The electronic health card, summer 2008

MICHAEL NÜSKEN, DANIEL LOEBENBERGER

5. Exercise sheet
Hand in solutions until Monday, 26 May 2008.

Exercise 5.1 (ElGamal Encryption). (7 points)

Let p be a prime number. We implement the ElGamal encryption scheme using the group $G = \mathbb{Z}_p^\times$. A is mapped to 0, B to 1 and so forth, Z is mapped to 25. We combine groups of three letters (a_0, a_1, a_2) to $a_0 + 26a_1 + 26^2 a_2$. Thus ABC corresponds to the value $0 + 26 \cdot 1 + 2 \cdot 26^2 = 1378$.

(i) For $a \in G$ holds: a is an element of order d in G if and only if $a^d = 1$ and $a^{d/t} \neq 1$ for all divisors $t > 1$ of d. $\boxed{2}$

Furthermore: An element $a \in \mathbb{Z}_p^\times$ is an element of order d in G if and only if $a^{d/t} \neq 1 \pmod{p}$ holds for all *prime* divisors t of d.

(ii) Using this show that 23 has order 24391 in $\mathbb{Z}_{146347}^\times$. Note that $146347 = 2 \cdot 3 \cdot 24391$. $\boxed{1}$

(iii) Encrypt the word "SYSTEM" using the ElGamal scheme. Use the group $G = \mathbb{Z}_{146347}^\times$ and the element $g = 23$. The receiver of the message has published the public key $a \leftarrow g^\alpha = 76441$. Choose your public key to be $b \leftarrow g^\beta$ with $b = 99970$. $\boxed{2}$

(iv) The following transcript of a conversation was intercepted, which contains a message encrypted with the ElGamal system (using the mapping from letters to numbers described above). Once more we have $G = \mathbb{Z}_{146347}^\times$ and $g = 23$: $\boxed{2}$

ALICE	has the public key 94645.
BOB to ALICE:	message (part 1) $(19053, 39572)$.
BOB to ALICE:	message (part 2) $(19053, 37442)$.
BOB to ALICE:	message (part 3) $(19053, 1752)$.

An indiscretion revealed that one part of the message corresponds to the clear text (value) 8324. Compute the (alphabetic) clear text of the entire message.

Exercise 5.2 (RSA signatures). (15+2 points)

Compute an RSA signature!

1 (i) Generate random RSA keys with N about 30 Bits. Keep the private key (N, d) secret and tell only the public key.

2 (ii) You are given a document, say x is your student identification number. Compute $y \leftarrow x^d$ in $\mathbb{Z}_N$.

2 (iii) Verify that $y = x^d$ without using the secret key. [So you may only use the public key here!]

4 (iv) Give a defintion explaining when y is a signature of x.

2 (v) Explain how a signature on xr^e can be used to get a signature on x.

4 (vi) Use the previous to decide whether the scheme is good (secure) or not. Prove it!

+2 (vii) Explain why using the same RSA key for encryption and signing is a very bad idea in practice.

Exercise 5.3 (RSA-signatures and hash functions). (6 points)

6 Consider the RSA signature scheme with a hash function h. Assume that the attacker can find a second preimage of h, ie. given one document x he can find a second document $y \neq x$ with $h(x) = h(y)$. Prove that the attacker can then break the scheme. Conclude a theorem: "If RSAsign(h) is secure then $h \ldots$".

Exercise 5.4 (Diffie-Hellman versus ElGamal). (2 points)

2 Prove that being able to distinguish two plaintexts by an ElGamal encryption (of one of two chosen plaintexts) implies breaking the decisional Diffie-Hellman problem in G. [We play the following game: We are given $(g, b, c, d) = (g, g^\beta, g^\gamma, g^\delta)$. Then we give a public key a to the attacker who will return two plaintexts x_0, x_1. We encrypt one of these and send its encryption (t, y) to the attacker. The attacker then returns which x_i we sent him (with high probability). Show that you can use this to check whether $\delta = \beta\gamma$.]