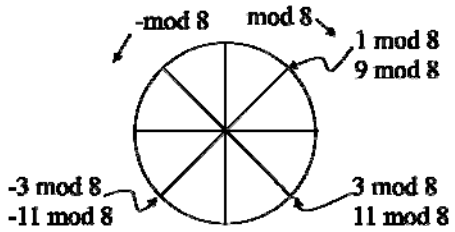
Number Theory

- ✓ The branch of mathematics that is important in IT security especially in cryptography.
- ✓ Deals only in integer numbers and the process can be done in a very fast manner.

Modular Arithmetic



- Primarily interested only in modular arithmetic rather than the congruence in general.
- Modular arithmetic is often introduced as 'clock arithmetic'.

- ✓ Example:
  - o 14 hrs after 3 pm is 5 am the next morning that is
  - o $14 + 3 \equiv 5 \pmod{12}$ or $14 + 3 = 1 * 12 + 5$
- ✓ $a \equiv b \pmod{n}$ if and only if $a \bmod n = b \bmod n$
- ✓ The notation $a \equiv b \pmod{n}$ is said as 'a is congruent to b modulo n'. It holds for integer a, b and $n \neq 0$.
- ✓ b is called a residue of 'a modulo n'.
- ✓ Has features that are appropriate for cryptography e.g. it can be used to compute inverse in fast mode.
- ✓ The intermediates results are restricted to a finite range, usually within (0, n-1), so it has less likelihood of overflow during computation.
- ✓ Some problems involving inverses are very, very hard to solve, yet when one of the inverses is known, to solve the other is simple.
- ✓ "Inverses" are important because they are good candidate for E/D keys.

Laws of Associativity, Commutativity, and Distributivity

- ✓ Associativity: $(a+b)+c = a+(b+c) \bmod n$
- ✓ Commutativity: $a+b = b+a \bmod n$
- ✓ Distributivity: $(a+b).c = (a.c)+(b.c) \bmod n$

$$a+/-b \bmod n = [a \bmod n +/- b \bmod n] \bmod n$$

Residues of Modulo *n*

- ✓ A set of n integers $\{r_1, \ldots..r_n\}$ is called complete set of residues of modulo n.
- ✓ For any modulus n, the set of integers {0,1, ….., n-1} forms a complete set of residues of modulo n.
- ✓ Note: $-12 \pmod 7 \equiv -5 \pmod 7 \equiv 2 \pmod 7 \equiv 9 \pmod 7$
- ✓ Example:
  - Find $(87 + 114) \bmod 11$
    $(87 + 114) \bmod 11 = (10 + 4) \bmod 11 = 14 \bmod 11 = 3 \bmod 11.$
    (And in fact, $87 + 114 = 201 = 11 \cdot 18 + 3$)
  - Find $14(34 \bmod 16)$
    $14(34 \bmod 16) = 14(2 \bmod 16) = 28 \bmod 16 = 12 \bmod 16.$
    (And, in fact, $14 \cdot 34 = 476 = 29 \cdot 16 + 12.$)
  - Find $(1234 - 456) \bmod 7$
    $(1234 - 456) \bmod 7 = 1234 \bmod 7 - 456 \bmod 7 = (2 - 1) \bmod 7 = 1 \bmod 7.$
    (And in fact, $1234 - 456 = 778 = 1 \bmod 7$.
  - Find $3^5 \bmod 7$

1.	Square 3	3* 3 = 9	3 * 3 mod 7 = 2 mod 7
2.	Square the result	9 * 9 = 81	2 * 2 mod 7 = 4 mod 7
3.	Multiply by 3	81 * 3 = 243	4 * 3 mod 7 = 5 mod 7
4.	Reduce mod 7	243 mod 7 = 5	

- Find $3^{12} \pmod 7$

$$3^{12} \pmod 7 \equiv (3^2 \pmod 7)^6$$
$$(3^2 \pmod 7)^6 \equiv (2 \pmod 7)^6$$
$$(2 \pmod 7)^6 \equiv 1 \pmod 7$$

