Cryptography

Lab no. 3 – till 29 III 2013

You can get max 10 points for this list. Test data will be provided soon.

Assignment 1 (5 pts.) Construct and implement an efficient statistical test that predicts (with non-negligible probability) next bits of *linear congruencial generator*.

Assignment 2 (5 pts.) Construct and implement an efficient statistical test that predicts (with non-negligible probability) next bits of *glibc*'s random().

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

Assignment 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.

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