ORIENTAL JOURNAL OF COMPUTER SCIENCE & TECHNOLOGY
An International Open Free Access, Peer Reviewed Research Journal
Published By: **Oriental Scientific Publishing Co., India.**
www.computerscijournal.org

ISSN: 0974-6471
December 2012,
Vol. 5, No. (2):
Pgs. 283-288

Double-reflecting Data Perturbation Method for Information Security

MARAM BALAJEE[1] and CHALLA NARASIMHAM[2]

[1]P.hD part-time Scholar from Bharathiar University,
Department of IT, G M R Institute of Technology, Rajam, Andhra Pradesh - 532 127, India.
[2]Amritha Sai Institute of Science and Technology, Vijayawada, India.

(Received: July 12, 2012; Accepted: August 04, 2012)

ABSTRACT

Information Security plays a vital role in data Communication through LAN, WAN, Internet etc. Cryptography is one of the best tools for Information Security. Cryptography is made up of two different tools that are Encryption and Decryption. Encryption is the method to hide the original data in Data Communication. While Data Communication, the data is masked using codes/shuffling. Here the purpose is to ensure privacy by keeping the information hidden/encoded to which it is not intended. When data reached destination, the encrypted data will be decrypted using some mathematical functions or decoding techniques is called Decryption. The processes are done using mathematical login, or algorithms. This paper proposes new methods for encryption and decryption by using some mathematical methods and number sequences.

Key words: cryptography, data perturbation, Fibonacci, Lucas, number sequence.

INTRODUCTION

Symmetric Cryptography

In Symmetric Cryptography, a single shared secret key is used for both encryption and decryption. Any person which has the key can use it to encrypt and decrypt the data. The technique in Symmetric Cryptography is very easy and fast for processing big-data. Here both the sender and receiver should agree in advance on the shared secret-key that will be used to encode and decode the data. Usually the people are sharing the shared secret-keys through data communication channels only. So there is no security while transmitting those keys in data communication channels. This is the one of the main disadvantage in Symmetric Encryption. In this method, we are using the same shared secret-key for encryption and decryption.

The most popular symmetric algorithms like

- Data Encryption Standard (DES)
- Triple Data Encryption Standard
- (Rivest Cipher) RC2
- Rijndael Advanced Encryption Standard (AES)

Asymmetric Encryption

In Asymmetric Encryption, there is a need of two different keys for encryption and decryption.

Those keys are mathematically related and formed as a pair. Those two keys are called Private-key and Public-key. Asymmetric Encryption is called as Public key Cryptography, since users typically create a mathematically related key pair, and make one public while keeping the other secret.

In this method, users can encrypt messages with their private keys. Here the recipient can verify that the sender's public key can decrypt the message, then it proves that the sender's secret key was used to encrypt the data. Users can send secret messages by encrypting a message with the recipient's public key. In this case, the only intended recipient can decrypt the message, because the only sender have access to the required secret key. Finally, both the sender and receiver should use both the keys i.e Private key and Public key.

The most popular Asymmetric algorithms like

- Rivest Shamir Adleman (RSA)
- Elliptic Curve Cryptography (ECC)
- El Gamal Digital Signature Algorithm (DSA)

Existing Systems

Fibonacci sequence

Fibonacci[2] (1170-1230) introduced Arabic numerals to Europe. Being a mathematician, he attempted to solve a problem which he had raised: How big would a rabbit colony be each month if rabbits gave birth to a pair of young every month and started breeding at two months of age? The solution he discovered was to add the rabbits from the previous month with the young from the current month. This gives a sequence (the Fibonacci[2] sequence) in which "each number is the sum of the two preceding numbers". Thus, the sequence progresses: 1 2 3 5 8 13 21 34 55 89 144 233 377 610 987 1597... . The Fibonacci[2] sequence is the series of numbers: 1, 1, 2, 3, 5, 8, 13, 21, 34 ...

