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

Date: 9/9/2020

1) (10 pts) The ciphertext "QZAPMACTJA" was encrypted using the Vigenere cipher with the keyword "LIGHT". What is the corresponding plaintext?

Solution
Q - L = 16 - 11 = 5 (F)
Z - I = 25 - 8 = 17 (R)
A - G = 0 - 6 = -6 = 20 mod 26 (U)
P - H = 15 - 7 = 8 (I)
M - T = 12 - 19 = -7 = 19 mod 26 (T)
A - L = 0 - 11 = -11 = 15 mod 26 (P)
C - I = 2 - 8 = -6 = 20 mod 26 (U)
T - G = 19 - 6 = 13 (N)
J - H = 9 - 7 = 2 (C)
A - T = 0 - 19 = -19 = 7 mod 26 (H)

Plaintext is **FRUITPUNCH.** **Grading: 1 pt per letter.**

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.

Solution
There are a total of $\frac{26\times27}{2} = 13 \times 27 = 351$ letters. The corresponding index of coincidence is as follows:

$$\frac{1 \times 2 + 2 \times 3 + 3 \times 4 + 4 \times 5 + \cdots + 25 \times 26}{351 \times 350}$$

The numerator is the pattern given in the hint with n = 26, so we can simplify that expression as follows:

$$\frac{\frac{25 \times 26 \times 27}{3}}{13 \times 27 \times 350} = \frac{25 \times 26 \times 27}{3 \times 13 \times 27 \times 350} = \frac{25 \times 2}{3 \times 350} = \frac{50}{3 \times 7 \times 50} = \mathbf{\frac{1}{21}}$$

Grading: 2 pts to calculate that there are 351 letters total, 1 pt for the denominator, 2 pts for the long hand written numerator, 3 pts for using the numerator formula correctly, 2 pts for reducing the fraction

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");
}
```

Solution

Instead of just adding the appropriate keyword letter to the plaintext letter, the index of the letter (position in the text) is added to the letter as well before modding. This does not add any extra security because if someone knew the system, they could just automatically subtract the value of i from the i^{th} character of the ciphertext and then they would be left with breaking a regular Vigenere cipher.

Grading: 3 pts for mentioning that the position number of the letter is added as well, 2 pts for describing why this isn't significant.