European Journal of Academic Essays 1(1): 11-16, 2014
ISSN: 2183-1904
www.euroessays.org

A Cognitive Cryptographic Approach Using DRDP Method

Balajee Maram[1], Dr Challa Narasimham[2]

[1] P.hD (CS) part-time Scholar from Bharathiar University,
Sr. Asst. Prof., Dept of IT, G M R Institute of Technology, Rajam,
Andhra Pradesh - 532 127, India. *balajee.m@gmrit.org*
[2] Professor, Dept. of CSE/IT, S R Engineering College, Warangal. *narasimham_c@yahoo.com*

Abstract: In Digital era, our life is bound with digital technology. In Information Technology, everything is available in digital form only. In the field of data communication, there is a need to send and receive data. But we don't know the data will reach the destination successfully and securely. Security and privacy plays an important role in digital and data communication. In the field of secure data communication, cryptography is very important technique.

Till now, we have seen many algorithms that are related to symmetric and asymmetric encryption and decryption. Most of the algorithms are related to text/data only. In this technique, there is a need to maintain one shared secret key or a pair of private-public keys. Why can't we send encrypted data without using any key(s)? This proposed method tells us how to implement cryptography using mathematical method "Double-Reflecting Data Perturbation Method".

Keywords: Double Reflecting Data Perturbation, Cryptography, Security, Data Communication, Information Technology

1. Introduction

1.1 What is the problem?

In every cryptographic algorithm, there is a need to either shared secret-key or private/public key pair. The strength of the encryption is based on the length of the key. When the length of the key is very small then it is very easy to crack the key as well as decrypt the data. In symmetric and asymmetric cryptography, the required keys should be shared in symmetric cryptography and the public key should be published in asymmetric cryptography techniques. Before data communication, all the required keys should be finalized. For exchange of keys, some effort is required to send the required keys with high security. Before sending the data, there is a need to finalize and share the keys successfully and securely. It is a regular process. Always we should take more care to send the keys.

1.2 Why is it interesting and important?

In cryptography, keys play an important role. Without using keys, we can't encrypt and decrypt the data. But in keys/data communication, it may have been hacked. After hacking the keys/data, cracking the key or data is not easy but may be possible. In existing technology, either shared secret-key or private-public key pair is required in data encryption/decryption. But providing protection to shared secret-key or private-public key pair in communication is somewhat difficult. Hence better to concentrate on mathematical methods for encryption and decryption.

1.3 Why is it hard?

Many cryptographic algorithms have been introduced to the world. Most of the algorithms have been cracked. If the size of the keys is more, then it is not easy to crack the keys. But in keys communication, there is a need of more and more attention for protecting the keys. While sending the keys, there is a chance to hack those passwords. It is very difficult to provide the protection all the time.

Corresponding Author: Balajee Maram, Email: balajee.m@gmrit.org

1.4 Why has not it been solved before?

The existing algorithms are working effectively. The exchange of keys and data is very difficult. So there is a need to exchange of keys before sending data. In existing technology, without using keys, we can't do anything. Why can't we shun existing technology which is using different keys?

1.5 What are the key components of my approach and results?

This paper proposes a new technique for encoding and decoding for data communication. Here we are trying to apply DRDP technique. In proposed encryption technique, each and every character has been calculated based on DRDP method only. This proposed algorithm has been checked and verified in PYTHON language successfully.

This proposed algorithm has been checked theoretically and practically.

2. Related Work

2.1 Database creation for Security Enhancement

This phase is implemented for security enhancement. This can be enhanced by taking the day of week into account. This proposed algorithm uses one file at a time. In our experimental setup both the sender and receiver has used 7 files (each file for a day of week). Both the sender and receiver should use same database and a file with both users should be of same name. This study has implemented this idea with 7 files but this can be extended even up to 'n' number of files [1].

The Primary goal is to provide protection in data communication through Internet. In such environment, the suitable algorithms should be used which provides security to our sensitive data. For data security, many approaches have been adopted. Among them, Data Perturbation is one of the important methods for data protection.

2.2 Translation data perturbation method

In the Translation Data Perturbation Method (TDP), the set of operations takes only the value {Add}. Here some fixed constant will be added to each character/number in the confidential data [2, 3].

Modified value = (Old value) + constant

Example: when we want to apply Data Perturbation method on 4th column by using the constant '5'.

Table 1: Example table of TDP

S.No	*Roll No*	*Name*	*Marks*	*Distorted Marks*
1	101	Rohan Raj	78	83
2	102	Shashank Raj	89	94
3	103	Prudvi Raj	92	96
4	104	Dhan Raj	82	86
5	105	Mythily Raj	80	85

2.3 The scaling data perturbation method

In the Scaling Data Perturbation (SDP) method, the set of operations takes only the value {Mult}. Here some fixed constant will be multiplied to each character/number in the confidential data.

