ISSN:0975-9646

New Approach for Data Encryption using Two Way Crossover

Deepak Nagde, Raviraj Patel[2], Dharmendra Kelde[3]
[1,2]*Department of Information Technology,SDITS, Khandwa.*
[3]*Department of Information Technology,MITM, Indore*

Abstract- The network security and data encryption is very important at present day. So for the data transmission in open network, we need to protect data transmission confidently from sender to recipient. In an open network for the transmission of any file like text file, binary file or any other file we used MSA method for encryption & decryption.MSA method used a random key generator to generate a random key from square matrix in which 256 elements are stored. If someone trying to know about actual key matrix, so we are applying a new technique on element which is randomly generate by square matrix. And this technique is called "Two Way Crossover". For the reliable and secure transmission of data in open network encryption must be required.

Keyword: [encryption, decryption, crossover operator and offspring.]

INTRODUCTION-

Now a day modern communication network security and data encryption is very important when we send some important data from client to recipient or one client to another client, than data should not be intercepted by someone. it means whenever we want to send some message to someone that should be encrypted in such a way that no one can decrypt without knowing the decrypt key for the decryption process. And encryption is the art of protecting information by transforming it into an unreadable format, called cipher text. Only those who possess a secret key can decipher the message into plain text. As the Internet and other forms of electronic communication become more prevalent, electronic security is becoming increasingly important. Cryptography is used to protect credit card information, e-mail messages and corporate data.

Cryptography systems can be broadly classified into (i) symmetric-key cryptography in which same key is used for encryption and for decryption. Symmetric-key cryptography is sometimes called secret-key cryptography. The most popular symmetric-key system is the Data Encryption Standard ***(DES)***. (ii) public-key cryptographic system that uses two keys -- a public key known to everyone and a private or secret key known only to the recipient of the message.

The symmetric key algorithms are more useful in modern communication between one client to another client because in which key management is very simple, one key are use to encryption and same key are use for decryption. In which various symmetric key cryptographic methods are present like DES, Double DES and Play fair method. If we are using symmetric key cryptographic method the key which we are using for encryption should not be disclosed to unauthorized user. The key must be secured. We can reduce these types of problem by using public key cryptographic method like RSA method and AES method etc. An important element to the public key system is that the public and private keys are related in such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used to decrypt them. In the present work we are proposing a symmetric key method in which we have to use a random key generator for generating the initial key and this key is used for encrypting the given file

CROSSOVER TECHNIQUE

Crossover is a process of taking more than one parent solutions and creating a child solution from them. It is also called as recombination operator. Crossover selects genes from parent chromosomes and creates new offspring's.

Chromosome 1: 11011 | 00100110110
Chromosome 2: 11001 | 11000011110
Offspring 1: 11011 | 11000011110
Offspring 2: 11001 | 00100110110

With the using of crossover operator technique in cryptography we can be more secure our data and increase the security reduce the memory utilization and increase the speed. our method can be used for encrypting digital signature, watermark before embedding in some cover file to make the entire system full secured.

TWO WAY CROSSOVERS

Two Way Crossover techniques apply on both sender and recipient end to increase the file security and reliable transmission of data or information in open network.

For example--

Chromosome 1: 1101100100110110
Chromosome 2: 1100111000011110

We are applying the single point crossover operator on the both level. A single crossover point on both parent strings is selected. All data beyond that point in the parents is swapped and the new offspring's are generated. {**Sender end crossover A**}

Chromosome 1: 11011 | 00100110110
Chromosome 2: 11001 | 11000011110
Offspring 1: 11011 | 11000011110
Offspring 2: 11001 | 00100110110

And same technique we are applying on receiver end by which massage may be decrypted (original massage). This complete process is called "**two way crossovers**".

