Advances in Computer Science and Information Technology (ACSIT)
p-ISSN: 2393-9907; e-ISSN: 2393-9915; Volume 2, Issue 13; July-September, 2015 pp. 68-70
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/Publication.html

Security of Internet using Cryptography through BREA, ASCII Code Method and Linear Algebra

Asmita Patel[1] **and Divya Sahu**[2]

[1,2]M.Sc.(CS) Final Year, Dev Sanskriti Vishwavidyalaya Haridwar (U.K)
E-mail: [1]patel.asmita30@gmail.com, [2]trdivya72@gmail.com

Abstract—*Now a days, the networking technology leads a practice of interchanging of the information, images, and personal data very frequently. The protection of multimedia data, sensitive information like credit cards, banking transactions and social security numbers is becoming very important. The protection of these confidential data from unauthorized access can be done with many encryption techniques. So for providing data security many cryptography techniques are employed, such as symmetric and asymmetric techniques. In this research paper we deals the various techniques of encryption of data with the help of linear algebra, ASCII values, Byte code rotation.*

1. INTRODUCTION

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient.

In cryptography, encryption is the process of encoding some information in a manner that hackers or eavesdroppers cannot read it. It is becomes readable only with a decryption code. The use of encryption/decryption is as old as the art of communication. Various secret or important messages have to be sent without any third party being able to read it. Encryption has long been used by militaries and governments to facilitate secret communication. Now a days, encryption is also used in protecting information within many kinds of civilian systems.

In an encryption scheme, the message or information (or simply the plaintext) is encrypted using an encryption algorithm, turning it into an unreadable form called as “cipher text”. The main purpose of encryption is the encrypted message or information should not be able to determine anything about the original message. Only authorized party, however, will be able to decode this cipher text using the corresponding decryption algorithm. The stronger the cipher text, that is, the harder it is for unauthorized people to break it, the better, in general. But this however means that as the strength of encryption/decryption increases, so does the cost.

All operations with modern encryption algorithms like Triple DES, AES, Blowfish and RSA, and message digest hash algorithms like SHA-1 and MD5 operate on a *sequence of bytes*, not on a string of characters. So the simple rule is always to convert your "String" type into an array of "Byte" types before passing it to the cryptographic function. And do not try to stuff ciphertext bytes back into a String type

2. TYPES OF CRYPTOGRAPHY:

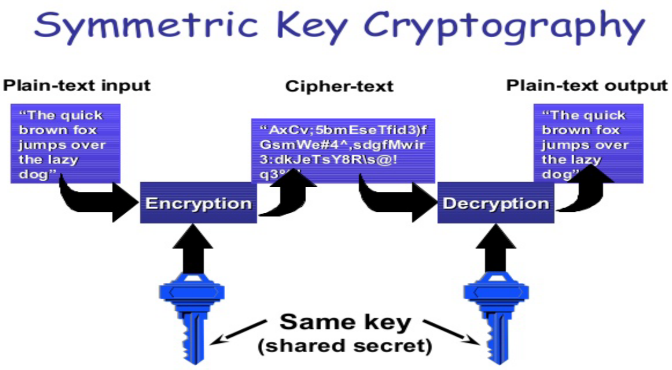
There are two main types of cryptography:

1) Secret key cryptography or symmetric key cryptography

2) Public key cryptography or asymmetric key cryptography

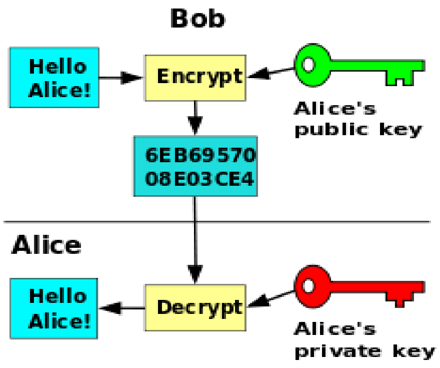
3. SYMMETRIC KEY CRYPTOGRAPHY

Symmetric key cryptography refers to encryption methods in which both the sender and receiver share the same key. In symmetric key cryptography, the same key is used by both parties. The sender uses this key and an encryption algorithm to encrypt data; the receiver uses the same key and the corresponding decryption Algorithm to decrypt the data. This was the only kind of encryption publicly known until June 1976.


