Riley Campbell
CSC 372
Project 4

Non-code part

1. [20 points] Use the RSA algorithm. If p=13 and q=15, e=11 …
   a. [2 points] What is n?
      n = p * q = 13 * 15 = 195

   b. [2 points] What is $\varphi(n)$?
      $\varphi(n)$ = (p – 1) * (q – 1) = (13 – 1) * (15 – 1) = 12 * 14 = 168

   c. [2 points] Name an invalid e for this problem.
      2

   d. [6 points] What is d (you MUST show your work for credit)?
      d*e% $\varphi(n)$ = 1
      11d % 168 = 1
      168x + 11y = 1
      Step1: Euclidean algorithm
         168 = 15(11) + 3
         11 = 3(3) + 2
         3 = 1(2) + 1
      Step2: back substitution
         1 = 3 – 1(2)
         1 = 3 – 1(11 – (3) *3)
         1 = 4(3) – 1(11)
         1 = 4(168 – 15(11)) – 1(11)
         1 = 4(168) – 60(11) – 1(11)
         1 = 4(168) – 61(11)
         Take the -61
         d = 168 – 61 = 107
      step3: check
         d*e% $\varphi(n)$ = 1
         107 * 11 % 168 = 1
         1177 % 168 = 1
         True
         d = 107

e. [8 points] Use the above values to encode 5 with e (use the MOD-Exp function and show the values for each iteration). You should only the first 5 iterations rather than all e interactions.

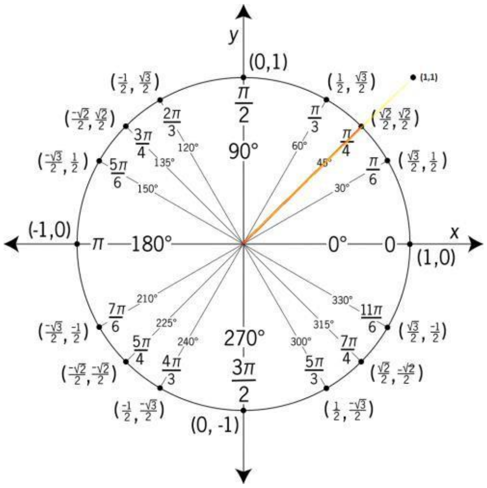
```
P(x) = x^e % n
MOD-EXP(a = 5, b = 11, n = 195) //a^b % n
        d = 1
        for 1 to b
                d = (d * a) mod n
        return d
```

Iteration	Value
1	(1 * 5) % 195 = 5
2	(5 * 5) % 195 = 25
3	(25 * 5) % 195 = 125
4	(125 * 5) % 195 = 40
5	(40 * 5) % 195 = 5

$P(5) = 5^{11} \% 195 = 125$

2. [50 points] Take the FFT n=4 quiz online. Closed book, closed note, but unlimited attempts while open. Your highest score will be kept. For ease of grading, the quiz scores to 100, and will be scaled to the weight of this problem. I capped the time to 30 minutes purely so that I can force a submit if needed. You would be surprised how often this is needed.

Finished 11/10/2020 with 100%



3. [30 points] Compute the DFT for n= 6 and $f(x) = 3x^5 + 4x^4 - 2x^3 - x^2 + 4$, for the 2nd power (w_6^2) Note the missing powers! It must be clear that this is the DFT (so a tree-like structure would be best). You **must** show your work for credit.
Your answers must be in a + bi format.

$$f(x) = 3x^5 + 4x^4 - 2x^3 - x^2 + 4$$

$$f(x) = 4 + 0x - x^2 - 2x^3 + 4x^4 + 3x^5 \qquad n = 6$$

$$\omega_n^{kj} = \frac{2\pi kj}{n}$$

Coefficients	**4**	**0**	**-1**	**-2**	**4**	**3**	
Powers ➔ **Roots🡇**	**0**	**1**	**2**	**3**	**4**	**5**	**totals**
0 $x_1 = \omega_6^0$	$\frac{2\pi * 0 * 0}{6}$ $= 0$ Angle: $4(1 + 0i)$ $= 4 + 0i$	$\frac{2\pi * 0 * 1}{6}$ $= 0$ Angle: $0(1 + 0i)$ $= 0 + 0i$	$\frac{2\pi * 0 * 2}{6}$ $= 0$ Angle: $-1(1 + 0i)$ $= -1 + 0i$	$\frac{2\pi * 0 * 3}{6}$ $= 0$ Angle: $-2(1 + 0i)$ $= -2 + 0i$	$\frac{2\pi * 0 * 4}{6}$ $= 0$ Angle: $4(1 + 0i)$ $= 4 + 0i$	$\frac{2\pi * 0 * 5}{6}$ $= 0$ Angle: $3(1 + 0i)$ $= 3 + 0i$	Angle: $8 + 0i$
1 $x_2 = \omega_6^1$	$\frac{2\pi * 1 * 0}{6}$ $= 0$ Angle: $4(1 + 0i)$ $= 4 + 0i$	$\frac{2\pi * 1 * 1}{6}$ $= \frac{\pi}{3}$ Angle: $0(\frac{1}{2} + \frac{\sqrt{3}}{2}i)$ $= 0 + 0i$	$\frac{2\pi * 1 * 2}{6}$ $= \frac{2\pi}{3}$ Angle: $-1(-\frac{1}{2} + \frac{\sqrt{3}}{2}i)$ $= \frac{1}{2} - \frac{\sqrt{3}}{2}i$	$\frac{2\pi * 1 * 3}{6}$ $= \pi$ Angle: $-2(-1+0i)$ $= 2+0i$	$\frac{2\pi * 1 * 4}{6}$ $= \frac{4\pi}{3}$ Angle: $4(-\frac{1}{2} - \frac{\sqrt{3}}{2}i)$ $=$ $-2 - 2\sqrt{3}i$	$\frac{2\pi * 1 * 5}{6}$ $= \frac{5\pi}{3}$ Angle: $3(\frac{1}{2} - \frac{\sqrt{3}}{2}i)$ $= \frac{3}{2} - \frac{3\sqrt{3}}{2}i$	Angle: $6 - 4\sqrt{3}i$
2 $x_3 = \omega_6^2$	$\frac{2\pi * 2 * 0}{6}$ $= 0$ Angle: $4(1 + 0i)$ $= 4 + 0i$	$\frac{2\pi * 2 * 1}{6}$ $= \frac{2\pi}{3}$ Angle: $0(-\frac{1}{2} + \frac{\sqrt{3}}{2}i)$ $= 0 + 0i$	$\frac{2\pi * 2 * 2}{6}$ $= \frac{4\pi}{3}$ Angle: $-1(-\frac{1}{2} - \frac{\sqrt{3}}{2}i)$ $= \frac{1}{2} + \frac{\sqrt{3}}{2}i$	$\frac{2\pi * 2 * 3}{6}$ $= 2\pi = 0$ Angle: $-2(1 + 0i)$ $= -2 + 0i$	$\frac{2\pi * 2 * 4}{6}$ $= \frac{8\pi}{3} = \frac{2\pi}{3}$ Angle: $4(-\frac{1}{2} + \frac{\sqrt{3}}{2}i)$ $=$ $-2 + 2\sqrt{3}i$	$\frac{2\pi * 2 * 5}{6}$ $= \frac{10\pi}{3} =$ $\frac{4\pi}{3}$ Angle: $3(-\frac{1}{2} - \frac{\sqrt{3}}{2}i)$ $=$ $-\frac{3}{2} - \frac{3\sqrt{3}}{2}i$	Angle: $-1+\sqrt{3}i$