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)

\[ ab \equiv 1 \pmod{\phi(n)} \]

RSA operation:

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

for all \( m, \, 0 \leq m < n \).

Wiener’s result: It is insecure to select \( a \) shorter than about \( \frac{1}{4} \) of the length of \( n \).

Wiener’s method is based on continued fractions.

RSA Equation

\[ ab - k \phi(n) = 1 \]

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

$$t = \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \frac{1}{\cdots + \frac{1}{q_{m-1} + \frac{1}{q_m}}}}}}$$

and we denote $t = [q_1, q_2, q_3, \ldots, q_{m-1}, q_m]$. 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 $q_i$, $i = 1, 2, \ldots, m$.

Fundamental 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 \( \frac{k}{a} \) can be computed as a convergent of \( \frac{b}{n} \), based on Euclidean algorithm, which is polynomial time. To see this, we estimate:

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

Wiener’s Algorithm

Then the convergents \( c/d_j = [q_1 q_2 q_3 \ldots q_j] \) of \( \frac{b}{n} \) are computed. For the correct convergent \( k/a = c/d_j \) 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 \( q \).