- Find $3^{20} \bmod 5$

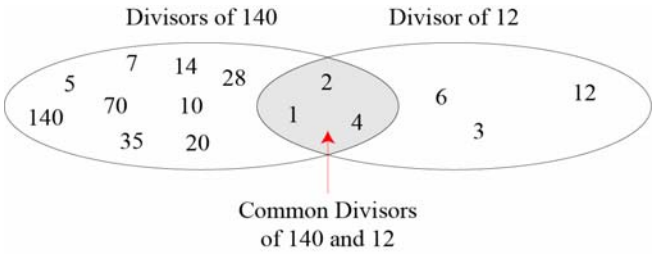
$3^2 \rightarrow 3 * 3 \pmod 5$
$(3^2)^2 = 3^4 \rightarrow 4 * 4 \pmod 5$
$(3^4)^2 = 3^8 \rightarrow 1 * 1 \pmod 5$
$(3^8)^2 = 3^{16} \rightarrow 1 * 1 \pmod 5$
$3^{16} * 3^4 = 3^{20} \rightarrow 1 * 1 \pmod 5$

- Find $12^{200} \bmod 5$

Start with $(12 * 12) \bmod 5 \rightarrow$
12^4
12^8
12^{16}
:
:
12^{200}

gcd : greatest common divisor

✓ Any positive integer has at least two divisors, 1 and itself (but it can have more).



✓ The largest integer that evenly divides the set of numbers.

✓ Given gcd (p, q) = r

- If r is a divisor for p and q.
- Any divisor for p and q is also a divisor for r.
- Divisor – number used to divide another. In the equation 15 ÷ 3 = 5, 3 is the divisor.

✓ Example:

If p = 8, q = 9

8 = 1 * 2 * 2 * 2

9 = 1 * 3 * 3

Then gcd (8,9) = 1

p = 48, q = 72

48 = 1 * 2 * 2 * 2 * 2 * 3

72 = 1 * 2 * 2 * 2 * 3 * 3

Then gcd(48,72) = 2 * 2 * 2 * 3 = 24

✓ Example:

gcd (4, 6) = 2

gcd (12, 25) = 1

gcd (12, 24) =12

gcd (3, 11) =

gcd (64, 63) =

✓ When gcd (*a, n*) = 1, it means that *a* and *n* do not share any other common factor except 1.

✓ Then we say that *a* is relatively prime to *n.*

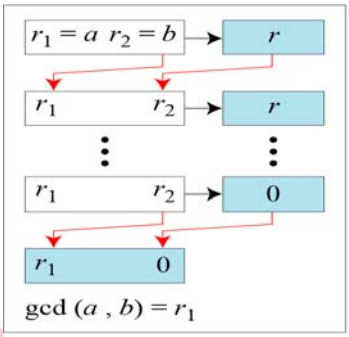
✓ Example:

p = 7, q =11

p = 9, q = 16

Euclid's Algorithm

- ✓ Used to find the Greatest Common Divisor (GCD) of two numbers a and n, $a < n$.
- ✓ Fact 1:
  gcd (a, 0) = a
  Fact 2:
  gcd (a, b) = gcd (b, r), where r is the remainder of dividing a by b
- ✓ Euclid's Algorithm



a. Process

```
r1 ← a;      r2 ← b;      (Initialization)
while (r2 > 0)
  {
   q ← r1 / r2;
   r  ← r1 − q × r2;
   r1 ← r2 ;  r2 ← r ;
  }
gcd (a, b) ← r1
```

b. Algorithm

- ✓ Find the gcd(2740, 1760)

  We have gcd (2740, 1760) = 20.

q	r_1	r_2	r
1	2740	1760	980
1	1760	980	780
1	980	780	200
3	780	200	180
1	200	180	20
9	180	20	0
	20	0	

Find gcd (56, 98)

q	***r1***	***r2***	***r***
1	98	56	42
1	56	42	14
3	42	14	0
	14	0	

Find gcd (36, 123)

q	***r1***	***r2***	***r***
	123	36	

Find gcd (81, 57)

Discrete Logarithm

- ✓ The inverse problem to exponentiation is that of finding the discrete logarithm of a number modulo *p*
  - find *x* where $a^x = b \bmod p$
- ✓ Exponentiation is relatively easy, finding discrete logarithm is generally a hard problem, with no easy way.
- ✓ If *p* is prime, then there exists *a* such that there is always a discrete logarithm for any b≠ 0

  Such *a* is called a primitive root and this is relatively hard to find.

Multiplicative Inverses

- ✓ Computation of multiplicative inverses i.e. given an integer *a* in the range [0, *n*-1], it may be possible to find a unique integer *x* in the range such that

  $a \bullet x \bmod n = 1$

  then *a* and *x* are said to be multiplicative inverses one another.

  Example:

  3 and 7 are multiplicative inverses mod 10
  because 21 mod 10 = 1.

