# PV181 Laboratory of security and applied cryptography

## Course organization

Marek Sýs

CROCS
Centre for Research on Cryptography and Security

# PV181

- No lectures
- Seminars
  - 2 hours per week (Wed)
  - All seminar groups run in English
  - Attendance obligatory
    - 2 absences ok
    - For more absences bring the excuse/documentation to the department of study affairs
  - **You have to attend your seminar group!**

# Assignments

- Homeworks/assignments
  - After each seminar
  - 10 points maximum
  - 13 weeks/semester (i.e. 130 points in semester)
  - 70 % required (i.e. 91 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

# Seminars overview

- 1-3. OpenSSL command line tool
  - Symmetric crypto, Asymmetric crypto, Digital signatures
- 4. ASN1
- 5-7. Crypto libs (C, C++)
  - OpenSSL and various libs
- 8. Crypto in JAVA
- 9. Standards
- 10-11. Biometrics
- 12. Microsoft crypto API
- 13. GnuTLS