Fall 2020 CIS 3362 Quiz #1 Part B: Vigenere, IC, MIC

Date: 9/9/2020

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) The ciphertext "QZAPMACTJA" was encrypted using the Vigenere cipher with the keyword "LIGHT". What is the corresponding plaintext?

2) (10 pts) Consider a set of letters with 1 A, 2 Bs, 3 Cs, 4 Ds, …, and 26 Zs. (Explicitly, the character with Ascii value 'A'+i appears i+1 times.) What is the index of coincidence of this set of letters? (Hint: The sum of the first n integers is $\frac{n(n+1)}{2}$, and the sum 1 x 2 + 2 x 3 + 3 x 4 + … (n-1) x n = $\frac{(n-1)n(n+1)}{3}$.) Express your answer as a fraction in lowest terms.

3) (5 pts) The following code represents an encryption function for a cipher that is a slight modification to the Vigenere cipher. Assume that both strings plain and key store uppercase letters only. Explain, in English, the method of encryption, given the plaintext and key. Does this extra twist provide any extra security?

```
void printCipher(char* plain, char* key) {

  int keyLen = strlen(key);
  int msgLen = strlen(plain);

  for (int i=0; i<msgLen; i++)
    printf("%c", (plain[i]-'A'+key[i%keyLen]-'A'+i)%26 + 'A');
  printf("\n");
}
```