

Worksheet 9

Math 391, Abstract Algebra

Monday, October 19, 2020

1. Choose some prime numbers p and q such that $p - 1$ and $q - 1$ are not divisible by $e = 3$. Your p should have at least 3 digits, and your q should have at least 4 digits. You can find lists of primes online, for example at <https://primes.utm.edu/lists/small/>.
2. Let $k = (p - 1)(q - 1)$, and find a number d such that $de \equiv 1 \pmod{k}$.
3. Let $N = pq$. Your *private key* is the numbers N , d , and e , while your *public key* is just N and e . Share your public key with your colleagues.
4. Write a short secret message for your colleagues. Break it into blocks of 3 letters, and encode it using Shiffrin's code:

A = 01	B = 02	C = 03	D = 04	E = 05	F = 06	G = 07
H = 08	I = 09	J = 10	K = 11	L = 12	M = 13	N = 14
O = 15	P = 16	Q = 17	R = 18	S = 19	T = 20	U = 21
V = 22	W = 23	X = 24	Y = 25	Z = 26	period = 27	
					space = 00.	
5. Once one of your colleagues has given you their public key, take your message $m_1, m_2, \dots$ and encrypt it:

$$c_1 \equiv m_1^e \pmod{N}$$

$$c_2 \equiv m_2^e \pmod{N}$$

...

If you know how to use python, you can use the function `pow(m,e,N)`. Or you can search online for “power mod calculator.” This one is nice: http://home.sandiego.edu/~cparker/old_classes/math370_sp18/powermod.html

Be sure to use your colleague's public key, not your own. Send them $c_1, c_2, c_3, \dots$

6. Decrypt the messages your colleagues sent you, using your private key:

$$m_1 \equiv c_1^d \pmod{N}$$

$$m_2 \equiv c_2^d \pmod{N}$$

...

Then decode them using Shifrin's code. Did it work?

7. If you have time, start on the homework: Write a message you want to send me, encode it in blocks of nine letters using Shifrin's code, encrypt it using the public key $N = 340196134436655019$ and $e = 3$, and email it to me. Also send me your public key. I'll send back the plain text of your message, and an encrypted message for you.

Bonus points if my computer can't factor the number N in your public key in less than a minute. But no bonus points if I can google your number.