KTH Computer Science
and Communication

Homework IV, Foundations of Cryptography 2014

Before you start:

1. The deadlines in this course are strict. This homework set is due as specified at `http://www.csc.kth.se/DD2448/krypto14/deadlines` and is May 20 at 15.00.
2. Read the detailed homework rules at `http://www.csc.kth.se/DD2448/krypto14/rules`.
3. Read about I and T-points, and how these translate into grades, in the course description at `http://www.csc.kth.se/DD2448/krypto14/handouts/course_description.pdf`.
4. Note that in problems with subproblem, the first number given is the total number of points for the problem and later there is information how this total is distributed over the subproblems.

The problems are given in no particular order. If something seems wrong, then visit `http://www.csc.kth.se/DD2448/krypto14/handouts` to see if any errata was posted. If this does not help, then email `johanh@csc.kth.se`. Don't forget to prefix your email subject with `Krypto14`.

1 (10T) A mother has decided to use the Shamir secret sharing scheme to tell her children who will inherit a worthless but emotionally important family treasure. Let us denote the children by C_1, C_2, C_3, C_4, and C_5. The mother has chosen a polynomial P of degree 3 such that $P(0)$ gives the identity of the beneficiary. Her goal was that any 4 can recover the identity of the child in question. The identity is given as an integer in the range 1 through 5. He has also given the value of $P(i)$ (here denoted by a_i) to C_i together with the specification that the polynomial is evaluated mod $2^{31}-1$. The two children C_4 and C_5 are good friends and are certain that C_2 is the recipient of the treasure. Suppose $a_4 = 103747344$ and $a_5 = 764235921$. Show that C_4 and C_5 can, without any additional knowledge, change their own values to make C_4 the beneficiary.

2 (10T+5I) On the course web page you have five sets of sequences, ser1, ser2, ser3, ser4 and ser5. In each you find five pairs of sequences. In each pair one of the sequences have been produced by a bad pseudorandom generator giving some nonrandom[1] property while the other is output from a much better generator. In each set, the same bad generator was used for the five bad sequences. Identify, at the reward of, 2T+I, for each pair, a nonrandom property for each set and identify which sequence in each pair was produced by the bad generator.

[1] Of course this notion is imprecise. We mean a fairly natural property that appears with very low probability (lower than 10^{-6} for a truly random sequence.

3 (13T) Let us study provable properties of pseudorandom generators in the complexity-theoretic setting.

Suppose that you have pseudorandom generator G_1 that achieves a minimal stretch in that it takes output n bits and produced $n+1$ bits as output. Suppose it is cryptographically strong that for any polynomial P, for any distinguisher D that runs in time $P(n)$ we have

$$|Pr[D(y) = 1] - Pr[D(G_1(x)) = 1]| \leq \frac{1}{P(n)}$$

.

Show, how to for any fixed polynomial $m = m(n)$ to construct (3T) a generator G_m that on input n bits outputs $n + m$ bits and which is also cryptographically strong in the same sense. Also supply (10T) a formal (and correct) proof that your claimed generator has the given properties.

4 (7I) Implement the recovery phase of Feldman's verifiable secret sharing scheme. A detailed description is found on Kattis. `https://kth.kattis.scrool.se/problems/feldman`. Make sure that your code is commented and well structured. Up to 7I points may be subtracted if this is not the case. Keep in mind that you must be able to explain your solution during the oral exam.

5 (10T) This is a loosely specified essay problem where you are supposed to speculate about the future given some understanding of the present (and of course include some references on how things are right now). The expected length of the answer is 1-3 pages of printed text.

Read the chapter on Public Key Infrastructures (PKI) in the book by Stinson (or any other source). As you will notice PKIs are about making sure that a certain public key belongs to a certain user. They are nice in theory but not fully implemented on today's Internet. One interesting alternative to a PKI is, in some circumstances, Identity Based Encryption (IBE) where the public key of each user is simply her/his identity in the system (one alternative might be the email address or other unique string). Assuming that there are no technical inventions that fundamentally changes the scenery and that the world looks, politically and economically, in a similar way as today (but of course the world is even more electronically connected), try to reason on how these problems will be solved in 50 years. In particular will we have a fully built up PKI, will we use IBE, or what do you think? Of course there is no correct answer to this problem and thus imagination of the future combined with your technical understanding of the situation today combined with sound reasoning is what is to be demonstrated in this problem.