A Cipher based on 3D Array Block Rotation

P. R. Suri† and Sukhvinder Singh Deora††

†Associate Professor, Department of Computer Science & Applications, Kurukshetra University, Kurukshetra, (Haryana) India.
††Assistant Professor, Department of Computer Applications, N.C. Institute of Computer Sciences, Israna, Panipat, (Haryana) India.

Summary
Security of the information over the insecure mode of communication, Internet, has been an area of research for years. There have been several techniques developed for encryption/decryption of the information over the years by various agencies. This paper discusses a new technique of enciphering data which enables good diffusion and is having a unique technique of decrypting it back to the plaintext and is easy to implement using 3D Array rotations.

Key words:
Encoding, Decoding, Block cipher, 3D Array, Confusion-Diffusion

1. Introduction

Since the conception of mankind, human beings tried to communicate between themselves for several reasons. Security of information has always played a central role while communication. The threats to the secure information transfer are many and we require a variety of countermeasures to safeguard our information. [] Data encryption/decryption is a primary method of protecting valuable electronic information.

1.1 Cipher

Cipher is a message written in a secret code. It can be thought of as a cryptographic system in which units of plaintext of regular length, usually letters are arbitrarily transposed or substituted according to a predetermined code (encoding technique) to convert it to ciphertext.

Fig. 1 Encoding.

The ciphertext is then transferred over the non-secure medium of communication and received by the receiver. The receiver then applies the decoding technique in accordance to the encoding technique to get the actual plaintext communicated to him by the sender.

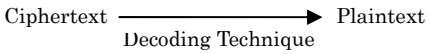

Fig. 2 Decoding.

1.2 Some Algorithms

The basic idea behind any cryptographic algorithm is same, using confusion and diffusion to change the actual information so that it is only the intended user who can decode and understand it. Still, there have been simple to complex algorithms like the Hill Cipher and Vernam Cipher to the DES, AES and A5 algorithms, which proved to be useful in the history and some of which are in use till date.

2. Our Algorithm

2.1 Characteristics

We are proposing a cipher which uses confusion and diffusion to encipher the text and uses the a random sequence generator which is capable of producing unique sequence of numbers each time it is started afresh using some specific seed (this condition is to ensure that there is a different ciphertext of the same plaintext each time encoding is done). It is assumed that the sender and receiver had such agreed upon generator at each end before actually communicating using this technique.

2.2 The Structure

We can use a three dimensional matrix to store the initial plaintext. The plaintext may also be stored as row-major/column major fashion, as agreed between the sender and receiver. Considering the three axis as the axis of rotation, X, Y and Z, as shown in Fig. 3, and each layer as a rotatable plate, we can diffuse the text using clockwise rotation of 90/180/270° of particular plate at a particular axis.

Manuscript received February 5, 2010
Manuscript revised February 20, 2010

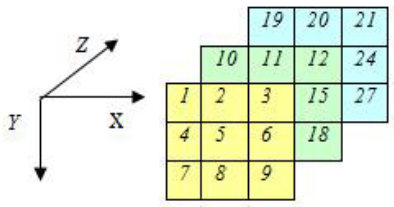

Fig. 3 The Structure.

2.3 Encryption Process

The process of rotation of plates can be repeated for some number of rounds, say n, to get the text diffused. The ciphertext can be obtained by collecting the text from the structure in the same row-major/column-major fashion, as it was stored.

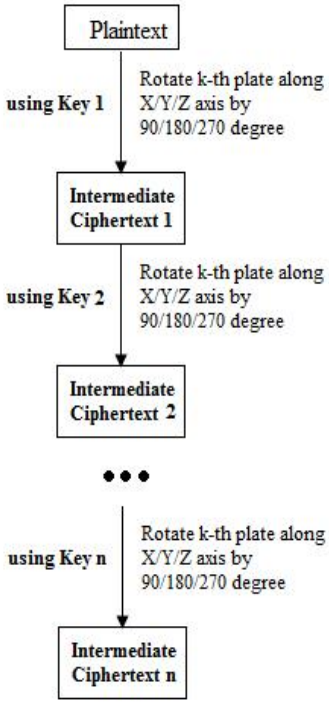

Fig. 4 Encryption Process

2.4 The Structure

We can use a three dimensional matrix to store the initial plaintext. Considering the three axis as the axis of rotation as shown in Fig. 3, and each layer, as shown in Fig. 5, as a rotatable plate, we can diffuse the text using clockwise rotations on a particular axis and plate number for 1/2/3 rotations. This can be done by using a random number generating function which generates unique sequence of numbers each time. We can generate two random numbers at a time. First one is say RAND_AXIS and other one is RAND_ROT. The two numbers can be used alternatively to determine the plate number to be rotated.

