Teaching Cryptography in a Wireless Environment using Maplets

Neil P. Sigmon
Email: npsigmon@radford.edu
Department of Mathematics
Box 6942
Radford University
Radford, VA 24142 USA

Abstract

Cryptography is a subject with much historical and modern significance that provides many interesting applications of mathematics. Due to intensive computations required in many algorithms in cryptography, the use of some type of technological resource is almost an essential component of any course involving this topic. This paper demonstrates the use of Maplets, which allow students to easily execute encryption and decryption algorithms with very little required programming knowledge. A description will be given of how these Maplets can be used in conjunction with electronic discussion groups to allow students to simulate encrypted communications. All materials involving Maplets accompanying this paper can be found at the following URL:

http://www.radford.edu/~npsigmon/Maplets/mapletpage.htm

1 Introduction

With society becoming more reliant on digital and computing technology, the ability to transfer information in a secure and confidential fashion using *cryptography*, the science of secret message writing, has increased dramatically in importance. Cryptography is used in everyday life, including applications involving the Internet, banking transactions, and in the military. As reliance on computing technology continues to grow, people will benefit in having at least some basic knowledge of this topic.

Cryptography can be taught at a variety of levels, ranging from the general education level to a graduate level course in mathematics. For the general education audience, a student only has to recall concepts such as prime numbers and arithmetic such as division and multiplication to understand some of the most modern methods used in cryptography today. Currently, a general education course for Radford University's Honors Academy (see [King, 2007]) involving cryptography is being offered. This course has been a very popular course with students. For the more mathematically inclined, cryptography provides an excellent demonstration of applications of topics in mathematics involving linear algebra, abstract algebra, number theory, probability, and statistics. Courses in cryptography are currently being taught in many undergraduate and graduate mathematics programs.

Although many of the mathematical concepts involved in cryptography are simplistic in nature, realistic applications can be computationally intensive, making them impractical to compute by hand. Fortunately, many cryptographic algorithms are easily programmable using programming languages

such as Java, Maple, and on graphing calculators. The downside of this approach is that students must obtain at least a basic knowledge of these languages in order to use these codes successfully.

However, this problem can be alleviated through the use of Maplets. Maplets allow one access to windows, dialogs, and other visual interfaces that are very simple to use and require no background programming knowledge. By simply typing information into text boxes and clicking buttons, students can easily execute the large amount of computations required with cryptography almost instantaneously. The Maplets are produced using written code involving the symbolic manipulator Maple, which is a powerful programming language specially designed to perform complex mathematical computations. However, to successfully use a Maplet, students do not have to have any working knowledge of Maple. They only need to have Maple installed on their machine and run the end product of the Maple code used to construct the Maplet.

Several Maplets have been successfully implemented by students in the Honors Academy course involving cryptography to encipher, decipher, and cryptanalyze messages (note that *cryptanalysis* is the process of an enemy trying to intercept and break an encrypted conversation between two correspondents). In conjunction with the use of wireless technology involving laptops and tablets, these Maplets also have given students the opportunity to communicate with each other using encrypted messages on discussion boards involving the use of virtual online learning environment tool Blackboard. The use of Maplets has greatly enhanced the ease of using technology in this class.

The purpose of this paper is to demonstrate how Maplets together with wireless communication can be used in teaching cryptography. An affine cipher will be used as an example.

2 Affine Ciphers

Affine ciphers use a congruence of the form

$$y \equiv ax + b \pmod{26} \tag{1}$$

to encipher and decipher messages. Here, x is the numerical representation of a plaintext letter, y is the numerical representation of the ciphertext letter, a is the multiplicative key, and b is the additive key. The plaintext letter is simply a letter that we want to disguise (encipher), and the ciphertext letter is the result of the encipherment. All computations are performed *modulo* 26, which, for the purposes of this paper, mean that we compute the integer remainder upon division by 26. For example, $29 \pmod{26} \equiv 3$ and $54 \pmod{26} \equiv 2$. To convert letters to numerical form, we let A = 0, B = 1, C = 2,…, Y = 24, Z = 25. The variables a and b are the two keys for the cipher and are the parameters that are used to disguise messages. Note, for decipherment purposes, the greatest of common divisor of a and 26, denoted by $\gcd(a, 26)$, must by 1.

