COMP 754 — Cryptography & Security — Aj. Phillip Rogaway
Problem Set #4 — Out: 13 Aug 02 — Due: 27 Aug 02 (in class)

Problem 1 Compute $17^{130} \bmod 100$. Do this without writing a computer program and without multiplying 17 by itself 129 times. Show your work. Your method should provide an efficient algorithm —polynomial time in the length of all numbers— to compute $a^b \bmod n$.

Problem 2 Use Euclid's algorithm to find $28^{-1} \pmod{75}$. Show all your work.

Problem 3 Let $p = 101$ and $q = 113$ so $pq = n = 11413$. Is $e = 3$ a valid encryption exponent for RSA modulus n? If so, find the corresponding decryption exponent d.

Problem 4 Recall that n is a *2-pseudoprime* if $2^{n-1} = 1 \pmod{n}$ even though n is *not* prime. Write a program to find all 2-pseudoprimes less than 1000.