_{11} & b_{11} & \cdots & b_{214} \\ . & . & . & . \\ b_{n1} & b_{n2} & \cdots & b_{n14} \end{bmatrix}$

We rotate the first column and see that it assumes the form $[b_{21}, b_{31}, \cdots b_{n1}, b_{11}]^T$, where T denotes the transpose of the vector. Here, each element has gone one step up and the first element has come down to the last position. This process is carried out for columns 1, 3, 5 and so on. Similarly, we carry out a circular left shift of the rows numbered 2, 4, 6, $\cdots$ etc. After carrying out the aforementioned steps, the matrix assumes the form

$$[b_{il}] = \begin{bmatrix} b_{21} & b_{12} & b_{23} & \cdots & b_{213} & b_{114} \\ b_{22} & b_{33} & b_{24} & \cdots & b_{214} & b_{31} \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ b_{n2} & b_{11} & b_{n4} & \cdots & b_{n14} & b_{11} \end{bmatrix}$$

Then we construct the modified plaintext matrix P wherein, the elements of the first column of P are obtained from the first seven columns of $[b_{il}]$, and the second column of P from the subsequent seven columns of $[b_{il}]$.

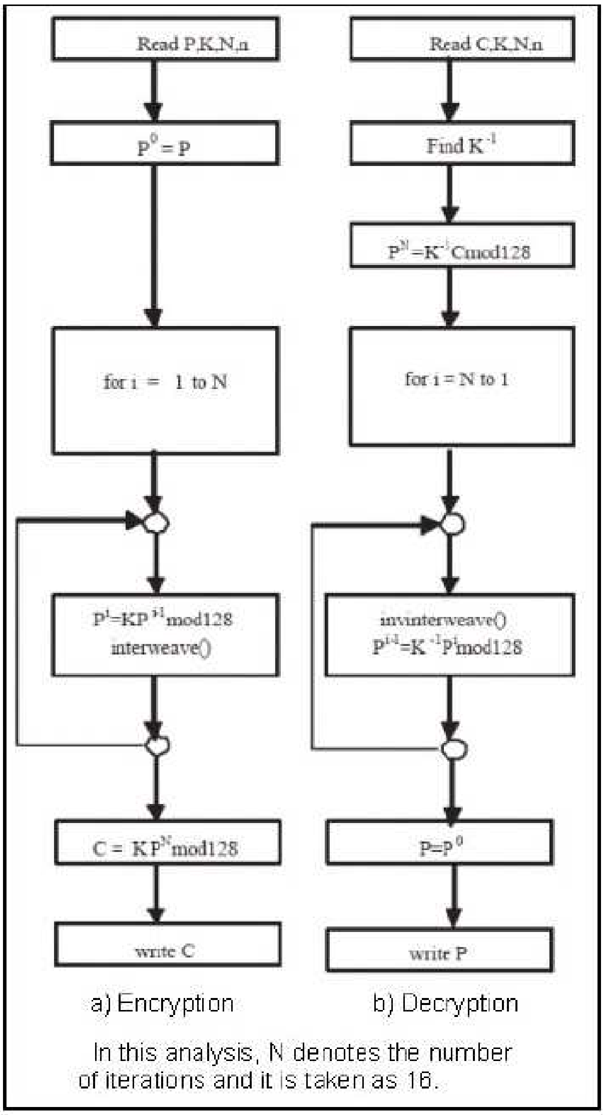

Figure 1: Schematic diagram of the cipher

This completes the process of interweaving. We denote the reverse process of interweaving as inverse interweaving.

The schematic diagram of the cipher is given in Figure 1. This shows the processes of the encryption and the decryption in detail.

3 Algorithms

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

3.1 Algorithm for Encryption

1) read n, N, K, P;

2) $P_0 = P$;

3) for $i = 1$ to N {
$P^i = KP^{i-1}$ mod 128;
$interweave()$;
}

4) $C = KP^N$ mod 128;

5) write C;

3.2 Algorithm for Decryption

1) read n, N, K, C;

2) find modinverse(K);

3) $P^N = K^{-1}C$ mod 128;

4) for $i = N$ to 1 {
invinterweave();
$P^{i-1} = K^{-1}Pi$ mod 128;
}

5) $P= P_0$;

6) write P;

3.3 Algorithm for Modinverse

1) read n, K;

2) find K_{ij}, Δ; /* K_{ij} are cofactors of the elements of K, and $\triangle$ is the determinant of K */

3) find d such that $(d\triangle)$ mod 128 = 1;/* d is the multiplicative inverse of $\triangle$ */

