T-79.159 Cryptography and Data Security **Spring 2003**
Home Assignment 2

To be returned by April 28 12:00 to the box next to room B336 in the 3rd floor of the T building.

Remember to write down:

- The code and name of the course.
- Your full name.
- Student number.

Try to solve at least 4 of 5 problems. Problems are related to lectures 5 – 9 (Public key cryptography – Pseudorandomness, Provable Security).

Markku-Juhani O. Saarinen `<mjos@tcs.hut.fi>` and Johan Wallén `<johan@tcs.hut.fi>` will be happy to help with the problems.

1. Recall (from lecture 5) that the standard Weierstrass form of an elliptic curve over an field with characteristic greater than 3 is $y^2 = x^3 + ax + b$. Rule for adding two distinct points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ is

$$\begin{aligned} \lambda &= \frac{y_2 - y_1}{x_2 - x_1} \\ P + Q &= (x_3, y_3) = (\lambda^2 - x_1 - x_2, \lambda(x_1 - x_3) - y_1). \end{aligned}$$

Similarly the double point $P + P = 2 * P$ can be computed as:

$$\begin{aligned} \lambda &= \frac{3x_1^2 + a}{2y_1} \\ 2 * P &= (x_3, y_3) = (\lambda^2 - 2x_1, \lambda(x_1 - x_3) - y_1). \end{aligned}$$

Using these equations and a binary "exponentiation" algorithm, we may compute any multiple $n * P$ of point P efficiently.

We define an elliptic curve over the finite field $\mathbb{Z}_p, p = 997$ by setting $a = 3$ and $b = 5$. Furthermore we define one particular point, $P = (1, 3)$.

a) Is P on the given elliptic curve ?

b) What is the order of the group ? [1]

c) Assume that the point $Q = (2, 824)$ is on the curve as well. If we take P as the generator, what is the discrete logarithm of Q ? [2]

[1] Order of the group may be defined as smallest $n > 0$ such that $(n + 1) * P = P$. Note that if n is the order of P, then $n * P$ is the identity element ("point at infinity"), which is *not* on the curve. Computing λ gives a division at zero at this point, so be careful. Obviously, $(k * n + 1) * P = P$ holds for any k.

[2] You need to find the smallest n so that $n * P = Q$.

2. Design a secure authentication protocol based on RSA signatures and hash functions (you may assume that the primitives work; you don't have to care about such things as message padding etc).

   Here Alice is trying to identify herself to Bob. Bob already has Alice's public key from a trusted source. Alice and Bob then exchange messages over an insecure channel, where an active attack may take place.

3. Present in reasonable detail a computational zero knowledge protocol for the **NP**-complete graph 3-colouring problem (e.g. based on the one from the lectures). In particular, explain the following:

   - What assumptions are you using? (Commitment schemes, encryption schemes, ...)
   - Why is your protocol complete? Give a lower bound for the probability that the verifier accepts if the prover indeed knows a 3-colouring of the graph.
   - Why is your protocol sound? Give an upper bound for the probability that the verifier accepts if the graph is not 3-colourable.
   - Why is the protocol zero knowledge? You do not have to give a proof—an intuitive explanation is enough.

4. Implement Shamir's (t, n)-threshold secret sharing scheme over the field $\mathbb{Z}_p$.

   (a) Test your program by reconstructing the secret from the shares

   $$\begin{array}{cccc} (3, 2329) & (7, 1323) & (28, 51) & (93, 17) \\ (113, 239) & (172, 11211) & (2368, 52572) & (4993, 6485) \end{array}$$

   when the parameters are $(t, n) = (5, 8)$ and $p = 2^{16} + 1$ (the shares are given in the form $(x, f(x))$, where f is the sharing polynomial). Test that you get the same secret for several different subsets of 5 shares.

   (b) Determine the share with first coordinate 10000. That is, compute $f(10000)$, where f is the sharing polynomial.

5. As mentioned during the lectures, pseudorandom generators (PRG) exists if and only if one-way functions (OWF) exists, and pseudorandom functions (PRF) exists if and only if PRGs exists. This problems deals with the easier parts of these claims. Namely, show that

   (a) The existence of PRGs implies the existence of OWFs and

   (b) The existence of PRFs implies the existence of PRGs.

   In both parts, describe your construction in detail and explain (or prove) why the construction works.

   (Hint: For 5a, consider very simple constructions. They will probably work. For 5b, think about block cipher modes.)