Example: when we want to apply Data Perturbation method on 4th column by using the constant '0.75'.

Table 2: Example table of SDP

S.No	*Roll No*	*Name*	*Marks*	*Distorted Marks*
1	101	Rohan Raj	78	58
2	102	Shashank Raj	89	66
3	103	Prudvi Raj	92	72
4	104	Dhan Raj	82	64
5	105	Mythily Raj	80	63

2.4 The hybrid data perturbation method

In the Hybrid Data Perturbation (HDP) method, the set of operations takes only the value {Add,Mult}. Here some fixed constant will be added and multiplied to each character/number in the confidential data.

Example: when we want to apply Data Perturbation method on 4th column by using the constant '5' for addition and constant '0.75' for multiplication.

Table 3: Example table of HDP

S.No	*Roll No*	*Name*	*Marks*	*Distorted Marks*
1	101	Rohan Raj	78	63
2	102	Shashank Raj	89	71
3	103	Prudvi Raj	92	77
4	104	Dhan Raj	82	69
5	105	Mythily Raj	80	68

2.5 The double-reflecting data perturbation method

The Double-Reflecting Data Perturbation Method denoted by DRDP shuffles all the elements in the same cluster of

values or all the values of the same attribute in the Data-Base Table by using the following formulas:

The distortion operation performed to the confidential attribute is given by

$o\rho_j = \rho_{Aj} + (\rho_{Aj - aj}) = 2\,\rho_{Aj - aj}.$

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 4: Example table of DRDP

S.No	Roll No	Name	Marks	Distorted Marks
1	101	Rohan Raj	78	92
2	102	Shashank Raj	89	81
3	103	Prudvi Raj	92	78
4	104	Dhan Raj	82	88
5	105	Mythily Raj	80	90

3. Proposed System

The proposed method is similar to symmetric encryption. In this method, no need to have shared secret key. But before starts communication, there is a need to send 7 **shared secret files** to the destination-side**.**

3.1 Encryption

Step 1: Be ready with the file which to be send to destination.

Step 2: Take 1st character from the file which is to be encrypt.

Step 3: Take 1st characters from all 7 shared secret files (mon, tue, wed, thu, fri, sat, sun).

Step 4: Now we have 8(1+7) characters. Apply Double-reflecting Data Perturbation Method on these 8 characters. Then it will produce a new character. The new character will be calculated in the following way:

If (character from file is either minimum or maximum) then new character = sum of minimum and maximum.

If (character from file is in between minimum and maximum) then new character = (sum of minimum and maximum)-(original character)

Step 5: Apply the same technique for remaining characters in the file.

Step 6: While encryption, when characters are not available in any one of the shared secret file then starts from first character in that file.

Step 7: Now every character has been replaced with some new character in the file which is to be sent to destination.

Step 8: Apply XOR operation on the resultant file and the corresponding file based on day of the week.

Step 9: Send the final copy to the destination.

3.2 Decryption

Step 1: The receiver should observe on which day of the week he received the file (eg: mon, tue, wed ..)

Step 2: Apply XOR operation on the received file and 'day of week' file (Eg: mon, tue, wed ….)

Step 3: Take 1st character from the received file.

Step 4: Take 1st character from all the shared secret files.

Step 5: Find the Minimum and Maximum in the list of 7 characters which are from all shared secret files.

Step 6: If Minimum is matched with Step 3 character then replace it with Maximum.

Step 7: If Maximum is matched with Step 3 character then replace it with Minimum.

Step 8: If Minimum and Maximum are not matched with Step 3 character then follow the below formula for decoding.

Original Character = (Minimum + Maximum)-(Step 3 Character)

Step 9: Apply the same method for the remaining characters.

Step 10: Now we will get original file.

Advantages:

4. Security Level

In 1st phase of proposed method, all the characters in the sentence are converted into UNICODE. Now those characters are shuffled according to their UNICODE 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:

$$A=\frac{VAR(A-A')}{VAR(A)}$$

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 [4].

5. Illustration

The file which to be encrypted:

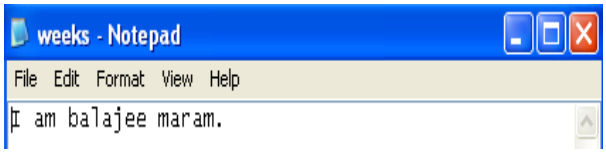


Figure 1: Original text file

The lists of shared secret files are as follows:

sun.txt, mon.txt, tue.txt, wed.txt, thu.txt, fri.txt, sat.txt

Figure 2: List of 7 files

5.1 Encryption

Step 1: Take 1st character from the file which is to be encrypted. Here the character is 'I'.

