Workshop Maputo

Testing

Marek Sýs
syso@mail.muni.cz, Masaryk University

CROCS
Centre for Research on Cryptography and Security

Notebook

- In the powershell and in Maputo_Workshop
  - git pull
- Start notebook:
  - python -m notebook
- Rename the notebook
  - Change the name '**Test**' to your name
- Hands on
  - Implement your solutions
- Save (Ctrl+S) and send me (before 14:40) notebook
  - Send it to syso@mail.muni.cz (I will confirm the receipt via email)

Practical test

- Helper function:
  extract_bits(value= 4844, lsb_bit=2, msb_bit=5)
  - Indexing from 0, lsb_bit=2(including),
    up to msb=5 (excluding)
  - 1001011101100 => 011 in binary = 3 in decadic
- Non-cryptographic generator (java.util.Random)
  - Check the page LCG to see which bits should be returned
- Number theoretic designs (BBS)
  - State = State * State mod M
  - next_bit() – lsb (as integer) of the state should be returned
  - next_byte() – 8 generated bits should be concatenated and returned as integer