Valutazione di generatori pseudocasuali

Un generatore per uso non crittografico deve superare dei test statistici che garantiscono che le sequenze prodotte siano simili a sequenze effettivamente casuali:

frequenza approssimativamente uguale per 0 e 1;

poker test sottosequenze di lunghezza uguale devono presentarsi con stessa frequenza;

autocorrelazione a distanze prefissate non deve ripetersi lo stesso bit;

run test frequenza di sottosequenze con stesso bit ripetuto n volte deve diminuire esponenzialmente con n.

Per le applicazioni crittografiche richiediamo il *test di prossimo bit*, ovvero non deve esistere un algoritmo *polinomiale* in grado di prevedere con probabilità $> 1/2$ l'$i+1$-esimo bit generato conoscendo gli i bit precedenti. Un generatore che supera questo test supera anche gli altri 4, ed è detto *crittograficamente sicuro*.