ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 6, June 2015**

# 2-Dimensional Multi Way Feedback Encryption Standard Version-1(2dMWFES-1)

Asoke Nath[1], Ranjini Mukherjee[2], Dona Sarka[3], Chaitali Patra[4]

Associate Professor, Dept. of Computer Science, St. Xavier's College (Autonomous), Kolkata, India

M.Sc. in Computer Science, Dept. of Computer Science, St. Xavier's College (Autonomous), Kolkata, India

M.Sc. in Computer Science, Dept. of Computer Science, St. Xavier's College (Autonomous), Kolkata, India

M.Sc. in Computer Science, Dept. of Computer Science, St. Xavier's College (Autonomous), Kolkata, India

**ABSTRACT:** In the present paper the authors have introduced a new symmetric key cryptographic method which is based on two dimensional simultaneous feedback method applied along two dimensions i.e. x and y axes on plain text. Nath et al already developed MWFES ver-1,2,3 where they have used encryption methods in one axis i.e. x-axis. The feedback was used along x-axis but in forward as well as back directions. In MWFES ver-1 for the first time Nath et al applied feedback from Left hand side as well as from right hand side along x-axis. Further in ver-2 and ver-3 of MWFES Nath et al used random feedback, random skip and it makes the whole system quite complex. The standard attack like brute force attack, known plain text attack or differential attack is not possible in MWFES ver-2 and 3. Without knowing the key it almost impossible to break the method. In the present work the authors have introduced multiway feedback along x-aaxis and y-axis one after the other. The entire content of the file is first converted to a 2 dimensional square matrix say nxn where n=number of characters along x-axis and along y-axis. After that there may be some characters not been accommodated within the largest square matrix and those characters will be kept sepate in some 1-dim array. Feedback applied along x-axis both orward and backward direction. After finishing encryption along x-axis encryption along y-axis also made. After finishing x-axis and y-axis encryption the residual characters taken on the front and again repeat the same encryption process. After completion of 2 passes one complete encryption will be completed. The encryption may be applied multiple times also. Apart from feedback some initial random key is also required for doing the encryption process. The decryption will be the reverse process of encryption. The present method is applied on small text such as password or some confidential key and the results are quite satisfactory. The present method is also free from standard cryptographic attack such as known plain text attack, brute force attack etc. This method applied on various types of files and the results were coming quite satisfactory.

**KEYWORDS**: forward feedback; backward feedback; plain text; cipher text; random key

## I. INTRODUCTION

In case of one dimensional multiway feedback encryption Nath et al used the entire plain text and then some random key whose size should be same as the size of plain text and then some random feedback taken on leftmost character of the plain text and also one backward feedback on the rightmost character of the same plain text. The ASCII code of plain text character, key character ,forward feedback character, backward feedback character are added and taken modulo with 256 and it is considered as the cipher text after first iteration and that will be also taken as the feedback for the next column. The same cipher text will be considered as the feedback in the next column. In the present work the authors extended the idea of multiway feedback from one dimension to two dimensions to make the whole system more complex. Initially the size of plain text file is calculated suppose it is m-bytes. Now value of greatest square is calculated from 'm' such that n*n <=m. So residual characters which will not come in perfect square is m-n*n. Initially the plain text of a perfect square size (i.e. n x n where n<=16) is encrypted as well as decrypted. But attempts have been taken to compute the text of any size. The residual elements which are not included in the matrix for the First iteration are also included for the Second Iteration by shifting the position of the previous encrypted elements.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 6, June 2015**

## II. RELATED WORK

In [2] authors used average residual battery level of the entire network and it was calculated by adding two fields to the RREQ packet header of a on-demand routing algorithm i) average residual battery energy of the nodes on the path ii) number of hops that the RREQ packet has passed through. According to their equation retransmission time is proportional to residual battery energy. Those nodes having more battery energy than the average energy will be selected because its retransmission time will be less. Small hop count is selected at the stage when most of the nodes have same retransmission time. Individual battery power of a node is considered as a metric to prolong the network lifetime in [3]. Authors used an optimization function which considers nature of the packet, size of the packet and distance between the nodes, number of hops and transmission time are also considered for optimization. In [ 4] initial population for Genetic Algorithm has been computed from the multicast group which has a set of paths from source to destination and the calculated lifetime of each path. Lifetime of the path is used as a fitness function. Fitness function will select the highest chromosomes which is having highest lifetime. Cross over and mutation operators are used to enhance the selection. In [5] authors improved AODV protocol by implementing a balanced energy consumption idea into route discovery process. RREQ message will be forwarded when the nodes have sufficient amount of energy to transmit the message otherwise message will be dropped. This condition will be checked with threshold value which is dynamically changing. It allows a node with over used battery to refuse to route the traffic in order to prolong the network life. In [6] Authors had modified the route table of AODV adding power factor field. Only active nodes can take part in rout selection and remaining nodes can be idle. The lifetime of a node is calculated and transmitted along with Hello packets. In [7] authors considered the individual battery power of the node and number of hops, as the large number of hops will help in reducing the range of the transmission power. Route discovery has been done in the same way as being done in on-demand routing algorithms. After packet has been reached to the destination, destination will wait for time δt and collects all the packets. After time δt it calls the optimization function to select the path and send RREP. Optimization function uses the individual node's battery energy; if node is having low energy level then optimization function will not use that node.

