Encoding Algorithm using Bit Level Encryption and Decryption Technique

Jayashree Singha
Computer Sc & Engg
Siliguri Institute of Technology
Siliguri, India

Saikat Jana
Software Consultant
Surflex Technology Pvt ltd
Kolkata, India

Souvik Singha
Computer Sc. & Engg.
Techno India University
Kolkata, India

ABSTRACT
Encryption is a process in which the sender encrypts or scrambles the message in such a way that only the recipient will be able to decrypt the message with the knowledge of the proper key. With the growth of internet, the need for secure data transmission become more essential and important, as security is a major concern in the internet world. So the plain text should be codified by the process of encryption. Different types of data have their own features, thus different techniques should be used to protect confidential data from unauthorized access. In this paper proposed in bit level encryption and decryption algorithm based on number of keys which can encrypt the 8 bit binary no to its corresponding 8 bit cipher text and a decryption algorithm which can convert that 8 bit cipher text to its corresponding 8 bit original no. It can also be extended to 16, 32 bit binary number.

Keywords
Bit level encryption; plaint text; cipher text; encoding; decoding

1. INTRODUCTION
The originality of data is a very important issue in data communication. No confidential message should be sent in raw format from one node to another via public domain as hacker can intercept that confidential message. Secure data transmission means that raw data can be sent from sender side to receiver side without any eavesdropping. Internet being open there is no guarantee that when a person sends some confidential data from one node to another node, the confidential message cannot be intercepted by any unwanted intruder. So the security of data is now has a big question mark [1, 6, 16, 18, 19]. So private data should not be sent in raw form from one computer to another.Encryption is the approach by which a message is transformed to another message so that only the sender and recipient can see. The confidential data must be converted to its encrypted form first and then should be sent over the insecure internet. To protect data from intruder or hacker, network security and cryptography is an emerging research area where the researchers are trying to evolve strong encryption algorithm so that the intruder cannot intercept the encrypted message.The efficient encryption schemes were developed and also broken subsequently over time. Continual research is going on in the field of cryptography to enhance the security as nothing is permanently secure. Also with the advancement of VLIW era with multiprogramming, mathematical functions are now a day's vulnerable to different attacks. Many different algorithms have been devised depending on various mathematical models, with each of them having their own merits and demerits. Breaking weak password is very easy for hackers. Messages with have repeated occurrences, plain texts which maps to same cipher texts are of prime interest of hackers and encryption of such texts may be rather difficult.

Different symmetric techniques [9, 10] have been developed and implemented which are very simple and easy to understand. In each case different variable length vectors have been introduced for variable length of blocks that enhances the security level of techniques. Matrix Based Bit Orientation Technique (MBBOT), Matrix Based Bit Shuffle Technique (MBBST), Magic Square Based Bit Orientation Technique (MSBBOT), Spiral Matrix Based Bit Orientation Technique (SMBBOT) [7], Permutative Cipher Technique (PCT) [5] and Session Based Symmetric Key Cryptographic Technique (SBSKCT) [2, 17] are few of them. Each of them considers source message as a stream of binary bits.

Reference [3] introduces a new symmetric key cryptographic method called Bit Level Encryption Standard (BLES) which is based on bit exchanging or bit reshuffling method with fixed block size which are multiple of 2. This method uses bit, byte exchange methods with complements and XOR operation. The key element is the bit exchange depending on the randomized matrix which is generated every time and also each matrix is unique. In an updated version called BLES-II [4] block size of square of numbers starting from three onwards have been taken. Roy devised a symmetric key algorithm [11] that performs encryption by advanced bitwise randomization and serial feedback generation. Reference [13] proposed a symmetric key block cipher which uses bit manipulation method that include bit exchange, right shift and XOR operation on the bits. Reference [15] proposed a method that combines NJJSSA algorithm with MSA method in random order. Modified Generalized Vernam Cipher and DJSA method which is an extension of MSA method [12] was combined to DJMNA symmetric key algorithm [14].

