1. Primality testing

primality $\longleftrightarrow$ Factoring

* Fermat test
  - Efficient
  - Reliable
* Generate random primes?

N n bits

$N \approx 2^{1000}$ $n = 1000$

RSA 250	829 bit	Feb 2020
	896 bit	$75K
	1024 bit	$100K

2. Hash functions

Fermat test:

Fermat's little theorem: If N is prime then

$$\forall a \not\equiv 0 \pmod N \quad a^{N-1} \equiv 1 \pmod N$$

Fermat test: Input N.

Pick a at random $a \not\equiv 0 \pmod N$

check whether $a^{N-1} \equiv 1 \pmod N$

Efficient: $a^{(N-1)} \pmod N$

$a^x \pmod N$ efficient.

Repeated squaring: suppose $x = 2^{1000}$

$y = x^2 \pmod N \longrightarrow z = y^2 \pmod N \equiv x^4 \pmod N$

$\downarrow$

$z^2 \bmod N \equiv y^4 \equiv x^8 \pmod N$

$x^k \xrightarrow{\text{square}} x^{2k} \pmod N$

$x^k \xrightarrow{\text{multiply by } x} x^{k+1} \pmod N$

exponent = $\underline{1011}\,101$

exponent = 1 $\xrightarrow{\text{square}}$ 10 $\xrightarrow{\text{square}}$ 100 $\xrightarrow{\times}$ 101

$\downarrow$ square

1010 $\xrightarrow{\times}$ 1011 $\xrightarrow{\text{square}}$ 10110 $\xrightarrow{\times}$ 10111 $\xrightarrow{\text{square}}$ 101110

square $\downarrow$

1011101 $\xleftarrow{\times}$ 1011100

Reliable?

Fermat: N prime $\quad a^{N-1} \equiv 1 \pmod N$
$\forall a \not\equiv 0 \bmod N.$

N composite $\qquad 3 \cdot 4 = 12$

$a = 3 \qquad 3^{11} \not\equiv 1 \pmod{12}$

$a \qquad 5^{11} \equiv 1 \pmod{12}$?

Carmichael numbers: N: $\forall a \ \gcd(a, N) = 1$
$a^{N-1} \equiv 1 \pmod N$

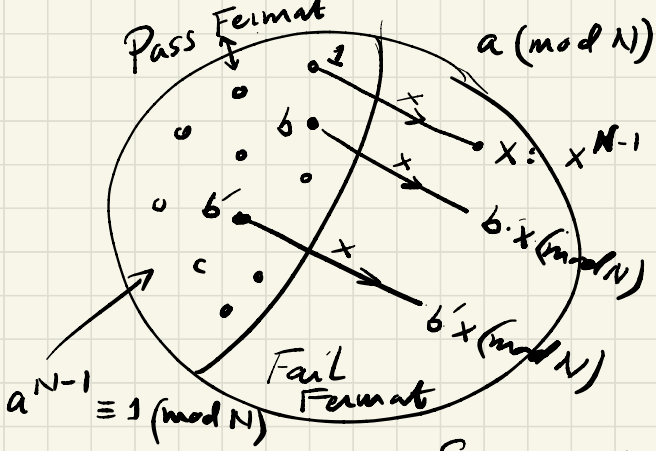
$N = 561 = 3 \cdot 11 \cdot 17$

Today's lecture: assume N is not Carmichael.

$\therefore \ \exists x : \gcd(x, N) = 1$ and $x^{N-1} \not\equiv 1 \pmod N$
$\exists x$ Fails Fermat test.

$\Downarrow$

For at least half choices of $a \pmod N$ $\quad \gcd(a, N) = 1$
$a^{N-1} \not\equiv 1 \bmod N.$
Half choices of a fail Fermat.



$a \pmod N$: $\gcd(a, N) = 1$

x: $x^{N-1} \not\equiv 1 \pmod N$

$b \cdot x \pmod N$

$b' x \pmod N$

$$(bx)^{N-1} \equiv b^{N-1} x^{N-1}$$
$$\equiv x^{N-1} \not\equiv 1 \pmod N$$

Since $x^{-1} \pmod N$ exists it follows that

$b \not\equiv b' \pmod N$ then $bx \not\equiv b'x \pmod N$

If N prime $\Rightarrow$ always passes Fermat test.

If N composite $\Rightarrow$ passes with probability $\leq 1/2$.
(2 is Carmichael)

Repeat Fermat test k times:

If N prime $\longrightarrow$ passes all k tests.

if N composite $\longrightarrow$ passes all k w.p. $\leq \frac{1}{2^k}$.

$k = 10$ wp $\leq \frac{1}{1000}$.