## III. MWFES VER-I METHOD

In MWFES Ver-1 Nath et al used Key, Forward feedback and backward feedback simultaneously to encrypt any plain text. Now the authors will show in tabular form how MWFES ver-I actually encrypts some plain text:

Suppose Plain text → **SCIENCE**
Key value → **ABCDEFG**
❖**Encryption process:-** The entire encryption process will be shown in step by step manner:

Encryption Step-1:

| Plain text | S | C | I | E | N | C | E |
|---|---|---|---|---|---|---|---|
| Key(plain text) | 83 | 67 | 73 | 69 | 78 | 67 | 69 |
| key stream | A | B | C | D | E | F | G |
| Corresponding key | 65 | 66 | 67 | 68 | 69 | 70 | 71 |
| Forward feedback | 0 | ~~0~~–148 | 0 | 0 | 0 | 0 | 0 |
| Backward feedback | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Intermediate state | 148 | | | | | | |
| Cipher text | 148 | | | | | | |

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 6, June 2015**

Encryption Step-2:

| Plain text | S | C | I | E | N | C | E |
|---|---|---|---|---|---|---|---|
| Key(plain text) | 83 | 67 | 73 | 69 | 78 | 67 | 69 |
| key stream | A | B | C | D | E | F | G |
| Corresponding key | 65 | 66 | 67 | 68 | 69 | 70 | 71 |
| Forward feedback | 0 | ~~0~~148 | 0 | 0 | 0 | 0 | 0 |
| Backward feedback | 0 | 0 | 0 | 0 | 0 | ~~0~~140 | 0 |
| Intermediate state | 148 | | | | | | 140 |
| Cipher text | 148 | | | | | | 140 |

Encryption Step-3:

| Plain text | S | C | I | E | N | C | E |
|---|---|---|---|---|---|---|---|
| Key(plain text) | 83 | 67 | 73 | 69 | 78 | 67 | 69 |
| key stream | A | B | C | D | E | F | G |
| Corresponding key | 65 | 66 | 67 | 68 | 69 | 70 | 71 |
| Forward feedback | 0 | ~~0~~148 | ~~0~~25 | 0 | 0 | 0 | 0 |
| Backward feedback | 0 | 0 | 0 | 0 | 0 | ~~0~~140 | 0 |
| Intermediate state | 148 | 281 | | | | | 140 |
| Cipher text | 148 | 25 | | | | | 140 |

……

Encryption Final Step→

| Plain text | S | C | I | E | N | C | E |
|---|---|---|---|---|---|---|---|
| Key(plain text) | 83 | 67 | 73 | 69 | 78 | 67 | 69 |
| key stream | A | B | C | D | E | F | G |
| Corresponding key | 65 | 66 | 67 | 68 | 69 | 70 | 71 |
| Forward feedback | 31 | 148 | 25 | 165 | 214 | 126 | 147 |
| Backward feedback | 148 | 123 | 214 | 168 | 21 | 140 | 71 |
| Intermediate state | 327 | 404 | 379 | 470 | 382 | 403 | 358 |
| Cipher text | 71 | 148 | 123 | 214 | 126 | 147 | 102 |

The Cipher text pattern shows that no brute force method may be applied to get back original plain text.

❖**Decryption process :** Decryption is a process which will just the reverse of Encryption process. Generally the last step done in Encryption process will be the first step in decryption process. Now the decryption process will be shown for the above encrypted text to get back original Plain text.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 6, June 2015**

Decryption Step1 :

| Cipher text | 71 | 148 | 123 | 214 | 126 | 147 | 102 |
|---|---|---|---|---|---|---|---|
| key stream | A | B | C | D | E | F | G |
| Corresponding key | 65 | 66 | 67 | 68 | 69 | 70 | 71 |
| Forward feedback | | | | | 214 | 126 | 147 |
| Backward feedback | 148 | 123 | 214 | | | | 71 |
| Intermediate state | | | | | | | -187 |
| plain text | | | | | | | 69 |

Decryption Step2:

| Cipher text | 71 | 148 | 123 | 214 | 126 | 147 | 102 |
|---|---|---|---|---|---|---|---|
| key stream | A | B | C | D | E | F | G |
| Corresponding key | 65 | 66 | 67 | 68 | 69 | 70 | 71 |
| Forward feedback | 31 | | | | 214 | 126 | 147 |
| Backward feedback | 148 | 123 | 214 | | | | 71 |
| Intermediate state | -173 | | | | | | |
| Plain text | 83 | | | | | | 69 |

