The thesis explores the theoretical and practical aspects of Cryptographically Secure Pseudorandom Number Generators (CSPRNGs) in modern cryptography and computer security. The study delves into theoretical background, the construction, security measures, and practical implementations of CSPRNGs, emphasizing their importance in secure communication channels and cryptographic protocols. Through an extensive literature review, this work highlights the challenges in achieving absolute security for pseudorandom number generators, establishing that they can be constructed from one-way functions and significantly expanded while maintaining security, provided.

The thesis also examines various well-known CSPRNG algorithms such as Yarrow, Fortuna, ChaCha20, ISAAC, ANSI X9.17, and others. The security features and known vulnerabilities are identified from available literary sources. Practical attacks on these generators, including state compromise, chosen-input attacks, and backtracking, are analyzed to underscore the importance of robust design and proactive security measures.

Moreover, the study presents practical implementations of unsecure algorithms in programming environments, showcasing their application and potential weaknesses in real-world scenarios, emphasizing that only verified means should be used for practical implementations. By analyzing historical and contemporary attacks, the research underscores the necessity for continuous improvements in PRNG designs to safeguard against evolving threats.