



# Euler's Theorem RSA encryption



## Euler $\phi$ function

$\phi(n) ::=$   
 $\# k \in 0, 1, \dots, n-1$  s.t.  
 $k$  has a  $(\text{mod } n)$   
 inverse



## Euler $\phi$ function

$\phi(n) ::= \# k \in 0, 1, \dots, n-1$  s.t.  
 $k$  rel. prime to  $n$

$\phi(7) = 6$     1,2,3,4,5,6

$\phi(12) = 4$

0,1,2,3,4,5,6,7,8,9,10,11



## Calculating $\phi$

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

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



## Euler $\phi$ function

$\phi(9)?$  0,1,2,3,4,5,6,7,8

$k$  rel. prime to 9 iff

$k$  rel. prime to 3

3 divides every 3rd number

so,  $\phi(9) = 9 - (9/3) = 6$



## Calculating $\phi(p^k)$

0,1,...,p,...,2p,...,p<sup>k</sup>-p,...,p<sup>k</sup>-1

$p$  divides every  $p$ th number

$p^k/p$  of these numbers  
 are not rel. prime to  $p^k$





### Calculating $\phi(p^k)$

So

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



Albert R Meyer,

April 2, 2010

lec 8F.8



### Calculating $\phi(a \cdot b)$

Lemma :

For  $a, b$  relatively prime,  
 $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$

pf: Pset 8. Another way  
in 2 weeks.



Albert R Meyer,

April 2, 2010

lec 8F.9



### Calculating $\phi(a \cdot b)$

$$\begin{aligned} \phi(12) &= \phi(3 \cdot 4) \\ &= \phi(3) \cdot \phi(4) \\ &= (3 - 1) \cdot (2^2 - 2^{2-1}) \\ &= 2 \cdot (4 - 2) = 4 \end{aligned}$$



Albert R Meyer,

April 2, 2010

lec 8F.10



### Euler's Theorem

For  $k$  relatively  
prime to  $n$ ,

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



Albert R Meyer,

April 2, 2010

lec 8F.11



### Fermat's Little Theorem

special case of Euler:

$$k^{p-1} \equiv 1 \pmod{p}$$

for prime  $p$



Albert R Meyer,

April 2, 2010

lec 8F.12



### Proof of Euler's Theorem

$n^* ::=$

$\{m \mid 0 < m < n, m \text{ rel prime to } n\}$

Note:  $m, k \in n^*$  implies

$$\text{rem}(mk, n) \in n^*$$



Albert R Meyer,

April 2, 2010

lec 8F.14



### Proof of Euler's Theorem

$n^* ::= \{m \mid 0 < m < n, m \text{ rel prime to } n\}$

Lemma: mult by  $k \in n^*$ , permutes  $n^*$ .



### permuting (mod 9)

$$\phi(9) = 3^2 - 3 = 6$$

$9^* =$ 

1	2	4	5	7	8
---	---	---	---	---	---



### permuting (mod 9)

$$\phi(9) = 3^2 - 3 = 6$$

$9^* =$ 

1	2	4	5	7	8	
2 ·	2	4	8	1	5	7



### permuting (mod 9)

$$\phi(9) = 3^2 - 3 = 6$$

$9^* =$ 

1	2	4	5	7	8	
2 ·	2	4	8	1	5	7
7 ·	7	5	1	8	4	2



### RSA Public Key Encryption


Photograph removed due to copyright restrictions.  
See here:  
<http://ams.org/samplings/feature-column/fcarc-internet> (under Public Key Systems)



### Beforehand


receiver generates primes  $p, q$   
 $n ::= p \cdot q$   
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




 **RSA**  $(0 \leq m < n)$

Encoding message  $m$ :  
 send  $m' ::= \text{rem}(m^e, n)$

Decoding  $m'$ :  
 receiver computes  
 $\text{rem}((m')^d, n) = m$

 Albert R Meyer, April 2, 2010 lec. 8F.26

 **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  $(\text{mod } (p-1)(q-1))$  inverse of  $e$


- easy using Pulverizer or Euler

 Albert R Meyer, April 2, 2010 lec. 8F.27


 **Why does this work?**


follows easily from Euler's Theorem when  $m$  has inverse mod  $n$

 Albert R Meyer, April 2, 2010 lec. 8F.28


 **Why does this work?**


actually works for all  $m$  ... explained in Class Problem 2

 Albert R Meyer, April 2, 2010 lec. 8F.29

 **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 so finding  $d$  must also be hard)
- RSA has withstood 30 years of attacks

 Albert R Meyer, April 2, 2010 lec. 8F.30

 **Team Problems**

# Problems

## 1 & 2

 Albert R Meyer, April 2, 2010 lec. 8F.31

MIT OpenCourseWare  
<http://ocw.mit.edu>

6.042J / 18.062J Mathematics for Computer Science  
Spring 2010

For information about citing these materials or our Terms of Use, visit: <http://ocw.mit.edu/terms>.