ISSN 2395-1621

Magic rectangle generation algorithm scheme for client side authentication using session passwords and colors

[#1]Prasad kulkarni, [#2]Aparajita Lakhani, [#3]Kartikey Gupta, [#4]Aditya Bhosale, [#5]Dr.S.M.Chaware

[1]Prasadkulkarni787@gmail.com
[2]aparajitalakhani2@gmail.com
[3]Kartikey63@gmail.com
[4]bhosaleaditya000@gmail.com

[#12345]Department of Computer Engineering,BhivrabaiSawant College of Engineering,Narhe, Pune,India

ABSTRACT

Today we live in Information Era. Security is required to transfer information over the network. Textual-based password Authentication scheme is the traditional method for Authentication. Textual-based password Authentication scheme is vulnerable to attacks such as Shoulder surfing, Eves Dropping, Dictionary Attacks. To overcome this an innovative algorithm namely Magic Rectangle Generation Algorithm (MRGA) is being proposed. Due to its complexity in encryption process, it enhances security.

Keywords- Cryptography,RSA,Magic Rectangle Generating Algorithm, MagicRectangle,Public Key Cryptosystem.

ARTICLE INFO

Article History

Received :16th April 2016

Received in revised form :

19th April 2016

Accepted : 21st April 2016

Published online :

27th April 2016

I. INTRODUCTION

We have seen that over the past few years an increase in demanding of data communication over the internet. Due to data communication over the internet it's very important that data must be securely transmitted, means increase in security level. Therefore, secure transmission is done in the presence of the third-party, using cryptography .Cryptography is the science of secret writing. It is a technique to transfer information through unreadable format. There are two techniques through which we can transfer our data securely using symmetric and asymmetric key. Symmetric key cryptosystem is the method in which sender and receiver require the identical key that is used to encryption and decryption of the data or message. The main drawback is sender and receiver must exchange a key in a secure way. To overcome drawbacks public key cryptosystem is used. In this technique the public key is shared to everybody, but the private key is kept secret and thereby this eliminates the exchange of key in a secure way. But, if this private key is cracked or known by the third party. Then the message is decrypted easily. So to overcome this drawback of key generation we are using Magic Rectangle Generation Algorithm (MRGA).In MRGA algorithm it is very difficult to translation the message.

II. LITERATURE SURVEY

1) **In terms of Time:**
Public key cryptosystem is not based on number theory and is very fastcomparatively more secure then RSA algorithms [2] and is provides more security [2].

2) **In terms of Encryption:**
It provides two different keys namely private and public key in which public key is Used for encryption and private key which is unique is used for decryption purpose [3].

3) **In terms of RSA:**
Takes ASCII values for the characters to encrypt, preferably differentnumeralsrepresents the location of ASCII characters are taken from magic square and encryption is performed using RSA cryptosystem. [7]

4) **Key exchange Algorithm:**
Key exchange algorithm, apublickey encryptionalgorithm and a digital signature algorithm-combination of 3 algorithm is used to invert the function: F(x) = (a - x) Mod (2p) Div (2q) which is used for

encrypting text [2]. Private and public keyprivate key is used fordecryption (unique) and public key for Encryption (not Unique) [3]. Magic Square is used which constructs different doubly even magic square of order 16 as possible and each magic square corresponds to one ASCII set which is further use to encrypttext.[7]

5) **Limitations:**

1. Due to use of 3 different Algorithm it is very difficult to understand and design.
2. Using of private and public key concept indirectly increases Communication load.
3. Use of Magic Square algorithm is time consuming as it requires time to encrypt text.

III.PROPOSED METHODOLOGY

The proposed security model is described in the following steps.

- Construct singleeven magicrectanglehaving orderof 32x48 and used in list of ASCII table with 128 values. The Magic rectangle contains 1536 values. It has divided into12 quadrants, each consists of 128 characters.

Each character of the plain text is converted into numeric value based on its location in magic rectangle in different quadrants. The numeric valuesare then encrypted and decrypted using RSA algorithm.