4) $K^{-1} = (K_{ji}d)$ mod 128;

3.4 Algorithm for Modinverse

1) read n, K;

2) find K_{ij}, $\triangle$; /* K_{ij} are the cofactors of the elements of K, and $\triangle$ is the determinant of K */

3) find d such that $(d\triangle)$ mod 128 = 1;/* d is the multiplicative inverse of $\triangle$ */

4) K^{-1}=$(K_{ji}d)$ mod 128;

3.5 Algorithm for Interweave

1) convert P^i into binary bits;

2) construct $[b_{ij}]$, $i = 1$ to n, $j = 1$ to 14;

3) for $j = 1$ to 14 in Step 2 {
$k = b_{1j}$;
for $i = 1$ to $n - 1$
{
$b_{ij} = b_{(i+1)j}$;
}
$b_{nj} = k$;
}

4) for $i = 2$ to n in step 2 {
$k = b_{i1}$;
for $j = 1$ to 13 {
$b_{ij} = b_{i(j+1)}$;
} $b_{i14} = k$; }

5) Construct P_i from b_{ij};

4 Illustration of the Cipher

Consider a plaintext given below.
The development of the nuclear technology of all the developed countries must be watched carefully by a super committee consisting of representatives of all the countries. This ensures the safety of all the nations if and only if a resolution is taken in this direction.

Let us focus our attention on the first sixteen characters given by "*The development*".

On substituting ASCII codes for these characters, and arranging them in the form of a matrix, we get

$$P = \begin{bmatrix} 84 & 109 \\ 104 & 111 \\ 101 & 112 \\ 32 & 109 \\ 100 & 101 \\ 101 & 110 \\ 118 & 116 \\ 101 & 32 \end{bmatrix} \tag{1}$$

Let us take the key matrix K as

$$K = \begin{bmatrix} 53 & 62 & 124 & 33 & 49 & 118 & 107 & 43 \\ 45 & 112 & 63 & 29 & 60 & 35 & 58 & 11 \\ 88 & 41 & 46 & 30 & 48 & 32 & 105 & 51 \\ 47 & 99 & 36 & 42 & 112 & 59 & 27 & 61 \\ 57 & 20 & 6 & 31 & 106 & 126 & 22 & 125 \\ 56 & 37 & 113 & 52 & 3 & 54 & 105 & 21 \\ 36 & 40 & 43 & 100 & 119 & 39 & 55 & 94 \\ 14 & 81 & 23 & 50 & 34 & 70 & 7 & 28 \end{bmatrix}$$

On multiplying the plaintext matrix with the key matrix, we get the modified P, denoted by P^1, as

$$P^1 = \begin{bmatrix} 27 & 112 \\ 17 & 83 \\ 83 & 113 \\ 108 & 41 \\ 37 & 25 \\ 38 & 86 \\ 59 & 61 \\ 127 & 11 \end{bmatrix}$$

On converting the numbers in these two columns into binary form and constructing the matrix b, we get

$$b = \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

On performing interweaving (see Section 2), we get the transformed b as

$$b = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}$$

We now convert these binary bits into decimal numbers and construct the modified P as

$$P^1 = \begin{bmatrix} 35 & 98 \\ 19 & 83 \\ 114 & 67 \\ 100 & 57 \\ 79 & 56 \\ 46 & 23 \\ 118 & 82 \\ 95 & 90 \end{bmatrix}$$

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

$$C = \begin{bmatrix} 114 & 8 \\ 100 & 65 \\ 56 & 81 \\ 71 & 24 \\ 8 & 81 \\ 37 & 4 \\ 0 & 73 \\ 117 & 99 \end{bmatrix} \quad (2)$$

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

$$K^{-1} = \begin{bmatrix} 35 & 46 & 15 & 49 & 89 & 0 & 77 & 16 \\ 1 & 126 & 107 & 112 & 15 & 51 & 50 & 69 \\ 7 & 49 & 24 & 28 & 96 & 38 & 117 & 44 \\ 76 & 111 & 44 & 75 & 78 & 98 & 36 & 73 \\ 33 & 91 & 27 & 6 & 6 & 49 & 27 & 72 \\ 25 & 114 & 56 & 102 & 99 & 88 & 27 & 92 \\ 48 & 101 & 23 & 112 & 39 & 35 & 39 & 94 \\ 71 & 55 & 69 & 18 & 106 & 30 & 63 & 85 \end{bmatrix}$$

It is to be noted that the modular arithmetic inverse of the key matrix K exists only when K is nonsingular and the determinant of K is relatively prime to 128. It can be readily verified that $KK^{-1} \bmod 128 = K^{-1}K \bmod 128 = I$.

