Cryptology – organization

Martin Stanek

Department of Computer Science
Comenius University
stanek@dcs.fmph.uniba.sk

Cryptology 1 (2023/24)

Contact

- room M-214
- e-mail: stanek@dcs.fmph.uniba.sk
- web: www.dcs.fmph.uniba.sk/~stanek
- lectures:
    - Wednesday: 16:30, room M-V
    - Thursday: 16:30, room M-IV

Grades

- Some (3 or 4) assignments through semester
- Written exam:
    - closed-book multiple choice test (+1, -1, -2)
    - open-book problems
- I expect you do *all* assignments (prerequisite for the exam).
- I expect you do the assignments by *yourself*.

- 2x exam-like exercises through semester (not graded)

Content (approx.)

- ▶ cryptanalysis of basic ciphers
- ▶ symmetric encryption: block ciphers (e.g. AES), modes, stream ciphers
- ▶ public key encryption: RSA, discrete logarithm and code-based schemes
- ▶ hash functions: properties, constructions (e.g. SHA families)
- ▶ message authentication codes
- ▶ digital signatures (e.g. RSA, DSA, ECDSA), elliptic curves
- ▶ hash-based signature schemes
- ▶ passwords: storing, key derivation
- ▶ secret sharing schemes
- ▶ cryptographic protocols: constructions and attacks
- ▶ TLS
- ▶ schemes based on LWE problem

Other resources

- ▶ many supplemental material available on the internet
- ▶ various books (introductory/advanced, applied/theory), lecture notes, textbooks, video lectures, etc.
- ▶ short intro to cryptology (informal introduction only):
  www.dcs.fmph.uniba.sk/~stanek
  documents "Kryptológia" and "Kryptológia 2" (SK)