Journal of Cybersecurity Education, Research and Practice

Volume 2017 | Number 1 Article 4

June 2017

How Much Should We Teach the Enigma Machine?

Jeffrey A. Livermore
University of Michigan-Flint, jlivermore@aol.com

How Much Should We Teach the Enigma Machine?

Abstract
Developing courses and programs in Information Assurance can feel like trying to force ten pounds of flour into a five pound sack. We want to pack more into our courses than we have time to teach. As new technologies develop, we often find it necessary to drop old technologies out of the curriculum and our students miss out on the historical impacts the old technologies had. The discipline is so broad and deep that we have to carefully choose what concepts and technologies we study in depth, what we mention in passing, and what we leave out. Leaving out important historical developments deprives our students of historical context and the evolution of technology into the profession. This paper presents an argument for including the Enigma Machine in our curriculum.

Keywords
Enigma

1. INTRODUCTION

The Enigma Machine is one of the most famous cryptography devices in the history of the profession. The Enigma machine marked a transition in the practice of cryptography from pure creativity to technology-based solutions. After World War I, it became apparent that cryptography had to move beyond simple substitution and book ciphers. Technology came to the forefront and electromechanical devices like the Enigma machine became popular. Both sides of the war used rotor-based devices with varying degrees of success during World War II.

Because of the great historical role that the Enigma Machine played in World War II, Enigma has been popularized in television, movies, and historical fiction. Many of our students have seen the movie U-571 and several of the other shows and historical accounts centered on the Enigma Machine. This historical knowledge is something that we, as cryptography instructors can exploit to our advantage and use to capture the attention of our students.

The Enigma Machine provides educators with the opportunity to raise a number of critical topics in the classroom including some history lessons, the role of technology in cryptography, and how cryptography has evolved with improvements in technology. There are numerous Enigma-based classroom activities and lab exercises that could provide students hands on experience with encryption and decryption.

Many instructors have had a great deal of success using history to set the context of their course material in a variety of disciplines (Williams, 2014). Placing current technologies and developments into a historical perspective can shed light on how they evolved from simple substitution ciphers to digital encryption algorithms.

2. HISTORICAL CONTEXT

There really is no one Enigma Machine. Enigma was a family of cryptography machines that were based on a series of rotating cipher wheels. The original Enigma machine was patented in 1918 to provide secure business communication (Smith, 2014). The Enigma was subsequently adopted by the military and played a significant role in the Second World War. Like most encryption technologies, the Enigma machine evolved as the military addressed weaknesses to make

Enigma more secure and easier to use. Different variations of the Enigma Machine were used during the war by Germany and Japan.

The Enigma machine was first deduced by Polish cryptographers who passed their information on the British government. The British government recruited Alan Turing and a team of cryptographers and code experts. Alan Turing led the invention of the Bombe device that helped defeat the Axis by breaking the Enigma Machine produced ciphertext. The Bombe was a brute force solution. The Bombe worked by simulating as many Enigma machines as possible. Attacking the Enigma machine with a Bombe machine shows that while brute force solutions may be inelegant, they can be effective.

After World War II, technology-based encryption devices continued to improve. The United States moved towards encrypted teletype devices like the SIGABA machine and Enigma transitioned from a state of the art device to become a historical footnote. The electromechanical Enigma machine was the bridge between ciphers and digital encryption algorithms.

3. CRYPTOGRAPHY CONCEPTS ILLUSTARTED WITH THE ENIGMA MACHINE

The Enigma Machine enables us to introduce a number of important cryptography concepts to our students while exploiting the popular media "sizzle" that surrounds Enigma. Some of the concepts that Enigma can illustrate are:

- The encryption advantage of polyalphabetic ciphers over monoalphabetic ciphers.
- The evolutionary improvement of Enigma technology over time. The Enigma machines were constantly being improved just as Ron Rivest improved his string of ciphers from RC2 up to RC6.
- The emergence of a brute force solution to a cryptography problem (Bombe).
- How human error is always the weak link in the cryptography chain.

For many centuries, most ciphers were simple substitution ciphers using a single alphabet. Simple substitution ciphers can typically be cracked using letter frequency analysis. In any language, some letters are used more often than others and given enough ciphertext, letter frequency can betray the substitution mapping. Students who have seen the popular television game show *Wheel of Fortune* are familiar with this concept. The weakness of a monoalphabetic substitution cipher

was addressed by the Vigenere, and other ciphers that used multiple alphabets for substitution.

