Implementation Of Simulation Of Byte Rotation Encryption Algorithm

Nidhi Gouttam

ABSTRACT: In this paper, we have imported some innovative advancement to the byte rotation encryption algorithm which is more secure and fast. The principal goal guiding the design of any encryption algorithm must be security against unauthorized attacks. Within the last decade, there has been a vast increase in the accumulation and communication of digital computer data in both the private and public sectors. Much of this information has a significant value, either directly or indirectly, which requires protection. The algorithms uniquely define the mathematical steps required to transform data into a cryptographic cipher and also to transform the cipher back to the original form. Performance and security level is the main characteristics that differentiate one encryption algorithm from another. We have simulate a new encryption algorithm (developed in 2012) "Byte – Rotation Encryption Algorithm (BREA)" with "Parallel Encryption Model" which enhances the security as well as speed of the encryption scheme. The BREA is applied on different blocks of plaintext and executes in parallel manner through multithreading concept of single processor system.

Keywords: Encryption, Decryption, key, BREA, Plain text, cipher text.

INTRODUCTION

Cryptography is the art of communicating with secret data. The cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication and data origin authentication, also it means hidden writing, and it refers to the practice of using encryption to conceal text. So changing the original data to a secret message is called Encryption, while Decryption is the reverse. The process of encryption and decryption of the data is based on a mathematical procedure called the Algorithm. The design of secure systems using encryption techniques focuses mainly on the protection of (secret) keys. Keys can be protected either by encrypting them under other keys or by protecting them physically, while the algorithm used to encrypt the data is made public and subjected to intense security. When cryptographers hit on an effective method of encryption (a cipher), they can patent it as intellectual property and earn royalties when their method is used in commercial products. Some of them are most popular in achieving data security at a great extent like AES and Blowfish. The AES has been adopted as a Standard for Encryption by NIST (National Institute of Standards and Technology's). The conventional methods of encryption can only maintain the data security. The information could be accessed by the unauthorized users for malicious purpose. Therefore, it is necessary to apply effective encryption / decryption methods to enhance data security. The multiple encryption and multilevel encryption system provides sufficient security. Therefore, it is necessary to apply effective encryption / decryption methods to enhance data security. The multiple encryption and multilevel encryption system provides sufficient security. But, as security level is increased, the time and complexity of algorithm is also increased and speed and performance of these system is low. This is the major cause of decreasing the speed and efficiency of the encryption system. In this work we have a new encryption algorithm "Byte – Rotation Encryption Algorithm (BREA)" with "Parallel Encryption Model" which enhances the security as well as speed of the encryption scheme.

RELATED WORK

Cryptography is the science of secret codes, enabling the confidentiality of communication through an insecure channel. It protects against unauthorized parties by preventing unauthorized alteration of use. It uses a cryptographic system to transform a plaintext into a cipher text, using most of the time a key. The cryptography is divided into two main categories, the first and the most common category is called classical cryptosystems encryption algorithms (also called single-key or symmetric) which uses a single shared key to encrypt and decrypt a message. The most common Algorithms within this category are called Data Encryption Standard (DES), AES, Triple DES (data encryption standard), RSA, Blowfish etc. Cryptography is considered not only a part of the branch of mathematics, but also a branch of computer science. There are three main forms of cryptosystems:-

- Symmetric Encryption System
- Asymmetric Encryption System and
- Hash Functions.

These models of encryption have been developed to provide security of information but each of them having some merits and demerits. No single algorithm is sufficient for this purpose. As a result researchers are working in the field of cryptography to remove the deficiency and finding better solution. As a result researchers are working in the field of cryptography to remove the deficiency and finding better solution. In this work, an effort has been made to develop a new simulation of algorithm BREA which is a block cipher and used with Block Wise Parallel Encryption Model .The multiple encryptions and multilevel encryption system provides sufficient security. But the performance and speed of these systems is low. Their complexity is very high. In this work, a new encryption algorithm named "**Byte – Rotation Encryption Algorithm (BREA)"** is simulate which is applied on different blocks of plaintext and executes in parallel manner through multithreading concept of single processor system. This algorithm is an attempt to invent a new encryption simulator which is more secure and very fast to others

