Cryptography (Math 116) Summer 2012

Here we review some of the attacks on RSA which are not mentioned (or mentioned only in passing) in the textbook.

Some basic mistakes in implementing RSA

Most attacks on RSA are based on the assumption that Alice or Bob (or both) have been careless in their implementation of the RSA cryptosystem. Here are two mistakes in implementation which you should know about:

1. Suppose Alice and Bob have public keys (N, e) and (N', e') but $\gcd(N, N') = p$ is prime. Then Eve can easily factor both Alice's and Bob's public moduli.

   Because of this attack, one should choose the prime factors p and q of an RSA key in a "suitably random" way (after which the primes p and q might be rejected as insecure for other reasons such as $p - 1$ being a product of small primes, making $N = pq$ vulnerable to factorization via Pollard's $p - 1$ algorithm). Accidental collisions could still feasibly occur, but it is desirable to keep such collisions at a minimum.

2. (Broadcast attack.) Suppose that Bob wants to invite Alice, Adam, and Adele to his birthday party, but doesn't want that shady Eve to crash it. Alice, Adam, and Adele have RSA keys $(N_1, 3)$, $(N_2, 3)$, and $(N_3, 3)$, and because they know about the attack above, they have ensured that $\gcd(N_1, N_2) = \gcd(N_2, N_3) = \gcd(N_3, N_1) = 1$. Bob's invitation is short enough so that, as an integer, m satisfies $0 < m < N_1, N_2, N_3$.

   Bob sends $m^3 \bmod N_1$, $m^3 \bmod N_2$, and $m^3 \bmod N_3$ to Alice, Adam, and Adele, respectively. Eve intercepts the encrypted messages, and using the CRT, she can compute $m^3 \bmod N_1 N_2 N_3$. Since $m^3 < N_1 N_2 N_3$, Eve recovers $m^3 \in \mathbb{Z}$, the cube of the integer m. Taking the cube root of m^3 (as a real number), Eve recovers m. Note that Eve can take nth roots of real numbers with relative ease. Result: Eve crashes Bob's party. :(

   In general, if Bob sends the same message to n people and they all have the same public exponent $e \leq n$, then Eve can decrypt the message quickly.

For more basic attacks, see Section 3.3 in the textbook.

Wiener's low private exponent attack on RSA

Next, we will show that Alice should *not* choose her private exponent d to be too small compared to N. This attack requires some basic theory of continued fractions.

Continued fraction expansion of rational numbers

A (finite) **continued fraction** is an expression of the form

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}}$$

where $a_0, \ldots, a_n \in \mathbb{Z}$ and $a_1, \ldots, a_n \geq 1$ (a_0 may be zero or negative). We will use the notation $[a_0; a_1, \ldots, a_n]$ for the continued fraction as above, as well as the rational number that continued fraction represents.

It is a theorem that every rational number u/v (with $v \neq 0$) has exactly **two** continued fraction expansions:

- If $u/v = [a_0; a_1, \ldots, a_n]$ with $a_n \neq 1$, then $u/v = [a_0; a_1, \ldots, a_n - 1, 1]$.
- If $u/v = [a_0; a_1, \ldots, a_n]$ with $a_n = 1$, then $u/v = [a_0; a_1, \ldots, a_{n-1} + 1]$.

So every rational number has a unique *shortest* continued fraction expansion. This expansion is easy to compute using the Euclidean algorithm: Let $u/v = u_0/u_1$ with $\gcd(u_0, u_1) = 1$ and perform the usual Euclidean algorithm computation:

$$\begin{aligned}
u_0 &= u_1 a_0 + u_2 && \text{with } 0 \leq u_2 \leq u_1 - 1, \\
u_1 &= u_2 a_1 + u_3 && \text{with } 0 \leq u_3 \leq u_2 - 1, \\
&\vdots \\
u_{n-1} &= u_n a_{n-1} + u_{n+1} && \text{with } 0 \leq u_{n+1} \leq u_n - 1, \\
u_n &= u_{n+1} a_n
\end{aligned}$$

(note the unusual indexing and also note that actually $u_{n+1} = 1$ because $\gcd(u_0, u_1) = 1$). Then $u_0/u_1 = [a_0; a_1, \ldots, a_n]$; this can be proven easily by induction on n.

