Povzetek. Delo vključuje tri področja matematične znanosti, ki so potrebna za razumevanje preverjanja naključnosti generatorjev naključnih zaporedij bitov. To so: kriptografija, verjetnostni račun in statistika. Delo najprej opiše, kako lahko zgeneriramo psevdonaključno zaporedje bitov z lepimi statističnimi lastnostmi (LFSR generator) in na kakšen način ga potem lahko uporabimo v kriptografiji. Nato predstavi osnovno znanje verjetnostnega računa in statistike, ki je potrebno za razumevanje ne le rezultatov, ampak tudi lastnosti posameznih statističnih testov, ki so opisani v četrtem poglavju. To so testi psevdonaključnih generatorjev bitov, ki poleg osnovnih statističnih lastnosti, ki naj bi jih imelo izhodno zaporedje generatorja, preverjajo tudi, ali je iz tega psevdonaključnega zaporedja možna rekonstrukcija semena.

Abstract. This dissertation includes three fields of mathematical science, which are needed to understand random bit generators' randomness testing. These are: cryptography, probability theory and mathematical statistics. In the beginning, this paper describes how to generate pseudorandom bit sequence with good statistical properties (LFSR generator) and how to use it in cryptography. Next, it presents the basic knowledge of probability theory and statistics, which is needed to understand not only the results, but also properties of statistical tests, which are described in the fourth chapter. These pseudorandom bit generators' tests verify basic statistical properties, which an output sequence generator should have, as well as establish the possibility of seed reconstruction from this pseuderandom sequence.

Math. Subj. Class. (2000): 60F05, 6204, 62G10, 68P25, 94A24, 94A55, 94A60

Ključne besede: kriptografija, varnost, razbijanje kriptosistemov, napadi, tokovni tajnopis, psevdonaključno, naključno zaporedje bitov, LFSR, Diehard, Crypt-X, verjetnostni račun, matematična statistika, statistični test, neparametrični testi, hi kvadrat test, test Kolmogorova.

Key words: cryptography, security, cryptoanalysis, attacks, stream cyphers, pseudorandom, random bit sequence, LFSR, Diehard, Crypt-X, probabylity theory, mathematical statistics, statistical test, nonparametric tests, chi square test, Kolmogorovs' test.

Literatura

[1] T. W. Anderson, D. A. Darling, *Asimptotic theory of certain "goodness of fit" criteria based on stohastic processes*, Annals of Mathematical Statistics, **23** (1952), 193–212.

[2] H. Beker, F. Piper, *Cypher Systems: The Protection of Comunications*, Northwood Publications, London, 1982.

[3] P. Billingsley, *Probability and measure, 2nd ed.*, John Wiley, New York, 1986.

[4] R. Durrett, *Probability: theory and examples, 2nd ed.*, Duxbury Press, Belmont, 1996.

[5] M. Fisz, *Probability Theory and Mathematical Statistics*, PWN, Polish Scientific Publishers, New York, 1967.

[6] G. R. Grimmett, D. R. Stirzaker, *Probability and Random Processes*, Clarendon Press, Oxford, 1992.

[7] P. Jakopin, *Zgornja meja entropije pri leposlovnih besedilih v slovenskem jeziku: doktorska disertacija*, samozaložba, Ljubljana, 1999.
`http://valjhun.fmf.uni-lj.si/~ajurisic/tecaj1/entropija.txt`

[8] R. Jamnik, *Matematična statistika*, Državna založba Slovenije, Ljubljana, 1980.

[9] R. Jamnik, *Verjetnostni račun*, Mladinska knjiga, Ljubljana, 1971.

[10] J. F. C. Kingman, S. J. Taylor, *Introduction to measure and probability*, Cambridge University Press, Cambridge, 1966.

[11] D. E. Knuth, *The Art of Computer Programming, Vol. 2: Seminumerical Algorithms*, Addison-Wesley Publishing Company, 1969. B. Košmelj, *Statistični terminološki slovar*, Statistično društvo Slovenije: Društvo matematikov, fizikov in astronomov Slovenije, Ljubljana, 1993.

[12] Susan Landau, *Communications Security for the Twenty-first Century: The Advanced Encryption Standard*, Notices of the AMS, **47** (2000), 450–459.

[13] G. Marsaglia, *A Current View of Random Number Generators*, Proceedings of the Sixteenth Symposium on the Interface (Atlanta, Georgia, March 1984), Computer Science and Statistics, Elsevier Science Publishers, New York, 1985, str. 3–10.
`http://www.evensen.org/marsaglia/`
Pseudo random number generators and stringent tests for randomness (keynote.ps)

[14] G. Marsaglia, *Monkey Tests for Random Number Generators*, Computers & Mathematics with Applications, **9** (1993), 1–10.
`http://www.evensen.org/marsaglia/`

[15] A. J. Menezes, P. C. Van Oorschot, S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press LLC, 1997.

[16] W. Rudin, *Real and complex analysis, 3rd ed.*, McGraw-Hill, New York, 1987.

[17] M. J. Schervish, *Theory of Statistics*, Springer-Verlag, New York, 1995.

[18] D. R. Stinson, *Cryptography: Theory and Practice*, CRC Press, 1995.

Internet, navodila za uporabo programov, ...

[19] Navodila za uporabo Crypt-XS testa:
W. Caelli, E. Dawson, H. Gustafson, L. Nielsen, *Crypt - XS, Statistical package manual for stream ciphers*, Queensland university of technology, Information security research centre and School of mathematics, 1994.
`http://www.isrc.qut.edu.au/cryptx/`

[20] Razlage Diehard testov, ki jih izpiše program:
`http://www.stata.com/support/cert/diehard/randnumb.out`

[21] Programski paket Diehard:
`http://stat.fsu.edu/~geo/diehard.html`