On taking the C given in Equation (2), and applying the decryption process, we get the P^N as

$$P^N = \begin{bmatrix} 5 & 107 \\ 2 & 93 \\ 96 & 58 \\ 24 & 56 \\ 125 & 115 \\ 16 & 104 \\ 41 & 32 \\ 47 & 40 \end{bmatrix}$$

On applying the inverse interweaving process described in Section 2, we get the modified P^N as

$$P^N = \begin{bmatrix} 106 & 32 \\ 2 & 93 \\ 18 & 93 \\ 48 & 61 \\ 92 & 56 \\ 58 & 121 \\ 20 & 64 \\ 5 & 120 \end{bmatrix}$$

After carrying out all the sixteen iterations, we get the plaintext in the form

$$P = \begin{bmatrix} 84 & 109 \\ 104 & 111 \\ 101 & 112 \\ 32 & 109 \\ 100 & 101 \\ 101 & 110 \\ 118 & 116 \\ 101 & 32 \end{bmatrix}$$

This is the same as the plaintext given in Equation (1).

5 Cryptanalysis

In the case of the Hill cipher, we have a direct relation between the plaintext P and the ciphertext C, where P and C are column vectors. This relation is given by

$$C = KP \bmod 26.$$

On using the known plaintext and ciphertext pairs, we can write an equation of the form

$$X = KY \bmod 26, \quad (3)$$

where Y is the plaintext matrix, and X is the ciphertext matrix.

From Equation (3), we can write

$$K = XY^{-1} \bmod 26.$$

Thus, the Hill cipher is broken.

In the case of the present cipher, as the interweaving and the iteration hinder obtaining a direct relation between the plaintext and the ciphertext, this cipher cannot be broken by the known plaintext attack.

Let us now consider the brute force (ciphertext only) attack. As the length of the plaintext block is sixteen characters, i.e., 112 binary bits, the space of the plaintext is $2^{112} \approx 10^{33.6}$. As the computation of the ciphertext in all these possible cases is unwieldy, brute force attack, in this way, is ruled out. In this cipher, the key matrix is of size $n \times n$, and each element of the key matrix lies between 0 and 127. Thus, the size of the key space is 2^{7n^2}. Identifying this key matrix by brute force attack is totally prohibitive when n $\geq$ 4. Thus the cipher cannot be broken by this attack.

The rest of the approaches such as chosen plaintext attack and chosen ciphertext attack are also impossible as the interweaving and the iteration lead to a lot of confusion and diffusion.

Hence, this cipher is a very strong one and it cannot be broken by any cryptanalytic attack.

6 Avalanche Effect

The plaintext given in (1) can be represented in its binary form as

$$\begin{array}{l}1010100110110011010001101111111001\\0111100000010000011011011100100110\\0101110010111011101110110111101001\\1001010100000.\end{array} \tag{4}$$

On changing the 9^{th} character from l to m, the modified plaintext (in its binary representation) assumes the form

$$\begin{array}{l}10101001101101110100011011111111001011\\11000001000000110110111001001100101111\\00101110111011101101110100110010101 0\\0000.\end{array} \tag{5}$$

It may be noted that the plaintexts given in Equations (4) and (5) differ by exactly one bit.

The cipher text corresponding to the plaintext given in Equation (4) is

$$\begin{array}{l}111001011001000111000100011100010000 10\\010100000001110101000100010000011010 00\\1001100010100010000100100100111000 11.\end{array} \tag{6}$$

The ciphertext pertaining to the plaintext given in Equation (5) can be obtained as

$$\begin{array}{l}0000001010001000011100010000011111010 00\\0100110001111101011111000010000100001 10\\001011110001101111110000000111100101.\end{array} \tag{7}$$

It can be readily seen that the ciphertexts given in Equations (6) and (7) differ by 57 bits, which is very significant.

We now change the key element K_{36} from 32 to 33. With this change, the original key and the modified key differ by exactly one bit. On applying the modified key on the original plaintext, given in Equation (1), we get the ciphertext as

$$\begin{array}{l}0101100100100110000111000110101001010 1\\1001100111001011000000010010110001000 0\\00100000101100010011110101001100110 00.\end{array} \tag{8}$$

It can be noticed that the ciphertexts given in Equations (6) and (8) differ by 62 bits, which very substantial.

From the above discussion, we conclude that this cipher produces strong avalanche effect and hence the cipher is a strong one.

