Number Theory
Spring 2014

Assignment 7.1
Due March 6

Exercise 1. The ciphertext `IWXHHIPITBTCIXHUPAHT` was encrypted using a shift cipher with a single letter encryption key. Use brute force (i.e. try every possibility) to determine the key and the plaintext. [*Suggestion:* Use a computer. Maple's `StringTools` package includes a number of functions that are well suited to this task.]

Exercise 2. Let $\alpha : \{\mathtt{A}, \mathtt{B}, \mathtt{C}, \mathtt{D}, \ldots\} \to \mathbb{Z}_{26}$ denote the function $\mathtt{A} \mapsto 0$, $\mathtt{B} \mapsto 1$, $\mathtt{C} \mapsto 2$, etc., and let β denote the associated bijection of the set all digraphs (two letter strings) with $\mathbb{Z}_{26^2}$:

$$L_1L_2 \mapsto \alpha(L_1) + \alpha(L_2) \cdot 26.$$

So, for example, $\beta(\mathtt{AA}) = 0$, $\beta(\mathtt{HI}) = 215$ and $\beta(\mathtt{MU}) = 532$.

The following cipher text was obtained using an affine transformation on the set of all digraphs, encoded numerically using β:

```
OZACWLXMUUMIOWAKVBUZLTXZXMEVOWOUVPHJLTKMDZVBOUILSMVBGECJ
HJOIDVEVVUOWKKWQBPHZNRJRXYKTWIOBKOKYSMVBOTVIXHOYLGAVBIOK
AVVACTTMLLQLKJVELTQYWKZBGZKOKKKZVIBIWLKBLSOTVXQUIJPCLEAY
KZAJBDWAVBKMDDMPSNKKKTBDSUWLXGKTWWVPHNVOZEBSHJTMXUKTJRUZ
LLKNJMHJOKQKCHDIOADZQZAEAYAVWLHNVCOSHJXIVBUZLTXMJXBGGEGY
KHDJDDVAACWQNXMZXWZBAKAVBIGYSUWEBIBHNVDPUUWQVBOSNRJXRQBF
   ACGYWBKMVBWSQKGLHUBXVBGEINHNVETMXSLPWCKKBHLEHJXWGE
```

A frequency count shows that the most common digraph occurring in this ciphertext is `VB`, and the second most common is `HJ`. In English, however, the most frequently occurring digraph is `TH`, followed by `HE`.

a. Determine the two possible encryption keys.

b. Determine the decryption keys corresponding to each of the encryption keys found in part **a**.

c. Decrypt the ciphertext. [*Suggestion:* Use a computer to try both decryption keys. Again, you might find Maple to be extremely helpful.]