The Daily Breaking of Enigma: A Student Project

Stuart Boersma ; Stuart.Boersma@cwu.edu
Central Washington University

This paper give a brief overview of the Polish attack on Enigma and presents an undergraduate class project that lets students experience the type of cryptanalytic work that the Polish codebreakers performed on a daily basis. The project can be tailored to a variety of difficulty levels depending on the number of hints and the type of scaffolding provided. Additionally, three curricular frameworks that allow for the teaching of the Polish attack on Enigma will be presented.

Keywords: Enigma, Marian Rejewski, Polish codebreakers, student project

Introduction

The story of the breaking of Enigma offers one a rich, complex, and intriguing context to teach a variety of cryptologic techniques and explore historical cryptology. A course that covers the details of the complete story of Enigma would clearly take an enormous amount of time. However, a course, or a module in a course, focusing on the work of the early Polish codebreakers is accessible to a wide audience of students, tells a forgotten story in which mathematicians are war heroes, and allows students to see how clever and careful thinking can solve seemingly unsolvable problems. I have taught this topic to undergraduates using a variety of course structures (see below) and have recently created a culminating project that allows students to experience the daily process the Polish codebreakers used for deducing the daily Enigma keys. This paper's main goal is to share this project along with some course structures where the Polish codebreaker's story can be explored and appreciated. However, in order to understand the mechanics of the project, one must understand some of the details surrounding the codebreaking techniques developed by Marian Rejewski, Jerzy Różycki, and Henryk

Zygalski in the 1930s.

The next section of the paper will present three different curricular settings in which this author has introduced students to the story of the Polish breaking of Enigma. The section "Polish Codebreaking" will give some of the details of the codebreaking techniques developed and used in the 1930s by the Poles and how these techniques are incorporated into the Enigma Project. The section "Project Logistics" will provide logistics for implementing this project in a class and provide readers with suggestions for increasing or decreasing the difficulty level of the Enigma Project.

Innovative Cryptology Curricula

Enigma in the Classroom

The story of the Polish codebreakers is appealing to many students. The complexity of the Enigma machine can be explored in many lower-level mathematics courses and the mathematical details can be carefully investigated in an upper-level mathematics course. However, the historical story of Enigma is naturally interdisciplinary and many of the details can be explored and understood by students without any significant undergraduate mathematical background. The full story of the Polish codebreakers includes classic espionage, secret agents, daring escapes, and, sadly, some unfortunate deaths. It is a story that deserves to be told and cryptologists and mathematicians are perfectly suited for bringing the details of this adventure to our students.

I have taught about Enigma and the work of the Polish codebreakers in three different curricular settings:

(1) A 10-week seminar meeting once a week.

(2) A two-week module in an upper level undergraduate mathematics class covering the broad historical development of cryptology.

(3) A two-week module in a Cryptology and Privacy course for non-STEM students offered through [author's University]'s Honors College.

10-week seminar

For those who teach in a department that offers regular seminars with varying topics, consider offering one on Enigma! Such a seminar can attract mathematics majors or bring an exciting topic to mathematics majors, computer science majors, or any other interested students. While this author's seminar did not assume any specific mathematical preparation, the audience consisted of mathematics majors from first-year students up through seniors. The class met once a week over Zoom for 50 minutes. The Enigma Project, described later in this paper, was used as a culminating activity for this seminar in Spring 2021. Table 1 shows a brief outline of topics covered each week.

Week	**During Class**	**After Class**
1	Build a Pringle can Enigma. Learn about the components of Enigma. Practice using Pringle can Enigma	Observe similarities/differences between the wirings of the rotors and reflector. Use Pringle can Enigma to encrypt a short word. Notice that the same setting appears to both encrypt and decrypt.
2	Small group activities to count the number of ways to wire a rotor and a reflector. Determine how many ways one could build an	Students practice encrypting and decrypting short words with Pringle can Enigma.

