Fall 2020 CIS 3362 Quiz #2 Part A: Playfair, ADFGVX

Date: 9/25/2020

Directions: Please use the reference sheet, 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 or write them on paper and scan that to .pdf. 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 scanning, and either use the equation editor or type out the necessary math in text.

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) (8 pts) Show the playfair box created with the keyword, "BLOODORANGELEMONADE".

2) (9 pts) Using your playfair box from question #1, encrypt the following plaintext: "TAKINGAPHONECALL". Please us the padding character 'Z', if necessary.

3) (8 pts) Consider a plaintext message of 91 symbols (letters/digits) encrypted with the ADFGVX cipher and the keyword "HARRYPOTTER". The ciphertext has 182 symbols. The plaintext symbol in the **zero-index based** position of 19 is represented in the ciphertext with two letters (A, D, F, G, V, or X, not necessarily distinct). What are the index positions of those two letters in the **ciphertext**? **Please give your answers as two distinct integers in between 0 and 181, inclusive.** Note: most of the credit for this question will be based on your work and not the actual answers.