Cryptography I, winter 2005/06

JOACHIM VON ZUR GATHEN, MICHAEL NÜSKEN

11. Last exercise sheet
Hand in before Monday, 2006/02/06, 14^{00} in b-it 1.22.

Exercise 11.1 (Identification, chronological order). (1 points)

We simplify the Schnorr identification scheme: Bob sends the challenge r and Alice answers with $C(A)$, γ und y. [1]

Explain why Bob should not verify Alice' identity like this.

Exercise 11.2 (Schnorr identification, example). (5+3 points)

Alice uses the Schnorr identification scheme with $q = 1201$, $p = 122503$, $t = 10$ and $\alpha = 11538$.

(i) Verify that $\alpha \in \mathbb{Z}_p^\times$ has order q. [This should be done using a polynomial time algorithm!] [1]

(ii) Alice' secret exponent is $e_A = 357$. Compute her public key β_A. [1]

(iii) Alice chooses $k = 868$. Compute γ. [1]

(iv) Bob issues the challenge $r = 501$. Compute Alice' response y. [1]

(v) Simulate Bob's calculations to verify y. [1]

(vi) Perform the entire scheme in MuPAD (or any other appropriate system) with $2^{1023} \leq p < 2^{1024}$ and $2^{159} \leq q < 2^{160}$. [+3]

Exercise 11.3 (Schnorr identification, attack). (4 points)

(i) Eve has intercepted two Schnorr identifications by Alice and now knows (γ_1, r_1, y_1) and (γ_2, r_2, y_2). Furthermore Eve has ensured that she knows $z := \mathrm{dlog}_\alpha(\gamma_1^a \gamma_2^{-1})$ for some a. Show that she can easily compute Alice' secret exponent e_A. [*Hint*: Look at the case $a = 1$ first.] [2]

(ii) Eve knows Alice' software dealer and has purchased the same idenfication software from him. This way she learned that Alice uses a linear congruential generator to generate her random, secret numbers k_i. Therefore it holds that $k_2 = (ak_1 + b)$ rem q for known values of $a \in \mathbb{Z}_q^\times$, $b \in \mathbb{Z}_q$. (The programmer has used q as the modulus for the random generator so that the numbers k_i are automatically in the correct range.) Show how Eve can compute the discrete logarithm $z = \text{dlog}_\alpha(\gamma_1^a \gamma_2^{-1})$. (And thus also Alice' secret exponent e_A!) [2]

Exercise 11.4 (Okamoto identification). (4 points)

Alice uses Okamoto's identification scheme with $q = 1201$, $p = 122503$, $t = 10$, $\alpha_1 = 60497$ and $\alpha_2 = 17163$.

[1] (i) Alice' secret exponents are $e_1 = 432$ and $e_2 = 423$. Compute β_A.

[1] (ii) Alice chooses $k_1 = 389$ and $k_2 = 191$. Compute γ.

[1] (iii) Bob issues the challenge $r = 21$. Compute Alice' response (y_1, y_2).

[1] (iv) Simulate Bob's calculations to verify y.

Exercise 11.5 (Attack on Okamoto identification). (0+4 points)

Alice uses Okamoto's identification scheme with the same parameters as in Exercise 11.4. Furthermore let $\beta_A = 119504$.

[+1] (i) Eve has discovered that the equality

$$\alpha_1^{70}\alpha_2^{1033}\beta_A^{877} \equiv \alpha_1^{248}\alpha_2^{883}\beta_A^{992} \bmod p$$

holds. Verify this.

[+1] (ii) Use this information to find numbers b_1 and b_2 satisfying

$$\alpha_1^{b_1}\alpha_2^{b_2} \equiv \beta_A \bmod p.$$

[+2] (iii) Alice makes common cause with Eve and gives Eve her secret exponents $e_1 = 717$ and $e_2 = 266$. Show how Alice and Eve together can compute $\text{dlog}_{\alpha_1} \alpha_2$.