NETWORKS AND CRYPTOGRAPHY — PROJECT 2
Cracking substitution ciphers

1 Part A: A needle in a haystack

To get started, click on the following link[1] to obtain a ZIP archive that has a collection of files. Download the archive and unzip them into their directory:
`https://www.amherst.edu/ sfkaplan/courses/2015/spring/COSC-281/`
`projects/project-2A-files.zip`

In this directory, you will find 8 files of the same length. All of them look, superficially, like random gibberish. However, **one** of them is, in fact, a file encrypted using the *substitution cipher*, while the others are, in fact, a sequence of random values. **Your task** is to find the real ciphertext and to decrypt it; the decrypted message will contain instructions that explain how to get started with Part B.

2 Part B: Vigenère cipher

In solving Part A, you will find instructions that lead you to another ciphertext—one formed using the Vigenère cipher. **Your task**, as you might have guessed, is to decrypt that message. You will readily notice that they ciphertext is long, providing suffient opportunity for the cryptanalytic techniques we discussed in class.

3 How to submit your work

Use the CS submission system to submit your decrypted messages, as well as any code or other calculation tools (e.g., spreadsheets) that you used to get the job done, for Project 2.

This assignment is due at **11:59 pm** on **Monday, Apr-20**.

[1] Although your PDF viewer may not show it in any special way, the text of that URL below is itself a link that you should be able to click. If you must (or choose to) copy and paste the URL into a browser, then **be sure to re-type the tilde before my username by hand**. For annoying reasons, it is often copied from these PDF's incorrectly.