Honors Discovery Seminar: Cryptography

Below is an algorithm to send coded messages. Use it to send encrypted messages to other people in the class and decrypt messages sent to you! We are going to use a limited alphabet to make the computations feasible, and each letter will be associated to a number using this table:

ALPHA NUMERIC CONVERSIONS

E	A	R	I	O	T	N	S	L	C
1	2	3	4	5	6	7	8	9	10

1. Choose two primes $p > 2$ and $q > 2$ of approximately equal size and compute $n = pq$. (Right now: don't pick things too large because you'll have to do computations with them. But, make sure n is greater than 10.)

   $p =$ _____

   $q =$ _____

   $n =$ _____

2. Compute $(p-1)(q-1)$. We will call this number $\phi(n)$.

   $\phi(n) =$ _____

3. Choose an integer e such that $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$, meaning e and $\phi(n)$ do not have any common factors. Also, find a positive integer d such that ed has a remainder of 1 when you divide by $\phi(n)$.

   Example: let's say $\phi(n) = 8$. Then, e needs to be a number between 1 and 8 without common factors with 8. For example, one choice is $e = 3$. Then, d will be some number we can multiply by e where the product has a remainder of 1 when we divide by 8. We can do this by guess-and-check or using a computer. To guess-and-check, let's just multiply: $2 \cdot 3 = 6$, which has remainder 6 when we divide by 8, so doesn't work. But, $3 \cdot 3 = 9$, which has a remainder of 1 when we divide by 8, so we can say $d = 3$.

   $e =$ _____

   $d =$ _____

4. Your **public key** is (n, e). Share this with people around you so your classmates can send messages to you.

public key $=$ _____

5. Your **private key** is (n, d). Don't tell this to anyone.

private key $=$ _____

6. Write a (short) message using the letters above. Convert each letter to a number.

message $=$ _____

numbers $=$ _____

7. Choose someone in the class to send your message to. Look up *their* public key. For each number m corresponding to a letter in your message, using *their* public key (n, e), compute the number m^e, and then find the remainder when m^e is divided by n. Call this number c. Do this for each number in your message. This new sequence of numbers is your coded message.

coded message $=$ _____

8. To decrypt a message sent to you, take each number c in the coded message sent to you, use **your** private key to compute the number c^d, and then find its remainder when you divide by n. Call this number l. This the decrypted number! Convert each number you get back to a letter and you have received the message sent to you.

decrypted numbers $=$ _____

decrypted message $=$ _____

9. Try again, as many times as you'd like! If you want, here are some implementation questions to think about:

   (a) How can we quickly find large prime numbers? How can we quickly determine if a random large number is prime?

   (b) How can we quickly find the number d?

   (c) Why is this a secure algorithm? What needs to be done for an outside observer to decrypt a message?