Some 15-251
~~Great~~ Theoretical Ideas
~~in~~ Computer Science
for

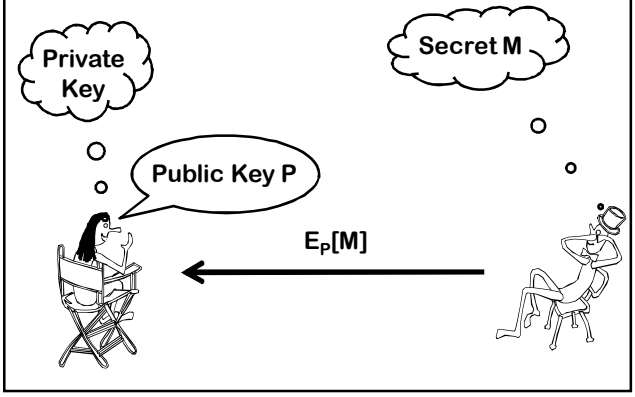
# Modular Arithmetic and the RSA Cryptosystem

Lecture 17 (March 18, 2008)


$\equiv_p 1$

# Public Key Cryptography


# Public Key Cryptography

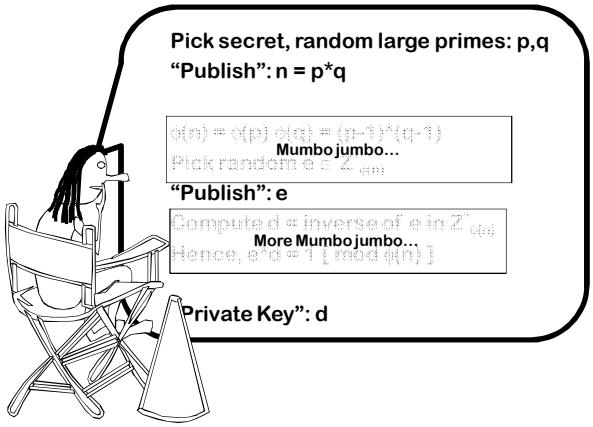


## The RSA Cryptosystem

**Rivest, Shamir, and Adelman (1978)**

**RSA is one of the most used cryptographic protocols on the net.**

**Your browser uses it to establish a secure session with a site.**




## But how does it all work?

What is $\varphi(n)$?
What is $Z_{\varphi(n)}^*$?
…
Why do all the steps work?

To understand this, we need a little number theory…

**MAX(a,b) + MIN(a,b) = a+b**

**n|m means that:**
**m is an integer multiple of n.**
**(We say that "n divides m".)**

Greatest Common Divisor:
GCD(x,y) = greatest $k \geq 1$ such that $k|x$ and $k|y$

Least Common Multiple:
LCM(x,y) = smallest $k \geq 1$ such that $x|k$ and $y|k$

Fact: $GCD(x,y) \times LCM(x,y) = x \times y$

You can use MAX(a,b) + MIN(a,b) = a+b to prove the above fact.

# Modulus

(a mod n) means:
the remainder when a is divided by n

If $a = dn + r$ with $0 \leq r < n$
Then r = (a mod n)
and d = (a div n)

# Modular Equivalence

$a \equiv b \text{ [mod n]} \Leftrightarrow$ (a mod n) = (b mod n)
$\Leftrightarrow$ n|(a-b)

Written as $a \equiv_n b$, and spoken
"a and b are equivalent modulo n"

Example: $31 \equiv 81 \text{ [mod 2]}$
$31 \equiv_2 81$

## $\equiv_n$ is an Equivalence Relation

In other words, it is:

Reflexive: $a \equiv_n a$

Symmetric: $(a \equiv_n b) \Rightarrow (b \equiv_n a)$

Transitive: $(a \equiv_n b \text{ and } b \equiv_n c) \Rightarrow (a \equiv_n c)$

$\equiv_n$ induces a partition of Z into n classes

a and b are said to be in the same "residue class" or "congruence class" when $a \equiv_n b$

$a \equiv_n b \Leftrightarrow n|(a-b)$

"a and b are equivalent modulo n"

Define Residue class [i] = the set of all integers that are congruent to i modulo n

Residue Classes Mod 3:

[0] = { …, -6, -3, 0, 3, 6, ..}
[1] = { …, -5, -2, 1, 4, 7, ..}
[2] = { …, -4, -1, 2, 5, 8, ..}
[-6] = { …, -6, -3, 0, 3, 6, ..}
[7] = { …, -5, -2, 1, 4, 7, ..}
[-1] = { …, -4, -1, 2, 5, 8, ..}

Fact: equivalence mod n implies equivalence mod any divisor of n.

