Fall 2020 CIS 3362 Quiz #5 Part A: Diffie-Hellman, RSA

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) (5 pts) Consider the situation where Alice and Bob attempt the Diffie-Hellman Key Exchange, but their modulus value, p, is NOT a prime number, and a (the base) is not a generator of p. If they perform the protocol as otherwise specified, are they guaranteed to calculate a shared key?

2) (8 pts) Bob is using $p = 23$ as his prime number and $a = 5$ for the Diffie-Hellman Key Exchange. Talia would like to use a different generator mod 23. Unfortunately, Talia is lazy and wants to do the least amount of arithmetic (multiplication and modding) possible, and she knows an efficient way to calculate a different generator mod 23, given that 5 is a generator mod 23. Determine the generator (**by hand**) that Talia is going to calculate.

3) (12 pts) In an RSA system n = 713 and e = 119. What is d? (In order to get credit, please do the following: you may use a calculator to factor any numbers necessary, but you **must show** each step of the Extended Euclidean Algorithm to earn full credit. You may plug into the calculator for the EEA, but you must write down/type out each step as shown in class. If you would like, you can gather terms quickly, to reduce the amount of writing.)