Izmir Institute of Technology

CENG 115
Discrete Structures

Slides are based on the Text
***Discrete Mathematics & Its Applications* (6th Edition)**
by Kenneth H. Rosen

Slides were prepared by Dr. Michael P. Frank & Zeph Grunschlag

Module #11:
Applications of Number Theory

Rosen 6th ed., § 3.7

Contents

- Modular Inverse and Extended Euclidean Algorithm
- Chinese Remainder Theorem
- RSA Cryptography

Last lecture's review

- Modular arithmetic
- The *greatest common divisor* gcd(a,b)
- *Euclidean algorithm* to find gcd(a,b)
- Encryption example: $f(a) = (3a + 9)$ **mod** 26
  1. STOP THIEF
  2. 19,20,15,16 20,8, 9, 5, 6
  3. 14,17, 2, 5 17,7,10,24,1
  4. NQBE QGJXA

Modular Inverses

For the encryption function

$$f(a) = (3a + 9) \textbf{ mod } 26$$

We claimed that an inverse function is given by:

$$f^{-1}(a) = (9a - 3) \textbf{ mod } 26$$

Check this: $f^{-1}(f(a)) \equiv f^{-1}(3a+9) \pmod{26}$

$\equiv 9(3a+9)-3 \pmod{26} \equiv 27a+81-3 \pmod{26}$

$\equiv 27a+78 \pmod{26} \equiv a \pmod{26}$.

So, for a in the range [0,25] we have $f^{-1}(f(a)) = a$ and f^{-1} and f are inverses of each other.

Modular Inverses

How one can invert f methodically?

Do a simpler example: $f(a) = 3a$ **mod** 26

Look for constant x and an inverse of the form:

$$f^{-1}(a) = xa$$

Then condition $f^{-1}(f(a)) \equiv a \pmod{26}$ gives:

$$f^{-1}(f(a)) \equiv x \cdot 3a \pmod{26} \equiv a \pmod{26}$$

The x satisfying this equality is:

$$3x \equiv 1 \pmod{26}$$

I.e. we wish to find an *inverse* of 3 modulo 26.

Modular Inverses

Definition: The ***inverse*** of e modulo N is the number s between 1 and N-1 such that

$$se \equiv 1 \pmod{N}$$

if such a number exists.

Q: What is the inverse of 3 modulo 26?

A: 9. Because $9 \cdot 3 = 27 \equiv 1 \pmod{26}$.

Q: What is the inverse of 4 modulo 8?

A: There is not any.

Modular Inverses

THM1: e has an inverse modulo N if e and N are relatively prime. I.e. $\gcd(e,N) = 1$.

This will follow from the following useful fact.

THM2: If a and b are positive integers, the gcd of a and b can be expressed as an integer combination of a and b. I.e., there are integers s,t for which

$$\gcd(a,b) = sa + tb$$

Modular Inverses Example

$5 \cdot 14 - 3 \cdot 23 = 1$ implies:

$\gcd(a,b) = sa + tb$

- $\gcd(14,23) = 1 = 5 \cdot 14 - 3 \cdot 23$
  - Any number dividing both 14 and 23 must divide 1
- The inverse of 14 modulo 23 is 5
  - $5 \cdot 14 = 1 + 3 \cdot 23$
  - $5 \cdot 14 \equiv 1 \pmod{23}$
- "An" inverse of 23 modulo 14 is -3
  - $-3 \cdot 23 = 1 - 5 \cdot 14$
  - $-3 \cdot 23 \equiv 1 \pmod{14}$
  - $11 \cdot 23 \equiv 1 \pmod{14}$
  - "The" inverse is 11

Modular Inverses

***Proof of* THM1 *using* THM2:**

If e,N are relatively prime, using THM2, we write $1 = se + tN$.

Rewrite this as $se = 1 - tN$.

In mod N, equivalent to $se \equiv 1 \pmod{N}$.

