YALE UNIVERSITY
DEPARTMENT OF COMPUTER SCIENCE

CPSC 467b: Cryptography and Computer Security *Handout #8*
Professor M. J. Fischer *March 19, 2012*

Problem Set 4

Due on Wednesday, March 28, 2012.

Instructions

Work the problems below, prepare your answers in electronic form, and submit your solutions using the submit script on the Zoo. Remember to specify "3" for the problem number argument to `submit`.

Some of the problems require computation. You may use a calculator or computer for the calculations, but you must show your work. For example, in problem 1, your answer should contain a table of the relevant values of $g^{(p-1)/q} \bmod p$ to demonstrate that the Lucas test gives the result you claim.

Some of the problems use terminology that we have not covered in class, even though we have talked about the concepts. You may use external resources to find out what these terms mean. As always, you must properly cite all resources that you use to solve the problems.

Problem 1: Primitive roots

(a) Find a primitive root g of $p = 761$ and use the Lucas test to prove that you have one.

(b) Find a non-trivial[1] number $g \in \mathbf{Z}^*_{761}$ that fails to be a primitive root of p, and use the Lucas test to prove your answer correct.

Problem 2: Security of Digital Signatures

(a) What is existential forgery of a digital signature scheme?

(b) What are practical mechanisms to prevent existential forgery? Describe the mechanisms and explain why it would be hard to produce a forged message-signature pair.

(c) Is the ElGamal signature scheme susceptible to the existential forgery attack? If yes, show how an attacker can produce a valid message-signature pair. If no, explain why the scheme is resistant to this attack. State all assumptions you make.

Problem 3: Quadratic Residues and the Legendre Symbol

(a) Let $p = 19$, $q = 37$, and $n = p \times q = 703$. For each $i, j \in \{-1, 1\}$, find a number $x_{i,j} \in \mathbf{Z}^*_n$ such that

$$\left(\frac{x_{i,j}}{p}\right) = i \quad \text{and} \quad \left(\frac{x_{i,j}}{q}\right) = j.$$

(b) Use the Euler criterion to justify your answers to part (a).

[1] Non-trivial means $g \notin \{1, p-1\}$.

Problem 4: Miller-Rabin Test

Let $n = 703$. Find a witness a for which the Miller-Rabin test succeeds in showing the compositness of n. Show the sequence of values $b_0, b_1, b_2, \ldots$ that the test generates from a, and explain clearly why you can conclude from this sequence that n is not a prime.

Problem 5: Properties of Hash Functions

Hash functions are frequently used for cryptographic applications. A cryptographic hash function must have at least the properties listed below in order to withstand known attacks. For each of these properties, (1) say what it is, (2) give a plausible scenario whereby an attack exploiting a hash function lacking such property might be carried out, and (3) say whether there is an efficient hash function that has that property. (If yes, list that hash function; if no, explain why.)

(a) Preimage resistance

(b) Second-preimage resistance

(c) Collision resistance