When, How, and What

Cryptology (1)

Martin Stanek

2025

KI FMFI UK Bratislava

Contact

- room M-214
- e-mail: stanek@dcs.fmph.uniba.sk
- web: http://www.dcs.fmph.uniba.sk/~stanek
  - slides, homeworks, etc.
  - language: English
- lectures:
  - Wednesday at 16:30, room M-I
  - Thursday at 14:00, room M-I
  - language: Slovak; individual consultations in English (Erasmus students)

Grades

- Assignments (3 or 4)
  - *implement/break/solve something* (sufficient time to do these homeworks)
  - **all** assignments are mandatory (it is a prerequisite for the exam)
  - Do the assignments by yourself!
- Written exam:
  - closed-book multiple choice test
  - open-book problems

Content (approximate)

- cryptographic constructions
  - algorithms and schemes: symmetric ciphers, public-key encryption, hash functions, MAC, digital signatures, post-quantum constructions
  - protocols: key agreement, authentication, secret sharing, zero-knowledge proofs
- how they work
  - correctness, implementation issues
- what makes them secure
  - how is the security defined, properties of various constructions
  - assumptions, computational problems

A note on other resources

- various supplemental material available on the internet
  - textbooks, lecture notes, video lectures, etc.
  - introductory/advanced, applied/theory

Don’t hesitate to ask if something doesn’t make sense.
If you are not sure about something, just ask.
Really.