Data Encryption by Excluding Repetitive Character in Cipher Text

Ajit Danti
Department of MCA
Jawaharlal Nehru National College of Engineering , Shimoga , Karnataka, India

Manjula G R
Department of Computer Science and Engineering
Jawaharlal Nehru National College of Engineering , Shimoga , Karnataka, India

Rajesh Nayak
Department of Computer Science and Engineering
Jawaharlal Nehru National College of Engineering , Shimoga , Karnataka, India

Abstract- In modern world, cryptography hackers try to break a cryptographic algorithm or try to retrieve the key, which is needed to encrypt a message (data), by analyzing the insertion or presence of repetitive bits / characters (bytes) in the message and encrypted message to find out the encryption algorithm or the key used for it. So it is must for a good encryption method to exclude the repetitive terms such that no trace of repetitions can be tracked down., Somdip Dey, Joyshree Nath and Ashoke Nath (SJA) is an amalgamation of Modified Caesar cipher(MCC), Bit Rotation Reversal(BRR), Neeraj Khanna, Joel James, Joyshree Nath, Sayantyan Chakraborty, Amlan Chakrabarti, Asoke nath (NJJSAA), Function Encryption (FE) methods.By using MCC, BRR, NJJSAA and FE methods we can reduce time complexity by exluding repetitive characters in the cipher text. The proposed method is robust in terms of efficiency and computational costs

Key words: Encryption, Decryption

I. INTRODUCTION

Due to tremendous growth in communication technology now the security of data is a really a big issue. In banking system the data must be fully secured. Under no circumstances the authentic data should go to hacker. In defense the security of data is much more prominent. The leakage of data in defense system can be highly fatal and can cause too much destruction. Due to this security issue different cryptographic methods are used by different organizations and government institutions to protect their data online. But, cryptography hackers are always trying to break the cryptographic methods or retrieve keys by different means. For this reason cryptographers are always trying to produce different new cryptographic method to keep the data safe as far as possible.

The present algorithm i.e. SJA is also symmetric key cryptographic method, which is basically based on advanced modified Caesar Cipher method [2], TTJSA [3], which itself is based on generalized modified Vernam Cipher [2], MSA [4] and NJJSAA [5]. Depending on the key entered by the user the functions of generalized modified Caesar Cipher and TTJSA are called randomly and then executed, and at last Bit Wise Rotation and Reversal technique will be executed on the final step to make the encryption more strong. In this paper multiple encryptions as well as multiple decryption method is also introduced.

As traditional encryption algorithm has the problem of repetitive character in the cipher text, in this project it has been taken care. So the objective is to develop an algorithm to exclude the repetitive terms in the cipher text. So that there will be no trace of repetitions in the cipher text. Also by applying additional algorithms like NJJSAA, Function Encryption and Bit Rotation and Reverse method, the encryption is made more secure and very hard to break.

The rest of the paper is organized as follows. Proposed embedding and extraction algorithms are explained in section II. Experimental results are presented in section III. Concluding remarks are given in section IV.

II. SYMMETRIC KEY ENCRYPTION

The symmetric key encryption is a cryptography technique that uses a shared secret key to encrypt and decrypt the data. Symmetric encryption algorithms are very efficient at processing large amounts of information and computationally less intensive than asymmetric encryption algorithms. Same key is used for both encryption and decryption technique. Maintaining the key secure is the most important task in symmetric key encryption.

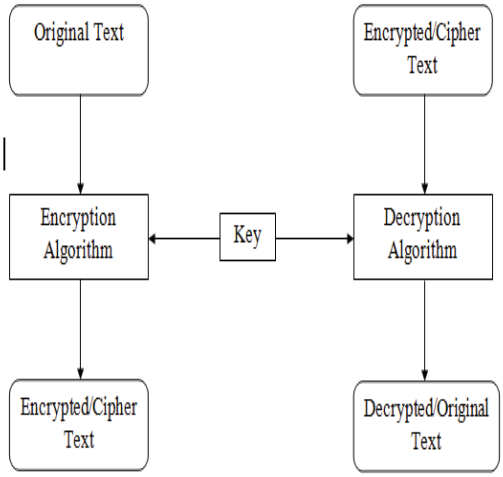


Fig. 1: Block diagram of data encryption and decryption.

