

## Development of cryptographic algorithm using bit shifting and Matrix XOR operations

S. Kiran<sup>1</sup>, A. Ashok Kumar<sup>2,\*</sup>, S. Diwakar<sup>1</sup>, T. Hari Kumar<sup>3</sup>, T. Mukthar Ahmed<sup>1</sup>

<sup>1</sup>Dept. of Computer Science and Engg., YSR Engineering College of YVU, Proddatur-516360, India

<sup>2</sup>Dept. of Physics, YSR Engineering College of YVU, Proddatur-516360, India

<sup>3</sup>Business Analyst, Tata Consultancy Services, Bangalore, Karnataka.

\*Corresponding Author: drashok.yvuce@gmail.com

### To Cite this Article

S. Kiran, A. Ashok Kumar, S. Diwakar, T. Hari Kumar, T. Mukthar Ahmed, "Development of cryptographic algorithm using bit shifting and Matrix XOR operations", *Journal of Science and Technology*, Vol. 07, Issue 02, March-April 2022.

### Article Info

Received: 03-02-2022

Revised: 24-02-2022

Accepted: 04-03-2022

Published: 10-03-2022

**Abstract:** Secured transmission of data is an important technological issue in the world. It is very much essential to develop intelligent cryptographic algorithm, which solves this purpose. A bit shifting and stuffing (BSS) system refers to shifting the printable character bits (ASCII characters of 7 bits each) by 01 bit. The 8th bit of one printable character is replaced by a new bit of other printable character. In the BSS system based encryption process, for every eight bytes of plain text of data in encryption process; the encryption produces seven bytes of cipher text. On contrary during decryption process, seven bytes of cipher text converted to original eight bytes of plain text. In this work a new replacement algorithmic rule for Digital encoding called as "Bit shifting and Matrix XOR Operation Conversion Technique" (BSMXOR) is proposed which increases the complexity of encryption of the data. The experimental results shows that the new theme has very fast encoding and safer for data transmission.

**Key Word:** Encryption, Decryption, Bit Shifting, Matrix XOR operation.

## I. Introduction

Cryptography refers to utilization of variety of techniques using mathematical and Boolean principles to provide security in the data transmission. The main goal of this area is to develop and analyse the algorithms which should not allow the third party malicious users to access the important transmitted data stored either locally or over a globe. Prevention of access to the transmitted data by the unauthorized users is an impossible task. Instead, the transmitted data may be made unreadable during transmission using encryption process which malicious user can't understand. On the other end the original plain text is obtained by the authorized user using a decryption algorithm. In this cryptographic process, a key used in both encryption and decryption process plays an important role in signifying the effectiveness in providing the security in data transmission.

The main issue associated with the design of cryptographic algorithms is to protect the cipher text against malicious attacks. The strengthening mechanisms can be designed in two dimensions by designing keys effectively using well organized protocols and also utilizing effectively the key management strategies like secure key generation, destruction, storage and distribution. Algorithms with poor key management generally fails, hence intelligent cryptographic algorithms generally embedded with a strong key management.

Over last decade, huge number of cryptographic algorithms is developed with symmetric and asymmetric key algorithms. All these algorithms have both merits and demerits in one way or the other. The algorithms are generally designed from mathematical concepts with a set of rules. A complex cryptographic algorithm convert the binary data into characters using either transposing the characters or modifying the characters. To decode the encrypted contents, you would need a grid or table that defines how the letters are transposed. The crucial application of these algorithms include secure data transactions in online trading, file transmission with digital signing and safe data visualization in internet.

## ***Development of cryptographic algorithm using bit shifting and Matrix XOR operations***

---

The main aim of this paper is to explore the benefits of bit shifting in cryptography and matrix XOR operation in enhancing the security and preserving privacy. Ciphers are generally a simple translational codes embedded with hand written codes where the computer can easily break and analyze. Hence the complex cryptographic algorithms need to be developed which even supercomputers can't break. Bit shifting shifts the plain text to remove the unused MSB bit and matrix XOR operation generates the cipher text using a key with bitwise XOR operation. During decryption process the same key is used using XOR operation and the plain text is obtained after doing bit shift operation.

