An Improved Approach of Cryptography using Triangulation and MSB Iteration Technique

Monalisa Dey[1], Dhirendra Prasad Yadav[2], Sanik Kumar Mahata[3], Anupam Mondal[4], Sudipta Sahana[5]

[1,3,4 and 5]: Assistant Professor, Dept. of CSE, JIS College of Engineering, Kalyani, Nadia, West Bengal
[2]: M.Tech Scholar, Dept. of CSE, JIS College of Engineering, Kalyani, Nadia, West Bengal

ABSTRACT
In our ever-increasingly connected world, the need for communicating data over the internet has grown considerably. This data can be intercepted and hence needs to be guarded against fraudulent access. In cryptography, encryption is a critical security measure for protecting data privacy. The proposed work introduces an encryption scheme to achieve this purpose. The entire process is done on binary data, so it will encompass all kinds of data in the field of Computer Science.

Keywords
Fraudulent access, Cryptography, Encryption**.**

I. INTRODUCTION
Information exchange over the internet is gaining more and more importance with each passing day. As the internet is an insecure channel, this data can be very easily accessed by an illegitimate entity. The need to provide data security has thus gained extreme importance.

Encryption is a cryptographic technique for encoding information (plaintext) using an algorithm, into a humanly unreadable format (cipher text) so that only an authorized entity can decrypt it. It uses mathematical schemes and algorithms to scramble the content of a message. In this paper, an encryption decryption algorithm is introduced which can protect the confidentiality of the information transmitted. Two concepts have been taken into account in the presented approach. The first concept, known as "Constant MSB Iteration", is described in section II. The second approach is known as "Triangulation" and its algorithm is described in section III. The algorithm for encryption and decryption using the approaches named above is described in section IV. The implementation of the algorithm with a suitable example is shown in section V followed by the conclusion in section VI.

II. CONSTANT MSB ITERATION
Algorithm

Initially an n bit data string is taken. After this, we consider the steps discussed below.

1. The data string that has been initialized is taken as it is.
2. Taking the MSB of the data string as it is, bit wise XOR operation of all the bits in the data string is done.
3. The above step is considered as the 1st iteration.
4. The iteration process is continued until and unless we get back the actual data string.
5. It is being noted that the original string will be attained after (n+1) number of iteration steps.
6. So, the number of iteration steps is equal to the number of bits in the original data string.

The above algorithm is implemented below, using a suitable example.

The data string taken is 1 0 0 0 1 1 0

Step1: 1 1 0 0 1 0 1

Step2: 1 0 1 0 1 1 1

Step3: 1 1 1 1 1 0 0

Step4: 1 0 0 0 0 1 0

Step5: 1 1 0 0 0 1 1

Step6: 1 0 1 0 0 1 0

Step7: 1 1 1 1 0 1 1

Final result: 1 0 0 0 1 1 0

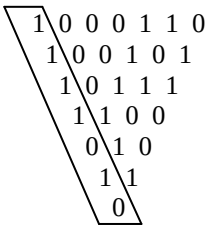
It is clear from the above example that the original text is obtained after seven steps, as the number of bits in the data string is equal to seven.

III. TRIANGULATION
Algorithm

Initially an n bit data string is taken. After this, we consider the steps discussed below.

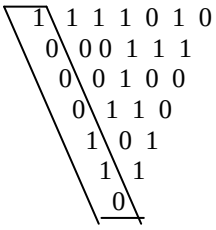
1. The data string initialized is taken as it is.
2. Bit wise XOR operation is performed of all the bits; however, the MSB is not kept constant .This step is considered as the 1st iteration.
3. The iteration process is continued until the data string is reduced to a single bit.
4. The MSB's from the data string obtained from each of the iterations and are then joined together and taken as the new output.
5. If we take the new output as the data string, and perform the above mentioned steps, i.e, step1-step4, we get the original output.

The implementation of the above algorithm is shown using the previous data string example. The data string taken is 1000110.



The output string obtained is 1111010.

Now, this data string is taken as the new data string, and triangulation is performed on it.



The output data string obtained is 1000110, which is the actual data string.

