EL-764 Cryptography **Problem Set 1** Due Date: **Sep 30th, 2019**

Q.1: In this question suppose you have a language with only the 3 letters *a*, *b*, c, and they occur with frequencies 0.7, 0.2, 0.1, respectively. The following ciphertext was encrypted by the Vigenere method

ABGBABBBBAC.

Determine the key length.

Q.2: Suppose that you want to encrypt a message using an affine cipher. You let $a = 0$, $b = 1, \ldots, z = 25$, but you also include ? = 26, ; = 27, " = 28, ! = 29. Therefore, you use $x \longrightarrow \alpha x + \beta \pmod{30}$ for your encryption function, for some integers a and /3.

(a) Show that there are exactly eight possible choices for the integer α (that is, there are only eight choices of α (with $0 < \alpha < 30$) that allow you to decrypt).

(b) Suppose you try to use $\alpha = 10$, $\beta = 0$. Find two plaintext letters that encrypt to the same ciphertext letter.

Q.3: Suppose we work mod 27 instead of mod 26 for affine ciphers. How many keys are possible? What if we work mod 29?

Q.4: Suppose you encrypt using an affine cipher, then encrypt the encryption using another affine cipher (both are working mod 26). Is there any advantage to doing this, rather than using a single affine cipher? Why or why not?