Cryptography

Lab no. 1 – till 11 III 2018

You can get max 10 points for this list.

Problem 1 (5 pts.) Construct an algorithm which predicts next bits of *linear congruencial generator*, use this algorithm to construct a distinguisher (statistical test) which can distinguish output generated by an instance of LCG from a random string.

Problem 2 (5 pts.) Your goal is the same as in Problem 1, but here, the generator is *glibc*'s random().

Problem 3 (5 pts.) Implement an attack on a modified version of A5/1 where in each round all LFSRs are moving.

Problem 4 (10 pts.) Design and implement a ciphertext-only attack on a modified version of A5/1 where:

- in each round all LFSRs are moving,
- the ouptut is a XOR of the first and the second LFSR,
- the output is computed only if the output of the third LFSR is equal to 1.

Problem 5 (10 pts.) Implement an attack on a shrinking generator.