

# NETWORKS AND CRYPTOGRAPHY — PROJECT 3

## Cryptanalysis, take II

### 1 Part A: A needle in a haystack

To get started, login to the department systems, obtain a directory of files, and change into it, like so:

```
$ tar -xvpf ~/public/cs28/project-3.tar
$ cd project-3
```

In this directory, you will find 16 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 the ciphertext is long, providing sufficient opportunity for the cryptanalytic techniques we discussed in class.

### 3 How to submit your work

Use the `cs28-submit` command to turn in your decrypted result from Part B, like so:

```
cs28-submit project-3 message.plaintext
```

This assignment is due at **5:00 pm on Friday, November 19.**