CS 5173/4173 Computer Security

Topic 5.1 Basic Number Theory -- Foundation of Public Key Cryptography

GCD and Euclid’s Algorithm

Some Review: Divisors

- Set of all integers is $\mathcal{Z} = \{\ldots,-2,-1,0,1,2,\ldots\}$
- *b divides a* (or b is a *divisor* of a) if $a = mb$ for some m
  - denoted $b|a$
  - any $b \neq 0$ divides 0
- For any a, 1 and a are *trivial divisors* of a
  - all other divisors of a are called *factors* of a

Primes and Factors

- *a* is *prime* if it has no non-trivial factors
  - examples: 2, 3, 5, 7, 11, 13, 17, 19, 31,…
- Theorem: there are infinitely many primes
- Any integer $a > 1$ can be factored in a unique way as $p_1^{a_1} \bullet p_2^{a_2} \bullet \ldots p_t^{a_t}$
  - where all $p_1>p_2>\ldots>p_t$ are prime numbers and where each $a_i > 0$

Examples:

$91 = 13^1 \times 7^1$

$11{,}011 = 13^1 \times 11^2 \times 7^1$

Common Divisors

- A number d that is a divisor of both a and b is a *common divisor* of a and b

Example: common divisors of 30 and 24 are 1, 2, 3, 6

- If $d|a$ and $d|b$, then $d|(a+b)$ and $d|(a-b)$

Example: Since $3 | 30$ and $3 | 24$, $3 | (30+24)$ and $3 | (30-24)$

- If $d|a$ and $d|b$, then $d|(ax+by)$ for any integers x and y

Example: $3 | 30$ and $3 | 24$ → $3 | (2*30 + 6*24)$

Greatest Common Divisor (GCD)

- $gcd(a,b) = \max\{k \mid k|a \text{ and } k|b\}$

Example: gcd(60,24) = 12,   gcd(a,0) = a

- Observations
  - gcd(a,b) = gcd(|a|, |b|)
  - gcd(a,b) $\leq$ min(|a|, |b|)
  - if $0 \leq n$, then gcd(an, bn) = n*gcd(a,b)
- For all positive integers d, a, and b…
  …if $d \mid ab$
  …and gcd(a,d) = 1
  …then $d|b$

GCD (Cont'd)

- Computing GCD by hand:
  if $a = p_1^{a1}\, p_2^{a2} \ldots p_r^{ar}$ and
  $b = p_1^{b1}\, p_2^{b2} \ldots p_r^{br}$,
  …where $p_1 < p_2 < \ldots < p_r$ are prime,
  …and ai and bi are nonnegative,
  …then $\gcd(a, b) =$

$$p_1^{\min(a1,\, b1)}\, p_2^{\min(a2,\, b2)} \ldots p_r^{\min(ar,\, br)}$$

$\Rightarrow$ Slow way to find the GCD

- requires factoring *a* and *b* first (which, as we will see, can be slow)

Euclid's Algorithm for GCD

- Insight:
  $\gcd(x, y) = \gcd(y, x \bmod y)$
- Procedure **`euclid(x, y)`**:

```
r[0] = x, r[1] = y, n = 1;
while (r[n] != 0) {
    n = n+1;
    r[n] = r[n-2] % r[n-1];
}
return r[n-1];
```

Example

n	r_n
0	595
1	408
2	595 mod 408 = 187
3	408 mod 187 = 34
4	187 mod 34 = 17
5	34 mod 17 = 0

gcd(595,408) = 17

Running Time

- Running time is logarithmic in size of *x* and *y*

```
Enter x and y: 102334155 63245986
Step   1: r[i] = 39088169
Step   2: r[i] = 24157817
Step   3: r[i] = 14930352
Step   4: r[i] =  9227465
…
Step  35: r[i] =        3
Step  36: r[i] =        2
Step  37: r[i] =        1
Step  38: r[i] =        0
gcd of 102334155 and 63245986 is        1
```

Extended Euclid's Algorithm

- Let $\mathcal{LC}(x,y) = \{ux+vy : x,y \in \mathcal{Z}\}$ be the set of linear combinations of x and y
- Theorem: if x and y are any integers > 0, then gcd(x,y) is the smallest positive element of $\mathcal{LC}(x,y)$
- Euclid's algorithm can be extended to compute u and v, as well as gcd(x,y)
- Procedure exteuclid(x, y):

