Improving Student Learning Outcomes by Using an Applet In Class

Dr. Russel O. Carlson
rcarlson@byuh.edu
Department of Mathematics
BYU – Hawaii
U.S.A.

Abstract

With the availability of computers in the classroom, a variety of active learning methods can be used to teach mathematics. This paper presents an example of using an applet to teach a mathematical principle during a unit on cryptology. As part of this unit, two sections of a general education math course were taught how to break the Vigenère cipher using an applet, one by lecture and demonstration of the applet, and the other by allowing the students to experiment with the applet for themselves. The students who had learned by experimenting with the applet retained more knowledge of the process used to break the code than those who had learned by lecture and demonstration. This paper discusses the Vigenère cipher and the method of teaching it using the applet, and summarizes the difference in outcome between the two sections of the course.

Introduction

Much research has been done on active learning in STEM (Science, Technology, Engineering and Mathematics) education. For example, Boswell et. al. [1], Goodwin et. al. [2], Prince [3], and Freeman et. al. [4] provide a tiny slice of a large body of research into active learning in higher education. Recently, I had an opportunity to run a comparison of active learning and traditional lecture for myself to observe the benefits of active learning.

While I was at a conference in Atlanta a colleague, Paul Jenkins [5], presented a talk using a web applet (https://bit.ly/2IEN0u1) which very clearly demonstrated the process by which you would break the Vigenère cipher, a popular cipher that was used by the Confederacy in the US Civil War. After being introduced to this applet, I wanted to try using it in the classroom to teach cryptology.

This past semester I taught two sections of a quantitative reasoning class and included a short unit on cybersecurity near the end of the course. This is a topic students often enjoy, and it introduces some useful mathematics. As a part of this course, the Vigenère cipher was presented as a way to demonstrate cryptosystems and keywords in a way that would be easy for the students to understand. I decided to use the applet in a different way in each section. In one section, I demonstrated how to break the Vigenère cipher using the applet, while in the other section I had the students use the applet themselves. As expected, the students that had engaged with the applet retained the information better than the students who had only observed it being used.

The Vigenère Cipher

An easy way to encode English is to shift the alphabet by a certain number of letters. For example you can take a message and replace all the letters with those that are two letters down. A would become C, B would become D, etcetera. This is the kind of cipher that Caesar famously used to send information to his generals. Many of the students were familiar with this cipher, which made it a good place to begin the discussion. This cipher is also very easy to break. Simply do a statistical analysis of the letters. The most common letters of the coded message will likely be E, T, S, and A when decoded. A little trial and error will reveal the amount of shift and make the message decipherable.

In 1553, Giovan Bellaso [6] introduced a variation on the shift cipher to make it much more secure. Now known as the Vigenère cipher, this cipher uses a keyword. The first letter of the message is encoded with a shift cypher that would replace A with the first letter of the keyword. If the keyword was DOG, then the first letter of the message would be encoded with the shift cipher that replaces A with D. The second letter of the message would be encoded with the shift cipher that turns A into O, the third letter of the message would be encoded with the cipher that turns A into G. For the fourth letter, now that we have reached the end of the keyword, the process begins again and the shift cipher turns an A into D. In this way the encoded text does not show the distribution of letters usually seen in English. Instead, the distribution is more evenly distributed. This makes the cipher more difficult to break.

Message →	I	L	I	K	E	D	O	I	N	G	M	A	T	H
Keyword →	D	O	G	D	O	G	D	O	G	D	O	G	D	O
Ciphertext →	L	Z	O	N	S	J	R	W	T	J	A	G	W	V

The Vigenère cipher is an accessible way for students to understand how more secure codes can be built from simpler codes, as well as how keywords can be used to build these codes. Also, it becomes obvious that a longer keyword would be more secure and would more effectively even out the distribution of letters.

Kasiski [7] was the first to publish a method to break the Vigenère cipher in 1863, although Charles Babbage had done it earlier but failed to publish. Once computers became more common, automated methods of breaking the code made it too insecure for most purposes. The mathematics of these methods can be found in many textbooks about cryptology such as "Making, Breaking Codes" by Paul Garrett [8] and "Invitation to Cryptology" by Thomas Barr [9].

The Vigenère cipher can be adapted into an unbreakable code called a one-time pad, where the key is a string of random letters, is longer than the message itself, and is never used twice. The one-time pad is a code in use today for very secure transactions. For example, Los Alamos National Laboratory employs a system that uses one-time pads in their quantum network to create effectively unbreakable security [10]. Once students understand the Vigenère cipher and

its weaknesses, it is easier for them to understand how the one-time pad eliminates these weaknesses and becomes unbreakable.