If $(x \equiv_n y)$ and $(k|n)$ then: $x \equiv_k y$

Example: $10 \equiv_6 16 \Rightarrow 10 \equiv_3 16$

Proof: $x \equiv_n y \Leftrightarrow n|(x-y)$
$\Rightarrow k|(x-y)$
$\Rightarrow x \equiv_k y$

## Fundamental lemma of plus, minus, and times mod n:

If $(x \equiv_n y)$ and $(a \equiv_n b)$, then:
1. $x + a \equiv_n y + b$
2. $x - a \equiv_n y - b$
3. $x * a \equiv_n y * b$

When doing plus, minus, and times modulo n, you can at any time replace a number with a number in the same residue class modulo n

What is (249)(504) mod 251?

When working mod 251: (-2)(2) = -4 = 247

## A Unique Representation System Modulo n:

We pick exactly one representative from each residue class.

We do all our calculations using these representatives.

## Unique Representation System Modulo 3

Finite set S = {0, 1, 2}

+ and * defined on S:

| + | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | 2 |
| 1 | 1 | 2 | 0 |
| 2 | 2 | 0 | 1 |

| * | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 |
| 2 | 0 | 2 | 1 |

## Unique Representation System Modulo 3

Finite set S = {0, 1, -1}

+ and * defined on S:

| + | 0 | 1 | -1 |
|---|---|---|---|
| 0 | 0 | 1 | -1 |
| 1 | 1 | -1 | 0 |
| -1 | -1 | 0 | 1 |

| * | 0 | 1 | -1 |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | -1 |
| -1 | 0 | -1 | 1 |

## Perhaps The Most Convenient Set of Representatives

The reduced system modulo n:

$Z_n = \{0, 1, 2, \ldots, n-1\}$

Define operations $+_n$ and $*_n$:

$a +_n b = (a+b \bmod n)$
$a *_n b = (a*b \bmod n)$

## The Reduced System Modulo 2

$Z_2 = \{0, 1\}$

Two binary, associative operators on $Z_2$:

| $+_2$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

| $*_2$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 1 |

## The Reduced System Modulo 2

$Z_2 = \{0, 1\}$

Two binary, associative operators on $Z_2$:

| $+_2$ XOR | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

| $*_2$ AND | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 1 |

## The Reduced System $Z_4 = \{0,1,2,3\}$

| + | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

| * | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 |
| 2 | 0 | 2 | 0 | 2 |
| 3 | 0 | 3 | 2 | 1 |

## The Reduced System $Z_6 = \{0,1,2,3,4,5\}$

| + | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 |
| 1 | 1 | 2 | 3 | 4 | 5 | 0 |
| 2 | 2 | 3 | 4 | 5 | 0 | 1 |
| 3 | 3 | 4 | 5 | 0 | 1 | 2 |
| 4 | 4 | 5 | 0 | 1 | 2 | 3 |
| 5 | 5 | 0 | 1 | 2 | 3 | 4 |

An operator has the permutation property if each row and each column has a permutation of the elements.

For every n, $+_n$ on $Z_n$ has the permutation property

## What about multiplication? Does $*_6$ on $Z_6$ have the permutation property?

| * | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 |
| 2 | 0 | 2 | 4 | 0 | 2 | 4 |
| 3 | 0 | 3 | 0 | 3 | 0 | 3 |
| 4 | 0 | 4 | 2 | 0 | 4 | 2 |
| 5 | 0 | 5 | 4 | 3 | 2 | 1 |

NO!

## What about $*_8$ on $Z_8$?

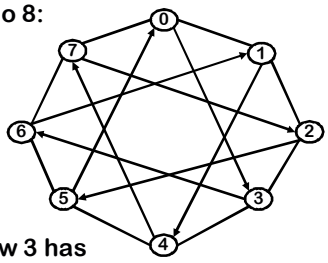
| * | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| 0 | | | | | | | | |
| 1 | | | | | | | | |
| 2 | | | | | | | | |
| 3 | 0 | 3 | 6 | 1 | 4 | 7 | 2 | 5 |
| 4 | 0 | 4 | 0 | 4 | 0 | 4 | 0 | 4 |
| 5 | | | | | | | | |
| 6 | | | | | | | | |
| 7 | | | | | | | | |

Which rows have the permutation property?