Step 2: Take 1st character from the shared-secret-files (sun.txt …. sat.txt). Those characters are 'S', 'M', 'T', 'W', 'T', 'F', 'S'.

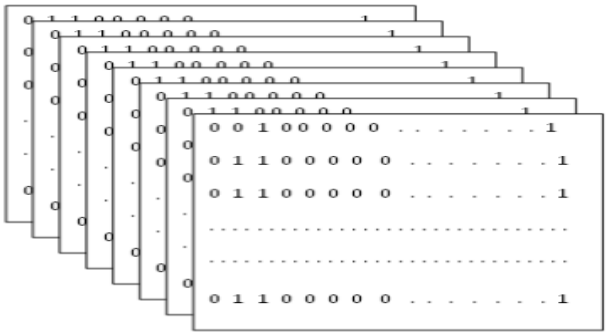


Figure 3: DRDP Method on list of files

Step 3: Apply DRDP method on those 8 characters ['I', 'S', 'M', 'T', 'W', 'T', 'F', 'S']

Step 4: Now apply the same procedure for all the characters in the file which is to be encrypted.

Step 5: After encryption, the encrypted file is in the following:

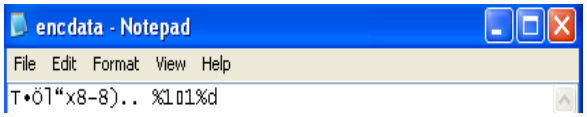
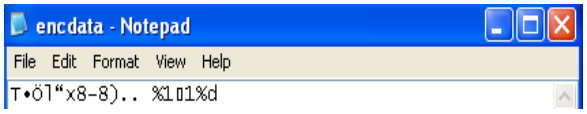


Figure 4: Encrypted file in sender-side

Step 6: Apply the XOR operation on the following two files i.e encrypted file and day of week file which is a shared secret file.



And

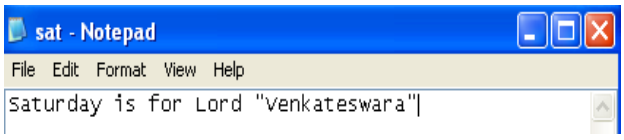


Figure 5: XOR operation on encrypted file & day of week file

Step 7: Now this file is to be sent to the destination.

5.2 Decryption

Step 1: The receiver should observe on which day of the week he received the file (eg: mon, tue, wed ..). For example

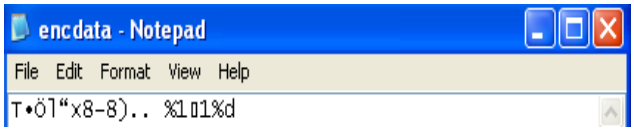
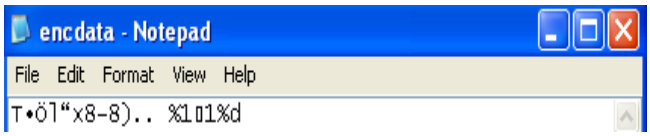


Figure 6: Received encrypted file in receiver-side

Step 2: Apply XOR operation on the received file and 'day of week' file (Eg: mon, tue, wed ….). For example



and

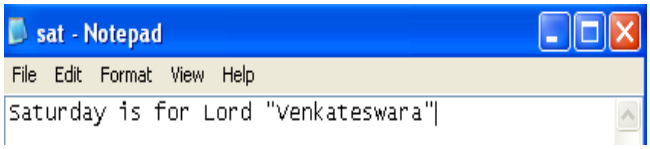


Figure 7: XOR op on encrypted and day-of-week files

Step 3: Take 1st character from the received file.

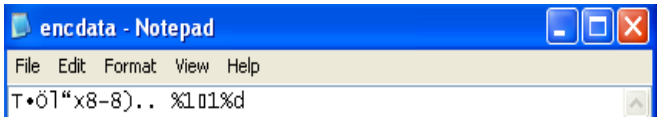


Figure 8: First char 'T' from encrypted file

Step 4: Take 1st character from all the shared secret files.

Figure 9: List of 7 files in receiver-side

Step 5: Find the Minimum and Maximum in the list of 7 characters which are from all shared secret files.

If (character from encrypted file is < (Minimum +maximum)) then new character = (character from encrypted file – maximum)

If (character from encrypted file is > (Minimum +maximum)) then new character = (character from encrypted file – minimum)

If (character from encrypted file is in between Minimum and maximum) then new character = ((minimum + maximum)-character from encrypted file)

Step 6: Apply the same method for the remaining characters.