Lucas Numbers

Francois-Edouard-Anatole Lucas[3] (4.4.1842 - 8.10.1891) is the French mathematician, professor. Lucas[3] is best known for his results in number theory: in particular he studied the Fibonacci[2] sequence and the associated Lucas[3] sequence is named after him. The main numerical sequence considered by Lucas[3] is the sequence of numbers 1, 3, 4, 7, 11, 18, 29, 47, ... given with the following recurrent formula:

$$Ln = Ln\text{-}1 + Ln\text{-}2 \text{ for } n > 2,\ L1 = 2,\ L2 = 1$$

for the initial terms L(1) = 1 and L(2) = 3. In the honor of Lucas [3] this numerical sequence was called "Lucas[3] numbers". Note that Lucas[3] numbers have the same significance for mathematics, as well as the classical Fibonacci[2] numbers.

The Double-Reflecting Data Perturbation Method

The Double-Reflecting Data Perturbation Method[7] denoted by DRDP reverberates the original data by x-axis and y-axis to achieve the perturbed data for some confidential attribute. In this method, the randomization function plays a very crucial rule, and if the function is not properly chosen it May degrade the clustering quality. The distortion operation performed to the confidential attribute is given by

$$op_j = \rho_{Aj} + (\rho_{Aj -\ aj\ ) = 2}\ \rho_{Aj - aj.}$$

Where Aj ($1 \leq j \leq n$) is a confidential attribute and a j ($1 \leq j \leq n$) is an instance of Aj. ρ_{Aj} is defined by the following formula

$$\rho_{Aj\ = |(\max Aj\ +\ \min Aj)/2|}$$

Where max Aj and min Aj are respectively the maximum value and minimum value of attribute Aj. The 'student' relational database before and after applying DRDP is shown in the following Table:

Table 1:

S.No	Roll No	Name	Marks	Distored Marks
1	101	Raj	78	92
2	102	Ravi	89	81
3	103	Rohan	92	78
4	104	Rani	82	88
5	105	Rahul	80	90

Proposed System

The proposed system is based on symmetric cryptography[1]. Before starting communication, one shared secret should be shared by both the parties which is same as in existing systems.

Encryption:

Assume the message is “THIS IS BOOK. IT IS NICE.”, the shared secret-key is “NETWORKS”.

Step 1

The characters (ASCII values) in the first sentence of the paragraph are shuffled based on the *Double-Reflecting Data Perturbation Method*. After shuffling, the first sentence “THIS IS BOOK.” is like the following:

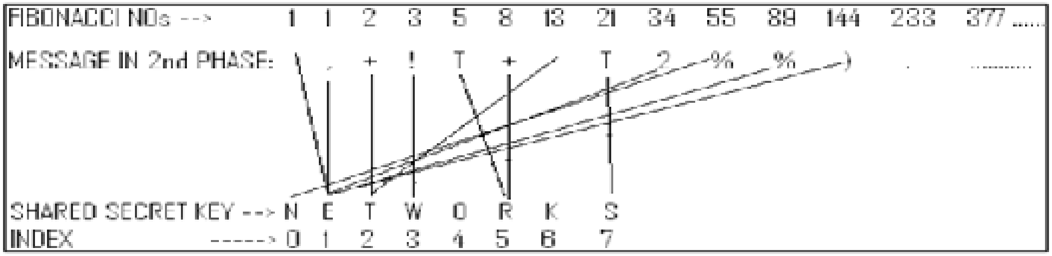
“ ,+!T+ T2%%).”

Step 2

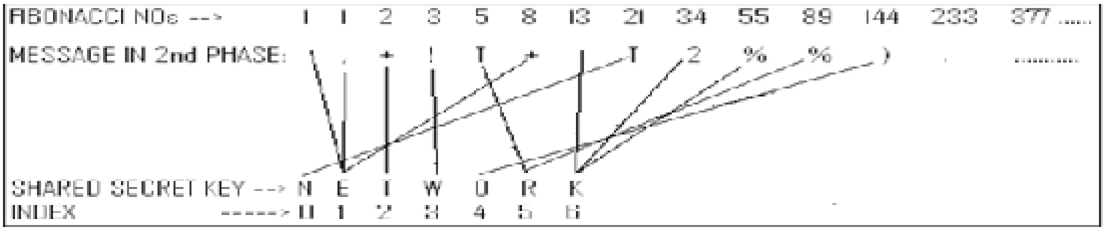
It considers all the characters in the sentence except “.”. Here “.” is copied from 1st phase to 2nd phase.

Step 3

Now the shuffled sentence “ ,+!T+ T2%%).” is XORed with shared secret-key in the following way. Here the shared secret-key is “NETWORKS” and its length is 8.



