Name:_____

In 1975, Whitfield Diffie introduced a method of cryptography where it would be very difficult to figure out the decryption key from the encryption key. In 1977, Rivest, Shamir, and Adelmen invented the RSA encryption method that we still use today. In summary it involves a type of encryption where the receiver chooses both the encryption key and the matching decryption key.

AND after the receiver chooses the key, he lists the key in a public directory so that anyone can send messages but only he knows how to decrypt it. Think of the mailbox example in the code.org video from U4L6 from yesterday.

The math behind how it works will be explained using 2 very small relatively prime numbers, however, in the real world this is done with very large prime numbers that are so large trying to solve the encryption key is computational too hard at this time.

1. You must pick 2 prime numbers for p and q

    We will use 5 for p and 11 for q

2. Then you must pick a number that is relatively prime to (p-1) x (q-1) for e

    Relatively prime means it doesn't share any factors with eachother

    We will use 7 for e

3. Calculate n = p x q

4. Encryption Key is (n, e)

    This is public and anyone can use it to send you a message

5. To encrypt a message using this key (55, 7) you would use the equation: $C = m^e \bmod n$ where C is the cipher text and m is the original message.

$C = 9^7 \bmod 55$ SO The letter j = 9 and after encrypting it becomes 4 or E

6. Now try to encrypt the message "I Love CS" with this encryption key.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
S	T	U	V	W	X	Y	Z										
18	19	20	21	22	23	24	25										

Now to decrypt using these numbers….

If the encrypted E or 4 was originally j or 9, then we can use that to help using $m = C^d \bmod n$ where C = the cipher text (E in this case), n is from the original prime numbers in the public key, and d is the decryption key.

So you have p, q, and e from the public key and now is where it is computationally hard, d is:

$ed = 1(\text{mod}(p-1)(q-1))$

So in our example $7d = 1\text{mod}(40)$ or the way I have been writing it in class: $7xN = 1\bmod 40$

Using a spreadsheet 23 is equal to N

So the public key is (55, 7) and the private key is 23

If we needed to unscramble the Cipher E back to j we would do the following:

$4^{23} \bmod 55 = 9$ and get the letter j

Decrypt your encrypted "I Love CS"

Now using $p = 3$, $q = 5$ and $e = 7$ find the following:

1. What is n?

2. What is the public encryption key? (n, e)

3. Encrypt "CS Rocks"

4. What is the decryption key?

5. Decrypt your original message? Are you correct?