Last time, CRT:

if we want to solve

$$x \equiv a \pmod{m}$$
$$x \equiv b \pmod{n}$$

can always do it if $\gcd(m,n) = 1$

answer is unique mod mn.

More generally, if $\gcd(m,n) = d$

you can solve iff $a \equiv b \pmod{d}$
and the answer is unique
mod $mn/d = \operatorname{lcm}(m,n)$.

Fermat's little thm. (Prop 3.3)

if p is prime then

$$n^p \equiv n \pmod{p}$$

if $p \nmid n$ then $\gcd(n,p) = 1$

$$n \cdot n^{p-1} \equiv n \cdot 1 \pmod{p}$$

so $n^{p-1} \equiv 1 \pmod{p}$

RSA Encryption
(based on §7.3 # 38)

I have a secret message to send you:

HAPPY MONDAY

Shifrin's code: A = 01, B = 02, ... Z = 26
space = 00 period = 27

08 01 16 16 25 00 13 15 14 04 01 25
m_1 m_2 m_3 ...

let $e = 3$ ⇝ or $65537 = 2^{16} + 1$ prime!

$p = 47$
$q = 59$

$k = (p-1)(q-1) = 2668$
$N = pq = 2773$

chose p, q so that

$\gcd(p-1, e) = 1$
$\gcd(q-1, e) = 1$
$\Leftrightarrow \gcd(k, e) = 1$

find d such that $de \equiv 1 \pmod{k}$

$d = 889 \equiv 1779 \pmod{k}$

You say "my public key is $e = 3$, $N = 2773$"

I encrypt the message:

$m_1 = 0801 \rightsquigarrow c_1 \equiv m_1^e \pmod N$

$c_1 = 2311$

$m_2 = 1616 \rightsquigarrow c_2 \equiv m_2^e \pmod N$

$c_2 = 662$

$m_3 = 2500 \rightsquigarrow c_3 = 1857$

etc.

I send it to you

You decrypt it by taking

$m_1 \equiv c_1^d \pmod N$

$2311 \rightsquigarrow 801$

$662 \rightsquigarrow 1616$

$1857 \rightsquigarrow 2500$

etc.

Why does it work?

$c \equiv m^e \pmod N$

so $c^d \equiv m^{de} \pmod N$

I claim $m^{de} \equiv m \pmod N$

by CRT, enough to show that

$m^{de} \equiv m \pmod p$

and $\pmod q$

we have $de \equiv 1 \pmod{k}$

so $de = kl + 1$ for some $l \in \mathbb{Z}$.

and $k = (p-1)(q-1)$

so $m^{de} = m^{kl+1}$

$= m^{(p-1)(q-1)l+1}$

$= (m^{p-1})^{(q-1)l} \cdot m$

if $p \nmid m$ then this $\equiv 1^{(q-1)l} \cdot m \pmod{p}$

if $p \mid m$ then both sides $\equiv 0 \pmod{p}$

either way, $m^{de} \equiv m \pmod{p}$

Similarly $m^{de} \equiv m \pmod{q}$