

MAT331 Exercises, Spring 08

set number 7

24. (*expires 5/13*) The string below was encrypted using an affine cipher on the 27 letter alphabet “ abcdefghijklmnopqrstuvwxyz” (there is a space in the 0th position.) Decrypt it.

fmw segjaweoouanerj a ceyqrype aswaheoaqbrqabeafrua eeaojerf afmjeayperjpu

Hint: this phrase follows the the typical pattern in English where there are (almost) as many spaces as words (and so spaces are very common), and the letter “e” is also very common. You can use the technique described in chapter 4 of the notes, section 7.3.

25. (*expires 5/13*) Recall that a Vignère cipher can be interpreted as a Caesar-like cipher on n -vectors, where n is the length of the key phrase. Can every affine encipherment on digraphs (two-character codes) be interpreted as an affine matrix encipherment on 2-vectors? That is, suppose I encode a message by affine enciphering on digraphs. Can I always get the same crypttext from the same plaintext using an affine matrix enciphering (using a 2×2 matrix) on 2-vectors? If your answer is yes, prove it. If no, give a counter-example that cannot be so interpreted.
26. (*expires 5/13*) Modify the `AffineMatEncode` routine from the notes so that you can use a text string as a key instead of a matrix and a vector. For example, if the phrase is k characters long, the key should be an $n \times n$ matrix and an n -vector, where $n^2 + n \approx k$. The elements of the key matrix and vector should be the numerical equivalents of the characters in the key phrase. Do something sensible with any extra letters (that is, if $k \neq n^2 + n$). Be sure to check that the resulting matrix is nonsingular.