Note that the length of the shortest continued fraction expansion of u/v is at most $2\lfloor \log_2 v \rfloor + 2 = O(\ln v)$.

Some examples of continued fractions and convergents

What is the continued fraction expansion of $-199/71$? We have

$$\begin{aligned}
-199 &= 71 \cdot (\mathbf{-3}) + 14, \\
71 &= 14 \cdot \mathbf{5} + 1, \\
14 &= 1 \cdot \mathbf{14},
\end{aligned}$$

so $-199/71 = [-3; 5, 14]$. That is, $-\frac{199}{71} = -3 + \frac{1}{5 + \frac{1}{14}}$.

How about $20411/30967$?

$$\begin{aligned}
20411 &= 30967 \cdot \mathbf{0} + 20411 \\
30967 &= 20411 \cdot \mathbf{1} + 10556 \\
20411 &= 10556 \cdot \mathbf{1} + 9855 \\
10556 &= 9855 \cdot \mathbf{1} + 701 \\
9855 &= 701 \cdot \mathbf{14} + 41 \\
701 &= 41 \cdot \mathbf{17} + 4 \\
41 &= 4 \cdot \mathbf{10} + 1 \\
4 &= 1 \cdot \mathbf{4}
\end{aligned}$$

so $20411/30967 = [0; 1, 1, 1, 14, 17, 10, 4]$.

Convergents and Poincaré's approximation theorem

If $u/v = [a_0; a_1, \ldots, a_n]$, then the rational numbers

$$[a_0], [a_0; a_1], [a_0; a_1, a_2], \ldots, [a_0; a_1, \ldots, a_n]$$

are called the **convergents** to u/v. The convergents to u/v are good approximations to u/v. For example, the convergents to $20411/30967 = 0.659121\ldots$ are 0, 1, $1/2$,

$$\begin{aligned}
2/3 &= 0.666667\ldots \\
29/44 &= 0.659091\ldots \\
495/751 &= 0.659121\ldots \\
4979/7554 &= 0.659121\ldots
\end{aligned}$$

and $20411/30967$.

Wiener's attack relies on the following theorem of Poincaré which gives sufficient conditions for a rational number a/b to be a convergent to a given u/v:

> **Theorem (Poincaré).** Let $u, v, a, b \in \mathbb{Z}$ with $v \geq 1$, $1 \leq b < v$, $\gcd(u, v) = 1$, $\gcd(a, b) = 1$. If
>
> $$\left|\frac{u}{v} - \frac{a}{b}\right| < \frac{1}{2b^2},$$
>
> then a/b is a convergent of u/v.

Wiener's attack

Conceptually, Wiener's attack is based on two facts:

- If $N = pq$ is a "good" RSA modulus (with $p \approx q \approx \sqrt{N}$), then $N \approx \phi(N)$.

- If $ed \equiv 1 \bmod m$ for some modulus $m \geq 1$ and positive integers e and d, then d appears as a denominator in the convergents of e/m. (For the same reason that one can use the Euclidean algorithm to compute multiplicative inverses modulo m.)

Wiener's idea is this: Because $ed \equiv 1 \bmod \phi(N)$, d appears as a denominator in the continued fraction expansion of $e/\phi(N)$. If $N \approx \phi(N)$, then e/N (which Eve knows) and $e/\phi(N)$ (which Eve does **not** know) have some convergents in common, namely those with "small denominator." More precisely,

> **Theorem (Wiener).** Let $N = pq$ where p and q are distinct odd primes and let e be an integer relatively prime with $\phi(N)$. Let d satisfy $ed \equiv 1 \bmod \phi(N)$ and $1 \leq d < \phi(N)$.
>
> If $q < p < 2q$, $1 \leq e < \phi(N)$, and $d < \frac{1}{3}N^{1/4}$, then k/d is a convergent to e/N, where $k = \frac{ed-1}{\phi(N)}$ (note that by this definition, k and d are relatively prime).
>
> In particular, if (N, e) is Alice's public RSA key and d is her decryption exponent, then Eve can factor N in time $O(\ln N)$.

