Cryptography, winter 2013/2014

PROF. DR. JOACHIM VON ZUR GATHEN, DR. DANIEL LOEBENBERGER

12. Exercise sheet
Hand in solutions until Saturday, 01 February 2014, 23:59:59

Exercise 12.1 (Secure email). (4 points)

(i) Send a digitally signed email with the subject [2]

`World supremacy plans`

to us at

`13ws-crypto-handin@lists.bit.uni-bonn.de`

from your personal account. The body of your email must be nonempty and the signature must be verifiable and correct. [It is a good idea to verify this by sending a blind carbon copy (Bcc) to oneself.]

With Thunderbird we recommend using `enigmail` and `gpg`. In any case make sure to register your key at `http://pgp.mit.edu/`.

Choose yourself among this solution and possible others. In any case use a pgp key pair.

(ii) Find the fingerprint of your own PGP key. Bring two printouts of it and an identification document to the next tutorial. (Do not send an email with it. Guess, why!) [2]

Exercise 12.2 (Security of ElGamal encryption). (8 points)

Fix a finite group $G = \langle g \rangle$ with order $d = \#G$, a secret key $a \in \mathbb{Z}_d$ and a public key $A = g^a \in G$.

(i) Show that ElGamal encryption over G is malleable under key-only attacks. [4]

(ii) Show that ElGamal encryption over G is decipherable under chosen-ciphertext attacks. [4]

Hint: ElGamal encryption enjoys a homomorphic property, namely that for messages $m_1, m_2 \in G$, we have $\mathrm{enc}_A(m_1) \cdot \mathrm{enc}_A(m_2) = \mathrm{enc}_A(m_1 \cdot m_2)$.

Exercise 12.3 (Schnorr identification, example). (4+4 points)

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

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

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

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

[+4] (v) Perform the entire scheme in a computer algebra system of your choice with $2^{1023} \leq p < 2^{1024}$ and $2^{159} \leq q < 2^{160}$.

Exercise 12.4 (Attack on Schnorr identification). (4 points)

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

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

[2] (ii) 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. Therefore $b_2 = sb_1 + t$ in $\mathbb{Z}_q$ for known values of q, $s \in \mathbb{Z}_q^\times$, and $t \in \mathbb{Z}_q$. (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 (i) also Alice's secret exponent a.

Exercise 12.5 (Teach!). (0+10 points)

[+10] Consider the material covered this winter term. Invent some good questions you would ask in a written exam.