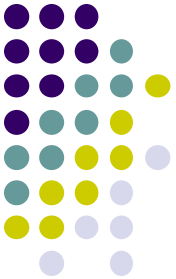
Homework

- **Write a cryptanalysis program to find the plaintext and key for the following ciphertext.**

MXDXBVTZWVMXNSPBQXLIMSCCSGXSCJXBOVQXCJZMOJZCVC
TVWJCZAAXZBCSSCJXBQCJZCOJZCNSPOXBXSBTVWJC
JZDXGXXMOZQMSCSCJXBOVQXCJZMOJZCNSPJZHGXXMOSPLH
JZDXZAAXZBXHCSCJXTCSGXSCJXBOVQX

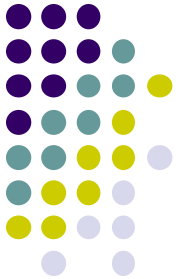
— plaintext from Lewis Carroll, *Alice in Wonderland*



Homework

- Use C/C++ language
- Assumptions:
  - The message was encrypted with the permutation-based substitution cipher.
  - The plaintext has no spaces or punctuation.
- **What to submit**:
  - Program source code written in C/C++
  - PDF file of your report that explains your program
    - Write your report using MS Word, convert the .docx to .pdf file, and submit the pdf file only.

Overall Process



1. Your program should take the ciphertext as input and compute letter frequency counts.
2. By comparing the computed letter frequency counts and the known frequencies of English, make an initial guess of the key.
3. Using the putative key, perform decryption of the ciphertext, count the number of dictionary words that appear on the decryption result, and use this as a score.
4. Try to increase the score by adjusting the key.
    1. If the score improves, update the key; otherwise, don't change the putative key.
5. Iterate this process until you have assurance that you have found the correct key.