- ✓ If *n* is very, very large , say 200 digits, then finding the inverses is very, very hard.
- ✓ Such features are the basis for highly secure cryptosystem such as RSA / public key encryption. (RSA is **R**ivest + **S**hamir + **A**dleman, the gang thet try to break DES using CRAY)
- ✓ How do we solve an equation of the form $a\,x \bmod n = b$?
  Example: $6\,x \bmod 10 = 4$. Find *x.*

Unique Inverse

- ✓ a^{-1} is inverse of a mod n if $a.a^{-1} = 1 \bmod n$
- ✓ Given $a \in [0, n-1]$, a has a unique inverse mod n when a and n are relatively prime i.e. a and x are guarantee unique iff

$$\gcd(a, n) = 1$$

- ✓ Example:

if $n = 5$ and $a = 3$

3*0 mod 5 = 0
3*1 mod 5 = 3
3*2 mod 5 = 1
3*3 mod 5 = 4
3*4 mod 5 = 2

Find the multiplicative inverse of 4 mod 7.

Therefore $a = 4$ and $n = 7$

4*0 mod 7 = 0
4*1 mod 7 = 4
4*2 mod 7 = 1
4*3 mod 7 = 5
4*4 mod 7 = 2
4*5 mod 7 = 6
4*6 mod 7 = 3

Find the multiplicative inverse of 2 mod 4.

2 *0 mod 4 = 0
2 *1 mod 4 = 2
2 *2 mod 4 = 0
2 *3 mod 4 = 2

Extended Euclid's (or Binary GCD) Algorithm

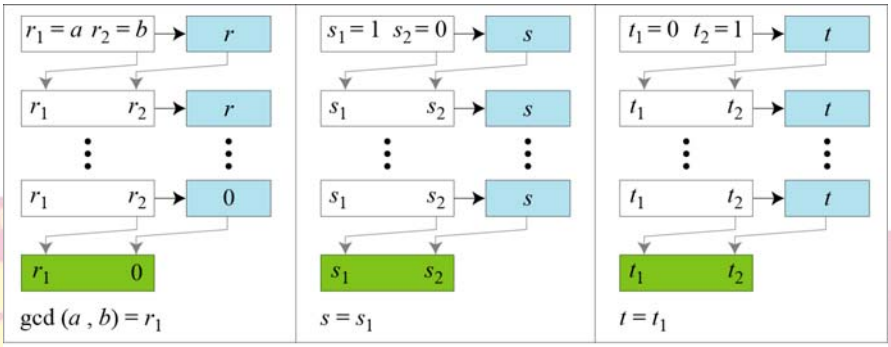
✓ To find Inverse of a number *a* mod *n* (where gcd (*a*, *n*)=1) that is $\frac{1}{a}$ mod 26 = ?

✓ Example: Find *d*, if 17 × *d* mod 19800 = 1

$d = \frac{1}{17} \bmod 19800$ → In other words, to find the inverse of (17, 19800).

The answer exist because gcd (17, 19800) = 1

✓ Extended Euclid's (or Binary GCD) Algorithm → *t* = multiplicative inverse



Example:

i. Given *a* = 161 and *b* = 28, find gcd (*a*, *b*) and the values of *s* and *t*.

q	r_1	r_2	*r*	s_1	s_2	*s*	t_1	t_2	*t*
5	161	28	21	1	0	1	0	1	−5
1	28	21	7	0	1	−1	1	−5	6
3	21	7	0	1	−1	4	−5	6	−23
	7	0		**−1**	4		**6**	−23	

$r_1 \leftarrow a;$ $r_2 \leftarrow b;$
$s_1 \leftarrow 1;$ $s_2 \leftarrow 0;$ (Initialization)
$t_1 \leftarrow 0;$ $t_2 \leftarrow 1;$

while $(r_2 > 0)$
{
$q \leftarrow r_1 / r_2;$

$r \leftarrow r_1 - q \times r_2;$
$r_1 \leftarrow r_2;$ $r_2 \leftarrow r;$ (Updating r's)

$s \leftarrow s_1 - q \times s_2;$
$s_1 \leftarrow s_2;$ $s_2 \leftarrow s;$ (Updating s's)

$t \leftarrow t_1 - q \times t_2;$
$t_1 \leftarrow t_2;$ $t_2 \leftarrow$ t; (Updating t's)

}
gcd $(a, b) \leftarrow r_1;$ $s \leftarrow s_1;$ $t \leftarrow t_1$

We get gcd (161, 28) = 7, s = −1 and t = 6.