  (next page…)

Extended Euclid's Algorithm

floor function

```
r[0] = x, r[1] = y, n = 1;
u[0] = 1, u[1] = 0;
v[0] = 0, v[1] = 1;
while (r[n] != 0) {
   n = n+1;
   r[n] = r[n-2] % r[n-1];
   q[n] = (int) (r[n-2] / r[n-1]);
   u[n] = u[n-2] - q[n]*u[n-1];
   v[n] = v[n-2] - q[n]*v[n-1];
}
return r[n-1], u[n-1], v[n-1];
```

Extended Euclid's Example

n	q_n	r_n	u_n	v_n
0	-	595	1	0
1	-	408	0	1
2	1	187	1	-1
3	2	34	-2	3
4	5	17	11	-16
5	2	0	-24	35

gcd(595,408) = 17 = 11*595 + -16*408

Relatively Prime

- Integers a and b are *relatively prime* iff $\gcd(a,b) = 1$
  - example: 8 and 15 are relatively prime
- Integers $n_1, n_2, \ldots n_k$ are pairwise relatively prime if $\gcd(n_i, n_j) = 1$ for all $i \neq j$

Review of Modular Arithmetic

Remainders and Congruency

- For any integer *a* and any positive integer *n*, there are two unique integers *q* and *r*, such that $0 \leq r < n$ and $a = qn + r$
  - r is the *remainder* of *a* divided by *n*, written $r = a \bmod n$

Example: $12 = 2*5 + 2 \rightarrow 2 = 12 \bmod 5$

- *a* and *b* are *congruent* modulo *n*, written $a \equiv b \bmod n$, if $a \bmod n = b \bmod n$

Example: $7 \bmod 5 = 12 \bmod 5 \rightarrow 7 \equiv 12 \bmod 5$

Remainders (Cont'd)

- For any positive integer n, the integers can be divided into n equivalence classes according to their remainders modulo n
  - denote the set as $\mathcal{Z}_{\mathrm{n}}$
- i.e., the (mod n) operator maps all integers into the set of integers $\mathcal{Z}_n=\{0, 1, 2, \ldots, (n-1)\}$

Modular Arithmetic

- Modular addition
  - $[(a \bmod n) + (b \bmod n)] \bmod n = (a+b) \bmod n$

Example: [16 mod 12 + 8 mod 12] mod 12 = (16 + 8) mod 12 = 0

- Modular subtraction
  - $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$

Example: [22 mod 12 - 8 mod 12] mod 12 = (22 - 8) mod 12 = 2

- Modular multiplication
  - $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$

Example: [22 mod 12 × 8 mod 12] mod 12 = (22 × 8) mod 12 = 8

Properties of Modular Arithmetic

- Commutative laws
  - $(w + x) \bmod n = (x + w) \bmod n$
  - $(w \times x) \bmod n = (x \times w) \bmod n$
- Associative laws
  - $[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$
  - $[(w \times x) \times y] \bmod \mathrm{n} = [w \times (x \times y)] \bmod n$
- Distributive law
  - $[w \times (x + y)] \bmod n = [(w \times x)+(w \times y)] \bmod n$

Properties (Cont'd)

- Idempotent elements
  - $(0 + m) \bmod n = m \bmod n$
  - $(1 \times m) \bmod n = m \bmod n$
- Additive inverse $(-w)$
  - for each $m \in Z_n$, there exists z such that $(m + z) \bmod n = 0$

Example: 3 are 4 are additive inverses mod 7, since (3 + 4) mod 7 = 0

- Multiplicative inverse
  - for each positive $m \in Z_n$, is there a z s.t. $(m * z) \bmod n = 1$

Multiplicative Inverses

- Don't always exist!
  - Ex.: there is no z such that $6 \times z = 1 \bmod 8$ (m =6 and n=8)

z	0	1	2	3	4	5	6	7
6×z	0	6	12	18	24	30	36	42
6×z mod 8	0	6	4	2	0	6	4	2

…

- An positive integer $m \in Z_n$ has a multiplicative inverse m^{-1} **mod** n **iff** gcd(m, n) = 1, i.e., m and n are **relatively prime**

  $\Rightarrow$ If n is a prime number, then all positive elements in Z_n have multiplicative inverses