Decryption Final Step:

| Cipher text | 71 | 148 | 123 | 214 | 126 | 147 | 102 |
|---|---|---|---|---|---|---|---|
| key stream | A | B | C | D | E | F | G |
| Corresponding key | 65 | 66 | 67 | 68 | 69 | 70 | 71 |
| Forward feedback | 31 | 148 | 25 | 165 | 214 | 126 | 147 |
| Backward feedback | 148 | 123 | 214 | 168 | 21 | 140 | 71 |
| Intermediate state | -173 | -189 | -183 | -187 | -178 | -189 | -187 |
| Plain text | 83(S) | 67(C) | 73(I) | 69(E) | 78(N) | 67 (C) | 69(E) |

After the final step one can see that original plain text has come i.e. “SCIENCE”

## IV. 2-DIMENSIONAL MULTIWAY FEEDBACK ENCRYPTION METHOD

With the view of the 1D multi way feedback encryption standard the authors proceeds towards the advancement of this concept in the field of 2 dimensions. Here one has to provide a text whose size should be a perfect square and so therefore it can accommodate the file in a ‘n x n’ square matrix format [matrix A] . The intitial forward and backward feedback can be taken any constant value. To make the process simple in the present work the authors have taken initial forward and initial backward feedback equal to zero(0). Now variations come in the process of encryption and decryption. During encryption process primordially individual rows are taken, i.e. encryption is done along the X-axis. After the completion of the encryption of the corresponding horizontal rows a new matrix consisting of those elements obtained after horizontal encryption [matrix B]. Now emphasizing on the 2D fact, encryption is carried out over the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 6, June 2015**

vertical columns, i.e. along the Y-axis. After all the columns have been encrypted vertically then a new sets of value of the new matrix [matrix C] is formed. This would be the final matrix or the final cipher text obtained from the proposed algorithm.

While in case of decryption, the phases are as follows:
Decryption process begins with the consideration of the vertical columns at first. Therefore, decryption is carried over along the Y-axis. The output of this process will be treated as the input of the second phase of the algorithm where decryption method is incorporated along the X-axis, i.e. decryption will be done according the horizontal rows. Finally the optimal cipher text is retrieved from our proposed 2D multi way feedback encryption standard algorithm.

**A. 2dMWFES Encryption algorithm :**

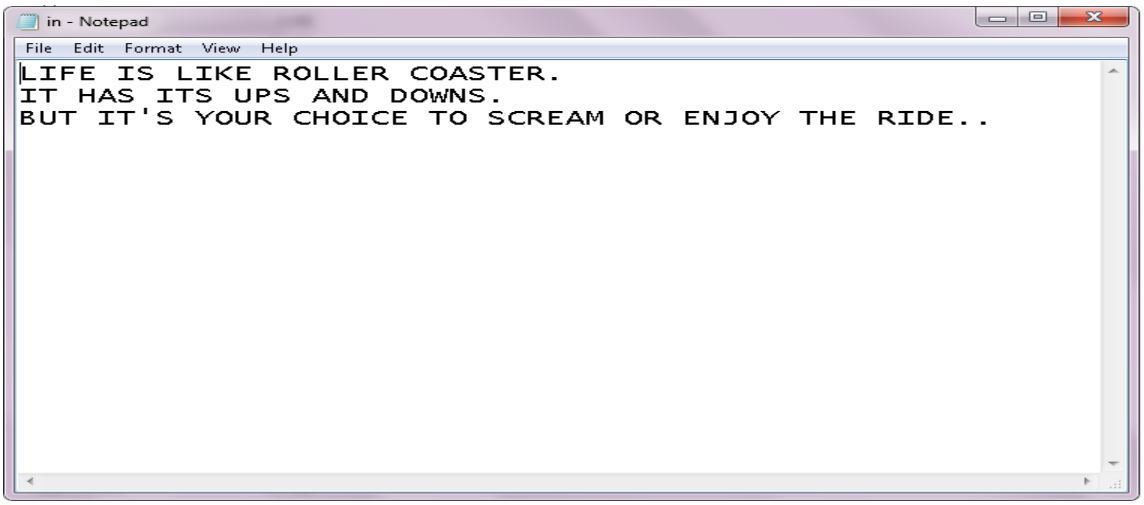
2dMWFES is the extension of MWFES version-1. The encryption mechanism of MWFES ver-1 is already described in the previous section. In 2dMWFES the authors have considerd the data of the entire file in a square matrix and then applied both x-direction forward and backward feedback and after that the same procedure applied along y-direction. After finishing pass-1 the residual characters brought in the beginning of the square matrix and applied the encryption method along x-axis and after that along y-axis. After completion of pass-2 one time encryption will be completed. Depending on user's choice the encryption method may be applied multiple times.

