



KTH Datavetenskap
och kommunikation

DD2448 Foundations of Cryptography 7.5 hp Spring 2010

Important Source of Information

Important information about the course will continuously be published at the course home page, <http://www.csc.kth.se/DD2448/krypto10>.

Goal

The goal of the course is to

- give an overview of modern cryptography

in order that students should

- know how to evaluate and, to some extent, create cryptographic constructions, and
- to be able to read and to extract useful information from research papers in cryptography.

Prerequisites

Corresponding to one of the courses:

- *DD1352 Algorithms, data structures and complexity*, or
- *DD2354 Algorithms and complexity*.

We also assume knowledge of mathematics and theory of algorithms corresponding to the required courses of the D or F-programmes at KTH.

Lecturer

Douglas Wikström is responsible for the course and gives most lectures. The safest way to reach him is by email at dog@csc.kth.se (please put Krypto10 in the subject), but he can sometimes be found in his office, room 1442, Lindstedtsvägen 3. If you email a question of general interest, the answer will be posted at <http://www.csc.kth.se/DD2448/krypto10/faq> and you get an empty email reply.

Schedule

Only the first two lectures are scheduled:

L1. Tue, Jan 19, 10:00-12:00, in Room D34.

L2. Fri, Jan 22, 13:00-15:00, in Room D41.

The remaining lectures will be scheduled in class during the first lecture and the resulting schedule will be posted at <http://www.csc.kth.se/DD2448/krypto10/schedule>. Please make sure that your constraints are presented at the first schedule by attending or by giving somebody attending a copy of your schedule.

Tentative Plan of Lectures

L1-L2. Introduction, scheduling of future lectures, classical cryptography, symmetric ciphers, security, entropy.

L3-L5. DES and AES. Attacks, linear cryptanalysis, side-channel attacks.

L6-L8. Asymmetric cryptography, trap-door hashfunctions, RSA, El-Gamal, McEliece.

L9. Hash-functions, theory and practice, SHA-1, and message authentication codes (MACs).

L10. Digital signatures, key distribution, and random oracle model.

L11. Identification schemes and signature schemes.

L12. Elliptic curve cryptography.

L13. Pseudorandom generators.

L14-L15. Make-up time, additional topic, and guest lecture.

Course Material

As a main text for the course we recommend *Stinson: Cryptography, Theory and Practice, Chapman & Hall CRC, 3rd edition*, but this book does not cover all of the material covered in class.

Pointers to additional literature, available for free online, are provided on the course home page.

Course Requirements

Know the Rules. All students are expected to have read and understood the *CSC code of honor* found at <http://www.kth.se/csc/student/hederskodex>. However, additional rules apply for this course, see <http://www.csc.kth.se/DD2448/krypto10/rules>. All students are required to read and understand the meaning of these rules before starting with any of the tasks below.

Homework 1-2. Each homework consists of a number of assignments; both theoretical and practical. Solutions may be written in Swedish or English.

Each assignment gives a number of homework points (H -points) or *basic* homework points (B -points). Basic points measure basic understanding of the course contents. Each homework satisfies $B + H \geq 100$ and $B \geq 40$.

Presentations. Give a brief presentation of one of the Round-2 candidates of the SHA-3 competition, <http://csrc.nist.gov/groups/ST/hash/sha-3>.

This task gives 0 or 30-80 presentation points (P -points) The presentation must be one of the following:

1. A written presentation. It must have 4 pages with reasonable margins and 11pt font.
2. A 12-min oral presentation.

Oral Exam. We discuss your solutions and their relations to the contents of the course, including the research presented.

The oral exam is scheduled at the end of the course and gives a single oral point (O -point) if it is passed. However, a number of (positive or negative) B or H -points may also be awarded for individual problems of the homeworks for which written solutions have been submitted, depending on the level of understanding displayed. No more points can be withdrawn (negative points), than was awarded for a solution.

All students aiming for grades A-B must do the oral exam, but any student may request to do the exam.

Deadlines.

- **Homework 1.** Before the start of Lecture 11.
- **Homework 2.** March 19, 09:00.

- **Written Presentation.** March 19, 09:00.
- **Oral Presentations.** During March 8 – March 19. Times will be available online for booking.
- **Oral Exam.** During March 8 – March 19. Times will be available online for booking.

Grading

The grade requirements are cumulative, e.g., to earn a C the requirements of the grades E-C must be fulfilled. Define the total points by $T = B + H + P + O$. The requirements are as follows:

- E. $B \geq 60$ and $P \geq 30$.
- D. $T \geq 120$.
- C. $T \geq 140$ and $P \geq 50$.
- B. $T \geq 170$ and $O \geq 1$.
- A. $T \geq 200$ and $P \geq 70$.

If the first homework gives less than 20 B -points, then the rest of the homework is not corrected and we assume that the student has dropped out of class. The same convention is used for the second homework, with 20 replaced by $60 - b$, where b is the number of B -points from the first homework.

Register For the Course

To register for the course, send an email to dog@csc.kth.se with subject `Krypto10_Register` and a body of the following form:

Firstname(s)
Lastname(s)
Email address(s)
Personal number
Study status

Below we give an example body:

Eva Stina
Güvendiren Olsson
eva@yagoo.se eva@guwendiren.tr
830121-1234
F-07