IV. PROPOSED APPROACH

Encryption Algorithm

1. The message to be sent is first converted into its ASCII format.
2. The plain text is the data string which is obtained after converting the ASCII code into the corresponding binary code.
3. The encryption process is initiated by first performing the constant MSB iteration algorithm on the string as described in section II.
4. From the various data strings obtained after performing the above step, a random string is chosen.
5. The step number is noted.
6. The selected string acts as an input to the Triangulation Algorithm described in section III.
7. After performing the previous step on the string, the output obtained is the encrypted version of the plaintext (cipher text) that will be transmitted.
8. Along with the cipher text, the noted step number, from which the input string was randomly chosen for the Triangulation Algorithm is also sent.

Decryption Algorithm

1. The receiver performs the Triangulation procedure described in section III, after receiving the encrypted message.
2. After joining the MSB's of the resultant steps, we get a data string.
3. The Constant MSB Algorithm is performed on the resultant string for a certain number of iterations.
4. The number of iterations are determined by using the following formula: No. of = [n-(step number received from the sender)]+1
5. The output data string obtained should match with the plain text or the original message that was sent.
6. If both of the strings differ, that means the data is tampered.

The implementation of the encryption and decryption algorithm is shown in section V with the help of the previous example.

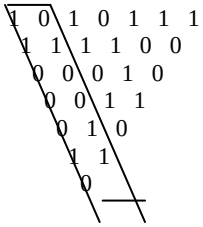
V. IMPLEMENTATION

Encryption Process

Let the initial string be 1 0 0 0 1 1 0

Step1:	1 1 0 0 1 0 1
Step2:	1 0 1 0 1 1 1
Step3:	1 1 1 1 1 0 0
Step4:	1 0 0 0 0 1 0
Step5:	1 1 0 0 0 1 1
Step6:	1 0 1 0 0 1 0
Step7:	1 1 1 1 0 1 1
Final result:	1 0 0 0 1 1 0

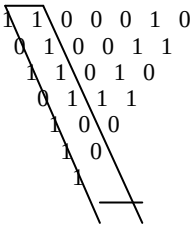
We take the result from step 2, i.e, 1010111 as input to the triangulation algorithm.



After joining the MSB's of the resultant steps, we get the data string 1100010. This serves as the cipher text. This cipher text along with the number 2, is sent to the receiver, where 2 is the step number of the data string from constant MSB iteration.

Decryption Process

The cipher text is taken as input to the triangulation algorithm.



The resultant output string obtained is 1010111. This string now becomes the input for the Constant MSB Algorithm shown below. Number of iterations performed are (7 – 2) + 1 = 6.

	1 0 1 0 1 1 1
Step1:	1 1 1 1 1 0 0
Step2:	1 0 0 0 0 1 0
Step3:	1 1 0 0 0 1 1
Step4:	1 0 1 0 0 1 0
Step5:	1 1 1 1 0 1 1
Final Step:	1 0 0 0 1 1 0

As seen from above, the final retrieved output obtained is the plain text that was sent by the sender.

V. CONCLUSION

Information that needs to be communicated over the internet may be of any kind, such as audio, video, image, sound etc. All these data, while being transmitted, are converted to their equivalent binary format. The proposed algorithm is designed to

work on any kind of binary data. Thus, it will provide data security efficiently irrespective of what information is being exchanged.

REFERENCES

[1] J. K. Mandal, S. Dutta, "A 256-bit recursive pair parity encoder for encryption", Advances D -2004, Vol. 9 nº1, Association for the Advancement of Modelling and Simulation Techniques in Enterprises (AMSE, France), www. AMSE-Modeling.org, pp. 1-14

[2] Dutta S., Mal S., "A Multiplexing Triangular Encryption Technique – A move towards enhancing security in ECommerce", Proceedings of IT Conference (organized by Computer Association of Nepal), 26 and 27 January, 2002, BICC, Kathmandu.

[3] William Stallings, Cryptography and network security, 2005, 4th Edition, Prentice Hall.

[4] Atul Kahate, Cryptography and network security, 2005, 4th reprint, Tata McGraw-Hill.