B. **2dMWFES Decryption algorithm**

The Decrytion is just the reverse of encryption process. The last operation in encryption should be the first operation in Decryption. In case of decryption first y-decryption is done and after that x-decryption is done. The decryption process for 1-dimension i.e. MWFES ver-1 is already described. In 2dMWFES decryption the y-direction decryption to added in addition to x-axis decryption.For odd and even dimension a minor adjustment in decryption method is to be used.

## V. RESULTS AND DISCUSSION

**Case-1 : Encryption of some arbitrary Plain Text :**
**The input file and also key file is:**



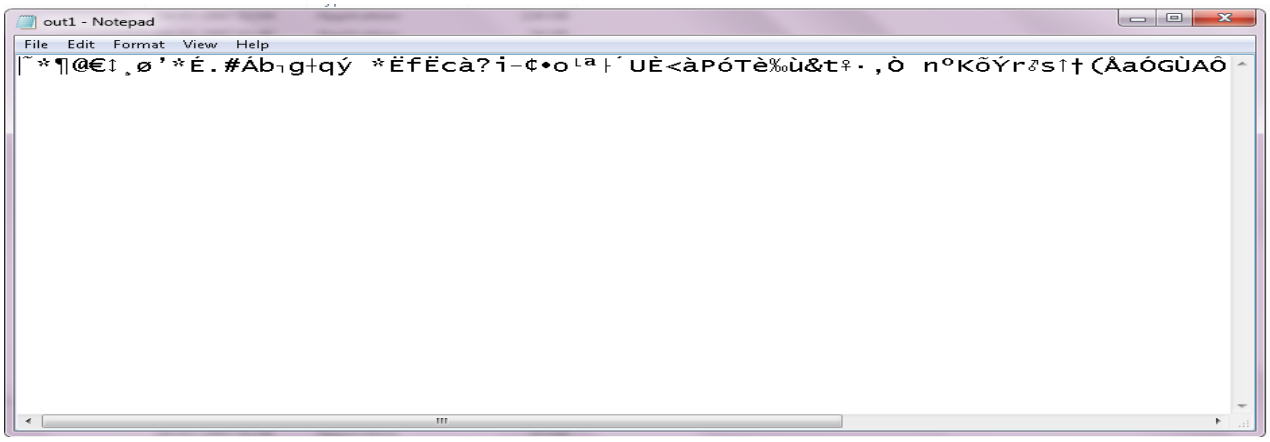
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

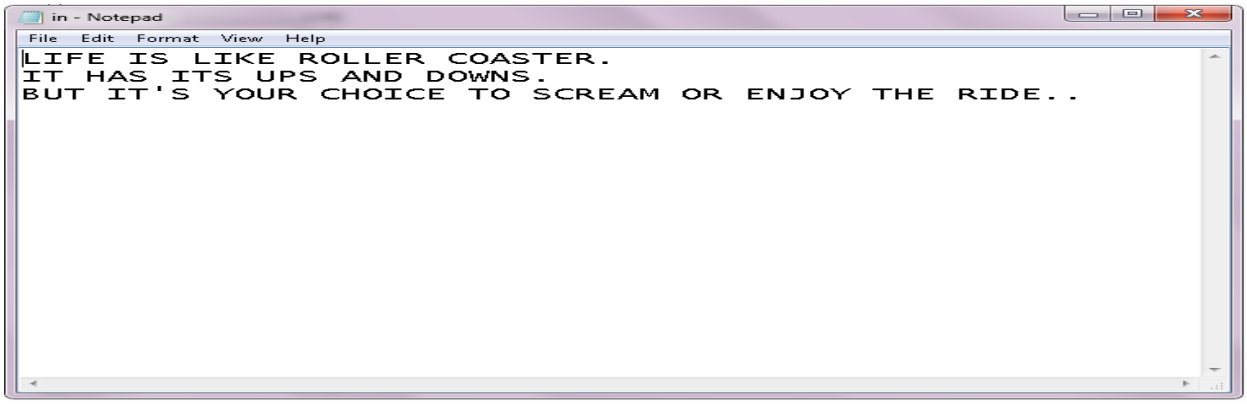
*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 6, June 2015**

