Cryptography, winter 2014/2015

PRIV.-DOZ. DR. ADRIAN SPALKA, DR. DANIEL LOEBENBERGER

6. Exercise sheet
Hand in solutions until
Wednesday, 10 December 2014, 23:59:59

Exercise 6.1 (Schnorr identification, example). (10 points)

As in the Schnorr signature scheme, we use a subgroup $G \subseteq \mathbb{Z}_p^\times$ of small order q inside the much larger group $\mathbb{Z}_p^\times$. Specifically, we take $q = 1201$, $p = 122503$, and $g = 11538$. Alice uses the Schnorr identification scheme in G.

(i) Alice's secret exponent is $a = 357$. Compute her public key A. [1]

(ii) Alice chooses $b = 868$. Compute B. [1]

(iii) Bob issues the challenge $c = 501$. Compute Alice's response r. [1]

(iv) Perform Bob's calculations to verify r. [1]

(v) Perform the entire scheme in a programming language of your choice with $2^{1023} \leq p < 2^{1024}$ and $2^{159} \leq q < 2^{160}$. Hand in transcripts of your program. Hint: Use your favorite computer algebra system! A nice, free one, which feels a lot like Python is the system sage, see `http://www.sagemath.org`. [6]

Exercise 6.2 (Attacks on Schnorr identification). (6 points)

(i) EVE somehow subverted BOB's random number generator and is able to correctly predict the challenge BOB will give to her. Show how EVE can produce a response $r \in \mathbb{Z}_d$ which Bob will accept. [2]

(ii) EVE has intercepted two Schnorr identifications by Alice and now knows (B_1, c_1, r_1) and (B_2, c_2, r_2). Furthermore, EVE somehow knows $\mathrm{dlog}_g(B_1^k B_2^{-1})$ for some k.

(a) Show that Eve can easily compute Alice's secret exponent a. [Hint: Look at the case $k = 1$ first.] [2]

(b) EVE knows Alice's software dealer and has purchased the same identification software from him. This way she learned that Alice uses a linear congruential generator to generate her random secret numbers b. Such a generator computes for any $i > 0$ values $b_{i+1} = sb_i + t$ in $\mathbb{Z}_q$ for known values of q, $s \in \mathbb{Z}_q^\times$, and $t \in \mathbb{Z}_q$ using seed $b_0 \in \mathbb{Z}_q$. (The programmer has used q as the modulus for the random generator so that the numbers b_i are automatically in the correct range.) Show how EVE can compute $\operatorname{dlog}_g(B_1^k B_2^{-1})$ for a specific value of k and by (ii.a) also Alice's secret exponent a. 2

Exercise 6.3. (4+5 points)

Consider the following identification protocol:

Algorithm. Okamoto's identification scheme.

Input: Publicly known $G = \langle g_1 \rangle = \langle g_2 \rangle$, d, ID(Alice), and $A = g^{a_1} g^{a_2}$.
Known to Alice: C_{Alice}.

1. Alice chooses $b_1, b_2 \in \mathbb{Z}_d$ at random and sends her certificate $C_A = (\text{ID(Alice)}, A, s)$ and $B = g_1^{b_1} g_2^{b_2}$ to Bob.
2. Bob verifies that $\text{ver}_{\text{TA}}((\text{ID(Alice)}, A), s) =$ "true" and chooses $c \xleftarrow{\$} \mathbb{Z}_d$.
3. Alice sends

$$r_1 = b_1 + a_1 c \quad \text{and} \quad r_2 = b_2 + a_2 c \text{ in } \mathbb{Z}_d$$

to Bob.
4. Bob verifies that $BA^c = g_1^{r_1} g_2^{r_2}$.

1 (i) Prove that the protocol is correct, i.e. if properly executed, Bob will accept Alice's identification.

3 (ii) Prove that if Eve has a value B for which she can impersonate Alice for at least two values of c, then Eve can easily compute $e_1, e_2 \in \mathbb{Z}_d$ such that $A = g_1^{e_1} g_2^{e_2}$.

+5 (iii) Prove that if Eve has a value B for which she can impersonate Alice for at least two values of r, then Alice and Eve together can, with probability at least $1 - d^{-1}$, easily compute $k = \operatorname{dlog}_{g_2} g_1$.