### **II. Literature Survey**

B. Ravi Kumar and Dr. P. R. K. Murti [1] discussed Encryption and Decryption by Using Bit Shifting and Stuffing (BSS) Methodology. The characters need to be transmitted in ASCII format containing 7 bits. Instead, the 8-bit format of a character is generally preferred. In the proposed BSS method, the author replaces the unused bit with a new bit using stuffing process. Further, shifting of data from adjacent printable character reduces eight bytes of plain text to seven bytes of data. Sanikommu Krishna Reddy and R. Sudha Kishore [2] proposed a new replacement algorithmic rule for digital encoding called as "Matrix Rotations and Bytes Conversion Technique" (MRBC). This algorithm provides both the encryption and data compression. The result shows that the new theme has very fast encoding and safer which reduces the size of data. Various substitution and transposition strategies are discussed, and analysed extensively [3]. Noor et al [4] suggested a shift method using double shift ciphers which can do two double shift operations such as shift operations that change both the bit positions of the cipher and also the values. The result shows significant improvement in encryption than compared to shift cipher method. Amit and Vashar [5] proposed to develop a two stage encryption method using invertible matrix followed by byte rotation technique. According to the results the proposed technique provides better security and hard to break the cipher text. Shareef [6] proposed a new shifting algorithm which shuffles the location of each character of cipher text based on the key value. Two key issues are addressed in the proposed method, one is sending the notification to the sender when the attacker modifies the cipher text. Second is shifting the cipher text using variable length based on the key length. This algorithm is tested using different strong cryptography attacks such as brute-force attacks and found that the proposed algorithm is very safe for the data transmission and hard to break the security. C.C.Chang et al [7] discussed encryption scheme using the RSA public key Cryptosystem and its master keys for database records. Two step encryption process is proposed in this paper. In the first step field based encryption process is proposed followed by record oriented encryption process. Santhosh et al [8] proposed a symmetric key encryption algorithm using random generation of prime numbers. Two level XOR operations are utilized in this algorithm. In the first level, randomly generated prime numbers are used in XOR1 operation and the key is used in XOR2. This algorithm is best suited for encrypting large amounts of data. An algorithm is proposed by Mohammad [9] with the combination of public key infrastructure for hybrid system and RC6 algorithm for confusion and diffusion operations. The result shows that this algorithm provides high security and for several attacks it is very hard to identify the patterns. A symmetric cryptographic algorithm for data encryption and decryption based on ASCII values of characters in the plaintext is proposed by Satyajeet and Patil [10]. This algorithm encrypts the plaintext using their ASCII values. The secret key is converted to another string and that string is used as a key to encrypt or decrypt the data. A new cryptographic algorithm is proposed based on ASCII algorithms with substitution arrays [11]. The author utilized ASCII algorithm for encryption and decryption of texts. According the results the algorithm is very fast, reliable and secure. Anupriya et al [12] proposed a secured symmetric algorithm to send the information present in the documents especially in a peer-to-peer environment. This symmetric key algorithm uses extended XOR based key to encrypt all characters. The main idea of this algorithm is to use the confusion and substitution methods in the encryption and decryption processes to produce junk characters instead of regular characters which generally confuse the attacker. Kodabagi et al [13] reported both compression and security of text data using bit stuffing and Huffman coding. The authors proposed three phases of encryption such as bit stuffing during the first phase followed by the data encryption with secret key using XOR operation and finally encryption using Huffman coding. It is evident from the results that a good multilevel security is provided during encryption process and also provides data compression at large extent.

### **III. Proposed Method**

Different encryption methods are presented in past decade. The existing study describes data encryption and decryption using bit shifting and stuffing method. There are some limitations in the existing study, such as security issue which means there may be chance of decoding the encrypted data. The main theme of cryptography is to encrypted the data for securing the information from the intruders but in existing system encrypted procedure is a bit easy to crack the encoding procedure. To avoid this limitation, the proposed work introduces a new digital

## Development of cryptographic algorithm using bit shifting and Matrix XOR operations

encryption and decryption process using bit-shifting and 3\*3 matrix XOR operation methodology to encrypt the information.

File encryption is the process of converting the original file into encrypted file. Now a days , information security is becoming more important in data storage and transmission. Therefore, the security of file data from unauthorized uses is important. The encryption of a file is very important for protecting the data information from the third party users like hackers. Here the file was encrypted in two levels to improve the security feature of file. The two levels of encryption contains performing mod 8 with bit shifting operation in the first level and matrix XOR operation with central pixel values at the later stage.