Inverses (Cont'd)

z	0	1	2	3	4	5	6	7
5×z	0	5	10	15	20	25	30	35
5×z mod 8	0	5	2	7	4	1	6	3

Finding the Multiplicative Inverse

- Given m and n, how do you find m^{-1} mod n?
- Extended Euclid's Algorithm
  `exteuclid(m,n)`:
  $m^{-1} \bmod n = \mathbf{v_{n-1}}$
  - if gcd(m,n) $\neq$ 1 there is no multiplicative inverse m^{-1} mod n

Example

x	q_x	r_x	u_x	v_x
0	-	35	1	0
1	-	12	0	1
2	2	11	1	-2
3	1	1	-1	$\boxed{3}$
4	11	0	12	-35

gcd(35,12) = 1 = -1*35 + 3*12

$12^{-1} \bmod 35 =$ **3** (i.e., 12*3 mod 35 = 1)

Modular Division

- If the inverse of b mod n exists, then
  $(a \bmod n) / (b \bmod n) = (a * (b^{-1} \bmod n)) \bmod n$

Example: $(13 \bmod 11) / (4 \bmod 11) = (13*(4^{-1} \bmod 11)) \bmod 11 = (13 * 3) \bmod 11 = 6$

Example: $(8 \bmod 10) / (4 \bmod 10)$ not defined since
4 does not have a multiplicative inverse mod 10

Modular Exponentiation (Power)

Modular Powers

Example: show the powers of 3 mod 7

i	0	1	2	3	4	5	6	7	8
3^i	1	3	9	27	81	243	729	2187	6561
$3^i \bmod 7$	1	3	2	6	4	5	1	3	2

And the powers of 2 mod 7

i	0	1	2	3	4	5	6	7	8	9
2^i	1	2	4	8	16	32	64	128	256	512
$2^i \bmod 7$	1	2	4	1	2	4	1	2	4	1

Fermat's "Little" Theorem

- If p is prime
  …and a is a positive integer not divisible by p,
  …then $a^{p-1} \equiv 1 \pmod{p}$

Example: 11 is prime, 3 not divisible by 11,
so $3^{11-1} = 59049 \equiv 1 \pmod{11}$

Example: 37 is prime, 51 not divisible by 37,
so $51^{37-1} \equiv 1 \pmod{37}$

The Totient Function

- $\phi(n) = |Z_n^*|$ = the number of integers less than n and relatively prime to n

  a) if n is prime, then $\phi(n) = n-1$

Example: $\phi(7) = 6$

  b) if $n = p^{\alpha}$, where p is prime and $\alpha > 0$, then $\phi(n) = (p-1)*p^{\alpha-1}$

Example: $\phi(25) = \phi(5^2) = 4*5^1 = 20$

  c) if $n=p*q$, and p, q are relatively prime, then $\phi(n) = \phi(p)*\phi(q)$

Example: $\phi(15) = \phi(5*3) = \phi(5) * \phi(3) = 4 * 2 = 8$

Exercise

- $\phi(21)$ = ?
- $\phi(33)$ = ?
- $\phi(12)$ =?

- $\phi(n) = |\mathcal{Z}_n^*|$ = the number of integers less than n and relatively prime to n
  a) if n is prime, then $\phi(n) = n-1$

Example: $\phi(7) = 6$

  b) if $n = p^\alpha$, where p is prime and $\alpha > 0$, then
  $\phi(n) = (p-1)*p^{\alpha-1}$

Example: $\phi(25) = \phi(5^2) = 4*5^1 = 20$

  c) if $n=p*q$, and p, q are relatively prime, then
  $\phi(n) = \phi(p)*\phi(q)$

Example: $\phi(15) = \phi(5*3) = \phi(5) * \phi(3) = 4 * 2 = 8$

Euler’s Theorem

- For every *a* and *n* that are relatively prime,
  $a^{\phi(n)} \equiv 1 \bmod n$

Example: For a = 3, n = 10, which relatively prime:

$\phi(10) = \phi(2*5) = \phi(2) * \phi(5) = 1*4 = 4$

$3^{\phi(10)} = 3^4 = 81 \equiv 1 \bmod 10$

Example: For a = 2, n = 11, which are relatively prime:

$\phi(11) = 11-1 = 10$

$2^{\phi(11)} = 2^{10} = 1024 \equiv 1 \bmod 11$

More Euler…

- Variant:
  for all n, $a^{k\phi(n)+1} \equiv a \bmod n$ for all a in $\mathcal{Z}_n^*$, and all non-negative k

Example: for n = 20, a = 7, $\phi(n) = 8$, and k = 3:

$$7^{3*8+1} \equiv 7 \bmod 20$$

- Generalized Euler's Theorem:
  for $n = pq$ (p and q distinct primes),
  $a^{k\phi(n)+1} \equiv a \bmod n$ for all a in $\mathcal{Z}_n$, and all non-negative k

Example: for n = 15, a = 6, $\phi(n) = 8$, and k = 3:

$$6^{3*8+1} \equiv 6 \bmod 15$$

Modular Exponentiation

- $x^y \bmod n = x^{y \bmod \phi(n)} \bmod n$

Example: $x = 5$, $y = 7$, $n = 6$, $\phi(6) = 2$

$$5^7 \bmod 6 = 5^{7 \bmod 2} \bmod 6 = 5 \bmod 6$$

- by this, if $y \equiv 1 \bmod \phi(n)$, then $x^y \bmod n = x \bmod n$

Example:

$x = 2$, $y = 101$, $n = 33$, $\phi(33) = 20$, $101 \bmod 20 = 1$

$$2^{101} \bmod 33 = 2 \bmod 33$$

The Powers of An Integer, Modulo *n*

- Consider the expression $a^m \equiv 1 \bmod n$
- If *a* and *n* are relatively prime, then there is at least one integer *m* that satisfies the above equation
- Ex: for *a* = 3 and *n* = 7, what is *m*?

i	1	2	3	4	5	6	7	8	9
3^i *mod 7*	3	2	6	4	5	1	3	2	6

The Power (Cont'd)

- The smallest positive exponent *m* for which the above equation holds is referred to as…
  - the *order of a (mod n),* or
  - the *length of the period generated by a*

Understanding Order of *a* (mod *n*)

- Powers of some integers *a* modulo 19

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}	a^{17}	a^{18}	order
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	**1**
2	**4**	**8**	**16**	**13**	**7**	**14**	**9**	**18**	**17**	**15**	**11**	**3**	**6**	**12**	**5**	**10**	**1**	**18**
4	**16**	**7**	**9**	**17**	**11**	**6**	**5**	**1**	4	16	7	9	17	11	6	5	1	**9**
7	**11**	**1**	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	**3**
8	**7**	**18**	**11**	**12**	**1**	8	7	18	11	12	1	8	7	18	11	12	1	**6**
9	**5**	**7**	**6**	**16**	**11**	**4**	**17**	**1**	9	5	7	6	16	11	4	17	1	**9**
18	**1**	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	**2**

Observations on The Previous Table

- The length of each period divides 18= $\phi(19)$
  - i.e., the lengths are 1, 2, 3, 6, 9, 18
- Some of the sequences are of length 18
  - e.g., the base *2* generates (via powers) all members of Z_n^*
  - The base is called the primitive root
  - The base is also called the generator when n is prime

Reminder of Results

Totient function:

if n is prime, then $\phi(n) = n\text{-}1$

if $n = p^{\alpha}$, where p is prime and $\alpha > 0$, then $\phi(n) = (p\text{-}1)*p^{\alpha\text{-}1}$

if $n=p*q$, and p, q are relatively prime, then $\phi(n) = \phi(p)*\phi(q)$

Example: $\phi(7) = 6$

Example: $\phi(25) = \phi(5^2) = 4*5^1 = 20$

Example: $\phi(15) = \phi(5*3) = \phi(5) * \phi(3) = 4 * 2 = 8$

Reminder (Cont'd)

- Fermat: If *p* is prime and *a* is positive integer not divisible by *p*, then $a^{p-1} \equiv 1 \pmod{p}$

> Example: 11 is prime, 3 not divisible by 11, so $3^{11-1} = 59049 \equiv 1 \pmod{11}$

Euler: For every *a* and *n* that are relatively prime, then $a^{\phi(n)} \equiv 1 \bmod n$

> Example: For a = 3, n = 10, which relatively prime: $\phi(10) = 4$, $3^{\phi(10)} = 3^4 = 81 \equiv 1 \bmod 10$

Variant: for all a in Z_n^*, and all non-negative *k*, $a^{k\phi(n)+1} \equiv a \bmod n$

