CAP
A Software Tool for Teaching Classical Cryptology

Dr. Richard Spillman
Department of Computer Science and Engineering
Pacific Lutheran University
Tacoma, WA 98447

OFFICE: 253-535-7406
FAX: 253–536-5055

spillmrj@plu.edu

ABSTRACT

The world of cryptology has a long and rich history. Many different cipher systems have been developed and ultimately broken. While these systems are no longer in use as main stream encryption methods, the study of such systems and their weaknesses remains important. Classical cryptology teaches students about the pitfalls of cipher design, develops an intuitive feel for the nature of cipher systems and motivates the study of modern ciphers. This paper describes a software tool called CAP (Cryptographic Analysis Program) that can be used in a course on classical cryptology. The program allows students to explore different implementations of classical ciphers and provides the tools necessary to break many of those ciphers. It can be downloaded from the author's web site at www.plu.edu/~spillmrj.

CAP: A Software Tool for Teaching Classical Cryptology

Dr. Richard Spillman

1.0 Introduction

Classical cryptology is the study of cipher systems that had their primary origin in the pre-computer era. However, that does not mean that these systems and the processes of breaking these systems are no longer of any use in the teaching of cryptology. There are at least three reasons why classical cryptology is still an important subject matter in today's computer security courses. First, classical cryptology can motivate a student's interest in contemporary cryptology. Second, classical cryptology can develop a student's intuitive feel for the strengths and weaknesses of any cipher system. Third, classical cryptology can teach students the necessary discipline that they will need for the development and analysis of contemporary systems.

1.1 Motivate Students

There is a critical need for individuals with a background in computer security hence ways in which students could be encouraged to consider computer security as a career could be very helpful. The study of classical cryptology can be such a motivator. The history and the mystery surrounding codes and ciphers is the stuff of Hollywood. I have found students to be very interested in the stories that come out of the study of cryptology and especially interested in trying out some of the ciphers. This level of interest seems to transcend grade levels. For example, I have taught a 2 day history of ciphers course to 7th graders and found that their level of interest matched that of the students in my computer security course at PLU.

1.2 Develop an intuitive sense

The process of cryptanalysis is as much an art as it is a science. As a result, a good cryptanalyst relies on intuition as well as knowledge to solve tough problems. Intuition is developed by experience and today's cryptanalyst must have experience with mathematics and language structure. Some of the intuition about language can be gained by working with classical ciphers. While exploring the strengths and weaknesses of classical ciphers, a student can learn about the characteristics of language and structure of ciphers and begin to understand at a intuitive level how language is used.

1.3 Teach Discipline

The art and science of cryptology requires a high level of discipline. This is especially true of cryptanalysis where the process of discovering weaknesses in a cipher system involves more than just skill and insight. It requires the discipline to engage in a trail and error process that produces more blind alleys than successes. It requires the ability to stick to a task without constant rewards. This discipline can be built up by teaching students how to analyze classical ciphers where the difficulty level grows as the student matures.

1.4 Goal

One problem with classical cryptology courses in computer science is that they are often programming courses as well. Requiring students to write programs to implement a given cipher or analysis tool limits the amount of time available to students to study the full range of ciphers and tools. Hence, the goal of this paper is to present a tool for use in classical cryptology courses that will enhance the teaching environment in order to increase the impact of the three advantages of such a course. The tool is called the

Cryptographic Analysis Program or CAP. It is written in Delphi and runs on PCs. It offers students the ability to explore the inner workings of classical ciphers and to utilize a set of standard tools for cryptanalysis.

2.0 **CAP**

CAP is a windows program that will allow a student to both make and break ciphers. It covers both the classical ciphers and cryptoanalysis techniques as well as some of the more contemporary systems. It even includes a challenge game which students can play on their own to test their cipher breaking skills and an automated cryptanalysis system that will guide them step-by-step through the process of breaking a cipher.

