T-79.159 Cryptography and Data Security

Lecture 10: 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
- Knowledge vs engineering

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 — at some moment there might be a course on that

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. . . . based on different assumptions

4. Prove the security of symmetric cryptosystems

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-79.513/514 — (graduate) seminars on current topics in cryptography (Helger Lipmaa, every semester)
- 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 bankrupt)

Advertisement 4: Guest lecture

Who Vincent Rijmen

Who??? One of the two authors of the AES, Flemish person of the year 2000

When? 26–28 May, 16:15-18:00

Where? Not decided yet

More information: `http://www.tcs.hut.fi/Research/Crypto/minicourses/`

Exams etc

- Two home assignments: both 15 points (Deadline for the second one: 28 April; corrected asap)
- To get to exam, must either
  - ⋆ Pass both, or
  - ⋆ Pass one of them and do an additional essay on an individual topic in English. (Essay will not increase the number of points, just allow you to get to the exam.)
    - ∗ To apply for essay topics, email to Markku and me as soon as you get to know your result of the second assigment
    - ∗ Due to tight schedule, essays either must be return before May 3, or you have a chance to take exam later (later June/August)
- Exam (6 May,...): 10 points, in total 15+15+10 points. Slightly more theoretical than home assigments. Security proofs, breaking of faulty ciphers/protocols, test of knowledge
- See the questions from the previous year...