Fall 2020 CIS 3362 Quiz #5 Part B: El-Gamal, ECC

Date: 11/13/2020

Directions: Please use your course notes and a calculator as aids for this exam. Do NOT attempt to look up information online. Even if you use a calculator, show each step of your calculations that you would do by hand. The role of the calculator will simply be to speed up individual calculations (13 x 29, for example), not to skip whole steps, as these steps are typically awarded points in the grading criteria.

Please either type your answers. The accepted file types for submission will be .doc, .docx, .txt and .pdf. I recommend that you directly type into the posted document to save time.

Please look at Webcourses to see when your due time and late due time are. It's recommended that you stop working at the due time and start uploading at that time. Anything turned in before the late due time will be accepted for full credit. Anything that doesn't make it in by the late due time will earn a 0. A 10 minute buffer will be provided after both due times. Please don't take advantage of these buffers as it's an unnecessary risk.

1) (12 pts) You have received the ciphertext (6, 10), which was encrypted using the public key system, El Gamal. Your secret key, $X_A = 19$ and the prime number modulus is $q = 31$. Decrypt the ciphertext and clearly mark the correct plaintext. **Please show your work for modular exponentiation by hand. You may plug in individual multiplications and mods in the calculator, but show each step you would normally show, by hand.**

2) (12 pts) Consider the Elliptic Curve $E_{29}(3, 8)$. (The prime number is 29, a = 3 and b = 8.) Two points on this curve are P = (8, 14) and Q = (21, 9). What is P + Q?

3) (1 pt) Hurricane Eta is named after which Greek letter?