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

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

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

#12345Department 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.

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 fast comparatively more secure than 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 different numerals represents 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, a public key encryption algorithm 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 key private key is used for decryption (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 encrypt text.[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 single even magic rectangle having order of 32x48 and used in list of ASCII table with 128 values. The Magic rectangle contains 1536 values. It has divided into 12 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 value are 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.

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.

Step 2: Replace the plaintext with numeric value using MR

Step 3: 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:

Step 1: 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 repeated twice consecutively in the plain text. The first occurrence of B value is taken from the 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 the information being transmitted. It will be 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 eavesdropping. 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