2. FORMS OF CRYPTOGRAPHIC SYSTEM

2.1 Secret Key Cryptography (SKC)
With secret key cryptography, a single key is used for both encryption and decryption. As shown in Figure 1, the sender uses the key to encrypt the plaintext and sends the cipher text to the receiver. The receiver applies the same key to decrypt the message and recover the plaintext. As a single key is used

for both functions, secret key cryptography is also known as symmetric encryption. Symmetric key cryptography is generally easier compare to asymmetric key cryptography.

2.2 Public key cryptography (PKC)
Public key cryptography or Asymmetric key cryptography uses public and private keys to encrypt and decrypt data. The keys are generally different large numbers paired together. One key in the pair called the public key can be shared and other one is known as private key which will be kept secret.PKC depends

upon the existence of so-called one-way functions, or mathematical functions that are easy to computer whereas their inverse function is relatively hard to compute. Fig 2 shows the concept of asymmetric key cryptography.

3. PROPOSED WORK

Here an encryption algorithm was developed which can encrypt the 8 bit binary no to its corresponding 8 bit cipher text and a decryption algorithm which can convert that 8 bit cipher text to its corresponding 8 bit original no. The code section of the above algorithms is developed by the JAVA language. This work can be extended up to 32 bit data. A swap function which can generate a public key for encryption and corresponding decryption algorithms are introduce here. It can transform the bit level data into several categories and using swap function minimum 8 bit of data can securely send from source to destination.

Proposed Encryption Algorithm:
Let us take 8 bits binary data as input to the encryption module. Our encryption process will stop when the decimal value of either block A or block B reaches a predefined number. '0' as the predefined value is chosen here.

Step1: Consider 8 bits block. Divide 8 bits block into two 4 bits blocks named A and B. And determine corresponding decimal number in each block.

Step 2: If (A>B) then multiply A and B. Else swap (A, B) and multiply A and B.

3: Convert AB as binary nos. and go to Step step1.

Step4: Continue till either A or B '0000'. If either A or B '0000' then AB is cipher text. And the swap value is the public key for this algorithm.

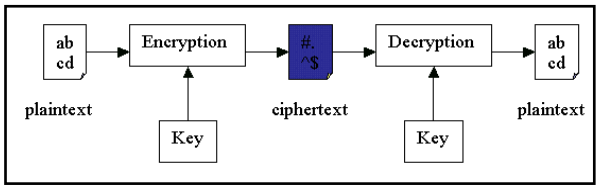

Fig. 1. Symmetric key cryptography

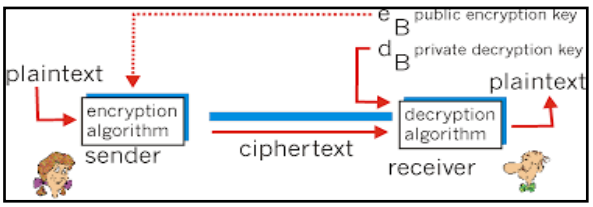

Fig. 2. Assymmetric key cryptography

Proposed Decryption Algorithm:
Step 1: Take 8 bits block. Divide it into two 4 bits blocks named P and Q.

Step 2: Checked if P and Q swapped or not in encryption. If yes then swap P and Q.

Step 3: Convert P and Q Corresponding decimal Number M and N and multiply M and N. Find out corresponding prime factor say A and B and test A>B if true then place AB else BA.

Step4: Convert AB to its corresponding binary number. And go to step1. Continue till cipher text=plaintext.

4. EXPERIMENTAL RESULTS

In this work, The bit level encoding algorithm are proposed here. The input of 8 bit plain text and its corresponding cipher text is given in TABLE I. The result shows that given plain texts are 10101100, 11000001, 00000001 and their corresponding cipher texts are 100000000, 00001100 and 00000001 respectively. The corresponding graph has been shown in figure 3.

Table1 , Plain text and corresponding cipher text for 8 bit experiment

Plain Text	Cipher Text
10101100	10000000
11000001	00001100
00000001	00000001

Explanation of Encryption Algorithm for 8 bit experiment

Let us take 8 bits blocks 10101100.