Thus, s seems to be an inverse of e.

Extended Euclidean Algorithm

Extended Euclidean Algorithm is a *constructive* version of THM2, it gives explicit inverses together with s and t.

The extended Euclidean algorithm works same as the regular Euclidean algorithm except that we keep track of the **quotient** ($q = x/y$).

This allows us to backtrack and write the gcd(a,b) as a linear combination of a and b.

Extended Euclidean Algorithm Examples

gcd(33,77)

Step	$x = qy + r$	x	y	gcd $= sx+ty$
0	–	33	77	

Extended Euclidean Algorithm Examples

gcd(33,77)

Step	$x = qy + r$	x	y	gcd $= sx+ty$
0	–	33	77	
1	$33=0\cdot 77+33$	77	33	

Extended Euclidean Algorithm Examples

gcd(33,77)

Step	$x = qy + r$	x	y	gcd = $sx+ty$
0	-	33	77	
1	$33=0\cdot 77+33$	77	33	
2	$77=2\cdot 33+11$	33	11	

Extended Euclidean Algorithm Examples

gcd(33,77)

Step	$x = qy + r$	x	y	gcd = $sx+ty$
0	-	33	77	
1	$33=0\cdot 77+33$	77	33	
2	$77=2\cdot 33+11$	33	11	
3	$33=3\cdot 11+0$	11	0	

Extended Euclidean Algorithm Examples

gcd(33,77)

Step	$x = qy + r$	x	y	gcd = $sx+ty$
0	–	33	77	
1	$33=0\cdot 77+33$	77	33	
2	$77=2\cdot 33+11$	33	11	
3	$33=3\cdot 11+0$	11	0	Solve for r. Plug it in.

Extended Euclidean Algorithm Examples

gcd(33,77)

Step	$x = qy + r$	x	y	gcd = $sx+ty$
0	–	33	77	gcd≠1 → (33,77) are not relatively prime
1	$33=0\cdot77+33$	77	33	
2	$77=2\cdot33+11$	33	11	$11 = 77 - 2\cdot33$
3	$33=3\cdot11+0$	11	0	Solve for r. Plug it in.

Extended Euclidean Algorithm Examples

gcd(244,117):

Step	$x = qy + r$	x	y	gcd $= sx+ty$
0	–	244	117	

Extended Euclidean Algorithm Examples

gcd(244,117):

Step	$x = qy + r$	x	y	gcd = $sx+ty$
0	–	244	117	
1	$244=2\cdot117+10$	117	10	

Extended Euclidean Algorithm Examples

gcd(244,117):

Step	$x = qy + r$	x	y	gcd $= sx+ty$
0	–	244	117	
1	$244=2\cdot117+10$	117	10	
2	$117=11\cdot10+7$	10	7	

Extended Euclidean Algorithm Examples

gcd(244,117):

Step	$x = qy + r$	x	y	gcd $= sx+ty$
0	–	244	117	
1	$244=2\cdot117+10$	117	10	
2	$117=11\cdot10+7$	10	7	
3	$10=7+3$	7	3	

Extended Euclidean Algorithm Examples

gcd(244,117):

Step	$x = qy + r$	x	y	gcd $= sx+ty$
0	–	244	117	
1	$244=2\cdot 117+10$	117	10	
2	$117=11\cdot 10+7$	10	7	
3	$10=7+3$	7	3	
4	$7=2\cdot 3+1$	3	1	

Extended Euclidean Algorithm Examples

gcd(244,117):

Step	$x = qy + r$	x	y	gcd = $sx+ty$
0	–	244	117	
1	$244=2\cdot117+10$	117	10	
2	$117=11\cdot10+7$	10	7	
3	$10=7+3$	7	3	
4	$7=2\cdot3+1$	3	1	
5	$3=3\cdot1+0$	1	0	

Extended Euclidean Algorithm Examples

gcd(244,117):

Step	$x = qy + r$	x	y	gcd $= sx+ty$
0	–	244	117	
1	$244=2\cdot117+10$	117	10	
2	$117=11\cdot10+7$	10	7	
3	$10=7+3$	7	3	
4	$7=2\cdot3+1$	3	1	$1=7-2\cdot3$
5	$3=3\cdot1+0$	1	0	Solve for r. Plug it in.