## A visual way to understand multiplication and the "permutation property".

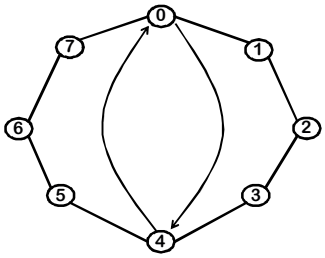
The multiples of c modulo n is the set:
$\{0, c, c +_n c, c +_n c +_n c, \ldots.\}$
$= \{kc \bmod n \mid 0 \leq k \leq n-1\}$

There are exactly 8 distinct multiples of 3 modulo 8:

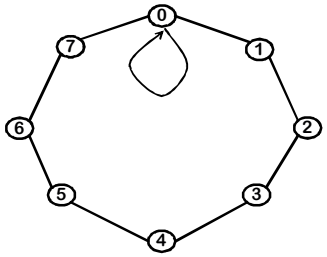



Hit all numbers $\Leftrightarrow$ row 3 has the "permutation property"

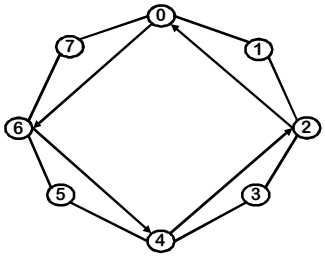
## There are exactly 2 distinct multiples of 4 modulo 8



## There is exactly 1 distinct multiple of 8 modulo 8




## There are exactly 4 distinct multiples of 6 modulo 8




There number of distinct multiples of c modulo n is:

$$LCM(n,c)/c = n/GCD(c,n)$$

Hence only those values of c with GCD(c,n) = 1 have the permutation property for $*_n$ on $Z_n$

**Theorem:** There are exactly
$k = n/GCD(c,n) = LCM(c,n)/c$
distinct multiples of c modulo n, and these are:
$\{ c*i \bmod n \mid 0 \le i < k \}$

**Proof:**

Clearly, $c/GCD(c,n) \ge 1$ is a whole number

$ck = cn/GCD(c,n) = n(c/GCD(c,n)) \equiv_n 0$

So there are at most k multiples of c mod n:
$c*0, c*1, c*2, \ldots, c*(k-1)$

Also, k = all the factors of n missing from c

$\Rightarrow cx \equiv_n cy \Leftrightarrow n|c(x-y) \Rightarrow k|(x-y) \Rightarrow x-y \ge k$

Hence, there are exactly k multiples of c.

**Fundamental lemma of plus, minus, and times mod n:**

If $(x \equiv_n y)$ and $(a \equiv_n b)$, then:

1. $x + a \equiv_n y + b$
2. $x - a \equiv_n y - b$
3. $x * a \equiv_n y * b$

**Is there a fundamental lemma of division modulo n?**

$$cx \equiv_n cy \Rightarrow x \equiv_n y \ ?$$

Of course not!
If $c=0 \pmod n$, $cx \equiv_n cy$ for all x and y.

Canceling the c is like dividing by zero.

**Let's Fix That!**

Repaired fundamental lemma of division modulo n?

$$\text{if } c \neq 0 \pmod n, \text{ then}$$
$$cx \equiv_n cy \Rightarrow x \equiv_n y \ ?$$

$6*3 \equiv_{10} 6*8$, but not $3 \equiv_{10} 8$

$2*2 \equiv_6 2*5$, but not $2 \equiv_6 5$

**This also doesn't work!**

**When Can't I Divide By c?**

Theorem: There are exactly n/GCD(c.n) distinct multiples of c modulo n

Corollary: If GCD(c,n) > 1, then the number of multiples of c is less than n

Corollary: If GCD(c,n) > 1 then you can't always divide by c.

Proof:

There must exist distinct x,y < n such that $c*x=c*y$ (but $x \neq y$). Hence can't divide.

