Cryptography, winter 2013/2014

Prof. Dr. Joachim von zur Gathen, Dr. Daniel Loebenberger

8. Exercise sheet
Hand in solutions until Saturday, 04 January 2014, 23:59:59

Exercise 8.1 (Empirical security). (10 points)

The ElGamal signature scheme works over some publicly known group of (often prime) order ℓ, where ℓ has length n. In many cases this is a subgroup of some $\mathbb{Z}_p^\times$ with another (larger) prime p; then $\ell | (p-1)$. However, it is necessary for its security that it is difficult to compute a discrete logarithm in the group and also, if applicable, in the surrounding group $\mathbb{Z}_p^\times$. The best known discrete logarithm algorithms achieve the following (heuristic, expected) running times:

method	year	time for a group size of n-bit
brute force (any group)	$-\infty$	$\mathcal{O}^\sim(2^n)$
Baby-step Giant-step (any group)	1971	$\mathcal{O}^\sim\left(2^{n/2}\right)$
Pollard's ϱ method (any group)	1978	$\mathcal{O}\left(n^2 2^{n/2}\right)$
Pohlig-Hellman (any group)	1978	$\mathcal{O}^\sim\left(2^{n/2}\right)$
Index-Calculus for $\mathbb{Z}_p^\times$	1986	$2^{(\sqrt{2}+o(1))n^{1/2}\log_2^{1/2} n}$
Number-field sieve for $\mathbb{Z}_p^\times$	1990	$2^{((64/9)^{1/3}+o(1))n^{1/3}\log_2^{2/3} n}$

It is not correct to think of $o(1)$ as zero, but for the following rough estimates just do it. Estimate the time that would be needed to find a discrete logarithm in a group whose order has n-bits assuming the (strongest of the) above estimates are accurate with $o(1) = 0$ (which is wrong in practice!)

(i) for $n = 1024$ (standard size), $\boxed{1}$

(ii) for $n = 2048$ (as required for Document Signer CA), $\boxed{1}$

(iii) for $n = 3072$ (as required for Country Signing CA). $\boxed{1}$

Repeat the estimate assuming that for the given group only Pollard's ϱ method is available, for example in case the group is a ℓ-element subgroup of $\mathbb{Z}_p^\times$ or an elliptic curve,

(iv) for $n = 160$, $\boxed{1}$

(v) for $n = 200$, $\boxed{1}$

(vi) for $n = 240$. $\boxed{1}$

In June 2005, Antoine Joux and Reynald Lercier reported (`https://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind0506&L=nmbrthry&T=0&P=20`) that they can solve a discrete logarithm problem modulo a 431-bit prime p within three weeks, using a 1.15 GHz 16-processor HP AlphaServer GS1280 computer and a number field sieve algorithm.

(vii) Which bit size for the prime p is necessary to ensure that they cannot solve the DLP problem in $\mathbb{Z}_p^\times$ given —say— 10'000 10GHz computers and 1 year (disregarding memory requirements). $\boxed{4}$

[Note: The record for computing discrete logs in $\mathbb{F}_{2^n}^\times$ lies at $n = 6168$, see Antoine Joux `https://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind1305&L=NMBRTHRY&F=&S=&P=3034`.]

