Cryptology
Assignment 4

Due Friday, May 18, at 10:15.

Note that this is an actual assignment which must be approved in order to take the exam in June. You may not work with others on the assignment. It must be turned in by 10:15 on Friday, May 18. If it is late, it will not be accepted. There will be no chance to redo the assignment if it is not acceptable the first time. There are two problems.

1. 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 $x, y \in Z_n^*$ both have Jacobi symbol $+1$.

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

1. x and y are both quadratic residues, or
2. 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

1. x and y are both quadratic residues, or
2. 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:

1. x and y are both quadratic residues, or
2. x and y are both quadratic nonresidues.

2. 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 (use definition 13.2 in the textbook).

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

To be discussed Wednesday, May 9, 2001.

1. Do problems 12.4, 13.1, 13.2, 13.3 and 13.4 in the textbook.
Always use definition 13.2, instead of 13.1 when it is relevant.

Reading

We will continue in chapter 13. After that we will cover a bit in chapter 7. Read sections 7.1, 7.2, 7.3, and 7.6.