

62 III. Cryptography

XGVRFXMAHWGXWLEHGZXKVBIAXKMXQM.

3. 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."
4. 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".
5. 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 (i.e., by the integers 0–9). 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", not the numeral zero). You know that the plaintext ends with the signature "007" (zero zero seven). What is the message?
6. You intercept 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.
 7. (a) How many different shift transformations are there with an N -letter alphabet?
(b) Find a formula for the number of different affine enciphering transformations there are with an N -letter alphabet.
(c) How many affine transformations are there when $N = 26, 27, 29, 30$?
 8. A plaintext message unit P is said to be *fixed* for a given enciphering transformation f if $f(P) = P$. Suppose we are using an affine enciphering transformation on single-letter message units in an N -letter alphabet. In this problem we also assume that the affine map is *not* a shift, i.e., that $a \neq 1$.
 - (a) Prove that if N is a prime number, then there is always exactly one fixed letter.
(b) Prove (for any N) that if our affine transformation is linear, i.e., if $b = 0$, then it has at least one fixed letter; and that, if N is even, then a linear enciphering transformation has at least two fixed letters.
(c) Give an example for some N of an affine enciphering transformation which has no fixed letter.
 9. Now suppose that our message units are digraphs in an N -letter alphabet. Find a formula for the number of different affine enciphering transformations there are. How many are there when $N = 26, 27, 29, 30$?