5.7.3 Wiener's Attack

As always, suppose that $n = pq$ where p and q are prime. In this section, we present an attack, due to M. Wiener, that succeeds in computing the secret decryption exponent a whenever the following hypotheses are satisfied:

$$3a < n^{1/4} \quad \text{and} \quad q < p < 2q. \tag{5.2}$$

If n has ℓ bits in its binary representation, then the attack will work when a has fewer than $\ell/4 - 1$ bits in its binary representation and p and q are not too far apart.

Note that Alice might be tempted to choose her decryption exponent to be small in order to speed up decryption. If she uses Algorithm 5.5 to compute $y^a \bmod n$, then the running time of decryption will be reduced by roughly 75% if she chooses a value of a that satisfies (5.2). The results we prove in this section show that this method of reducing decryption time should be avoided.

Since $ab \equiv 1 \pmod{\phi(n)}$, it follows that there is an integer t such that

$$ab - t\phi(n) = 1.$$

Therefore we have that

$$\left| \frac{b}{\phi(n)} - \frac{t}{a} \right| = \frac{1}{a\phi(n)}.$$

Since $n = pq > q^2$, we have that $q < \sqrt{n}$. Hence,

$$0 < n - \phi(n) = p + q - 1 < 2q + q - 1 < 3q < 3\sqrt{n}.$$

Now, we see that

$$\begin{aligned}
\left| \frac{b}{n} - \frac{t}{a} \right| &= \left| \frac{ba - tn}{an} \right| \\
&= \left| \frac{1 + t(\phi(n) - n)}{an} \right| \\
&\leq \frac{3t\sqrt{n}}{an} \\
&= \frac{3t}{a\sqrt{n}}.
\end{aligned}$$

Since $t < a$, we have that $3t < 3a < n^{1/4}$, and hence

$$\left| \frac{b}{n} - \frac{t}{a} \right| \leq \frac{1}{an^{1/4}}.$$

Finally, since $3a < n^{1/4}$, we have that

$$\left| \frac{b}{n} - \frac{t}{a} \right| < \frac{1}{3a^2}.$$

Therefore the fraction t/a is a very close approximation to the fraction b/n. From the theory of continued fractions, it is known that any approximation that is this close must be one of the convergents of the continued fraction expansion of b/n. This expansion can be obtained from the EUCLIDEAN ALGORITHM, as we describe now.

A (finite) *continued fraction* is an m-tuple of non-negative integers, say $[q_1, \ldots, q_m]$, which is shorthand for the following expresson:

$$q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ldots + \frac{1}{q_m}}}.$$

Suppose a and b are positive integers such that $\gcd(a, b) = 1$, and suppose that the output of Algorithm 5.1 is the m-tuple $(q_1, \ldots, q_m)$. Then is is not hard to see that $a/b = [q_1, \ldots, q_m]$. We say that $[q_1, \ldots, q_m]$ is the *continued fraction expansion* of a/b in this case. Now, for $1 \leq j \leq m$, define $C_j = [q_1, \ldots, q_j]$. C_j is said to be the jth *convergent* of $[q_1, \ldots, q_m]$. Each C_j can be written as a rational number c_j/d_j, where the c_j's and d_j's satisfy the following recurrences:

$$\begin{aligned}
c_0 &= 1 \\
c_1 &= q_1 \\
c_j &= q_j c_{j-1} + c_{j-2} \quad \text{if } j \geq 2\text{; and} \\
d_0 &= 0 \\
d_1 &= 1 \\
d_j &= q_j d_{j-1} + d_{j-2} \quad \text{if } j \geq 2.
\end{aligned}$$

Example 5.16 We compute the continued fraction expansion of $34/99$. The EUCLIDEAN ALGORITHM proceeds as follows:

$$\begin{aligned}
34 &= 0 \times 99 + 34 \\
99 &= 2 \times 34 + 31 \\
34 &= 1 \times 31 + 3 \\
31 &= 10 \times 3 + 1 \\
1 &= 3 \times 1.
\end{aligned}$$