$K = 20$ wp $\leq \frac{1}{1000000}$

Repeat

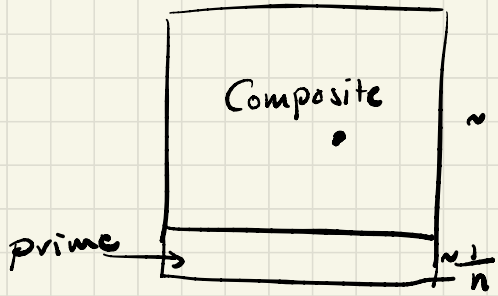
N: Fermat 20 times $\Rightarrow$ N is prime w.p $\geq 1 - \frac{1}{1000000}$

N=12 Prime number theorem:

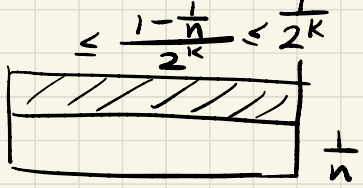
Numbers $\leq x$ $\quad$ # primes $\approx \frac{x}{\ln x}$

n bit numbers $\approx \frac{1.44}{n}$ $\quad$ n-bit number are prime.

choose $k = 3 \log n$, $2^k \approx n^3$



k reps of Fermat



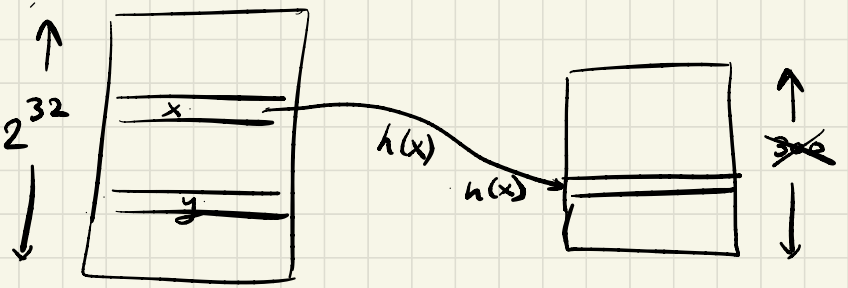
$P[\text{composite}] \leq \frac{\frac{1}{2^k}}{1/n} \approx \frac{n}{2^k} \approx \frac{1}{n^2}$

Hash Functions

Set of IP addresses : 32 bit # $4 \times \underbrace{8 \text{ bits}}_{0 - 255}$

$$x = (x_1, x_2, x_3, x_4)$$

membership
insert
delete



$h(x)$

$p > 256$

$p = 257$

$|S| = K$

$E[\#\text{keys that map to } h_a(x)] \text{ is } \frac{K}{p}$

$a = (a_1, a_2, a_3, a_4)$ at random (mod 257)

$$h_a(x) = a_1 x_1 + a_2 x_2 + a_3 x_3 + a_4 x_4 \pmod{257}$$

Universal hash function : $x \neq y$ $\quad P[h_a(x) = h_a(y)] = \frac{1}{p} = \frac{1}{257}$

$$h_a(x) = a_1 x_1 + a_2 x_2 + a_3 x_3 + a_4 x_4 \pmod p$$

a_1, a_2, a_3, a_4 chosen at random mod p.

Claim $x \neq y$ then $P[h_a(x) = h_a(y)] = \frac{1}{p}$ ✓

$$a_1 x_1 + a_2 x_2 + a_3 x_3 + a_4 x_4 \equiv a_1 y_1 + a_2 y_2 + a_3 y_3 + a_4 y_4 \pmod p$$

Say $x_2 \neq y_2$

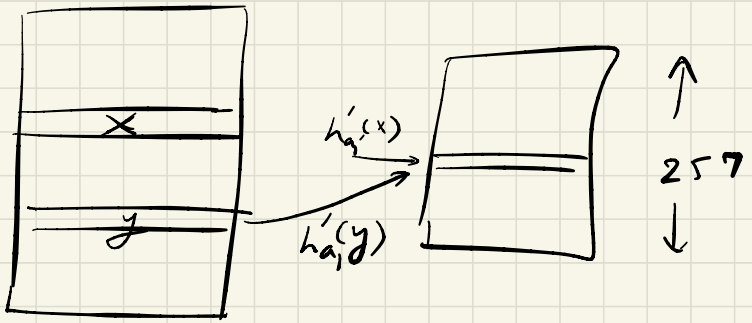
Pick a_1, a_3, a_4. What condition must a_2 satisfy to result in $h_a(x) = h_a(y)$?

$$a_2(x_2 - y_2) \equiv a_1 y_1 + a_3 y_3 + a_4 y_4 - a_1 x_1 - a_3 x_3 - a_4 x_4 \pmod p$$

$$\equiv c \pmod p$$

$$a_2 \equiv (x_2 - y_2)^{-1} c \pmod p$$

$$h'_{a_1}(x_1, x_2, x_3, x_4) = x_1 + x_2 + x_3 + x_4 + a_1 \pmod p$$



$$x \neq y \quad \Rightarrow \quad P\left[h'_a(x) = h'_a(y)\right] = \frac{1}{p} \; ?$$

but $\quad x_1 + x_2 + x_3 + x_4 \equiv y_1 + y_2 + y_3 + y_4 \pmod p$