Cryptography I, winter 2005/06

JOACHIM VON ZUR GATHEN, MICHAEL NÜSKEN

10. Exercise sheet
Hand in before Monday, 2006/01/30, 14^{00} in b-it 1.22.

Exercise 10.1 (ElGamal signatures). (4 points)

We choose a prime number $p = 12347$ and the group $G = \mathbb{Z}_p^\times$. We use $a = 9876$ as the secret part of the key $K = (p, g, \beta, a)$. The message x to be signed consists of the last four digits of your student registration number. Use $k = 399$ as your random number from $\mathbb{Z}_{p-1}^\times$.

(i) Show: $g = 2$ generates G. Compute $\beta = g^a \in G$. $\boxed{2}$

(ii) Compute the signature $\mathrm{sig}_K(x, k) = (x, \gamma, \delta)$. Here $\gamma = g^k \bmod p$ and $\delta = (x - a\gamma)k^{-1} \bmod (p-1)$. Verify your signature. $\boxed{2}$

Exercise 10.2 (A mysterious equation). (3+2 points)

Let $p \in \mathbb{N}$ be a prime number. The central operation in verifying an ElGamal signature is checking the equation $g^x = \beta^\gamma \cdot \gamma^\delta$ in $\mathbb{Z}_p$, where $g, \beta, \gamma \in \mathbb{Z}_p^\times$ and $\delta \in \mathbb{Z}_p$ and $x \in \{0, 1, \ldots, p-1\}$ is the message or its hash, respectively. For now we consider the somewhat simpler congruence

(*) $$g^x = \beta^\gamma \cdot \gamma \quad \text{in } \mathbb{Z}_p$$

with $g, \beta \in \mathbb{Z}_p^\times$, $\gamma \in \mathbb{Z}_{p(p-1)}$ and $x \in \mathbb{N}$, $0 \le x \le p-1$.

(i) Show: $\gamma = g^x(1-p) \text{ rem } (p^2 - p)$ is a solution to the equation (*). $\boxed{1}$

(ii) It holds that $\mathbb{Z}_{p(p-1)} \cong \mathbb{Z}_p \times \mathbb{Z}_{p-1}$. We identify $\mu \in \mathbb{Z}$, $0 \le \mu < p$ with $(\mu, 0) \in \mathbb{Z}_p \times \mathbb{Z}_{p-1}$. Let μ be a solution to congruence (*). For which $\ell \in \mathbb{Z}_{p-1}$ is there a $\lambda \in \mathbb{Z}_p$ so that also $(\mu \cdot \lambda, \ell) \in \mathbb{Z}_p \times \mathbb{Z}_{p-1}$ is a solution to (*)? Compute the dependency of λ on ℓ for that case. $\boxed{1}$

(iii) Is $\mathrm{sig}_K(x) = (x, g^x(1-p), 1)$ a legal ElGamal signature? What is the consequence of this discovery for the practical use of the ElGamal signature scheme? $\boxed{1}$

(iv*) How many solutions γ are there for the congruence (*) and fixed g, β, x, p? $\boxed{+2}$

Exercise 10.3 (DSA Practice). (10 points)

In this exercise you will make practical computations with the DSA algorithm, using *real life* key sizes.

$\boxed{1}$ (i) Generate a random prime number q with exactly 160 bits.

$\boxed{1}$ (ii) Generate a prime p with exactly 1024 bits, such that q divides $p - 1$.

$\boxed{1}$ (iii) Find a $g \in \mathbb{Z}_p^\times$ which has the exact order q. Let $G = \langle g \rangle \subset \mathbb{Z}_p^\times$ be the cyclic group with q elements generated by g.

$\boxed{1}$ (iv) Let $a < p$ be a random number and $y = g^a \in G$. We shall consider a to be Alice's secret key and y her public key.

$\boxed{2}$ (v) Let $m \in \mathbb{Z}_q$ be the integer value of the ASCII text: `DSA␣for␣real` (note the two blanks in the text!). Using a random number $k \in \mathbb{Z}_q$ produce a DSA signature $S(m) = (m, x, b)$ on the message m on behalf of Alice.

$\boxed{1}$ (vi) Let Bob know the public key (p, g, y). Verify the signature $S(m)$ on behalf of Bob.

$\boxed{1}$ (vii) Let m' be the integer value of the ASCII text:

`The␣Lord␣of␣the␣Rings␣has␣no␣secrets.`

Can you produce a DSA signature of this text using the same setting as above? If no, what additional steps are required?

$\boxed{2}$ (viii) The DSA system can be attacked in two different ways:

(a) By solving the index problem in the group G iwth q elements, with the baby-step giant step algorithm (or the Pollard-ϱ method) in this group.

(b) By solving the general discrete logarithm problem in $\mathbb{Z}_p^\times$, using the up to date Number Field Sieve. The complexity of this method is given by the function:

$$L(p) = \exp\left(1.992 \cdot \left(\log p \cdot (\log\log p)^2\right)^{1/3}\right).$$

The function log is the natural logarithm.

Compare the two estimated times, when $p \sim 2^{1024}$ and $q \sim 2^{160}$.