For example, suppose we want to encipher the message “RU” using the affine cipher with keys $a = 11$ and $b = 3$, that is, using the affine cipher $y \equiv 11x + 3 \pmod{26}$. Using the fact that R = 17 and U = 20 in numerical form, the encipherment is carried out in the following way.

$$\text{R} \Rightarrow x = 17 \Rightarrow y \equiv 11(17) + 3 \pmod{26} \equiv 187 + 3 \pmod{26} \equiv 190 \pmod{26} \equiv 8 \Rightarrow \text{I}$$

$$\text{U} \Rightarrow \quad x = 20 \Rightarrow \quad y \equiv 11(20) + 3 \pmod{26} \equiv 220 + 3 \pmod{26} \equiv 223 \pmod{26} \equiv 15 \Rightarrow \quad \text{P}$$

Hence, the ciphertext is the message "IP" (note that I = 8 and P = 15 in numerical form).

For longer messages, the process can become cumbersome since the encipherment must take place for each letter individually. However, through the use of a Maplet, longer messages can be enciphered instantaneously. Figure 1 demonstrates the result of using a Maplet for affine ciphers to encrypt the message "RU IS SHORT FOR RADFORD UNIVERSITY WHICH IS LOCATED IN RADFORD VIRGINIA" with the affine cipher $y \equiv 11x + 3 \pmod{26}$. Here, we select the **encipher** option, enter the message, enter the values 11 and 3 for a and b, and click **Encipher Message**.

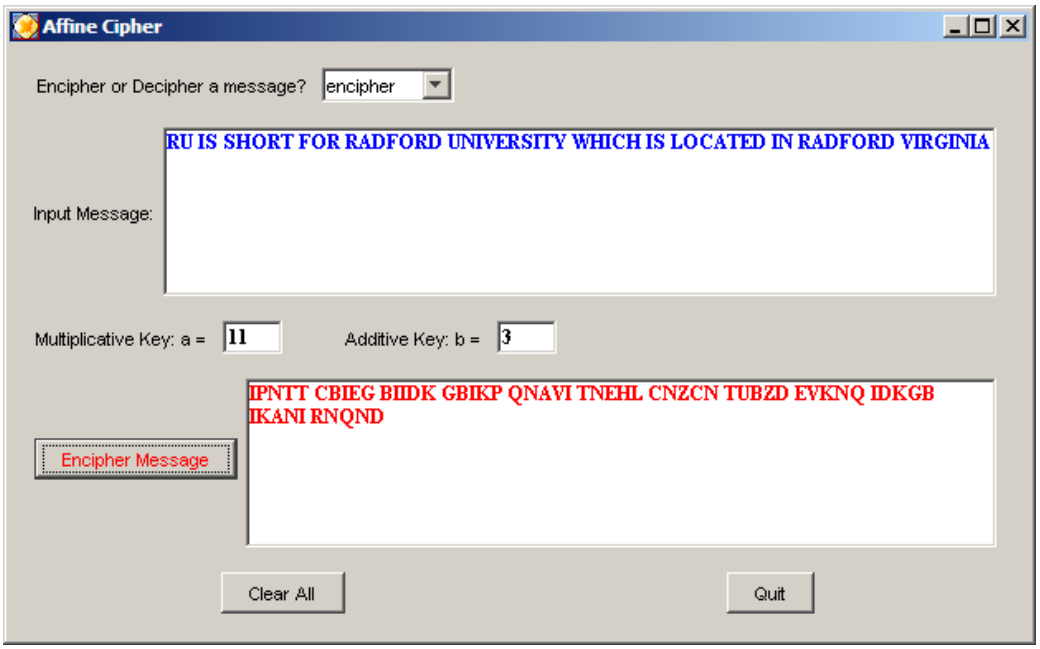

Figure 1: Encipherment of a Message using the affine cipher Maplet

Thus the ciphertext is "IPNTT CBIEG BIIDK GBIKP QNAVI TNEHL CNZCN TUBZD EVKNQ IDKGB IKANI RNQND". Note that for the plaintext, the affine cipher Maplet will strip out any characters (in this case spaces) that are not a part of the plaintext alphabet (which consists of the capital letters A..Z). The ciphertext will be displayed in blocks of 5 characters to increase legibility.

