Abstrakt:

V předložené práci se zabýváme testy generátorů pseudonáhodných bitů. Generátory pseudonáhodných bitů jsou jedním z nejdůležitějších kryptografických nástrojů. V první části této práce uvádíme základní definice a tvrzení z teorie pravděpodobnosti a statistiky potřebné k testování náhodnosti. Dále uvedeme některé základní pojmy a fakta z kryptografie. V druhé části této práce popíšeme deset různých statistických testů a jejich modifikace. Také uvádíme výsledky testů provedených na proudové šifře Decim, Geffe generátoru a Blum Blum Shub generátoru.