Coding Theory and Cryptography: HW 5

Paridhi Latawa

April 2021

Abstract

This assignment covers number theory, public key cryptosystems, and RSA. 1. Module: Public Key Cryptography and the RSA Cryptosystem, pages 7 - end. Problems: 6, 8, 10, 11, 12, 14, 15, 16, 17, 18, 19 2. Trappe and Washington: 3.1 - 3.6, 6.1 Problems: Pages 104-5 - 4, 8, 9, 12, 13, 14, 16. Pages 192 - 3: 1, 2, 3, 4, 5, 6, 7, 8 3. Hankerson: Section 12.2 4. Video: Public Key Cryptography - Diffie-Hellman Key Exchange

1 Public Key Cryptography and the RSA Cryptosystem

Problem 6: Suppose $a|x$ and $a|y$. Show that $a|(x * n + y * m)$ for any integers n and m.

$x = k_1 a, k_1 \in$ set of integers

$y = k_2 a, k_2 \in$ set of integers

$nx = n * k_1 a$ $my = m * k_2 a$ $(nx + my) = nk_1 a + mk_2 a = (k_3 + k_4)a$ $(nx + my) = k_5 a$

So, $a|(nx + my)$

Problem 8: Show that if $a|bc$ and (a, b) = 1, then a—c

(use the fact that 1 can be written as a linear combination of a and b)

Use the theorem ax + by = gcd(a, b)

gcd(a, b) = 1

So

$k_1 a + k_2 b = 1$

Multiplying both sides by C

$k_1ac + k_2bc = c$

Since a divides bc (given), $a|bc$ and a divides k, ac and $a|k_2bc$, so $k|c$

Problem 10: Show that a zero divisor in Z_n does not have a multiplicative inverse

$a * b = 0$, a and b are zero divisors

Assume $(a * b)^{-1}$ exists

$(a * b)^{-1} * (ab) = 0$, since $a * b = 0$

Which is a contradiction since if multiplicative inverse exists, then $(a*b)^{-1}*(ab) = 1$, but here it's 0

So,

$(ab)^{-1}$ does not exist

Problem 11: Find $\phi(11)$. What is $\phi(p)$ for a prime number p?

$\phi(11) = 10$ as we can have 1, 2, 3, 4, 5, 6, 7, 8, 9, 10.

$\phi(p) = p - 1$

Problem 12:

Order of:

$4 = 3$

$5 = 6$

$7 = 3$

$8 = 2$

Others are

1, 2, 4, 5, 7, 8

Problem 14: Prove part a of the above theorem.

For a prime p, and a positive integer r, $\phi(p^r) = p^r - p^{r-1} = p^{r-1}(p - 1)$

The gcd(q, p^r)can by multiples of p - either$p^0, p^1, p2, ..., p^r$

If gcd(q, p^r) doesn't equal 1, then q is a multiple of p

All the multiples of p are less than or equal to the multiples of p^r - 1p, 2p, 3p, ..., $p^{r-1}p$, which means total p^{r-1} multiples

The total multiples are p^r

So the other multiples with gcd = 1 are $p^r - p^{r-1}$

So, $\phi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1)$

Question 18:

Deciphertext - [785370257809172143083511086611 57,619234988813872054440483 5244]

2 Trappe and Washington: 3.1 - 3.6, 6.1

Pages 104-5: Problem 4: a) Use the Euclidean algorithm to compute gcd(30030, 257) The Euclidean algorithm consists of a series of division that can be written in the following forms: $a = q_1 b + r_1$ and the numbers are shifted such that the order is remainder, divisor, divided, ignore. 30030 = 116 * 257 + 218

257 = 1 * 218 + 39

218 = 5 * 39 + 23

39 = 1 * 23 + 16

23 = 1 * 16 + 7

16 = 2 * 7 + 2

7 = 3 * 2 + 1

2 = 2 * 1 + 0

So gcd(30030, 257) = 1

b) Using the result of part a and the fact that $30030 = 2 * 3 * 5 * 7 * 11 * 13$, show that 257 is prime.