The process of deciphering a message involves recovering the plaintext message from the ciphertext. Mathematically, we take (1) and solve for the variable x. The solution of this equation is given by

$$x \equiv a^{-1}(y - b) \pmod{26}$$

Thus, for $y \equiv 11x + 3 \pmod{26}$, the decipherment formula is found to be

$$x \equiv 11^{-1}(y - 3) \pmod{26}.$$

Using basic concepts in number theory, it can be shown that $11^{-1} \pmod{26} \equiv 19$ and $-3 \pmod{26} \equiv 23$. Thus, the decipherment formula becomes

$$x \equiv 19(y + 23) \pmod{26}.$$

For example, to decipher the ciphertext "IP", we perform the following computations to recover the plaintext message "RU".

$$\text{I} \Rightarrow \quad y = 8 \Rightarrow \quad x \equiv 19(8 + 23) \pmod{26} \equiv 19(31) \pmod{26} \equiv 589 \pmod{26} \equiv 17 \Rightarrow \quad \text{R}$$
$$\text{P} \Rightarrow \quad y = 15 \Rightarrow \quad x \equiv 19(15 + 23) \pmod{26} \equiv 19(38) \pmod{26} \equiv 722 \pmod{26} \equiv 20 \Rightarrow \quad \text{U}$$

The plaintext message for the ciphertext "IPNTT CBIEG BIIDK GBIKP QNAVI TNEHL CNZCN TUBZD EVKNQ IDKGB IKANI RNQND" can be easily recovered using the affine cipher Maplet. To do this, we specify the **decipher** option as the first parameter in the affine cipher Maplet, enter the message, enter the values 11 and 3 for *a* and *b*, and click the **Decipher Message** button. Figure 2 demonstrates what will be seen.