The Enigma machine does not use a simple substitution cipher. When a letter is typed into keyboard to be encrypted, a series of wheels are rotated to provide a brand new substitution alphabet for the subsequent letter. If the same plaintext letter is encrypted again, a different ciphertext letter will appear. Instead of using a large table with a manual process like the Vigenere cipher, the Enigma machine accomplishes the same result mechanically and quickly.

Just as Enigma was an improvement over prior polyalphabetic ciphers, the Enigma machine itself was improved several times before and during the course of World War II. To simplify the operation of Enigma, the military added lights to indicate the machine's progress. When the Germans suspected that their code had been broken they added an additional rotor wheel to Enigma which increased the security by an order of magnitude. This is the nature of cryptography. When an algorithm is broken, a new and improved algorithm is developed. It is a never ending cycle of good guys trying to stay ahead of the bad guys.

The security of the Enigma Machine was basically broken by cryptographers when they developed the Bombe after getting information from Polish scientists and cryptographers. The Bombe was a brute force solution that tried all possible rotor combinations. Anyone who has worked on dictionary attacks or applications like Jack the Ripper will see the parallels. Students may have only seen brute force attacks by criminals and will have to do a paradigm switch to accept brute force applications as a defensive tool.

Defeating the Enigma machine was a massive project. At one point, there were over 1,000 people trying to decrypt Enigma messages (DeBrosse & Burke, 2004). There was an American team working near Dayton, Ohio and a British team working at Bletchley Park near London. These teams included mathematicians, scientists, engineers, and military personnel. The two teams did not always work well together and each suspected the other of compromising the security of the project. The role of Alan Turing in defeating the Enigma machine and the start of the digital era is an interesting sidebar that can be introduced through classroom discussions.

One of the best tools that instructors have in the classroom is a concrete example of the principle we are trying to teach. You cannot teach cryptography without pointing out that the user is always the weak link. This is perfectly illustrated by the Enigma machine. The demise of the Enigma machine was

ultimately due to human error. German military staff got lazy and did not maintain key security. The original plan was to use key settings that changed every day and avoid repeated phrases (Smith, 2014).

The basic design of the Enigma machine served as the basis for the Hummingbird encryption algorithm (Engels, Fan, Gong, Hu, & Smith, 2010). Enigma's algorithms were able to be used for encryption in resource-constrained devices. This is an example of how old ideas can be reworked to solve current problems with new technologies. The practice of cryptography has been a never ending cycle of improved encryption methods followed by improved cryptanalysis. The Enigma machine is a great example of technology improving.

4. PEDAGOGICAL POSSIBILITIES

Many instructors like to utilize videos in their classrooms to break up long lecture sessions. There are dozens of videos about the Enigma Machine hosted on YouTube. These videos can be used in the classroom and within online classes. Instructors simply need to select the videos that most closely match their curriculum and lesson plans and put them to use. Table One lists several of the author's favorites among the thousands of videos that were available on YouTube in March, 2017. In addition to videos, there are many books, articles, movies, and Websites dedicated to the enigma machine.

Video Name	Length	Content
Enigma Machine – Andy Eggebraaten	2.5	How a student built an Enigma Machine for a science fair project
How Was Hitler's Enigma Machine Cracked?	3	Historical videos of Alan Turing's work at Bletchley Park
Enigma Machine Spreadsheet	3	How to replicate Enigma functionality with modern software
The Turing Bombe – Cracking Enigma	12	A demonstration of a Bombe replica with visible working parts
The Inner Workings of an Enigma Machine	14	A discussion of the rotors and inner workings

Table 1: YouTube Videos on the Enigma Machine

The Enigma Machine was a central character in the movies *U-571* and *Imitation Game*. *U-571* is a fictional account of capturing an Enigma Machine. The movie is very dramatic and action packed. Many of the facts are not historically accurate but the importance of the Enigma Machine to the German

war effort is emphasized. The Bombe and the decryption effort was the central "character" in the movie *Imitation Game*. These movies make cryptography exciting and challenging. Instructors can assign or recommend that students watch these films. There are not many areas of modern cryptography that have movies made about them which can capture the attention of our students like the Enigma Machine already has.

