

Pseudorandom generators belong to the primary focus of cryptology. The key to every cipher has to be generated at random, otherwise the security of the whole cipher is threatened. Another point of importance is the pseudorandom generators' close relationship to the stream ciphers. In this work, we first introduce statistical theory related to randomness testing. Then, we describe 8 classical statistical tests. We introduce a concept of next bit testing and derive variants of previous tests. Moreover, with this new battery of tests we examine the randomness of SHA-3 second round candidates and present the results. Also a sensitivity of tests is investigated and several useful transformations are shown.