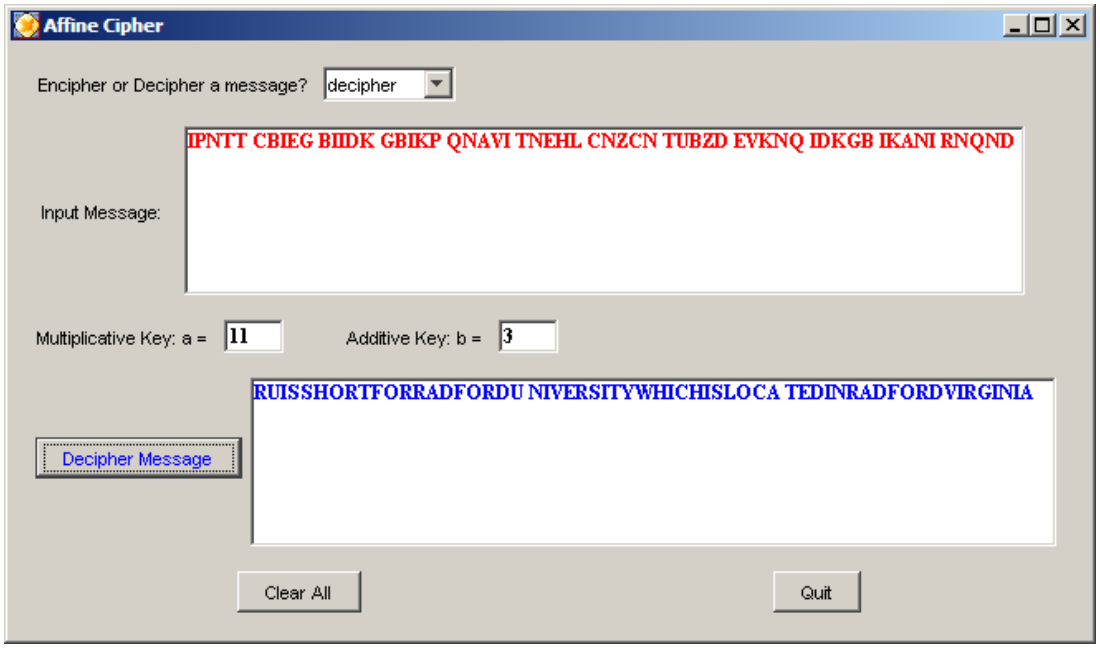

Figure 2: Decipherment of a message using the affine cipher Maplet

It is worth noting that if the user attempts to encipher a message where $\gcd(a, 26) \neq 1$, the affine cipher Maplet will inform the user of this requirement and not encrypt the message. An example can be seen in Figure 3.

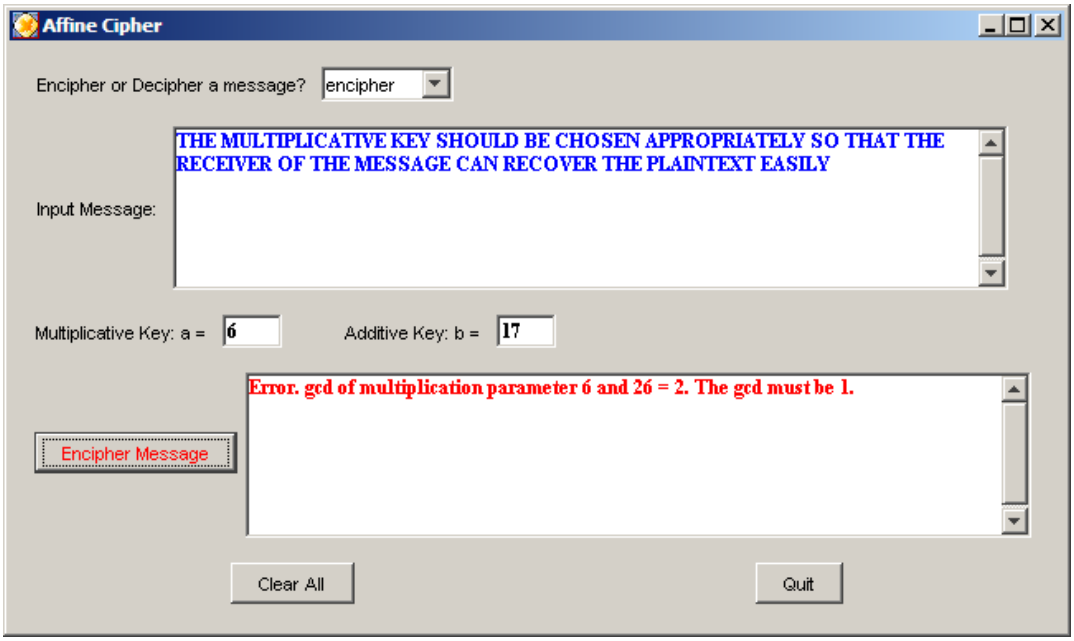

Figure 3: Encryption attempt without proper multiplicative parameter *a*.

Cryptanalysis is the process of an enemy trying to intercept and break an encrypted conversation between two correspondents. Affine ciphers are vulnerable to *frequency analysis*, which uses the fact that the most frequently occurring letters in the ciphertext produced by affine cipher has a good chance of corresponding to the most frequently occurring letters in the standard English alphabet. The most frequently occurring letters in English are E, T, A, O, I, and N. By setting up a one-to-one correspondence between the frequently most occurring letters in English and the most frequently occurring letters in the ciphertext, a message can be broken fairly quickly.

For example, suppose we want to cryptanalyze to message "EZORH AUZWR LOUCP MQQAS MJCEM WRRBC EWHCA JQADS WHLMS WHCEQ HLWHE WJNMH WYULH HAWPW ZCMHO ADBMP MBQCJ EBYVC JUUMJ MZWBM VYEWH CAJHL MNAAK NOHLA SWQNW ZZCJH ZAVYE HCAJH AEZOR HABAU ORZAP CVMQW JCEMZ MQAYZ EMDAZ HMWEL CJUHL CQQYN TMEHW QWUMJ MZWBM VYEWH CAJEA YZQM", which was encrypted by an affine cipher. Figure 4 (next page) demonstrates a Maplet designed to assist in breaking affine ciphers. In this window, the ciphertext message is entered and the **Frequency Letter Count** button, which displays the frequency in descending order of all letters occurring in the ciphertext, is clicked.