MOTIVATION

Cryptography is the art of communicating with secret data. The cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication and data origin authentication, also it means hidden writing, and it refers to the practice of using encryption to conceal text. So changing the original data to a secret message is called Encryption, while Decryption is the reverse. The process of encryption and decryption of the data is based on a mathematical procedure called the Algorithm. The design of secure systems using encryption techniques focuses mainly on the protection of (secret) keys. Keys can be protected either by encrypting them under other keys or by protecting them physically, while the algorithm used to encrypt the data is made public and subjected to intense security. When cryptographers hit on an effective method of encryption (a cipher), they can patent it as intellectual property and earn royalties when their method is used in commercial products. Some of them are most popular in achieving data security at a great extent like AES and Blowfish. The AES has been adopted as a Standard for Encryption by NIST (National Institute of Standards and Technology's). The conventional methods of encryption can only maintain the data security. The information could be accessed by the unauthorized users for malicious purpose. Therefore, it is necessary to apply effective encryption / decryption methods to enhance data security. The multiple encryption and multilevel encryption system provides sufficient security. Therefore, it is necessary to apply effective encryption / decryption methods to enhance data security. The multiple encryption and multilevel encryption system provides sufficient security. But, as security level is increased, the time and complexity of algorithm is also increased and speed and performance of these system is low. This is the major cause of decreasing the speed and efficiency of the encryption system. In this work we have an encryption algorithm "Byte – Rotation Encryption Algorithm (BREA)" with "Parallel Encryption Model" which enhances the security as well as speed of the encryption scheme.

BYTE -ROTATION ENCRYPTION

ALGORITHM

The BREA algorithm has the following features…

1. It is a Symmetric Key Block Cipher Algorithm.
2. Each block size is of 16 bytes.
3. Size of Key matrix is 16 bytes.
4. Values of Key matrix are randomly selected and ranging from 1 to 26.
5. Mono alphabetic substitution concept is followed.
6. Byte-Rotation technique is used.

The steps of proposed Byte-Rotation Encryption Algorithm:

1. The letters of alphabet are assigned numerical values from 1 to 26 in sequence i.e. A, B, C, ..., X, Y, Z assigned numerical values 1, 2, 3, ..., 24, 25, 26 Respectively, the digits from 1 to 9 assigned numerical values from 27 to 35 respectively and the zero (0) remains as it is.
2. The plaintext is partitioned into fixed-length blocks of size 16 bytes (or 128 bits) each. These blocks are represented by a matrix Mp.
3. The values of Key matrix (K) are randomly selected from the range 1 to 26. The size of Key matrix is equivalent to the block size of plaintext i.e. 16 bytes.

K = [k1, k2, ..., k16]

K = Random (1, 26, 16)

4. Calculate the Transpose matrix of plaintext block matrix (Mp), which is denoted by MpT.

5. Calculate encrypted Key matrix Ke using the following formula:

Ke = K mod 2

6. Add both the matrices MpT and Ke and the resultant matrix is denoted by Cpk.

Cpk = MpT + Ke

7. Rotate first three rows horizontally of Cpk matrix such that rotate one byte from first row, rotate two bytes from second row, rotate three bytes from third row and fourth row remains untouched. The resultant matrix is denoted by Chr.

8. Rotate first three columns vertically of Chr matrix such that rotate one byte from first column, rotate two bytes from second column, rotate three bytes from third Column and fourth column remains untouched. The resultant matrix is denoted by Cvr.

9. Replace numeric values of Cvr matrix by their corresponding letters and if 36 exist in Cvr matrix, it is replaced by the special character #. The resultant Matrix is denoted by Ce.

Results Demonstration

To demonstrate the potency of BREA, we tested our system with some online application Fig-1 BREA encryption interface of Fig-2 to complete encrypt-decrypt process. Each message is secure because this method is followed matrix rotation and substitution method. Both substitution method and transposition method. encryption are easily performed with the power of computers. The combination of these two classic techniques provides more secure and strong cipher. The final cipher text is so strong that is very difficult to break. Substitution method only replaces the letter with any other letter and transposition method only change position of characters. The BREA method (algorithm) is the combination of both the transposition and substitution method which provides much more secure cipher. One biggest power of BREA is that it requires less computer resources when compared to other encryption algorithms.

