

A Password-Based Key Derivation Algorithm Using the KBRP Method

¹Shakir M. Hussain and ²Hussein Al-Bahadili

¹Faculty of CSIT, Applied Science University, P.O. Box 22, Amman 11931, Jordan

²Faculty of Information Systems and Technology,
Arab Academy for Banking and Financial Sciences, P.O. Box 13190, Amman 11942, Jordan

Abstract: This study presents a new efficient password-based strong key derivation algorithm using the key based random permutation the KBRP method. The algorithm consists of five steps, the first 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 features of keys generated using the WLAN strong key generator v2.2 by Warewolf Labs.

Key words: Key derivation, key generation, strong key, random permutation, Key Based Random Permutation (KBRP), key authentication, password authentication, key exchange