To start CAP, double click on the CAP icon, and the main CAP window will open (see Figure 1.0). From this window the student can navigate though the various features of CAP. The two major fields in the CAP main window are the plaintext and ciphertext boxes. Both boxes are like small word processors so you can directly type text into one of the boxes and save it to a file. Later, the saved file can be opened into either box.

All the cipher implementations have the same type of CAP interface. Enter the plaintext in the plaintext window and then select a cipher type from the Ciphers main menu option. Depending on the cipher chosen, a cipher window will open asking for a key. Once the key is entered, the student can either encipher or decipher (if ciphertext is available in the ciphertext window). Possible ciphers currently available in CAP include: simple shift, multilateral, affine, keyword, Vigenere, column transposition, Hill, Playfair, Nihilist, stream, ADFVGX, rotor, autokey, four square, Turning Grille, and the Bazeries cylinder. Additional ciphers are being added as the capabilities of CAP grow.

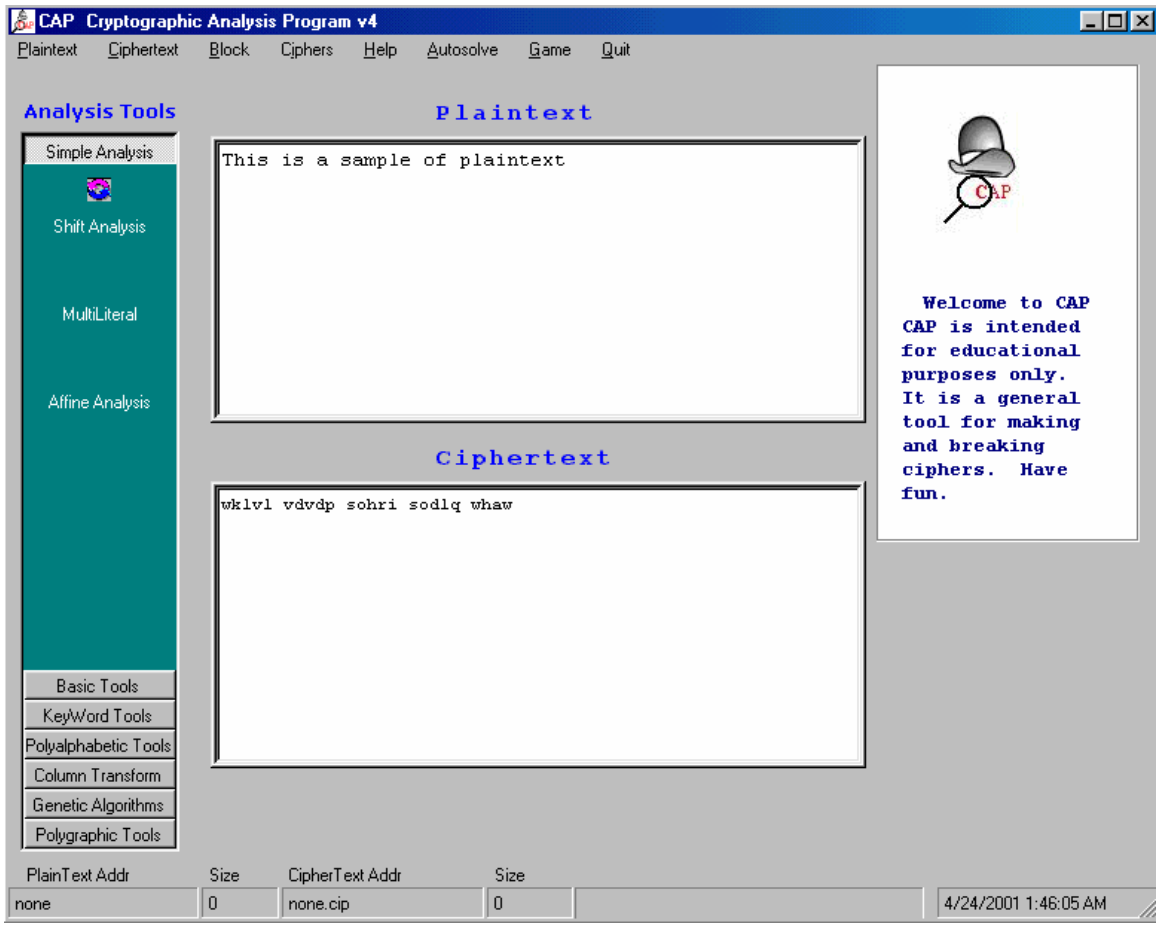


Figure 1.0: Main CAP Window