Set AxisOfRotation = RAND_AXIS % 3

Set NumberOfRotations = RAND_ROT % 3

Set PlateNumber = (RAND_AXIS+RAND_ROT) % n

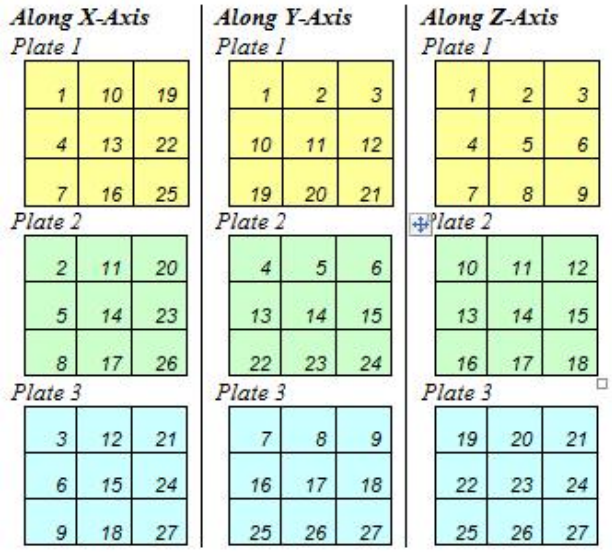

Fig. 5 Axis-wise Plates view for 3X3X3 Array

We are then to use minimum of 16 rotations for a 3X3X3 matrix and then communicate the ciphertext along with the seed to the intended receiver. He, on looking at the size of the text can generate the sequence of numbers to be used for reversing the entire process.

Initial lab experimentations done on randomly selected data and using Turbo C's Random Number Generator, has shown that 16 rotations for a 4X4X4 matrix and 16 rotations for a 5X5X5 matrix are sufficient to confuse and diffuse the entire data. It is however recommended to use 16-32 rotations as per the volume of data to be encrypted.

3. Some Results

On implementing the above algorithm on data of the size comparable to that of from a 3X3X3 matrix upto 5X5X5 matrix, the results comply to high level of diffusion.

--------TEST DATA 1----------
1 2 3 4 5 6 7 8 ← Shows input bit sequence
-----------ENCRYPTION ENDS-------------
2 6 1 7 4 3 8 5←Shows the bits shuffling after encryption
rotation sequence is-------
1 0 2 0 1 1 0 1 1 0 1 0 1 1 0 0
-----------DECRYPTION ENDS-------------
1 2 3 4 5 6 7 8 ←Shows decrypted bit sequence

--------TEST DATA 2----------
1 2 3 4 5 6 7 8 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27
1 1 ----------Rotation from Y--------
2 1 ----------Rotation from Z--------
1 1 ----------Rotation from Y--------
0 1 ----------Rotation from X--------
1 1 ----------Rotation from Y--------
1 2 ----------Rotation from Y--------
1 1 ----------Rotation from Y--------
0 1 ----------Rotation from X--------
-----------ENCRYPTION ENDS-------------
1 26 3 4 11 6 25 20 7 16 23 10 13 14 15 8 5 2 19 12 21 22 17 24 27 18 9
Reverse sequence is-------
0 1----------Rotation from X--------
1 1----------Rotation from Y--------
1 2----------Rotation from Y--------
1 1----------Rotation from Y--------
0 1----------Rotation from X--------
1 1----------Rotation from Y--------
2 1----------Rotation from Z--------
1 1----------Rotation from Y--------
-----------DECRYPTION ENDS-------------
1 2 3 4 5 6 7 8 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27

--------TEST DATA 3----------
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27
1 1----------Rotation from Y--------
2 1 ----------Rotation from Z--------
1 1 ----------Rotation from Y--------
0 1 ----------Rotation from X--------
1 1 ----------Rotation from Y--------
1 2 ----------Rotation from Y--------
1 1 ----------Rotation from Y--------
0 1 ----------Rotation from X--------
0 0 ----------Rotation from X--------
2 0 ----------Rotation from Z--------
2 1 ----------Rotation from Z--------
2 2 ----------Rotation from Z--------
2 2 ----------Rotation from Z--------
0 0 ----------Rotation from X--------
1 1 ----------Rotation from Y--------
0 1 ----------Rotation from X--------
-----------ENCRYPTION ENDS-------------
9 18 19 2 13 4 1 16 3 24 23 22 17 14 11 20 5 10 21 12 25 8 15 26 7 6 27
Reverse sequence is-------
0 1----------Rotation from X--------
1 1----------Rotation from Y--------
0 0----------Rotation from X--------
2 2----------Rotation from Z--------
2 2----------Rotation from Z--------
2 1----------Rotation from Z--------
2 0----------Rotation from Z--------
0 0----------Rotation from X--------
0 1----------Rotation from X--------
1 1----------Rotation from Y--------
1 2----------Rotation from Y--------
1 1----------Rotation from Y--------
0 1----------Rotation from X--------
1 1----------Rotation from Y--------
2 1----------Rotation from Z--------
1 1----------Rotation from Y--------
-----------DECRYPTION ENDS-------------
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27

