CS530
Public Key Cryptography

Bill Cheng

http://merlot.usc.edu/cs530-s10

Public Key Cryptography

- aka asymmetric cryptography
- Based on some NP-complete problem
  - traveling salesman problem
    - n cities, connected
    - find shortest tour, all cities must be visited
    - solution complexity is $n!$
  - unique factorization
    - factor an integer into product of prime numbers (unique solution)
  - discrete logarithms
    - for any integers b, n, y Find x such that $b^x \bmod n = y$
    - modular arithmetic produces folding

A Short Note on Primes

- Why are public keys (and private keys) so large?
  - because key space is *sparse*
- What is the probability that some large number p is prime?
  - about 1 in $\ln(p)$
    - 2 digit numbers: 25 primes (1 in 4)
    - 10 digit numbers: 1 in 23 are primes
    - 100 digit numbers: 1 in 230 are primes
    - but... the more digits, the more primes
  - when $p = 2^{512}$ ($\approx 10^{150}$), equals about 1 in 355
    - about 1 in 355^2 numbers = 2^{1024} is product of two primes (and there's one valid RSA module)

RSA

- Rivest, Shamir, Adleman
- Generate two primes p, q
  - let $n = pq$
  - choose e, a small number, relatively prime to $(p-1)(q-1)$
  - choose $d (< n)$ such that $ed \equiv 1 \bmod (p-1)(q-1)$
- RSA public-key is $<e, n>$ (e is called the *public exponent*)
  RSA private-key is $<d, n>$ (d is called the *private exponent*)
  - n is called the *public modulus*
- Then, $c = m^e \bmod n$ and $m = c^d \bmod n$
  - can also encrypt with d and decrypt with e
    i.e., $c = m^d \bmod n$ and $m = c^e \bmod n$
- Note: encryption is fast (because e is small) and decryption is slow

An Example

- Let $p = 5$, $q = 11$, $e = 3$ (recall that p & q are primes)
  - then $n = 55$ (recall that $n = pq$)
  - pick $e = 3$ (recall that e is relatively prime to $(p-1)(q-1)$)
  - $d = 27$, since $(3)(27) \bmod 40 = 1$
    (recall that $ed \equiv 1 \bmod (p-1)(q-1)$)
- If $m = 7$, then $c = 7^3 \bmod 55 = 343 \bmod 55 = 13$
- Then m should be $= 13^{27} \bmod 55$
- Computing $13^{27} \bmod 55$
  - $13^1 \bmod 55 = 13$, $13^2 \bmod 55 = 4$, $13^4 \bmod 55 = 16$, $13^8 \bmod 55 = 36$, $13^{16} \bmod 55 = 31$
  - $27 = 16 + 8 + 3$
  - $13^{27} \bmod 55 = (13)(4)(36)(31) \bmod 55 =$
    $(1872 \bmod 55)(31) \bmod 55 = 52 \bmod 55 = 7$ (check)

Calculating the Private Exponent

- $ed \equiv 1 \bmod (p-1)(q-1)$
  - d is the *multiplicative inverse* of e modulo $(p-1)(q-1)$
  - multiplicative inverse of e is like the *reciprocal* of e since $e \cdot (1/e) = 1$
  - let a be an integer such that $a < n$ has a multiplicative inverse modulo n only if $gcd(a, n) = 1$
    - a has a multiplicative inverse modulo n if and only if $gcd(a, n) = 1$
- How to compute multiplicative inverses?
  - use the *Extended Euclidean Algorithm*

Euclidean Algorithm

- Input: two non-negative integers a and b with $a \geq b$
  Output: $gcd(a,b)$
  1) while $b > 0$ do
    1.1) $r \leftarrow a \bmod b$, $a \leftarrow b$, $b \leftarrow r$
  2) return (a)
- Ex: $a = 423$, $b = 153$, $gcd(a,b) = 17$

q	r	a	b
		423	153
2	117	153	117
1	36	117	36
3	9	36	9
4	0	9	0

$423 = 2 \cdot 153 + 117$
$153 = 1 \cdot 117 + 36$
$117 = 3 \cdot 36 + 9$
$36 = 4 \cdot 9 + 0$

Extended Euclidean Algorithm (p.NC 2.4)

- Input: two non-negative integers a_0 and b_0 with $a_0 \geq b_0$
  Output: $d = gcd(a_0, b_0)$ and integers x, y satisfying $a_0 x + b_0 y = d$
  1) if $b_0 = 0$ then set $d \leftarrow a_0$, $x \leftarrow 1$, $y \leftarrow 0$, and return (d,x,y)
  2) set $a \leftarrow a_0$, $b \leftarrow b_0$, $x_2 \leftarrow 1$, $x_1 \leftarrow 0$, $y_2 \leftarrow 0$, $y_1 \leftarrow 1$
  3) while $b > 0$ do
    3.1) $q \leftarrow \lfloor a/b \rfloor$, $r \leftarrow a - qb$, $x \leftarrow x_2 - qx_1$, $y \leftarrow y_2 - qy_1$
    3.2) $a \leftarrow b$, $b \leftarrow r$, $x_2 \leftarrow x_1$, $x_1 \leftarrow x$, $y_2 \leftarrow y_1$, $y_1 \leftarrow y$
  4) set $d \leftarrow a$, $x \leftarrow x_2$, $y \leftarrow y_2$ and return (d,x,y)
  - and e' each iteration $a_0 x_2 + b_0 y_2 = a$
- Ex: $a_0 = 423$, $b_0 = 153$, $gcd(a_0, b_0) = 17$, and $423 \cdot 4 + 153 \cdot (-11) = 17$

q	r	x	y	a	b	x_0	x_1	y_0	y_1
				423	153	1	0	0	1
2	117	1	-2	153	117	0	1	1	-2
1	36	-1	3	117	36	1	-2	-2	5
3	9	4	-11	36	9	-2	5	5	-12
4	0	-17	47	9	0	5	-12	-12	29

- A simple way to implement the Extended Euclidean Algorithm
  - http://en.wikipedia.org/wiki/Extended_Euclidean_algorithm

The Table Method (Cont...)

Ex: $a_0 = 425$, $b_0 = 153$, $gcd(a_0, b_0) = 17$, and $425 \cdot 4 + 153 \cdot (-11) =$ [illegible]

q	r	x	y	a	b	x_2	x_1	y_2	y_1
-	-	-	-	425	153	1	0	0	1
2	119	1	-2	153	119	0	1	1	-2
1	34	[illegible]	[illegible]	119	34	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	17	[illegible]	-11	34	17	[illegible]	[illegible]	[illegible]	-11
2	0	[illegible]	[illegible]	17	0	4	[illegible]	-11	[illegible]

- Table Method

quo	rem	x	y
-	425	0	1
-	153	1	0
2	119	-2	1