Nifty Assignments:
Encryption & the Enigma Machine

David Reed
Department of Computer Science
Creighton University
davereed@creighton.edu
Overview

3 CS1/CS2 assignments based on encryption & the Enigma machine

- could be assigned independently, or as connected assignments in a course

why nifty?

- historical significance & modern relevance of encryption
- each assignment can have a hands-on component, building physical models out of paper
1. Cipher Disks & Cryptograms

historical motivation:
- substitution ciphers have been used for millenia
  - Atbash cipher (6th century B.C.)
  - Caesar cipher (1st century B.C.)
  - Vigenère cipher (16th century)
  - Civil War cipher disks

more recent:
- cryptogram puzzles
- motivation for discussing modern uses of encryption
  - e.g., process underlying secure Web-based transactions
1. Rotating Ciphers (CS1)

Hands-on activity:
- Can build a cipher disk out of paper
- E.g., various templates at http://www.secretcodebreaker.com/ciphrdk.html

CS1 assignment:
- Given a class for a simple, fixed substitution cipher
- Generalize to handle capitals & non-letters, arbitrary keys, key rotation to strengthen code
- Focus: class modification, string manipulation, file processing
2. Multiple, Rotating Disks

rotating substitution keys are the underlying mechanism of the Enigma

- can obtain Enigma-like behavior from a generalized 3-ring cipher disk
- 2-stage mapping to encode a letter:
  - 'A' inner $\rightarrow$ 'H' outer; 'H' middle $\rightarrow$ 'N' outer
- odometer-style disk rotation
  - rotate inner disk after each encoding;
  - also rotate middle when inner completes cycle

hands-on activity:
- similarly, can build a paper model
- e.g., http://www.jambe.co.nz/makeenigma.html
2. Simple Enigma Model (CS1)

CS1 assignment:

- based on the paper model of 3-ring cipher disk, design and implement a simple Enigma simulator
- must support both encoding & decoding
- allow for different rotors & settings
- focus: class design, string manipulation, GUI design
3. Enigma Machine

historical motivation:
- Enigma used by Germany in WWII
- original design utilized 3 rotors
  - interchangeable, could vary order & setting
  - rotors contained circuitry, connecting to adjacent rotors
  - effectively defined a 6-stage mapping
- rotors are interlocked to produce a complex, automatic rotation pattern

hands-on activity:
- I have designed a 3-D paper model (inspired by Koss' Paper Enigma)
- http://dave-reed.com/DIYenigma
3. Enigma Simulator (CS1/CS2)

CS1/CS2 assignment:

- based on the paper model, design and implement a complete Enigma simulator
- must allow for different initial rotor settings
- focus: complex design, interacting classes, string manipulation, GUI design
Summary

assignments with a story & context are more interesting to students than artificial applications

assignments that have a hands-on component are engaging to students
- can help to build a mental model of what they are designing/implementing

the topic of encryption can lead to exploration
- just turn on the History Channel
- online resources on encryption, Enigma, Bletchley Park, …