Since gcd (161, 28) ≠ 1, there is no multiplicative inverse.

ii. Find the multiplicative inverse of 3 mod 460.

Q	*r1*	*r2*	*r*	*s1*	*s2*	*s*	*t1*	*t2*	*t*
153	460	3		1	0		0	1	
3	3	1					1	-1	
	1	0					15		

iii. Find multiplicative inverse of 15 mod 26

Reduced Residues and Euler Totient Function, $\phi(n)$

- ✓ Euler's phi-function, $\phi(n)$, which is sometimes called the Euler's totient function plays a very important role in cryptography.
- ✓ Reduced set of residues mod n is the subset of residues {0, ….., n-1} relatively prime to n.
  Example: Reduced set of residues mod 10 is {1, 3, 7, 9}
- ✓ If n is prime, the reduced set of residues is the set of n-1 elements {1, 2,…, n-1}
- ✓ Euler Totient function, $\phi(n)$ is the number of elements in the reduced set of residues modulo n.

1. $\phi(1) = 0$.
2. $\phi(p) = p - 1$ if p is a prime.
3. $\phi(m \times n) = \phi(m) \times \phi(n)$ if m and n are relatively prime.
4. $\phi(p^e) = p^e - p^{e-1}$ if p is a prime.

- ✓ We can combine the above four rules to find the value of $f(n)$. For example, if n can be factored as $n = p_1^{e1} \times p_2^{e2} \times \ldots \times p_k^{ek}$
  then we combine the third and the fourth rule to find

$$\phi(n) = (p_1^{e_1} - p_1^{e_1-1}) \times (p_2^{e_2} - p_2^{e_2-1}) \times \cdots \times (p_k^{e_k} - p_k^{e_k-1})$$

- ✓ Example

i. Find $\phi(15)$
$\phi(15) = \phi(3) \times \phi(5) = (3 - 1)(5 - 1) = 8$.
Check: Reduced set of residues mod 15 {1, 2, 4, 7, 8, 11, 13, 14}.

ii. Find $\phi(n)$ for $n = 24 = 2^3 3^1$
$\phi(24) = \phi(2^3 3^1) = 2^2(2 - 1)\, 3^0(3 - 1) = 8$

iii. Find the value of $\phi(13)$?

iv. What is the value of $\phi(10)$?

v. What is the value of $\phi(240)$?

vi. What is the number of elements in Z_{14}*?

Other Theorems

✓ Fermat's Theorem

Let *p* be prime. Then for every *a* such that gcd *(a, p)* = 1,

$$a^{p-1} \bmod p = 1 \bmod p.$$

or

$$a^p = a \bmod p$$

✓ Example:

i. Find the result of $6^{10} \bmod 11$.

We have $6^{10} \bmod 11 = 1$. This is the first version of Fermat's little theorem where $p = 11$.

ii. Find the result of $3^{12} \bmod 11$.

$3^{12} \bmod 11 = 3^{10} \times 3^2 \bmod 11 = 3^{10} \bmod 11 \times 3^2 \bmod 11 = 1 \times 9 = 9$

✓ Euler's Generalization

For every *a* and *n* such that gcd (*a*, *n*) = 1, then

$$a^{\phi(n)} \bmod n = 1.$$

Algorithm for solving $ax \bmod n = 1$, where gcd (*a*, *n*) = 1 is

$$x = a^{\phi(n)-1} \bmod n$$

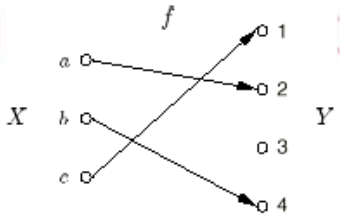
If *n* is prime, then $x = a^{(n-1)-1} \bmod n$ or $x = a^{(n-2)} \bmod n$

Background on Function

- ✓ A function is alternately referred to as a *mapping* or a *transformation*.
- ✓ A *set* consists of distinct objects which are called *elements* of the set. For example, a set might consist of the elements a, b, c and is denoted $X = \{a, b, c\}$.
- ✓ A *function* is defined by two sets X and Y and a *rule* f which assigns to each element in X precisely one element in Y.
- ✓ Set X is called the *domain* of the function and Y the *co-domain*.
- ✓ If x is an element of X (usually written $x \in X$) the *image* of x is the element in Y which the rule f associates with x.
- ✓ Image y of x is denoted by $y = f(x)$.
- ✓ Standard notation for a function f from set X to set Y is $f: X \rightarrow Y$.
- ✓ If $y \in Y$, then a *pre-image* of y is an element $x \in X$ for which $f(x) = y$.
  - o The set of all elements in Y which have at least one pre-image is called the *image* of f, denoted Im(f)

