Introduction to Cryptography

Homework 3

November 2, 2006

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

1. Consider $n = 143$ first. We have to check whether $n = a^b$ for $b > 2$; from $b = \log n / \log a < \log n / \log 2 < 8$ we see that we have to test whether n is a square, cube, or a fifth or seventh power. Computing $n^{1/r}$ for $2 = 2, 3, 5, 7$ immediately shows that this is not the case.

Then we have to find some r such that $n \bmod r$ has order ≥ 208 (note that $\log 31 \approx 5$ since we are working with the logarithm to base 2). Let us pick a few primes r and compute the order of $n \bmod r$ (pari can do this: just type in $\mathtt{x} = \mathtt{Mod(143, r); znorder(x)}$). We get $r = 227$, with the order of $n \bmod r$ being 226.

Now we set $\ell = \lceil 2\sqrt{r} \log n \rceil + 1$. This gives us $\ell = 215$. Strictly speaking we now find that $\gcd(11, n) = 11$ and declare n to be composite, but let's pretend this never happened. Then we have to perform the actual primality test: checking whether $(X - a)^n \equiv X^n - a \bmod (X^r - 1, n)$ for small a. Since $r > n$, we do not have to compute mod $X^r - 1$ at all. Here's how to do the rest using `pari`

```
n=143;X=Mod(1,n)*X;lift((X-1)^n)
```

Here the second command creates the polynomial $\overline{1} \cdot X$ in $\mathbb{Z}/n\mathbb{Z}$; the third one lifts the result to an actual polynomial. The output given by pari is: $X^{143} + 130 * X^{132} + 132 * X^{130} + \ldots + 13 * X^{11} + 142$. Since this is not equal to $X^{143} + 142$, the integer n is not prime.

Now for $n = 31$. Pick $r = 107$; the order of $n \bmod r$ is then 106. Here we find, using the program

```
a=1;n=31;X=Mod(1,n)*X;lift((X-a)^31)
```

that 31 indeed behaves as a prime.

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

   Here is one:

   ```
   {for(n=2,1000,if(isprime(n),,
    if(Mod(2,n)^(n-1)-1,,
    print(n,"    ",factor(n)))))}
   ```

   The output is $341 = 11 \cdot 31$; $561 = 3 \cdot 11 \cdot 17$; $645 = 3 \cdot 5 \cdot 43$.

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

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

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

   Observe that

   $$\sum_{k=1}^{B} \frac{1}{\sqrt{k}} < 1 + \int_1^B \frac{dk}{\sqrt{k}} = 1 + 2(\sqrt{B} - 1) < 2n^{1/6},$$

   hence

   $$\sum_{k=1}^{B} \frac{n^{1/6}}{4\sqrt{k}} = \frac{n^{1/6}}{4} \sum_{k=1}^{B} \frac{1}{\sqrt{k}} < \frac{n^{1/3}}{2}.$$

4. Show that $n = 568971935269420243703269723 21$ is a strong pseudoprime (i.e., passes Miller-Rabin) for $a = p$ for all primes $p \leq 29$. (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?

   We find that $n - 1 \equiv 32 \bmod 64$, so we put $r = \frac{n-1}{32}$. Now the following program

   ```
   a=2;for(j=0,5,print(j,"   ",lift(Mod(a,n)^(2^j*r))))
   ```

computes the remainders we need. Here we see that we get -1 for $j = 1$, so n is a strong 2-pseudoprime. In fact we get the remainder -1 for all primes $2 \le a \le 29$ except $a = 3$; for $a = 3$ and $a = 31$ we find that $a^r \equiv 1 \bmod n$.

Note that n does not pass the Fermat test for $n = 37$ or 41. Here's the output for $a = 37$:

0	17282940531730601543271515221
1	41146895604985750006510897616
2	12698298841514531247159417876
3	15750297921955861215440087548
4	12698298841514531247159417876
5	15750297921955861215440087548

and the first two lines for $a = 41$:

0	39507312774642251961139492209
1	41146895604986163154886884773
2	12698298841514531247159417876

Here we see that the results for $i = 2$ are the same, but that they are different for $i = 1$. Thus if we set $x \equiv 37^{2r} \bmod n$ and $y \equiv 41^{2r} \bmod n$, then $x^2 \equiv y^2 \bmod n$. Now $\gcd(x - y, n)$ gives us the factor 413148375987157 of n.

We can also factor n with the Fermat method and multiplier $k = 3$: $\sqrt{3n} \approx 413148375987157.99999\ldots$; with $x = 413148375987158$ we find $x^2 - 3n = 1$, and $\gcd(x - 1, n) = 413148375987157$.

The reason for this behavior is that n has the factorization $n = p(3p - 2)$ for $p = 137716125329053$, so the prime factors have a ratio very close to the multiplier $k = 3$.

5. Use the `pari` program

```
n=13231;k=10;x=lift(Mod(3,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.

If you use $a = 2$, you won't be able to factor n. This is because for $n = 2^p - 1$ and odd primes p, we always have $2^p \equiv 1 \bmod n$.

With base $a = 3$ and $k = 3000$, however, you find the prime factor $q = 193707721$ in an instant. The reason is that $q - 1 = 2^3 3^3 \cdot 5 \cdot 67 \cdot 2677$ factors into primes < 3000.

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.

Here's what we find:

c	a	iterations
2	1	40
3		186
6		186
7		186
8		186
39		186
111		30
112		186

Thus there seem to be only a few possible cycle lengths for a fixed a. Here's the correspspnding table for $a = 2$:

c	a	iterations
2	2	110
3		55
6		110
7		165
8		55
39		110
111		110
112		55

Note that the number of iterations needed for finding the prime factor $10007 \approx 10^4$ is expected to be of magnitude 100. The situation is totally different for $a = -2$:

c	a	iterations
3	-2	69
6		2501
7		69
8		69
39		2501
111		2501
112		69

Here we sometimes find the factor after 69 iterations, but for some starting values the number of iterations needed is a lot larger than $\sqrt{p}$. The reason is that if $x \equiv r + \frac{1}{r} \bmod n$, then $x^2 - 2 \equiv r^2 + \frac{1}{r^2} \bmod n$, so the values of $f(x) = x^2 - 2$ lie in the subset of all residue classes mod n that can be written in the form $r + \frac{1}{r} \bmod n$. then