PROOFS: HOMEWORK 5

ANDREW TSENG: ART2589

Problem 3.5

Part A
If p and q are distinct primes, then $\phi(pq) = \phi(q) * \phi(p)$.
Part B
If p is prime, then $\phi(p^2) = p * \phi(p)$.
We will prove that:
If p is prime, then $\phi(p^j) = p^{j-1} * \phi(p)$.

Proof:
We know that if p is prime, then $\phi(p^2) = p * \phi(p)$ and $\phi(p^4) = p^2 * p * \phi(p) = p^3 * \phi(p)$ Factoring out the values that have a factor of p in the range of 1 to $p^j - 1$. Since $\phi(p)$ are all the values that are relative prime up to p, then every p intervals will have $\phi(p)$ values thus $\phi(p^j) = p^{j-1} * \phi(p)$.

Part C
Since $\gcd(M, N) = 1$, then M, N are distinct primes, then it is proven from part a that $\phi(MN) = \phi(M)\phi(N)$.

Part D

Part E
$\phi(1728) = 576$ $\phi(1575) = 720$ $\phi(889056) = 254016$

Problem 3.8

Since Bob chose an N that is too small. Eve can iterate and test all values to find p. This allows Eve to find p and q very easily. Since we know that $ed \equiv 1 \mod (p-1)(q-1)$, then finding d by iterating through values will be considered "easy" for Eve. Program used to solve this is in eve.py Using the program, we conclude that $d = 11629$.

Problem 3.10

Part A
We know that if N is large that the $\gcd(k_1(p-1)(q-1), k_2(p-1)(q-1)) = (p-1)(q-1)$ where $k_1, k_2 \in Z$. Because we can find a specific pair of d, e, we can get the k(p-1)(q-1) by $de-1$. Finding $(p-1)(q-1)$ allows us to find $p+q$ which makes it easy to find a factor of N as we know the bounds of it in this case. In other words, you can test from values from 3 to $q+p$.

Part B
$p = 5347$, $q = 7247$
Part C
$p = 10867$, $q = 20707$
Part D
$p = 13291$, $q = 97151$

Problem 3.11

Since p and q are relatively prime, we know that

Problem 3.13

Found that the gcd of e_1, e_2 is 1. Thus:

$$m \equiv (c_1 * c_2) \mod N$$

$m = 13917916680$