CS-627: CRYPTOLOGY

Readings AND Assignments

NOTE that readings in addition to those enumerated here *may* also be assigned in class.

Where chapter and problem numbers are cited in the HOMEWORK, these refer to the same textbook that is featured in that week's READING assignment.

Week 1:

READING: Singh, Chapters 1 through 4.

ASSIGNMENT: Write a computer program that takes a text file as input and that can EITHER encrypt it OR decrypt it, as the user desires. The program operates with three files, all of which contain simple text. The plaintext text consists only of alphabetic characters of mixed case, spaces, commas, semicolons, and periods. The ciphertext file consists of ONLY upper-case alphabetic characters, spaces, and punctuation. The cryptokey file consists of 26 upper-case alpha characters. The punctuation carried over unchanged from plaintext to ciphertext. User input is:

(a) The filespec of the input file (either plaintext or ciphertext).
(b) The filespec of the output file (either ciphertext of plaintext).
(c) The filespec of the file containing the cryptokey
(d) Whether encryption or decryption is to be performed.

Week 2:

READING: Singh, Chapters 5 through 7.

ASSIGNMENT: All students are to complete the decryption of the ciphertext that we worked on in class, specifically to include determining the keyword as well as recovering the original plaintext message. In addition, each student is assigned an individual program to write, as follows:

Student 1: **Vigenere-Encryption:**

- takes an ASCII text file as plaintext message input;
- queries user for key word or key phrase;
- strips non-alpha characters out of plaintext file and out of key phrase;

- outputs Vigenere-encrypted ciphertext as an ASCII file in the form of blocks of five characters separated by five spaces.

Student 2: **Vigenere-Decryption:**

- takes an ASCII text file as ciphertext message input;
- queries user for key word or key phrase;
- strips non-alpha characters out of ciphertext file and out of key phrase;
- outputs Vigenere-decrypted plaintext as an ASCII file in the form of a continuous stream of alphabetic characters.

Student 3: **Program to Compile Statistics from Texts:**

- takes various ASCII text files as input (queries user for filespecs);
- strips out non-alpha characters from files, and converts to all-lower-case;
- counts frequencies of individual letters, of all possible digrams, and of common trigrams, tetragrams, and pentagrams.

All Students:

Locate and compile text file groups from several distinct sources, such as:

- **High-quality news reports (e.g.,** ***New York Times*****)**
- **Classic texts of distinct authorship (e.g., Shakespeare, Melville, Stevenson, Poe, Clemens, Dickens)**
- **General scientific writing (e.g.,** ***Scientific American, Science*****)**
- **Computer Science (*****IEEE Computer, Communications of the ACM*****)**
- **other sources of distinctly different content**
- **WARNING: use ASCII text only, <u>not</u> HTML.**

FILE NAMING CONVENTIONS:

- **plaintext-*n*.txt**
- **ciphertext-*n*.txt**

Week 3:

READING: Mel & Baker: Foreword, Preface, Introduction, and Part I (Secret Key Cryptography; chapters 1 through 8)

ASSIGNMENT: Develop a plan of cryptanalytic attack for an unknown ciphertext consisting of a sequence of alphabetic characters. All that you know about the message is that the plaintext is an English-language message. You do not know whether the encryption was effected by transposition or substitution, of by substitution whether it is monoalphabetic or polyalphabetic. How would you proceed to tackle the problem?