**Fundamental lemma of division modulo n:**
**if GCD(c,n)=1, then $ca \equiv_n cb \Rightarrow a \equiv_n b$**

**Proof:** $ca \equiv_n cb \Rightarrow n|(cb-ca)$

$\Rightarrow n|c(b-a)$

$\Rightarrow n|(b-a)$ (because GCD(c,n)=1)

$\Rightarrow a \equiv_n b$

**Fundamental lemma of division modulo n:**
**if GCD(c,n)=1, then $ca \equiv_n cb \Rightarrow a \equiv_n b$**

**Consider the set:**

$$Z_n^* = \{x \in Z_n \mid GCD(x,n) = 1\}$$

**Multiplication over this set $Z_n^*$ will have the cancellation property**

$Z_6 = \{0, 1,2,3,4,5\}$

$Z_6^* = \{1,5\}$

| * | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 |
| 2 | 0 | 2 | 4 | 0 | 2 | 4 |
| 3 | 0 | 3 | 0 | 3 | 0 | 3 |
| 4 | 0 | 4 | 2 | 0 | 4 | 2 |
| 5 | 0 | 5 | 4 | 3 | 2 | 1 |

$Z_{12}^* = \{0 \le x < 12 \mid \gcd(x,12) = 1\}$

$= \{1,5,7,11\}$

| $*_{12}$ | 1 | 5 | 7 | 11 |
|---|---|---|---|---|
| 1 | 1 | 5 | 7 | 11 |
| 5 | 5 | 1 | 11 | 7 |
| 7 | 7 | 11 | 1 | 5 |
| 11 | 11 | 7 | 5 | 1 |

$Z_5^* = \{1,2,3,4\} = Z_5 \setminus \{0\}$

| $*_5$ | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 |
| 2 | 2 | 4 | 1 | 3 |
| 3 | 3 | 1 | 4 | 2 |
| 4 | 4 | 3 | 2 | 1 |

For all primes p, $Z_p^* = Z_p \setminus \{0\}$,
since all $0 < x < p$ satisfy $\gcd(x,p) = 1$

## Euler Phi Function $\phi(n)$

Define $\phi(n)$ = size of $Z_n^*$

(number of $1 \le k < n$ that
are relatively prime to n)

If p is prime, then $\phi(p) = p-1$

$Z_{12}^* = \{0 \le x < 12 \mid \gcd(x,12) = 1\}$
$= \{1,5,7,11\}$

| $*_{12}$ | 1 | 5 | 7 | 11 |
|---|---|---|---|---|
| 1 | 1 | 5 | 7 | 11 |
| 5 | 5 | 1 | 11 | 7 |
| 7 | 7 | 11 | 1 | 5 |
| 11 | 11 | 7 | 5 | 1 |

$\phi(12) = 4$

Theorem: if p,q distinct primes then:
$\phi(pq) = (p-1)(q-1)$

Proof:

# of integers from 1 to pq: pq

# of multiples of q up to pq: p

# of multiples of p up to pq: q

# of multiples of both p and q up to pq: 1

$\phi(pq) = pq - p - q + 1 = (p-1)(q-1)$

## Additive Inverse

The additive inverse of $a \in Z_n$ is the unique $b \in Z_n$ such that $a +_n b \equiv_n 0$.

We denote this inverse by "–a"

It is trivial to calculate:
"-a" = n-a

## Multiplicative Inverse

The multiplicative inverse of $a \in Z_n^*$ is the unique $b \in Z_n^*$ such that $a *_n b \equiv_n 1$

We denote this inverse by "$a^{-1}$" or "1/a"

The unique inverse of "a" must exist because the "a" row contains a permutation of the elements and hence contains a unique 1.

| * | 1 | b | 3 | 4 |
|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 |
| 2 | 2 | 4 | 1 | 3 |
| a | 3 | 1 | 4 | 2 |
| 4 | 4 | 3 | 2 | 1 |

## Efficient Algorithm To Compute $a^{-1}$ From a and n

Run Extended Euclidean Algorithm on the numbers a and n

It will give two integers r and s such that ra + sn = gcd(a,n) = 1

Taking both sides modulo n,
we obtain: $ra \equiv_n 1$

Output r, which is the inverse of a

## Fundamental Lemmas Until Now

If $(x \equiv_n y)$ and $(a \equiv_n b)$, then:
1. $x + a \equiv_n y + b$
2. $x - a \equiv_n y - b$
3. $x * a \equiv_n y * b$