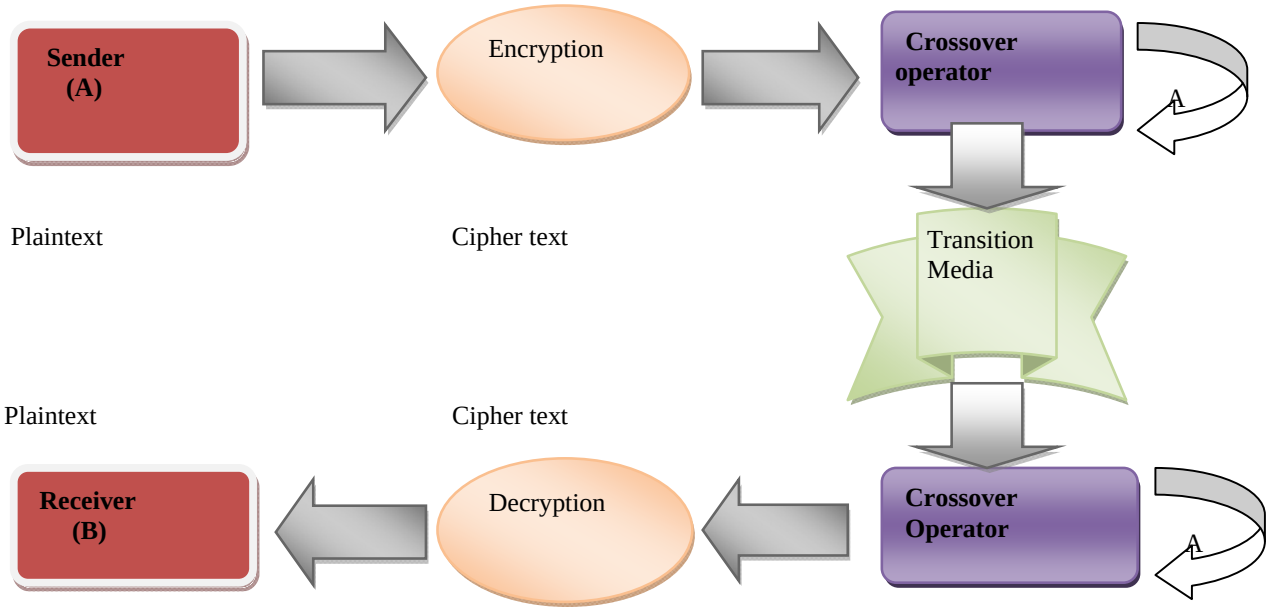

Fig. (a). Show Two Way Crossover Operator

PROCESS OF TWO WAY CROSSOVER

The figure (a) show the Two Way Crossover Operator which is provides the more security to transmit the data. In which text **A** represent the sender end crossover operation and text **B** represent the receiver end crossover operation.

Now we are applying crossover method on 256 character on the sender end like side A. than the chromosome is that-

Chromosome:
1101011100001010101000111010100010100101001000010
1110010010000011111100001101011110101001101010010
1111000010100001001010101110001010101000010111101
0101011101011110111000101010101010100011110101001
0101100110101010001010100101011101010011000101001
00011110101

Than we are apply the crossover on this 256 character that means we have to dive 256 characters into two chromosomes, cromosome1: 128 and cromosome2:128 as shown in below

Cromosome1:
1101011100001010101000111010100010100101001000010
1110010010000011111100001101011110101001101010010
1111000010100001001010101110000

Cromosome2:
1010101000010111101010101110101111011100010101010
1010100011110101001010110011010101000101010010101
1101010011000101001000111101 01

Now we have to again apply crossover operator on both chromosome and again we have to dived both chromosome like-

Cromosome1:
1101011100001010101000111010100010100101001000010
111001001000001|
1111100001101011110101001101010010111100001010000
100101010111000

Cromosome2:
1010101000010111101010101110101111011100010101010
101010001111010|
1001010110011010101000101010010101110101001100010
100100011110101

Than the offspring will be generates shown below-

Offspring1:
1101011100001010101000111010100010100101001000010
111001001000001|
1001010110011010101000101010010101110101001100010
100100011110101

Offspring2:
1010101000010111101010101110101111011100010101010
101010001111010 |
1111100001101011110101001101010010111100001010000
100101010111000

Now we apply reveres technique on recipient end (**B**) and finally recipient (**B**) get secured original message.

CONCLUSIONS-

In this paper we have to propose a new approach for data security. We use the concept of genetic algorithms in cryptography along with the randomness properties of MAS method. This total way of transferring secret information is highly safe and reliable. So without the knowledge of the pseudorandom sequence no. one will be able to extract the massage.

In the feature work we plan to design sophisticated software based on this technique which will target to use in highly secure multimedia data transmission application.

REFERENCES:

[1] A new Symmetric key Cryptography Algorithm using extended MSA method DJSA symmetric key algorithm, Dripto Chatterjee, Joyshree Nath, Suvadeep Dasgupta and Asoke Nath : accepted for publication in IEEE CSNT-2011 to be held at SMVDU(Jammu) 03-06 June 2011.

[2] Symmetric key cryptography using random key generator, A.Nath, S.Ghosh, M.A.Mallik, Proceedings of International conference on SAM-2010 held at Las Vegas(USA) 12-15 July,2010, Vol-2,P-239-244.

[3] Advanced Symmetric key Cryptography using extended MSA method: DJSSA symmetric key algorithm, Dripto Chatterjee, Joyshree Nath, Soumitra Mondal, Suvadeep Dasgupta and Asoke Nath, Journal of Computing, Vol 3, Issue 2, Page-66-71,Feb(2011)

[4] A new approach for data encryption using genetic algorithms .

[5] Clark A and Dawson Ed, "Optimisation Heuristics for the Automated Cryptanalysis of Classical Ciphers", Journal of Combinatorial Mathematics and Combinatorial Computing, Vol.28,pp. 63-86, 1998.

[6] M. Matsui, Linear cryptanalysis method for DES cipher, Lect. Notes Comput. Sci. 765 (1994) 386–397.

[7] William Stallings, Cryptography and Network Security Principles and Practices, Third Edition,Pearson Education Inc.,2003.

[8] Vimalathithan.R, M.L.Valarmathi, "Cryptanalysis of SDES Using Genetic Algorithm", International Journal of Recent Trends in Engineering, Vol2, No.4, November 2009, pp.76-79.