Cryptography: course for master's degree in EDGE COMPUTING

LABORATORY: Randomness

1. Find out how two random generators work in the linux environment - **/dev/random** and **/dev/urandom.**
2. Which one is truly random and which one is pseudo-random?
3. Read about the operation of the **ent** program to study randomness.
4. Generate sample random strings and report them by assessment **ent** program.
5. Using the **ent** program, evaluate the randomness of a file that does not contain random data.
6. Read about how to use the **NIST** test for randomness program (section 5.6 Running the Test Code from manual).
7. Using the random generator from point 1, generate a test data file, which you will then analyze with **NIST** tests.
8. Where the results for each test are stored?
9. Why can't some of the tests be taken?
10. Report the test results for the analyzed file.
11. Explain in written form in the report of the exercises done how the results of the NIST tests presented in the form as in Figure 5-1 in the NIST manual should be interpreted.
12. Create a file with data that is not random. Have the file analyzed by NIST tests. Present the results in a report.