Wiener's attack on small private RSA exponent

October 7, 2023

1 Explanation from YouTube

A really nice explanation from Jeff Suzuki on YouTube. I transcribed it and added some extra comments.

Recall the basic components of RSA:

1. a *public* encryption exponent e and public modulus N,
2. a *private* decryption exponent d and factorization $N = pq$,
3. where $ed = k\phi(N) + 1$, i.e., e and d are each other's modular inverse wrt modulus $\phi(N)$ ($\phi(N) = (p-1)(q-1)$ since p and q are primes).

Note then that what we need to break the thing given the public key is $\phi(N)$, and not the actual factorization of N. This idea is the basis of Wiener's attack.

$$\begin{aligned}\phi(N) &= (p-1)(q-1)\\ &= pq - (p+q) + 1\\ &\approx N\end{aligned}$$

To summarize, since p and q are large, $\phi(N)$ is reasonably close to N. But then, we can solve the equation $ed = k\phi(N) + 1$ as follows:

$$\begin{gathered}ed - k\phi(N) = 1\\ \frac{e}{\phi(N)} - \frac{k}{d} = \frac{1}{d\phi(N)}\\ \frac{e}{N} \approx \frac{k}{d}\end{gathered}$$

In the first step, we divided both sides by $d\phi(N)$. Then, since $\frac{1}{d\phi(N)}$ is tiny enough to approach zero, we concluded that $\frac{e}{N}$ is approximately equal to $\frac{k}{d}$.

Now we'll try to find $\frac{e}{N}$ using the theorem of continued fractions: we're going to try and find a set of fractions (the *convergents*) $\frac{k}{d}$ that approximate $\frac{e}{N}$. We intend to save ourselves a lot of trouble by making the following observations:

1. Since $ed \equiv 1 \mod \phi(N)$, and $\phi(N)$ will be an even number (this is because p and q are large primes and thus odd - 2 is the only even prime number - $(p-1)$ as well as $(q-1)$ are even, and so is their product), d must be odd since if it were even, ed wouldn't be equal to $k\phi(N)+1$, which is an odd number. Thus, if we find a convergent where the denominator d is odd, we will move on to the next.

2. Since $\phi(N)$ must be a whole number, we'll check $\frac{ed-1}{k}$. If this isn't a whole number, we'll move on to the next convergent.

So, for all convergents where these two exclusion criteria don't apply and we thus have found a potential candidate for d, how do we check if we have indeed found the right value? This is where we'll harness the theory of quadratic equations. Suppose p, q are the primes whose product is N. Then we have:

$$\begin{aligned}
&\phi(N) = (p-1)(q-1) \\
&\phi(N) = pq - (p+q) + 1 \\
&\phi(N) = N - (p+q) + 1 \\
&p + q = N - \phi(N) + 1
\end{aligned}$$

Now consider the quadratic equation $(x-p)(x-q)$, whose roots are p, q, the prime factors of N. We have:

$$\begin{aligned}
(x-p)(x-q) &= 0 \\
x^2 - (p+q)x + pq &= 0
\end{aligned}$$

There are a few things of note about this equation: firstly, $pq = N$; secondly, as we've seen above, $p + q = N - \phi(N) + 1$. Thus:

$$x^2 - (N - \phi(N) + 1)x + N = 0$$

If we've found the correct value for $\phi(N)$, then the roots of this equation will be whole numbers, and the factors of N.

2 Proof seen in class at TUB

Wiener's assumptions:

1. $q < p < aq$

2. $e < \phi(N)$

3. $d < \frac{1}{\sqrt{2(a+1)}} n^{\frac{1}{4}}$

Then, the error between N and $\phi(N)$ is:

$$\begin{aligned}
0 &< N - \phi(N) \\
N - \phi(N) &= pq - (p-1)(q-1) \\
&= pq - pq - (p+q) + 1 \\
&= (p+q) + 1 \\
(p+q) + 1 &< (a+1)q \\
(a+1)q &\leq (a+1)\sqrt{N}
\end{aligned}$$

Where we used assumption one from above: $(p+q) < aq + q$ as well as the fact that $q \approx \sqrt{N}$ since $N = pq$. a is some small number, e.g. 2.

For the error between the fractions, we have:

$$\begin{aligned}
|\frac{e}{n} - \frac{k}{d}| &= |\frac{ed - k\phi(N) - kn + k\phi(N)}{Nd}| \\
&= |\frac{1 - k(N - \phi(N))}{nd}| < \frac{(a+1)k\sqrt{N}}{Nd} = \frac{(a+1)k}{d\sqrt{N}} \\
|\frac{e}{n} - \frac{k}{d} &< \frac{a+1}{\sqrt{N}} \leq \frac{a+1}{2(a+1)d^2} = \frac{1}{2d^2}
\end{aligned}$$

In line one, we did the standard expansion to achieve a common denominator, and then used a classic Mathematician's trick: we added and subtracted $k\phi(N)$, i.e., we added zero.

This helps us because now we can use the fact that $ed \equiv 1 \mod \phi(N)$, and thus $ed - k\phi(N) = 1$. That's how we get to line two.

Then, we use the result from above: $N - \phi(N) \leq (a+1)\sqrt{(N)}$.

For the last step in line two, we simply divide by $\sqrt{(N)}$.

Then, to get to line three, we use: $k\phi(N) = ed - 1$ and $e < \phi(N) \implies k < d$.

All of this to arrive at the magical value $\frac{1}{2d^2}$, which tells us that $\frac{k}{d}$ is a continued fraction of $\frac{e}{n}$.