	Enigma with three rotors and a reflector.	
3	Create a simple mathematical model of Enigma and state theorem which claims conjugate permutations have the same cycle structure. Thus, every Enigma permutation simply swaps 13 pairs of letters. Small group activity to count the number of plugboard connections. Count the number of possible daily keys.	Students use standard frequency analysis techniques to break a MASC (preserving word length).
4	Finish counting the number of daily keys and look at the effectiveness of a brute force attack on Enigma. If all messages for a single day were sent with the same key, an "in depth" attack is possible (much like a MASC). Introduce the early German "indicator" method of encrypting a randomly chosen session key twice.	Students practice using the indicator method to encrypt and decrypt messages to/from each other or the instructor.
5	Introduce cycle notation for writing permutations. Begin following the Polish method of identifying the three product permutations using a collection of encrypted session keys.	Use encrypted session keys to determine the three product permutations.
6	Learn how to factor permutations and count	Practice factoring permutations.

	the number of possible factorizations.	
7	Learn about the Poles construction of a catalog of rotor positions and cycle structures. Practice identifying certain session keys from a large collection of encrypted session keys.	Begin final Enigma Project
8	Use crib dragging to identify possible crib placement. Use cribs to deduce plugboard connections.	Continue work on Enigma Project.
9	Brief overview of Rejewski's work on solving the wiring of the "fast" rotor.	Continue work on Enigma Project.
10	Brief historical wrap up of Enigma: Germany abandoning the indicator method; Poles devising new methods to recover keys. Turing and Bletchley Park. Elizebeth Smith Friedman's work in South America.	Finish Enigma Project

Table 1: Brief outline of 10-week seminar

Mathematics Major Course

While not common, some mathematics departments are able to offer a Cryptology course on a regular basis. Central Washington Univeristy offers a junior-level Cryptology course every two or three years that satisfies an elective credit towards the mathematics major. This course covers the broad historical development of cryptology

from Caesar ciphers up through RSA and Elliptic Curve Cryptography using (Bauer, 2013) as the textbook. This course spends about ten days on Enigma and the Polish codebreaking efforts. Unlike the 10-week seminar, since the students are more advanced mathematics majors, we are able to study Rejewski's algebraic approach to deducing the wiring of the "fast" rotor in addition to all the topics covered in the 10-week seminar.

Non-STEM Honors Course

The Honors College at Central Washington University offers a few variable topics courses in their curriculum. One such course, Integrated Learning, is tasked with taking an interdisciplinary approach to examining social, economic, technological, ethical, cultural, or aesthetic implications of knowledge. I designed a course titled "Ciphers, Secret Communication, and Personal Privacy" which examines the historical development of ciphers and other forms of secret communication. Throughout the course, students learn how linguists, mathematicians, and computer scientists have broken "unbreakable" ciphers and how technology has given us tools to encrypt all our thoughts while simultaneously exposing our private lives across social media. One component of this course requires students to conduct a small independent research project on an approved topic related to cryptology and privacy. Some topics that students have explored include Herbert Yardley and the Black Chamber, Philip Zimmermann and PGP, the Clipper Chip, the Snowden disclosures, the right to privacy and the 4th amendment, privacy under the Trump administration, and the Signal app. Of course, one component of this course is also the study of Enigma and the story of the Polish codebreakers. While this course does not have any specific mathematical prerequisites, students are still able to master many of the skills that the Polish codebreakers used on a daily basis: identifying the product permutations, factoring

permutations, identifying possible crib placements, and using online Enigma simulators to encrypt and decrypt messages. The next time this course is offered, the Enigma Project will be integrated into this module.

The exciting and unbelievable story of the Polish codebreakers can be woven into a variety of college courses and used to bring the study of cryptology to a broader audience.

Polish Codebreaking

This section of the paper will primarily focus on the techniques developed by the Polish Cipher Bureau from 1932 to 1938 and are largely attributed to Marian Rejewski, Jerzy Różycki, and Henryk Zygalski. For more details on the individual contributions of each of these three codebreakers, please refer to a more comprehensive history of the breaking of Enigma such as (Hugh, 2000) or (Kahn, 2012).

The following sections will provide enough information about the Polish codebreaking techniques so one can understand the Enigma Project. However, readers are encouraged to consult (Christensen, 2007) and (Bauer, 2013) for more mathematical details regarding the Polish breaking of Enigma as well as a more complete description of the Enigma machine.

