Number Theory
Problem Set 4
Simple Cryptosystems

1. In the 27-letter alphabet (with blank=26), use the affine enciphering transformation with key $a = 13$, $b = 9$ to encipher the message "HELP ME."

2. In a long string of ciphertext which was encrypted by means of an affine map on single-letter message units in the 26-letter alphabet, you observe that the most frequently occurring letters are "Y" and "V", in that order. Assuming that those ciphertext message units are the encryption of "E" and "T", respectively, read the message "QAOOYQQEVHEQV".

3. You are trying to cryptanalyze an affine enciphering transformation of single-letter message units in a 37-letter alphabet. This alphabet includes the numerals 0-9, which are labeled by themselves. The letters A-Z have numerical equivalents 10-35, respectively, and blank=36. You intercept the ciphertext "OH7F86BB46R3627O266BB9" (here the O's are the letter "oh"). You know that the plaintext ends with the signature "007" (zero zero seven). What is the message?

4. You intercepted the ciphertext "OFJDFOHFXOL", which was enciphered using an affine transformation of single-letter plaintext units in the 27-letter alphabet (with blank=26). You know that the first word is "I " ("I" followed by blank). Determine the enciphering key, and read the message.

5. You intercept the ciphertext message "PWULPZTQAWHF", which you know was encrypted using an affine map on digraphs in the 26-letter

alphabet, where, as in the text, a digraph whose two letters have numerical equivalents x and y corresponds to the integer $26x + y$. An exensive statistical analysis of earlier ciphertexts which had been coded by the same enciphering map shows that the most frequently occurring digraphs in all of that ciphertext are "IX" and "TQ", in that order. It is known that the most common digraphs in the English language are "TH" and "HE", in that order.

(a) Find the deciphering key, and read the message.

(b) You decide to have the intended recipient of the message incapacitated, but you don't want the sender to know that anything is amiss. So you want to impersonate the sender's accomplice and reply
"GOODWORK". Find the enciphering key, and determine the appropriate ciphertext.