that $x' \not\equiv \pm x$ (*mod* n), in which case you immediately obtain a nontrivial factor, i.e., $g.c.d.(x'+x, n)$. By repeating the procedure T times, you have probability $1 - 2^{-T}$ of factoring n.

6. Yes. Suppose that another person Pícara$_2$ playing the role of Pícara intercepts the message $(b^{y_1}, b^{y_2}, \alpha_1, \alpha_2)$ that Pícara sent to Vivales, and wants to fool Vivales into believing that she also knows the factorization of n (or the 3-coloring, or the discrete logarithm, etc.). Suppose also that Vivales will not accept from Pícara$_2$ a repetition of the exact same four-tuple that Pícara sent. Without knowing Pícara's secret random integers y_1, y_2 or her messages m_1, m_2 or the discrete logarithm of either β_1 or β_2, Pícara$_2$ has no way to construct a different four-tuple that gives Vivales the impression that she knows the factorization.
7. Pícara randomly selects $0 \le x' < N$, and sends Vivales $y' = b^{x'}$. Then the two messages for oblivious transfer are $m_1 = x'$ and $m_2 = x + x'$ (*mod* N). Vivales verifies either $b^{x'} = y'$ or else $b^{x+x'} = yy'$. If the procedure is repeated T times, then the odds against Pícara being lucky (i.e., being able to fool Vivales into thinking she knows the discrete log of y) are 2^T to 1.
8. Vivales can easily get Pícara to betray the factorization of n, as follows. He randomly chooses integers z until he finds a z whose Jacobi symbol modulo n is -1. He then sends Pícara $y = z^2$ *mod* n. Pícara replies with the value x^2 of a square root of y *mod* n which is different from $\pm z$. Vivales can now find a nontrivial factor of n, namely, $g.c.d.(x^2 + z, n)$.
9. The proof of zero knowledge transmission using a simulator Clyde will not work. Another problem is that Pícara would have to be certain that every y_i had been produced by the trusted Center, and not by Vivales pretending to be the trusted Center.

§ V.1.

1. (a) 4, 11; (b) 8, 13; (c) see part (d); (d) Show that $n - 1 \equiv p - 1$ *mod* $2p - 2$, so that $b^{n-1} \equiv 1$ *mod* p, and $b^{n-1} \equiv b^{(2p-1-1)/2} \equiv \left(\frac{b}{2p-1}\right)$ *mod* $2p - 1$. Then $b^{n-1} \equiv 1$ *mod* $p(2p-1)$ if and only if $\left(\frac{b}{2p-1}\right) = 1$.
2. (a) Use the fact that $n = n'p = n'(p - 1 + 1) \equiv n'$ *mod* $p - 1$. (b) Use part (a) with $n' = 3$ to conclude that p would have to be a divisor of $2^2 - 1$, $5^2 - 1$, $7^2 - 1$. (c) p would have to be a divisor of $2^4 - 1$, $3^4 - 1$, $7^4 - 1$. (d) Any smaller n would be the product of 2 primes greater than 5 (by part (c)). Then check 49 and 77.
3. Divide the congruence (1) with $n = p^2$ by the congruence $b^{p^2-p} \equiv 1$ *mod* p^2, which always holds by Euler's theorem (Proposition I.3.5).
4. (a) 217; (b) 341.
5. (a) First suppose that n is a pseudoprime to the base b. Since $n - 1 = pq - 1 \equiv q - 1$ *mod* $p - 1$, you have $b^{q-1} \equiv 1$ *mod* p; but since $b^{p-1} \equiv 1$ *mod* p always by Fermat's little theorem, and since d is an integer linear combination of $p - 1$ and $q - 1$, it follows that $b^d \equiv 1$ *mod* p.