--------TEST DATA 4----------
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64
1 2 ----------Rotation from Y--------
2 2 ----------Rotation from Z--------
1 1 ----------Rotation from Y--------
0 3 ----------Rotation from X--------
1 2 ----------Rotation from Y--------
1 2 ----------Rotation from Y--------
1 3 ----------Rotation from Y--------
0 0 ----------Rotation from X--------
0 1 ----------Rotation from X--------
2 3 ----------Rotation from Z--------
2 1 ----------Rotation from Z--------
2 1 ----------Rotation from Z--------
2 1 ----------Rotation from Z--------
0 3 ----------Rotation from X--------
1 0 ----------Rotation from Y--------
0 3 ----------Rotation from X--------
-----------ENCRYPTION ENDS-------------
61 20 8 16 45 59 21 3 17 18 44 50 1 2 29 49 62 25 7 15 19 22 27 58 34 38 43 35 56 55 54 12 63 37 47 53 6 26 23 46 10 39 42 30 32 28 31 14 64 51 9 13 48 11 40 60 5 41 24 33 4 57 36 52
Reverse sequence is-------
0 3----------Rotation from X--------
1 0----------Rotation from Y--------
0 3----------Rotation from X--------

2 1----------Rotation from Z--------
2 1----------Rotation from Z--------
2 1----------Rotation from Z--------
2 3----------Rotation from Z--------
0 1----------Rotation from X--------
0 0----------Rotation from X--------
1 3----------Rotation from Y--------
1 2----------Rotation from Y--------
1 2----------Rotation from Y--------
0 3----------Rotation from X--------
1 1----------Rotation from Y--------
2 2----------Rotation from Z--------
1 2----------Rotation from Y--------
----------DECRYPTION ENDS----------
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64

--------TEST DATA 5----------
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 7
6 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125
1 0 ----------Rotation from Y--------
2 0 ----------Rotation from Z--------
1 2 ----------Rotation from Y--------
0 0 ----------Rotation from X--------
1 1 ----------Rotation from Y--------
1 3 ----------Rotation from Y--------
1 4 ----------Rotation from Y--------
0 0 ----------Rotation from X--------
0 1 ----------Rotation from X--------
2 2 ----------Rotation from Z--------
2 1 ----------Rotation from Z--------
2 0 ----------Rotation from Z--------
2 4 ----------Rotation from Z--------
0 1 ----------Rotation from X--------
1 1 ----------Rotation from Y--------
0 1 ----------Rotation from X--------
----------ENCRYPTION ENDS----------
105 26 115 116 121 24 45 86 91 16 111 70 61 114 11 22 97 36 81 6 21 122 23 104 101 96 7 108 109 110 41 34 93 94 95 72 59 62 57 52 47 92 37 32 27 20 119 18 17 2 103 14 113 66 71 98 43 88 83 78 73 68 63 58 53 48 87 38 33 28 15 56 13 12 3 120 19 54 29 4 99 42 89 84 79 118 67 64 39 8 117 82 69 44 9 46 107 74 49 10 25 102 123 124 125 100 31 90 85 80 75 112 65 60 55 50 77 40 35 30 1 106 51 76 5
Reverse sequence is-------
0 1----------Rotation from X--------
1 1----------Rotation from Y--------
0 1----------Rotation from X--------
2 4----------Rotation from Z--------
2 0----------Rotation from Z--------
2 1----------Rotation from Z--------
2 2----------Rotation from Z--------
0 1----------Rotation from X--------
0 0----------Rotation from X--------
1 4----------Rotation from Y--------
1 3----------Rotation from Y--------
1 1----------Rotation from Y--------
0 0----------Rotation from X--------
1 2----------Rotation from Y--------
2 0----------Rotation from Z--------
1 0----------Rotation from Y--------
----------DECRYPTION ENDS----------
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125

4. Tests of Randomness

We have applied some tests of randomness of bits, taken from NIST specifications, to the outputs generated by the cipher. The tests were applied on the bits shuffled using the above algorithm, which were initially divided in equal number of 0s and 1s. The cipher was then used to shuffle the bits. The resultant bits of 0s and 1s were then analyzed for checking the status of bits shuffled. The following were the results of the tests:

4.1 Monobit Test

The focus of the test is the proportion of zeroes and ones for the entire sequence. The purpose of this test is to determine whether the number of ones and zeros in a sequence are approximately the same as would be expected for a truly random sequence. The test assesses the closeness of the fraction of ones to ½, that is, the number of ones and zeroes in a sequence should be about the same.