**The encrypted file after 2dMWFES encryption algorithm is:**

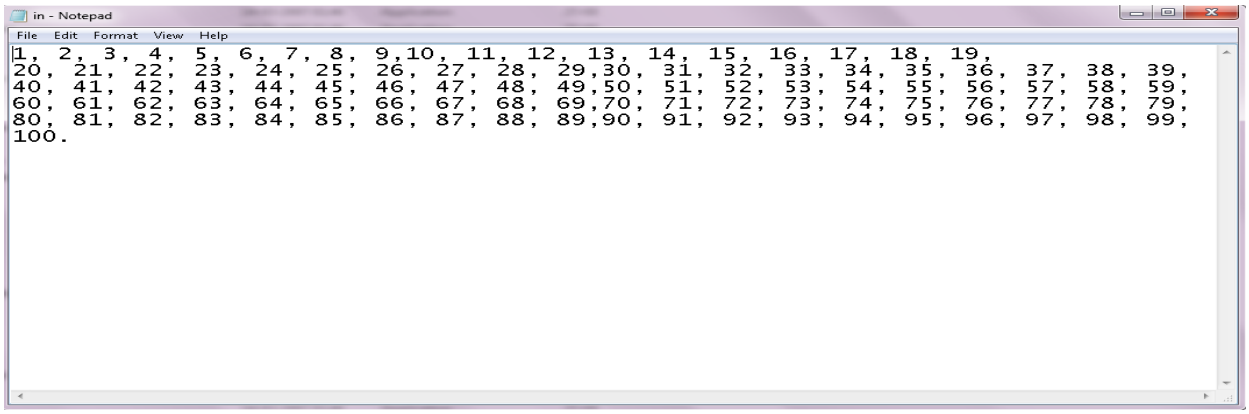



**After Decryption output is :**




**Case-2: Encryption of Plain text type-2:**

**The input file is :**



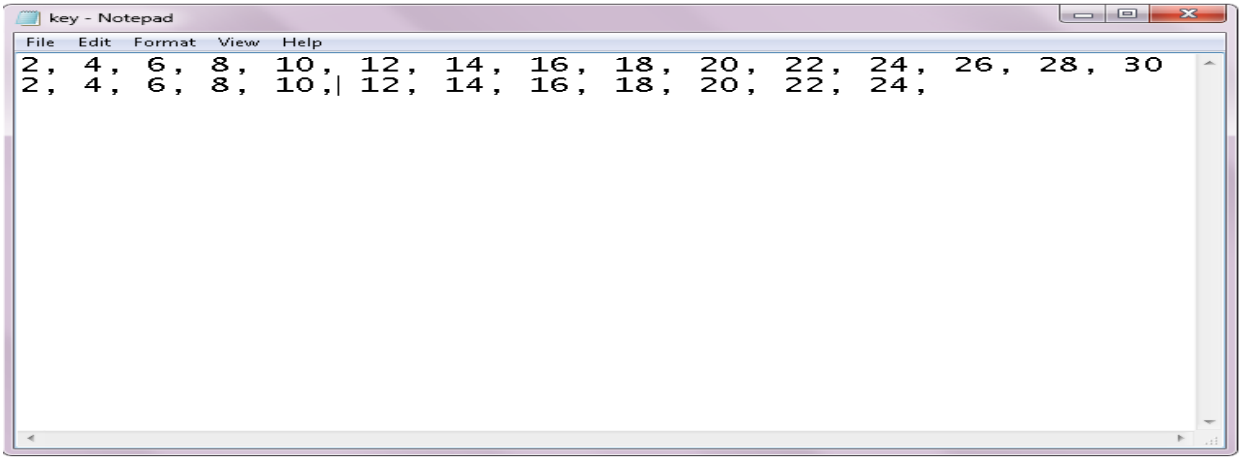
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

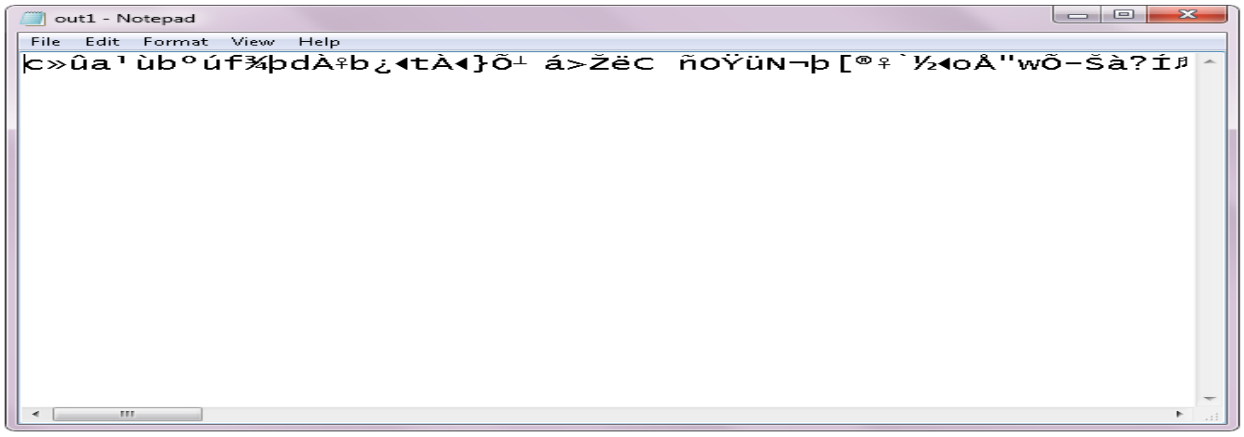
*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 6, June 2015**

