Assignment 1

This assignment consists in comparing the output of a substitution cipher with the output of one-time pad.

Implement substitution cipher and one-time pad using by writing the following three programs for each (total 6 programs).

1. **Key generation program (`gen`).**
   - **For substitution cipher:** Takes no input, and outputs a file `key.txt` that contains a random key encoded as follows. The file is composed of a single line of 26 characters. Each character is a lowercase letter of the English alphabet. The first letter corresponds to how '`a`' is encrypted, and so on. (In the example on my slides, `key.txt` would contain `ejinbmo`...)
   - **For one-time pad:** Takes no input, and outputs a file `key.dat` which contains 100 kB of random bits
2. **Encryption program (`enc`).**
   - **For substitution cipher:** Takes as input the name of the file containing the plaintext, loads the key from `key.txt` (stored in the same directory as the program) and outputs `ciphertext.txt`, which is a file containing the encryption of the plaintext under the key in `key.txt`. All characters that are not letters or whitespaces (spaces, tabs, newlines, etc.) are removed from the plaintext prior to encryption, then the input is converted to lowercase characters.
   - **For one-time pad:** Takes as input the name of the file containing the plaintext, loads the key from `key.dat` (stored in the same directory as the program) and outputs `ciphertext.dat`, which is a file containing the encryption of the plaintext under the key in `key.dat`.
3. **Decryption program (`dec`).**
   - **For substitution cipher:** Takes as input the name of the file containing the ciphertext, loads the key from `key.txt` (stored in the same directory as the program) and outputs `plaintext.txt`, which is a file containing the decryption of the ciphertext under the key in `key.txt`.

- **For one-time pad:** Takes as input the name of the file containing the ciphertext, loads the key from `key.dat` (stored in the same directory as the program) and outputs `plaintext.txt`, which is a file containing the decryption of the ciphertext under the key in `key.dat`.

Write a one-page report in which you discuss how you could distinguish between ciphertexts generated with the encryption algorithms you implemented in this assignment. Assume that you do not have access to the key used to generate the ciphertexts. In other words, given a ciphertext c, describe how, you would determine whether c was generated using substitution cipher or one-time pad, without access to c's decryption key.

Extra Credit

Write a program that distinguishes between ciphertexts generated using the substitution cipher and one-time pad.

Items to Submit

1. Academic integrity form
2. Source code of `gen`, `enc`, and `dec` for substitution cipher and one-time pad (one source code file per program)
3. Report on how to distinguish between ciphertexts from the two algorithms
4. *Optionally*, the program that distinguishes between ciphertexts generated using the two encryption schemes. The extra credit program will be graded **only** if items 1-3 have been submitted

Items not to Submit

Anything not mentioned under items to submit. For example, do not submit:

- Eclipse projects
- Program binaries
- Keys
- Sample plaintexts or ciphertexts