The Applet

The way the applet works is as follows. The encoded text can be entered into the applet or a sample text can be used. The applet then generates histograms based on letter counts and compares them to the histograms of typical English texts as seen in the following figures.

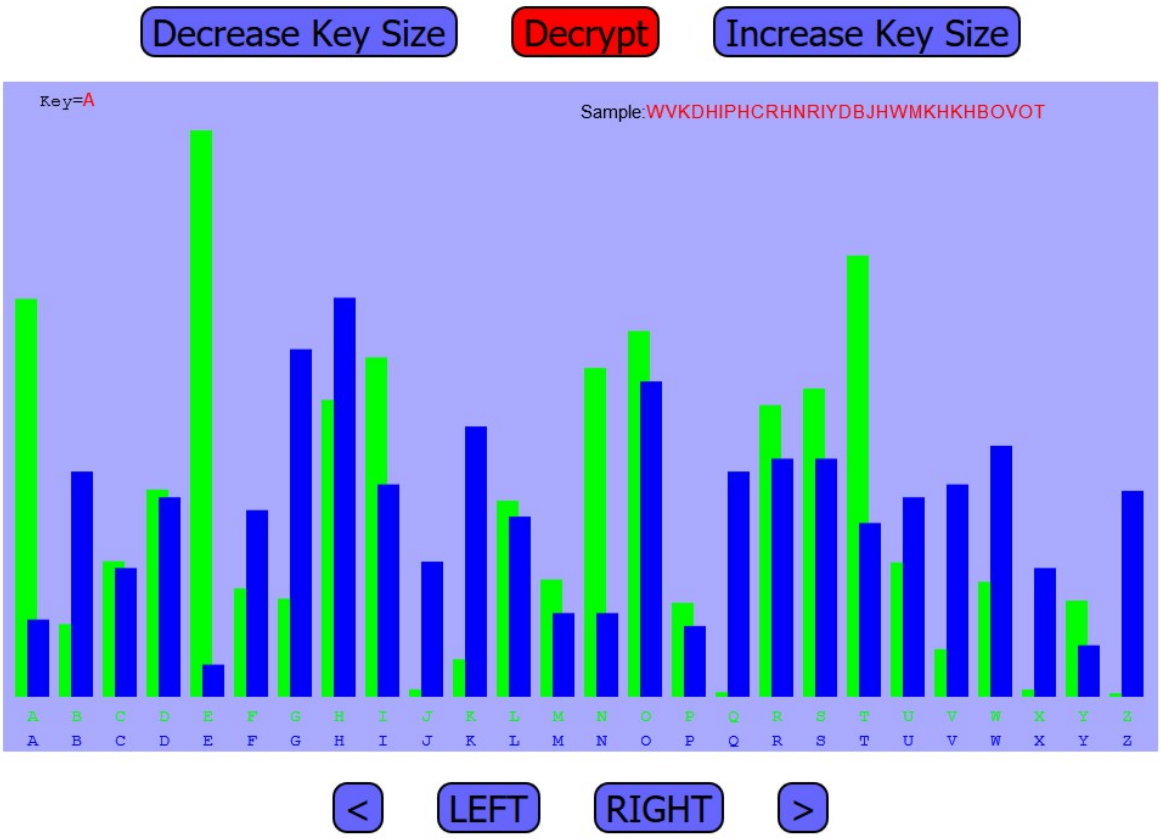

Fig. 1 In this figure the light green histogram represents the distribution of letters in English. The dark blue histogram represents the distribution of letters in the encoded message. Notice how the dark blue lines show a more even distribution while the green lines have a very distinctive pattern.

In order to break the cypher, start by looking at the frequency of letters in the encoded message. If the distribution of letters does not have significant spikes in letter frequency, as does English, then try looking at every other letter. If the distribution of these letters still doesn't have any letters that occur significantly more frequently, try every third letter, and so on.