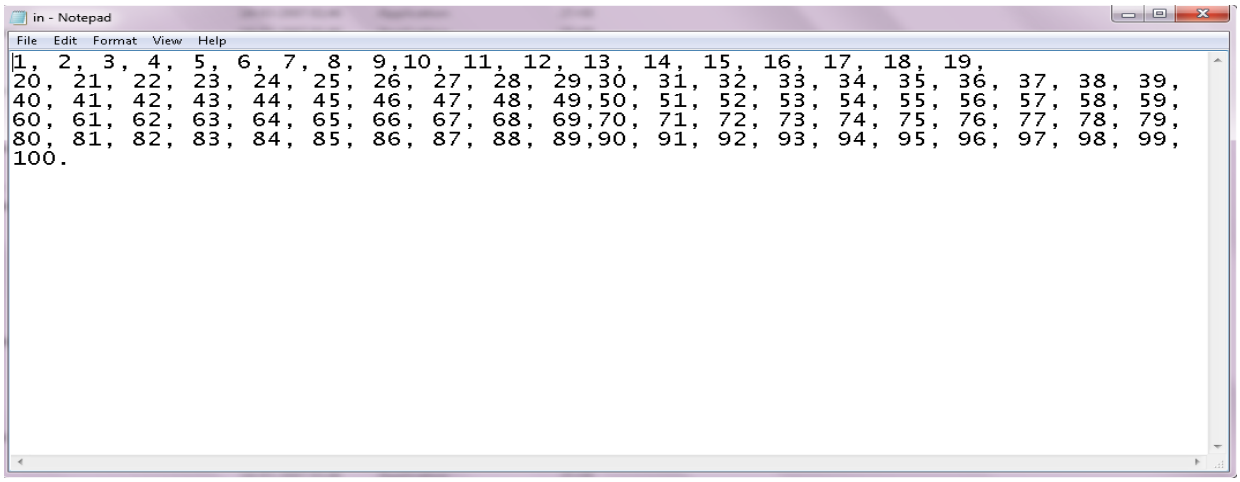
**The key file is :**




**The encrypted file is:**




**After Decryption Output File is:**



ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

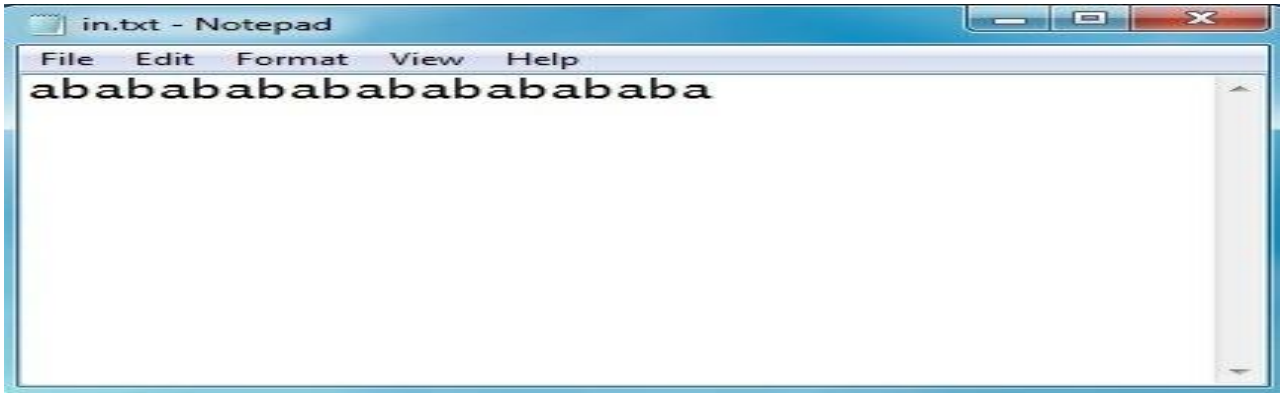
International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

