COMP 424 Fall 2016 Homework 1

Due: October 13th at 11:55PM

You intercepted a single ciphertext. Decipher it as much as you can. To receive full or partial credit you *must* show all your work. Attach any code you have implemented (you can use any programming language) or any code you have found anywhere that is publicly online (but you must include citations of all sources you used in the report).

```
DRPWPWXHDRDKDUBKIHQVQRIKPGWOVOESWPKPVOBBDVVVDXSURWRLUEBKOLVHIHBKHLHBLNDQRFLOQ
```

You may assume you already know:

- The encryption/decryption algorithm is a combination of columnar transposition and simple shift substitution.
- The key length is less than or equal to 10 letters long.
- The original message is in English.
- The original message contains only letters (i.e., no punctuation marks, numbers, etc).

How and what to Submit:

You will submit a .zip file on Moodle that includes all the source code, dictionary files, etc. that you used to decipher this. Also included in the zip file, a one-page report that includes the original message (if successfully deciphered) as well as a detailed description of your approach. To receive partial credit, you must also describe in the report what components of your implementation are missing in your submission, that if had them completed you would have successfully deciphered the ciphertext.

Important: To receive full credit, in addition to your Moodle submission, you must submit a *hardcopy*[1] of your submitted report on Moodle at the *beginning* of the lecture (7:10PM) on Oct 18th.

Cheating: This assignment is an individual assignment. You can discuss this with other students. You cannot share source code. If two submissions show significant similarity in source code then both students will receive an F in the course. Note a person who gives his code to another student also fails the class (you are facilitating the dishonest actions of another).

Good luck!

[1] hardcopy != e-mail