PV204 Security Technologies

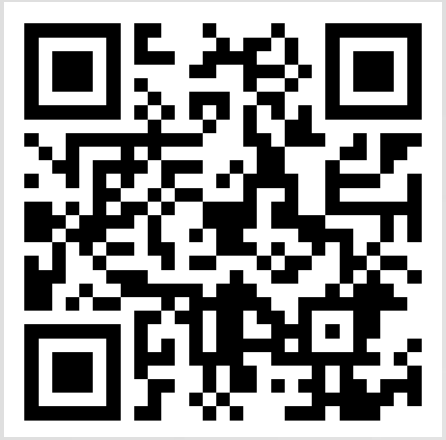
Course overview and grading

Petr Švenda *svenda@fi.muni.cz* *@rngsec*
Centre for Research on Cryptography and Security, Masaryk University

Please report any inaccuracies or suggestions for improvements here:
https://drive.google.com/file/d/1qp-V_VUMUOlIEuBWQWSEqy0_0kjJvTQk/view?usp=share_link

People and semester organization

- Main contact: Petr Švenda (CRoCS@FI MU)
  - svenda@fi.muni.cz, @rngsec
  - https://crocs.fi.muni.cz/people/svenda
- Other lectures, seminars, project
  - Lukasz Chmielewski (MU), Milan Brož (MU), Vašek Lorenc (HERE Technologies), Jiří Gavenda (project)
- Spring 2025 semester organization
  - Interactive lectures + Q&A lecture sessions
  - Seminars (mandatory attendance, >2 absences must be excused formally in IS)
    - Bring your own laptops with software prepared in advance (email)
  - Sometimes pre-recorded/online lectures/seminars (national holidays)



Top questions (1)

PetrS 0

Is my password brute-force-able if consists of 9 printable characters?

- **Place questions, topics and news you would be interested to discuss**
- **We will together discuss these during every week lecture Q&A (towards the end)**

Join at

slido.com

#pv204_2025

Planned lectures (tentative)

- 17.2. Password managers, iVault, OTP, Nostr (Petr Svenda)
- 24.2. FIDO2, Passkeys, ECDH, PFS, PQC, KEM (Petr Svenda)
- 3.3. ePassports, OTR, Signal, Noise (Petr Svenda)

Project phase I. deadline

- 10.3. Programming smartcards, management (Petr Svenda)
- 17.3. Practical threshold cryptography (Petr Svenda)
- 24.3. Secure Boot, TPM, SGX, AMD SEV (Petr Svenda)

Project phase II. deadline

- 31.3. Memory analysis (Vaclav Lorenc)
- 7.4. Disk/file encryption (Milan Broz)

Project phase III. deadline

- 14.4. Trusted element, usage scenarios, side-channel attacks (Lukasz Chmielewski)
- 21.4. Advanced SCA Attacks & Business Perspective (Lukasz Chmielewski)

- 28.4. Bitcoin-related topics I. (Petr Svenda)
- 5.5. Bitcoin-related topics II. (Petr Svenda)

Project phase IV. deadline

- 12.5. Project presentation (Jiri Gavenda)

Project phase V. deadline

Organization

- Lectures + seminars + assignments + project + exam (open book + oral)
- Assignments
  - 6 regular homework assignments
  - **Individual work of each student**
- Project
  - **Team work** (3 members)
  - Details in pv204_project_2025.pdf (IS)
  - Design and implementation of security system atop of Nostr protocol
- Exam
  - Drill questions, Open book open questions, Oral exam
  - During oral part of the exam, you will be asked to explain two of your homework assignments and your contribution to project (if doubts, points may be removed)

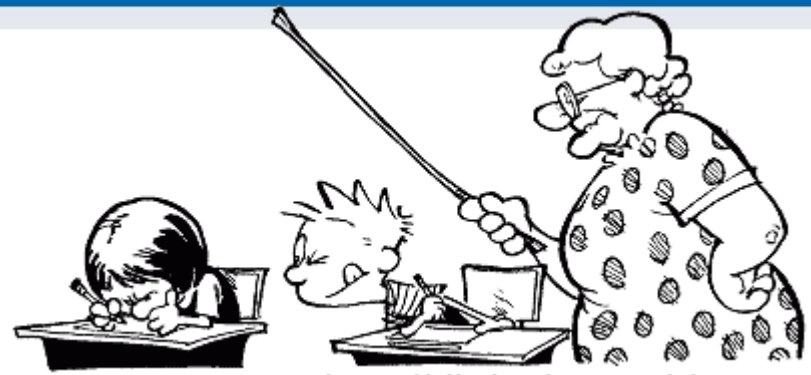
Grading

- Credits: 2+2+2 credits, plus 2 if exam
- Points [Notice minimal number of points required!]
  - Questionnaire from lectures (10) [no minimum limit]
  - Assignments (30) – [minimum 15 required]
  - Project (30) – [minimum 15 required]
  - Exam (30) – [written and oral part] + 95% correct from drill questions
  - Occasional bonuses ☺
- Grading 100 (max)
  - A ≥ 90, B ≥ 80, C ≥ 70, D ≥ 60, E ≥ 50, F < 50
  - Z ≥ 50 (including minimum numbers from Assignments and Project)

Previous knowledge requirements

- This is advanced and time-consuming master course!
  - Typically taken after PV080, PV079, PV181 courses
  - (if you like to start with security, take PV080)
- Basic practical knowledge of (applied) cryptography
  - Symmetric vs. asymmetric cryptography, PKI
  - Block vs. stream ciphers and usage modes
  - Some experience with usage of cryptographic libraries
- Practical experience with C/C++/Java/Python languages
  - Git, debugging…

Plagiarism



http://dkdavis.weebly.com

- Assignments
  - Must be worked out independently by each student
- Projects
  - Must be worked out by a team of 3 students
  - Every team member must show his/her contribution (description of workload distribution, git commits, activity during presentation)
- Plagiarism, cut&paste, etc. is not tolerated
  - Plagiarism is use of somebody else words/programs or ideas without proper citation
  - IS helps to recognize plagiarism
  - If plagiarism is detected student is assigned -5 points
  - In more serious cases the Disciplinary committee of the faculty will decide

Discussion forum in Information System

- Discussion forum in Information System (IS)
  - https://is.muni.cz/auth/cd/1433/jaro2025/PV204/
- Mainly for discussion among the students
  - Not observed by us all the time!
  - Write us email if necessary please
- What to ask?
  - OK to ask about ambiguities in assignment
  - NOT OK to ask for the solution
  - NOT OK to post your own code and ask what is wrong

Course resources

- Lectures (video, PDF) available in IS
  - IS = Information System of the Masaryk University
  - Lecture questionares in IS opened till end of Monday
- Assignments (what to do) available in IS
  - Submissions done also via IS (homework Vault)
- Additional tutorials/papers/materials from time to time will also be provided in IS
  - To better understand the issues discussed
- Recommended literature
  - To learn more …

Questions ?