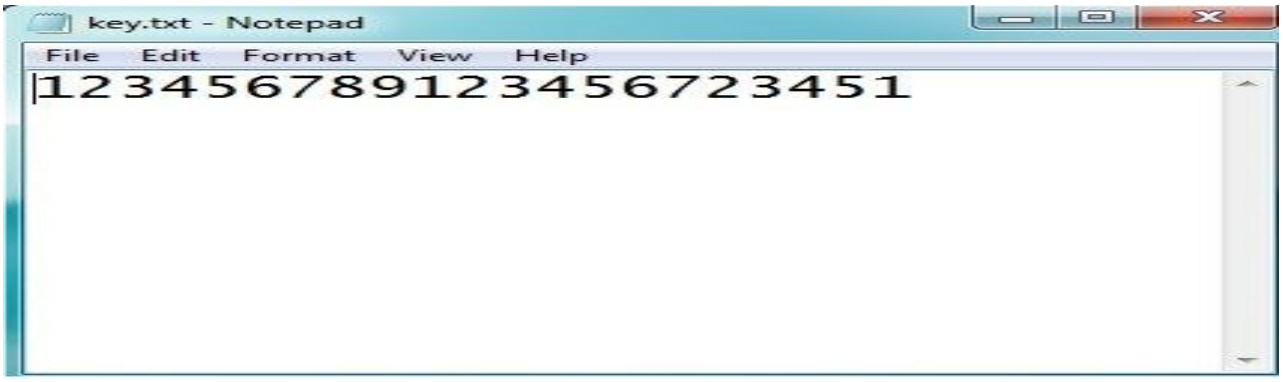
**Vol. 3, Issue 6, June 2015**

**Case-3 Encryption of Plain Text file using 2dMWFES:**

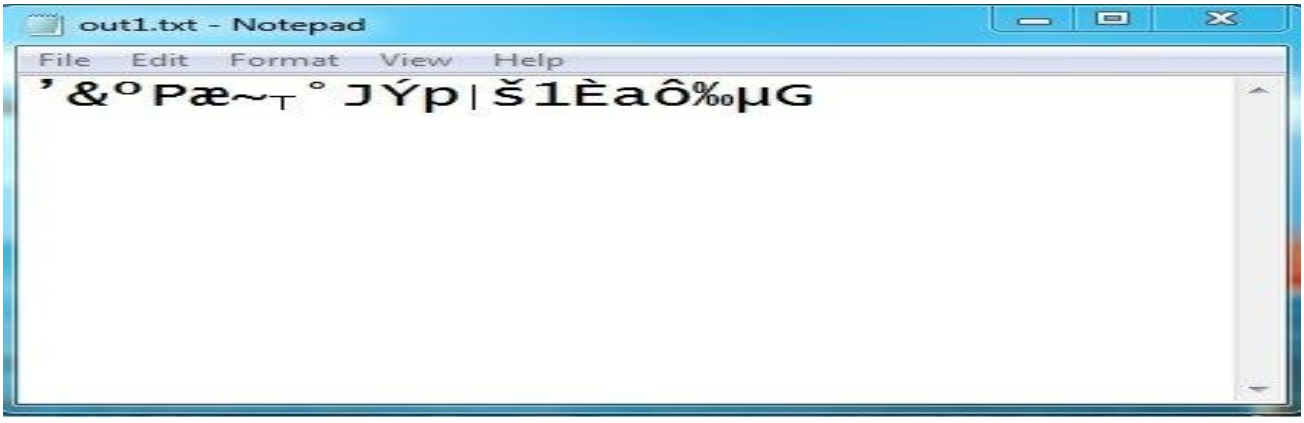
**The input file is:**




**The key file is :**




**The encrypted file is:**



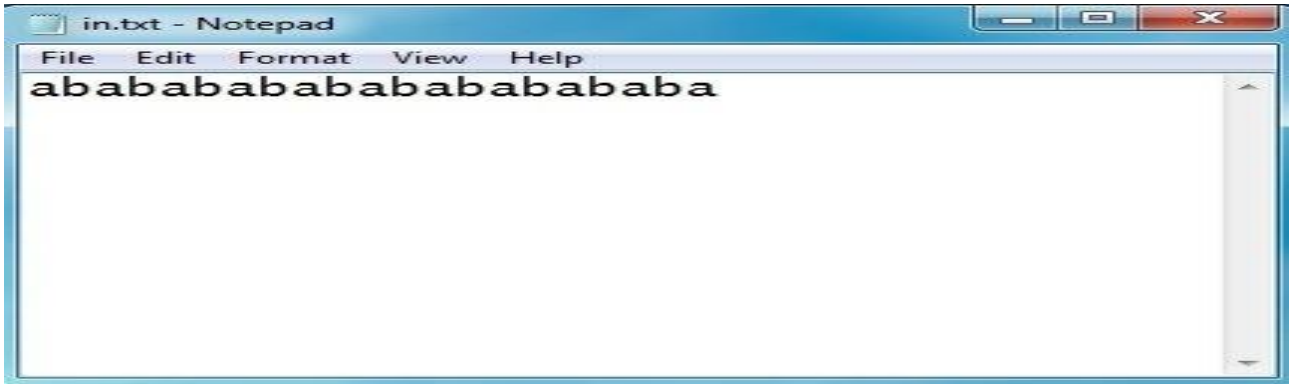
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 6, June 2015**

**The decrypted file is:**




## VI. SOME LIMITATIONS OF 2DMWFES VER-1

(i) In present method the authors haven't considered intial feedback random. However, there is a scope to introduce intial feedbacks random.

