Assignment 1

Jared Roesch (4826574)

Problem 1

I didn't finish this one.

Problem 2

```
  456
  555
  ------------------------------------
            | 2     | 2 + 0 | 5 + 3 | 0
            | 2     | 2     | 8     | 0
  ------------------------------------
    | 2     | 2 + 0 | 5 + 3 | 0     | 0
    | 2     | 2     | 8     | 0     | 0
  ------------------------------------
  2 | 2 + 0 | 5 + 3 | 0     | 0     | 0
  2 | 2     | 8     | 0     | 0     | 0
  ------------------------------------
  2 | 4 + 1 | 2 + 1 | 0     | 8     | 0

  256 * 555 = 253080
```

Problem 3

```
                      | 4      | 5           | 6
*                     | 4      | 5           | 6
-----------------------------------------------
0 |         |         | 2 * 24 | 2 * 30      | 36
0 |         | 2 * 20  | 25     | 0           | 0
0 | 16      | 0       | 0      | 0           | 0
0 | 16 + 4  | 40 + 7  | 73 + 6 | 60 + 3      | 6
2 | 0       | 7       | 9      | 3           | 6
-----------------------------------------------
= 207936
```

Problem 4

Assume $r = 32$, $n = 21$, $a = 13$, $b = 15$

$$\begin{aligned}
\bar{a} &= 13 * 32 \ (mod\ 21) \\
\bar{a} &= 17 \\
\bar{b} &= 15 * 32 \ (mod\ 21) \\
\bar{b} &= 18 \\
r * r^{-}1 &= 1(modm) \\
32 * r^{-}1 &= 1(mod21) \\
r^{-}1 &= 2
\end{aligned}$$

$$\begin{aligned}
n' &= (1 - r * r^{-}1)/ - n \\
n' &= 3
\end{aligned}$$

Compute:

$c = \bar{a} * \bar{b} * r^{-}1 \ (mod\ n)$

Using the algorithm described:

$$\begin{aligned}
t &= \bar{a} * \bar{b} \\
t &= 17 * 18 \\
t &= 306 \\
m &= t * n'(mod\ r) \\
m &= 306 * 3(mod\ 32) \\
m &= 22 \\
u &= (t + m * n)/r \\
u &= (306 + 22 * 21)/32 \\
u &= 24
\end{aligned}$$

Then: $u - n = 3$

Problem 5

$p = 29, a = 23, g = 10$

Compute $g^a(mod\ p)$:

Didn't finish

Problem 6

$\{p, q, n, e, d\} = \{17, 23, 391, 29, 85\}$

Didn't finish