9.3 Wiener's attack on RSA

Since the number of operations for modular exponentiation is linear in the number of bits of the exponent, it seems at first glance that it might be a good idea to try to choose parameters of the RSA cryptosystem such that one of the exponents e or d is small. This could shorten the time needed for encryption or decryption, which would be especially of interest in situations when there is a big disproportion in the power of two devices taking part in communication, as when, for instance, a "smart card" is communicating with a central computer. In that situation, we might wish to assign a small private exponent to the card and a small public exponent to the computer in order to minimize the calculations done by the card. However, we will see that such a choice of exponents also implies severe dangers for the security of the cryptosystem. The following result demonstrates that in the case of choosing a relatively small private exponent d (with respect to n), there is an efficient algorithm for breaking RSA and that is the foundation for Wiener's attack on RSA from 1990, which is described in [418].

Theorem 9.1. *Let $n = pq$ where $p < q < 2p$, and let $e < \varphi(n)$ and $d < \frac{1}{3}n^{0.25}$. Then there is a polynomial time algorithm which, from given n and e, calculates d.*

Proof: From $ed \equiv 1 \pmod{\varphi(n)}$, it follows that there is a positive integer k such that $ed - k\varphi(n) = 1$. From this, we have

$$\left|\frac{e}{\varphi(n)} - \frac{k}{d}\right| = \frac{1}{d\varphi(n)}. \tag{9.1}$$

Hence, $\frac{k}{d}$ is a good approximation of $\frac{e}{\varphi(n)}$. However, we do not know $\varphi(n)$; therefore, we will approximate $\varphi(n)$ by n. From $\varphi(n) = n - p - q + 1$ and $p + q - 1 < 3\sqrt{n}$, it follows that $|n - \varphi(n)| < 3\sqrt{n}$. By replacing $\varphi(n)$ by n in (9.1), we obtain

$$\begin{aligned}\left|\frac{e}{n} - \frac{k}{d}\right| &= \left|\frac{ed - k\varphi(n) - kn + k\varphi(n)}{nd}\right| = \left|\frac{1 - k(n - \varphi(n))}{nd}\right| \\ &< \frac{3k\sqrt{n}}{nd} = \frac{3k}{d\sqrt{n}}.\end{aligned}$$

Now, $k\varphi(n) = ed - 1 < ed$, so from $e < \varphi(n)$ (this is a standard assumption in RSA), it follows that $k < d < \frac{1}{3}n^{0.25}$ and we obtain

$$\left|\frac{e}{n} - \frac{k}{d}\right| \leq \frac{1}{d\sqrt[4]{n}} < \frac{1}{2d^2}. \tag{9.2}$$

From Legendre's theorem (Theorem 8.26) and (9.2), it follows that k/d is a convergent in the continued fraction expansion of e/n. From the recurrence for denominators of convergents $\frac{p_k}{q_k}$ of the continued fraction, it follows that $q_k \geq F_k$, where F_k is the k-th Fibonacci number, meaning that the denominators of convergents grow exponentially. Therefore, there are $O(\ln n)$ convergents of $\frac{e}{n}$. One of them is $\frac{k}{d}$. Hence, we calculate all convergents of $\frac{e}{n}$ and test which one of them satisfies the condition $(x^e)^d \equiv x \pmod{n}$ for a randomly chosen x. This gives a polynomial time algorithm for determining the private key d. □

The second method to test the correctness of a guess that some concrete convergent is equal to $\frac{k}{d}$ is that, assuming that the guess is correct, we calculate $\varphi(n) = (p-1)(q-1) = (ed-1)/k$. Then we can calculate $\frac{p+q}{2}$ from the identity

$$\frac{pq - (p-1)(q-1) + 1}{2} = \frac{p+q}{2}$$

and $\frac{q-p}{2}$ from the identity $(\frac{p+q}{2})^2 - pq = (\frac{q-p}{2})^2$. If, in this way, we obtain that $\frac{p+q}{2}$ and $\frac{q-p}{2}$ are integers, we conclude that the guess was correct, and the considered convergent is indeed equal to $\frac{k}{d}$. Then, from $\frac{p+q}{2}$ and $\frac{q-p}{2}$, we can easily obtain the factorization of the modulus $n = pq$.

Example 9.1. Assume that in the RSA cryptosystem, we have the modulus

$$n = 7978886869909,$$

the public exponent

$$e = 3594320245477,$$

and that it is known that the private exponent d satisfies $d < \frac{1}{3}n^{0.25} < 561$. In order to apply Wiener's attack, we calculate the continued fraction expansion of $\frac{e}{n}$. We obtain

$$[0, 2, 4, 1, 1, 4, 1, 2, 31, 21, 1, 3, 1, 16, 3, 1, 114, 10, 1, 4, 5, 1, 2].$$

We then calculate the corresponding convergents:

$$0, \frac{1}{2}, \frac{4}{9}, \frac{5}{11}, \frac{9}{20}, \frac{41}{91}, \frac{50}{111}, \frac{141}{313}, \frac{4421}{9814}, \ldots$$

Finally, we test which of the denominators 2, 9, 11, 20, 91, 111, 313 satisfies the congruence $(x^e)^d \equiv x \pmod{n}$ for e.g. $x = 2$. In this way, we find that the private exponent is $d = 313$.

