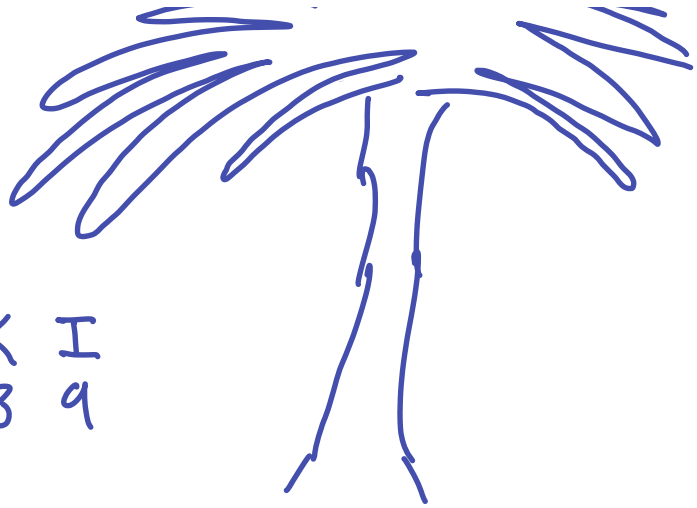
Math 4400
Week 6 - Thursday.
RSA

But the way, this all takes

place in Hawaii.
(Didn't you see the palm tree?)



E	A	O	H	L	M	N	K	I
1	2	3	4	5	6	7	8	9

Bob needs to tell Alice "KONA"

K	O	N	A
8	3	7	2

← Break up in to 2 numbers $< M = 1517$.

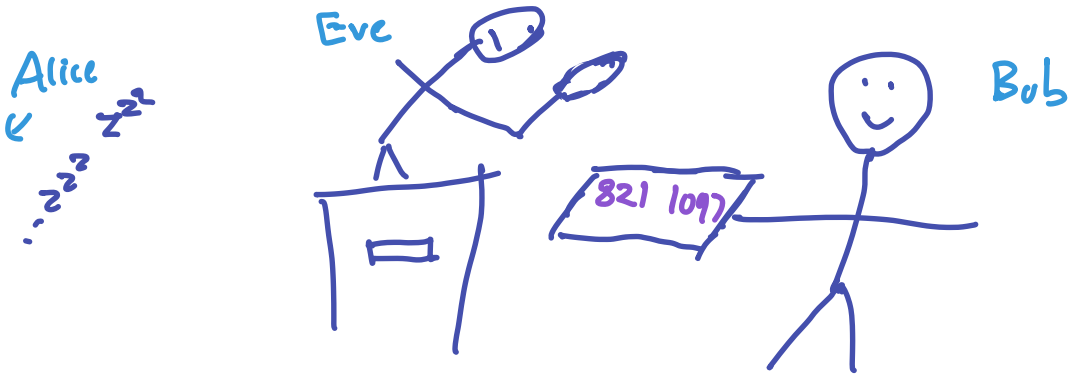
KO - NA

83 72

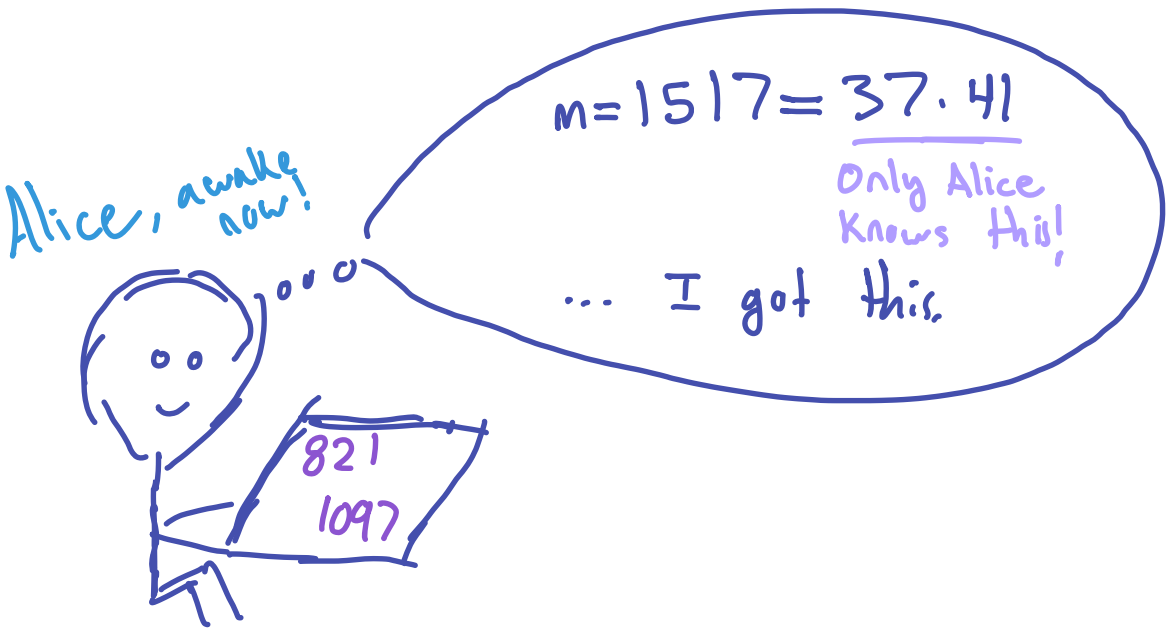
Bob computes $83^{11} \equiv 821 \mod 1517$

$72^{11} = 1097 \mod 1517$.

