MACM 203 Assignment 8
Spring 2025

This assignment is due Tuesday March 25th at 10pm. Upload your solutions to Crowdmark. Write your solutions as a single Matlab Live Script and export the script to PDF. Write the course number and assignment number as the title of the Matlab Live Script, followed by the table of contents, and then create a section for each part of the question.

Keep in mind that your assignment, including the source code, is a document that will be read in order to be marked. It has to be very clear and properly formatted.

Assignments must be written individually. You can discuss in groups, but you have to write your assignment yourself. In case of academic dishonesty SFU policies will be applied.

Preamble

This week's assignment focuses on cryptography. All calculations must be performed in Matlab.

Question 1 (15 marks)

Part (a)

Consider Hill Cipher with block length $b = 2$. That is, the secret key is a 2×2 matrix over $\mathbb{Z}_{26}$. The definition of Hill Cipher is given in the lecture notes.

Let X be a 2×2 matrix whose rows are *some* two plaintexts, and let Y be the 2×2 matrix whose rows are the corresponding ciphertexts, in the same order. Let K be the secret key. Determine a relation among the matrices X, Y and K. Solve this relation (equation) for K, which is still just linear algebra using pen and paper. Once you have a general expression for K in terms of X and Y, only then start working on the numerical data with Matlab. Note that some matrices X can not be used in this method (specify the required condition on X).

Part (b)

In the data file `a8.mat` posted on Canvas you will find string `y`. It is known that `y` is a ciphertext obtained by Hill Cipher encryption with block size $b = 2$. It is also known that the encrypted plaintext contains the word *country,* which for the purpose of encryption was split into blocks of size $b = 2$ in the following way: `|_c|ou|nt|ry|` where _ denotes some unknown letter. The location of the word "country" in the encrypted plaintext is not known.

Using the method that you developed in part (a), perform a known plaintext attack on this version of Hill Cipher. Explain details of your work. Print the secret key that was used in the encryption process.

Part (c)

Decrypt the ciphertext given in the variable `y` that is contained in the downloaded file `a8.mat`. Print the decrypted plaintext string (which is English text) in lines containing 40 characters each. Note the decrypted plaintext does not contain spaces, punctuation, capital letters etc. (since those characters are not part of the alphabet that we use). You do *not* need to insert these features back into the decrypted plaintext; just print the raw string returned by the decryption.