257 would have to be divisible by prime numbers less than 16 approximately for it to not be prime. These values are what are the factors of 30030. The greatest common denominator of 30030 and 257 (as shown in part a) is 1 though, so 257 has to be prime.

Problem 8: Let p $\geq$ 3 be prime. Show that the only solution to $x^2 \equiv 1$ (mod p) are $x \equiv +/-1$ (mod p).

Given the hint, we are told to apply exercise 7a to $(x+1)(x-1)$, so we can rewrite this statement as (x + 1) (x - 1) = 0 (mod p).

This can be written as

(x + 1) = 0 (mod p)

(x - 1) = 0 (mod p)

Simplifying these equations, we get x = - 1 or x = 1, which proves the statement.

Problem 9: Suppose $x \equiv 2 \pmod 7$ and $x \equiv 3 \pmod{10}$. What is x congruent to mod 70?

We basically have to find values of x (multiples) that can fit both the congruences given.

The properties of the desired values are that when multipled by 7, the ones digit should have a value of 1, such that when 2 is added to the value (satisfying the first congruency), it will have a ones digit value of 3 (satisfying the second congruency).

Possible values that x can be congruent to mod 70 include 23, 163, 233, 303.

Problem 12: Divide 2^{10203} by 101. What is the remainder?

Basically this question is asking what we get when computing $2^{10203} \pmod{101}$

It should be noted that 101 is a prime number.

From Fermat's theorem, we know that $2^100 \equiv 1 \pmod{101}$

So, we can write

$2^{10203} \equiv (2^{100})^{102}(2^3) \equiv 1^102(2^3) \equiv 8 \pmod{101}$

Problem 13: Find the last 2 digits of 123^{562}

The last two digits can be found by taking mod 100.

Problem 14: a) Evaluate $7^7 \pmod 4$

b) Use part a to find the last digit of 7^{77}, noting that $a^{bc} = a^(b^c)$.

Fining the last digit is mod 10.

This can be written in the equation form of $7^7 = 3 + 4k$.

Euler's theorem tells us that $\phi(10) = 4$

So the above function can be broken into

$7^{77} = (7^4)^k(7^3) = 1^k * 7^3 = 343 = 3 \pmod{10}$

Problem 16:

a) Let p = 7, 13, or 19. Show that $a^{1728} \equiv 1 \pmod p$ for all a with pa.

$a^p - 1 \equiv 1 \pmod p$ if p is not divisible by a.

We can input the values of p given into the above equation

$a^{7-1} \equiv 1(\text{mod } 7)$

$a^6 \equiv 1 \text{ (mod } 7)$

$a^{1728} = (a^6)^{288}$

$1^{188} = 1 \text{ (mod } 7)$

$a^{13-1} \equiv 1(\text{mod } 13)$

$a^{12} \equiv 1(\text{mod } 13)$

$a^{1728} = a^{12144} = 1^{144}(\text{mod } 13)$

$a^{19-1} \equiv 1(\text{mod } 19)$

$a^{18} \equiv 1(\text{mod } 19)$

$a^{1728} = (a^{18})^{96} = 1^{96} = 1(\text{mod } 19)$

b)

p = 7

$a^{1729} = a^{1728} * a$

$a^{1728} = 1 \text{ (mod p)}$

a mod p = a

Pages 192 - 3: 1. The ciphertext 5859 was obtained from the RSA algorithm using n = 11413 and e = 7467. Using the factorization 11413 = 101 * 113, find the plaintext.

$\phi(n) = (p-1)(q-1) = (101-1)(113-1) = (100)(112) = 11200$

From section 6.5, we can get that 7467^{-1} mod 11200 = 3.

We can then take

$5859^3 = 1415 \text{ (mod } 11413)$ as we are taking mod n

So, the plaintext is the word 1415