Merging of Vigenère Cipher with XTEA Block Cipher to Encryption Digital Documents

International Journal of Computer Applications
Foundation of Computer Science (FCS), NY, USA

Volume 132
Number 1

Year of Publication: 2015

Authors:
Fathir Maruf, Imam Riadi, Yudi Prayudi

10.5120/ijca2015907262
{bibtex}2015907262.bib{/bibtex}

Abstract

Security and confidentiality of documents or information has become a very important concern, in this modern era of computing speed increases dramatically, certainly considered threatening for some algorithms that are used to secure documents or information, it spawned an option to increase the security of documents by combining two cryptographic algorithms are Vigenère cipher with XTEA. Selection Vigenère cipher because it is not so vulnerable to solving method code is called frequency analysis, but some cryptanalyst has found security flaws of this algorithm, for it Vigenère cipher in this research carried out modifications to operations of mathematics, the results of these modifications will be combined with the algorithm-based XTEA block cipher, because his strength has been proven to secure the document (text). Based on the results of research conducted, the merger of the two algorithms are (VixTEA) can improve the security of ciphertext, it is measured by various indicators, namely, a visual comparison of encryption (frequency analysis), entropy value analysis, and analysis of bruteforce attacks. The results also showed that the VixTEA concept does not change the performance of the algorithm and the integrity of the digital documents can secured.
References


Index Terms

Computer Science  Security

Keywords
Vigenère cipher, XTEA, Block cipher, VixTEA, Digital documents.