4/24/03
fd

Lecture 18: Computational Number Theory

Public Key Encryption Systems

Alice and Bob want to communicate private messages on a public communications channel.

1. Encryption: How can Bob encode a message into cyphertext that only Alice can decode?
2. Digital Signatures: How can Alice send a message so Bob knows it is from her?

If Alice and Bob announce the encryption scheme, couldn't any eavesdropper then decrypt the msg?

Public Key (P_A, P_B) ← Alice, Bob

Secret Key (S_A, S_B)

} Keys map to functions that can be applied to msgs.

Properties: $S_A(\underbrace{P_A(M)}_{\text{encrypted msg = cyphertext} = C}) = M$ → $P_A()$ & $S_A()$ are functional inverses

$P_A(S_A(M)) = M$

How to Use:

Encryption Bob: $M \xrightarrow{P_A} C = P_A(M)$ Alice: $C \xrightarrow{S_A} M = S_A(C)$

transmit on insecure channel

↳ eavesdropper

Digital Signature

Alice signs M':

$M' \xrightarrow{S_A} \sigma = S_A(M')$

transmit (M', σ) on insecure channel

Bob verifies M' comes from Alice

Does $M' \stackrel{?}{=} P_A(\sigma)$?

Combined (Sign encrypted msg): Transmit $P_B((M', \sigma))$

Problem: Trusting a Public Key

Fundamental Difficulty: Create system of functions whereby many pair combinations of P_A and S_A can be easily formed such that disclosure of P_A does not allow others to determine S_A.

RSA Public Key Cryptosystem → World Standard

Ronald Rivest (MIT EECS; author of CLRS)
Adi Shamir
Leonard Adleman

2002 Turing Award winners

→ Based on relative ease of finding large prime numbers and extreme difficulty of factoring product of two primes.

RSA

① Let $p \neq q$ be 2 large prime integers (512 or 1024 bits)

② Let $n = p \cdot q$ and $\phi(n) = (p-1)(q-1)$

③ Let e be small, odd integer such that

$$\underbrace{\gcd}_{\text{greatest common divisor}}(e, \phi(n)) = 1 \implies e \text{ and } \phi(n) \text{ are "relatively prime"}$$

④ Compute d such that $d \cdot e \equiv 1 \pmod{\phi(n)}$ [multiplicative inverse]

Publish $P = (e, n)$ as Public Key

Keep $S = (d, n)$ as ~~Private~~ Secret Key

Encryption: $C = P(M) \equiv M^e \pmod{n}$

Decryption:
$$
\begin{aligned}
S(C) &= C^d \pmod{n} \\
&\equiv M^{ed} \pmod{n} \qquad ed = 1 + k\overbrace{(p-1)(q-1)}^{\phi(n)} \\
&\equiv M^{1+k(p-1)(q-1)} \pmod{n} \\
&\ \ \vdots \\
&\equiv M \pmod{n}
\end{aligned}
$$

Number theoretic results beyond the scope of this class

One method of cracking code is to find $\underline{d}$. This requires factoring n into p and q to construct $\phi(n) = (p-1)(q-1)$ to compute $\underline{d}$ in step ④. Factoring product of two large primes turns out to be very difficult.

The desity of prime numbers is rather large

Prime distribution function $= \pi(n) =$ # of primes less than or equal to n.

Prime number theorem: $\lim_{n \to \infty} \pi(n) = \frac{n}{\ln n}$

Probability that n is prime is $\approx \frac{1}{\ln n}$

Thus need to examine $\approx \ln n$ integers near n to find a prime

For 512-bit prime number, examine $\approx \ln 2^{512} \approx 355$ random numbers (half that value if restrict to odds).

Primality Testing

(A) Naive: Trial Division

- Divide by each integer $2, 3, \ldots$ up to $\lfloor \sqrt{n} \rfloor$
- can skip evens beyond 2
- exponential in length of n because β bits $\Rightarrow$ — assuming division can be done in constant time.

$$\beta = \lceil \lg(n+1) \rceil \rightarrow 2^\beta - 1 \; n \Rightarrow \sqrt{n} = \Theta(2^{\frac{\beta}{2}})$$

(B) Pseudo-primality Testing (almost works)

Definition: $\underline{n}$ is a base-a pseudoprime if n is composite and
$a^{n-1} \equiv 1 \pmod{n}$

Note: By Fermat's theorem if p is prime then $\underline{a^{p-1} \equiv 1 \pmod{p}}$
for $\underline{\text{all}}$ ~~...~~ integer $a : 0 < a < p$

$p = 7$: $a^6 \underset{a^{p-1}}{\equiv} 1 \pmod{7}$

p		
7:	$a = 2$	$a^6 = 2^6 = 64 \xrightarrow{\text{mod } 7} 1$
6:	$a = 2$	$a^5 = 2^5 = 32 \xrightarrow{\text{mod } 6} 2$
5:	$a = 2$	$a^4 = 2^4 = 16 \xrightarrow{\text{mod } 5} 1$

If n does $\underline{\text{not}}$ satisfy above for some $\underline{a}$, then n is composite

While not rigorously true, it turns out that if $\underline{n}$ does satisfy above for some $\underline{a}$, $\underline{n}$ is usually prime.

Errors are rare. Let $a = 2$

For only 22 values of $n < 10{,}000$ does this fail

512-bit # will be prime in all but ~1 out of 10^{20} trials

1024-bit # " " " " " " ~1 out of 10^{41} trials

You might try to improve by checking more values of $\underline{a}$. However, there is a small class of #s (Carmichael numbers) for which this strategy will fail for all values of a.

↘ better soln.

(c) Miller-Rabin Randomized Primality Testing

Two fixes:

- multiple, random values of a
- detects possibility of Charmichael numbers

Let WITNESS (a, n) be a routine that reports whether the integer a can demonstrate n is composite.

let $n-1 = 2^t u$, where $t \geq 1$ and u is odd
$x_0 \leftarrow a^u \bmod n$ [can be done efficiently]
for $i \leftarrow 1$ **to** t
  do $x_i \leftarrow x_{i-1}^2 \bmod n$
    if $x_i = 1$ and $x_{i-1} \neq 1$ and $x_{i-1} \neq n-1$ → Provably not prime (can detects Charmichael)
      then return TRUE
  if $x_t \neq 1$
    then return TRUE → detects base-a pseudoprime failure
return FALSE → n is not provably composite & may be prime

MILLER-RABIN (n, s)
  for $j \leftarrow 1$ **to** s
    do $a \leftarrow$ RANDOM $(1, n-1)$
      if WITNESS (a, n)
        then **return** COMPOSITE → guaranteed
  return PRIME → highly probable

<u>Running Time</u>: Let n be represented as β bits

M-R uses $O(s\beta)$ arithmetic operations

$O(s\beta^3)$ bit operations

$\rightarrow$ much less than trial division

<u>Theorem</u>: If n is an odd composite number, then the # of witnesses to the compositeness of n is at least $(n-1)/2$

<u>Theorem</u>: For any odd integer $n > 2$ and positive integer s, the probability that M-R(n,s) errs is at most 2^{-s}. <u>proof</u>

Effectively some large $s \sim 50$ should suffice.

In fact, when applied to <u>randomly chosen</u> large integers, a much smaller value $(s \sim 3)$ should suffice.