Homework 1, 550.371/650.471 Cryptology and Coding, Spring 2017

Important Instructions: You may discuss this homework (including MATLAB questions) with students currently in the class, with the TAs, and with me, up until the time that you do your write-up; but the solutions and code that you submit should be entirely your own. You need to submit a hard copy of the MATLAB function you write for Problem 4, and a hard copy of a diary in which you use MATLAB interactively in Problems 1 through 4. You may (and should) clean the diary of extraneous material before submitting it. At no time may you consult any existing written solutions; this would be in violation of the homework rules and, in addition, would be plagiarism if sources are not cited.

Problem 1: You have intercepted the following ciphertext encrypted with a Caesar cipher: sdgyevnlocydowzdsxqdytecdgbsdomkxiyerokbwoxyg. Decrypt it by trying all possible keys.

Problem 2: You have intercepted the following ciphertext encrypted with a 1-dimensional affine cipher: cowcbfxiviagwiuxivixcdcbscbfxofrgbsrcafgnscttivcax. Decrypt in by trying all possible keys. (In the diary that you submit, edit out all but a sample of this output, since it would otherwise be many hundreds of lines.)

Problem 3: You have intercepted the following ciphertext encrypted with a Hill Cipher using block length 4: krtayyxvnitxnxombrhhloeuhnexxumazwltmfsf. Knowing that the first part of the plaintext reads thetipofthemonth, decrypt this ciphertext.

Problem 4: Write a MATLAB function that breaks the Vigenere cipher. The input is any Vigenere ciphertext, and the output should be the Vigenere key. Run your code on the fours ciphertexts in the accompanying file vigciphertexts.m.

Problem 5: Suppose a particular language's alphabet has only five letters, they are (consecutively) a,b,c,d,e, and their population relative frequencies are $.05, .20, .25, .35, .15$.
Would the method from lecture of breaking a Vigenere cipher work? Exactly what difference would there be in the implementation? (Your answer should include two specific numbers that you should compute and that are different here than for the English language.)