Electronic passport and biometrics, winter 2006

MICHAEL NÜSKEN

3. Exercise sheet
Hand in solutions until Tuesday, 21 November, $12^{\underline{15}}$.

Exercise 3.1 (Diffie Hellman key exchange). (5+1 points)

Perform a toy example of a Diffie Hellman key exchange: Fix $p = 47$ and $g = 2 \in \mathbb{Z}_p^\times$.

(i) Show that the order of g is 23. (Recall the order of g is the number of elements in the subgroup $\langle g \rangle = \{1, g, g^2, \dots\}$ of $\mathbb{Z}_p^\times$ generated by g.) [1]
[If you are clever then you only need to calculate g^{23}.] [+1]

(ii) Choose $x \in \mathbb{Z}_{23}$ (take $x \notin \{0, 1\}$ to get something interesting) and calculate $h_A := g^x$. [1]

(iii) Choose $y \in \mathbb{Z}_{23}$ (take $y \notin \{0, 1, x\}$ to get something interesting) and calculate $h_B := g^y$. [1]

(iv) Now compute h_B^x and h_A^y and compare. [2]

Exercise 3.2 (ElGamal signatures). (7 points)

Compute a signature for the document $010101 \in \{0,1\}^*$. Use $p = 263$ and $g = 2 \in \mathbb{Z}_p^\times$ and work in $G = \langle g \rangle$. For simplicity, we take the function $\mathrm{HASH}\colon \{0,1\}^* \to \mathbb{Z}_{131},\ x \mapsto (\sum_{0 \le i < |x|} x_i 2^i) \bmod 131$.

(i) Here $\#G = 131$ and thus $\exp_g\colon \mathbb{Z}_{131} \to G,\ a \mapsto g^a$ is an isomorphism. [1]
[Note that $23^2 = 2$ and thus $g^{131} = 1$. Since $g \neq 1 \dots$]

(ii) Setup: Compute Alice' public key with $\alpha = 9$. [1]

(iii) Sign: Sign the hash value 42 of your document 010101. [3]

(iv) Verify: Verify the signature. [2]

Exercise 3.3 (A mysterious equation). (0+6 points)

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

(*) $$g^x \equiv \beta^\gamma \cdot \gamma \bmod p$$

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

+1 (i) Show: $\gamma = g^x(1-p)$ rem (p^2-p) is a solution to congruence (*).

+2 (ii) It holds that $\mathbb{Z}_{p(p-1)} \cong \mathbb{Z}_p \times \mathbb{Z}_{p-1}$. We identify $\mu \in \mathbb{Z}$, $0 \leq \mu < p$ 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.

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

+1 (iv) Extra credit: How many solutions γ are there for the congruence (*) and fixed g, β, x, p?