These ciphers allow the student to explore the characteristics of a large and varied number of classical ciphers within the confines of a single quarter or semester class. The real power of CAP, however, lies in its set of analysis tools. They are available to students from the Analysis Tools menu on the LHS of CAP. The student selects a cipher type and is offered a set of tools related to the cryptanalysis of that cipher.

For example, under the list of Basic Tools, CAP offers a standard frequency analysis option as shown in Figure 2.0.

Figure 2.0: Basic Tools Options

When this tool is selected, a frequency analysis window opens as shown in Figure 2.1.

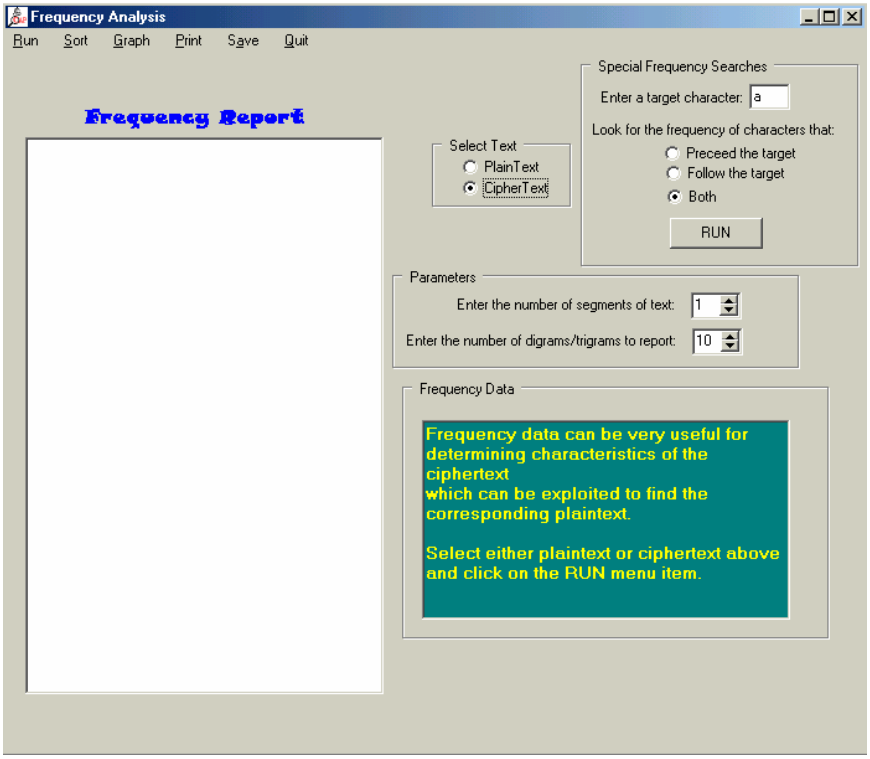
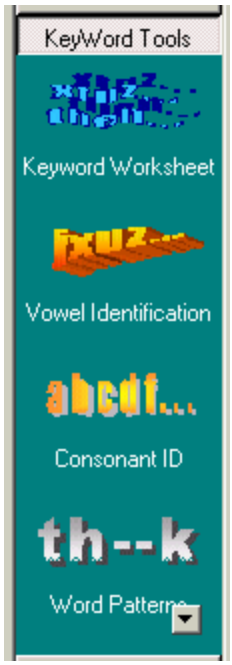


Figure 2.1: Frequency Report Window

From this window, the student may select single, double or triple frequency runs. The results are reported in both table and graph format and can be saved for future analysis. Specific tools for a keyword analysis are shown in Figure 2.2. These tools allow the student to search for known words, exploit the standard characteristics of vowels and consonants, and experiment with possible keywords in a keyword worksheet as shown in Figure 2.3.