For a,b,c in $Z_n^*$
then $ca \equiv_n cb \Rightarrow a \equiv_n b$

If $(a \equiv_n b)$ then $x^a \equiv_n x^b$ ? **NO!**

$(2 \equiv_3 5)$ , but it is not the case that: $2^2 \equiv_3 2^5$

**Euler's Theorem:**
$a \in Z_n^*$, $a^{\Phi(n)} \equiv_n 1$

**Fermat's Little Theorem:**
p prime, $a \in Z_p^* \Rightarrow a^{p-1} \equiv_p 1$

**Fundamental Lemma of Powers:**

If $a \equiv_{\Phi(n)} b$ Then $x^a \equiv_n x^b$

**Equivalently,**
$x^a \equiv_n x^{a \bmod \Phi(n)}$

What is $2^{4444444441} \bmod 5$?

$x^a \pmod n = x^{a \bmod \Phi(n)} \pmod n$

$44444444441 \equiv_{\Phi(5)} 1$

So $2^{4444444441} \bmod 5 = 2$

## Negative Powers

Suppose $x \in Z_n^*$, and a,n are naturals. $x^{-a}$ is defined to be the multiplicative inverse of $x^a$

$x^{-a} = (x^a)^{-1}$

## Rule of Integer Exponents

Suppose $x,y \in Z_n^*$, and a,b are integers:

$(xy)^{-1} \equiv_n x^{-1} y^{-1}$

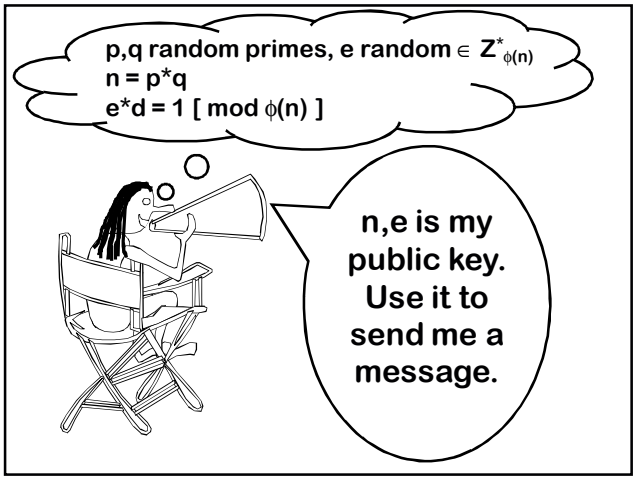
$X^a X^b \equiv_n X^{a+b}$

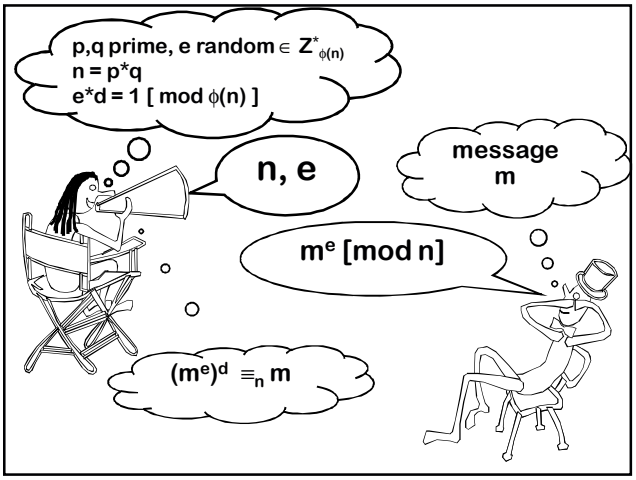
## The RSA Cryptosystem

Pick secret, random large primes: p,q
"Publish": n = p*q

$\phi(n) = \phi(p)\ \phi(q) = (p-1)*(q-1)$
Pick random $e \in Z^*_{\phi(n)}$
"Publish": e
Compute d = inverse of e in $Z^*_{\phi(n)}$
Hence, $e*d = 1 \ [\text{mod } \phi(n)]$

"Private Key": d




Here's What You Need to Know…

Working modulo integer n

Definitions of $Z_n$, $Z_n^*$
and their properties

Fundamental lemmas of +,-,*,/
When can you divide out
How to calculate $c^{-1}$ mod n.

Fundamental lemma of powers
Euler phi function $\phi(n) = |Z_n^*|$
Euler's theorem
Fermat's little theorem

RSA algorithm