The proposed system using new Authentication technique consists of 3 different phases: registration, login and verification phase respectively. During registration, user enters his password in first method &rates the colors in the second method. While logging in to the system, the user has to enter the password based on the graphical user interface Shown on the screen. The system verifies the password entered in comparison with content of the password generation during registration.

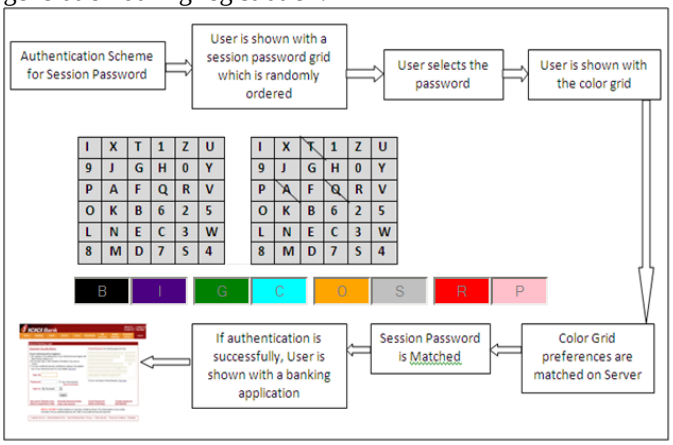


Figure 1. System Architecture

1. Pair-based Authentication scheme

During registration user submits password. Minimum length of the password is 8 and it can be called as secret pass. The secret password should contain even number of characters. Session passwords are generated based on this secret password during the login phase, when the user enters his username an interface consisting of a grid is shown. The grid is of size 6 x 6 and it consists of alphabets and numbers. These are randomly placed on the grid and the user interface changes every time.

User has to enter the password depending upon the secret pass. User considers his secret password in terms of pairs. The session password consists of alphabets and digits. The first letter in the pair first letter is used to select the row and the second letter is used to select the column. The intersection letter is the part of the session password. These steps are repeated for all pairs of secret pass. L is the intersection symbol for the pair "AN". The password entered by the user is verified by the security server to authenticate the user. If the password is correct, it allows to enter in to the system. The grid size can be increased to include special characters in the password.

Figure 2. Interaction letter for the pair AN

2. Hybrid Textual Authentication Scheme

During registration, user should rate colors as shown in figure 9. The User should rate colors from 1 to 8 and he can remember it as "BIGCROPS". Same rating can be given to different colors. During the login phase, when the user enters his username an interface is displayed based on the colors selected by the user. The login interface consists of grid of size 8×8. This grid contains digits 1-8 placed randomly in grid cells. The interface also contains strips of colors as shown. The color grid consists of 8 pairs of colors. Each pair of color represents the row and the column of the grid.

3. Registration

This module is used to registered user Details in three parts. They are Name authentication password, Color Priority Password and Other details. First, user is going to enter the normal password but it using capital A-Z letters and 0-9 Numbers. Second the user to put the color priority in eight colors.

Steps of execution of proposed system:

1. Authentication schema using session password.
2. User is shown with password grid.
3. User credential is converted into ASCII values.
4. Session password is matches.
5. Color Password entered.
6. Color Password is matched.
7. Authentication successful user is logged in.

ALGORITHMS

1) Magic Rectangle generating Algorithm

Input: 4 digit seed number, starting number and column sum of magic rectangle.

Output: Singly even magic rectangle **Method**:

Step 1:Read seednumber,Minstart, Maxstart value and Initial column sum

Step 2: compute the row sum and column sum
Step 3: Generate the magic rectangle
Step 4: If (seednumbers == 1)
Shift either row/column Else step
2.

2) RSA Encryption process

Input: Magic rectangle, plain Text, public key RSA algorithm

Output: cipher text **Method**:

Step 1: Read plain text.

Step2: Replace the plaintext with numeric value using MR

Step3: Encrypt using public key

Step 4: Produce the cipher text.

3) RSA Decryption Process

Input: Magic rectangle, cipher text, private key RSA algorithm

Output: Plain text **Method**:

Step1: Read cipher text.

Step 2: Decrypt using private key

Step 3: Replace the result with the position value of MR.