S No	My3DCipher
1	0.230139
2	0.317311
3	0.317311
4	0.689157
5	0.230139

6	0.317311
7	0.230139
8	0.016395
9	0.230139
10	0.230139

Table 1 P-values for Monobit Test.

All Monobit tests have passed.

4.2 Frequency Within a block

The focus of the test is the proportion of ones within M-bit blocks. The purpose of this test is to determine whether the frequency of ones in an M-bit block is approximately M/2, as would be expected under an assumption of randomness.

Test Number	X2Observed, 10	P-value
1	16	0.066882
2	14	0.122325
3	12.4	0.191687
4	24	0.004301
5	9.6	0.383827
6	16.4	0.058984
7	12.8	0.171867
8	21.6	0.010237
9	12	0.213309
10	11.2	0.262249

Table 2 P-values for Frequency within a Block Test.

The P-values for Block test are given in Table 2 above. Only one test out of ten has failed. This again proves 90% of the times the results are random.

4.3 Run Test

The focus of this test is the total number of runs in the sequence, where a run is an uninterrupted sequence of identical bits. A run of length k consists of exactly k identical bits and is bounded before and after with a bit of the opposite value. The purpose of the runs test is to determine whether the number of runs of ones and zeros of various lengths is as expected for a random sequence. The test was applied to 10 randomly selected sequences of the encrypted data for which the p-values observed were as Table 3 below.

Test No	P-Value	Test of Randomness
1	0.022081619	PASS
2	0.054960057	PASS
3	0.47952254	PASS
4	0.235662962	PASS
5	0.795064135	PASS
6	0.363302144	PASS
7	0.580983947	PASS
8	0.031736965	PASS
9	0.505676771	PASS
10	0.139602589	PASS

Table 3 P-values for Run Test.

All the ten tests have passed.

4.4 Random Excursions Test

The focus of this test is the number of cycles having exactly K visits in a cumulative sum random walk. The cumulative sum random walk is derived from partial sums after the (0,1) sequence is transferred to the appropriate (-1, +1) sequence. A cycle of a random walk consists of a sequence of steps of unit length taken at random that begin at and return to the origin. The purpose of this test is to determine if the number of visits to a particular state within a cycle deviates from what one would expect for a random sequence. This test is actually a series of eight tests (and conclusions), one test and conclusion for each of the states: -4, -3, -2, -1 and +1, +2, +3, +4.

FAIL	0
PASS	180
Min	0.1572993
Max	1
Average	0.7456489

Table 4 P-values for Random Excursions Test.

The above Table 4 shows the number of tests passed/failed and Min/Max/Average P-value. Out of the 180 tests applied on the random sequences, all tests have passed.

5. Analysis

The above algorithm assumes a pre-requisite of having a good unique generating function for random numbers based on a seed value, the results show that the cipher based on the 3D matrix rotation technique works good and

implements confusion/diffusion technique very effectively. This 3D Block ciphering technique can be used in everyday encryption/decryption as it is having good encrypting/decrypting efficiency too.

6. Conclusions

The above tests prove high rate of randomness of the bits shuffled using the above technique. Also since the bits were initially divided in equal numbers in the two halves of the array, this shows that the cipher produces a good confusion-diffusion. It only requires seed value and number of rounds to be applied to be send to receiver along with the ciphertext. Although the new cipher can have variable number of keys used while encrypting the message, we recommend 2xn keys for nxnxn size array of input bits/text.

References

[1] Bruce Schneier, Applied Cryptography, John Wiley & Sons (Asia) Pte Ltd, ISBN 9971-51-348-X
[2] William Stallings, Cryptography and Network Security, Principles and Practices, Fourth Edition, Pearson Education.
[3] Seymour Lipschutz, Data Structures, Tata McGraw Hill Publishing Company Ltd.
[4] A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, NIST Specifications. SP800-22

AUTHOR INFORMATION

Dr. (Mrs) Pushpa R. Suri is Associate Professor in the Department of Computer Science and Applications at Kurukshetra University, Haryana, India. She has supervised a number of PhD students. She has also published a number of research papers in National and International Journals and Conference proceedings.

Sukhvinder Singh Deora holds the degrees of M.C.A., M.Phil. in Computer Science and is working as Assistant Professor in N.C. Institute of Computer Sciences, Israna, Panipat, India. He is also a Research Scholar at Department of Computer Science and Applications, Kurukshetra University, Kurukshetra, India. To his credit are many prominent papers in the area of data security and issues related to it, published in eminent Journals of India. He has edited Proceedings of National Level Seminars/Conferences. He also has an industry experience of 1.5 years in the areas of Testing, Java and Database design issues. His interest areas include Network Security, Theoretical Computer Sciences, Data Structures, S/W Testing and Database Designing. He is also a member of Indian Society of Information Theory and Applications (ISITA).