AGH University of Science
and Technology

Introduction to Cryptography

Piotr Chołda

Department of Telecommunications

March 14, 2018

Outline

Outline

Teachers' Data

Leading Teacher + Seminar

Piotr Chołda, Dr.habil.

Pavilion D-5, first floor, room 113

Wednesdays 1.00-2.30^{PM}; Thursdays, 2.30-4.00^{PM}; + e-mail

(+48 12 617–)26–16

piotr.cholda@agh.edu.pl

http://www.cholda.pl/teaching

Teachers' Data

Project + Laboratory Classes

Krzysztof Pomorski, PhD

Pavilion D-5, first floor, room 107

Fridays, 2.00-3.00^{PM} + after setting an appointment via e-mail

(+48 12 617–)40–36

kdvpomorski@kt.agh.edu.pl

Purpose of the Course

- To get knowledge on the basic problems in cryptography (ALL).
- To practice to learn on one's own (SEM).
- To exercise to prepare and give presentations, moderate discussions, etc. (SEM).
- To practice in implementation of algorithms (PROJ).
- To practice to use encryption software (LAB).

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.
- 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. (preferably via the group representative).

Connection between Me/Us and You

Representative (*starosta*):

Mr. Kasper Biegun (E&T)

Teacher's Wednesdays

Classical and Introductory Issues

- Today (March 14): Overview of cryptography problems.
- March 21: Basic ciphers (substitution and transposition ciphers) and perfect secrecy.
- March 28: Symmetric cryptography (including DES and AES).
- April 18: Congruence arithmetic and asymmetric cryptography (RSA).
- April 25: Hashes, digital signatures, and PKI.

How to Get a Credit (1)

Seminar

- TEN meetings:
  - FIVE (5) lecture-like meetings led by the teacher (today: course rules, and an overview of basic cryptography problems), and then:
  - FIVE (5) seminar meetings led by the students (two presentations per meeting).
- Presence is obligatory (up to four absences with no excuse are acceptable).

How to Get a Credit (2)

Seminar Meetings Led by the Students

- You are given a pre-selection of topics. You can pick one for you to present to the classmates.
- Topics should be described thoroughly. Search for information wherever you want, but some obligatory issues are (in some cases) provided and you should cover them.
- Each attendant has to prepare one presentation and lead the discussion on selected topics.
- Each presentation is prepared by a group of 2-3 students (but we need 10 topics to be dealt with by the students).

How to Get a Credit (3)

Seminar

- Duties of the presenter(s):
  - A presentation should be prepared for 40 minutes (appr. 18-22 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 **two weeks** before the scheduled presentation.
  - A concept of the discussion with the classmates should be prepared: appr. 5 minutes of discussion (e.g. controversions, how to implement in practice, examples from real life — you may have some experience as company employees ☺, questions).
  - If it is possible to show operation of some concepts with software, etc. please show this as well.

How to Get a Credit (4)

Seminar

- The regular and advisable method to obtain the credit:
  - No more absences than four (obviously if you have a good excuse, e.g., you are ill, the absence is not counted).
  - 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** (Wednesday, 11.59^{PM}, two weeks 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)

Seminar

- Grade for seminar: 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)

Seminar

- 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 (20 questions, 20 minutes).
- Grade: according to the test results.

How to Get a Credit (7)

Student's Seminar Meetings

- May 9.
- May 16.
- May 23.
- May 30.
- June 6.
- (backup: June 13).

Topics for Selection

The Selected Topics Should be Presented in the Given Order

- Theory: computational complexity.
- Theory: complexity of cryptography-related problems — discrete logarithm.
- Theory: complexity of cryptography-related problems — factoring of composite numbers.
- Methods: secret sharing.
- Methods: homomorphic encryption.
- Methods: watermarking.
- Methods: steganography.
- Methods: key exchange based on neural networks.

Topics for Selection

The Selected Topics Should be Presented in the Given Order

- Protocols: IPSec.
- Protocols: TSL/SSL.
- Protocols: OAuth.
- Applications: application of VPNs.
- Applications: blockchains (and Bitcoin).
- Applications: cryptocurriencies other than Bitcoin.
- Applications: stealth malware attacks.

You can also propose topic on your own (consult via e-mail).

How to Get a Credit (8)

Next Steps related to Student's Seminars

- You: the given Google Docs file covers the topics.
- The deadline for the declarations: Wednesday, April 11^{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: Wednesday, May 9^{th}.
- The first presentation must be sent to the teacher two weeks before Wednesday, April 25^{th}.

How to Get a Credit (9)

Projects (Led by Dr Krzysztof Pomorski)

- Groups of 5–6 students.
- Implementation of an important cryptography-related topic not covered at the seminar:
  - random number generator (software or hardware),
  - primality testing,
  - implementation of a hash function (SW or HW),
  - a newly standardized element of telecommunication protocols (e.g., recently it concerns elliptic curve cryptography).
- Four consultation meetings are obligatory:
  - up to March 29 — selection of a topic (formation of teams and selection of what to do),
  - up to April 27 — decision on how the project is realized/implemented,
  - up to June 1 — presentation of the initial results,
  - up to June 22 — final presentation of the results (a short, 5-pages long, report + public presentation of the results).

How to Get a Credit (10)

Labortory Classes and Final Grade

- Observation of algorithms and practice with encryption software.
- Four meetings:
  - May 22: symmetric ciphers — DES and AES.
  - May 29: asymmetric ciphers — RSA and certificates.
  - June 5: hashes and digital signatures.
  - June 12: cryptography based on elliptic curves.
- Credit will be obtained if you are present at all the meetings.
- Grades (>3,0) based on activity level.

Grade for the course: mean of the grade for the seminar, project and laboratory classes.

AGH

Any questions, comments?

Thank you for your attention!