Extended Euclidean Algorithm Examples

gcd(244,117):

Step	$x = qy + r$	x	y	gcd $= sx+ty$
0	–	244	117	
1	244=2·117+10	117	10	
2	117=11·10+7	10	7	
3	10=7+3	7	3	1=7-2·(10-7) = -2·10+3·7
4	7=2·3+1	3	1	1=7-2·3
5	3=3·1+0	1	0	Solve for r. Plug it in.

Extended Euclidean Algorithm Examples

gcd(244,117):

Step	$x = qy + r$	x	y	gcd = $sx+ty$
0	–	244	117	
1	244=2·117+10	117	10	
2	117=11·10+7	10	7	1=-2·10+3·(117-11·10) = 3·117-35·10
3	10=7+3	7	3	1=7-2·(10-7) = -2·10+3·7
4	7=2·3+1	3	1	1=7-2·3
5	3=3·1+0	1	0	Solve for *r*. Plug it in.

Extended Euclidean Algorithm Examples

inverse of 244 mod 117

inverse of 117 mod 244

gcd(244,117):

Step	$x = qy + r$	x	y	gcd $= sx+ty$
0	–	244	117	
1	244=2·117+10	117	10	1=3·117-35·(244-2·117) = **-35**·244+**73**·117
2	117=11·10+7	10	7	1=-2·10+3·(117-11·10) = 3·117-35·10
3	10=7+3	7	3	1=7-2·(10-7) = -2·10+3·7
4	7=2·3+1	3	1	1=7-2·3
5	3=3·1+0	1	0	Solve for *r*. Plug it in.

Extended Euclidean Algorithm

<u>Summary</u>: EEA works by keeping track of how remainder r results from dividing x by y. Last equation (at the bottom) gives *gcd* in terms of last x and y.

In reverse direction, by repeatedly inserting r into the last equation, one can get the *gcd* in terms of bigger and bigger values of x,y until the very top is reached, which gives the *gcd* in terms of the inputs a,b.

Chinese Remainder Theorem

An ancient tale: Chinese Emperor used to count his army by giving a series of tasks.

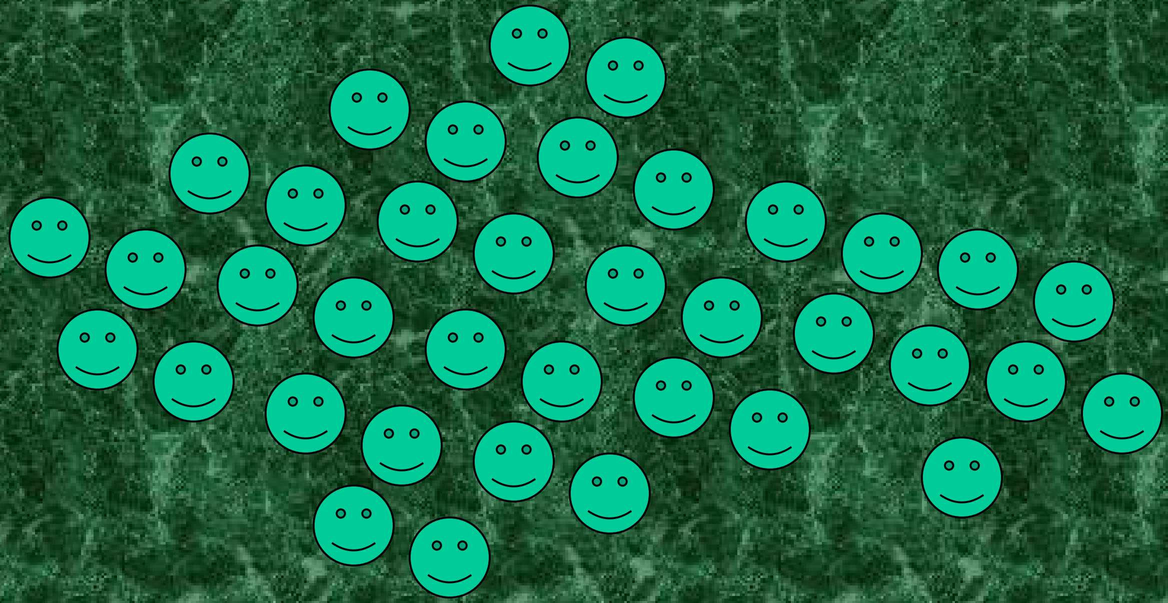
1. All troops should form groups of 3. Report back the number of soldiers that were not able to do this.

