Test 2

CIS 306  
John P. Baugh, Ph.D.  
Winter 2021

**Total: \_\_\_\_\_\_\_\_\_\_\_\_ / 150**

**Printed Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**GRADER/TA: *[No CO Data]***

I, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, have neither given nor received assistance on this examination except that which is provided by, or approved by, the instructor.

1. [15 pts] Bob wants to send a secret message to Alice using RSA. Alice’s public key is PUA = {e, n} = {11, 15}  
   Bob wants to send the message M = 4  
   Show your calculations, and the resultant ciphertext, C

1. [15 pts] Alice receives the ciphertext, C, from Bob (resulting from question 1 above.) She wants to decrypt the message, M, using the ciphertext, and her private key PRA = {d, n} = {3, 15}  
   Show the calculations for decryption, and the result.
2. [15 pts] Solve the following modular arithmetic questions, using the integer representation discussed in class, namely, x = cq + r (find the remainder, r. Hint: r should *always* be non-negative)
   1. -14 mod 3
   2. 21 mod 4

* 1. -42 mod 4

1. [15 pts] Determine whether the following congruences hold using the modular difference/division property [Hint: (a-b)/c is an integer?]
   1. Is 11 7 mod 4?
   2. Is -5 5 mod 3?
   3. Is 14 4 mod 3?
2. [20 pts] Use Euclid’s algorithm the find the following greatest common divisors (GCDs)
   1. GCD(20, 55)

* 1. GCD(14, 28)

1. [20 pts] The following are **clear equilibrium strategies** for you and your opponent. Find the pairs of choices (yours, opponents), e.g., (a, x), (b, y), etc. (you don’t need mini-max solution for this – the choice should be obvious given your goals and your opponents’ goals, and that you are both rational.)

|  |  |  |  |
| --- | --- | --- | --- |
|  | Opponent | | |
| You |  | x | y |
| a | 2 | 4 |
| b | 6 | 8 |

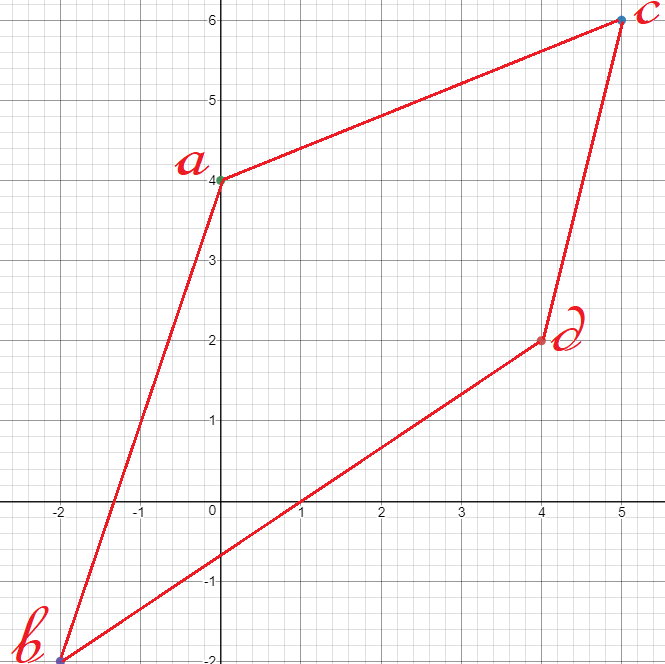
|  |  |  |  |
| --- | --- | --- | --- |
|  | Opponent | | |
| You |  | x | y |
| a | 12 | 10 |
| b | 9 | 8 |



1. [15 pts] Consider the line segments connecting points p1 and p2 in each of the following scenarios. Find a vector = (x, y) that represents these line segments.
   1. p1 = (2, 2) and p2 = (3, 6)
   2. p1 = (-4, 2) and p2 = (4, 15)
   3. p1 = (5, 4) and p2 = (6, 6)
2. [15 pts] Given your solutions in question (7) above, find the **magnitudes** of each of the vectors.
   1. =
   2. =
   3. =
3. [10 pts] Find the distances from a point to a line, given the following information
   1. You are given a point (3, 3) **not** on the line, and two points (1, 2) and (12, 20) through which the line passes

* 1. You are given a point (6, 4) **not** on the line, and a line y = 2x + 4

1. [10 pts] Given the following polygon, use the Surveyor’s Formula to find its area



The ordered pairs of vertices, in counter-clockwise order are thus (a, b, d, c)

**a = (0, 4) b = (-2, -2) d = (4,2) c = (5,6)**