

# DES Enhancement Using Key-Based Randomized Initial Permutation

Shakir M. Hussain<sup>1</sup> and Hussein Al-Bahadili<sup>2</sup>

<sup>1</sup>Faculty of IT, Applied Science University, Amman, Jordan

<sup>2</sup> Faculty of IT and Systems, Arab Academy for Banking and Financial Sciences, Amman, Jordan

**Abstract** - *This paper introduces a new method to enhance the performance of the Standard Data Encryption Standard (DES), or any permutation dependent encryption algorithms, by increasing the brute-force attack time complexity by a factor of  $64!$ . The new algorithm is referred to as Enhanced DES (EDES). This is done by replacing the predefined initial permutations (IP) and its inverse ( $IP^{-1}$ ) that are used in the standard DES design with key-based permutations. The new permutations are derived using the Key-Based Random Permutation (KBRP) method. These permutations are derived by using the same cipher key that is used in the standard DES. Therefore, these permutations will not be fixed and can be considered as pseudorandom permutations. The performance of the new EDES algorithm is examined in term of the features of the generated ciphertext and processing time.*

**Keywords:** DES; Block cipher; Random Permutation; Key-Based Random Permutation (KBRP) method; Randomness test; Brute-force attack.

WORLDCOMP08 USA 2008