CSCI 454/554 Computer and Network Security

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

Outline

- GCD and Euclid's Algorithm
- Modulo Arithmetic
- Modular Exponentiation
- Discrete Logarithms

GCD and Euclid's Algorithm

Some Review: Divisors

- Set of all integers is Z = {…,-2, -1,0,1,2, …}
- *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*

4

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:
$91 = 13^1 \times 7^1$
$11011 = 13^1 \times 11^2 \times 7^1$

5

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)

6

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) ≤ min(|a|, |b|)
  - if 0 ≤ 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 $d|b$

7

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 a_i and b_i are nonnegative,
  …then gcd(a, b) =
  $p_1^{\min(a1, b1)} p_2^{\min(a2, b2)} \ldots p_r^{\min(ar, br)}$
- Slow way to find the GCD
  - requires factoring a and b first (which can be slow)

8

Euclid's Algorithm for GCD

- Insight:
  gcd(x, y) = gcd(y, x mod 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];
```

9

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

10

Running Time

- Running time is logarithmic in size of *x* and *y*
- Worst case occurs when *???*

```
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  34: r[i] =        5
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
```

11

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…)

12

Extended Euclid's Algorithm

WILLIAM & MARY

```
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];
```

floor function

Exercise: Show r[n]=u[n]x+v[n]y

13

Extended Euclid's Example

WILLIAM & MARY

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

14

Extended Euclid's Example

WILLIAM & MARY

n	q_n	r_n	u_n	v_n
0	-	99	1	0
1	-	78	0	1
2				
3				
4				
5				
6				

gcd(99,78) = 3 = -11*99 + 14*78

15

Extended Euclid's Example

WILLIAM & MARY

n	q_n	r_n	u_n	v_n
0	-	99	1	0
1	-	78	0	1
2	1	21	1	-1
3	3	15	-3	4
4	1	6	4	-5
5	2	3	-11	14
6	2	0	26	-33

gcd(99,78) = 3 = -11*99 + 14*78

16

Relatively Prime

WILLIAM & MARY

- 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 $i \neq j$

17

WILLIAM & MARY

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 $0 \le r < n$ and $a = qn + r$
  - *r* is the *remainder* of division by *n*, written $r = a \bmod n$

Example: 12 = 2*5 + 2 ➔ 2 = 12 mod 5

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

Example: 7 mod 5 = 12 mod 5 ➔ 7 ≡ 12 mod 5

19

Negative Numbers

- In modular arithmetic,
  …a negative number *a* is usually replaced by the congruent number *b* mod *n*,
  …where *b* is the smallest non-negative number
  …such that $b = a + m*n$

Example: -3 ≡ 4 mod 7

20

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 Z_n
- i.e., the (mod *n*) operator maps all integers into the set of integers Z_n={0, 1, 2, …, (*n*-1)}

21

Modular Arithmetic

- Modular addition
  - [(*a* mod *n*) + (*b* mod *n*)] mod *n* = (*a*+*b*) mod *n*

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

- Modular subtraction
  - [(*a* mod *n*) – (*b* mod *n*)] mod *n* = (*a* – *b*) mod *n*

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

- Modular multiplication
  - [(*a* mod *n*) × (*b* mod *n*)] mod *n* = (*a* × *b*) mod *n*

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

22

An Exercise (n=5)

- Addition

+	1	2	5	7
2				
3				
5				
9				

- Multiplication

	2	3	4	5
1				
3				
5				
6				

23

An Exercise (n=5)

- Addition

+	1	2	5	7
2	3	4	2	4
3	4	0	3	0
5	1	2	0	2
9	0	1	4	1

- Multiplication

	2	3	4	5
1	2	3	4	0
3	1	4	2	0
5	0	0	0	0
6	2	3	4	0

24

Properties of Modular Arithmetic

WILLIAM & MARY

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

25

Properties (Cont'd)

WILLIAM & MARY

- 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 $(m + z) \bmod n = 0$
  - alternatively, $z = (n - m) \bmod n$

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. $m * z = 1 \bmod n$?

26

Multiplicative Inverses

WILLIAM & MARY

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

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 $m^{-1} \bmod n$ iff $\gcd(m, n) = 1$, i.e., m and n are relatively prime
  - If n is a prime number, then all positive elements in $\mathbf{Z}_n$ have multiplicative inverses

27

Inverses (Cont'd)

z	0	1	2	3	4	5	6	7
5×z								
5×z mod 8								

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} mod n = $\mathbf{v_{n-1}}$
  - if gcd(m,n) ≠ 1 there is no multiplicative inverse m^{-1} mod n

Example

WILLIAM & MARY

n	q_n	r_n	u_n	v_n
0	-	35	1	0
1	-	12	0	1
2	2	11	1	-2
3	1	1	-1	3
4	11	0	12	-35

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

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

31

Modular Division

WILLIAM & MARY

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

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

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

32

WILLIAM & MARY

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 mod 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 mod 7	1	2	4	1	2	4	1	2	4	1

34

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 $51^{37-1} \equiv 1 \pmod{37}$

Useful?

35

Multiplicative Group Z_n^*