Above fig. 1 shows the block diagram of data encryption and decryption. In encryption process, encryption algorithm is applied to the original text, which transforms the original text into the encrypted or cipher text. During decryption process, decryption algorithm is applied to the encrypted text to get back the original text. Same key is used for both processes.

III. SYSTEM DESIGN AND IMPLEMENTATION

This chapter presents the proposed algorithm used for the encryption. The encryption algorithm converts the original message mathematically based on the key to create encrypted message. The decryption algorithm restores an encrypted message to its original form. Here, the overall design of the algorithm and the various phases of the algorithm are discussed along with their respective flowcharts and implementation.

Whole system architecture depends on three modules which are explained below.

1. Modified Caesar Cipher[6].
   This is one of the encryption techniques which will recover the problem in the Caesar cipher method. It will encrypt the given message based on the key given by the user. It will generate some unique code which are used during encryption and decryption.
2. NJJSAA and Function Encryption.
   This is also an encryption technique which will perform its operation on each bit separately by performing mathematical operations on it.
3. Bit Rotation and Reversal Method.
   This technique will perform the rotation and it will reverse the each bit of the message.

3.1 System Architecture

Following are the system architecture for proposed algorithm. Architecture of both encryption and decryption process are described.

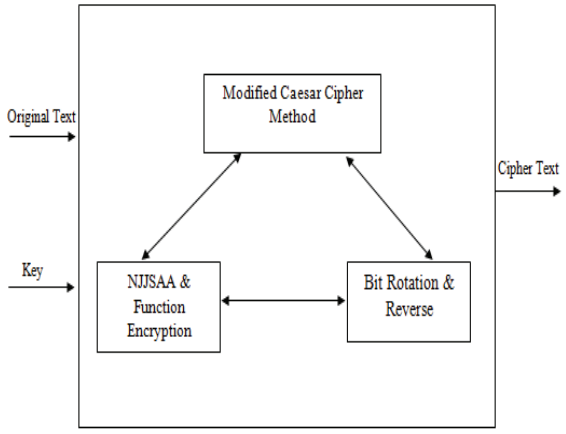
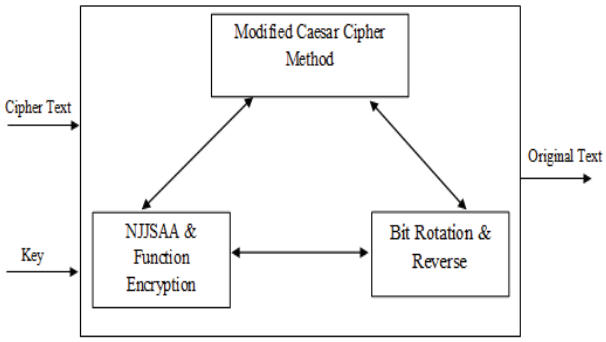


Fig. 2: Architecture diagram of Encryption.

The above Fig. 2 shows the encryption technique which is used in the proposed method. The encryption includes three parts. One is encryption using Modified Caesar cipher method; next is the encryption using combination of NJJSAA and Function encryption method, and finally encryption using Bit rotation and reverse method. These three methods are called randomly.

Original message to be encrypted and the key are given by the user. The key is of maximum 16-bit in length. Based on these information some unique codes are calculated which is used for successive encryption. Each encryption algorithm will give the encrypted message as output after doing some mathematical operations on the input message using the unique number which are generated by the key given by the user. In different order different algorithms are used so that it become very strong and very hard to break.

For different key provided by the user, even the input message is same, results will be different. Hence it's clear that the key plays an important role in creating the unique code as well as in the encryption



p

Fig. 3: Architecture diagram of Decryption.

The above Fig. 3 shows the decryption technique which is used in the proposed method. As in the encryption process, decryption also includes three parts. One is decryption using Modified Caesar cipher method; next is the decryption using combination of NJJSAA and Function encryption method, and finally decryption using Bit rotation and reverse method. These three methods are called randomly.

