COMP 8920: Cryptography Winter 2025

Lecture 21 — March 25, 2025

Prof. Curtis Bright *Scribe: Rajat Yadav*

Miller-Rabin primality test:

Write $n-1 = 2^k m$ for $k \in \mathbb{Z}$ and m odd, then consider the sequence $a^{n-1} \bmod n, a^{(n-1)/2} \bmod n, a^{(n-1)/2^2} \bmod n, \ldots, a^{(n-1)/2^k}$, Recall if n is prime, the first entry will be 1 by Fermat's little theorem, and the second entry will be ± 1 by Euler's criterion. In general if n is prime, this sequence must be of the form $(1, 1, \ldots, 1, -1, *, *, *)$ or $(1, 1, \ldots, 1)$ where $*$ denotes a number not ± 1. So, given n, if the above sequence is of the form $(*, *, \ldots, *)$ (quite likely if n is not prime) or $(1, 1, 1, *, *, *, \ldots, *)$ then we can be sure that n is not prime. Every number in the sequence is the square of the number to its right, so in this case we would have a number not ± 1 when squared gives 1 which cannot happen when n is prime. The first case cannot happen when n is prime by Fermat's little theorem. So, Miller-Rabin computes this sequence starting from the right entry $(a^{(n-1)/2^k}) \bmod n = a^m \bmod n$. If it is ± 1, n is likely prime. Then square it to compute the number to its left. If this is -1 n is likely prime, but if it is 1, n cannot be prime as we found a square root of 1 that is not ± 1. Repeat this until the 2^{nd} last entry which must be ± 1 by Euler's criterion if n is prime. The error probability is at most $1/4$, and this is very pessimistic in practice.

Square roots mod n: Say n is odd and $a \in \mathbb{Z}_n^*$. We know if n is prime that has either two square roots $\bmod n$ (when $\left(\frac{a}{n}\right) = 1$) or no square roots $\bmod n$ when $\left(\frac{a}{n}\right) = -1$). In fact, when n is a prime power, i.e., $n = p^e$ for prime p and $e \in \mathbb{Z}^*$, a has two square roots exactly when $\left(\frac{a}{p}\right) = 1$. For general n, we have the following:

Thm: If $n > 1$ is odd and $n = \prod_{i=1}^{l} p_i^{e_i}$ is its prime factorization then if $a \in \mathbb{Z}_n^*$ there are 2^l square roots of a when $\left(\frac{a}{p_1}\right) = \left(\frac{a}{p_2}\right) = \cdots = \left(\frac{a}{p_l}\right) = 1$ and no square roots if $\left(\frac{a}{p_i}\right) = -1$ for any $1 \le i \le l$

Proof by CRT:

$$y^2 \equiv a \pmod{n} \Leftrightarrow \begin{cases} y^2 \equiv a \pmod{p_1^{e_1}} \\ y^2 \equiv a \pmod{p_2^{e_2}} \\ \vdots \\ y^2 \equiv a \pmod{p_l^{e_l}} \end{cases}$$

When $\left(\frac{a}{p_i}\right) = -1$ for some i, then $y^2 \equiv a \pmod{p_i^{e_i}}$ has no solutions, so $y^2 \equiv a \pmod{n}$ has none either. When $\left(\frac{a}{p_i}\right) = 1$ for all i, then each $y^2 \equiv a \pmod{p_i^{e_i}}$ has exactly two solutions, say $\pm b_i$. Each choice of $\pm$ results in a different system of congruences

$$\begin{cases} y \equiv \pm b_1 \pmod{p_i^{e_i}} \\ \vdots \\ y \equiv \pm b_l \pmod{p_i^{e_i}} \end{cases}$$

which for each choice of $\pm$ gives a unique solution by CRT. Thus, as there are 2^l choices of $\pm$, there are 2^l solutions of $y^2 \equiv a \pmod{n}$. A special case of this theorem says that for RSA moduli $n = p \cdot q$ there are exactly $2^2 = 4$ square roots of 1 mod n. Clearly ± 1 are square roots of 1 mod n so, there are two non-trivial square roots of 1 mod n. E.g., if $n = 403 = 13 \cdot 31$, the roots of 1 are ± 1 and ± 92 as $92^2 \equiv 1 \pmod{403}$. We'll show that knowledge of either non-trivial root of 1 allows factoring n.

For suppose $y^2 \equiv 1 \pmod{n}$, but $y \not\equiv \pm 1 \pmod{n}$ so y is a non-trivial square root of 1 mod n. This means that $n \mid (y^2 - 1)$ but $n \nmid (y \pm 1)$. This means $pq \mid (y^2 - 1) = (y-1)(y+1)$, so we know $p \mid (y-1)(y+1)$ which since p is prime, $p \mid (y-1)$ or $p \mid (y+1)$. In the first case, we must have $q \nmid (y-1)$, because if $q \mid (y-1)$ and $p \mid (y-1)$ then $pq \mid (y-1)$ as p, q are distinct primes, and this contradicts $n \nmid (y-1)$. In the second case, we must have $q \nmid (y+1)$ as otherwise $pq \mid (y+1)$ but $n \nmid (y+1)$. Since p is a common divisor of $y \pm 1$ and n, we can compute $\gcd(n, y \pm 1) = p$ (in the first case, $\gcd(n, y-1) = p$ and in the second case $\gcd(n, y+1) = p$). E.g. in the example $y = 92$ and $\gcd(403, 92+1) = 31$ and $\gcd(403, 92-1) = 13$.

The best general factoring algorithm, The number field sieve uses this kind of idea to factor n. The simplest factoring algorithm is trial division by all small primes up to some bound. Since any composite n will have a prime factor $\leq \sqrt{n}$ you only need to trial divide by $\sqrt{n}$. However, if n is 1024 bits then $n \approx 2^{512}$, there are far too many divisors to check. Trial division is feasible up to 2^{40} or so, but becomes exponentially slower as n increases. We'll cover some other attacks on RSA. First, note that it is crucial that $\phi(n)$ is not publicly revealed. For suppose $n = pq$ and $\phi(n) = \phi(pq) = \phi(p)\phi(q) = (p-1)(q-1)$. Then substitute $q = n/p$ into this to get $\phi(n) = (p-1)(n/p-1) = n - n/p - p + 1$ so, multiply by p to get $p \cdot \phi(n) = np - n - p^2 + p \Rightarrow p^2 + (\phi(n) - n - 1)p + n = 0$ which can be solved with the quadratic equation $p = (n - \phi(n) + 1 \pm \sqrt{(\phi(n) - n - 1)^2 - 4n})/2$. E.g., if $n = 84773093$ and $\phi(n) = 84754668$ then $p = (18246 \pm \sqrt{425104})/2 = 9213 \pm 326$, so p is 9539 or 8887.