(ii) In the present method the feedback is always moving from one column to immediate next column. However, teher is a scope to skip feedback in random manner..

(iii) The present method is plemented for a perfect square matrix. However, the method will be much stronger if one introduces a rectangular matrix of any size.

(iv) The present method may be further improved by introducing random key generator like the method used by Nath et al in MSA algorithm.

## VII. CONCLUSION AND FUTURE SCOPE

The present method is free from common attacks such as brute force attack, known plain text attack etc. Without knowing the exact key it is almost impossible to decrypt an encrypted text. Initial forward and backward feedback is is taken zero both in x-direction as well as in y-direction. The Initial feedback may be taken random which was used in MWFES Ver-2,3 etc. The present encryption method may be applied multiple times to make the whole system more complex. The key may be randomized to make the present system more complex. 2dMWFES may applied for small key, password encryption, e-mail encryption, data encryption in sensor networks.

## ACKNOWLEDGEMENT

The authors are very much grateful to Department of Computer Science, St. Xavier's College(Autonomous), Kolkata for giving the ooportunity to work in the area of Cryptography. One of the authors AN is very much grateful to Fr. Dr. John Felx Raj, Principal of St. Xavier's College(Autonomous), Kolkata for his constant encouragement to research work in Computer Science and Information Technology.

## REFERENCES

1. Purnendu Mukherjee, Prabal Banerjee, Asoke Nath, Multi Way Feedback Encryption Standard Ver-I(MWFES-I) , International Journal
2. of Advanced Computer Research(IJACR), Volume-3, Number-3, Issue-11, September 2013, Pages:176-182.
3. Asoke Nath, Debdeep Basu, Surajit Bhowmik, Ankita Bose and Saptarshi Chatterjee, Multi Way Feedback Encryption Standard Ver-2(MWFES-2),. Paper submitted in International Conference : IEEE WICT 2013 to be held in December 15-18, 2013 at Hanoi, Vietnam.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 6, June 2015**

4. Asoke Nath, Payel Pal, Modern Encryption Standard Ver-IV(MES-IV), International Journal of Advanced Computer Research(IJACR), Volume-3, Number-3, Issue-11, September 2013, Page:216-223.
5. Asoke Nath, Bidhusundar Samanta, Modern Encryption Standard Ver-V(MES-V), International Journal of Advanced Computer Research(IJACR), Volume-3, Number-3, Issue-11, September 2013, Pages:257-264.
6. Prabal Banerjee, Asoke Nath, Bit LevelGeneralized Modified Vernam Cipher Method with Feedback: Proceedings of International Conference on Emerging Trends and Technologies held at Indore, Dec 15-16,2012.
7. Prabal Banerjee, Asoke Nath, Advanced Symmetric Key Cryptosystem using bit and byte level encryption methods with feedback: Proceedings of International conference Worldcomp 2013 held at LasVegas, July 2013.
8. Arijit Ghosh, Prabhakar Chakraborty, Asoke Nath, Shamindra Parui, "3d Multi Way Feedback Encryption Standard Version 1(3DMWFES-1)". International Journal of Advance Research in Computer Science and Management Studies, ISSN:2321-7782(online), Vol 2, Issue 10, Oct, Page:206-218(2014)

## BIOGRAPHY

**Dr. Asoke Nath** is the Associate Professor, Department of computer Science, St. Xavier's College(Autonomous), Kolkata, India. Dr. Nath is involved in various research fields such as Cryptography and Network Security, Visual Cryptography, Quantum Computing, Steganography, Green Computing, MOOCs and e-learning, Mathematical modelling of Social Networks, Big Data etc. He has published more than 146 research papers in National and International Journals and also in proceedings of Conferences. Dr. Nath is the Life members of MIR Labs(USA) and CSI Kolkata Chapter.

**Ranjini Mukherjee** passed M.Sc. in Computer Science from St. Xavier's College(Autonomous), Kolkata, India in June, 2015. She has already published one paper in International Journal on "Ethical Hacking". The present paper is actually her project work in M.Sc.

**Dona Sarkar** passed M.Sc. in Computer Science from St. Xavier's College(Autonomous), Kolkata, India in June, 2015. She has already published one paper in International Journal on "Big data Analytics". The present paper is actually her project work in M.Sc.

**Chaitali Patra** passed M.Sc. in Computer Science from St. Xavier's College(Autonomous), Kolkata, India in June, 2015. She has already published two papers in International Journal on "Green Computing". The present paper is actually her project work in M.Sc.