LELEC 2770 - Session 7 - Post-Snowden Cryptography

1 Dual-EC backdoor

In this exercise, you will implement a backdoored Dual EC PRNG and attack it. Complete the provided code in `dual_ec.py`. The code depends on the `fastecdsa` python package (`pip install --user fastecdsa`, you will probably need gmp.h header as well (in libgmp-dev in debian)). The way Dual EC works, and how it can be backdoored is explained in [1], Sections 5.1, 5.2 and 5.3. (Sections 1, 2, 3 and 4 are and interesting easy reading about how a cryptography standardization process can fail.)

[1] D. J. Bernstein, T. Lange, and R. Niederhagen. Dual EC: A standardized back door. `https://eprint.iacr.org/2015/767`