RSA (CONTINUED): WHEN THE EXPONENT IS LEAKED

MATH 195

We prove the following fact:

Claim. There is a fact algorithm that given $n > 1$ odd and given $m \in \mathbb{Z}_{>0}$ satisfying

$$\forall a \in (\mathbb{Z}/n\mathbb{Z})^* : a^m = 1,$$

'in practice' factors n completely into primes.

We do so via factoring by means of square roots of 1. Suppose that we have a nonstupid way of generating elements $x \in \mathbb{Z}/n\mathbb{Z}$ such that $x^2 = 1 \pmod{n}$ (i.e. $x \neq 1, -1$). Namely, $x^2 \equiv 1 \pmod{n}$ implies that

$$n \mid (x^2 - 1) = (x + 1)(x - 1)$$

so $n \mid \gcd(n, x+1) \gcd(n, x-1)$. Since $x \neq 1, -1$, this 'in practice' gives a nontrivial factorization of n.

Example. For $n = 35$, $x = 29$ gives $26^2 = 841 \equiv 1 \pmod{35}$, and indeed

$$35 = n \mid \gcd(35, 30) \gcd(35, 28) = 5 \cdot 7.$$

Theorem. *Suppose n is a positive* odd *integer. Then*

$$\#\{x \in \mathbb{Z}/n\mathbb{Z} : x^2 \equiv 1 \pmod{n}\} = 2^t$$

where t is the number of distinct prime factors of n.

The proof of this involves the Chinese remainder theorem. Factor for example $n = 45 = 3^2 \cdot 5$. The roots are then the unique solutions to $x \equiv \pm 1 \pmod{3}$ and $x \equiv \pm 1 \pmod{5}$. For example, $x \equiv 1 \pmod{3}$, $x \equiv 1 \pmod{5}$ gives $x \equiv 1 \pmod{45}$, whereas $x \equiv 1 \pmod{3}$ and $x \equiv -1 \pmod{5}$ gives $x \equiv 19 \pmod{45}$ and $19^2 = 361 \equiv 1 \pmod{45}$.

Here, then, is the algorithm in the claim.

(1) Write $m = 2^k \cdot u$ where u is odd and $k \geq 1$. [Note: m is even, take $a = -1$.]
(2) Pick $a \in \mathbb{Z}/n\mathbb{Z}$, $a \neq 0$, at random.
(3) Compute $a^u \in \mathbb{Z}/n\mathbb{Z}$. If $a^u \equiv 1$, pronounce failure and go back to the previous step.
(4) [Suppose $a^u \neq 1$.] By repeated squarings, compute $a^{2u} = (a^u)^2$, $a^{2^2 u} = (a^{2u})^2$, and so on, until for the first time we have $a^{2^i u} = 1$. [Note: If $a \in (\mathbb{Z}/n\mathbb{Z})^*$ then this happens for $i = k$ and maybe earlier.]
(5) Put $x = a^{2^{i-1} u}$. [Note $i \geq 1$.] [Then $x \neq 1$, $x^2 = 1$.] If $x = -1$, pronounce failure and go back to (2).
(6) [Now $x \neq -1$.] Compute $\gcd(n, x + 1) = n_+$, $\gcd(n, x - 1) = n_-$. Then $n = n_+ n_-$ is a nontrivial factorization, and n_+ and n_- can be factored recursively. [With the same m.]

This is some of the material covered March 5, in Math 195: Cryptography, taught by Hendrik Lenstra, prepared by John Voight `jvoight@math.berkeley.edu`.

(7) If no $i < k$ can be found in (4), then compute $\gcd(a, n)$ [it is > 1 and $< n$] and factor $\gcd(a, n)$ and $n/\gcd(a, n)$ recursively.
(8) If 'many' choices of a lead to failure in (3) or (5), then 'most likely' n is of the form p^ℓ with p prime and $\ell \geq 1$.

The heuristics in (8) are explained by the following theorem:

Theorem. *Suppose n has at least 2 distinct (odd) prime factors (so $t \geq 2$). Then the number of $a \in \mathbb{Z}/n\mathbb{Z}$ such that $a \neq 0$, a leads to failure in* (3) *or* (5) *above has*

$$\frac{\#\{a \in \mathbb{Z}/n\mathbb{Z} : a \neq 0,\ a \text{ fails}\}}{n-1} < \frac{1}{2}.$$