Here's how Eve mounts Wiener's attack: Eve begins by computing the set

$$S = \{ \text{ convergents } k/d \text{ to } e/N : d < \tfrac{1}{3}N^{1/4} \}$$

which has size $O(\ln N)$. Eve then enumerates $S = \{k_1/d_1, \ldots, k_r/d_r\}$ and computes the values $t_i = \frac{e_i d_i - 1}{k_i}$. If t_j is an integer and $X^2 - (N - t_j + 1)X + N$ has integer roots, then $t_j = \phi(N)$ and the roots of that quadratic are the prime factors of N.

An example of Wiener's attack

Suppose that Alice's public key is $(27962863, 25411171)$. Eve suspects that Alice has chosen her decryption exponent $d < \frac{1}{3}N^{1/4} \approx 24.2395$. Eve computes the first few terms of the continued fraction expansion of $25411171/27962863$:

$$\frac{25411171}{27962863} = [0; 1, 9, 1, 23, 7, \ldots]$$

and the first few convergents:

$$0, \quad 1, \quad \frac{9}{10}, \quad \frac{10}{11}, \quad \frac{239}{263}, \quad \ldots$$

so (with notation as above), $S = \{0, 1, 9/10, 10/11\}$.

- Eve can reject the possibility that $k/d = 0$ and the possibility that $k/d = 1$, because either would mean that Alice chose $d = 1$, which would mean that $e = 1$.
- Eve can also reject $k/d = 9/10$ because $d = 10$ is not relatively prime with $\phi(N)$, which must be even (because $N \geq 3$).

Thus, Eve suspects that $k = 10$ and $d = 11$. Taking $t = \frac{ed-1}{k} = 27952288$, she computes the roots of

$$X^2 - (N - t + 1)X + N = X^2 - 10576X + 27962863$$

using the quadratic formula (for example), and finds that $N = 5279 \cdot 5297$.

Motivation and ways around Wiener's attack

In the usual formulation of RSA, Alice chooses p and q, then an integer e relatively prime with $(p-1)(q-1)$. The pair $(N, e) = (pq, e)$ is her public key, and her private key is $(\{p, q\}, d)$ where d is an integer such that $ed \equiv 1 \mod (p-1)(q-1)$.

However, it is totally reasonable for Alice to begin by choosing d, her **private exponent** before e, her **public exponent**. That is, Alice can choose p and q, then d relatively prime to $(p-1)(q-1)$, and publish (N, e) where e satisfies $ed \equiv 1 \mod (p-1)(q-1)$. Alice might want to choose d to be small because the speed of decryption is directly dependent on the size of d.

As shown above, Alice should not take her d to be *too* small compared to N, because then Eve can implement Wiener's attack. There are two ways around this from Alice's point of view:

- Alice can keep her small private exponent d and replace e with $e' = e + t\phi(N)$ for some $t \geq 1$. If $e' > N^{3/2}$, then the proof of Wiener's attack actually fails—this is why the theorem statement above requires $e < \phi(N)$ (note that $\phi(N) \leq N$). Hence, if Alice publishes (N, e') with $e' > N^{3/2}$ and $e' \equiv e \mod \phi(N)$, then Eve can't use Wiener's attack, but $ed \equiv e'd \equiv 1 \mod \phi(N)$ so e' and d still function as a public exponent and private exponent for RSA.

  Counterpoint: If Alice chooses a value of e which is too large, encryption becomes *slower*. Even though encryption and decryption are fast "asymptotically" (because of fast powering e.g., they take only polynomial time), Bob might still notice a slowdown in encryption for large values of e.

- Another way Alice might save memory and time is by instead storing her decryption exponent d as a pair (d_p, d_q) where $1 \leq d_p < p-1$, $1 \leq d_q < q-1$, $\gcd(d_p, p-1) = 1$ and $\gcd(d_q, q-1) = 1$. Alice then can choose (in some predetermined way) a value d such that $1 \leq d < \phi(N)$ satisfying $d \equiv d_p \mod (p-1)$ and $d \equiv d_q \mod (q-1)$ (there are multiple such d because $\gcd(p-1, q-1) > 1$).

  Now, if d_p and d_q are small, d might still be large enough to thwart Wiener's attack! Furthermore, to decrypt a ciphertext c which Bob has sent her, Alice just has to compute $m_p \equiv c^{d_p} \mod p$ and $m_q \equiv c^{d_q} \mod q$ and use the CRT to recover the plaintext $m \mod pq$. This approach still has some vulnerabilities, but we won't touch on them here, and they are not serious enough to allow Eve to factor N in polynomial time.