### **Methodology of encryption process**

In this method, a new way of file encryption is presented. The mathematical techniques were used to encrypt the file. The procedure of encryption process is described below using an algorithm. Figure 1 and 2 shows the original file and encrypted file using the proposed method.

### **Algorithm**

- First read the plain text from file.
- Check the length of the file content is modulo divisible by 8 remains 0 or not
- If the remainder is not zero perform padding operation by adding extra characters up to given condition satisfies.
- Convert each character into 8 bit binary values.
- Perform bit shifting operation by separating two middle values of binary data.
- Combine separated and non separated binary data.
- Represent the data into 3\*3 matrix form.
- Perform matrix XOR operation by central pixel values with other cells data.
- Group the resultant data into 7 bit binary form convert each group into specified ASCII character formation.
- Final data write into encrypted file.

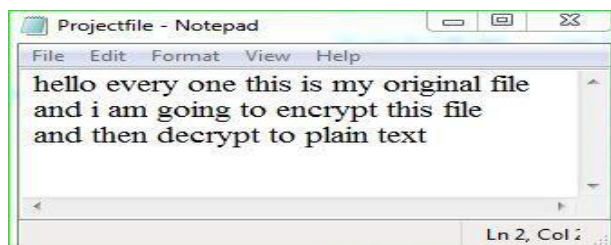


Figure 1. Plain text file

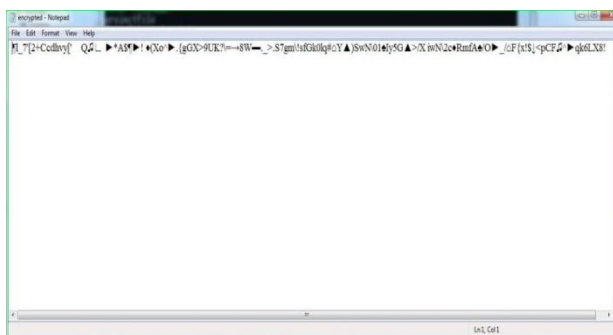


Figure 2. Encrypted file

### **Methodology of Decryption process**

The procedure of decryption process is described below using an algorithm. Figure 3 and 4 shows the encrypted file and decrypted original file.

### **Algorithm**

- Start
- Read the data from encrypted file.
- Convert the each character into 7 bit binary data.
- Represent the binary data into 3\*3 matrix form.
- Perform XOR operation by central pixel values with remaining matrix cell data.
- Grouping the data like 8 bits as one group
- Perform bit shifting operation with grouping data to its original places
- Convert the each 8 bit group into specified ASCII character
- Identify the extra padding characters.
- If extra padding characters found remove the padding characters and save into decrypted file.
- If extra padding characters are not found then save the resultant data into decrypted file.
- Stop.

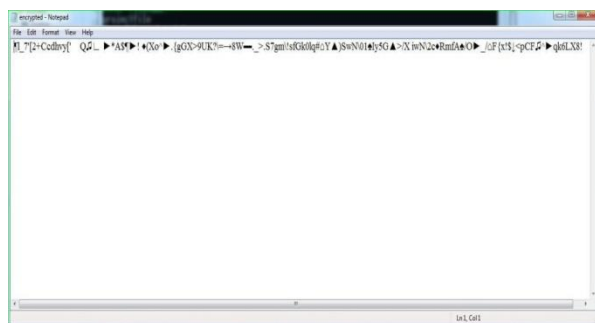


Figure 3. Encrypted file

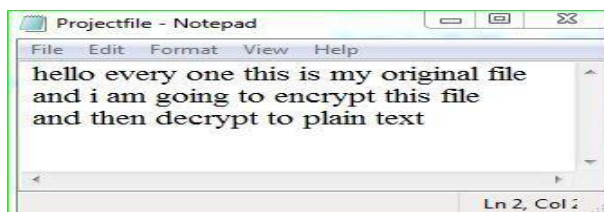


Figure 4. Decrypted original file

#### IV. Results and Discussion

##### Comparison of Existing and Proposed Methods of Encryption Process

Comparison of time complexity for existing and proposed methods of Encryption Process is shown in Table 1 & 2. Here files are taken to encrypt the data the file sizes are 5 Kb, 10 Kb, 15 Kb, 20 Kb, 25 Kb, 30 Kb, 35 Kb, 40 Kb.

