Feb 6th.

Recall: Euler's Theorem
if $\gcd(a,m)=1 \quad a,m>1$
then $a^{\varphi(m)} \equiv 1 \pmod m$

Let $b_1, b_2, \cdots, b_{\varphi(m)}$ be all #s relatively prime to m.

look at $ab_1, ab_2, ab_3, \cdots, a\cdot b_{\varphi(m)}$

① $\gcd(a,m)=1$
$\gcd(b_i,m)=1$
$\Rightarrow a\cdot b, a b_2, \cdots ab_{\varphi(m)}$ are relatively prime to m.

② Claim:
$a\cdot b_i \not\equiv a\cdot b_j \pmod m$ if $i\neq j$
if $a\cdot b \equiv a\cdot b_j \bmod m \Rightarrow m \mid a\cdot b_i - ab_j = a(b_i-b_j)$

last $\gcd(m,a)=1$

$\Rightarrow m / b_i-b_j$ but $|b_i-b_j|<m$

$\Rightarrow b_i-b_j=0 \Rightarrow b_i=b_j$

$\Rightarrow a\cdot b, a\cdot b_2, \cdots, ab_{\varphi(m)}$ are distinct (mod m)

③ Let $a\cdot b_i \equiv m_i \pmod m$ divide $a\cdot b_i$ by m with remainder $0\le m_i<m$

$ab_1 \quad a\cdot b_2 \quad \cdots \quad ab_{\varphi(m)}$
$\|| \quad\quad \||$
$m_1 \pmod m \quad m_2 \pmod m \quad\quad m_{\varphi(m)} \bmod m$

④ Claim $\gcd(m_i,m)=1$
In general if $x\equiv y \bmod m \Rightarrow x=y+km$
then $\gcd(x,m)=\gcd(y,m) \quad\quad d\mid x \ \&\ d\mid m \Leftrightarrow d\mid y \ \&\ d/m$

in particular if $\gcd(x,m)=1 \Leftrightarrow \gcd(y,m)$
$\Rightarrow$ have $m_1, \cdots, m_{\varphi(m)}$ are all $\le m$, distinct & relatively prime to m

$\Rightarrow m_1 \cdots m_{\varphi(m)}$ are the same as
$b_1 \cdots b_{\varphi(m)}$ in the same order

$\Rightarrow m_1 \cdots m_{\varphi(m)} \equiv b_1 \cdots b_{\varphi(m)} \pmod m$
$\|$
$(ab_1)(ab_2)\cdots(ab_{\varphi(m)})$

$a^{\varphi(m)}\cdot b_1 \cdots b_{\varphi(m)} \equiv b_1 \cdots b_{\varphi(m)} \pmod m$
$\Rightarrow m \mid a^{\varphi(m)} b_1 \cdots b_{\varphi(m)} - b_1 \cdots b_{\varphi(m)} = (a^{\varphi(m)}-1) b_1 \cdots b_{\varphi(m)}$
but $\gcd(m, b_1 \cdots b_{\varphi(m)})=1 \quad\quad \Rightarrow m \mid a^{\varphi(m)}-1 \Rightarrow a^{\varphi(m)} \equiv 1 \bmod m$

Ex: $m=10$ $\varphi(m)=\varphi(10)=\varphi(5\cdot 2)=(5^1-5^0)(2^1-2^0)=(5-1)(2-1)=4$

If $(a,m)=1 \Rightarrow a^4 \equiv 1 \bmod 10$
ex: $a=3$ $3^4=81\equiv 1 \bmod 10$
$a=7$ $7\equiv -3 \bmod 10$
$7^2\equiv(-3)^2\equiv 9 \bmod 10$
$7^4\equiv(-3)^4\equiv 81\equiv 1 \bmod 10$

Ex: Find $5^{999} \bmod 9 = ?$
$\gcd(5,9)=1$
$\Rightarrow 5^{\varphi(9)}\equiv 1 \bmod 9$
* $\varphi(9)=\varphi(3\cdot 3)=3^2-3^1=6$
$5^6\equiv 1 \bmod 9$
* $999\equiv 996+3$
↳ divisible by 2 & 3

