{tag}

{/tag}

International Journal of Computer Applications

Volume 50 - Number 5

Year of Publication: 2012

Authors:

Sukalyan Som

Moumita Som

10.5120/7771-0853

{bibtex}pxc3880853.bib{/bibtex}

Abstract

A symmetric key cryptographic system has been proposed and it is termed as DSWLT. This proposed technique is very fast, suitable for encryption of large files. DSWLT consider the plain text (i. e. the input file) as binary string with finite no of bits. The input string converted to DNA nucleotides using DNA coding and then the DNA codes are converted to positive integers. Laplace transform is applied considering these numbers to be the co-efficient of the expansion. To provide multilevel security the resultant coefficients are converted to their binary equivalent and another level of encryption with cumulative XOR is performed and respective MSBs found at every iteration are taken to construct the cipher text. Decryption is performed in the reverse manner. Experimental results are tested, analyzed and a comparison with existing and industrially accepted TDES and AES has been performed.

References

- J. D. Watson, F. H. C. Crick, "A structure for deoxy ribose nucleic acid", Nature, vol. 25, pp. 737-738, 1953.
- G. Z. Cui, L. M. Qin, Y. F Wang and X. C. Zhang, "Information Security

Technology Based on DNA Computing", IEEE International Workshop on Anti counterfeiting Security, pp. 288–291, 2007

- G. Z. Cui, "New Direction of Data Storage: DNA Molecular Storage Technology," Computer Engineering and Applications, vol. 42, pp. 29–32, 2006.
- Xing Wang, Qiang Zhang ,"DNA computing-based cryptography", Fourth International Conference on Bio-Inspired Computing, 2009.
- L. M. Adleman, "Molecular computation of solution to combinatorial problems", Science, vol. 266, pp. 1021-1024, November 1994.
- C. Taylor, V. Risca, and C. Bancroft, "Hiding messages in DNA microdots", Nature, vol. 399, pp. 533-534, 1999.
- R. J. Lipton," Using DNA to Solve NP-Complete problems," Science, vol. 268, pp. 542 545, 1995.
- G. Z. Cui, "New Direction of Data Storage: DNA Molecular Storage Technology," Computer Engineering and Applications, vol. 42, pp. 29–32, 2006.
- Sherif T. Amin, Magdy Saeb, Salah El-Gindi, "A DNA based Implementation of YAEA Encryption Algorithm," IASTED International Conference on Computational Intelligence,2006
- Pankaj Rakheja, "Integrating DNA Computing in International Data Encryption Algorithm (IDEA)", International Journal of Computer Applications, pp 1 – 6, Volume 26, No. 3, July 2011
- Murray R Spiegel, "Schaum's Outline of Laplace Transforms", Mcgraw-hill, 1965
- "Triple Data Encryption Standard" FIPS PUB 46-3 Federal Information Processing Standards Publication, Reaffirmed, 1999 October 25 U. S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology.
- "Advanced Encryption Standard", Federal Information Processing Standards Publication 197, November 26, 2001.
- Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, Elaine Barker, Stefan Leigh, Mark Levenson, Mark Vangel, David Banks, Alan Heckert, James Dray, San Vo, "A statistical Test Suite for Random and pseudorandom Number Generators for Cryptographic Applications", April 2010, National Institute of Standards and Technology.

Index Terms

Computer Science Applied Sciences

Keywords

DNA DNA Cryptography Laplace Transform Symmetric key Cryptography Cumulative XOR

Most Significant Bit

Serial Test

Monobit Test

Frequency Test