> Example: for n = 20, a = 7, $\phi(n) = 8$, and k = 3: $7^{3*8+1} \equiv 7 \bmod 20$

Generalized Euler's Theorem: for $n = pq$ (*p* and *q* are distinct primes), all *a* in Z_n, and all non-negative *k*, $a^{k\phi(n)+1} \equiv a \bmod n$

> Example: for n = 15, a = 6, $\phi(n) = 8$, and k = 3: $6^{3*8+1} \equiv 6 \bmod 15$

$x^y \bmod n = x^{y \bmod \phi(n)} \bmod n$

> Example: x = 5, y = 7, n = 6, $\phi(6) = 2$, $5^7 \bmod 6 = 5^{7 \bmod 2} \bmod 6 = 5 \bmod 6$

Computing (Cont'd)

Algorithm **`modexp(a,b,n)`**

```
d = 1;
for i = k downto 1 do
      d = (d * d) % n;              /* square */
      if (b_i == 1)
            d = (d * a) % n;        /* step 2 */
      endif
enddo
return d;
```

at each iteration, not just at end

Requires time $\propto k$ = logarithmic in b

Example

- Compute $a^b \pmod{n} = 7^{560} \bmod 561$
  - $560_{10} = 1000110000_2$

i		10	9	8	7	6	5	4	3	2	1
b_i		1	0	0	0	1	1	0	0	0	0
d	1	7	49	157	526	160	241	298	166	67	1

step 2

Q: Can some other result be used to compute this particular example more easily? (Note: 561 = 3*11*17.)

Discrete Logarithms

Square Roots

- x is a *non-trivial square root of 1 mod n* if it satisfies the equation $x^2 \equiv 1 \bmod n$, but x is neither 1 nor -1 mod n

Ex: 6 is a square root of 1 mod 35 since $6^2 \equiv 1 \bmod 35$

- Theorem: if there exists a non-trivial square root of 1 mod n, then n is not a prime
  - i.e., prime numbers will not have non-trivial square roots

Roots (Cont'd)

- If $n = 2^{\alpha_0} p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, where $p_1 \ldots p_k$ are distinct primes > 2, then the number of square roots (including trivial square roots) are:
  - 2^k if $\alpha_0 \leq 1$

Example: for $n = 70 = 2^1 * 5^1 * 7^1$, $\alpha_0 = 1$, $k = 2$, and the number of square roots $= 2^2 = 4$ (1,29,41,69)

  - 2^{k+1} if $\alpha_0 = 2$

Example: for $n = 60 = 2^2 * 3^1 * 5^1$, $k = 2$, the number of square roots $= 2^3 = 8$ (1,11,19,29,31,41,49,59)

  - 2^{k+2} if $\alpha_0 > 2$

Example: for $n = 24 = 2^3 * 3^1$, $k = 1$, the number of square roots $= 2^3 = 8$ (1,5,7,11,13,17,19,23)

Primitive Roots

- Reminder: the highest possible order of $a \pmod{n}$ is $\phi(n)$
- If the order of $a \pmod{n}$ is $\phi(n)$, then a is referred to as a *primitive root of n*
  - for a prime number p, if a is a primitive root of p, then $a, a^2, \ldots, a^{p-1} \bmod p$ are all distinct numbers
- No simple general formula to compute primitive roots modulo n
  - trying out all candidates

Discrete Logarithms

- For a primitive root a of a number p, where $a^i \equiv b \bmod p$, for some $0 \leq i \leq p\text{-}1$
  - the exponent i is referred to as *the index of b* for the base a (mod p), denoted as $\text{ind}_{a,p}(b)$
  - i is also referred to as the *discrete logarithm of b to the base a, mod p*

Logarithms (Cont'd)

- Example: 2 is a primitive root of 19.
  The powers of 2 mod 19 =

b	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
$\text{ind}_{2,19}(b) =$ log(b) base 2 mod 19	0	1	13	2	16	14	6	3	8

10	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**
17	12	15	5	7	11	4	10	9

Given *a*, *i*, and *p*, computing $b = a^i \bmod p$ is straightforward

Computing Discrete Logarithms

- However, given *a*, *b*, and *p*, computing i = $\text{ind}_{a,p}(b)$ is difficult
  - Used as the basis of some public key cryptosystems