

Tato diplomová práce zkoumá teoretické a praktické aspekty kryptograficky bezpečných generátorů pseudonáhodných čísel (CSPRNG) v moderní kryptografii a počítačové bezpečnosti. Studie se ponoří do teoretického zázemí, konstrukce, bezpečnostních opatření a praktických implementací CSPRNG, přičemž zdůrazňuje jejich význam v zabezpečených komunikačních kanálech a kryptografických protokolech. Prostřednictvím rozsáhlého přehledu literatury tato práce zdůrazňuje výzvy při dosahování absolutní bezpečnosti pro generátory pseudonáhodných čísel a prokazuje, že mohou být konstruovány z jednodušších funkcí a významně rozšířeny při zachování zabezpečení.

Tato práce také zkoumá různé známé algoritmy CSPRNG jako Yarrow, Fortuna, ChaCha20, ISAAC, ANSI X9.17 a další. Bezpečnostní prvky a známá zranitelnost jsou identifikována z dostupných literárních zdrojů. Praktické útoky na tyto generátory, včetně kompromitace stavu, útoků se zvoleným vstupem a zpětného sledování, jsou analyzovány, aby se zdůraznila důležitost robustního návrhu a proaktivních bezpečnostních opatření.

Studie navíc představuje praktické implementace nezabezpečených algoritmů v programovacích prostředích, ukazuje jejich aplikaci a potenciální slabiny v reálných scénářích, přičemž zdůrazňuje, že pro praktické implementace by měly být používány pouze ověřené prostředky. Analýzou historických a současných útoků výzkum podtrhuje nezbytnost neustálého vylepšování návrhů PRNG pro ochranu proti vyvíjejícím se hrozbám.