HW 5 CMSC 389. DUE Jan 12

NOTE- THIS HW IS ONE PAGE!!!!!!!!!!!!!
AGAIN EMAIL THE TA THE HW:

`michaelroberts94@gmail.com`

You MUST email it to him BEFORE 1:00 on Monday.

1. (10 points) READ my NOTES on line. What is your name? Write it clearly.

2. (30 points) Alice and Bob are using a matrix code with matrix

$$\mathbf{A} = \begin{pmatrix} 1 & 2 \\ 4 & 7 \end{pmatrix}$$

Alice wants to send the message *math*. What does she send?

3. (30 points) Describe an algorithm for the following problem: Given a ciphertext T that has been coded by a 2×2 matrix cipher, and given 2×2 matrix M with det rel prime to 26, determine if the ciphertext was coded with M. (HINT AND GRADING NOTE: This is similar to hw03 problem on Affine Ciphers. If you get this one RIGHT and got the one about Affine ciphers on HW3 WRONG, I will give you the points back for the Affine Ciphers one. On Monday between 2 and 2:30 come to me with your HW03 to show me that it was marked wrong. I will have from mike a list of who got THIS problem (hw05, prob 3) right. If you are on both lists I will give you points for hw03 problem 3.

4. (30 points) Alice and Bob are using a a matrix cipher with matrix

$$\mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

(Letters are $a = 0$, $b = 1$, ..., $z = 25$, NO capitol letters, NO numbers. Eve knows that yesterday Alice send the message *hats* by encoding it as vohy. Is this enough information for Eve to find the matrix? If YES then derive what the matrix is. If NO then prove that there are at least two matrices consistent with the known data.