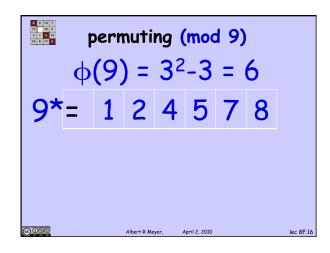
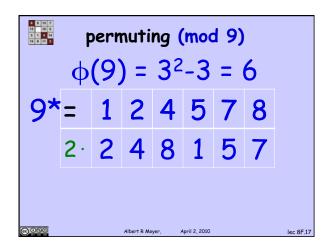


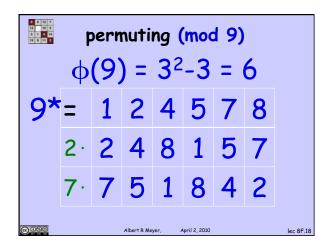
```
Proof of Euler's Theorem

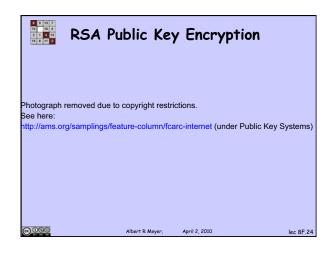
n*::=
{m|0<m<n, m rel prime to n}

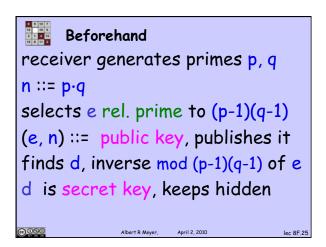
Lemma: mult by k∈n*,
permutes n*.
```











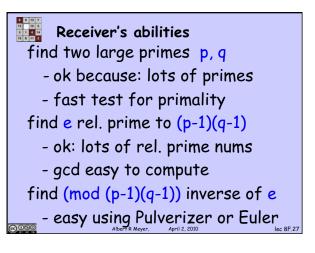
```
Encoding message m:

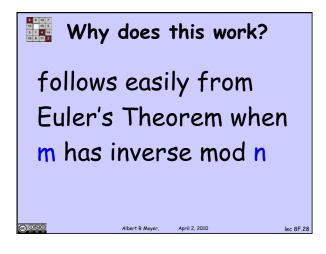
send m' ::= rem(me, n)

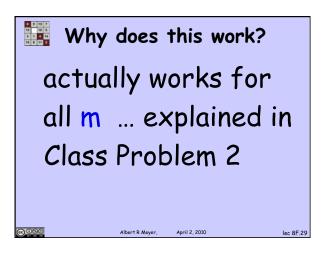
Decoding m':

receiver computes

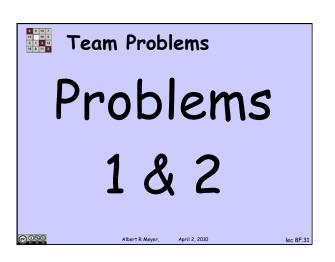
rem((m')d, n) = m
```











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.