PV181 Laboratory of security and applied cryptography

Course organization

Marek Sýs
syso@mail.muni.cz, A405

CROCS
Centre for Research on Cryptography and Security

Course style

- May vary – different lecturers
- No lectures just small intro for every seminar:
  - Instructional videos posted few days ahead and/or
  - document/presentation with instructions
  - or only online discussions

- Discussion:
  - online – during given slot on Tuesdays
  - and/or IS discussion group

Seminars overview

- 3xOpenSSL command line tool(Marek Sys)
  – will be moved to PV080 (overlap for this year)
- 1x ASN1 (Marek Sys)
- 3xCrypto libs in C, C++) (Milan Broz)
  – OpenSSL and various libs
- 1xCrypto in JAVA (Dusan Klinec)
- 1xStandards (Zdenek Riha)
- 1xMicrosoft crypto API (Marek Sys)
- 2xBiometrics (Martin Ukrop, Agata Kruzikova)
  – also partly in PV080

Assignments

- Homeworks/assignments
  - After each seminar
  - 10 points maximum
  - 12 weeks/semester (i.e. 120 points in semester)
  - 70 % required (i.e. 84 points)
  - Deadline is one week
  - Submit files into is.muni.cz
  - Points for your HW within one week in is.muni.cz

Credit/colloquium

- To get the credit or colloquium
  - You must be present at seminars
  - You must be active at seminars
  - You must submit assignments and get:
    - 50 % of maximum number of points for the credit
    - 70 % of maximum number of points for the colloquium