The encrypted message to be decrypted and the key are given by the user. The key is of maximum 16-bit in length, and should be as same as that of the key used for the encryption. Based on these information some unique codes are calculated which is used for successive decryption. Each decryption algorithm will give the decrypted message as output after doing some mathematical operations on the input message using the unique number which are generated by the key given by the user. In different order different algorithms are used so that it become very strong and very hard to break.

As all know that the decryption process is the reverse of the encryption process. So the order of algorithms is exactly the reverse of the encryption algorithms. As in proposed algorithm combination of two algorithms are used, same combinations of algorithms are applied in exactly the reverse order. In each decryption step, previously encrypted message is obtained. If different key used for decryption, then obtained message will not be the original message which is encrypted.

3.2 Flow Chart

Following are the flow chart for encryption and decryption of proposed method

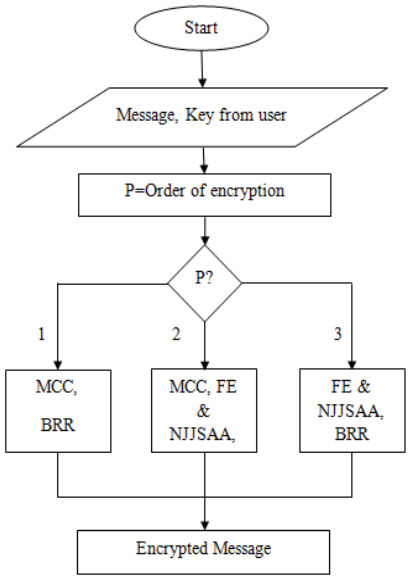


Fig. 4: Flow chart for encryption process in the proposed algorithm

The fig. 4 shows the flow chart for the encryption process which is implemented in this project. In the starting of the process, the user is asked to enter the password which is used as the key, which is used for encryption. Two unique numbers called " code " and "power_ex" are calculated using the key. These unique numbers are calculated by performing some mathematical operation on the key.

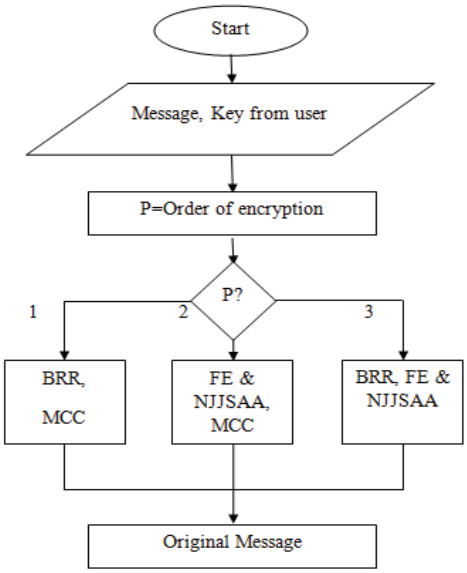


Fig.5: Flow chart for decryption process in the proposed algorithm

The fig 5 shows the flow chart for the decryption process which is implemented in this project. By applying the reverse order to that of encryption, corresponding original message is obtained. If the order is changed, result will be different.

IV RESULTS AND ANALYSIS

This chapter presents the details about the conduction of the experiments. It gives the details about each processing steps of the different algorithms which are included in this method. It also gives the details about the performance of the performance analysis of the different combination of the algorithms.

In each stage the message which needs to be encrypted is given for encryption, in which combination of two or more algorithms are used. Each algorithms process the message given by the user differently. But the final result is the encrypted message only. During decryption, the algorithms are applied in the reverse order. Corresponding original message is obtained. User should take care of selecting the order, because if the order of encryption and decryption is changed, then result will be wrong.