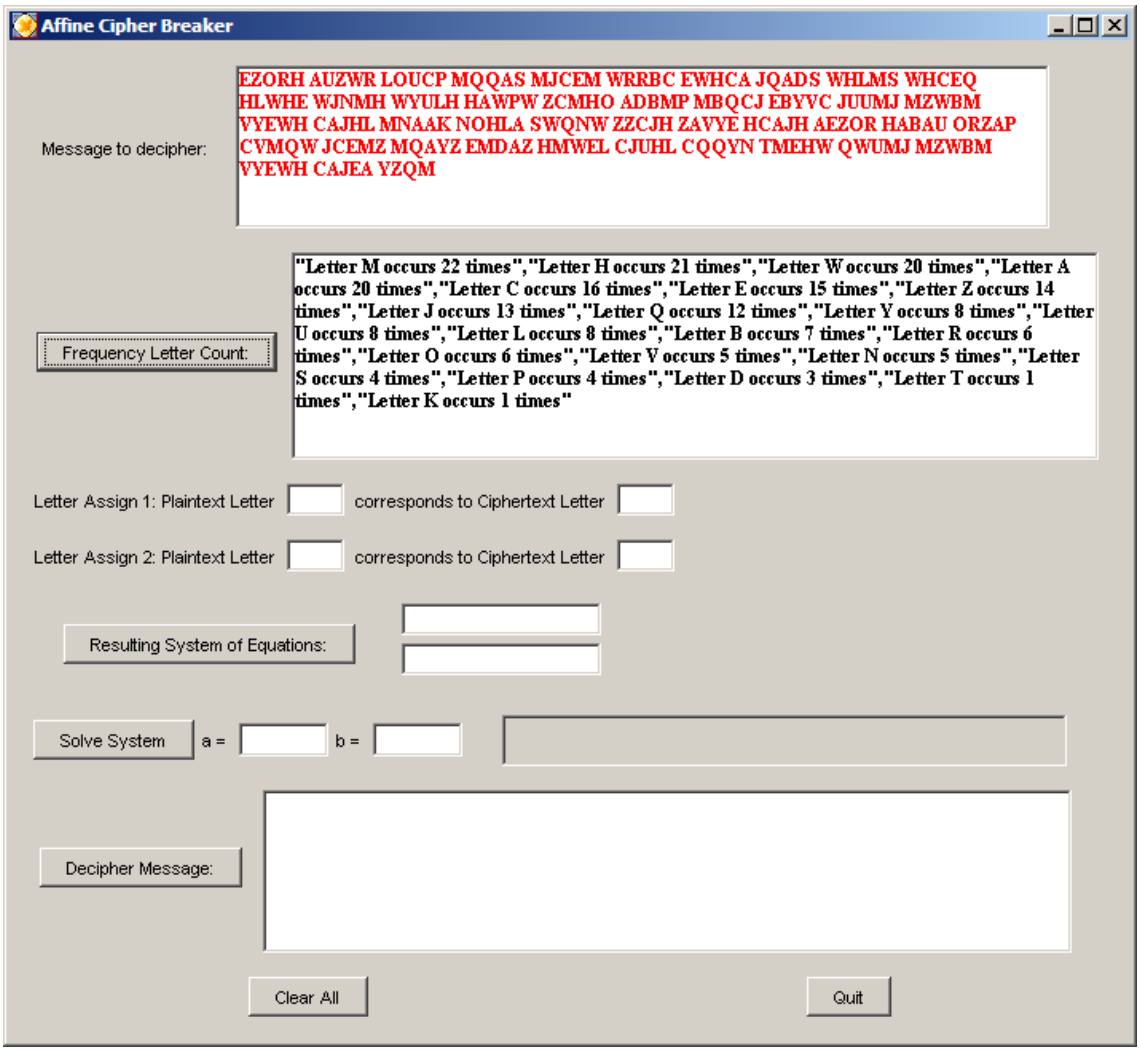

Figure 4: Affine cipher breaker Maplet with frequency count.

