Abstract

In today's world, security is required to transmit confidential information over the network. Security is also demanded in wide range of applications. Cryptographic algorithms play an important role in providing the data security against malicious attacks. The efficiency of cryptographic algorithm is not only based on its time taken for encryption and decryption, and it also accounts for number of stages used to obtain the cipher text from a plain text. Rivest-Shamir-Adleman (RSA) algorithm is a popular encryption scheme that guarantees confidentiality and authenticity over an insecure communication channel. However, several attacks are introduced to break the security of these algorithms due to certain constraints. Also, it may not be guaranteed that the cipher text is fully secured. One such limitation in the past crypto system is using ASCII Characters for numerical representation of the selected text. To overcome the above said issue, an innovative algorithm, namely, Magic Rectangle is being proposed in this work. It is helpful to enhance the security on account of its complexity of the encryption process. The singly even magic rectangle is constructed based on the seed number, start number, row sum and column sum. It is very difficult to trace these values because of their randomness. After construction of the rectangle, the columns / rows of resultant rectangle are
Add-on Security Level for Public Key Cryptosystem using Magic Rectangle with Column/Row Shifting

shifted based on the seed value. The proposed work introduces additional level of security in public key algorithms such as RSA, ECC and Rabin, Elgamal etc. Finally, Magic Rectangle helps to rectify the existing issues of public key cryptosystem. Cipher text generated by using the proposed method can be completely different when compared to the plain text and will be suitable for the secured communication through the internet. Since this model is acting as a wrapper to public key algorithm, it confirms that the network security is reasonably improved.

References

- Sonal Sharma, Saroj Hiranwal, Prashant Sharma A new variant of subset-sum cryptosystem over RSA, International Journal of Advances in Engineering & Technology, Jan 2012. @IJAET ISSN: 2231-1963
- Ravi Shankar Dhakar, Amit Kuar Gupta, Prashant Sharma Modified RSA Encryption Algorithm (MREA); 978-0-7695-4640-7/12, IEEE2012
- en.wikipedia.org/wiki/Golden_rectangle
- Omotheinwa T. O, Ramon S. O., Fibonacci Numbers and Golden Ratio in Mathematics and Science, International Journal of Computer and Information Technology (ISSN&qurot;2279-0764) Volume 03-Issue 04, July 2013
Add-on Security Level for Public Key Cryptosystem using Magic Rectangle with Column/Row Shifting

- Ashish Agarwala R Saravanan, &quot;A Public Key Cryptosystem Based on Number Theory&quot;; 978-1-4673-0255-5/12, IEEE 2012.

Index Terms

Computer Science  Security

Keywords

Magic Rectangle  Column/Row shifting  Public Key Cryptosystem  RSA  Security

Public key

Secret Key

MR