AGH University of Science and Technology

Selected Topics in Cryptography

Introduction to the Course

Piotr Chołda

Department of Telecommunications

Outline

1 Course Rules

Outline

1 Course Rules

Teacher's Data

Piotr Chołda, Dr.habil.

Pavilion D-5, first floor, room 113

Thursdays, 2.45-4.15^{PM} + after setting an appointment via e-mail

(+48 12 617–)26–16

piotr.cholda@agh.edu.pl

http://www.cholda.pl/teaching

Purpose of the Course

- To get knowledge on the basic problems in cryptography.
- To practice to learn on one's own.
- To exercise to prepare and give presentations, moderate discussions, etc.
- To practice in implementation of algorithms.

How to Get a Credit (1)

- TEN meetings:
  - TWO (2) introductory meetings led by the teacher (today: course rules, and a short presentation on mathematical fundamentals of cryptography),
  - EIGHT (8) seminar meetings led by the students on the basis of the readings (typically: three presentations per meeting are necessary).
- The schedule is presented at the course webpage.
- Presence is obligatory (up to three absences with no excuse are acceptable).
- All the attendees are required to get acquainted with the topics, even if they are not presenting.

How to Get a Credit (2)

- You are given a pre-selection of topics. You can pick one for you.
- Topics should be described thoroughly, you can base on readings from the suggested books. Search for information wherever you want, but some obligatory issues are provided and you should present them.
- Each attendant has to prepare one presentation and to lead the discussion on selected topics.
- If you are well acquainted with some topics, it is advisable to pick something you do not know — then you learn something new ☺

How to Get a Credit (3)

- Duties of the presenter:
  - A presentation should be prepared for 35 minutes (appr. 15-20 technical slides).
  - A presentation must be prepared in the LaTeX `beamer` class: the template is given at the course webpage.
  - A set of slides must be sent to the teacher at last **a week** before the scheduled presentation (except for the first meeting's presentations).
  - A concept of the discussion with the classmates should be prepared: appr. 10 minutes of discussion (e.g. tough problems, how to implement, examples from real life — you may have some experience as company employees ☺).

How to Get a Credit (4)

- The regular and advisable method to obtain the credit:
  - No more absences than three.
  - Presentation on the scheduled topic given to the classmates in your group and the leading role in the discussion after the presentation.
  - Provisioning of the slides to the teacher **on time** (Monday, 11.59^{PM}, a week prior to the presentation), in the required format and at an appropriate quality level.
  - Taking into account the suggestions given by the teacher (before the seminar) with respect to the initial version of the presentation.

How to Get a Credit (5)

- Grade: based on the assessment of the teacher and the group:

$$\max\{t, c\}, \quad \text{where:}$$

  - t: is the grade proposed by the teacher,
  - c is the median of the grades proposed by other participants (your classmates) of the course (Google Forms will be used for voting).

How to Get a Credit (6)

- The irregular and non-desirable way to obtain the credit:
  - Necessary when a student fails to conform to any of the previously given conditions.
  - Still: necessity to present the scheduled topic to the classmates (most probably the group will be forced to find an additional time slot for a meeting).
  - Need to pass a test covering all the topics of the seminar (25 questions, 25 minutes).
- Grade: according to the test results.

How to Get a Credit (7)

Project:

- Groups of 3–4 students.
- Implementation of a random number generator or hash function.
- First meetings with the instructor (Andrzej Kamisiński, MSc): Oct. 17-18.
- Information on the course webpage.

Suggested Books

- Lynn Margaret Batten. *Public Key Cryptography.*
  John Wiley & Sons, Inc., Hoboken, NJ, 2013.
- Johannes A. Buchmann. *Introduction to Cryptography.*
  Undergratudate Texts in Mathematics. Springer-Verlag, New York, NY, 2004.
- Joshua Holden. *The Mathematics of Secrets. Cryptography from Caesar Ciphers to Digital Encryption.*
  Princeton University Press, Princeton, NJ, 2017
- Dominic Welsh. *Codes and Cryptography.*
  Clarendon Press, Oxford, UK, 1988.
- Song Y. Yan. *Computational Number Theory and Modern Cryptography.*
  Wiley & Higher Education Press, Singapore, 2013.

The books can be borrowed from the teach for scan, copy, etc. (only via the group representative).

Topics for Selection

The Selected Topics Should be Presented in the Given Order

For the topics numbered in a series (such as *'B1'*, *'B2'*, ...), a topic number $(n+1)$ must not be selected if topic number (n) is not selected!

- Properties of good ciphers
- Computational complexity (B1)
- Basic methods for cryptanalysis
- Modes of ciphers' operation
- Affine ciphers (C1)
- Cryptanalysis of affine ciphers (C2)
- Polyalphabetic substitution ciphers and the related cryptanalysis
- Enigma

Topics for Selection (cont.)

The Selected Topics Should be Presented in the Given Order

- Transposition ciphers (D1)
- DES (D2)
- AES (D2)
- The LibreSSL Library (D3)
- Homomorphic encryption
- Exponentiation ciphers (E1)
- Diffie-Hellman key agreement and ElGamal encryption system (E2)
- Generation of prime numbers and primality testing (E3)
- Public-key infrastructures (E3)
- Knapsack-based cryptosystem
- Stream ciphers (F1)

Topics for Selection (cont.)

The Selected Topics Should be Presented in the Given Order

- Generation of pseudo-random numbers (F2)
- Family of A5 ciphers for cellular systems (F2)
- Hashes (G1)
- Digital signatures (E3, G2)
- GPG (E4, G3)
- Cryptosystems based on elliptic curves
- Complexity of cryptography-related problems: factoring of composite numbers (B2)
- Complexity of cryptography-related problems: discrete logarithm (B3)
- Cryptanalisys based on quantum computing (H1)
- Post-quantum cryptography (H2)
- Quantum cryptography (E3)

Next steps

- You: the given Google Docs files for different groups (11.05–1.20, 1.30–3.45, 3.45–6.00) cover the topics (for some topics, 90 min. of presentation is assumed: then it can be covered by two persons).
- The deadline for the declarations: Friday, October 6^{th}, 11.59^{PM}. Then, the teacher fixes the schedule for presentations.
- The presentations are performed in the order given in the previous slide. The non-covered topics are just skipped.
- The final schedule with the presenters will be given at the teacher's webpage.
- The first seminar meeting: Monday, October 16^{th}.
- The first presentation must be sent to the teacher a little bit less than a week before (**exceptionally!**), on Wednesday, October 11^{th}, 11.59^{PM}.

AGH

Any questions, comments?

AGH

Thank you for your attention!