Fig-1: Encryption Interface

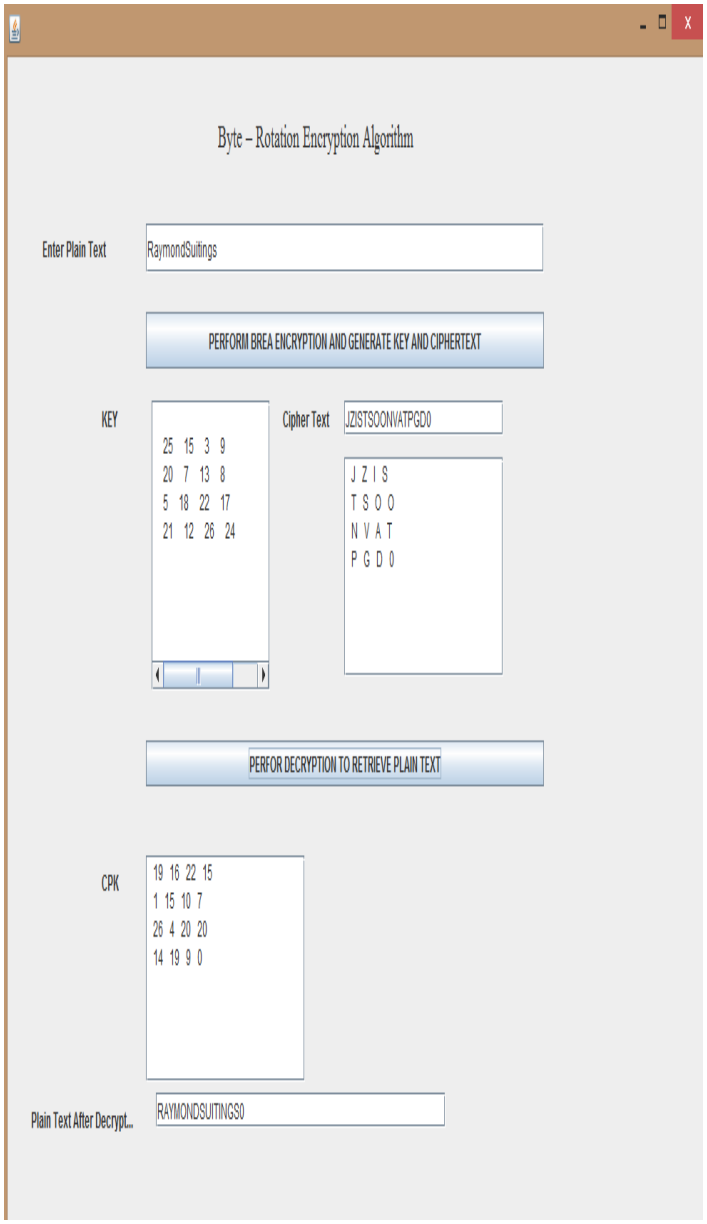

Fig-2: Encryption-Decryption Interface

REFERENCES

[1]. http:/www.laits.utexas.edu/anorman/BUS.FOR/course.mat/SSim/history.html

[2]. www.iaeng.org/publication/WCECS2012/WCECS2012_pp979-982.pdf
Himanshu Gupta, “Multiphase Encryption Technique”, An Article Amity UniversityU.P.March2011http://en.wikipedia.org/wiki/A_New_Concept_for_Multiphase_Encryption_Techniques

[3]. www.aect.cuhk.edu.hk/ect7010/Materials/Lecture/Lec4.pdf

[4]. http://www.banasthali.org/banasthali/wcms/en/home/

[5]. www.amazon.com/Introduction.Cryptography/dp/1584885513

[6]. www.springer.com/computer/cryptology/978-3-540-49243-6

[7]. hackme.wablab.com/cryptography-two-basic-cryptographic-principles

[8]. ssmy.safaribooksonline.com/book/certification/cryptography/sect1- 99

[9]. http:/en.wikipedia.org/wiki/Multithreading

[10]. Walter Tuchman, “A brief history of the data encryption standard", ACM Press/Addison-Wesley Publishing Co. NY, USA, pp. 275–280, 1997

[11]. Sunita Bhati & Prof. S. K. Sharma, “Block Wise Parallel Encryption through Multithreading Concept”, Research Paper published in Aishwarya Research Communication Journal (ISSN: 0975-3613) Vol. 3, August 2011, pp. 100-106.Proceedings of the World Congress on Engineering and Computer Science.

Nidhi Gouttam is a student of Master of Technology in information technology at Banasthali University, NEWAI, Rajasthan, India. She has received her B.TECH. Degree from Stani memorial college of engineering and Technology, Phagi, JAIPUR, India. Her Current research interest is Information Security.