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

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

Solution

$\varphi(2520) = \varphi(2^3 \times 3^2 \times 5 \times 7) = \varphi(2^3)\varphi(3^2)\varphi(5)\varphi(7) = (2^3 - 2^2)(3^2 - 3^1)(5 - 1)(7 - 1) =$ **576.**

Grading: 2 pts for prime factorization, 2 pts total for individual phi terms, 1 pt to multiply together

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.)

Solution

1073 = 29 x 37, via trial division (I tried 2, 3, 5, 7, 11, 13, 17, 19, 23 which all failed before 29 worked)

$\varphi(1073) = \varphi(29)\varphi(37) = 28 \times 36 = 1008.$

Since gcd(54, 1073) = 1, it follows that $54^{1008} \equiv 1 \pmod{1073}$ via Euler's Theorem.

Now, we have:

$54^{12099} = 54^{1008 \times 12 + 3} = (54^{1008})^{12}54^3 \equiv 1^{12}54^3 \equiv 54^3 \equiv 157464 \equiv$ **806 mod 1073.**

Thus, the desired remainder is **806.**

Grading: 1 pt for prime fact, 1 pt for phi, 1 pt for exponent breakdown, 1 pt to get to 54^3, 1 pt to reduce to 806

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.)

Solution

Let g be some generator. Then we know that g^x is a generator if and only if gcd(x, p-1) = 1, since only when this condition holds is it the case that $g^x, g^{2x}, g^{3x}, \ldots, g^{(p-1)x}$ are all distinct mod p because each of the exponents themselves are inequivalent mod p-1, where the last value on the list is equivalent to 1 mod p, and the exponent, is of course equivalent to 0 mod (p-1).

If we want HALF of this list to be unique, then we would want the number halfway through the list to be 1, so we would want $g^{\left(\frac{p-1}{2}\right)x} \equiv 1 \ (mod\ p)$, which would mean that $(p-1)|[\frac{x(p-1)}{2}]$, and that we would want this to be the SMALLEST value of x for which this is true. (The end of this is critical, because we over count without keeping this in mind.) Thus, we need x to be divisible by 2, but then the rest of x can NOT share any common factors with p-1. Another way of saying this is that the gcd(x, p-1) = 2. But if x and p-1 share a common factor of 2, why not just divide that out of both and now we find that gcd(x, (p-1)/2) = 1 and x ranges from 1 to (p-1)/2. So we want to know the number of integers x in the given range that satisfy the gcd requirement. But, this is precisely the definition of the phi function, so it turns out that the answer to the question is $\boldsymbol{\phi(\frac{p-1}{2})}$**.**

Grading: This is hard to grade because it's reasonably difficult to make good progress without solving it. So, partial credit will be sparingly given. It's definitely the hardest question on the whole exam. Feel free to give partial credit if you think someone has made some good observations. Here is a guide for some items to offer credit for:

Explaining how we count generators given one generator - 2 points
Stating the idea that we want the loop to stop halfway through the whole cycle - 1 pt
Figuring out the relationship between gcd of p-1 and x that makes it possible for the loop to stop halfway through - 1 pt
Making the final realization to use the phi function to describe the answer - 1 pt

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

Solution

First, we need to prime factorize n. Use trial division to find: $259 = 7 \times 37$

Thus, $\varphi(259) = \varphi(7)\varphi(37) = (7 - 1)(37 - 1) = 6 \times 36 = 216$.

Thus $d \equiv 77^{-1} \bmod 216$.

Run the Extended Euclidean Algorithm:

$216 = 2 \times 77 + 62$
$77 = 1 \times 62 + 15$
$62 = 4 \times 15 + 2$
$15 = 7 \times 2 + 1$

$15 - 7 \times 2 = 1$
$15 - 7(62 - 4 \times 15) = 1$
$15 - 7 \times 52 + 28 \times 25 = 1$
$29 \times 15 - 7 \times 52 = 1$
$29(77 - 62) - 7 \times 52 = 1$
$29 \times 77 - 29 \times 52 = 7 \times 52 = 1$
$29 \times 77 - 36 \times 52 = 1$
$29 \times 77 - 36(216 - 2 \times 77) = 1$
$29 \times 77 - 36 \times 216 + 72 \times 77 = 1$
$101 \times 77 - 36 \times 216 = 1$

Taking this equation mod 216, we find

$101 \times 77 \equiv 1 \pmod{216}$

It follows that **d = 101.**

Grading: 2 pts for prime factorization of n (without it just give 0 out of 10)
1 pt for phi calculation
2 pts for Euclidean Algorithm
4 pts for Extended Euclidean Algorithm
1 pt to extract answer