By the second testing method, for $\frac{k}{d} = \frac{141}{313}$, we first obtain

$$(p-1)(q-1) = (ed-1)/k = 7978881112300,$$

then $(p+q)/2 = (n-(p-1)(q-1)+1)/2 = 2878805$ and $(q-p)/2 = 555546$. Hence, we conclude again that the private exponent is $d = 313$, and we also obtain the factors of n, which are $p = 2878805 - 555546 = 2323259$ and $q = 2878805 + 555546 = 3434351$. ♢

In the previous example, we saw that the correct convergent was precisely the last one that satisfied the condition for the size of the denominator. This suggests that perhaps it is not necessary to test all convergents in the given range, but it could be possible to characterize the exact convergent. Indeed, this can be done by more precise estimates on $\varphi(n)$. With a reasonable assumption that $n > 10^8$, $\frac{k}{d}$ is the unique convergent which satisfies the inequality

$$\frac{2e}{n\sqrt{n}} < \frac{k}{d} - \frac{e}{n} < \frac{2.122\,e}{n\sqrt{n}}.$$

The paper [119] demonstrates a variant of Wiener's attack on RSA in which the private key is slightly greater than $\sqrt[4]{n}$. Let $d = D\sqrt[4]{n}$. If D is not very large, then we can try to express $\frac{k}{d}$ in the form $\frac{rp_{m+1} \pm sp_m}{rq_{m+1} \pm sq_m}$, where r, s are nonnegative integers and $\frac{p_m}{q_m}, \frac{p_{m+1}}{q_{m+1}}$ are consecutive convergents of the continued fraction of $\frac{e}{n}$. By the generalization of Legendre's theorem (Worley's theorem 8.27), we can get an estimate for the number of pairs (r, s) which need to be tested in the worst case. This estimate is roughly $O(D^2)$, thus, exponential in $\ln D$.

We will illustrate that variant of Wiener's attack on the following example.

Example 9.2. Let $n = 7978886869909$, $e = 4603830998027$, and assume that $d < 10000000$. The continued fraction expansion of $\frac{e}{n}$ is

$$[0, 1, 1, 2, 1, 2, 1, 18, 10, 1, 3, 3, 1, 6, 57, 2, 1, 2, 14, 7, 1, 2, 1, 4, 6, 2],$$

and the first few convergents are

$$0,\ 1,\ \frac{1}{2},\ \frac{3}{5},\ \frac{4}{7},\ \frac{11}{19},\ \frac{15}{26},\ \frac{281}{487},\ \frac{2825}{4896},\ \ldots$$

We are searching for two consecutive convergents such that $\frac{e}{n} + \frac{2.122e}{n\sqrt{n}}$ lies between them. We obtain

$$\frac{281}{487} < \frac{e}{n} + \frac{2.122e}{n\sqrt{n}} < \frac{11}{19}.$$

Now, we search for the private exponent d among numbers of the forms $26r + 19s$ or $487s - 26t$ or $4896r' + 487s'$. By applying the criterion for testing candidates for $\frac{k}{d}$ described in the proof of Theorem 9.1, we find that $d = 5936963$, which is obtained for $s = 12195$, $t = 77$. $\diamondsuit$

The time complexity of this attack can be improved by applying the method "meet in the middle" for testing candidates, which is demonstrated in [123] and [218, Chapter 5.1.1]. We want to test whether

$$2^{e(rq_{m+1}+sq_m)} \equiv 2 \pmod{n},$$

holds. Let us notice that the index m is almost fixed. Namely, if m' is the largest odd positive integer such that

$$\frac{p_{m'}}{q_{m'}} > \frac{e}{n} + \frac{2.122e}{n\sqrt{n}},$$

then $m \in \{m', m'+1, m'+2\}$.

Let us introduce the notation:

$$2^{eq_{m+1}} \bmod n = a, \quad (2^{eq_m})^{-1} \bmod n = b.$$

Then we actually test the congruence

$$a^r \equiv 2b^s \pmod{n}.$$

We can do that by calculating $a^r \bmod n$ for all r; we sort the results and then calculate $2b^s \bmod n$ for each s and check whether the result appears in the previously obtained sorted list. In this manner, the number of steps in testing becomes roughly (the number of possibilities for r) + (the number of possibilities for s). To be more precise, the time complexity of the testing phase is reduced from $O(D^2)$ to $O(D \ln D)$ (with the space (memory) complexity $O(D)$). This attack works efficiently for values D less than 2^{30}, i.e. for $d < 2^{30} n^{0.25}$.

9.4 Attacks on RSA using the LLL algorithm

There are also attacks on RSA, which, instead of using continued fractions, use Coppersmith's method for finding solutions to polynomial congruences. Namely, the following problem is encountered. Consider a polynomial $f(x) \in \mathbb{Z}[x]$ of degree d and assume that it is known that there exists a "small" solution of the congruence $f(x) \equiv 0 \pmod{N}$, i.e. the