DD2448 Foundations of Cryptography 7.5 hp
Spring 2019

Sources of Information

Information given during lectures takes precedence. Additional information may be posted at Canvas: https://kth.instructure.com/courses/7509.

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

DD1352 Algorithms, data structures and complexity (or *DD2354 Algorithms and complexity* for older students). 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 he gives most lectures. The safest way to reach him is by email at dog@kth.se (please put `DD2448` in the subject), but he can mostly be found in his office, Room 1518, Lindstedtsvägen 3 (5th floor in the E-building).

Tentative Content

- Administration, introduction, classical cryptography. Information about group project.
- Symmetric ciphers, substitution-permutation networks, linear cryptanalysis, differential cryptanalysis.
- AES, Feistel networks, Luby-Rackoff, DES, modes of operations, DES-variants.
- Entropy and perfect secrecy.
- Security notions of hash functions, random oracles, iterated constructions, SHA, universal hash functions.
- Public-key cryptography, RSA, primality testing, textbook RSA, indistinguishability.
- RSA in ROM, Rabin, discrete logarithms, Diffie-Hellman, El Gamal.
- Message authentication codes, identification schemes, signature schemes, PKI.
- Elliptic curve cryptography.
- Pseudorandom generators.
- Guest lecture?
- Make-up time and/or special topic.

Course Material

A suitable book to study is *Stinson: Cryptography, Theory and Practice, Chapman & Hall CRC (any edition)*, but this book does not cover all of the material covered in class. Pointers to additional books and other literature are provided at Canvas. Part of the course requirement is to find the necessary resources to learn more and solve problems. No reading instructions will be given.

Course Requirements

Know the Rules. All students are expected to have read and understood the *CSC code of honor*, https://www.kth.se/en/eecs/utbildning/hederskodex, but additional rules apply for this course which can be found at Canvas. All students are required to read and understand the meaning of these rules before starting with any of the tasks below.

Group project. Students in groups of three study a topic assigned by the lecturer and write a report

based on their findings. The report is peer reviewed by random assignment, but the lecturer makes the final decision on the number of G-points awarded. Denote by G_0 the nominal number of G-points.

Detailed instructions will appear at Canvas.

Exercises and take-home exam. A large number of exercises will be distributed early in the course. Each exercise is assigned a number of *implementation* points (I-points) and/or *theory* points (T-points) as an indication of how they would be valued in a take-home exam. These exercises are *optional* to solve, i.e., solutions are not submitted, but we *strongly* advise all students to study them seriously.

Towards the end of the course a single take-home exam is handed out. Some exercises will appear as part of the take-home exam, possibly in slightly modified form and with slightly different number of points, but there will be novel problems as well. Denote by I_0 and T_0 the nominal number of implementation and theory points of the take-home exam, respectively.

The deadline for the take-home exam will be at least one week from the handout date and negotiated with students to avoid conflicts with other courses.

Students are expected to prepare by solving as many problems as they can. This leaves time to typeset solutions and solve a few novel problems when the take-home exam is handed out.

Detailed instructions will appear at Canvas.

Oral exam. The oral exam is scheduled individually at the end of the course and gives a single oral point (O-point) if it is passed. The purpose of the oral exam is to give a fair grade.

The starting point of the exam is the group project and the solutions to the take-home exam submitted by the student. A number of (positive or negative) G, I or T-points may be awarded for the group project, or individual problems of the take-home exam 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.

We expect students to pay special attention to anything we marked EXPLAIN and be ready to give the necessary details for us to award points. We use this label to indicate that a solution is ambiguous. We stress that students can get full points on solutions we initially awarded zero points.

Thus, an oral exam proceeds as follows:

1. Student points out any counting errors we may have made.
2. Student explains details for solutions marked EXPLAIN.
3. Student asks about any grading that they consider to be unfair.
4. Student answers any questions about submitted theory or practical solutions, or about the group project, that we ask.
5. Points awarded to student may be updated at our discretion and the updated total is used to derive the course grade.

The grading of a submitted group project or solutions to take-home exam are neither completed nor official until after the oral exam.

Grading

The grade requirements are cumulative, e.g., to earn a C the requirements of the grades E-C must be fulfilled. Define $A_0 = G_0 + I_0 + T_0$ as the total nominal number of points and define the sum of all points earned by $A = G + I + T$. The minimal grade requirements are as follows:

Grade	O	A/A_0	G/G_0	I/I_0	T/T_0
E	1	0.5	0.4	0.4	0.4
D		0.6			
C		0.7	0.5	0.5	0.5
B		0.8			0.6
A		0.8			0.8

Ratio between nominal points. We guarantee that $0.15 \leq I_0/(I_0 + T_0) \leq 0.3$ and $0.3 \leq G_0/(I_0 + T_0) \leq 0.5$.

Kattis

Kattis is a judging server for programming competitions and for grading programming assignments, see https://kth.kattis.com. We use this for all problems where you submit code. By default we assume that your Kattis id is the same as your KTH user name, e.g., if your KTH email is `xyz@kth.se`, then we assume that your Kattis user name is `xyz`. If that is not the case, then please email us your kattis user name using the subject `DD2448 Kattis`, and don't forget to put your name in there as well. Please ask a fellow student to give you a brief introduction to Kattis if you have not used it before.

Register at https://kth.kattis.com/courses/DD2448/krypto19 to let us to see your results.