$999=6k+3$ for some k

$5^{999}\equiv 5^{6k+3}\equiv 5^{6k}\cdot 5^3\equiv 5^3 \bmod 9 = -1 \bmod 9$
↳ $1 \bmod 9$

✡
$6^{3^{101}} \pmod{22} = ?$
$\varphi(22)=\varphi(2\cdot 11)=(2-1)(11-1)=10$
~~$6^{10}\equiv 1 \bmod 22$~~ b/c 6 & 22 aren't relatively prime
$\gcd(6,22)\neq 1$

Let's first find $6^{3^{101}} \bmod 11$
$\gcd(6,11)=1$
$\Rightarrow 6^{\varphi(11)}\equiv 1 \bmod 11$
$6^{10}\equiv 1 \bmod 11$ * $\varphi(11)=10$
Need to find $3^{101} \bmod 10$, $\gcd(3,10)=1$
$3^{\varphi(10)}\equiv 1 \bmod 10$
$\varphi(10)=\varphi(2\cdot 5)=(2-1)(5-1)=4$
$3^4\equiv 1 \bmod 10$

$101\equiv 1 \bmod 4$
* $101=4\cdot 25+1$
$3^{101}=3^{100}\cdot 3=(3^4)^{25}3\equiv 1\cdot 3\equiv 3 \bmod 10$
$\Rightarrow 3^{101}=10k+3$ for some k

$6^{3^{101}}=6^{10k+3}=(6^{10})^k\cdot 6^3\equiv 6^3 \bmod 11$
$6^2=36\equiv 3 \bmod 11$
11 | 33+3

$\Rightarrow 6^3\equiv 36\cdot 6\equiv 3\cdot 6\equiv 18\equiv 7 \bmod 11$

What about $6^{3^{101}} \bmod 22$?
$(6^3)^{3^{101}}\equiv 7 \pmod{11}\equiv 7+11\equiv 18 \bmod 11$
$\Rightarrow 6^{3^{101}}\equiv 18 \bmod 22$

* $11 \mid 6^{3^{101}}-18$ even
$2 \mid 6^{3^{101}}-18$ also even
$\Rightarrow 22 \mid 6^{3^{101}}-18$

RSA Encryption

Lemma: Let $N=p\cdot q$ where p and q are prime and $p\neq q$ then $a^{k\varphi(N)+1}\equiv a \pmod N$ for any a

Proof: $\gcd(a,N)=1,\ p,q$ or pq

Case 1: $\gcd(a,N)=1 \Rightarrow a^{\varphi(N)}\equiv 1 \pmod N$ By Euler's Thm

$\Rightarrow a^{k\varphi(N)}=a^{\varphi(N)k}\equiv 1 \bmod N$

$a^{k\varphi(N)+1}\equiv a\cdot 1\equiv a \bmod N$

Case 2: $\gcd(a,N)=pq=N$ i.e N/a

$\Rightarrow a\equiv 0 \bmod N \quad a^{k\varphi(N)+1}\equiv 0 \bmod N$

$a^{k\varphi(N)+1}\equiv 0\equiv a \bmod N$

Case 3: $\gcd(a,N)=p \quad a=p\cdot\tilde{a}$, $\tilde{a}$ is not divisible by q

$\Rightarrow \tilde{a}^{\varphi(q)}\equiv 1 \pmod q$ $\gcd(\tilde{a},q)=1$

$\tilde{a}^{q-1}\equiv 1 \pmod q$ $\varphi(q)=q-1$, $N=pq$, $\varphi(p)=p-1$

$\Rightarrow (\tilde{a}^{q-1})^{p-1}\equiv 1 \pmod q$

$\tilde{a}^{\varphi(N)}\equiv 1 \bmod q$

$a=\tilde{a}\cdot p$

$a^{\varphi(N)}=\tilde{a}^{\varphi(N)}p^{\varphi(N)}\equiv$

$\gcd(a,N)=p$ a is divisible by p but not by q

$\gcd(a,q)=1$

$a^{\varphi(q)}\equiv 1 \bmod q \Rightarrow (a^{q-1})^{p-1}\equiv 1^{p-1} \bmod q$

