KUNGL TEKNISKA HÖGSKOLAN
Datavetenskap och kommunikation
Johan Håstad

14 februari 2007

2D1449, Foundations of Cryptography, 2007

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 2D1352 Algorithms, data structures and complexity or 2D1354 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	2007–01–23	Ti	15-17	D32
	F2	2007–01–24	On	8-10	D32
	F3	2007–01–26	Fr	15-17	D32
vecka 5	F4	2007–01–30	Ti	15-17	D32
	F5	2007–01–31	On	8-10	D32
	F6	2007–02–02	Fr	15-17	D32
vecka 6	F7	2007–02–06	Ti	15-17	D32
	F8	2007–02–07	On	8-10	D32
	F9	2007–02–09	Fr	15-17	D32
vecka 7	F10	2007–02–13	Ti	15-17	D32
	F11	2007–02–14	On	8-10	D33
vecka 8	F12	2007–02–20	Ti	15-17	D32
	F13	2007–02–21	On	8-10	D32
vecka 9	F14	2007–02–27	Ti	15-17	**D3**
	F15	2007–02–28	On	8-10	D32

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.

F14-15: A guest lecture by Mats Näslund, Ericsson, some additional topic, maybe digital money.

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, 2nd 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.

Last years lecture notes available from the home page of last years course might also 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 krypto07» to make sure that your score can be reported and also »course join krypto07» 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 krypto07» 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, 14/2 and 7/3, respectively. A fixed date for the presentation has to be set by March 7.

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 presentation is graded by pass/fail while the two problem sets are given numerical values and the maximum score on each set will be at least 100 points. To get a passing grade on the course a passing grade on the presentation is required. The value of the final grade is then determined as follows.

Scoring at least 30 points on each of the two sets guarantees a passing grade. If, apart from this requirement, the total is 95 or more the grade 4 is assured and total scores above 130 are awarded the grade 5. For students at SU the requirements for passing the course is the same while a total score of 110 is sufficient for VG.

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 homeworks. 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 homepage, <http://www.csc.kth.se/utbildning/kth/kurser/2D1449/krypto07/>.