When the shared secret-key is “NETWORK”, then the length is 7. So the message “ ,+!T+ T2%%).” is encrypted in the following way:



Here the size of the secret-key “NETWORKS” is 8. The first character in the sentence is XORed with the character which is having the index is equal to first Fibonacci[2] number % size of shared secret-key. The 2nd character is XORed with the character which is having the index is equal to second Fibonacci[2] number % size of shared secret-key and so on. It will continue up to 23 iterations.

Now the 24th character is XORed with the character which is having the index is equal to first Fibonacci[2] number % size of shared secret-key. The 25th character is XORed with the character which is having the index is equal to second Fibonacci[2] number % size of shared secret-key and so on. Again it will continue up to 23 iterations.

STEP 4: After completion of current sentence, the shared secret-key is rotate right-shift with the number which is equal to FIRST NUMBER IN LUCAS[3] SEQUENCE % SIZE OF SHARED SECRET-KEY. Now it is a new temporary key which is based on shared secret-key. In our example, the temporary key “ETWORKSN” for 2nd sentence.

Step 5

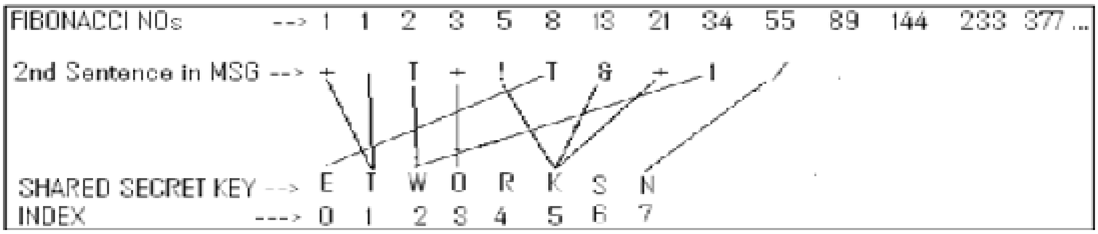
The next sentence in the paragraph is shuffled according to the *Double-Reflecting Data Perturbation Method*. After shuffling, the 2nd sentence is "+ T+!T&+1/."

Step 6

Now the shuffled sentence is XORed with shared secret key in the following way:

Step 7

In this way, all sentences will have been encrypted using a single shared secret-key. Internally that key will be rotate right shifted based on the number sequence from LUCAS [3] NUMBER SEQUENCE which are 1 , 3, 4, 7, 11, 18, 29, 47, 76, 123, 199, 322, 521, 843, 1364, 2207, 3571, 5778, 9349, 15127, 24476, 39603, 64079 (23 numbers from LUCAS[3] NUMBER SERIES) as



explained above. In this example, the shared secret-key is rotate right shifted with 1,3,4,7,3,2,5,7,4,3,7,2,1 and so on up to 23 numbers only.

Step 8

The final result is like the following:

ei□v□er□fv`g.□t□dj□m`fa.

Step 9

This encrypted message will be transferred to the Destination system.

Decryption

Step 1

The received message is like the following:

Step 2

It is converted to binary form like the following:

01100101 01101001 01111111 01110110 00000110 01100101 01110010 00000110 01100110 01110110 01100000 01100111 00101110 01111111 01110100 00000011 01100100 01101010 00011010 01101101 01100000 01100110 01100001 00101110

Step 3

Here the shared secret-key "NETWORKS" is converted into binary form like the following:

01001110 01000101 01010100 01010111 01001111 01010010 01001011 01010011

Step 4

Now the STEP 2 message is XORed with STEP 3 massage. It will continue up to the resultant character is equal to '.'. For next sentence, all the characters in shared secret-key is rotate right shifted according to the remainder when LUCAS[3] NUMBER SERIES i.e. 1 , 3, 4, 7, 11, 18, 29, 47, 76, 123, 199, 322, 521, 843, 1364, 2207, 3571, 5778, 9349, 15127, 24476, 39603, 64079 (23 numbers from LUCAS[3] NUMBER SERIES) is divided by the length of shared secret-key.

According to our example, the remainders are like 1,3,4,7,3,2,5,7,4,3,7,2,1 and so on up to 23 numbers only. So for 2nd sentence, the shared secret-key is "ETWORKSN". For 3rd sentence, the shared secret-key is "TWORKSNE" and so on.