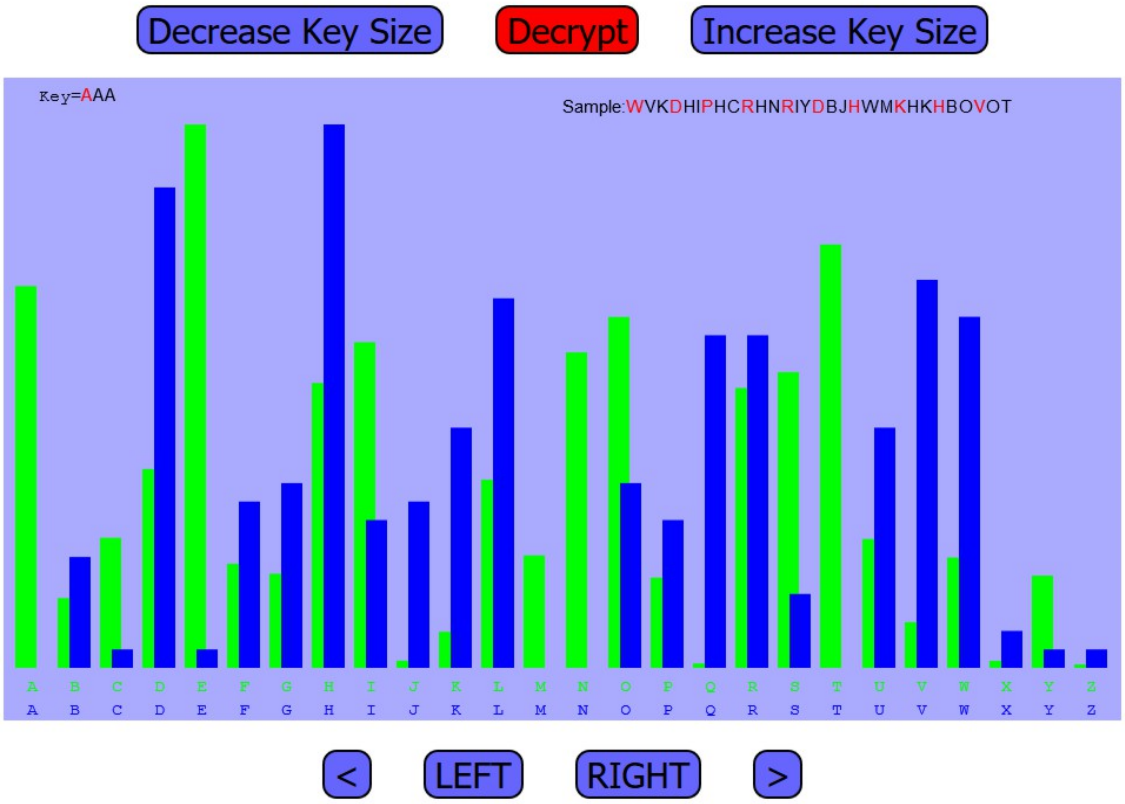

Fig 2. By choosing every third letter, a distinctive pattern emerges in the dark blue histogram. This indicates that the keyword is three letters long.

When you reach the length of the keyword, the distribution of letters suddenly becomes more sharply varied and mimics the distribution found in English. By a quick analysis of this distribution it is easy to see what the first letter of the key would be. Simply shift the distribution of the encoded letters to most closely match the distribution of letters in the English language. This will reveal the first letter of the keyword.