Table 1. Comparison of existing and proposed methods in encryption process.

File Size	Existing Method <sup>[3,4]</sup> Encryption time (Sec)	Proposed Method Encryption time (Sec)
5Kb	7	9
10Kb	26	26
15Kb	62	59
20Kb	110	104
25Kb	163	165
30 Kb	241	242
35Kb	359	345
40Kb	460	442

##### Comparison of Existing and Proposed Methods of Decryption Process

The time complexity for existing and proposed methods of decryption Process is compared and results are analysed. The files of different sizes such as 5 Kb, 10 Kb, 15 Kb, 20 Kb, 25 Kb, 30 Kb, 35 Kb, 40 Kb are taken to decrypt the data.

##### Comparison of Existing and Proposed Methods of Data Transmission Time

Comparison of time complexity for existing and proposed methods of data transmission over the client and server communication is shown in Table 3 & 4, figure 5 & 6. Here files are taken to encrypt the data, the file sizes are: 5 Kb, 10 Kb, 15 Kb, 20 Kb, 25 Kb, 30 Kb, 35 Kb, 40 Kb.

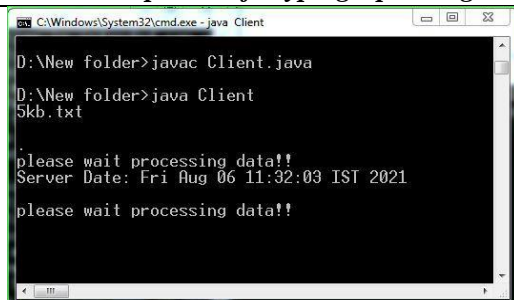
The result shows the improvement in encryption time and decryption as the larger file sizes. The client server interaction for the data transmission shows reduced transmission time for larger file sizes than compared to existing methods [3,4].

Table 2. Comparison of existing and proposed methods in decryption process

File Size	Existing Method <sup>[3,4]</sup> Decryption time (Sec)	Proposed Method Encryption time(Sec)
5Kb	3	7
10Kb	27	28
15Kb	86	80
20Kb	117	113
25Kb	186	185
30 Kb	283	272
35Kb	396	386
40Kb	560	554

Table 3. Comparison of existing and proposed methods based on transmission time.

File Size	Existing Method <sup>[3,4]</sup> Encryption (sec)	Proposed Method Encryption (sec)
5Kb	9	11
10Kb	36	37
15Kb	83	84
20Kb	179	175
25Kb	275	262
30 Kb	450	445
35Kb	750	736
40Kb	810	786

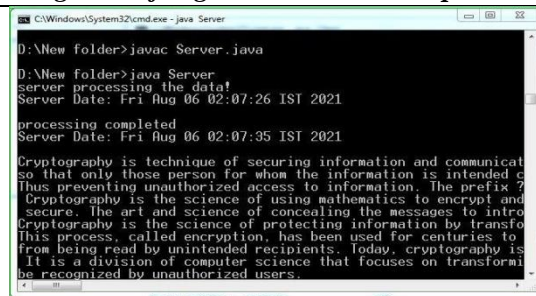


```
C:\Windows\System32\cmd.exe - java Client
D:\New folder>javac Client.java
D:\New folder>java Client
5kb.txt

please wait processing data!!
Server Date: Fri Aug 06 11:32:03 IST 2021

please wait processing data!!
```

Figure 5. Client Request



```
C:\Windows\System32\cmd.exe - java Server
D:\New folder>javac Server.java
D:\New folder>java Server
server processing the data!
Server Date: Fri Aug 06 02:07:26 IST 2021

processing completed
Server Date: Fri Aug 06 02:07:35 IST 2021

Cryptography is technique of securing information and communicat
so that only those person for whom the information is intended c
thus preventing unauthorized access to information. The prefix ?
Cryptography is the science of using mathematics to encrypt and
secure. The art and science of concealing the messages to intro
Cryptography is the science of protecting information by transfo
This process, called encryption, has been used for centuries to
from being read by unintended recipients. Today, cryptography is
It is a division of computer science that focuses on transformi
be recognized by unauthorized users.
```

Figure 6. Server Processing

## V. CONCLUSION

Cryptanalysis seems to be very demanding field due to increased digital transactions. The implementation of efficient cryptographic algorithms to provide security and privacy for the data transmitted in the form of text and image plays a crucial role. The proposed system concludes that this algorithm provide much more security. While sending the data from client to server, the data received by the server with low bit error rate and less transmission time compared to the existing methodology. At the time of transmission, the effect of changing in the cipher text will be high if the intruder changes at least one bit of encrypted data. The main objective of this algorithm is to provide security to the file transmission over the network. The results showed that the proposed algorithm was very effective in complexity and security.

