Cryptography

Programming 2 – till 22 III 2013

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

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