- ✓ Example:

  i. Consider the sets $X = \{a, b, c\}$, $Y = \{1, 2, 3, 4\}$, and the rule f from X to Y defined as $f(a) = 2$, $f(b) = 4$, $f(c) = 1$.
  The pre-image of the element 2 is a.
  The image of f is {1, 2, 4}.



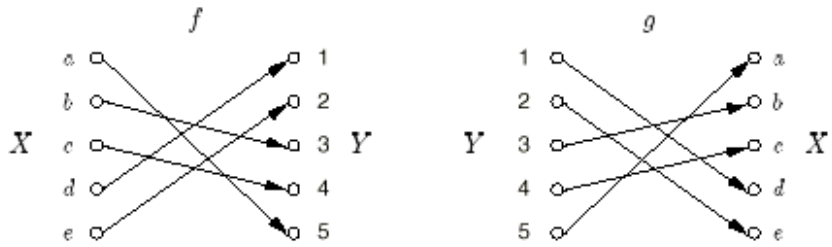
  ii. $f(x) = r_x$, where r_x is the remainder when x^2 is divided by 11. Explicitly then

$f(1) = 1$	$f(2) = 4$	$f(3) = 9$	$f(4) = 5$	$f(5) = 3$
$f(6) = 3$	$f(7) = 5$	$f(8) = 9$	$f(9) = 4$	$f(10) = 1$

1-1 Functions

- ✓ A function (or transformation) is 1 – 1 *(one-to-one)* if each element in the co-domain *Y* is the image of at most one element in the domain *X*.
- ✓ If a function $f: X \rightarrow Y$ is 1 – 1 and Im(*f*) = *Y*, then *f* is called *bijection*.
- ✓ If *f* is a bijection from *X* to *Y* then it is a simple matter to define a bijection *g* from *Y* to *X* as follows:
  For each $y \in Y$ define g(*y*) = *x* where $x \in X$ and *f*(*x*) = *y*. This function *g* obtained from *f* is called the inverse function of *f* and is denoted by $g = f^{-1}$.

Bijection *f* and Inverse $g = f^{-1}$



One-way Functions

- ✓ There are certain types of functions which play significant roles in cryptography.
  - o At the expense of rigor, an intuitive definition of a one-way function is given.
- ✓ A function *f* from a set *X* to a set *Y* is called a one-way function if *f*(*x*) is 'easy' to compute for all $x \in X$ but for 'essentially all' elements $y \in$ Im(*f*) it is 'computationally infeasible' to find any $x \in X$ such that *f* (*x*) = *y*.
- ✓ Example
  - i. Let *X* = {1, 2, 3, .., 16} and define *f* (x) = r_x for all $x \in X$ where r_x is the remainder when 3^x is divided by 17. Explicitly:

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$f(x)$	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

  - ii. Given a number between 1 and 16, it is relatively easy to find the image of it under *f*. However, given a number such as 7, without having the table in front of you, it is harder to find *x* given *f*(*x*) = 7.

Permutations

- ✓ Permutations are functions which are often used in various cryptographic constructs.
- ✓ Let *S* be a finite set of elements. A permutation *p* on *S* is a bijection from *S* to itself (i.e, $p: S \rightarrow S$).
- ✓ Example:
  Let $S = \{1, 2, 3, 4, 5\}$. A permutation $p: S \rightarrow S$ is defined as follows:
  $p(1) = 3$ $p(2) = 5$ $p(3) = 4$ $p(4) = 2$ $p(5) = 1$
- ✓ Since permutations are bijections, they have inverses.

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix}$$

$$p^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 3 & 2 \end{pmatrix}$$

- ✓ Its inverse is easily found by interchanging the rows in the array and reordering the elements in the new top row if desired (the bottom row would have to be reordered correspondingly).

Encryption Scheme

- ✓ Let $M = \{m_1, m_2, m_3\}$ and $C = \{c_1, c_2, c_3\}$. There are precisely 3! = 6 bijections from *M* to *C*. The key space $K = \{1, 2, 3, 4, 5, 6\}$ has six elements in it, each specifying one of the transformations.