We can compute $ax \equiv b \pmod{n}$

$$m = 1873 \cdot 131$$

$$\phi(m) = 1872 \cdot 130$$

$e = 323$ $\quad = 243360$ (same order of magnitude as m)

Solve:

$$d \cdot 323 + l \cdot 243360 = 1$$

$$\iff d \cdot 323 \equiv 1 \pmod{243360}$$

$$243360 = 753 \cdot 323 + 141 \qquad 243360 + 753 \cdot 323 = 141$$

$$323 = 2 \cdot 141 + 41 \qquad 323 - 2 \cdot 141 = 41$$

$$141 = 3 \cdot 41 + 18 \qquad 141 - 3 \cdot 41 = 18$$

$$41 = 2 \cdot 18 + 5 \qquad 41 - 2 \cdot 18 = 5$$

$$18 = 3 \cdot 5 + 3 \qquad 18 - 3 \cdot 5 = 3$$

$$5 = 1 \cdot 3 + 2 \qquad 5 - 3 = 2$$

$$3 = 1 \cdot 2 + 1 \implies 3 - 2 = 1$$

$$\implies \underbrace{148247}_{d} \cdot 323 + \underbrace{l}_{e} \cdot 243360 = 1$$

$$M = 7210 \pmod{26} \equiv 8 \rightarrow \text{"I"}$$

$$\left\lfloor 7210/26 \right\rfloor = 277 \pmod{26} \equiv 17 \rightarrow \text{"R"}$$

$$\left\lfloor 277/26 \right\rfloor = 10 \pmod{26} \equiv 10 \rightarrow \text{"K"}$$

~~"IQH"~~

~~"KRI"~~

$$\cancel{10 \cdot 26^0 + 17 \cdot 26^1 + 8 \cdot 26^2 =}$$

"IRK" $8 \cdot 26^0 + 17 \cdot 26^1 + 10 \cdot 26^2 =$

$= 7210$

A	0
B	1
C	2
D	3
E	4
F	5
G	6
H	7
I	8
J	9
K	10
L	11
M	12
N	13
O	14
P	15
Q	16
R	17

$$2905^{323} \pmod{245363}$$

$$2905^{322} \cdot 2905 \equiv$$

$$2905^{322} \equiv \left(2905^{161}\right)^2$$

$$2905^{161} \equiv 2905 \cdot 2905^{160}$$

$$2905^{160} \equiv \left((2905)^{80}\right)^2$$

Why it works:

$$M^e \equiv C \pmod{m}$$

then

$$C^d \equiv (M^e)^d \pmod{m}$$

$$\equiv M^{ed} \equiv M^{k\phi(m)+1} \equiv (M^{\phi(m)})^k M^1 \pmod{m}$$

as long as $M^{\phi(m)} \equiv 1 \pmod{m}$ then $\equiv M \pmod{m}$

because $ed \equiv 1 \pmod{\phi(m)}$

is the same as $ed - 1 = k\phi(m)$

Rare case if M and m have factor of (say q) then there is an issue.

$M = ql$ and $m = p \cdot q$

$$M^{ed} \equiv q^{ed} l^{ed} \pmod{m}$$

but mod p

$$M^{ed} \equiv M^{k\phi(m)+1} \equiv M^{k(p-1)(q-1)+1} \pmod{p}$$

$$\equiv (M^{k(q-1)})^{(p-1)} \cdot M^1 \equiv M \pmod{p}$$

$$= lq(M^{k(q-1)(p-1)} - 1) = lkpq = lkm$$

$$M\left(M^{k(q-1)(p-1)}-1\right) = l\cdot k\cdot m$$

$$M\cdot M^{k(q-1)(p-1)} \equiv M \pmod{m}$$

$\Rightarrow$ even if M has a factor with q we still have

$$M^{ed} \equiv M \pmod{m}$$

but we don't have $M^{\phi(m)} \equiv 1 \pmod{m}$

To sign a message:

$$E_{Danielle}\left(D_{Mike}(Sig)\right) \xrightarrow[\text{Danelle}]{\text{send to}} D_{Danielle}\left(E_{Mike}\left(E_{Danielle}\left(D_{Mike}(Sig)\right)\right)\right)$$

$$E_{Danielle}\left(D_{Mike}(Sig)\right) = \text{encryped Signature}$$

$$D_{Danielle}\left(E_{Mike}\left(E_{Danielle}\left(D_{Mike}(Sig)\right)\right)\right) = Sig$$

We know that this Sig came from Mike because the public key of Mike $E_{Mike}(\quad)$ was the thing that decrypts it.

Moreover, only Danielle can tell that it came from me.

Public Key Exchange: An Example

Powers of 2 mod 37

s	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
2^s	2	4	8	16	32	27	17	34	31	25	13	26	15	30	23	9	18	36

s	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
2^s	35	33	29	21	5	10	20	3	6	12	24	11	22	7	14	28	19	1

Powers of 17 mod 37

s	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
17^s	17	30	29	12	19	27	15	33	6	28	32	26	35	3	14	16	13	36

s	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
17^s	20	7	8	25	18	10	22	4	31	9	5	11	2	34	23	21	24	1

Say that *Alice* and *Bob* wish to communicate after agreeing on on a public modulus 37 and a primitive root 17. *Alice* also chooses a secret key 9 and so she sends $17^9 \equiv 6 \ (mod\ 37)$ to *Bob*. At the same time *Bob* chooses 10 as his secret key and so he sends $17^{10} \equiv 28 \ (mod\ 37)$ to *Alice*. *Alice* and *Bob* do not know each others secret keys but they *do* know $17^{\text{secret key}} \ (mod\ 37)$.

The common key to *Alice* and *Bob* is

$$\boxed{6^{10} = 17^{9\times 10} = 28^9 \bmod 37}$$

$2^6 \equiv 27 \qquad 27^2 \equiv (2^6)^2 \equiv 2^{12} \qquad 27^3$

s	1	2	3	4	5	6	7	8	9	10	
27^s	27	26	36	10	11	1	27	26	36	10	.....

s	1	
32^s	32	

32 is also a primitive root. mod 37

but 27 is not. mod 37

if a is a primitive root mod n then a^s is also a primitive root mod n iff

$$\gcd(s, \phi(n)) = 1$$

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

$$ax \equiv b \pmod{n}$$

Note

$a^r \equiv a^s \pmod{n}$ $\cancel{ax \equiv b}$ $\pmod{37}$

$\Rightarrow r \equiv s \pmod{\phi(n)}$

if $\gcd(a,n) = 1$

$$13^x \equiv 5 \pmod{37}$$

$$2^{23+k36} = (2^{11})^x \equiv 2^{23}(2^{36})^k \pmod{37}$$

$$2^{36} \equiv 1 \pmod{37}$$

$= 4 \cdot 36 - 13 \cdot 11$

$= 4(36 - 3 \cdot 11) - 11$

$= 4 \cdot 3 - 11$

$= 3 - (11 - 3 \cdot 3)$

$1 = 3 - 2$

$23 + k36 = 11x \Longrightarrow \underbrace{13 \cdot 11}x \equiv 23 \cdot 13 \pmod{36}$

$36 = 3 \cdot 11 + 3$

$11 = 3 \cdot 3 + 2$

$3 = 2 + 1$

$$-x \equiv 23 \cdot 13 \pmod{36}$$

$$x \equiv 23^2 \pmod{36}$$