- Let Z_n^* be the set of numbers between 1 and n-1 that are relatively prime to n
- Z_n^* is closed under multiplication mod n
- Ex.: $Z_8^* = \{1,3,5,7\}$

*	1	3	5	7
1				
3				
5				
7				

36

The Totient Function

WILLIAM & MARY

- $\phi(n)$ = $|Z_n^*|$ = 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: $\phi(15) = \phi(5*3) = \phi(5) * \phi(3) = 4 * 2 = 8$

37

Euler's Theorem

WILLIAM & MARY

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

Example: For a = 2, n = 11, which are relatively prime:
$\phi(11) = 10$
$2^{\phi(11)} = 2^{10} = 1024 \equiv 1 \bmod 11$

38

More Euler…

WILLIAM & MARY

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

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

39

Modular Exponentiation

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

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 $x^y \bmod n \equiv x \bmod n$

Example:
x = 2, y = 101, n = 33, $\phi(33) = 20$, 101 mod 20 = 1
$2^{101} \bmod 33 = 2 \bmod 33$

40

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
$3^i \bmod 7$	3	2	6	4	5	1	3	2	6

41

The Power (Cont'd)

- The least 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*

42

Understanding Order of a (mod n)

WILLIAM & MARY

- 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

43

Observations on The Previous Table

WILLIAM & MARY

- 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

44

Reminder of Results

WILLIAM & MARY

Totient function:

if n is prime, then $\phi(n) = n$-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: $\phi(15) = \phi(5*3) = \phi(5) * \phi(3) = 4 * 2 = 8$

45

Reminder (Cont'd)

WILLIAM & MARY

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

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

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

46

Computing Modular Powers Efficiently

WILLIAM & MARY

- The repeated squaring algorithm for computing $a^b \pmod{n}$
- Let b_i represent the i^{th} bit of b (total of k bits)

47

Computing (Cont'd)

WILLIAM & MARY

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

48

Example

WILLIAM & MARY

- Compute a^b (mod n) = 7^{560} mod 561 = 1 mod 561

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.)

49

WILLIAM & MARY

Discrete Logarithms

Square Roots

WILLIAM & MARY

- 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 $6^2 \equiv 1$ mod 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

51

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 $\alpha_0 \le 1$

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)

52

Primitive Roots

- Reminder: the highest possible order of *a* (mod *n*) is $\phi(n)$
- If the order of *a* (mod *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 $a, a^2, \ldots, a^{p-1}$ are all distinct numbers mod *p*
- No simple general formula to compute primitive roots modulo n
  - there are methods to locate a primitive root faster than trying out all candidates

53

Primitive Roots (Cont'd)

- Theorem: the only integers with primitive roots are of the form 2, 4, p^α, and $2p^\alpha$, where
  - *p* is any prime > 2
  - α is a positive integer

Example: for n = 4, $\phi(n)$ = 2, primitive roots = {3}

Example: for n = 3^2 = 9, $\phi(n)$ = 6, primitive roots = {2,5}

Example: for n = 19, $\phi(n)$ = 18, primitive roots = {2,3,10,13,14,15}

54

Discrete Logarithms

- For a primitive root a of a number p, where
  $a^i \equiv b \bmod p$, for some $0 \le i \le p-1$
  - 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*

55

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

56

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

57

Computing (Cont'd)

WILLIAM & MARY

- Some properties of discrete logarithms
  - $\text{ind}_{a,p}(1) = 0$ because $a^0 \bmod p = 1$ *warning: $\phi(p)$, not p!*
  - $\text{ind}_{a,p}(a) = 1$ because $a^1 \bmod p = a$
  - $\text{ind}_{a,p}(yz) = (\text{ind}_{a,p}(y) + \text{ind}_{a,p}(z)) \bmod \phi(p)$

Example: $\text{ind}_{2,19}(5*3) = (\text{ind}_{2,19}(5) + \text{ind}_{2,19}(3)) = 11 \bmod \mathbf{18}$

  - $\text{ind}_{a,p}(y^r) = (r\ \text{ind}_{a,p}(y)) \bmod \phi(p)$

Example: $\text{ind}_{2,19}(3^3) = (3*\text{ind}_{2,19}(3)) = 3 \bmod \mathbf{18}$

58

More on Discrete Logarithms

WILLIAM & MARY

- Consider:
  $x \equiv a^{\text{ind}_{a,p}(x)} \bmod p$,
  $y \equiv a^{\text{ind}_{a,p}(y)} \bmod p$, and
  $xy \equiv a^{\text{ind}_{a,p}(xy)} \bmod p$

Ex: $3 = 2^{13} \bmod 19$

Ex: $5 = 2^{16} \bmod 19$

Ex: $3*5 = 2^{11} \bmod 19$

1) $a^{\text{ind}_{a,p}(xy)} \bmod p \equiv (a^{\text{ind}_{a,p}(x)} \bmod p)(a^{\text{ind}_{a,p}(y)} \bmod p)$

Ex: $15 = 3 * 5$

2) $a^{\text{ind}_{a,p}(xy)} \bmod p \equiv (a^{\text{ind}_{a,p}(x)+\text{ind}_{a,p}(y)}) \bmod p$

Ex: $15 = 2^{13+16} \bmod 19$

3) by Euler's theorem: $a^z \equiv a^q \bmod p$ *iff* $z \equiv q \bmod \phi(p)$

Ex: $15 = 2^{11} \bmod 19 = 2^{29} \bmod 19 \Leftrightarrow 11 \equiv 29 \bmod 18$

59

Summary

WILLIAM & MARY

1. Number theory is the basis of public key cryptography
2. Euclid's algorithm is used to find GCD and multiplicative inverse
3. Computing a ^{b} (mod n) is accomplished by repeated squaring
4. Only primes have discrete logarithms, and they are expensive to compute

60