Cryptology
Assignment 4

Due 8:30 Monday, May 22, 2000

Let n be an integer with unknown factorization $n = pq$, where p and q are prime, and let $x_0, x_1 \in Z_n^*$ 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 $v_b, v_{1-b} \in Z_n^*$. Compute $y_b = v_b^2 \pmod{n}$ and $y_{1-b} = v_{1-b}^2 (x_{1-b}^i)^{-1} \pmod{n}$.	$\xrightarrow{y_0, y_1}$	
		Choose a random $c \in \{1, 0\}$.
	$\xleftarrow{c}$	
Compute $z_b = u^{i \oplus c} v_b \pmod{n}$, $z_{1-b} = v_{1-b}$.	$\xrightarrow{z_0, z_1}$	
		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 (use definition 13.2 in the textbook).