Table 1: Encrypted Messages in different combination

Original Message	**Modified Caesar Cipher and Bit Rotation & Reversal**	**Modified Caesar Cipher and NJJSAA & FA**	**NJJSAA & FA and Bit Rotation & Reversal**
abcde	ÙšÛ-bª	'—7_Ò	'ñáÁÙù'
aabbcc	ñáÁÙù	'×·¯"&	ññááÁÁ
abcxyz	ÙšÛ#g¯	'—7rú¾	ñáÁ×÷ç
hi hello	›\ b,#ê	·Ïu ÒNr	ÕõQÕùÝÝÍ

Table 1 shows the results obtained by using different combinations.

4.1 Performance Analysis

The performance graph gives the efficiency of the algorithms used in the proposed method. The efficiency is in terms of the time taken for encrypting and decrypting the message by different algorithms. It shows which combination of algorithms will run faster, and have good performance.

The performance graph shown in figure 6 is plotted by taking length of the message in X-axis and time taken to encrypt and decrypt in Y-axis. We will compare the time of 3 combinations of algorithms.

1. Modified Caesar Cipher method (MCC).
2. Combination of NJJSAA and Function Encryption (FE).
3. it Rotation and Reverse method (BRR).

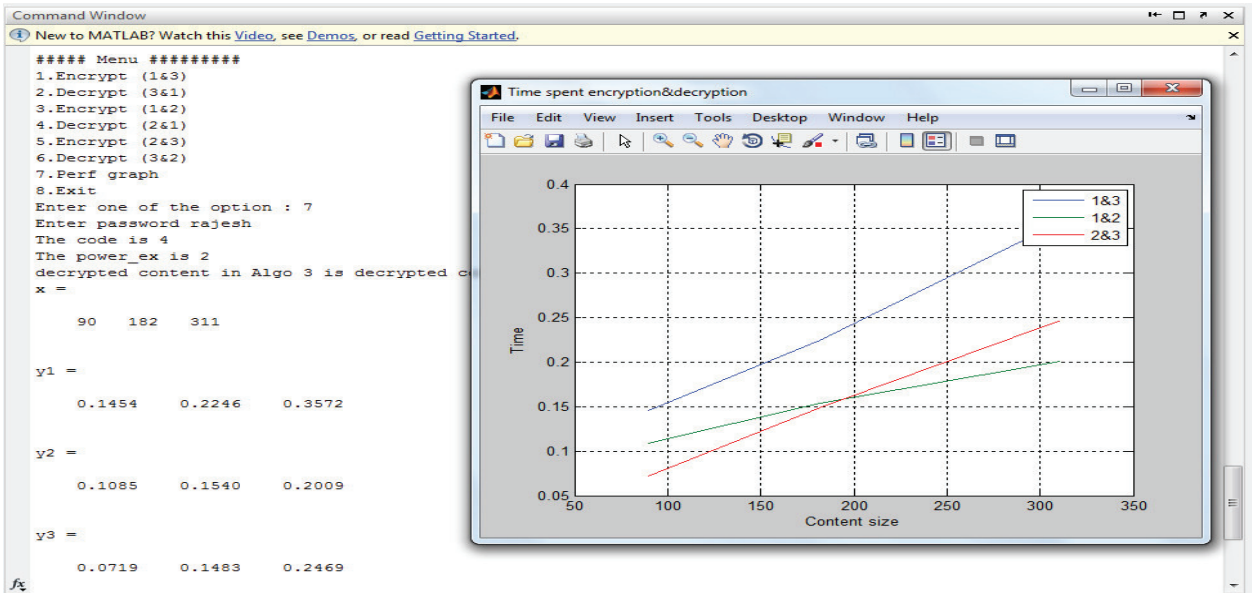


Fig. 6: Graph showing time taken for encryption and decryption

The combinations of these 3 algorithms are taken as 1&3, 1&2 and 2&3. By comparing the time taken by different combination, we can make out that combination of NJJSAA & FE and BRR performs better.

Table 2: Time taken for encryption and decryption for different length messages (with password as rajesh).