Since M and H are the most frequently occurring ciphertext letters, we suspect that these letters most likely would correspond to the most frequently occurring letters in the English alphabet, E and T. Suppose we assume that E was enciphered as M and that T was enciphered as H. In the alphabet assignment, E is represented by 4 and M as 12. Setting $x = 4$ and $y = 10$ in (1) gives the first equation

$$12 \equiv (a(4) + b) \bmod 26 . \tag{2}$$

Also, T is represented by 19 and H is represented by 7. Setting $x = 19$ and $y = 7$ gives the equation

$$7 \equiv (a(19) + b) \bmod 26 . \tag{3}$$

Combining equation (2) and (3) gives the system of equations

$$4a + b \equiv 12 \pmod{26}$$
$$19a + b \equiv 7 \pmod{26}$$

By placing the appropriate letters in the affine cipher breaker Maplet and clicking the **Resulting System of Equations** button, we can set up the system of equations. Then by clicking **Solve System** and **Decipher Message**, we can then see if the right values of *a* and *b* have been found in order to break the message. Figure 5 illustrates the result.

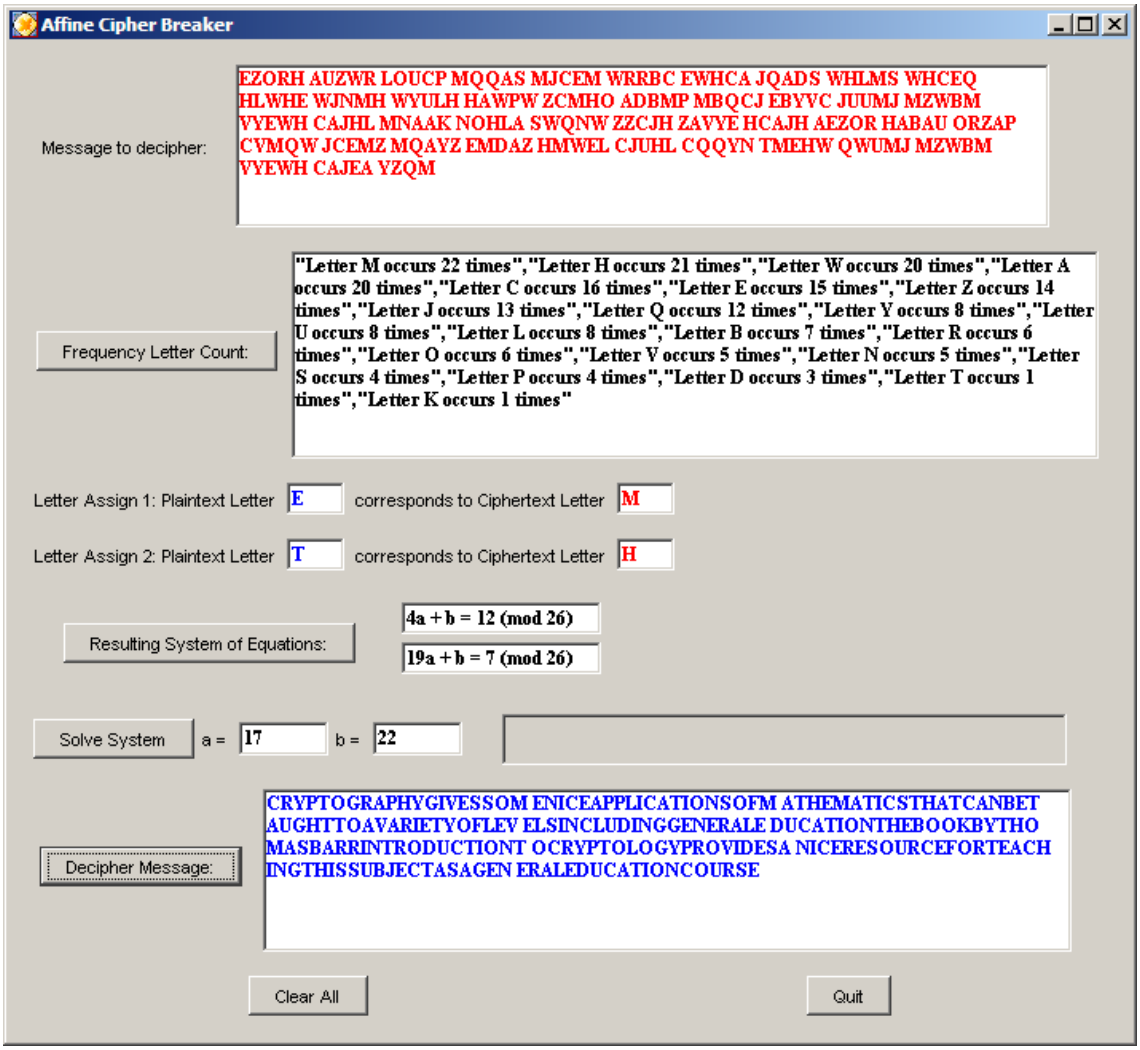

Figure 5: Affine cipher breaker Maplet cryptanalysis example.

Hence, the plaintext is "CRYPTOGRAPHY GIVES SOME NICE APPLICATIONS OF MATHEMATICS THAT CAN BE TAUGHT TO A VARIETY OF LEVELS INCLUDING GENERAL EDUCATION THE BOOK BY THOMAS BARR INTRODUCTION TO CRYPTOLOGY PROVIDES A NICE RESOURCE FOR TEACHING THIS SUBJECT AS A GENERAL EDUCATION COURSE". If the correct plaintext is not found, different assignments between highly frequently occurring letters can be applied until the correct combination is found.

3 Using Maplets in the Classroom

The affine cipher and other Maplets have been successfully tested in the general education course offered by the Honors Academy at Radford University involving cryptography. Students have successfully used these Maplets to encipher, decipher, and cryptanalyze messages. These Maplets have also given students the opportunity to communicate with each other using encrypted messages on discussion boards involving the use of Blackboard in a wireless setting. Figure 6 displays a sample discussion board provided by students working in groups using an affine cipher with a key of their choice.