2. Now form groups of 5. Report back.

3. Now form groups of 7. Report back.

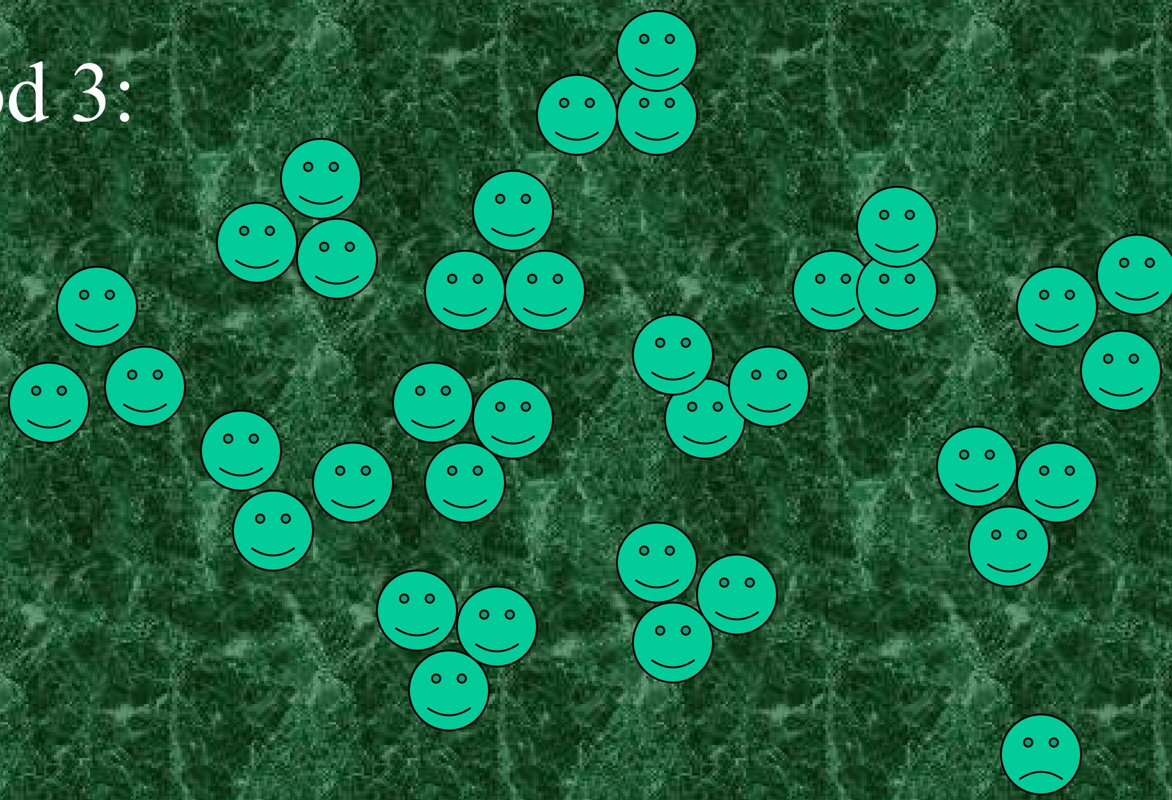
At the end, the emperor can ingeniously figure out how many troops there are.

