Abstract

This paper proposes to put forward an innovative algorithm for symmetric key block cipher named as “Triple Prime Symmetric Key Block Cipher with Variable Key-Spaces (TPSKBCVK)” that employs triple prime integers as private key-spaces of varying lengths to encrypt data files. Principles of modular arithmetic have been elegantly used in the proposed idea of the cipher. Depending on observations of the results of implementation of the proposed cipher on a set of real data files of several types, all results are registered and analyzed. The strength of the underlying design of the cipher and the liberty of using a long key-space expectedly makes it reasonably non-susceptible against possible cryptanalytic intrusions. As a future scope of the work, it is intended to formulate and employ an improved scheme that will use a carrier media (image or multimedia data file) for a secure transmission of the private keys.

References

- James J. Tattersall – “Elementary Number Theory in Nine Chapters”, Cambridge
Introduction of a Triple Prime Symmetric Key Block Cipher

University Press.
- Menezes, P. van Oorschot, and S. Vanstone – “Handbook of Applied Cryptography “, CRC Press, 1996.
- Bruce Schneier - “Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C”, Publisher: John Wiley & Sons, Inc.
- Clay S. Turner, Euler's Totient Function and Public Key Cryptography - http://web.cs.du.edu/~ramki/courses/security/2011Winter/notes/RSAmath.pdf.
- MIRACL Library web link: - http://www.shamus.ie
- Saurabh Dutta - An Approach to Design New Efficient Encryption Techniques, ISBN: 978-3-8443-0082-6, Lap Lambert Academic Publishing, Germany.
- William Stallings – “Cryptography and Network Security Principles and Practices, Fourth Edition”, Prentice Hall

Index Terms

Computer Science
Security

Keywords
Data Security Cryptography Prime Number Block Cipher