

CIS 400/628
Homework #5
Spring 2005
Due: 31 Mar 2005

In class, I have left some statements unexplained in proofs. As part of this assignment, you will prove some of them.

1. In the proof of Euler's Criterion, I said when examining $\alpha^{i(p-1)/2}$ that i must be even. Why is this true? (hint: an alternative definition of a primitive root is this: an integer α is a primitive root modulo n if $\phi(n)$ is the smallest possible positive integer l so that $g^l \equiv 1 \pmod{n}$. Given this definition, we can use the Division Algorithm to write $l = q * \phi(n) + r$, and use the properties of primitive roots to show that $\phi(n) | l$).
2. In the proof of the proposition following Euler's Criterion, I said that if $p \equiv 3 \pmod{4}$, and p is prime, then there is no solution to $x^2 \equiv -1 \pmod{p}$. Prove this (this is exercise 3.15 in Trappe & Washington; the hint there is to suppose that x exists, then raise both sides to the power $(p-1)/2$ and use Fermat's Little Theorem).
3. (Trappe & Washington, 8.4) Let p be a prime and let α be an integer $\ni p \nmid \alpha$. Let $h(x) \equiv \alpha^x \pmod{p}$. Explain why $h(x)$ is not a good cryptographic hash function.
4. (Trappe & Washington, 9.3) In the electronic coin system presented in class, the numbers g_1 and g_2 are powers of g , but the exponents are supposed to be hard to find. Suppose we take $g_1 = g_2$.
 - (a) Show that if the Spender replaces r_1 and r_2 with r'_1 and r'_2 such that $r_1 + r_2 = r'_1 + r'_2$, then the verification equations still work.
 - (b) Show how the Spender can double spend without being identified.
5. (Trappe & Washington, 10.8) Suppose there are four people in a room, exactly one of whom is a foreign agent. The other three people have been given pairs corresponding to a Shamir secret sharing scheme in which any two people can determine the secret (i.e., $t = 2$). The foreign agent has randomly chosen a pair. The people and pairs are as follows. All the numbers are mod 11. Determine who the foreign agent is and what the message is.

Alice: (1, 4)

Bob: (3, 7)

Carol: (5, 1)

Dan: (7, 2)