World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:9, No:04, 2015

Deterministic Random Number Generator Algorithm for Cryptosystem Keys

Authors : Adi A. Maaita, Hamza A. A. Al Sewadi

Abstract : One of the crucial parameters of digital cryptographic systems is the selection of the keys used and their distribution. The randomness of the keys has a strong impact on the system's security strength being difficult to be predicted, guessed, reproduced or discovered by a cryptanalyst. Therefore, adequate key randomness generation is still sought for the benefit of stronger cryptosystems. This paper suggests an algorithm designed to generate and test pseudo random number sequences intended for cryptographic applications. This algorithm is based on mathematically manipulating a publically agreed upon information between sender and receiver over a public channel. This information is used as a seed for performing some mathematical functions in order to generate a sequence of pseudorandom numbers that will be used for encryption/decryption purposes. This manipulation involves permutations and substitutions that fulfills Shannon's principle of "confusion and diffusion". ASCII code characters wereutilized in the generation process instead of using bit strings initially, which adds more flexibility in testing different seed values. Finally, the obtained results would indicate sound difficulty of guessing keys by attackers.

Keywords : cryptosystems, information security agreement, key distribution, random numbers
Conference Title : ICISAI 2015 : International Conference on Information Security and Artificial Intelligence
Conference Location : Venice, Italy
Conference Dates : April 13-14, 2015