Technology & Privacy Issues: A Freshman Course at Pacific Lutheran University

Dr. Richard Spillman
Pacific Lutheran University

Introduction

Pacific Lutheran University (PLU) has developed a special freshman year program that includes two unique courses. One is a freshman writing seminar and the other, which is the focus of this paper, is a critical conversation course. All freshmen are required to select among the various writing seminars one semester and select one of the critical conversation courses the next semester. The critical conversation courses are designed to introduce PLU freshman to important topics in a manner that stimulates their critical thinking abilities. Freshman students may satisfy this requirement with courses such as:

Issues in Human Reproductive Technology
TV: Visions and Values
Health Beliefs Along the Pacific Rim
Ethics in Psychology
Gangs and Public Policy
Privacy and Technology

Each semester, new classes are added to this list providing students with many different and interesting choices. The subject of this paper is the use of cryptography in the Privacy and Technology class.

Course Content

The goal of the Privacy and Technology course is to provide students with an understanding of the importance of privacy and the impact of technology on their privacy rights. It is designed to address the irony of a society that at once promotes privacy yet embraces a technology that has the potential to violate privacy. At the beginning of the course, most students believe that privacy is a right that is totally guaranteed by the US Constitution. They feel secure and safe in their rights as US citizens. Very few suspect that computer technology might have any impact on their privacy rights. By the end of the course, these same students understand both the extent and the limits of their privacy rights. They have gained some insight into the vast amounts of personal data that have been and continue to be collected and stored in computer systems. Perhaps most importantly, they understand that "information is power" and, hence,

information must be protected. As a result, they learn how cryptography can be used to secure information while gaining a healthy respect for the hidden weaknesses of what appear to be complicated cryptographic schemes.

The class uses two text books: The Right to Privacy by Alderman and Kennedy and Information Warfare by Schwartau. These texts cover issues in privacy rights and the impact of technology. They also use a software tool developed by the author called CAP, Cryptographic Analysis Tool. This tool is available from the author's ftp site at http://www.plu.edu/~spillman/cap.html

Class Structure

The class meets once a week for 2 hours. The classroom sessions consist of lectures, discussions, and demonstrations. Each lecture/discussion section is broken down into two parts. The lectures begin with a look at the historical development of privacy and its protection. The second part is a study of the means to protect and expose information. The topics for each lecture are listed the following table:

Lecture Number	Historical/Social Topic	Cryptographic Topic
1	Introduction to Privacy	<none>
2	Privacy Rights	Simple shift
3	Privacy Rights	Keyword substitution
4	Early history of cryptograpy	Breaking keyword
5	Privacy during the Dark Ages	Polyalphabetic methods
6	Spies in WWI	Breaking Vigener Ciphers
7	WWII technology	Transposition Ciphers
8	WWII	Breaking Transpositions
9	NSA	Block ciphers, DES
10	WWW	Public Key Systems, RSA

The assignments involve reading and problem solving. The reading assignments include reading from the two textbooks used in the course and from a list of articles. The student must select three articles from a list that includes current comments on privacy issues and selected articles on the history of cryptography (most of these are taken from the journal Cryptologia). For each article read, the student must have in a short one-page article review. The problem solving assignments require the use the CAP tool (see the following section). They are asked to create ciphers and explore the characteristics of the resulting ciphertext. They are also given ciphertext and challenged to use the CAP tools to discover the plaintext.

There is one unique exam in the course. It is administered in the week before dead week. The students are handed a sheet of paper containing 4 or more paragraphs. They are told that all they need to know about the exam is described on that page. Unfortunately each paragraph is encipher with a different code. They are told that they could leave the classroom and use any resource they need to complete the exam. In order to ensure that the students experience an early

success, the first paragraph is an example of a simple shift cipher. That paragraph explains the ground rules for the exam which include the option to work on the remainder of the exam with another student; the requirement that all the plaintext be handed in to the instructor by the next morning; and a clue or instructions where on campus they may find a clue to the cipher used for the next paragraph. From that point on, the ciphers are increasingly more difficult to solve but each points the student to some clue. They may be asked to go to the department secretary and ask for their "secret decoder ring"; they may be sent to the library to look up some fact or check out a clue which had been placed on reserve; or they may be asked to call a certain phone number where the answering machine will offer a clue. They are also told that if they can not break a given cipher, they may contact the instructor and "buy" additional clues. The cost of a clue is a certain number of points on the exam.

