LAB

Old srand() / rand()

- srand(1) + rand
- srand(time(NULL)) + rand

Other options:

- gettimeofday()
- clockgettime()

Linux

- /dev/random
- /dev/urandom
- Write function that will return random data from /dev/random

- int getrdata (int number, unsigned char *buffer)
- read() can be interrupted (when handling signals etc.)
- take care of ‘short’ read

Linux

- check entropy available
  - use system() func – previous LAB
- What is returned value of system() call?

- How to get
  - print to file
  - or use popen()

Windows CryptoAPI

- CryptAcquireContext()

  - PROV_RSA_FULL – default provider

- CryptReleaseContext()

CryptGetRandom()