KUNGL TEKNISKA HÖGSKOLAN
Datavetenskap och kommunikation
Johan Håstad

14 januari 2008

# DD2449, Foundations of Cryptography, spring 2008

## Goal

The goal of the course is to

- give a good 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. Knowledge of probability theory, mathematics and theory of algorithms corresponding to the required courses of the KTH educations D or F.

## Professor

Johan Håstad is responsible for the course and also the principal lecturer. The safest way to reach him is by email at <johanh@kth.se>, but he can also sometimes (usually?) be found in his office, room 1435, Lindstedtsvägen 3.

## Schedule

| | | | | | |
|---|---|---|---|---|---|
| vecka 4 | F1 | 2008–01–21 | Må | 15-17 | E3 |
| | F2 | 2008–01–23 | On | 10-12 | E3 |
| | F3 | 2008–01–24 | To | 8-10 | D3 |
| vecka 5 | F4 | 2008–01–28 | Må | 13-15 | E3 |
| | F5 | 2008–01–30 | On | 10-12 | D3 |
| | F6 | 2008–01–31 | To | 10-12 | E2 |
| vecka 6 | F7 | 2008–02–04 | Må | 13-15 | E3 |
| | F8 | 2008–02–06 | On | 10-12 | E3 |
| | F9 | 2008–02–07 | To | 15-17 | E2 |
| vecka 7 | F10 | 2008–02–11 | Må | 13-15 | E3 |
| | F11 | 2008–02–13 | On | 10-12 | E3 |
| vecka 8 | F12 | 2008–02–18 | Må | 13-15 | E3 |
| | F13 | 2008–02–20 | On | 8-10 | E3 |
| vecka 10 | F14 | 2008–03–03 | Må | 13-15 | E3 |
| | F15 | 2008–03–05 | On | 10-12 | E3 |

A preliminary plan of the lectures is as follows.

**F1-F2:** Introduction, classical cryptography, security, entropy.

**F3-F5:** DES and AES. Attacks, linear cryptanalysis, timing and power attacks.

**F6-F8:** Asymmetric cryptography, RSA, El-Gamal, McEliece.

**F9:** Hash-functions, theory and practice, SHA-1, MAC,

**F10-F11:** Digital signatures, key distribution, identification.

**F12:** Elliptic curves.

**F13:** Pseudorandom generators.

**F14:** Make-up time or additional topic.

**F15:** A guest lecture by Mats Näslund, Ericsson on some cryptography in practice.

## Course material

The lectures cover essentially all the course material. As a main text for the course we recommend Stinson: “Cryptography, Theory and Practice”, Chapman & Hall /CRC, 3rd edition.

Another possibility that contains the material of the course is Trappe, Washington: “Introduction to Cryptography, with coding theory”, Pearson International.

For the student interested in more details and depth about the theoretical foundations of cryptography we recommend Goldreich: “Foundations of Cryptography”, Cambridge University Press.

Lecture notes from the course of 2006 are available from the home page of that course (<http://www.nada.kth.se/kurser/kth/2D1449/krypto06/>) and might be of value for the student.

## To register and check in

Many categories of students are welcome to this course and different students might face different administrative problems. We encourage each student to make sure that he/she does not have any such problems.

You must also do the following commands from a Unix computer at CSC. Do »res checkin krypto08» to make sure that your score can be reported and also »course join krypto08» which among other effects makes sure that messages intended for all course participants reach you each time you log in. When the course is over you can give the command »course leave krypto08» to return to your initial configuration.

Log-in messages and the course home page are important and vital information for the course might be given only through these channels.

## Examination

There is no final exam. The course is graded through two traditional sets of homework problems and one presentation. To the problem sets, written solutions are supposed to be handed in and then discussed orally. A first approximation of the deadlines for handing in solutions to the problems sets are, 13/2 and 7/3, respectively. A fixed date for the presentation has to be set by March 5, the last lecture.

The CSC Code of Honor applies to these homework problems but there are also some rules specific to this course. These rules are available electronically from the course home page.

The questions on the two problem sets are divided into two parts, theory and practical problems, each containing at least problems of total value 50 points. Passing grades on the oral presentation are given a numeric value which is a multiple of 10 and in the range [30,80]. The performance of the student is thus summarized in three numbers, Theory points (T), Practical problem points (P) and Oral presentation points (O).

To get a passing grade (E or better), it is required that each of T, P and O is at least 30. If on top of this $T + P + O \geq 120$ then the grade D is obtained. To get a grade of C or better it is required that each of T, and P is at least 45 and that O is at least 50. If on top of this $T + P + O \geq 170$ a grade of B is obtained. Finally if each of T and P is at least 55 and $T + P \geq 140$ and O is at least 70, the final grade is A.

The grade determined by the score on the homework is final and the deadlines for handing in the solutions are normally not negotiable. Note that late solutions are accepted with some penalties described in the rules for the homework. Some circumstances such as severe illnesses can, however, be taken as an excuse for late homework, while lack of time due to work outside the university or many parallel courses are not considered as legitimate reasons for a change of this policy. If you feel you have a good reason to hand in homework late, please contact the lecturer as soon as possible.

## Important source of information

Important information about the course will continuously be published at the course home-page, <http://www.csc.kth.se/utbildning/kth/kurser/DD2449/krypto08>.