Institut for Matematik og Datalogi
Syddansk Universitet

May 1, 2011
JFB

Cryptology – F11 – Week 11

Announcement

There will be a "pizza meeting" for all students of IMADA on Tuesday, May 3 from 16:15 to 18:30 in room U49(C).

At the meeting, IMADA will give some short general information on the bachelor and candidate studies, and specific information on the elective courses in mathematics and computer science planned for the next semester.

The meeting will end with free pizza, beer, and soft drinks :)

Lecture, April 28

We continued with zero-knowledge (from the notes by Ivan Damgård and Jesper Buus Nielsen, and another set of notes by Ivan Damgård, both available through the course's homepage).

Lecture, May 4

We will continue with zero-knowledge, from the notes and slides, and begin on chapter 9 in the textbook.

Class cancelled on May 5.

Lecture, May 11

We will finish chapter 9 in the textbook and begin on chapter 10.

Problem sessions May 2 and May 9.

1. Do exercises 1, 3, 4, and 6 in the notes by Damgård and Nielsen.

2. Do exercises 4 and 5 in the notes by Damgård.

3. Let p be a large prime and let $x, y \in Z_p^*$. Suppose that $x = g^k \pmod p$ and $y = h^k \pmod p$. Assume the Prover knows the value k and that both the Prover and the Verifier are given the values p, g, h, x, and y. To show that the discrete logarithm of x with respect to g is equal to the discrete logarithm of y with respect to h, one can execute the following protocol:

Prover		Verifier
Choose random $s \in Z_{p-1}$. Let $u \equiv g^s \pmod p$ $v \equiv h^s \pmod p$.	$\xrightarrow{u, v}$	
		Choose a random $c \in Z_{p-1}$.
	$\xleftarrow{c}$	
Let $e \equiv c \cdot k + s \pmod{p-1}$.		
	$\xrightarrow{e}$	
		Check that $g^e \equiv x^c \cdot u \pmod p$ and $h^e \equiv y^c \cdot v \pmod p$. If so, accept. Otherwise, reject.

---

a. Prove completeness for the above protocol, showing that (assuming that both the Prover and Verifier follow the protocol) the Verifier will accept if the discrete logarithm of x with respect to g is equal to the discrete logarithm of y with respect to h.

b. Prove soundness for the above protocol. Assume that the discrete logarithm of x with respect to g is not equal to the discrete logarithm of y with respect to h. (Hint: after assuming that the Prover can give acceptable answers for two different values of c, show how a transcript containing both executions could be used to find the discrete logarithm of x with respect to g and the discrete logarithm of y with respect to h.)

c. Prove that the above protocol is honest verifier zero-knowledge, i.e., show that one can efficiently generate conversations $((u, v), c, e)$ with the same distribution as produced by the honest Prover and Verifier, without knowing k.

4. The Subgroup Membership Problem is as follows: Given a positive integer n and two distinct elements α, $\beta \in Z_n^*$, where the order of α is l and is publicly know, determine if β is in the subgroup generated by α.

   Suppose that α, β, l, and n are given as input to a Prover and Verifier, and that the Prover is also given k such that $\alpha^k = \beta \pmod{n}$. Consider the interactive protocol in which the following is repeated $\log_2 n$ times:

Prover		Verifier
Choose random $0 \leq j \leq l-1\}$. Compute $\gamma = \alpha^j \pmod{n}$.	$\xrightarrow{\gamma}$	
		Choose a random $c \in \{0, 1\}$.
	$\xleftarrow{c}$	
Compute $h = j + ck \pmod{l}$.	$\xrightarrow{h}$	
		Check that $\alpha^h \equiv \beta^c \gamma \pmod{n}$. If not, reject and halt.

   (a) Prove that the above protocol is an interactive proof system for Subgroup Membership.

   (b) Suppose that β is in the subgroup generated by α. Show that the number of triples (γ, c, h) which the Verifier would accept is

$2l$ and that each such triple is generated with equal probability if both the Prover and Verifier follow the protocol.

(c) Suppose that β is in the subgroup generated by α. What is the distribution of the values γ, h sent by a Prover following the protocol?

(d) Prove that the above protocol is perfect zero-knowledge.

(e) If n is a prime, what value can you use for l? If n is not prime, is it reasonable to make this value l known?

Assignment due Thursday, May 19, 10:15

Note that this is part of your exam project, so it must be approved in order for you to take the exam in June, and you may not work with others not in your group. If it is late, it will not be accepted (though it could become the assignment you redo). You may work in groups of two or three. Submit it through Blackboard.

1. Give a zero-knowledge proof for Vertex Cover. Thus, your input is a graph, G, and a positive integer k, where G has a vertex cover of size at most k. Assume that the Prover knows such a vertex cover. (Hint: Consider the proof given in Damgård's notes for Hamiltonian Circuit.) Note that you should do a direct proof, rather than a reduction to another NP-Complete problem and then doing the zero-knowledge proof for the other problem. Prove that your protocol has the following properties:

   - Completeness
   - Soundness
   - Zero-knowledge

2. Let n be the product of two large primes, $p \equiv q \equiv 3 \pmod 4$. Suppose the Prover knows s pairs, $(x_1, y_1), (x_2, y_2), ..., (x_s, y_s)$, such that $y_i \equiv x_i^2 \pmod n$, for $1 \leq i \leq s$. All of these values are in Z_n^*. The Verifier knows the y_i values, but not the x_i values. The Prover convinces the Verifier that all of the y_i are quadratic residues modulo n by repeating the following protocol $\lceil \log_2 n \rceil$ times:

Prover		Verifier
Choose random $v_1, v_2, ..., v_s \in Z_n^*$. Let $u_i \equiv v_i^2 \pmod{n}$, $1 \leq i \leq s$.		
	$\xrightarrow{u_1, u_2, ..., u_s}$	
		Choose a random $c \in \{0, 1\}$. Choose random $(b_1, b_2, ..., b_s) \in \{0, 1\}^s$.
	$\xleftarrow{c, (b_1, b_2, ..., b_s)}$	
If $c = 0$, let $z = \prod_{i=1}^{s} v_i^{b_i} \pmod{n}$.	$\xrightarrow{z}$	
If $c = 1$, let $z_i \equiv x_i \cdot v_i \pmod{n}$.		
	$\xrightarrow{(z_1, z_2, ..., z_s)}$	
		If $c = 0$, check that $z^2 \equiv \prod_{i=1}^{s} u_i^{b_i} \pmod{n}$ for $1 \leq i \leq s$. If $c = 1$, check that $u_i \cdot y_i \equiv z_i^2 \pmod{n}$ for $1 \leq i \leq s$. If so, accept. Otherwise, reject.

- Prove completeness for the above protocol, showing that (assuming that both the Prover and Verifier follow the protocol) the Verifier will accept if all of the y_is are quadratic residues modulo n.
- Assume that at least one of the u_i is not a quadratic residue modulo n and the Verifier chooses the b_i randomly. What is the probability that the product $\prod_{i=1}^{s} u_i^{b_i}$ is not a quadratic residue modulo n?

- Prove soundness for the above protocol.
- Prove that the above protocol is perfect zero-knowledge.