ECS 227 — Modern Cryptography — Winter 00
Problem Set 5

Phillip Rogaway

Out: 29 February 2000. Due: 9 March 2000.

1. Let $n = 167 \times 149 = 24883$ be an RSA modulus. Find the decryption exponent d associated to RSA encryption exponent $e = 3$.

2. Suppose you have a fast deterministic algorithm I that inverts $f(x) = x^e \bmod n$ on 1% of all inputs—the inputs in Z_n^* that your algorithm likes. Construct a usually-fast probabilistic algorithm J that inverts $f(x) = x^e \bmod n$ on every point in Z_n^*. Analyze the efficiency of your algorithm: what is the expected running time of J? Your algorithm should be of the "Las Vegas" variety: it is always correct, and on every input it is usually fast. Analyze the efficiency of your algorithm.

3. When p and q are distinct odd primes, $n = pq$, points in Z_n^* have either zero or four square roots. A quarter of the points have four square roots; the rest have no square root. The four square roots will look like $a, -a, b, -b$ (where $-a$ means $n - a$, of course). Suppose Sam designs an efficient algorithm S that, on input of a square x, finds some square root of x. You don't know which. Use S to make an efficient (probabilistic) algorithm F that factors n. (*Hint: try to find two square roots of a number, a and b, which are not of the form $a = \pm b \pmod{p}$. Show how, if you do this, you can factor n.*)