MAT 331, Spring 2010, Problems

13. Write a procedure in `Maple` that counts the frequency of letters in a string of text. For example, here is what it looks like when I use mine:

    ```
    freqs("time flies like an arrow, fruit flies like a bananna.");

        [[" ",9], ["i",6], ["a",6], ["e",5], ["n",4], ["l",4], ["r",3],
    ["f",3], ["t",2], ["s",2], ["k",2], ["w",1], ["u",1], ["o",1], ["m",1],
                          ["b",1], [",",1], [".",1]]
    ```

    In the above phrase, there are 9 spaces, 6 each of the letters "i" and "a", "e" appears 5 times, and so on. [Hint: See `StringTools`. If you feel adventurous, as EXTRA CREDIT you can try to make a step by step procedure. In this case, you might find useful to group identical letters in the text using `Implode(sort(Explode(text))`]

14. The text below was encrypted with a substitution cipher. Only the letters (both upper-case and lower-case) were substituted, leaving punctuation and spaces alone. Figure out what the original message was.

    > "wA'r aBeD WUeK AP XNaB NM U rALKNP USUeAJBMA NM zUM nPrB ZNAW U JUM ZWP'r XBUeMNMO AP SXUD AWB aNPXNM." yWUA'r ZWUA rWB APXK AWB SPXNCB ZWBM rWB WUMKBK AWBJ AWB BJSAD eBaPXaBe.
    >
    > lNCWUeK heULANOUM, "yWB zCUeXUAAN yNXA"

    If you wish, you can find the encrypted text in the file `subscrypt.txt` from the problems area on the class web page.

15. The cryptography chapter in the notes is called "fsqFsHn sGGousG", which is actually the result of applying a Caesar cipher to its original title. A 53-character alphabet consisting of all the upper-case letters, a space, and all the lower-case letters was used; consequently the space in the middle might or might not correspond to a space in the title. Determine what the original title was.

16. The string below was encrypted using an affine cipher on the 27 letter alphabet " abcdefghijklmnopqrstuvwxyz" (there is a space in the 0^{th} 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.

17. 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.

18. 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.

19. Reimplement the `AffineMatEncode` and `AffineMatDecode` programs from the notes (section 4.8) to use the routines from the `LinearAlgebra` package instead of `linalg`.

20. Twenty-one pirates are dividing their horde of gold dubloons. Since they are a democratic outfit, they first try to divide the coins evenly, but they find there are 19 coins left over. The "discussion" about how to divide the remaining coins results in only 16 pirates still needing to divide the horde (the remaining five went to a place where you can't bring money or anything else with you). The redivision among 16 pirates leaves 1 coin left over, and three of the pirates make a grab for it. These three find themselves to be missing their hands after this attempt, and the remaining thirteen pirates decide to divide the share among themselves, leaving the handless ones with nothing. Fortunately, the horde divides evenly among the thirteen. What is the minimum number of coins in the horde?

21. Use RSA with the modulus $n = 119$ and the exponent $e = 7$, with the 95-character alphabet consisting of the printable ASCII characters to encrypt the word "Yes". Recall that the alphabet is given by

```
Alphabet:=cat(op(select(IsPrintable, [seq( convert([i],bytes), i=1..255)])))
```

    so that Y=58, e=70, s=84. Give your encryption as a list of three numbers.

22. With the same setup as the previous problem (that is $n = 119$, $e = 7$), the message after encrypting with RSA is the list of numbers

$$[42, 59, 4, 59, 27, 59].$$

    Decrypt the message. (This is doable because 119 is easily factored).