

Pseudonáhodné generátory jsou jedním z nejdůležitějších témat kryptologie. Ke každé šifře musí být klíč generován náhodně, jinak můžeme ohrozit bezpečnost celé šifry. Dalším důvodem důležitosti pseudonáhodných generátorů je jejich úzký vztah k proudovým šifrám. V předložené práci nejdříve zformulujeme základní poznatky z matematické statistiky potřebné k testování náhodnosti. Popíšeme 8 klasických statistických testů. Představíme nový způsob předpovídání dalších bitů a ukážeme variaty dříve popsaných testů. S touto baterií testů otestujeme kandidáty na SHA-3, kteří se dostali do druhého kola. Dále je zde studován pojem senzitivity testů a jsou navrženy nové transformace.