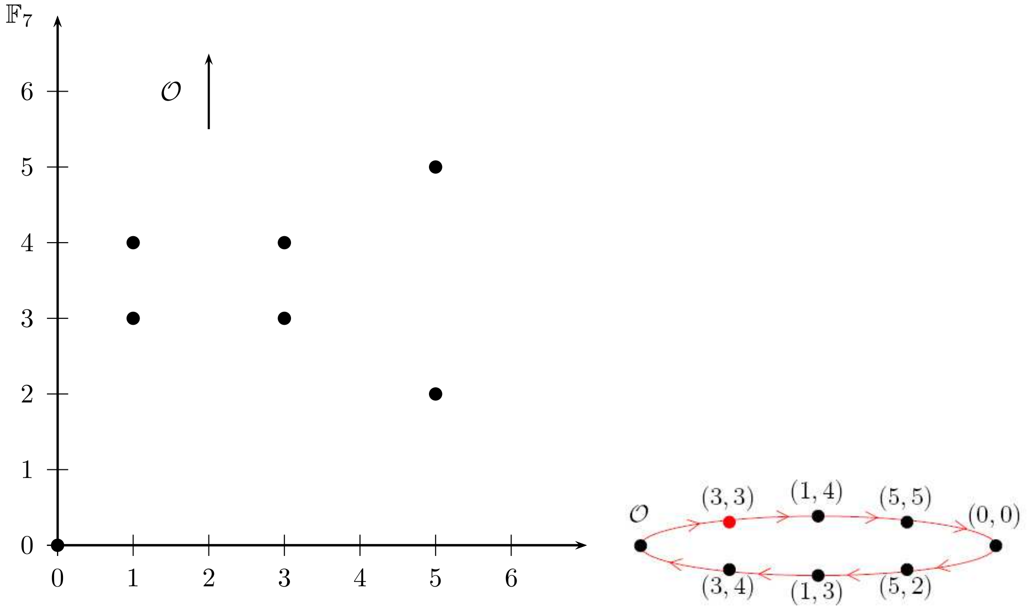

Figure 8.1: Graph and diagram for the group structure of E

Exercise 8.2 (Working in elliptic curves). (5+4 points)

Consider the example $E = \{(u, v) \in \mathbb{F}_7^2 : v^2 = u^3 + u\} \cup \{\mathcal{O}\}$ for an elliptic curve over $\mathbb{F}_7$ from the lecture (see Figure 8.1).

$\boxed{2}$ (i) Let $P = (5, 5)$. Determine $S = 2 \cdot P$ and $T = 5 \cdot P$ from the diagram on the right of Figure 8.1.

The addition of two distinct points corresponds to a secant of the graph. The doubling of a point corresponds to a tangent to the graph.

$\boxed{2}$ (ii) Draw the tangent corresponding to $S = 2 \cdot P$ into the graph on the left of Figure 8.1.

$\boxed{1}$ (iii) Determine $S + T$ from the graph on the left and check your result by doing the same computation in the diagram on the right.

ALICE and BOB heard about the cryptographic applications of elliptic curves. They want to perform a DIFFIE-HELLMAN key exchange using the elliptic curve E.

$\boxed{+1}$ (iv) List all possible generators for the cyclic group E.

ALICE and BOB publicly agree on the generator P from above. The secret key of ALICE is 3 and the secret key of BOB is 4.

$\boxed{+3}$ (i) Which messages are exchanged over the insecure channel and what is ALICE's and BOB's common secret key?

Exercise 8.3 (MERKLE-DAMGÅRD construction). (4 points)

Modify h^* in the MERKLE-DAMGÅRD construction as follows:

(i) Drop the last y_i and show how to construct a collision for h^* without having one for h. $\boxed{2}$

(ii) Omit the final bit for all y_j and show how to construct a collision for h^* without having one for h, but with the assumption that $h(0 \ldots 0) = 0 \ldots 0$. $\boxed{2}$

Exercise 8.4. (0+7 points)

You and your bank want to agree on a common key via the `Diffie-Hellman protocol` in a multiplicative group $\mathbb{Z}_p^\times$. You know that in order to do so, a *large* prime number p has to be chosen and a generator for the multiplicative group $\mathbb{Z}_p^\times$ has to be determined. These may be tedious tasks. $\boxed{+7}$

As part of their Christmas campaign, the hardware company PIERPONTPRIMESUNLIMITED advertises their exceptionally fast and cheap hardware for computations in specific multiplicative groups $\mathbb{Z}_p^\times$. Your bank has received a tempting offer, where p is the following 1024-bit prime number:

```
107313728214633881402529727601234051403339214228664318228\
594610689786788510081514444448995981953428599841775383351\
951139720719345087913170517242877080174958539637745468107\
816500403651171504387721743806870756270010931915093460113\
178239400149273770492545819805495452964968476117438596882\
036667823702963803652097
```

Of course, a long list of generators is included, so they would also spare themselves the work of searching for one of those.

Now, your bank turns to you: Since those two pieces of information (the chosen group and the chosen generator) are public anyways, there seems to be no reason to reject this offer.

Reply to this and justify your answer. (You may assume that the hardware really does the computations as claimed and nothing else.)

(Hint: To spare you the nuisance of copying 309 decimal digits, there is a text-file containing p on the course-webpage.)