Cryptographic Tool

To learn cryptography and cryptanalysis, students use a general-purpose tool called CAP for Cryptographic Analysis Program. This tool, in its current version, allows students to create and break several types of ciphers. It comes with a built in tutorial and a separate handbook. The handbook is in the form of an Power Point presentation that runs on a PC. It not only covers the operation of CAP, it also contains general information on cipher design and cryptanalysis. It is used to supplement in class lectures and as an on-line aid to students while working on their assignments.

When CAP runs, it presents the main window shown in Figure 1. Plaintext or ciphertext is entered directly or loaded from a file. The students, then, use the menu item, Encipher/Decipher, to select a cipher. Each cipher selection opens a window that contains a brief explanation of the cipher and prompts for a key entry. Once the key is entered, the student may select to encipher the plaintext or decipher the ciphertext. The handbook may be used to help them understand the operation of each cipher. The ciphers which version 1 of CAP implements includes are simple shift, keyword substitution, multiliteral substitution, Vigenere cipher, Playfair, and column transposition. Future versions of CAP will include the knapsack, other transpositions, and additional polyalphabetic ciphers.

Most students enjoy the cryptanalysis segment of CAP. In order to learn about the hidden weakness of what appear to be complicated (and hence secure) schemes, CAP provides a set of tools for the analysis of ciphers. These tools include: a simple shift search; frequency analysis; a keyword worksheet; a multiliteral analysis; Index of Coincidence calculations; Kasiski method; low frequency search; an anagram tool; and column transposition analysis. Most important for the beginning student is the AutoSolve menu item. This opens a window that guides the student through an analysis of an unknown cipher. It suggests tools to use, asks questions about the findings, records results, and suggests courses of action. With AutoSolve, students can systematically break down an unknown cipher. The AutoSolve window is shown in Figure 2. The flow chart suggests operations that can be performed by double clicking on the highlighted suggestion. As the student completes the tasks, they are recorded and saved in a summary file. By checking the observations in the flow chart, CAP will make additional suggestions that also are saved in the summary file. The summary file allows students to conduct a cryptanalysis

effort in more than one session. By reviewing the summary file in a later session, they can avoid repeating tests. It may also be used to document their efforts. As a result, students are required to hand in their summary file with their assignments.

These cryptanalysis tools are designed to help the beginning student as much a possible. For example, the frequency analysis tool not only determines single character, digram, and trigram frequencies, it also uses observations on the structure of English to aid in the identification of characters. Figure 3 shows the character ID window. In addition, there is a window that searches the ciphertext looking for word patterns and includes a small dictionary that may be modified by the student.

The keyword worksheet allows the student to enter part of a possible substitution key and use it to decipher the ciphertext. Examination of the result may provide clues to words that will aid in the identification of other substitutions.

The column transposition tool is perhaps the most sophisticated. It involves several operations beginning with one that will suggest possible rectangle sizes and allow the student to run tests based on vowel distribution to determine the best sizes. Once the size has been determined, the student can move to the anagram tool. This tool provides additional functions that allow the student to easily move rows and test possible row combinations. In this way, it provides an easy anagram tool as shown in Figure 4.

Additional tools, including stream cipher analysis and genetic algorithms are planned for future versions of CAP. In this way, the course content will be expanded to include an examination of other ciphers and their weaknesses.