$a^{q-1}\equiv 1 \bmod q$

$a^{(p-1)(q-1)=\varphi(N)}\equiv 1 \bmod q$

$a^{\varphi(N)}\equiv 1 \bmod q$

$a^{k\varphi(N)}\equiv 1 \bmod q$

$a^{k\varphi(N)+1}\equiv 1\cdot a\equiv a \bmod q$

* $q \mid a^{k\varphi(N)+1}-a$ $p\mid a$ since $\gcd(a,N)=a$

$p\mid a^{k\varphi(N)+1} \Rightarrow p\mid a^{k\varphi(N)+1}-a \Rightarrow pq\mid a^{k\varphi(N)+1}-a$

$q\mid a^{k\varphi(N)+1}-a$

$\Rightarrow k^{\varphi(N)+1}\equiv a \bmod (pq)$, $pq=N$

How RSA Encyption Works?

Recevier picks 2 very large prime #'s p and q

Compute $N=p\cdot q$ and $\varphi(N)=(p-1)(q-1)$

Receiver also picks an encoder which is a number E relatively prime to $\varphi(N)$

$$\gcd(E, \varphi(N)) = 1$$

$\Rightarrow$ Receiver broadcasts the pair (N, E)
Sender waits to send secret message

$$0 < M < N$$

Sender takes M and computes $M^E \bmod N$
$0 \leq R < N$

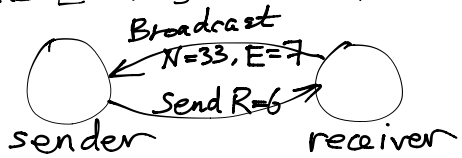
The Receiver gets R and the sender wants to recover M
E is relatively prime to $\varphi(N) \Rightarrow$ there exists D-decoder such that $ED \equiv 1 \bmod \varphi(N)$

$\gcd(a, m) = 1 \Rightarrow a^{\varphi(m)} = 1 \bmod m \Rightarrow a \cdot a^{\varphi(m)-1} \equiv 1 \bmod m$
if $\gcd(a, m) = 1 \Rightarrow a^{\varphi(m)} = 1 \bmod m \Rightarrow a \cdot a^{\varphi(m)-1} \equiv 1 \bmod m$
Receiver computes
$R^D \bmod N$
Claim: $R^D \equiv M \bmod N \longrightarrow$ Why is this so?
$R = M^E \bmod N$

$R^D = (M^E)^D = M^{ED} = M^{1+k\varphi(N)} \equiv M \pmod N$
$\hookrightarrow$ by Lemma.

The spy hears (N, E) that the receiver broadcast and hears R.
Why can't the spy recover M?
To recover M, one needs D s.t. $DE \equiv 1 \bmod \varphi(N)$
if you know $D \Rightarrow$ take $R^D \bmod N \equiv M$
The problem is that the spy can't compute $\varphi(N) = (p-1)(q-1)$
The spy can't factor N or pq

Ex) $p = 3$, $q = 11$, $N = p \cdot q = 3 \cdot 11 = 33$
$\varphi(N) = (3-1)(11-1) = 2 \cdot 10 = 20$
Take $E = 7$, $\gcd(7, 20) = 1$



What was the secret message M ($M < 33$)
Recevier needs D such that
$D \cdot E \equiv 1 \bmod \varphi(N)$
$\quad\;\; \| \qquad\quad \|$
$\quad\;\; 7 \qquad\quad 20$

$7D \equiv 1 \bmod 20$
$D = 3$ works ✓

$R^D = 6^3 \bmod 33 \equiv 18 \bmod 33$

$6^2 = 36 \equiv 3 \bmod 33$

$6^3 \equiv 3 \cdot 6 \equiv 18 \bmod 33$

$N = 18$ —Original Secret Message

Check $M = 18$ take $M^E \bmod N$ (M^E = R)

$18^7 \bmod 33 = 6 \bmod 33$

Check