↑ Raise to the $e=11$ mod $M=1517$



Later that day...



To decrypt, Alice needs to solve

$x^{11} \equiv 821 \mod 1517$

$y^{11} \equiv 1097 \mod 1517$

FACT: Unique solutions are given by

$X \equiv 821^d \mod 1517$

$y = 1097^d \bmod 1517$

where d is a mutiplicative inverse of $e = 11 \bmod \phi(1517)$

Why? $x^{11} \equiv 821 \bmod 1517$

$(x^{11})^d \equiv 821^d \bmod 1517$

$x^{11d} \equiv 821^d \bmod 1517$

$11d = 1 + q\phi(1517)$

$x \cdot x^{q\phi(1517)} \equiv 821^d \bmod 1517$

$x \cdot (x^q)^{\phi(1517)} \equiv 821^d \bmod 1517$

$1^{11} = 1$

$x \equiv 821^d \bmod 1517$

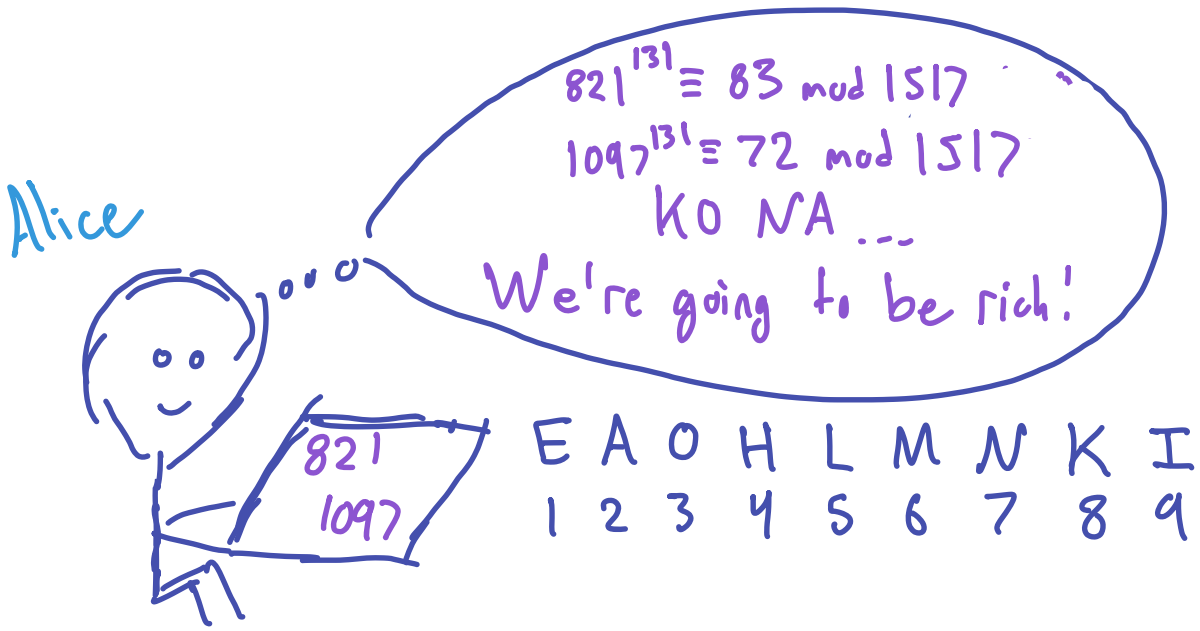
Basically Lagranges Theorem
- if $x^q \in (\mathbb{Z}/1517)^x$ the size of the group is $\phi(1517)$
- still Lagrange's Theorem + Chinese Remainder Theorem in general.

Alice can compute d because she can compute $\phi(1517)$:

Alice Knows $1517 = 37 \cdot 41$ (prime factorization)

so $\phi(1517) = 36 \cdot 40 = 1440$

Multiplicative inverse of 11 mod 1440 is $d = 131$.



RSA:

Alice wants people to be able to send her encryted messages

① She picks (big) prime numbers p, q.

$1517 = 37 \cdot 41$

$m = pq$

$37 \quad 41$

② She computes $\phi(m) = \phi(p)\phi(q) = (p-1)(q-1)$

$1440 = 36 \cdot 40$

③ She picks a number e (11) with $\gcd(e, \phi(m)) = 1$.

and computes

d = mult. inverse of e mod $\phi(m)$. (131)

④ She makes publicly available:

1517 m, the modulus

11 e, the encryption/public key.

She keeps private:

$p, q, \phi(m)$ and together made

131 d, the decryption/private key.

To send her a message, I:

1) Turn the letters into numbers

KONA → 8372

2) Break it into chunks with fewer digits than m

8372 → 83 72

3) Take each chunk x and send x^e mod m.

Send 821, 1017

$821^{131} \equiv 83 \pmod{1517}$ $1017^{131} \equiv 72 \pmod{1517}$

To decrypt the message, Alice

① Takes each chunk y and computes $y^d \bmod n$

$821^{131} \equiv \underline{83} \bmod 1517$ $1017^{131} \equiv \underline{72} \bmod 1517$

② Converts the result back into letters

83 72

KO NA

KONA.

In RSA, you see $m, e,$ transmit $x^e \equiv$ ← message

In Diffie-Hellman, you see p, g transmit g^a (to start key exchange)

Careful not to swap the base and exponent!

A stays on the ground

e^{v} e^{v} e^{v} is an exponent.