Chapter 5: Attacks on RSA (Other than factoring)

Math 495, Fall 2008

Hope College

November, 2008

Computing $\phi(n)$

- Recall that $n = pq$ and $\phi(n) = (p-1)(q-1)$.
- If we substitute $q = n/p$ into the second equation, we get

$$p^2 - (n - \phi(n) + 1)p + n = 0$$

- We can use the quadratic formula to find the two roots.
- These roots are p and q–the factors of n.
- Let's see an example in Maple.
- Thus, if we know $\phi(n)$, we can factor n.
- We already know that if we can factor n, we can compute $\phi(n)$.
- Thus, factoring n and computing $\phi(n)$ are equivalent.

Determining the decryption exponent

- If you can determine a (the decryption exponent), you can factor n with a randomized algorithm.
- Here is the idea: If we have an x such that $x^2 \equiv 1^2 \bmod n$, with $x \not\equiv \pm 1 \bmod n$, then $gcd(x+1, n)$ and $gcd(x-1, n)$ are factors of n.
- Let's see an example–in Maple!
- It can be proven (read the book) that the algorithm succeeds with probability at least $1/2$.
- Thus, factoring n and computing the decryption exponent are *almost* equivalent (why almost?).
- Similarly, being able to compute inverses modulo $\phi(n)$ (without necessarily knowing $\phi(n)$) implies the ability to factor.
- Notice that knowledge of any decryption exponent a means n is no longer usable.

Continued Fractions

- Before we can discuss the next attack, we need to understand continued fractions.
- We will explore the concept in Maple.
- Now that we know what continued fractions are, we can continue.
- An interesting result:

Theorem π

Suppose that $\gcd(a, b) = \gcd(c, d) = 1$ and that

$$\left|\frac{a}{b} - \frac{c}{d}\right| < \frac{1}{2d^2}$$

Then c/d is one of the convergents of the continued fraction expansion of a/b.

Wiener's Low Decryption Exponent Attack

- Observe that $ab - t\phi(n) = 1$ for some integer t (Since $ab \equiv 1 \bmod \phi(n)$).
- Assume $a < n^{1/4}/3$ and $q < p < 2q$
- Then it can be shown that

$$\left|\frac{b}{n} - \frac{t}{a}\right| < \frac{1}{2a^2}$$

- So, one of the convergents of the continued fraction of b/n will give us t and a.
- Given t and a, we can compute $\phi(n) = (ab - 1)/t$.
- Once we have $\phi(n)$, we can factor n as we did above.
- Since we don't know which convergent is correct, we try them until one works.
- Let's see an example–using Maple!