Homework

Encrypt the first three letters of your first name in uppercase letter

*Background information: pxq=n (11x17=187)
p, q - chosen prime numbers, the bigger the better, more secure
e - chosen prime number
m - message to encrypt in corresponding ASCII code
c - ciphered text (m^e mod n)

ASCII Table:

A	B	C	D	E	F	G	H	I	J	K	L	M
65	66	67	68	69	70	71	72	73	74	75	76	77
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
78	79	80	81	82	83	84	85	86	87	88	89	90

ENCRYPTION

Instructions	Example: H	First Letter: [M]	Second Letter: [A]	Third Letter: [R]	Fourth Letter: [I]	Fifth Letter: [S]	Sixth Letter: [A]
1. Find the corresponding ASCII code to your letter	72	77	65	82	73	83	65
2. Calculate m^e	$72^3 =$ **373248**	$77^3=456533$	$65^3 = 274625$	$82^3= 551368$	$73^3 = 389017$	$83^3 = 571787$	$65^3 = 274625$
3. Find c = m^e mod n	373248 mod 187 = **183**	456533 mod 187 = 66	274625 mod 187 = 109	552368 mod 187 = 92	389017 mod 187 = 57	571787 mod 187 = 128	274625 mod 187 = 109
4. Your ciphered letter (c value)	183	66	109	92	57	128	109

DECRYPTION

Instructions	Example: **183**	Ciphered letter: 77	Ciphered letter: 166	Ciphered letter: 137
1. Calculate m=c^d mod n	m = c^d mod n = 183^{107} mod 187 = **72**	77^{107} mod 187 = 66	166^{107} mod 187 = 89	137^{107} mod 187 = 69
2. Convert m to letter based on ASCII table	72 = **H**	66 = O	89 = Y	69 = E

Use https://www.wolframalpha.com/ to calculate modulo mathematics and huge exponents

Extension: Encrypt your full first name (add columns to the table above - right click on the table and choose "insert column right" option)

Use this code to check your work in the Homework above for Encryption ONLY:

```python
import math

message = input("Enter the letter to be encrypted: ")
ascii_code = ord(message)

p = 11 #private key
q = 17 #private key
e = 3  #public key

n = p*q #public key

#Encryption, c = m^e mod n
def encrypt(msg):
    m_power_e = math.pow(msg,e) #calculates m to the power of e
    c = m_power_e % n #find modulo to get the ciphered text
    print("Encrypted Message is: ", c)
    return c

print("ASCII Code is: ", ascii_code)
c = encrypt(ascii_code)
```

https://github.com/hunter-teacher-cert/work-topics-leungbenson/blob/master/public_key/RSA.md

ASYNC:

Find another type of encryption and give a brief summary of how it works. Post on Slack and comment on one other person's post.