CIS 3362 Final Exam - Part C (Number Theory, Public Key Crypto) - 25 pts

Date: 12/9/2020
Start Time: 11:20 am EST
End Time: 12:05 pm EST

You may use your class notes, reference sheets and calculator. Please still show each step but just put answers of calculations you made in your calculator.

Note: Please put your name in the document you turn in.

1) (5 pts) What is $\varphi(2520)$?

2) (5 pts) What is the remainder when 54^{12099} is divided by 1073? (Note: please use a calculator to prime factorize 1073 and just show your end result of its factorization.)

3) (5 pts) A generator, g, of a prime p is a number such that the set $\{g^1 \bmod p, g^2 \bmod p, \ldots, g^{p-1} \bmod p\}$ contains each of the integers from 1 to p-1 precisely once. We will call a half-generator, g, of a prime number p a number such that the set $\{g^1 \bmod p, g^2 \bmod p, \ldots, g^{p-1} \bmod p\}$ contains half of the integers from 1 to p-1 precisely twice. How many half generators are there for a prime p? Please give your answer in terms of the Euler phi function and p with a rationale for your answer. (Note: This one is challenging, but the answer can be derived from the reasoning behind counting the number of generators of a prime p, using a particular generator, g.)

4) (10 pts) In an RSA system, n = 259 and e = 77. What is the value of d?