T-79.5501
Cryptology

Lecture 8 (April 8, 2008):

- Wiener's Low decryption Exponent Attack, Sec 5.7.3

RSA Cryptosystem

$n = pq$ where p and q are two different large primes

$$\phi(n) = (p-1)(q-1)$$

a decryption exponent (private)

b encryption exponent (public)

$$ab \equiv 1 \left(\bmod\, \phi(n)\right)$$

RSA operation:

$$(m^b)^a \equiv m \pmod{n}$$

for all m, $0 \le m < n$.

Wiener's result: It is insecure to select a shorter than about ¼ of the length of n.

RSA Equation

$$\boxed{ab - k\,\phi(n) = 1}$$

for some k where only b is known.

Additional information: $pq = n$ is known and $q < p < 2q$

$$n > \phi(n) = (p-1)(q-1) = pq - p - q + 1 \geq n - 3\sqrt{n}$$

Also we know that a, $b < \phi(n)$, hence $k < a$.

Wiener (1989) showed how to exploit this information to solve for a and all other parameters k, p and q, if a is sufficiently small.

Wiener's method is based on continued fractions.

Continued Fractions

Every rational number t has a unique representation as a finite chain of fractions

$$q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ddots\, q_{m-1} + \cfrac{1}{q_m}}}}$$

and we denote $t = [q_1\, q_2\, q_3\, \ldots\, q_{m\text{-}1}\, q_m]$. The rational number $t_j = [q_1\, q_2\, q_3\, \ldots\, q_j\,]$ is called the j^{th} convergent of t. For $t = u/v$, just run the Euclidean algorithm to find the q_i, i = 1, 2,…,m.

Convergent Lemma

Theorem 5.14 *Suppose that* gcd(u,v)= gcd (c,d) = 1 *and*

$$\left|\frac{u}{v}-\frac{c}{d}\right|<\frac{1}{2d^2}.$$

Then c/d is one of the convergents of the continued fraction expansion of u/v.

Recall the RSA problem: $ab - k\phi(n) = 1$

Write it as:

$$\frac{b}{\phi(n)}-\frac{k}{a}=\frac{1}{a\phi(n)}$$

Then, if $2a < \phi(n)$, then k/a is a convergent of $b/\phi(n)$.

Wiener's Theorem

If in RSA cryptosystem

$$a < \frac{1}{3}\sqrt[4]{n},$$

that is, the length of the private exponent a is less than about one forth of the length of n, then a can be computed in polynomial time with respect to the length of n.

Proof. First we show that *k/a* can be computed as a convergent of *b/n*, based on Euclidean algorithm, which is polynomial time. To see this, we estimate:

$$\left|\frac{b}{n} - \frac{k}{a}\right| = \left|\frac{ab - kn}{an}\right| = \left|\frac{1 + k\phi(n) - kn}{an}\right| \leq \frac{3k}{a\sqrt{n}} < \frac{3}{\sqrt{n}} < \frac{1}{2a^2}.$$

Wiener's Algorithm

Then the convergents $c_j/d_j = [q_1\, q_2\, q_3\, \ldots\, q_j]$ of b/n are computed. For the correct convergent $k/a = c_j/d_j$ we have

$$bd_j - c_j\,\phi(n) = 1.$$

For each convergent one computes

$$n' = (d_j b - 1)/c_j$$

and checks if $n' = \phi(n)$. Note that $p + q = n - \phi(n) + 1$. Then if $n' = \phi(n)$, the equation

$$x^2 - (n - n' + 1)x + n = 0$$

has two positive integer solutions p and q.

EXAMPLE

Stinson, Problem 5.32: Suppose that $n = 317940011$ and $b = 77537081$ in the *RSA Cryptosystem*. Using Wiener's Algorithm, attempt to factor n. If you succeed, determine the secret exponent a and $\phi(n)$.

Solution: Running Wiener's algorithm we get:

j	r_j	q_j	c_j	d_j	n'
0	77537081	0	1	0	-
1	317940011	0	0	1	-
2	77537081	4	1	4	310148323
3	7791687	9	9	37	318763555.111
4	7411898	1	10	41	317902032
5	379789	19	199	816	317940995.452
6	195907	1	209	857	
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

$j = 2$ no solution, since n' is odd ($\phi(n)$ is divisible by 4).

$j = 3$ no solution, since n' is not integer.

$j = 4$ looks promising. Substitute $n = 317940011$ and $n' = 317902032$ to equation $x^2 - (n - n' + 1)x + n = 0$ and get

$$x^2 - 37980x + 317940011 = 0,$$

from where we get solutions for p and q, which are $x = 18990 \pm 6533$. Then $a = d_4 = 41$, and $\phi(n) = n' = 317902032$.