Networks and Cryptography — Project 3
The Hill Cipher

1 Your assignment

Begin by grabbing some files as a ZIP archive from this (clickable) link:

> https://www.amherst.edu/ sfkaplan/courses/2015/spring/COSC-281/projects/project-3-yourusername.zip

Of course, replace `yourusername` with, well, *your username* (e.g., `sfkaplan`). You should find, in this archive, a trio of files:

1. `yourusername.ciphertext`: A file encrypted with the Hill cipher. This is the secret message that you want to decrypt, even though you don't have the key.
2. `yourusername-known-pair.cleartext`: A cleartext message from which a ciphertext (see below) is created. Notice, critically, that this message is **not particularly readable**. It was chosen because it provides an invertable matrix of plaintext that you can use for a known-plaintext attack.[1]
3. `yourusername-known-pair.ciphertext`: The ciphertext message created from the known plaintext, above, and the same key that was used to generate the unknown ciphertext (also above) with a Hill cipher.

Your mission: Decrypt the unknown ciphertext. Submit it by following the instructions below.

2 Submitting your work

When you are done, submit the following:

1. The decrypted unknown ciphertext.
2. The key used to decrypt the message (`my-key.txt`), as a matrix of byte values.
3. Your source code, etc., for encrypting, decrypting, or cracking Hill ciphertexts.

Submit each of these three elements at the the CS submission system under Project-3.

This assignment is due at **5:00 pm** on **Friday, May 15** (the end of exam period).

[1] So how hard is it to find, in, say, an actual text file, a portion of it whose bytes constitute an invertable matrix? I have no idea. Grab some text files and write something that uses your inversion code to answer that question. I'd happily share experimental results with the class.