

Title: A Password-Based Key Derivation Algorithm Using the KBRP Method

Author: Shakir M. Hussain and Hussein Al-Bahadili

Source: American Journal of Applied Sciences 5(7): 777-782 , 2008

Abstract: This study presents a new efficient password-based strong key derivation algorithm using a key based random permutation the KBRP method. The algorithm consists of five steps, three steps are similar to those formed the KBRP method. The last two steps are added to derive a key and to ensure that the derived key has all the characteristics of a strong key. In order to demonstrate the efficiency of the algorithm, a number of keys are derived using various passwords of different content and length. The features of the derived keys show a good agreement with all characteristics of strong keys. In addition, they are compared with the features of keys generated using the WLAN strong key generator v2.2 by Warewolf L.