International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR)
ISSN(P): 2249-6831; ISSN(E): 2249-7943
Vol. 4, Issue 2, Apr 2014, 275-286

DUAL CONGRUENT INTEGER CRYPTOGRAPHIC ALGORITHM TO SECURE SENSITIVE INFORMATION TRANSIENT

YAHIA S. AL-HALABI

Professor, Princess Sumaya University for Technology, Amman, Jordan,

ABSTRACT

Cryptography is one of the most important tools that provide hiding data and information security usually done through mathematical manipulation of the data with an incomprehensible format for unauthorized users. It has long been used by government, public and private companies and militaries too to facilitate secret communication. Mainly, it is commonly used within many kinds of civilian systems in protecting information. Building and creating a key that would prevent an unauthorized decryption of message is the challenging part of cryptography. This paper aimed at providing algorithms to secure sensitive information transit via unsecure channels from the hands of the Internet criminals by scrambling the sensitive information using consecutive mathematical-based algorithm which performs dual ciphered and re-ciphered operation (Dual encryption), then dual decryption and re-decryption, by principles of congruent, for both consecutive encryption and decryption schemes (Dual decryption). Additionally, the use of basic mathematical characteristics of integer numbers generators applied in both steps in dual encryption and dual decryption which are the novel of our project.

The suggested algorithm was tested with samples of real data and the result practically demonstrated how dual schemes are indeed of relevance in providing strong and complex decryption keys to protect sensitive information. The dual consecutive schemes proved that more illegal trials attempted, the more difficult it is for the criminals or hackers to unveil the sensitive information. The results of this algorithm shows that discourage the criminals will be based on the complexity of the dual encryption and decryption key. This paper is part of a commercial big project considered as a first step to be extended to use finally randomized integers during encryption process which will never be predicted and will be applied as a first step by using different distinct or random process during encryption and decryption processes.

KEYWORDS: Cryptographic Algorithms, Cryptology, Cryptanalyst, Decryption, Encryption, Cipher, Protocol, Data Security.