Institut for Matematik og Datalogi
Syddansk Universitet

April 28, 2003
JFB

Cryptology – F03 – Note 11

Lecture, April 15

We continued with chapter 7, skipping sections 7.5 and 7.7. The description of undeniable signatures will followed that handout given in class.

Lecture, April 29

We will finish undeniable signatures, covering the denial protocol, and begin on protocols. There are handouts for this; it is not in the textbook. Read sections 11.1.3 and 11.1.4 in Goldwasser and Bellare's lecture notes. We will also start on section 11.2.

Discussion section, April 24

We discussed the programming assignment, including the meaning of the confidence level in the primality test, how to choose a generator (or at least a generator of a large subgroup), how k should be chosen, and which methods (subroutines) should know what. We did not get as far as covering problem 3 (problem 4.12 in the textbook), so it will be covered on May 1.

Lecture, May 6

We will continue with zero-knowledge from the notes.

Assignment due Thursday, May 15, 8:30 AM

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. If it is late, it will not be accepted.

Let $p = 4k + 3$ be a prime, and let g and h be quadratic residues modulo p. Assume that h is in the subgroup generated by g and that the Prover knows an x such that $g^x = h \pmod{p}$. Suppose that p, g, and h are given as input to a Prover and Verifier. Consider the interactive protocol in which the following is repeated $\log_2 p$ times:

Prover		Verifier
Choose a random $k \in \{1, ..., \frac{p-1}{2}\}$. Let $z = h \cdot g^{2k} \pmod{p}$.	$\xrightarrow{z}$	
		Choose a random $b \in \{0, 1\}$.
	$\xleftarrow{b}$	
Let $r = 2k + b \cdot x \pmod{p-1}$.	$\xrightarrow{r}$	
		Check that r is even, $z = g^r h^{1-b} \pmod{p}$, $p \pmod{4} = 3$, and $g^{\frac{p-1}{2}} = 1 \pmod{p}$. If not, reject and halt.

(Actually, the last two checks only need to be done once and could be done before the first round of the protocol. Don't let their placement here confuse you.)

a. Prove that the above protocol is an interactive proof system showing that $h = g^{2y} \pmod{p}$ for some integer y.

b. Suppose that $h = g^{2y} \pmod{p}$ for some integer y. What is the probability distribution of the values (z, r) sent by a Prover following the protocol?

c. Prove that the above protocol is perfect zero-knowledge.

d. Suppose $p = 4k + 3$. Note that any quadratic residue g modulo p has odd order. Use this fact to show that if h is in the subgroup generated by a quadratic residue g, then it is always possible to write h as $h = g^{2y} \pmod p$ for some integer y. (Thus, the above protocol is an alternative zero-knowledge proof of subgroup membership for this special case.)

e. Suppose $p = 4k+3$, $g \neq 1$ is a quadratic residue modulo p, and $q = \frac{p-1}{2} = 2k + 1$ is a prime. Then, there is a more efficient secure way, than using the above protocol, to convince the Verifier that $h = g^y \pmod p$ for some integer y. What is it? (Hint: no Prover is necessary.)

Problems for Thursday, May 8

1. Give a protocol for digital signatures in which the verification (which can be shown to the judge) does not reveal to the judge the contents of the document which was signed.

2. Some applications are sensitive to *replay attacks*, where an adversary takes a copy of an original signed message and sends it again later. (For example, it should not be possible to repeat a request to transfer money from one bank account to another.) Design a protocol (using signatures) to prevent replay attacks.

3. According to Ivan Damgård, the essence of SSL (authentication between a server S and a client C) is as follows:

   (a) C sends a hello message containing a nonce (a random challenge) n_C.

   (b) S sends a nonce n_S and its certificate *Cert(S)* (issued by a certification authority and containing the public key K_S of S.)

   (c) C verifies *Cert(S)* and chooses a pre-master secret pms at random. C sends $E(K_S, pms)$, its certificate *Cert(C)* to S, and its signature sig_C on the concatenation of n_C, n_S, and $E(K_S, pms)$.

   (d) S sends C a MAC on all messages sent so far in this protocol, using pms as the secret key.

   (e) C verifies the MAC. IF OK, it send S a MAC on all messages sent so far in this protocol.

(f) Use a shared function to compute keys for authentication and encryption from n_S, n_C, and pms.

In this protocol, how does S authenticate itself? How does C authenticate itself. Why do the keys depend on n_S and n_C, instead of just pms? Is it important that C actually send a MAC at the end, or would OK be enough?

4. Let n be an integer with unknown factorization $n = pq$, where p and q are prime, and let $x_0, x_1 \in \mathbb{Z}_n^*$ be such that at least one of x_0 and x_1 is a quadratic residue modulo n. Assume that both x_0 and x_1 have Jacobi symbol $+1$ modulo n. (Assume that it is x_b and $u^2 \equiv x_b \pmod{n}$). Suppose that x_0, x_1, and n are given as input to a Prover and Verifier. Consider the interactive protocol in which the following is repeated $\log_2 n$ times:

Prover		Verifier
Choose random $i \in \{0,1\}$ and random $v_b, v_{1-b} \in \mathbb{Z}_n^*$. Compute $y_b = v_b^2 \pmod{n}$ and $y_{1-b} = v_{1-b}^2 (x_{1-b}^i)^{-1} \pmod{n}$.	y_0, y_1 $\longrightarrow$	
		Choose a random $c \in \{1, 0\}$.
	$\longleftarrow$ c	
Compute $z_b = u^{i \oplus c} v_b \pmod{n}$, $z_{1-b} = v_{1-b}$.	z_0, z_1 $\longrightarrow$	
		Check that either ($z_0^2 \equiv y_0 \pmod{n}$ and $z_1^2 \equiv x_1^c y_1 \pmod{n}$) or ($z_0^2 \equiv x_0 y_0 \pmod{n}$ and $z_1^2 \equiv (x_1)^{1-c} y_1 \pmod{n}$). If not, reject and halt.

Note that $\oplus$ is addition modulo 2.

a. Prove that the above protocol is an interactive proof system showing that at least one of x_0 and x_1 is a quadratic residue modulo n.

b. Suppose that x_{1-b} is also a quadratic residue. What is the distribution of the values y_0, y_1, z_0, z_1 sent by a Prover following the protocol?

c. Suppose that x_{1-b} is a quadratic nonresidue. What is the distribution of the values y_0, y_1, z_0, z_1 sent by a Prover following the protocol?

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

5. Throughout this problem, suppose it is known that $n = p \cdot q$, where p and q are distinct primes, though the factorization of n is unknown to the Verifier. Let $x, y \in \mathbb{Z}_n^*$ both have Jacobi symbol $+1$.

   a. Prove that $x \cdot y \pmod{n}$ is a quadratic residue modulo n if and only if either

   (a) x and y are both quadratic residues, or

   (b) x and y are both quadratic nonresidues.

   b. Prove that $x^3 \cdot y^5 \pmod{n}$ is a quadratic residue modulo n if and only if either

   (a) x and y are both quadratic residues, or

   (b) x and y are both quadratic nonresidues.

   c. Give a perfect zero-knowledge proof showing that x and y satisfy one of the following two conditions modulo n:

   (a) x and y are both quadratic residues, or

   (b) x and y are both quadratic nonresidues.