Symmetric Key Cryptography
Plain-text input
Cipher-text
Plain-text output
“The quick brown fox jumps over the lazy dog”
“AxCv;5bmEseTfid3)fGsmWe#4^,sdgfMwir3:dkJeTsY8R\s@!q3%”
“The quick brown fox jumps over the lazy dog”
Encryption
Decryption
Same key (shared secret)

4. PUBLIC KEY CRYPTOGRAPHY

Public key cryptography, where different keys are used for encryption and decryption. In asymmetric or public key cryptography, there are two keys: a private key and a public key are used. The private key is kept by the receiver and public key is announced to the public.



5. DESCRIPTION OF DIFFERENT TECHNIQUES

1. PROPOSED 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.

2. Cryptography through ASCII Code

The architecture consists of the following steps:

- Firstly select any number randomly
- After selection use starting and ending number and make subset, followed selection of modulus and remainder as well
- When subset is selected then it is divided by mode
- After division take only those number which gives remainder
- Finally selected numbers will be resumed as substitution array

6. MECHANISM

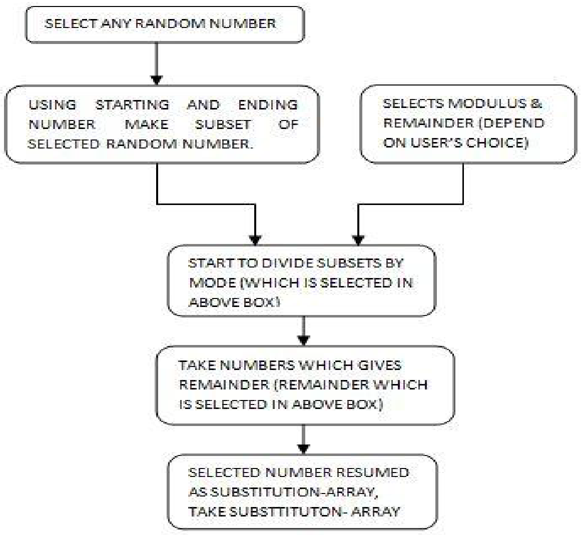
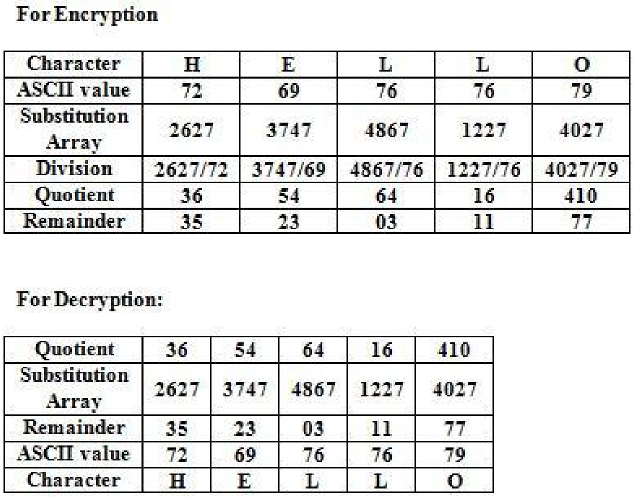

SELECT ANY RANDOM NUMBER
USING STARTING AND ENDING NUMBER MAKE SUBSET OF SELECTED RANDOM NUMBER.
SELECTS MODULUS & REMAINDER (DEPEND ON USER'S CHOICE)
START TO DIVIDE SUBSETS BY MODE (WHICH IS SELECTED IN ABOVE BOX)
TAKE NUMBERS WHICH GIVES REMAINDER (REMAINDER WHICH IS SELECTED IN ABOVE BOX)
SELECTED NUMBER RESUMED AS SUBSTITUTION-ARRAY, TAKE SUBSTTITUTON- ARRAY

