Cryptography, winter term 16/17: Assignment 12

Prof. Markus Bläser, Cornelius Brand, Marc Roth
http://www-cc.cs.uni-saarland.de/course/55/

Due February 8th, 2017

This is the last regular assignment sheet for the course.

Exercise 12.1 (Be nice to your tutors and TAs, 1 Bonus Point)
Write the name and matriculation number of every author as well as number, time slot and the name of the tutor of your tutorial group on the first page of your solution. Furthermore write in english and staple *all* sheets of your solution.

Exercise 12.2 (Grading, 2 + 2 Bonus Points) The cryptography lecture is graded as follows: Every student scored a percentage p of points in the midterm exam (no-shows scored zero percent). The number of bonus points b_{endterm} for the endterm exam is computed by multiplying p to a quarter of the total number of points achievable in the endterm exam and rounding up. b_{reexam} is computed likewise. Now let N_{endterm} and N_{reexam} be the number of points a student achieved in the endterm and reexam, respectively. Furthermore let T_{endterm} and T_{reexam} be the total number of points achievable in the endterm and reexam, respectively. The final score S of a student is calculated as follows

$$S := \max\left\{\frac{N_{\text{endterm}} + b_{\text{endterm}}}{T_{\text{endterm}}}, \frac{N_{\text{reexam}} + b_{\text{reexam}}}{T_{\text{reexam}}}\right\}$$

The course is passed if $S \geq \frac{1}{2}$.

(a) A student got 18 out of 42 points in the midterm exam. The total number of points in the endterm is 120 and the total number of points in the reexam is 180[1]. In the endterm the student scored 45 points. Is the course already passed? If not: Calculate the minimum number of points the student has to achieve in the reexam to pass the course.

(b) Let T_{endterm} be as above. Furthermore, the total number of points in the midterm exam is 42. Assume a student scored N_{midterm} points in the midterm exam. Compute the minimum number N_{endterm} of points the student has to score in the endterm exam such that the course is passed without taking the reexam.

Exercise 12.3 (Breaking RSA with a parity-oracle, 5 points) Let (N, e) be a fixed RSA public-key, and suppose you are given access to an oracle $\oplus(\cdot)$ that computes the *parity* of x, i.e., the remainder of x after division by two, when given $x^e \bmod N$ as input.

[1] Those numbers are only for the purpose of this exercise. The actual number of points in the exams may differ.

Give an algorithm that, given $y = x^e \bmod N$, reconstructs x. Prove that your algorithm is correct and performs a polynomial (in $\log N$) number of operations and oracle queries.

Exercise 12.4 (Signature schemes and one-way functions, 6 Points)
Let $\Pi = (\mathrm{Gen}, \mathrm{Sign}, \mathrm{Vrfy})$ be a *secure* signature scheme for 1-bit messages. Without loss of generality, we can assume that there is a polynomial p such that Gen uses exactly $p(n)$ random bits on input 1^n. Now consider the following algorithm A_f:

(1) On input x, A_f searches n such that $p(n) \leq |x| \leq p(n+1)$.[2]

(2) Then A_f simulates $\mathrm{Gen}(1^n)$ with random bits x and obtains a pair (pk, sk).

(3) A_f outputs pk.

Now let f be the function that is computed by A_f. Show that f is a one-way function.

Exercise 12.5 (From fixed- to arbitrary-length signatures, 5 Points) Adapt Construction 4.7 (see the lecture slides) for constructing variable-length MACs from fixed-length MACs so that it produces a signature scheme for arbitrary-length messages from any signature scheme for fixed-length messages of length $\ell(n) \geq n$. It may be advisable to go through the proof of Theorem 4.8 and to adapt it to the new requirements.

[2] You can assume that this n exists for every x and can be found in polynomial time in $|x|$.