KUNGL TEKNISKA HÖGSKOLAN
Datavetenskap och kommunikation
Johan Håstad

20 januari 2009

DD2449, Foundations of Cryptography, spring 2009

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 be found in his office, room 1435, Lindstedtsvägen 3.

Schedule

vecka 4	F1	2009–01–19	Må	10-12	D41
	F2	2009–01–20	Ti	15-17	D41
	F3	2009–01–22	To	10-12	D41
vecka 5	F4	2009–01–26	Må	10-12	D41
	F5	2009–01–27	Ti	15-17	D41
vecka 6	F6	2009–02–02	Må	10-12	D41
	F7	2009–02–03	Ti	15-17	D41
vecka 7	F8	2009–02–09	Må	10-12	D41
	F9	2009–02–10	Ti	15-17	D41
vecka 8	F10	2009–02–16	Må	10-12	D41
	F11	2009–02–17	Ti	15-17	D41
vecka 10	F12	2009–03–02	Må	10-12	D41
	F13	2009–03–03	Ti	15-17	D41
	F14	2009–03–04	On	10-12	Q21
	F15	2009–03–05	To	13-15	D41

A preliminary plan of the lectures is as follows.

F1-F3 Introduction, classical cryptography, security, entropy.

F4-F5 DES, modes of block ciphers, linear and differential cryptanalysis.

F6 Finite fields and AES.

F7 Primality testing, Fermat's little theorem, RSA.

F8 The discrete logarithm problem, Diffie-Hellman key exchange, El-Gamal encryption.

F9 Hash functions. Theoretical constructions and practical considerations. SHA-1.

F10 MACs, digital signatures , RSA and DSS.

F11 Schnorr identification and zero-knowledge.

F12 Elliptic curves.

F13 Pseudorandom generators.

F14 Make up time or extra topic.

F15 A guest lecture by Mats Näslund, Ericsson.

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 at 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 krypto09» to make sure that your score can be reported and also »course join krypto09» 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 krypto09» 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, 16/2 and 11/3, 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 grade of the course is based on the scores on the homework problems and on the oral presentation where each presentation is given a value which is either 0 (fail) or an integer multiple of 10 in the range [30,80]. The performance of the student is thus summarized in three numbers, first problem set (P1), second problem set (P2), and Oral presentation points (O).

To get a passing grade (E or better), it is required that each of P1, P2 and O is at least 30. If on top of this $P1 + P2 + O \geq 120$ then the grade D is obtained. To get a grade of C or better it is required that each of P1, and P2 is at least 45 and that O is at least 40. If on top of this $P1 + P2 + O \geq 170$ a grade of B is obtained. Finally if each of P1 and P2 is at least 55 and $P1 + P2 \geq 140$ and O is at least 60, 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 which is located at <http://www.csc.kth.se/utbildning/kth/kurser/DD2449/krypto09>.