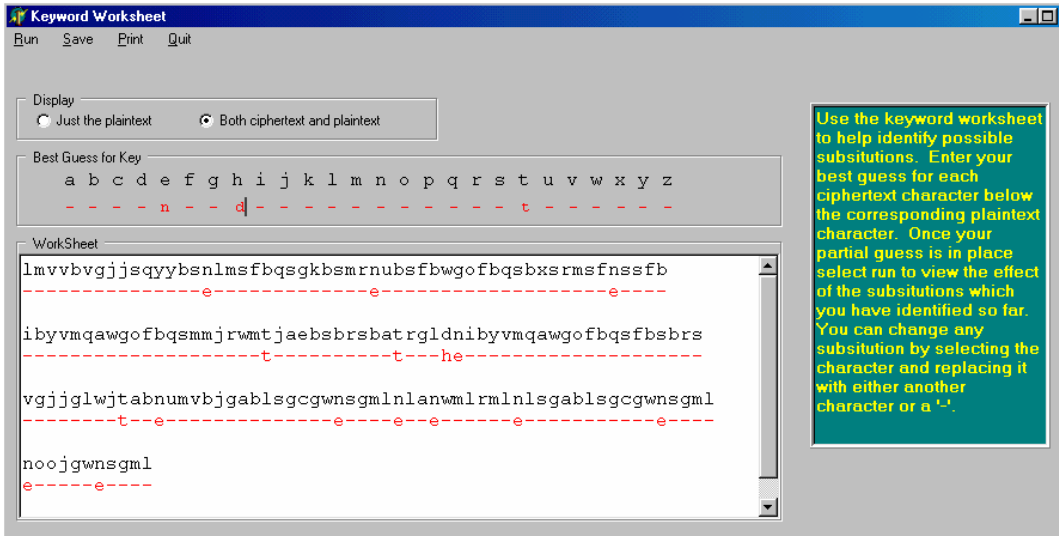


Figure 2.3: Keyword Worksheet

Figure 2.2: Keyword Tools

The polyaphabet tool set includes a Kasiski analysis; a low frequency character analysis, as well as a set of Autokey analysis tools. The Column Transposition tool set includes an anagram analysis tool and a size estimate tool. The set of tools available to students is also growing as CAP improves.

2.1 **Example Run**

For example, confronted with a Vigenere cipher, a student would begin with a Kasiski analysis to determine possible keyword lengths. A sample run is shown in Figure 2.4. Once a keyword length has been determined, the student could run a low frequency analysis which, in this case, immediately discovers the keyword as shown in Figure 2.5.