Step 7: Now apply the XOR operation on the newly calculated file and day of week file i.e on which day it was received.

Step 8: Now we will get original file.

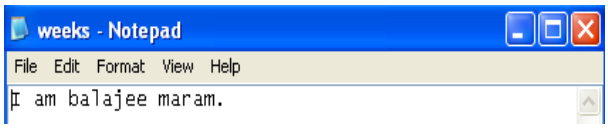


Figure 10: Original file in receiver-side

6. Practical Proof (Screen Shots)

6.1 Encryption

Step 1: The file which is to be encrypted.

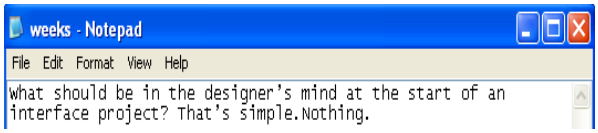


Figure 11: Original file in example 2

Step 2: After Encryption and XOR operation with concerted day of week file.

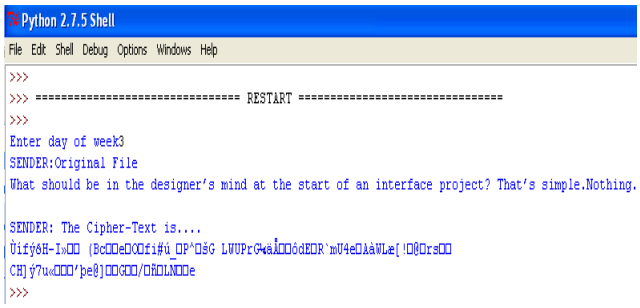


Figure 12: Screen-shot of encryption

6.2 Decryption

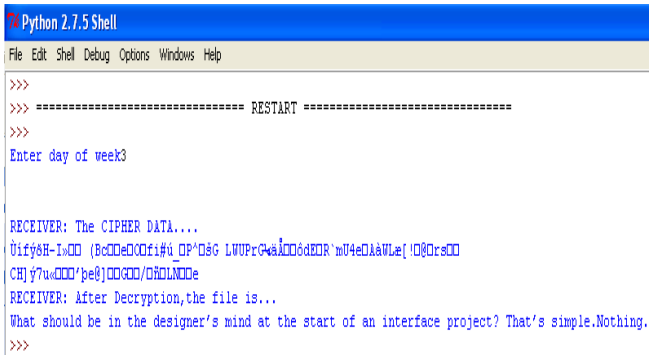


Figure 13: Screen-shot of decryption

7. Conclusion

Till the date, many algorithms have been introduced to market. Most of the algorithms are based on shared-secret-keys. Some algorithms are related to private/public key combination. Some more algorithms are based in Images. Among them, very few algorithms have been accepted by International Organizations and Reviewers. This proposed cryptographic algorithm is based on mathematical techniques only. This proposed algorithm would be enhanced with the help of UNICODE concept in near future. Then we will go for IMAGES.

References

[1]. B. Santhi, K.S. Ravichandran, A.P. Arun and L. Chakkarapani "A Novel Cryptographic Key Generation Method Using Image Features", Research Journal of Information Technology 4(2): 88-92, 2012, ISSN: 2041-3114.

[2]. Wang Jing, Wang Xiaogang, A New Clustering Algorithm of Preserving the Original Data's Privacy, 2008.

[3] Ali Inam, Selim. V. Kaya, Privacy preserving clustering on horizontally partitioned data, Data & Knowledge Engineering, vol.63, pp. 646-666, 2007.

[4] Maram Balajee, Challa Narasimham, "Double-reflecting Data Perturbation Method for Information Security", ISSN: 0974-6471 December 2012, Vol. 5, No. (2):Pgs. 283-288

Authors' Profile

Maram Balajee, working as an Sr. Asst. Prof in GMR Inst. Of Tech., Rajam, Andhra Pradesh, INDIA. Obtained his degrees in M.E (CSE) from Anna University, Chennai, MBA(GENERAL) & MA(MCJ) from Alagappa University, Karaikudi. Now he is pursuing P.hD(CS) Part-Time from Bharathiar University, Coimbatore, Tamil Nadu. He Published 14 research papers in International / National Journals / Conferences.

Dr. Challa Narasimham obtained Ph.D (Computer Science) in the year 2009, after completion of his MCA and MTech(IT) degrees. Currently, working as rofessor in S R Engg College (Autonomous) .Warangal, INDIA. He is having about 18 years of experience in industry & Teaching. He has published more than 30 papers in International / National Journals / Conferences.