T-79.159 Cryptography and Data Security

Lecture 12: Epilogue

Helger Lipmaa
Helsinki University of Technology
helger@tcs.hut.fi

Overview of the Lecture

- What we have done?
- New directions in cryptography
- Advertisements
- Exam, etc

What we have done?

- Undergraduate course — not much, actually
- Symmetric and asymmetric cryptography
- Primitives and protocols

What we did not do?

- We did not look very closely at primitives — see Kaisa Nyberg's course for this
- Did not have very much time for protocols either
  - ⋆ Possibly a new course on cryptographic protocols this Autumn

Current directions in cryptographic research

1. The general MPC protocols are too slow for many problems. Devise fast specific protocols.

2. Construct fast public-key cryptosystems

3. Prove the security of symmetric cryptosystems

4. . . . base all this on weaker assumptions

5. Efficient reductions: if A is secure construct B that is *almost* as secure

Advertisement 1: Follow-up courses

- T-79.103 — Basics of Cryptology (Kaisa Nyberg, autumn). More on primitives!
- T-79.514/515 — (graduate) seminars on current topics in cryptography (Helger Lipmaa, every semester)
- Possible new course on cryptographic protocols starting this Autumn
- Practical security courses given by the TML lab

Advertisement 2: Not scared yet?

- Want to do a thesis (MSc, PhD) in cryptography?
  - ⋆ Contact me. . .
  - ⋆ Perfect background (select one to four): mathematics, puzzles, wants to see the results applied in practice, (paranoid)
- Thesis topics are available
- Might also possible to apply for a job at the university

Advertisement 3: Not scared yet?

- Helsinki area features many security/cryptography-related companies:
  - ⋆ Nokia — large research group active also in standardization etc
  - ⋆ SSH
  - ⋆ F-Secure
  - ⋆ Nixu
  - ⋆ ...
- Bright future? (If the economy does not go down again)

Exams etc

- Course homepage has the list of students accepted to the exam (contact Markku if it is wrong)
- Exam (12 May or 17 May): Slightly more theoretical than home assigments. Security proofs, breaking of faulty ciphers/protocols, test of knowledge
- See the questions from the previous year. Redo the tutorials. Read the slides until you reach enlightment :-)

Good luck!