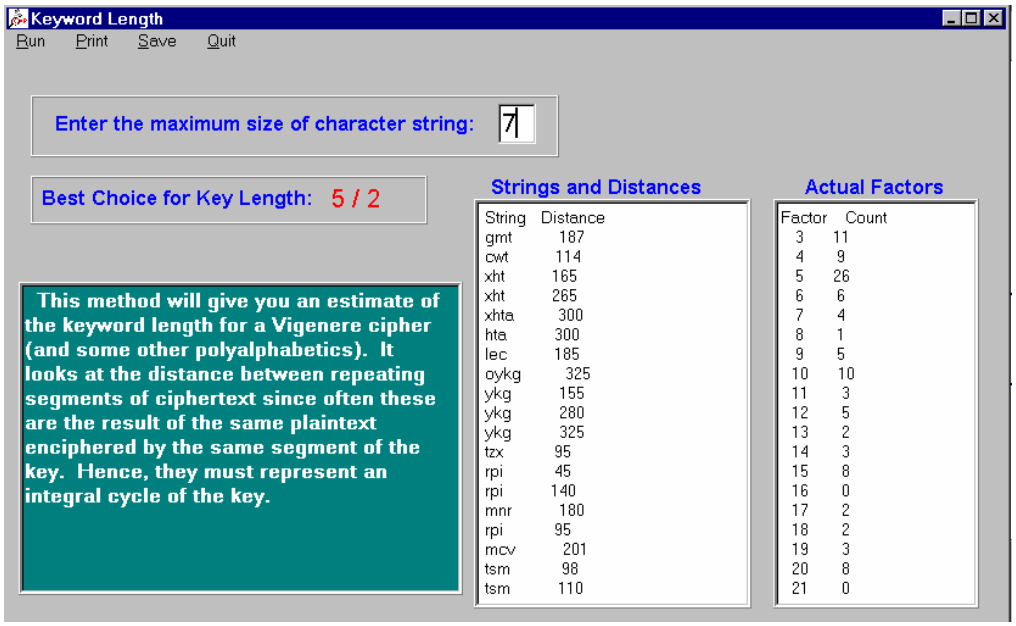


Figure 2.4: Results of a Kasiski run

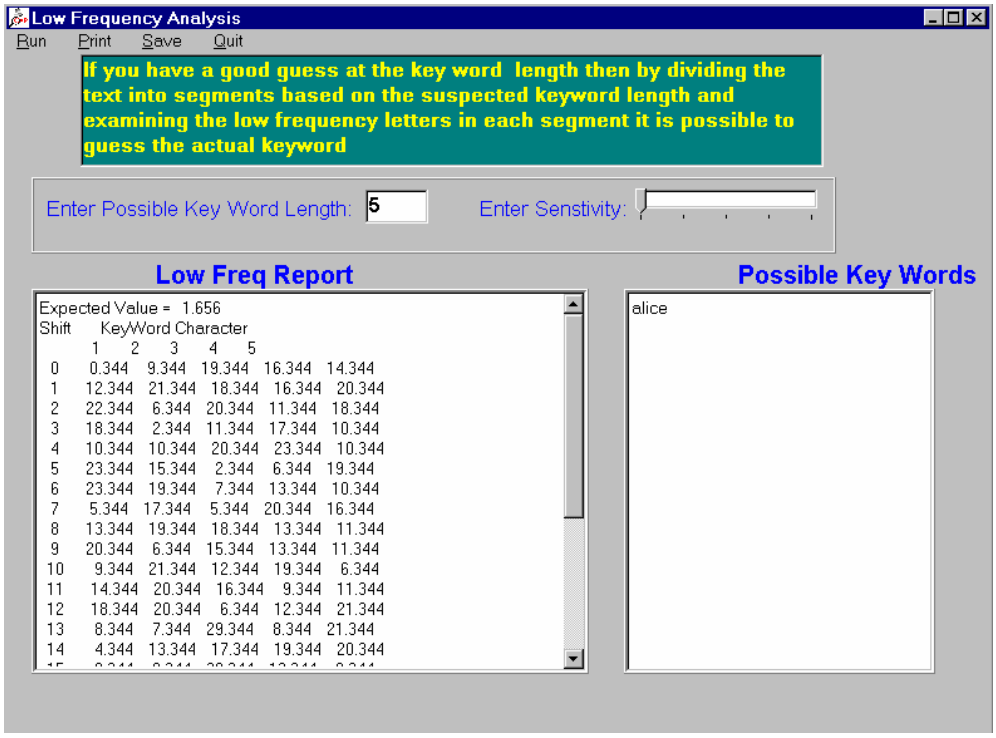


Figure 2.5 CAP Low Frequency Run

3.0 **Summary**

The limitations of this short paper do not allow for a full discussion of all the features of CAP. However, it should indicate that the CAP can relieve the burden of programming from a classical cryptology course and allow students to explore a larger set of topics in order to mutative an interest in computer security, develop a useful level of intuition, and expose them to the necessary discipline required by this field.