Hence, the continued fraction expansion of $34/99$ is $[0, 2, 1, 10, 3]$, i.e.,

$$\frac{34}{99} = 0 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{10 + \frac{1}{3}}}}.$$

The convergents of this continued fraction are as follows:

$$\begin{aligned}[0] &= 0\\ [0,2] &= 1/2\\ [0,2,1] &= 1/3\\ [0,2,1,10] &= 11/32, \text{ and}\\ [0,2,1,10,3] &= 34/99.\end{aligned}$$

The reader can verify that these convergents can be computed using the recurrence relations given above. □

The convergents of a continued fraction expansion of a rational number satisfy many interesting properties. For our purposes, the most important property is the following.

THEOREM 5.12 *Suppose that* $\gcd(a,b) = \gcd(c,d) = 1$ *and*

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

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

Now we can apply this result to the *RSA Cryptosystem*. We already observed that, if (5.2) holds, then the unknown fraction t/a is a close approximation to b/n. Theorem 5.12 tells us that t/a must be one of the convergents of the continued fraction expansion of b/n. Since the value of b/n is public information, it is a simple matter to compute its convergents. All we need is a method to test each convergent to see if it the "right" one.

But this is also not difficult to do. If t/a is a convergent of n/b, then we can compute the value of $\phi(n)$ to be $\phi(n) = (ab-1)/t$. Once n and $\phi(n)$ are known, we can factor n by solving the quadratic equation (5.1) for p. We do not know ahead of time which convergent of n/b will yield the factorization of n, so we try each one in turn until the factorization of n is found. If we do not succeed in factoring n by this method, then it must be the case that the hypotheses (5.2) are not satisfied.

A pseudocode description of WIENER'S ALGORITHM is presented as Algorithm 5.11.

Algorithm 5.11: WIENER'S ALGORITHM(n, b)

$(q_1, \dots, q_m; r_m) \leftarrow$ EUCLIDEAN ALGORITHM(n, b)
$c_0 \leftarrow 1$
$c_1 \leftarrow q_1$
$d_0 \leftarrow 0$
$d_1 \leftarrow 1$
for $j \leftarrow 1$ **to** m
do $\begin{cases} n' \leftarrow (d_j b - 1)/c_j \\ \textbf{comment: } n' = \phi(n) \text{ if } c_j/d_j \text{ is the correct convergent} \\ \textbf{if } n' \text{ is an integer} \\ \quad \textbf{then } \begin{cases} \text{let } p \text{ and } q \text{ be the roots of the equation} \\ \quad x^2 - (n - n' + 1)x + n = 0 \\ \textbf{if } p \text{ and } q \text{ are positive integers less than } n \\ \quad \textbf{then return } (p, q) \end{cases} \\ j \leftarrow j + 1 \\ c_j \leftarrow q_j c_{j-1} + c_{j-2} \\ d_j \leftarrow q_j d_{j-1} + d_{j-2} \end{cases}$
return ("failure")

We present an example to illustrate.

Example 5.17 Suppose that $n = 160523347$ and $b = 60728973$. The continued fraction expansion of b/n is

$$[0, 2, 1, 1, 1, 4, 12, 102, 1, 1, 2, 3, 2, 2, 36].$$

The first few convergents are

$$0, \frac{1}{2}, \frac{1}{3}, \frac{2}{5}, \frac{3}{8}, \frac{14}{37}.$$

The reader can verify that the first five convergents do not produce a factorization of n. However, the convergent $14/37$ yields

$$n' = \frac{37 \times 60728973 - 1}{14} = 160498000.$$

Now, if we solve the equation

$$x^2 - 25348x + 160523347 = 0,$$

then we find the roots $x = 12347, 13001$. Therefore we have discovered the factorization $160523347 = 12347 \times 13001$.

Notice that, for the modulus $n = 160523347$, WIENER'S ALGORITHM will work for $a < n^{1/4}/3 \approx 37.52$. ∎