NETWORKS AND CRYPTOGRAPHY — PROJECT 4
The Hill Cipher

1 Your assignment

Begin by grabbing some files:

```
$ mkdir project-4
$ cd project-4
$ cp -v ~sfkaplan/public/COSC-281/project-4/yourusername* .
```

Of course, replace `yourusername` with, well, *your username* (e.g., `sfkaplan`). You should copy 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.
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 ciphertext (whose plaintext was previously unknown to you).
2. In a text file named `my-key.txt` that contains the key that you used to decrypt the message.
3. The source code to any code your wrote for encrypting, decrypting, or cracking Hill ciphertexts.

Submit your work like so:

```
$ cs281-submit project-4 yourusername.plaintext my-key.txt *.java
```

This assignment is due at **11:59 pm** on **Thursday, May 02**.