Introduction to Cryptography

Homework 3

October 6, 2006

1. Apply the AKS test to $n = 31$ and $n = 143$.

2. Write a `pari` program that determines the three smallest composite integers n that pass a Fermat test with base $a = 2$.

3. Show that, in Lehman's algorithm, we have

$$2\sqrt{kn} \le a \le 2\sqrt{kn} + \frac{n^{1/6}}{4\sqrt{k}}.$$

   Use this to prove that the number of iterations in the loops on k and a is at most $\sum_{i=1}^{B} \frac{n^{1/6}}{4\sqrt{k}}$ (recall that $B = \lfloor n^{1/3} \rfloor$, and that this is $O(n^{1/3})$.

4. Show that $n = 568971935269420243703269 72321$ is a strong pseudoprime (i.e., passes Miller-Rabin) for $a = p$ for all primes $p \le 29$. (Note: you can cut and paste this number into `pari` if you go to `http://www.trnicely.net/misc/mpzspsp.html`)

   Show that the primality tests reveal different square roots of $-1 \bmod n$; show how you can use this information to factor n.

   Also use Fermat's method with multiplier $k = 3$ to factor the number. What do you observe?

5. Use the `pari` program

```
n=13231;k=10;x=lift(Mod(2,n)^(k!));print(gcd(x-1,n))
```

   to factor $2^{67} - 1$ using $k = 1000, 2000, 3000, \ldots$; Explain why the method was not successful for the first two choices, but found the prime factor with the last.

6. Consider the integer $n = 10007030021$. Write a little `pari` program and apply Pollard's rho method with various functions $f(x) = x^2 + a$ and starting values c, and count how many iterations it takes to find the factorization.