5. PRACTICAL LAB EXERCISES

A number of programs are trying to incorporate more hands-on exercises into their curriculum. Faculty that want to get away from the traditional "sage on a stage" format will find that the Enigma machine offers a variety of options for lab activities. There are several excellent simulators that students can use. The author has had great success with the EnigmaSim v7 developed by Dirk Rijmenants. Some are embedded in Websites and others can be downloaded and installed on student computers. Simulators have been used to help students develop an understanding of how difficult key management can be. Students can be required to develop a set of monthly tables containing rotor settings and establish a schedule of encryption keys.

Using a simulator can really illustrate the inner workings of the Enigma Machine. Students will have to select which rotor wheels to use and what plug settings to make. Manipulating these settings makes it simple for instructors to alter assignments from semester to semester to make it more difficult for students to collect answers from friends who have previously taken the course. Hands-on exercises can help kinesthetic learners grasp concepts that they might never have learned through listening to a lecture or reading from a text.

If your program is a hands-on program, requiring students to install an Enigma emulator is an excellent way for the students to gain experience in software installation. The emulators are quick installs with no known risk. Running the emulators in a lab exercise gives students an appreciation of encryption before it was computerized.

It is very simple to pick a series of rotor settings and encrypt a series of simple text messages. You can ask the students to encrypt a plaintext message and then decrypt one of your ciphertext messages. These messages can be used for several semesters without repetition. This type of lab exercise is very easy to empirically assess.

The mechanical rotor system of the Enigma machine makes it an ideal candidate for a coding assignment if your students have coding proficiency. Writing software that emulates an Enigma machine has been done at a number of colleges. A few minutes with a search engine can locate all of the specifications and rubrics.

Assigning students to calculate the number of possible combinations are possible with an Enigma Machine. Students can be asked to calculate the possibilities for

- An Enigma Machine with one rotor
- An Enigma Machine with two rotors
- An Enigma Machine with three rotors
- An enigma machine with three rotors and ten plug combinations

This mathematical exercise illustrates the challenges of launching a brute force attack or defense. The exercise can also show students that mathematics is the key to understanding cryptography and computer science (Singh, 2003). Depending on school politics, programming an Enigma machine might be the basis for a cross-disciplinary project between the math and computer science departments.

6. PAPER WRITING ASSIGNMENTS

There is a lot of material available on the Enigma Machine to build a lesson or paper writing assignment round. There are numerous images, videos, emulators, and articles about the Enigma Machine. Students can be asked to write papers about the Enigma Machine and there is no doubt that they can find adequate supporting materials. Papers could be assigned on:

- Military versus commercial applications
- The evolutionary process of cryptographic technologies
- The defeat of a cryptosystem
- The role of Enigma in popular media
- The career and accomplishments of Alan Turing
- This case study of a brute force attack on a cryptosystem

Any of these topics can be turned into a robust academic paper. The length and rigor of the paper would vary depending on how much “space” in the curriculum that is assigned to the Enigma Machine.

7. CONCLUSIONS

It is tempting to gloss over the history of our profession and concentrate on the amazing new technologies coming out on an increasingly frequent basis. The Enigma machine was a significant development in the history of our profession. Enigma was important because it heralded the arrival and adoption of computing technology into cryptography and should be taught. Enigma is important as a historical foundation and an illustration of important cryptographic concepts. Educators can use Enigma to teach history, important concepts, and the evolutionary nature at the heart of cryptography.

Engels, D, Fa n, X., Gong, G., Hu, H., & Smith, E. (2010). Hummingbird : Ultra-Lightweight Cryptography for Resource-Constrained Devices. *Lecture Notes in Computer Science Volume 6054*, pp 3-18.

DeBrosse, J., & Burke, C. (2004). The secret in building 26: The untold story of America's war against the U-boat Enigma codes. Random House.

Singh, S. (2003). Cryptogrphy in the classroom. *Mathematics Teaching*. 9-12.

Smith, C. (2014). How I learned to stop worrying and love the Bombe: Machine research and development at Bletchley Park. *History of Science*. 52(2), 200-222.

Smith, N. (2014). Classic Project. *Engineering & Technology*. 9(11), 42-43.

Williams, J. (2014). Teaching the professions. *Radical Teacher*. 99, 69-75.