Step 5

Here the result is in the following:

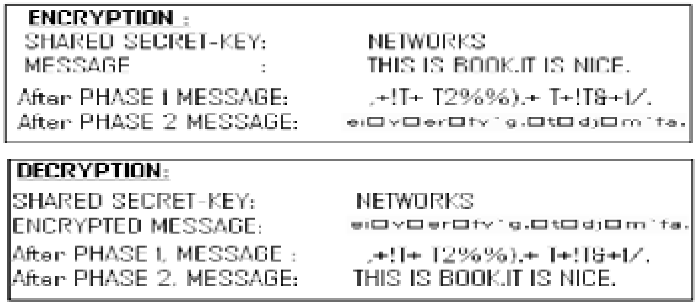
" ,+!T+ T2%%).+ T+!T&+1/."

Step 6

All the characters (ASCII values) in each sentence will be reshuffled based the Double-Reflecting Data Perturbation Method which explained previously in this paper.

Step 7

After applying "Double-Reflecting Data Perturbation Method", the final result is like the following:


ENCRYPTION :
SHARED SECRET-KEY: NETWORKS
MESSAGE : THIS IS BOOK.IT IS NICE.
After PHASE I MESSAGE: ,+!T+ T2%%).+ T+!T8+1/.
After PHASE 2 MESSAGE: ei□v□er□tv`g.□t□dj□m`ta.

DECRYPTION:
SHARED SECRET-KEY: NETWORKS
ENCRYPTED MESSAGE: ei□v□er□tv`g.□t□dj□m`ta.
After PHASE I. MESSAGE : ,+!T+ T2%%).+ T+!T8+1/.
After PHASE 2. MESSAGE: THIS IS BOOK.IT IS NICE.

This Is Book. It Is Nice.

Pictorial Representation Of *Encryption & Decryption*

Advantages in Proposed System

1) For each sentence, a new key will be generated based on shared secret-key only.
2) For XOR operation, characters will be selected based on the length of the shared secret-key only.
3) The same sentence will be encrypted differently when the length of the shared secret-key is different.
4) The same consecutive characters will be encrypted differently (in some cases).

Security level

In 1st phase of proposed method, all the characters in the sentence are converted into ASCII. Now those characters are shuffled according to their ASCII value based on Double Reflecting Data Perturbation Method. The privacy of data is measured by the variance between the actual and the perturbed values which is given by the following formula

$$S = \frac{Var(X - X')}{Var(X)}$$

It has been analyzed that the privacy or the security level of the confidential data is improved a lot by the proposed method for Encryption and Decryption. The Security level of the Double Reflecting Data Perturbation Method for 1st sentence "THIS IS BOOK" is shown the following table,

Char(before DRDP)	Char(After DRDP)
84 (T)	32 (space)
72 (H)	44 (,)
73 (I)	43 (+)
83 (S)	33 (!)
32	84 (T)
73 (I)	43 (+)
84 (S)	32 (space)
32	84 (T)
66 (B)	50 (2)
79 (O)	37 (%)
79 (O)	37 (%)
75 (K)	41 ())

After observing this Chart, easily we can identify no similarities between Character (before DRDP) and Character (after DRDP). So it is a good significance in Cryptography.

CONCLUSION

Now a day, Information Security is very important for data communication. Till now we have seen many algorithms, methods and techniques. But the proposed system in this paper explains an advanced technique for giving security to the Information. In the future work, the work will be extended to Cloud computing.

REFERENCES

1. http://www.symmetriccryptography.com/
2. http://protea.worldonline.co.za/fibon.htm
3. http://milan.milanovic.org/ math /english/ fibo/ fibo3.html
4. Wang Jing, Wang Xiaogang, A New Clustering Algorithm of Preserving the Original Data's Privacy (2008).
5. Ali Inam, Selim. V. Kaya, Privacy preserving clustering on horizontally partitioned data, Data & Knowledge Engineering, **63**: 646-666 (2007).
6. Weijia Yang, Shangteng Huang, Data privacy protection in multi-party clustering, Data & Knowledge Engineering, **67**: 185-199, (2008).
7. A. Viji Amutha Mary, Dr. T. Jebarajan, A Novel Data Perturbation Technique with higher Security, IJCET, **3**(2): 126-132 (2012)