Birthday Paradox

r people / elements

N days of year / possible values

Q: any repeats?

Prob. of no repeats: $\left(1-\frac{1}{N}\right)\left(1-\frac{2}{N}\right)\left(1-\frac{3}{N}\right)\cdots\cdots\left(1-\frac{r-1}{N}\right) \approx 1-e^{-\frac{r^2}{2N}}$

prob. 2nd doesn't match 1

prob. 3rd doesn't repeat

r^{th} person

drops below $\frac{1}{2}$ around $\frac{r^2}{2N} \sim 0.8$ ie. $r \sim O(\sqrt{N})$

Collision Attacks (Birthday Attacks)

① Baby-Step-Giant-Step is an "organized" Birthday attack:

List A: g^{r_i}

List B: hg^{-s_i}

Collision: $g^{r_i} = hg^{-s_j}$

$h = g^{r_i + s_j}$

② Birthday Attack on RSA:

Public key (n, e) c = ciphertext

Recall: $c = m^e \pmod n$

List A: $cx^{-e} \pmod n$ for various x

List B: $y^e \pmod n$ " " y

Collision: $cx^{-e} \equiv y^e \pmod n$

$c \equiv (xy)^e \pmod n \Rightarrow$ message could be xy

Notes ① random x, y $\longrightarrow$ need lists of size $O(\sqrt{n})$

② If we know $m < B$ for some small bound B

then try $0 < x, y < \sqrt{B}$, chances are decent (?)

that we find $xy = m$.

Lesson: pad short messages.

Finding Primes

How many primes are there?

$$\pi(N) = \#\text{ of primes } 0 < p < N \sim \frac{N}{\log N} \sim \int_2^N \frac{dt}{\log t}$$

So, for integers of size $\sim N$, the "probability" of being prime is $\frac{1}{\log N}$ (not bad).

So with polynomially many ($O(\log N)$ tries, we'll stumble on a prime.

So all we really need is primality testing.

Recall: Fermat's Little Theorem

Let p be prime, a coprime to p, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Observation: Generally fail for p not prime!

Fermat Primality Test

Let $n > 1$ be a number to test.

Choose $1 < a < n$. (Could check $\gcd(a, n) = 1$.)

Compute $a^{n-1} \pmod{n}$.

(If n is prime, gives 1.) If $a^{n-1} \not\equiv 1$ then n is not prime.

If $a^{n-1} \equiv 1$ then n is probably prime.

Examples.

① $n = 1007$

Choose $a = 2$

Compute $2^{1006} \equiv 271 \pmod{1007}$

$\Rightarrow$ Composite

② $n = 1009$

Choose $a = 2$

Compute $2^{1008} \equiv 1 \pmod{1009}$

$\Rightarrow$ Probably prime!

Try $a = 3$

$3^{1008} \equiv 1 \pmod{1009}$

$\Rightarrow$ Very probably prime!

③ $n = 561$

Choose $a = 2$

Compute $2^{560} \pmod{561}$

$\equiv 1$

ACK! $3 \mid 561$

$3^{560} \neq 1$

Actually composite.

$\Rightarrow$ probably prime

Notes: ① For more confidence, try more a's.

② Stronger versions, eg. Miller-Rabin, Solovay-Strassen

Q: How many "fakers" (false positives)?

Data: $X < 10^{10}$

$\exists$ 455 052 511 primes

14 884 pseudoprimes to base = 2
i.e. composite n s.t. $2^{n-1} \equiv 1 \pmod{n}$

3 291 strong pseudoprimes to base = 2
i.e. composites that pass Miller-Rabin test

0 strong pseudoprimes to base 2, 3, 5, 7 simultaneously

A Carmichael number: is an integer n s.t. for all $0 < a < n$ if $\gcd(a, n) = 1$ then $a^{n-1} \equiv 1 \pmod{n}$ but n is composite.

In practice, we use these tests to find p, q for RSA.

("good enough")

Square roots & Factoring

Sps $x^2 \equiv y^2 \pmod{n}$ but $x \not\equiv \pm y \pmod{n}$