Length of the message In Bytes	**Time taken for Encryption and Decryption in seconds**		
	MCC and BRR	**MCC and combination of NJJSAA & FE**	**Combination of NJJSAA & FE and BRR**
90	0.1454	0.1085	0.0719
182	0.2246	0.1540	0.1483
311	0.3572	0.2009	0.2469

The table 2 contains the results obtained by taking the three different length of the message which is applied for encryption, and time taken for encrypting and decrypting that length message by different algorithms with the password “rajesh”.

Table 3: Time taken for encryption and decryption for different length messages (with password as veeresh).

Length of the message In Bytes	**Time taken for Encryption and Decryption in seconds**		
	MCC and BRR	**MCC and combination of NJJSAA & FE**	**Combination of NJJSAA & FE and BRR**
90	0.1754	0.1234	0.0792
182	0.2295	0.1487	0.1533
311	0.3636	0.1967	0.2511

The table 3 contains the results obtained by taking the three different length of the message which is applied for encryption, and time taken for encrypting and decrypting that message by different algorithms with the password "veeresh".

V.CONCLUSION

Results which are shown in section 4.1 shows that the proposed algorithm can avoid the problem with Caesar cipher method. That is the repetition of the characters in the cipher text. The implemented algorithm is not breakable by attack like brute force attack. The results in table 2 and 3 shows that the combination of Modified Caesar Cipher and NJJSAA and Function Encryption method will consume less time compare to other two combinations like Modified Caesar Cipher - Bit Rotation and Reverse method and NJJSAA and Function Encryption - Bit Rotation and Reverse method. But as far as the security concern, all the three combination will give more security. In real time applications combination of NJJSAA & FE and BRR is better as it takes less time for encryption.

5.1 Future Scope

The following issues may be considered for future work.

- Key length can be more than 16-bit.
- Some other encryption techniques can be combined with the proposed algorithm in order to increase the security.
- Encryption characteristics i.e. Security level can be studied especially when the proposed method is combined with other encryption techniques.

REFERENCES

[1] Somdip Dey, Joyshree Nath, Asoke Nath " An Integrated Symmetric Key Cryptographic Method – Amalgamation of TTJSA Algorithm , Advanced Caesar Cipher Algorithm, Bit Rotation and Reversal Method: SJA Algorithm" I.J.Modern Education and Computer Science, 2012, 5, 1-9.

[2] JoAnn Ward, "Caesar Ciphers: An Introduction to Cryptography", Purdue University GK-12, 2006. Http://www.purdue.edu/discoverypark/gk12/downloads/Cryptography.pdf

[3] Tamodeep Das, Trisha Chatterjee, Shayan dey, Joyshree Nath, Asoke Nath,, "Symmetric key cryptosystem using combined cryptographic algorithms - Generalized modified Vernam Cipher method, MSA method and NJJSAA method: TTJSA algorithm" Proceedings of Information and Communication Technologies (WICT), 2011 held at Mumbai, 11th – 14th Dec, 2011, Pages:1175-1180.

[4] 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.

[5] Dripto Chatterjee, Joyshree Nath, Suvadeep Dasgupta and Asoke Nath : "A new Symmetric key Cryptography Algorithm using extended MSA method : DJSA symmetric key algorithm", Proceedings of IEEE CSNT-2011 held at SMVDU(Jammu) 3-5 June,2011, Page-89-94(2011).

[6] Somdip Dey. "SD-AREE: An Advanced Modified Caesar Cipher Method to Exclude Repetition from a Message". International Journal of Information & Network Security (IJINS) Vol.1, No.2, June 2012, pp. 67-76.

[7] Dripto Chatterjee, Joyshree Nath, Sankar Das, Shalabh Agarwal and Asoke Nath, "Symmetric key Cryptography using modified DJSSA symmetric key algorithm". Proceedings of International conference Worldcomp 2011 held at LasVegas 18-21 July 2011, Page-306-311, Vol-1(2011).

[8] Dennis Luciano, Gordon Prichett, "Cryptography: From Caesar Cipher to Public key cryptosystems". The college mathematical journal, January 1987, vol-18, pp. 2-17.

[9] Dr. Natarajan Meghanathan, "Classical ciphers and their cryptanalysis", Jackson State University, Jackson MS. June 2002.