## REFERENCES

- [1] B. Ravi Kumar, P.R.K.Murti, "Data Encryption and Decryption process Using Bit Shifting and Stuffing (BSS) Methodology", International Journal of Computer Science and Engineering (IJCSSE), Vol. 3, Issue 7, pp. 2818-2827, 2011.
- [2] Sanikommu Krishna Reddy, R. Sudha Kishore, "A New Digital Encryption Scheme Matrix Rotations and Bytes Conversion Encryption Algorithm", International Journal of Engineering Research & Technology (IJERT) Volume 03, Issue 07 pp. 487-494, July 2014.
- [3] Sumathy Kingslin, R.Saranya, "Evaluative Study on Substitution and Transposition Ciphers", International Journal of Creative Research Thoughts (IJCRT), Volume 6 Issue 1, pp. 155-160, 2018.
- [4] H. N. Noor Muchsin, D. E. Sari, D. R. Ignatius Moses Setiadi and E. H. Rachmawanto, "Text Encryption using Extended Bit Circular Shift Cipher," Fourth International Conference on Informatics and Computing (ICIC), 2019, pp. 8138-8143, doi: 10.1109/ICIC47613.2019.8985708.
- [5] Amit Kumar Mandle, Varsha Namdeo, "Encryption and Decryption of a Message Involving Byte Rotation Technique and Invertible Matrix", International Journal of Engineering and Advanced Technology (IJEAT), Volume 9 Issue 2, pp. 1160-1163, 2019.
- [6] Farah R. Shareef, A novel crypto technique based ciphertext shifting, Egyptian Informatics Journal, Volume 21, issue 2, pp. 83-90, 2020.
- [7] C.C.Chang ,and Chao-Wen Chan," A database record encryption scheme using the RSA public key Cryptosystem and its master keys", International Conference on Computer Networks and Mobile Computing (Washington, DC, USA), IEEE Computer Society, 2003.
- [8] Ch.Santhosh,Ch. Sowjanya, P. Praveena, Shalini L. " Poly-alphabetic Symmetric Key Algorithm Using Randomized Prime Numbers", International Journal of Scientific and Research Publications, volume 2, Issue 9, pp. 1-3, 2012.
- [9] Obaida Mohammad Awad Al-Hazaimah, A New Approach for Complex Encrypting and Decrypting Data, International Journal of Computer Networks and Communications, Volume 5, Issue 2, pp. 95-103, 2013.
- [10] Satyajee R. Shinge , Rahul Patil ." An Encryption Algorithm Based on ASCII Value", International Journal of Computer Science and Information Technologies, Volume 5, Issue 6, pp. 7232-7234, 2014.
- [11] Vineet Sukhraliya , Sumit Chaudhary, Sangeeta Solanki." Encryption and Decryption Algorithm using ASCII values with substitution array Approach", International Journal of Advanced Research in Computer and Communication Engineering, Volume 2, Issue 8, pp. 3094-3097, 2013.
- [12] E.Anu Priya,Amit Agnihotri, Sachin Soni, Sourabh Babelay." Encryption using XOR based Extended key for Information security- A Novel Approach", International Journal on Computer Science and Engineering (IJCSSE), Volume 3, Issue 1, pp. 146-153, 2011.

*Development of cryptographic algorithm using bit shifting and Matrix XOR operations*

---

- [13] Kodabagi, M. M.; Jerabandi, M. V.; Gadagin, Nagaraj (2015). [IEEE 2015 International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT) - Davangere, Karnataka, India (2015.10.29-2015.10.31)] 2015 International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT) - Multilevel security and compression of text data using bit stuffing and huffman coding. , (), 800–804. doi:10.1109/ICATCCT.2015.7456992