Summary

This course addresses a significant issue that will face our students as they move into the workplace. In discussions with the students during and after the course, the instructor has notices several common themes. Overall, the students seem to enjoy the course. They find the exam to be very unique and even fun. Some students have asked if they can take the exam again the next time it is offered. The class covers many different topics and the students find the blend of history, law, English, political science, and technology provides a unique way at looking at the forces that shape their world. But more important than the general positive experience that students report is the increase in awareness of the impact of technology on their private lives. Most enter the class with the idea that privacy is a right that is protected by law. They leave the class with the understanding that privacy is a dynamic concept, which they have a responsibility to preserve.

RICHARD SPILLMAN
Department of Engineering
Pacific Lutheran University
Tacoma, WA 98447
Spillmrj@plu.edu

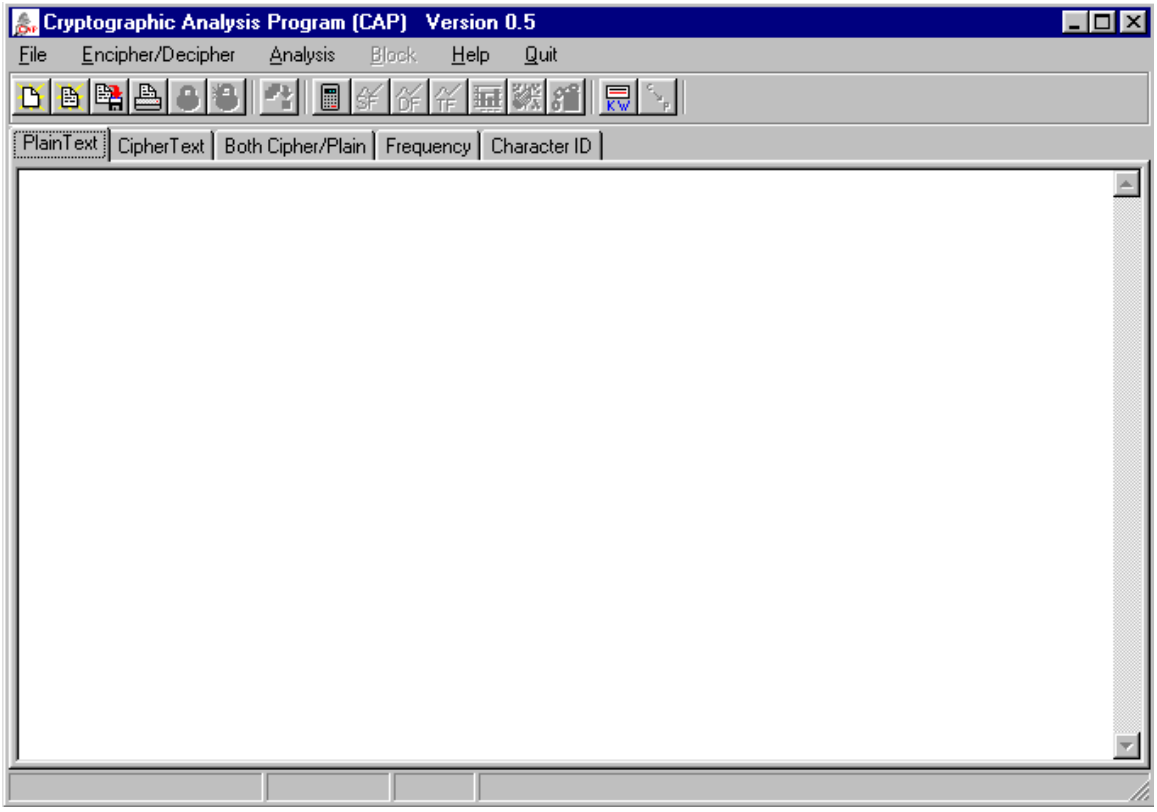

Figure 1: CAP Main Window

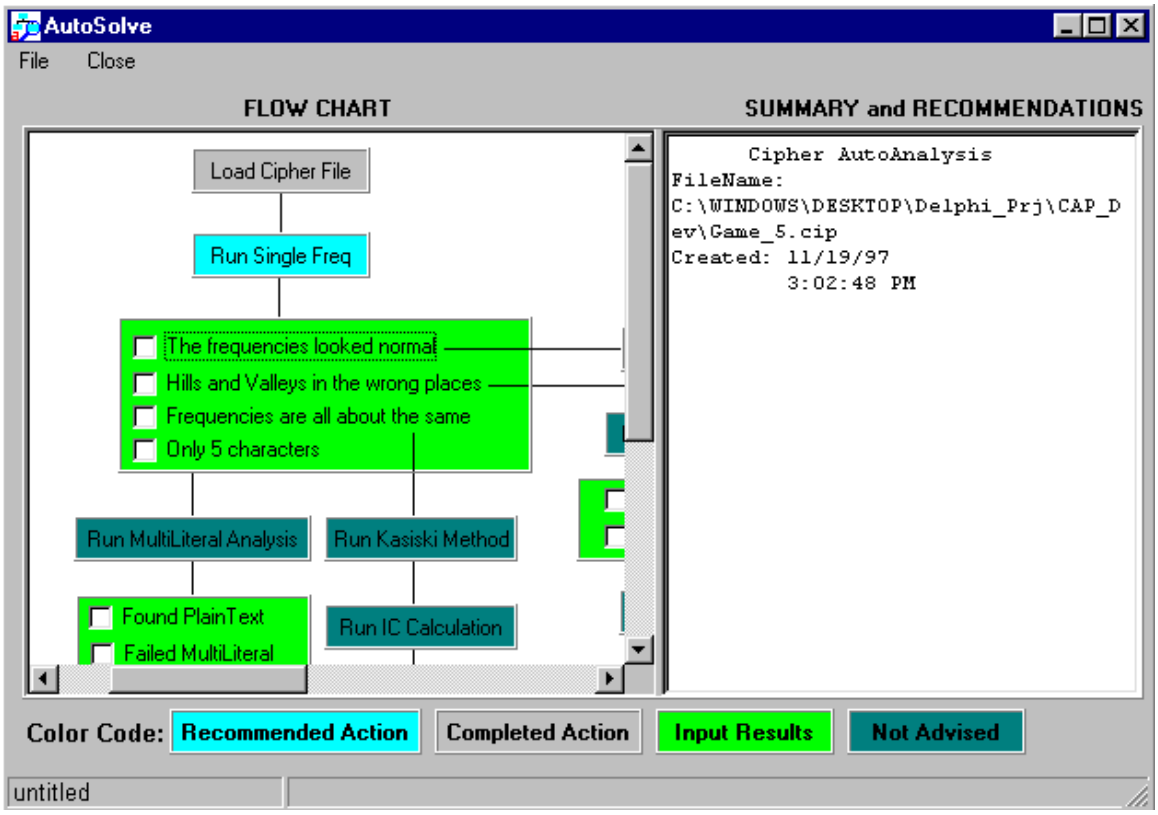

Figure 2: AutoSolve Window

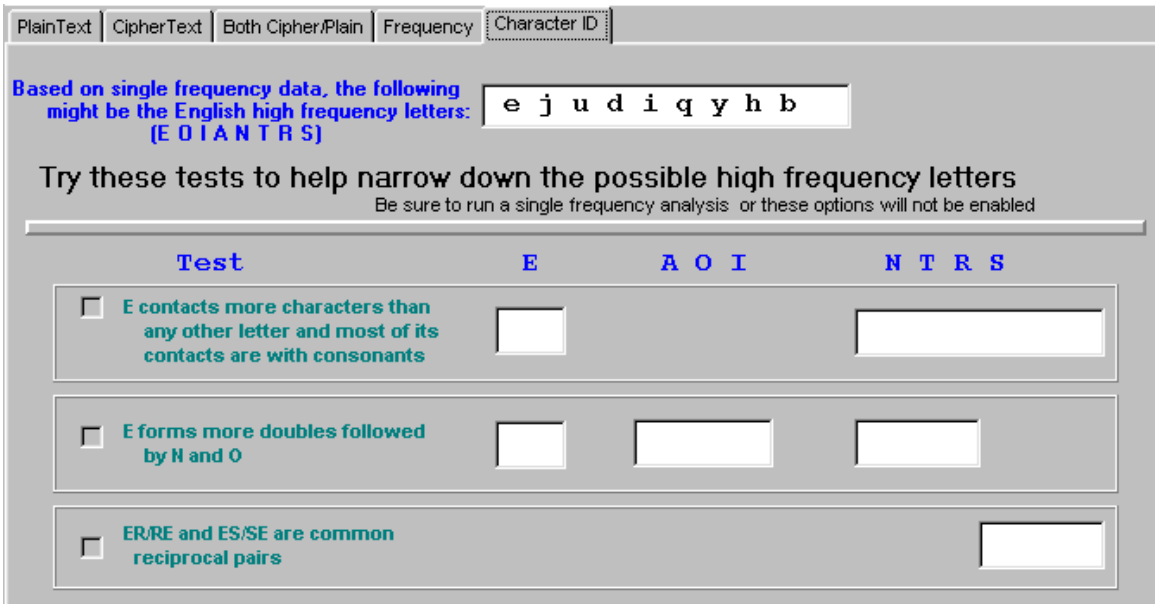

Figure 3: Character ID Screen

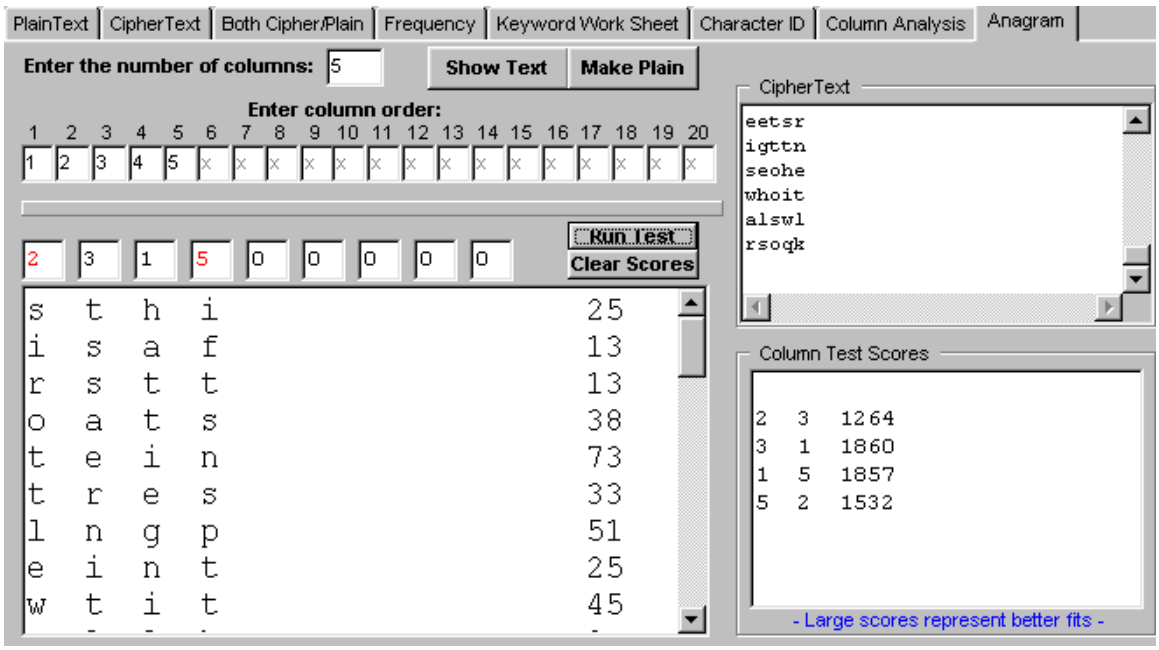

Figure 4: Anagram Screen