Fig. 1: Procedure of Substitution array



For Encryption

Character	H	E	L	L	O
ASCII value	72	69	76	76	79
Substitution Array	2627	3747	4867	1227	4027
Division	2627/72	3747/69	4867/76	1227/76	4027/79
Quotient	36	54	64	16	410
Remainder	35	23	03	11	77

For Decryption:

Quotient	36	54	64	16	410
Substitution Array	2627	3747	4867	1227	4027
Remainder	35	23	03	11	77
ASCII value	72	69	76	76	79
Character	H	E	L	L	O

Fig. 4: Table Content of Encryption & Decryption

3. Cryptography using Linear Algebra

Encoding Algorithm

- Find the latitude (Y˚Z’) and longitude (Q˚R’) of the location you want to encode.
- Encoding the latitude (Y˚Z’) Take any two 3 x 3 matrices A, B such that determinant (A) = Y, determinant (B) = Z.
- Take any sentence S1 in English language. Form a 3 x 3 matrix X, where the entry values of the matrix represent the first nine letters of the sentence.
- Determine K = X – A, Y= K – B.
- Write all the entry of Y row wise and convert them into a string of letters using the encoding chart. Prefix and suffix this string with N or S depending on the north or south position in the latitude to obtain a string S2
- Encoding the longitude (Q˚R’)
- Construct a string S3 using numbers letters and symbols. This string will start with 6 and end with 9 if the location is to the east, else string will start with 8 and end with 7 if the location is to the west.
- R = the 2 symbols of S3 with less ASCII value added with each other and the result will be subtracted from the symbol with greatest ASCII value of symbols in S3.
- Q = addition of the ASCII values of the remaining symbols in S3.
- Encrypt < S1 > < S2 > < S3 > to the receiver.

Decryption Algorithm

- Determine the matrix X from S1 and hence A = X – K.
- Determine the matrix Y from S2 and hence B = Y – K.
- Determinant A and determinant B decides the latitude.
- Determine the values of R and Q using the formula in the string S3 which decides the longitude.
- Decode the location from world map.

7. CONCLUSION

In this paper the existing encryption techniques are studied and analyzed. Each algorithm having its own advantages and disadvantages, our system proposed a good strategy of making most out of the advantages of BREA, ASCII CODE Method, and Linear Algebra Method while trying to eliminate the limitations. The developed system ignoring the front end could be used in any network services for network security. The concept of block wise parallel encryption using multithreading technique enhances the speed of encryption system. Everyday new encryption technique is evolving hence fast and secure conventional encryption techniques will always work out with high rate of security.

8. FUTURE RESEARCHES

The system can be easily modified to accept any encryption algorithm which would be framed in future. Just by adding or removing another module in the main function, any number of algorithms can be included or reduced. Moreover, we currently concentrate on our next work which adopts Parallelism through multiprocessor system where we can run various Encryption Algorithms in parallel environment which enhances the performance and speed of Encryption/ Decryption process.

REFERENCES

[1] W.Stallings, “Cryptography and Network Security: Principles and Practices”, Prentice Hall, 1999.

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

[3] Swati Paliwal Ravindra Gupta,”A Review of Some Popular Encryption Techniques”,International Journal of Advanced Research in Computer Science and Software Engineering,Volume 3, Issue 2, February 2013 ISSN: 2277 128X.

[4] Nitin Jirwan, Ajay Singh, Dr. Sandip Vijay,”Review and Analysis of Cryptography,Techniques”,International Journal of Scientific & Engineering Research Volume 4, Issue3, March-2013 ISSN 2229-5518.

[5] Perrig, J. Stankovic, and D. Wagner,“Security In Wireless Sensor Networks,” ACM,Vol.