

Key Based Random Permutation (KBRP)

Shakir M. Hussain¹ and Naim M. Ajlouni

¹ Applied Science University Jordan
Amman Arab University for Graduate Studies, Jordan

Abstract: This study introduces a method for generating a particular permutation P of a given size N out of $N!$ permutations from a given key. This method computes a unique permutation for a specific size since it takes the same key; therefore, the same permutation can be computed each time the same key and size are applied. The name of random permutation comes from the fact that the probability of getting this permutation is 1 out of $N!$ possible permutations. Besides that, the permutation cannot be guessed because of its generating method that is depending completely on a given key and size.

Key words: Random permutation, indexing, block cipher, hashing