Step 4: Produce the plain text.

C. EXAMPLE

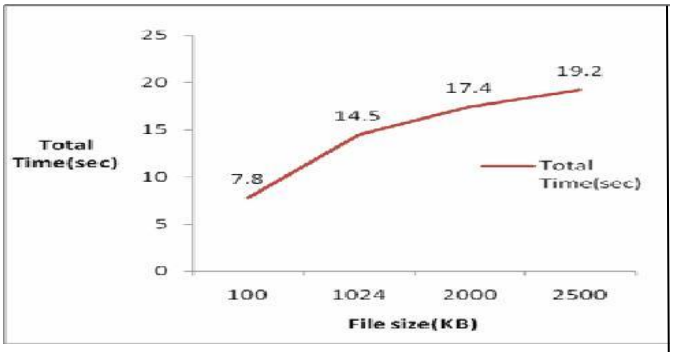
The given message is ―BABA.

Step 1: First, each and every character of the message is converted to the numerical value by using magic rectangle. The ASCII value of B‘,‘A‘,‘B‘,‘A‘ is 66,65,66 and 65 respectively.

Step 2: To encrypt B the value of the 66 position in the first Magic rectangle 16x24 is taken, then the value of the second and third characters are also taken from the same matrix.

Step 3: The character B and A is repeatedtwiceconsecutively in the plain text. The first occurrence of B value is taken from first matrix of order 16*24 and the second occurrence uses another matrix of the same size. So the value of the cipher text can't be repeated even if the character is repeated more than once.

IV. EXPECTED RESULT



IV. CONCLUSION

Proposed work (MRGA) introduces an additional level of security using singly even magic rectangle. By using this, any intruder may find it difficult to ascertain in theinformationbeing transmitted. It willbe helpful to increase the efficiency and security of the algorithm. One of the issues in the proposed work is additional time needed for the construction of magic rectangle.

V. FUTURE SCOPE

The basic idea of our system is to provide security. The aim of our system is to prevent Attacks such as dictionary attack and evesdropping. Time required for encryption and decryption is reduced and enhances more security. This security model can be further extended to provide security against other attacks.

VI. REFERENCES

[1]Dr.D.I.GeorgeAmalarethinam, J.SaiGeetha, Enhancing Security level for Public KeyCryptosystem using MRGA, 2014 World Congress on Computing and Communication Technologies, 978-1-4799-2876-7/13 $31.00 © 2013 IEEE DOI10.1109/WCCCT.2014.32.

[2] Samir Bouftass,on a new fast public key cryptosystem, July 20, 2015.

[3] Israt Jahan, Mohammad Asif, Liton JudeRozario,―ImprovedRSAcryptosystem based On the study of number theory and public key cryptosystems, American JournalofEngineering Research (AJER)-2015,e-ISSN:2320-0847 p-ISSN: 2320-0936Volume-4, Issue-1, pp-143-149.

[4]D.I.GeorgeAmalarethinam,J.SaiGeetha,K.Mani,―Add-on Security Level for Public Key Cryptosystem using Magic Rectangle with Column/Row Shifting, International Journal of Computer Applications (0975 -8887) Volume 96-No.14, June 2014 .

[5]Ravi Shankar dhakar, PrashantSharma, Amit KumarGupta, RSA Encryption Algorithm (REA), 2012 Second International Conference on Advanced Computing&CommunicationTechnologies,978-0-7695-4640-7/12$26.00 ©2012 IEEE,DOI.10.1109/ACCT.2012.74.

[6]MSREELATHA,M.SHASHI,MANIRUDH ,MD SULTAN AHAMER,VMANOJ KUMAR ,―Authentication Schemes for Session Passwords using Colour and Images, International Journal of Network Security & Its Applications (IJNSA),Vol.3, No.3, May 2011.

[[7] GopinanathGanapathy, and K. Mani,‖ Add-On Security Model for Public-Key Cryptosystem Based on Magic Square Implementation‖, Proceedings of the World Congress on Engineering and Computer Science 2009 Vol IWCECS 2009,October 20-22, 2009, San Francisco, USA.

