# Recoverable RNG

## PA193 – Secure coding

Marek Sýs
Faculty of Informatics, Masaryk University, Brno, CZ

CROCS
Centre for Research on
Cryptography and Security

# Old rand, srand

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

Other options:

- gettimeofday()
- clockgettime()

# Linux

- /dev/random
- /dev/urandom
- Write function **int getrdata (int number, unsigned char *buffer)**
- that will return random data from /dev/random

- read() can be interrupted (when handling signals etc.)
- take care of ‘short’ read

# Linux

- Check entropy available
  - Use system() func
- What is returned value of system() call?

- How to get value?:
  - print to file
  - use popen()

# Windows CryptoAPI

- CryptAcquireContext()
  - PROV_RSA_FULL – default provider
- CryptReleaseContext()
- CryptGetRandom()
  - part of MS Crypto API