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 $\phi(p^2) = p - 1$.
We will prove that:
If p is prime, then $\phi(p^j) = p^j - p^{j-1}$.
Let m be a number that is less than p^k, the only way $\gcd(m, p^k) > 1$ if m is a multiple of p. Through since there are a number of p^{j-1} multiples in a range of 1 to p^j. Thus the number of m that have suffice with the requirements of the phi function is $p^j - p^{j-1}$.

Formula was analyzed from running many results from phi.py

Part C
Since $\gcd(M, N) = 1$, then M, N are distinct primes, which proves from part A that $\phi(MN) = \phi(M)\phi(N)$.

Part D Proof:

We will prove that $\phi(N) = N \prod_{i=1}^{r}(1 - \frac{1}{p_i})$ such that $p_1, p_2, \dots, p_r$ are the distinct prime factors of N.

$$\phi(N) = \phi((p_1)^{k_1})\phi((p_2)^{k_2}) \dots \phi((p_r)^{k_r}))$$

Using the formula from part b:

$$\phi(N) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1}) \dots (p_r^{k_r} - p_r^{k_r-1})$$

$$\phi(N) = p_1^{k_1}(1 - \frac{1}{p_1})p_2^{k_2}(1 - \frac{1}{p_2}) \dots p_r^{k_r}(1 - \frac{1}{p_r})$$

$$\phi(N) = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}(1 - \frac{1}{p_1}) \dots (1 - \frac{1}{p_r}) = N(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_r})$$

Thus:

$$\phi(N) = N \prod_{i=1}^{r}(1 - \frac{1}{p_i})$$

Part E
$\phi(1728) = 576$ $\phi(1575) = 720$ $\phi(889056) = 254016$
Solutions done from formula in part D and checked with the program phi.py

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

Part A We know that g, r, s are modulo N
Part B

Problem 3.13

We found $\gcd(e_1, e_2)$ is 1. The equation $e_1 u + e_2 v = 1$ from section 3.5 indicate the following:

$$c_1 * c_2 = m^{\gcd(e_1, e_2)} = m$$
$$m \equiv (c_1 * c_2) \mod N$$

Using the numbers given: $m = 13917916680$