7 Computations and Conclusions

In this paper, we have developed a block cipher by introducing interweaving and iteration. As the interweaving is done in each step of the iteration, the plaintext has undergone several transformations before it has become the ciphertext. The cryptanalysis and the avalanche effect have fully indicated that the cipher is a very strong one and it cannot be broken by any cryptanalytic attack.

The algorithms presented in this paper for encryption and decryption are implemented in C language.

The modular arithmetic inverse of the 8×8 matrix is calculated by using the systematic procedure developed in [6].

The ciphertext corresponding to the entire plaintext given in Section 4 is presented below in hexadecimal notation.

E591C4710940751106898A2124E3748
854D546D204894FFC5EDA5055E8737
89485440D23B6A7989668A72A6BDC
F7BCFB82315BAEC7D8429E0EBAD
C4B04D242F5264C45BD452EE5512F7
74EEE9BCDC0B1C3E4B76EC4173BC
14AFCD853E3922818165D3037C198D
1743381A79A1A24C058B843A13D67
C13CBFD585E2450EE495EA8081A4D
4F37FBD1CF7C898B7.

The time required for encryption and decryption of the plaintext given in Section 4 is $6.1 * 10^{-3}$ and $12*10^{-3}$ seconds respectively. The cipher developed in this analysis is a potential one and it is quite comparable with all the other block ciphers existing in the literature.

The analysis presented in this paper can be extended to the case, wherein the plaintext block is enormously large. This problem is considered in the ensuing paper.

References

[1] A. Bagherzandi, M. Salmasizadeh, and J. Mohajeri, "A related key attack on the feistel type block ciphers," *International Journal of Network Security*, vol. 8, no. 3, pp. 221-226, 2009

[2] H. Feistel, "Cryptography and computer privacy," *Scientific American*, vol. 228, pp. 15-23, 1973.

[3] H. A. A. Hassan, M. Saeb, and H. D. Hamed, "The PYRAMIDS block cipher," *International Journal of Network Security*, vol. 1, no. 1, pp. 52-60, 2005.

[4] Y. Kurniawan, A. S. A., M. S. Mardiyanto, I. S. S., and S. Sutikno, "The new block cipher: BC2," *International Journal of Network Security*, vol. 8, no. 1, pp. 16-24, 2009.

[5] P. Lin, W. L. Wu, C. K. Wu, "Security analysis of double length compression function based on block cipher," *International Journal of Network Security*, vol. 4, no. 2, pp. 121-127, 2007.

[6] V. U. K. Sastry, and V. Janaki, "On the modular arithmetic inverse in the cryptology of hill vipher," *Proceedings of North American Technology and Business Conference*, pp. 105, Montreal, Canada, Sep. 2005.

[7] V. U. K. Sastry, and N. Ravi Shankar, "Modified hill cipher with interlacing and iteration," *Journal of Computer Science*, vol. 3, no. 11, pp. 854-859, Science Publications, 2007.

[8] V. U. K. Sastry, and V.Janaki, "A block cipher using linear congruences," *Journal of Computer Science*, vol. 3, no. 7, pp. 556-561, Science Publications, 2007.

[9] V. U. K. Sastry, and V. Janaki, "A large block cipher using linear congruences," *World Congress on Engineering and Computer Science, WCECS*, pp. 294, Sanfrancisco, USA, 2007.

[10] V. U. K. Sastry, and N. R. Shankar, "Modified hill cipher for a large block of plaintext with interlacing and iteration," *Journal of Computer Science*, vol. 4, no. 1, pp. 15-20, Science Publications, 2008.

[11] V. U. K. Sastry, and V. Janaki, "A modified hill cipher with multiple keys," *International Journal of Computational Science*, vol. 2, no. 6, pp. 815-826, 2008.

[12] L. S. Hill, "Cryptography in an algebraic alphabet," *The American Mathematical Monthly*, vol. 36, pp. 306-312, 1929.

V. Umakanta Sastry was formerly a professor at Indian Institute of Technology, Kharagpur, India. Presently he is the Director, School of Computer Science and informatics and Dean (R&D) at Sree Nidhi Institute of Science and Technology, Hyderabad, India. He is currently guiding a number of Research Scholars for Ph.d in the areas of Information Security and Image Processing.

N. Ravi Shankar is a Professor and is currently heading the department of Computer Science and Engineering, Sree Nidhi Institute of Science and Technology, Hyderabad, India. He is actively engaged in research in the area of Information Security.

S. Durga Bhavani has obtained her Ph.D from University of Hyderabad, India in the area of Evidential Reasoning. She is presently a Professor in Computer Science & Engineering, School of Information Technology, JNT University, Hyderabad, India. Her research interests are applications of uncertain reasoning techniques and Information Security.