Fall 2020 CIS 3362 Quiz #1 Part B: Hill, Enigma, Transposition, Navajo Code

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) (10 pts) In the cryptanalysis of Hill cipher, you've determined that two values of the key matrix satisfy the following equations:

$$19a + 4b \equiv 13 \pmod{26}$$
$$18a + 19b \equiv 14 \pmod{26}$$

Determine the values of a and b. Please express both as integers in between 0 and 25, inclusive.

2) (6 pts) Consider an Enigma for an alternative language with 10 symbols in its alphabet and four slots for rotors instead of three. Also, imagine that to fill the slots for the rotors, there were a total of 6 potential rotors to be placed. Assume that similar look up charts could be constructed (to the ones that Rejewski had constructed), one for each possible rotor placement and rotation of each of the rotors. How many different charts would need to be calculated?

3) (8 pts) The following ciphertext has been encrypted via column transposition, using the keyword "TENNESSEE". What is the decrypted plaintext?

```
EFCEV DMGEM VENTD RENDE IIALO HMOIL RMELL EEABE AATNE MRTIA RNN
```

4) (1 pt) Which company created Google Maps?