

6	9	13	7
12	10	5	
3	4	14	
15	8	11	2

Euler's Theorem RSA encryption

6	9	13	7
12	10	5	
3	4	14	
15	8	11	2

Inverses mod n

Thm. If k is relatively prime to n , there is an inverse k'
 $k \cdot k' \equiv 1 \pmod{n}$

Cor.

OK to **cancel** (mod n)

6	9	13	7
12	10	5	
3	4	14	
15	8	11	2

The interval from 0 to n

$$[0, n) ::= \{0, 1, \dots, n-1\}$$

$$[0, n] ::= \{0, 1, \dots, n\}$$

6	9	13	7
12	10	5	
3	4	14	
15	8	11	2

Euler ϕ function

$\phi(n) ::= \# k \in [0, n)$ s.t.
 k rel. prime to n

$$\phi(7) = 6 \quad 1, 2, 3, 4, 5, 6$$

$$\phi(12) = 4 \quad 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11$$

6	9	13	7
12	10	5	
3	4	14	
15	8	11	2

Calculating ϕ

If p prime, everything from 1 to $p-1$ is rel. prime to p , so

$$\phi(p) = p - 1$$

6	9	13	7
12	10	5	
3	4	14	
15	8	11	2

Euler ϕ function

$\phi(49)?$

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, ..., 13, 14, 15, ..., 21, ...

every 7th number is divisible by 7

$$\text{so, } \phi(49) = 49 - 7$$

6	9	10	7
12	18	5	
3	1	4	14
15	8	11	2

Calculating ϕ

For $[0, p^k)$ every p th element is **not** rel. prime to p^k :

$0, 1, \dots, p-1, p, \dots, 2p, \dots, (p^{k-2})p, \dots, p^{k-1}$

$(1/p)p^k$ elements
not rel. prime to p^k

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 4, 2007

lec 8W.7

6	9	10	7
12	18	5	
3	1	4	14
15	8	11	2

Calculating ϕ

$$\phi(p^k) = p^k - p^{k-1}$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 4, 2007

lec 8W.8

6	9	10	7
12	18	5	
3	1	4	14
15	8	11	2

Calculating ϕ

For $1, 2, \dots, p-1, p, \dots, 2p, \dots, p^{k-1}, p^k$
every p th is **not** rel. prime to p^k

$$\phi(p^k) = p^k - p^{k-1}$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 4, 2007

lec 8W.9

6	9	10	7
12	18	5	
3	1	4	14
15	8	11	2

Calculating ϕ

Lemma :

For a, b relatively prime,

$$\phi(a \cdot b) = \phi(a) \cdot \phi(b)$$

pf: Pset 7 now;
another way in 3 weeks

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 4, 2007

lec 8W.10

6	9	10	7
12	18	5	
3	1	4	14
15	8	11	2

Euler's Theorem

For k relatively prime to n ,

$$k^{\phi(n)} \equiv 1 \pmod{n}$$

Fermat Thm a special case.
Euler proof essentially
same as Fermat:



Copyright © Albert R. Meyer, 2007. All rights reserved.

April 4, 2007

lec 8W.11

6	9	10	7
12	18	5	
3	1	4	14
15	8	11	2

Proof of Euler's Thm

For k relatively prime to n , let
 $r ::= \phi(n)$ and

k_1, \dots, k_r
the integers in $[0, n)$ relatively
prime to n . Then
 $\text{rem}(k_1 k, n), \text{rem}(k_2 k, n), \dots, \text{rem}(k_r k, n)$
is a permutation of k_1, \dots, k_r .
pf: cancel $k \pmod{n}$.

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 4, 2007

lec 8W.12

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Proof of Euler's Thm

So

$$\begin{aligned} k_1 \dots k_r &= \text{rem}(k_1 k, n) \dots \text{rem}(k_r k, n) \\ &\equiv k_1 k \dots k_r k \pmod{n} \\ &= k^r \cdot k_1 \dots k_r \pmod{n} \end{aligned}$$

But OK to cancel k_1, \dots, k_r , so
 $1 \equiv k^r \pmod{n}$.

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 4, 2007

lec 8W.13

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

RSA Public Key Encryption



Copyright © Albert R. Meyer, 2007. All rights reserved.

April 4, 2007

lec 8W.14

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Beforehand

- receiver generates primes p, q
- $n ::= pq$
- selects e rel. prime to $(p-1)(q-1)$
- $(e, n) ::=$ public key, publishes it
- finds d , inverse mod $(p-1)(q-1)$ of e
- d is secret key, keeps hidden

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 4, 2007

lec 8W.15

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Receiver's abilities

- find two large primes p, q
 - ok because: lots of primes
 - fast test for primality
- find e rel. prime to $(p-1)(q-1)$
 - ok: lots of rel. prime nums
 - gcd easy to compute
- find inverse of e
 - easy using Pulverizer or Euler

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 4, 2007

lec 8W.16

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

RSA

- Encoding message m :
 send $m' ::= \text{rem}(m^e, n)$
- Decoding m' :
 receiver computes
 $\text{rem}((m')^d, n) = m$

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 4, 2007

lec 8W.17

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Why does this work?

...explained in
 Team Problem

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 4, 2007

lec 8W.18



1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Why is it secure?

- easy to break *if* can factor n
(find d same way receiver did)
- conversely, from d can factor n
- but factoring appears hard
- has withstood 25 years of attacks

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 4, 2007

lec 8W.19



1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Team Problems

Problems 1&2

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 4, 2007

lec 8W.20