Chinese Remainder Theorem



Chinese Remainder Theorem

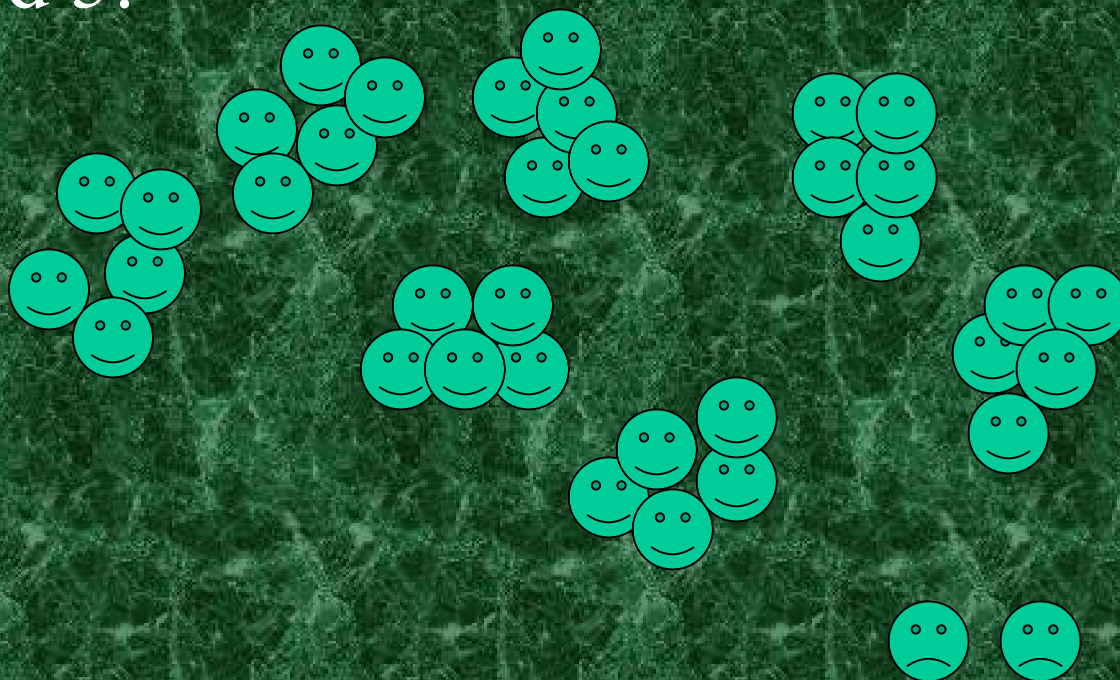
mod 3:



N **mod** $3 = 1$

Chinese Remainder Theorem

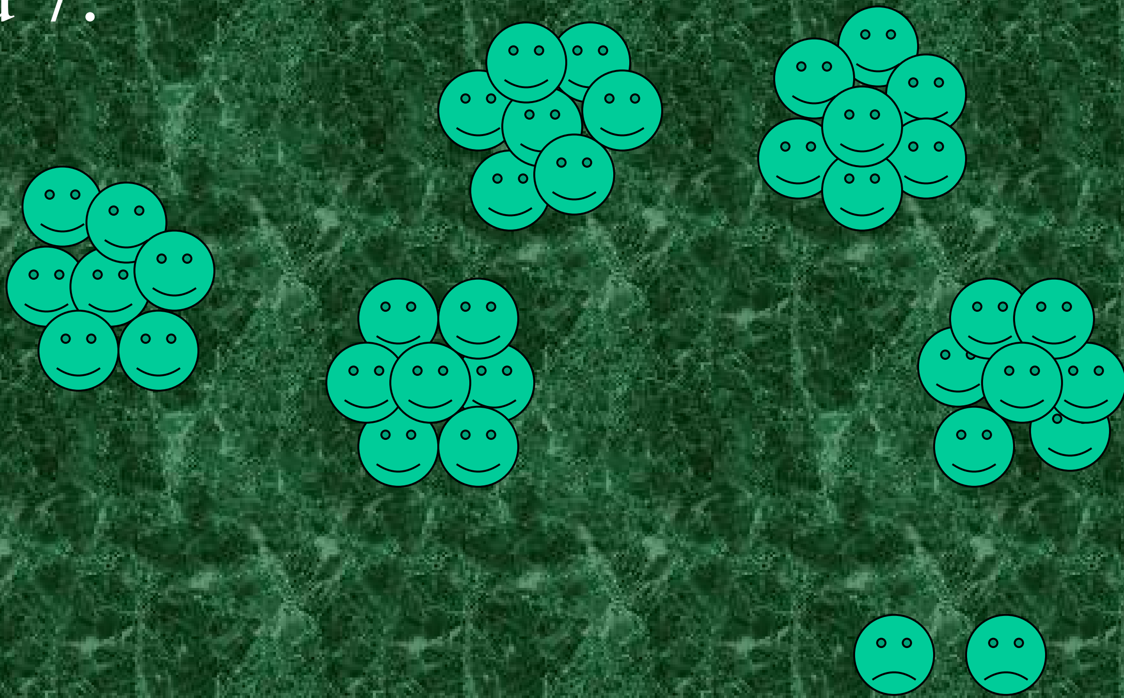
mod 5:



N **mod** $5 = 2$

Chinese Remainder Theorem

mod 7:



N **mod** $7 = 2$

Chinese Remainder Theorem

Secret inversion formula (for $N < 105 = 3 \cdot 5 \cdot 7$):

$$N \equiv a \pmod 3$$

$$N \equiv b \pmod 5$$

$$N \equiv c \pmod 7$$

Implies that $N = (70a + 21b + 15c)$ **mod** 105.

So in our case $a = 1$, $b = 2$, $c = 2$ gives:

$N = (70 \cdot 1 + 21 \cdot 2 + 15 \cdot 2)$ **mod** 105

$= (70 + 42 + 30)$ **mod** 105

$= 142$ **mod** 105

$= 37$

Chinese Remainder Theorem Example

1. Find three numbers l,m,n with following properties
   - $l \equiv 1 \pmod{3}$, $l \equiv 0 \pmod{5}$, $l \equiv 0 \pmod{7}$
   - $m \equiv 0 \pmod{3}$, $m \equiv 1 \pmod{5}$, $m \equiv 0 \pmod{7}$
   - $n \equiv 0 \pmod{3}$, $n \equiv 0 \pmod{5}$, $n \equiv 1 \pmod{7}$
2. Then $N = al + bm + cn$ [secret formula] satisfies
   - $N \equiv al + bm + cn \pmod{3}$

     $\equiv a \cdot 1 + 0 + 0 \pmod{3} \equiv a \pmod{3}$
   - Similarly, $N \equiv b \pmod{5}$
   - Similarly, $N \equiv c \pmod{7}$

Chinese Remainder Theorem Example

Find three numbers l,m,n. E.g., to find l :

a) Multiply all modulii that are different from 3.
Result: $5 \cdot 7 = 35$

b) Find an inverse of this number mod 3:
$2 \cdot 35 \equiv 1 \pmod 3$. Thus, 2 is an inverse of 35.

c) l is the product of (a) and (b): $l = 70$

l is 0 mod 5 and 7 since it's divisible by $5 \cdot 7$.
But (c) guarantees that it is 1 modulo 3!

Similarly, $m = 21$ (inverse of 21 modulo 5 is 1).

Similarly, $n = 15$ (inverse of 15 modulo 7 is 1).