Divide it into two 4 bits blocks

A=1010 → 10 and B=1100 → 12

A<B then swap (A, B) then A=1100(12) B=1010(10)

AB=120. 120→01111000

A=0111→ 7 B=1000→ 8

Swap (A, B) then A=1000 B=0111 then

AB=56→00111000

A=0011→3 B=1000→8

A<B swap (A, B) A=1000, B=0011, AB=24=00011000

A=0001→1, B=1000→8

A<B swap (A, B) A=1000 B=0001 AB=8*1=8→00001000

A=0000→0, B=1000→8

AB=0

A<B swap (A, B) A=1000 B=0000

AB=10000000 is cipher text.

Explanation of Decryption Algorithm for 8 bit experiment

Let us take 8 bits blocks 10000000

P=1000→8 and Q=0000→0

Checked whether swapped or not in encryption or not.

If yes swap (P, Q)

P=0000→0

Q=1000→8

Combine P and Q then PQ=00001000=8=8X1.

P=1000→8

Q=0001→1

Swap (P, Q) then P=0001 and Q=1000

PQ=00011000=24=8X3.

P=1000→8 and Q=0011→3

Swap (P, Q) then P=0011 Q=1000.

PQ=0011100=56=8X7

P=1000→8 and Q=0111→7

Swap (P, Q) P=0111 Q=1000

PQ=01111000=120=12X10

P=1100 and Q=1010

Swap (P, Q) P=1010 and Q=1100

PQ=10101100.

Check PQ=AB.

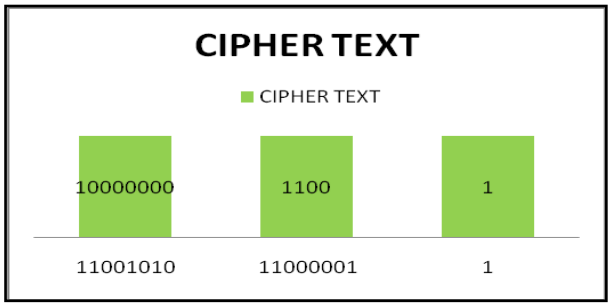

Fig. 3. Graph of converting 8 bit plain text to cipher text

16 bit plain text will take again and got the corresponding cipher text after encryption shown in TABLE II. The experimental result is shown in Figure 4.

Table 2, Plain text and corresponding cipher text for 16 bit experiment

Plain Text	Cipher Text
0000110000001010	0000000001111000
0000111100000001	0000000000001111
0000000000000001	0000000000000001

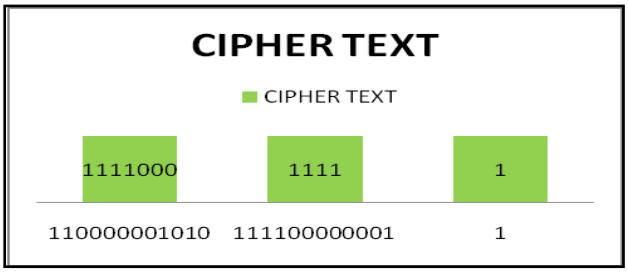

Fig. 4. Graph of converting 16 bit plain text to cipher text

5. CONCLUSION

In this paper, A new algorithm based encoding technique are presented here which is converted into binary bits. Algorithm encryption is performed on binary data. All data which is under stable by the computer is finally converted into binary bits. So it can be implemented for any data type encryption process. In the proposed algorithm the key length is not fixed and the length of the plan text is not restricted for applicable of any large file.

6. REFERENCES

[1] Alfred J. Menezes , Paul C.van Oorschot, and Scott A. Vanstone, Handbook of Applied Cryptography, Taylor & Francis Ltd.

[2] Manas Paul, Tanmay Bhattacharya, Suvajit Pal and Ranit Saha, "A novel generic session based bit level encryption technique to enhance information security" , International Journal of Computer Science and Information Security,Vol. 3, No. 1, 2009.

[3] Neeraj Khanna, Dripto Chatterjee and Asoke Nath, "Bit level encryption standard (BLES): Version-I", International Journal of Computer Applications (0975 – 8887) Volume 52– No.2, August 2012.

