In the present paper the authors have introduced a new updated two-way generalized vernam cipher method called TTSJA. Chatterjee et. al developed a method [1] where they used three independent methods such as MSA [2], NJJSAA [3] and modified generalized vernam cipher method. Nath et al already developed some symmetric key methods [2,3,4,5] where they have used bit manipulation method and some randomized key matrix for encryption and decryption purpose. In the present work the authors have used updated generalized vernam cipher method in two directions. One from first character to last character and then we perform vernam method with XOR operation from last to first We found the results are quite satisfactory even for short message and repeated characters also. The advantage of the present method is that the overhead is minimum but the encryption is very hard. This method may be applied to encrypt short message such as SMS, password, ATM code etc. In the present work the authors
have introduced updated Vernam Cipher method. The authors modified the standard Vernam Cipher method for all characters (ASCII code 0-255) with randomized keypad and also introduced feedback. After first phase encryption the modified vernam cipher method applied from last character to the first using random keypad and feedback. In the second phase instead of adding the keypad ASCII the authors performed the XOR with keypad and the encrypted text (after first phase). This method closely monitored on different known plain text and it was found that this method is almost unbreakable. The present method allows the multiple encryption and multiple decryption. To initiate the encryption process a user has to enter a text-key which may be maximum of 16 characters long. From the text-key the randomization number and the encryption number is calculated using a method proposed by Nath et al [2]. A minor change in the text-key will change the randomization number and the encryption number quite a lot. The present method is a block cipher method and it can be applied to encrypt confidential data in Defense system, Banking sector, mobile network, Short message Service, Password, ATM key etc. The advantage of the present method is that one can apply this method on top of any other standard algorithm such as MSA, DJSA, NJJSAA, TTJSA, DJMNA etc [2,4,3,1,5]. The method is suitable to encrypt any type of file.

References

- Symmetric key Cryptography using modified DJSSA symmetric key algorithm, Dripto Chatterjee, Joysheer Nath, Sankar Das, Shalabh Agarwal and Asoke Nath, WORLDCOMP-2011 held at Las Vegas,USA 18-21 Jul 2011
- Modified Version of Playfair Cipher using Linear Feedback Shift Register, P. Murali and
Symmetric key Cryptography using two-way updated -Generalized Vernam Cipher method: TTSJA algorithm


Index Terms

Computer Science

Security

Keywords

Msa Algorithm  Njjsaa  Ttjsa  Djmna  Vernam Cipher Method