Chinese Remainder Theorem Example

So our solution to all three congruences is:

$$N = \underset{\text{inv. of 35 mod 3}}{2}\cdot\underset{5\cdot 7}{35}\cdot a + \underset{\text{inv. of 21 mod 5}}{1}\cdot\underset{3\cdot 7}{21}\cdot b + \underset{\text{inv. of 15 mod 7}}{1}\cdot\underset{3\cdot 5}{15}\cdot c$$

- Remember, in our case $a = 1$, $b = 2$, $c = 2$
- If the solution is not between 0 and 104, just compute N **mod** 105.

RSA Cryptography

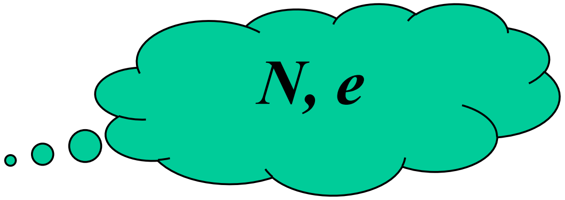
Most internet shopping sites offer a “secure connection” option that allows shoppers to disclose personal information such as credit card, address, etc. without fear that a snoop on the communication.

RSA Cryptography

There are several encryption methods. Perhaps the simplest "unbreakable" system is the RSA (Rivest, Shamir, Adleman).

The server site provides a large number ***N*** (e.g. a 400 digit number) and an ***encryption*** exponent ***e***.

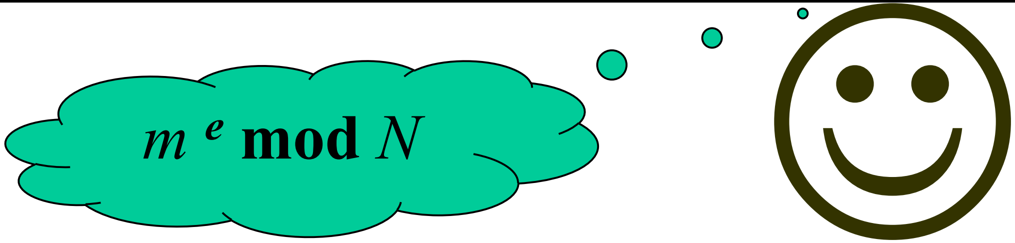
(N,e) is the ***public key.***



RSA Cryptography

- Mr. Smiley's browser then converts his message into numbers. The letters are put together into number blocks with each block less than N.
- Mr. Smiley's browser exponentiates each number block by the exponent e modulo N and broadcasts these garbled blocks back to the server site.

RSA Cryptography



$N = 4559$, $e = 13$.

Mr. Smiley Transmits: "Last name Smiley"

- 1201^{13} **mod** 4559, 1920^{13} **mod** 4559, …
- 2853 0116 1478 2150 3906 4256 1445 2462

RSA Cryptography

The server site receives the encrypted blocks:

$n = m^{e}$ **mod** N.

It has a ***private key***, decryption exponent d, which when applied to n recovers the original blocks

$m : (m^{e} \textbf{ mod } N)^{d} \textbf{ mod } N = m$

E.g. For $N = 4559$ and $e = 13$, the decryptor $d = 3397$.

RSA Cryptography

$N = 4559$, $d = 3397$

- 2853 0116 1478 2150 3906 4256 1445 2462
- 2853^{3397} **mod** 4559, 0116^{3397} **mod** 4559, …

RSA Cryptography

Public key is known by everyone, but private key, d, is kept secret. Why is this secure?

N is the product of two large prime numbers p,q. Each of them has approximately 200 digits.

e is relatively prime with $(p-1)\cdot(q-1)$.

d is inverse to e modulo $(p-1)\cdot(q-1)$.

To get d, someone (an intruder) should find p and q. However factorization of a 400 digit number N takes huge amount of time (billions of years in 2005).