[4] Gaurav Bhadra, T. Baia and S. Banik, "Bit level encryption standard (BLES): Version-II", Information and Communication Technologies (WICT), 2012 World Congress on, 30 Oct.-2 Nov. 2012.

[5] Manas Paul and J.K.Mandal, "A permutative cipher technique(PCT) to enhance the security of network based transmission", Proceedings of 2nd National Conference on Computing for Nation Development, Bharati Vidyapeeth's Institute of Computer Applications and Management, New Delhi, India, pp. 197-202,08th-09th February 2008, pp. 217-222.

[6] Douglas R Stinson, Cryptography:Theory and Practice, CRC press.

[7] Manas Paul and Jyotsna Kumar Mandal, "A novel symmetric key cryptographic technique at bit level based on spiral matrix concept", International Conference on Information Technology, Electronics and Communications (ICITEC – 2013), Bangalore, India, March 30 – 31, 2013.

[8] Hsien-Chou Liao and Yun-Hsiang Chao, "A new data encryption algorithm based on the location of mobile users", Information Technology Journal 7 (1), pp. 63-69, 2008.

[9] J.K. Mandal and S. Dutta, "A universal bit-level encryption technique", Seventh Vigyan Congress, Jadavpur University, India, 28Feb to Ist March, 2000.

[10] J.K. Mandal and P.K. Jha, "Encryption through cascaded arithmetic operation on pair of bits and key rotation (CAOPBKR)", National Conference of Recent Trends in Intelligent Computing (RTIC-06), Kalyani Government Engineering College, Kalyani, Nadia, 17-19 Nov. 2006,India, pp 212-220.

[11] Satyaki Roy , Shalabh Agarwal, Asoke Nath, Navajit Maitra and Joyshree Nath," Ultra encryption algorithm (UEA): Bit level symmetric key cryptosystem with randomized bits and feedback mechanism", International Journal of Computer Applications (0975 – 8887) Volume 49– No.5, July 2012.

[12] Asoke Nath, Saima Ghosh and Meheboob Alam Mallik," Symmetric key cryptography using random key generator"," Proceedings of the 2010 International Conference on Security & Management, SAM 2010, July 12-15,2010,Vol-2,239-244.[13] Neeraj Khanna, Joel James, Joyshree Nath, Sayantan Chakraborty, Amlan Chakrabarti and Asoke Nath, "New symmetric key cryptographic algorithm using combined bit manipulation and MSA encryption algorithm: NJJSAA symmetric key algorithm", Proceedings of IEEE CSNT-2011 held at SMVDU(Jammu) 03-06 June 2011, Page 125-130.

[14] Debanjan Das, Joyshree Nath, Megholova Mukherjee, Neha Chaudhury and Asoke Nath, "An integrated symmetric key cryptography algorithm using generalized vernam cipher method and DJSA method: DJMNA symmetric key algorithm", Proceedings of IEEE conference WICT-2011 held at Mumbai University Dec 11-14,2011.

[15] Trisha Chatterjee, Tamodeep Das, Joyshree Nath, Shayan Dey and Asoke Nath, "Symmetric key cryptosystem using combined cryptographic algorithms- generalized modified vernam cipher method, MSA method and NJJSAA method: TTJSA algorithm", Proceedings of IEEE International conference : World Congress WICT-2011 held at Mumbai University 11-14 Dec, 2011, Page No. 1179-1184(2011).

[16] Willian Stallings, Cryptography and Network, Prentice Hall of India.

[17] J.K. Mandal and P.K. Jha, "Encryption through cascaded recursive key rotation of a session key with transposition and addition of blocks (CRKRTAB)", Proceed. National Conference of Recent Trends in Information Systems (ReTIS-06), IEEE Calcutta Chapter & Jadavpur University, 14-15 July, 2006.

[18] FOROUZAN, CRYPTOGRAPHY AND NETWORK SECURITY, McGraw Hill Education.

[19] Abhijit Das and C. E. Veni Madhavan, Public-Key Cryptography : Theory and Practice, Pearson India.