Mathematical Cryptology 2013

Dept. of EIT
Lund University
Box 118, 221 00 Lund, Sweden

WEEK 5,

Reading instructions:

- Chapter 24-25, 17
- Chapter 18 (read through)
- Chapter 19

There will be 4 hours of lectures covering the above.

Hand-in exercises:

1) Review exercises: 24-25, 19

2) Standard exercises: 16,17

3) Programming exercise: -

Hand in no later than **March 7, 2013.**

Ch 24-25: Review exercises:
24.1 What is a committment scheme?
24.2 What does it mean for a committment scheme to be binding or concealing?
25.3 How can a zero-knowledge protocol for proof of knowledge be used as an identification scheme?
25.4 In the protocol for graph isomorphism, show that if Peggy produces the same graph H in two different runs of the protocol, then Victor can determine the secret graph isomorphism.
25.5 How do you turn an interactive zero-knowledge identification scheme into a digital signature scheme?

Ch 24-25: Standard exercises:
24.6 Given a group G and four elements g_1, g_2, h_1, h_2, suppose Peggy knows that

$$log_{g_1}(h_1) = log_{g_2}(h_2) = x$$

and that Peggy knows x. Give a protocol for Peggy to convince Victor that not only she knows the discrete logarithm but that the two discrete logarithms are equal.
25.7 Show that the zero-knowledge proof of validity for the committment $B_a(x)$ given in the text for when $x \in \{-1, 1\}$ satisfies the three requirements.

Ch 17: Review exercises:
17.1 How does one compute the continued fraction expansion of a real number α?
17.2 In Wiener's attack on small private exponent RSA, what number does one compute the continued fraction of?
17.3 What is a lattice?
17.4 What do you think is the most important property of an LLL reduced lattice basis, from the point of view of a cryptographer?
17.5 Suppose I have the equation $f(x_0) = 0 \pmod N$ where f is a polynomial of degree d. How small must x_0 be before Coppersmith's method will find it in polynomial time?
17.6 Explain Håstad's attack on RSA.

Ch 17: Standard exercises:
17.7 Show that for an LLL reduced basis of an n-dimensional lattice L, if x is a nonzero vector in L then

$$||b_1|| \leq 2^{(n-1)/2}||x||.$$

Ch 18: Review exercises:
18.1 What is meant by semantic security, and how does this relate to perfect security?
18.2 Give the definition of polynomial security.
18.3 What restriction is put on the decryption oracle in an adaptive chosen ciphertext attack?
18.4 Give two problems with the RSA algorithm as described in earlier chapters.

Ch 19: Review exercises:
19.1 Describe the complexity classes $\mathcal{P}, \mathcal{NP}, \rfloor\wr - \mathcal{NP}$.
19.2 What is a super-increasing knapsack?
19.3 How does the Merkle-Hellman cryptosystem translate a super-increasing knapsack into a hard knapsack problem?

19.4 What is meant by a hard predicate for a function and how is this concept related to the concept of semantic security?
19.5 Explain the difference between a Monte-Carlo, an Atlantic City and a Las Vegas algorithm.