RSA experience

Bob wants to **receive** secret messages

Choose 2 prime numbers p1 and p2

p1 = 11

p2 = 13

Compute public n = p1*p2:

n = 143

Compute φ(n) = (p1-1)*(p2 -1) and keep it private

φ(n) = 10*12 = 120

Choose public encryption exponent e to be a random prime number less than φ that is also not a divisor of φ, but such that kφ(n)+1 is divisible by this number
Non-divisors of φ: 1, 2, 3, 4, 5, 6, **7**, 8, 9, ...
Chosen public e = 7

Post n and e for everyone to use: n= 143, e = 7

Compute decryption exponent d= (kφ(n)+1)/e (must be an integer)
(1*120 + 1)/7 = 17.3
(2*120 + 1)/7 = 34.4
(3*120 + 1)/7 = 51.6
(4*120 + 1)/7 = 68.7
(5*120 + 1)/7 = 85.9
(6*120 + 1)/7 = **103**

d= (6*120 + 1)/7 = **103**
d = 103

Alice wants to **send** secret messages

Get public values of n and e: n = 143, e = 7

Select a secret number to send to Bob (make it a small prime to be a coprime with n)):
Alice wants to send number x= 19

Encrypt it using formula x^e mod n, and e and n provided by Bob.
She computes encrypted number y = x^e mod n = 19^7 mod 143 = 46
https://www.mtholyoke.edu/courses/quenell/s2003/ma139/js/powermod.html

Send y = 46

Bob receives secret messages

Receive y from Alice:

y = 46

Bob decrypts it using decryption exponent d:

x = y^d mod n

x = 46^103 mod 143 = 19