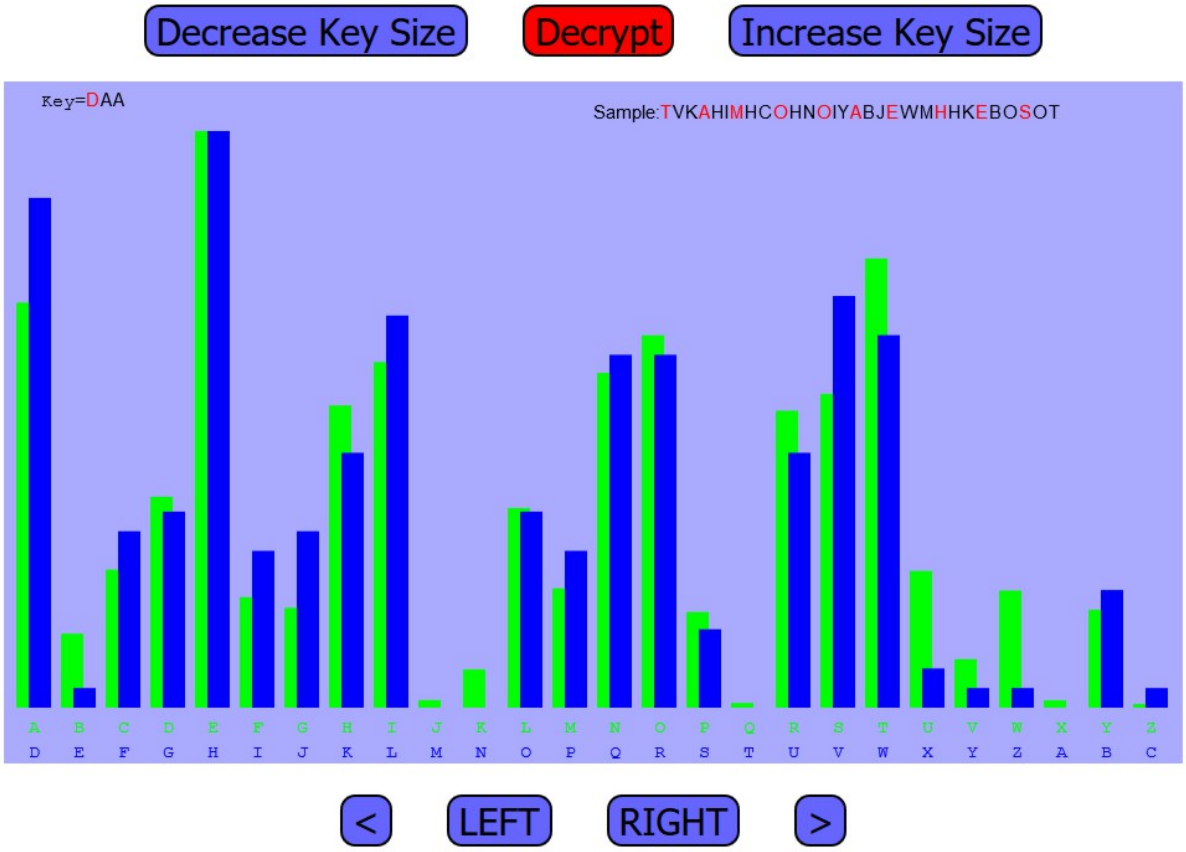

Fig. 3. We align the dark blue histogram with the light green histogram until the pattern matches, and by noting the amount of the shift, the first letter of the keyword is revealed.

Once the first letter of the keyword is found, look at the next set of letters in the code. Start with the second letter and then skip the length of the keyword to find the next letter, and so on. Look at the distribution of this second set of letters. Match those with the distribution of English until you have the second letter of the key. Continue this process until you have found the entire keyword and can then decode the full message.

Teaching Students to Decode the Vigenère Cipher

When I taught one of the two sections, which I will refer to as section A, I first demonstrated on the board what a Vigenère cipher was and how to encode a message using it. Then I brought up the applet and displayed it for the class. I went through in detail the process of breaking the code, and explained each step carefully as I did it. The whole process took fifteen to twenty minutes.

In the other section which I shall call section B, I again started by showing how to encode a message using the Vigenère cipher. I then brought up the applet and spent about 3 minutes demonstrating how to use it. I then had the class move to the computer lab and gave them 15-

20 minutes to try out the applet for themselves. Both processes took about the same amount of time.

A few days later I gave all the students an anonymous survey to see how well they had learned the material from the unit. One of the questions on that survey specifically asked about the process of breaking a Vigenère cipher. As expected, the students in section B were better at answering the question correctly than the students in section A, but I was surprised by the difference between the sections. Only 17% of the students in section A got the correct answer while 73% of the students in section B got it right.

Conclusion

After performing a small, informal experiment in teaching cryptology in a general education math setting, I gained some insight into the learning process of the students. I found that using an applet was an effective and engaging way to help students learn, and that it was important to have the students use the applet themselves. Even though I expected that students would learn more about breaking a cipher if they participated in the process rather than just watching a demonstration, I was surprised by the magnitude of the difference it made. It appears that certain skills benefit greatly from active learning experiences.

References

[1] Bonwell, C.C., and J. A. Eison, *Active Learning: Creating Excitement in the Classroom*, ASHEERIC Higher Education Report No. 1, George Washington University, Washington, DC, 1991.

[2] Goodwin L, Miller JE, Cheetham RD. *Teaching freshmen to think: does active learning work?* Bioscience. 1991; 41:719–722.

[3] Prince, M., *Does Active Learning Work? A Review of the Research*, Journal of Engineering Education, Vol. 93, No. 3,2004, pp. 223-231.

[4] Freeman S, Eddy SL, McDonough M et al. *Active learning increases student performance in science, engineering, and mathematics*, Proc Natl Acad Sci U S A. 2014;111(23): 8410–8415.

[5] Jenkins, Paul. *Broken One-time Pads and Other Projects*, Joint Mathematics Meetings, MAA Session on Cryptology for Undergraduates, January 4, 2017.

[6] Bellaso, Giovan Battista. *La Cifra del Sig. Giovan Battista Belaso*, Venice, Italy, 1553

[7] Kasiski, F. W. *Die Geheimschriften und die Dechiffrir-Kunst*, Berlin, (Germany): E.S. Mittler und Sohn, 1863.

[8] Garrett, Paul. *Making, Breaking Codes: Introduction to Cryptology*, Pearson, New York, 2001.

[9] Barr, Thomas. *Invitation to Cryptology*, Pearson, New York, 2002.

[10] *Government Lab Reveals It Has Operated Quantum Internet for Over Two Years*, MIT Technology Review, May 6, 2013.