Figure 6: Sample Blackboard encryption discussion.

The use of Maplets has greatly enhanced the ease of using technology in this class. Students, with the use of a tablet or laptop with wireless capabilities, have been able to use the Maplets in conjunction with the Blackboard discussion boards to simulate the techniques and issues involved with performing encrypted communications.

Besides affine ciphers, other Maplets to perform more advanced and modern encryption methods, including the RSA and AES cryptosystems, can be found at [Sigmon, 2007]. There is a strong likelihood that this technology can be used to enhance the implementation of other cryptographic algorithms, which will be a topic of future work.

4 Conclusion

The purpose of this paper is to demonstrate how Maplets together with wireless technology can provide an easy to use technology resource for enhancing the teaching and learning of cryptography. This technology should be of high interest to instructors wanting to teach general education and more advanced courses in cryptography. Students will benefit by having an easy to use technology resource for performing the large amount of computations required without the burden of having to use and understand complex programming languages and deep mathematical concepts.

For more information on cryptography and ways of teaching it to a general education audience, consult [Barr, 2002]. A more advanced discussion on cryptography and the use of Maple can be found in [Klima, 2007]. More information concerning the honors course in cryptography taught at Radford University can be found by consulting [Sigmon, 2007]. Demonstrations of how the Maplets can be used in conjunction with Blackboard can be found by contacting the author by electronic mail.

References

[1] Barr, Thomas H., 2002. *Invitation to Cryptology*, New Jersey, Prentice Hall, Inc.

[2] King, Joseph S., 2007. Radford University Honors Academy Website: https://php.radford.edu/~honors/

[3] Klima, Richard E., Sigmon, Neil P., and Stitzinger, Ernest L., 2007. *Applications of Abstract Algebra with Maple and MATLAB,* Taylor & Francis Group, LLC.

[4] Sigmon, Neil P., 2007. Course Website: http://www.radford.edu/~npsigmon/courses/cryptography/crypthome132.html .