This paper will be discussing the techniques used by the Poles to break the early three-wheel Enigma (with plugboard) developed for use by the German Military. Marian Rejewski started working on breaking Enigma in 1932 (Rejewski, 1981). We will assume readers are familiar with the basic workings of an Enigma machine. That is, the rotors essentially turn over in a manner similar to a car's odometer each time a letter is encrypted, thereby ensuring that each letter of a message is being encrypted using a different mono-alphabetic substitution cipher (MASC) than any other letter in the message. Ultimately, each MASC that the Enigma performs is a product of

transpositions. That is, every Enigma cipher swaps 13 pairs of letters. This has the advantage that the same Enigma settings (initial rotor positions, plugboard settings, etc.) work both for encryption and decryption. If a sender and a receiver both have their Enigma machines set up the same way, the sender can type in plaintext to produce ciphertext and the receiver can type in the resulting ciphertext to recover the plaintext. In order to make sure all Enigma operators could send and receive messages, a codebook was distributed every month with daily keys. Each Enigma operator could look up the correct daily key and be sure that their Enigma machine was set up the same way as any other Enigma machine, thereby allowing for distant parties to securely communicate with each other. If one is teaching about Enigma in a mathematics course, counting the number of possible daily keys makes for a great assignment when studying permutations and combinations. A daily key is determined by the order the three rotors are placed into Enigma, the initial positions of each rotor, the ring settings, and the plugboard settings. In the end, there are over 7×10^{18} possible daily keys, which clearly makes any brute force attack on Enigma unlikely to succeed.

Of course, if hundreds of messages were being sent across Germany on any given day and all these messages were being encrypted using the same daily key, then an in-depth attack is certainly possible. If a hundred messages were all encrypted using the same daily key, then that means the first letter of each message was encrypted using the same MASC. The second letter of each message would be encrypted using a second MASC, and so on. Thus, one could conceivably use a frequency analysis attack to uncover the cipher alphabet used to encrypt the first letter of each message, and then the second letter, and so on. Thus, the Germans needed a way to make sure that 1) all Enigma operators could set up their machines to agree with all other operators and 2)

different messages sent on the same day were encrypted with different keys! The Germans solved this problem by using the "Indicator Method".

Indicator Method:

To encrypt a message on a given day, an Enigma operator would

(1) Set up their machine according to the daily key.
(2) Pick three random letters, like CWU, called the session key.
(3) Type the session key into Enigma, twice, thereby encrypting the session key, twice.
(4) Adjust the three rotors of their machine so the session key appears through the windows at the top.
(5) Use this unique setting to encrypt the message.
(6) The operator would then send (via Morse Code using a radio transmitter) the six letters of the session key twice encrypted followed by the encrypted message.

Of course, a receiving operator could reverse this process:

(1) Set up their machine according to the daily key.
(2) Type in the first six letters they receive. In this example they should get CWUCWU. The session key was likely encrypted twice to make it apparent if there were any transmission errors at this stage.
(3) Reset the rotors to CWU.
(4) Type in the ciphertext to recover the plaintext.

The Polish codebreakers were aware of the above protocol developed by the Germans and were able to exploit the fact that the session key was encrypted twice to break Enigma! To see the unintended weaknesses of the Indicator Method, we first need to

introduce some notation.

When an Enigma machine is set up according to the daily key, the first letter will be encrypted according to some permutation (of the 26 letters). We will call this permutation A. The second letter will be encrypted with a different permutation, call it B. Proceeding similarly we have:

A : first permutation

B : second permutation

C: third permutation

D: fourth permutation

E: fifth permutation

F: sixth permutation

Suppose Marian Rejewski intercepted the following first six letters of a message: QGF BQP. What does he know? Recall that QGF comes from three randomly chosen letters, each being encrypted with three different MASCs. We also know that those three randomly chosen letters were encrypted a second time with, again, three different MASCs to produce BQP. While it appears that one does not know much in this situation, a little clever thinking begins to unravel the secrets of Enigma!

Marian Rejewski does not know what the operator picked as his first letter, but permutation A sent it to the letter Q. Let us denote this fact by

$$A: ? \to Q.$$

We also know that permutation D sent this same unknown letter to B:

$$D: ? \to B.$$

Now comes the clever part! Permutation A is an Enigma cipher, so it must swap 13 pairs of letters. Therefore, we also know

$$A: Q \rightarrow ?$$

That is, if the operator had typed a Q, his first randomly chosen letter would appear (remember that the same Enigma settings can be used for encryption **or** decryption). While we do not know very much about permutation A or permutation D, we do know something about the product (or composition) DA. DA refers to the permutation that results by first performing A and then performing D. Since A sends Q to the unknown letter ?, and D sends this unknown letter to B, we ultimately know

$$DA: Q \rightarrow B.$$

Similarly, we also know

$$EB: G \rightarrow Q$$

$$FC: F \rightarrow P.$$

We have extracted quite a bit of information from random letters being encrypted in essentially random ways! Intercepting another message and just focusing on the first six letters would likely give us more information about the three product permutations DA, EB, and FC. The first part of the Enigma Project tasks students with determining these three product permutations from the first six letters of forty-seven intercepted messages. In the Enigma Project, students are given a one page Intelligence Briefing. The first section of this page is reproduced in Figure 1. Looking at the information in this portion of the Intelligence Briefing, one can determine:

DA = (AYKRBXHFSWDC) (EZGIOPNUQJTM)(L)(V)

EB = (ASUGKHC)(DFYTZVR) (EOJM) (IQLX) (B) (N) (P) (W)

FC = (BNQRFES) (GKHPLMY) (CWJ) (OTV) (DU) (AI) (X) (Z)

where the three permutations are written as products of disjoint cycles. For example, under DA we have: $A \rightarrow Y, Y \rightarrow K, K \rightarrow R$, ..., $E \rightarrow Z, Z \rightarrow G, G \rightarrow I, \ldots, L \rightarrow L$, and $V \rightarrow V$.

9 May, 1940 Polish Cipher Bureau, Poznan'

Intelligence Briefing

Session Key intercepts from 12:00 a.m. – 3:00 a.m. [local German time]

Op1 IVI ORA	Op13 FVO SRT	Op25 CYN ATQ	Op37 LWM LWY
Op2 FBK SBH	Op14 RHY BCG	Op26 HYQ FTR	Op38 IUZ OGZ
Op3 KMO RET	Op15 ETM ZZY	Op27 MSO EUT	Op39 GZD IVU
Op4 PHS NCB	Op16 KVK RRH	Op28 TDW MFJ	Op40 FOL SJM
Op5 RAJ BSC	Op17 AIM YQY	Op29 GFM IYY	Op41 JIE TQS
Op6 XKA HHI	Op18 IRU ODD	Op30 WFJ DYC	Op42 ZER GOF
Op7 DQD CLU	Op19 FRX SDX	Op31 EGB ZKN	Op43 SJC WMW
Op8 VYT VTV	Op20 NVZ URZ	Op32 AQR YLF	Op44 BXN XIQ
Op9 BPY XPG	Op21 XTY HZG	Op33 JPM TPY	Op45 UCH QAP
Op10 YFT KYV	Op22 SIN WQQ	Op34 EHO ZCT	Op46 QTF JZE
Op11 FRG SDK	Op23 KRL RDM	Op35 NLP UXL	Op47 DNR CNF
Op12 NBV UBO	Op24 DEN COQ	Op36 OSY PUG	

Figure 1: First section of Intelligence Briefing

The first time students work out these product permutations, some patterns are clearly noticeable. The product DA is composed of two twelve-cycles and two one-cycles. The product EB is composed of two seven-cycles, two four-cycles and four one-cycles. Product FC is composed of two seven-cycles, two three-cycles, two two-cycles, and two one-cycles. A theorem guarantees that these product permutations will always be composed of pairs of cycles of the same length. If one is teaching a course to students with a background in Abstract Algebra, one might consider proving this theorem. If one is teaching to students without such a background, it can still be stated that mathematicians, such as Marian Rejewski, knew this result. And, even more important, they knew how to use this result to help them factor the product permutations and recover the original Enigma permutations A, B, C, D, E, and F!

However, before moving on to factoring permutations, there are a few important consequences about the cycle structure of these product permutations one should note. As one might expect, Enigma machines set up according to different daily keys will produce product permutations that have different cycle structures. For each product permutation, these cycles will always come in pairs, but the lengths will vary depending on the corresponding daily key. While we pointed out earlier that there are over seven quintillion daily keys, it turns out that the plugboard settings do not affect the cycle structure of these product permutations! That is, if the plugboard settings on the Enigma were changed in the above example, it would still be the case that the permutation DA would be composed of two twelve-cycles and two one-cycles (the actual cycles would likely be different, but there would still be two twelve-cycles and two one-cycles). This is because conjugate permutations have the same cycle structure, a fact that is sometimes proven in an Abstract Algebra course at the undergraduate level. If we ignore the effect of the plugboard, instead of having seven quintillion settings to worry about, there are only 105,456 different settings! Furthermore, there exist 21,230 different cycle structures that might result (Bauer, 2013, 274). Being a roughly 1:5 ratio, determining the cycle structure of the three product permutations might give one around five possible daily keys (minus the plugboard) to try. Now, that is manageable! In reality, these cycle structures are not uniformly distributed among the different daily keys. In fact, about 54% of the cycle structures correspond to unique rotor settings (Bauer, 2013, p274). That means, once these three product permutations are found, there is a greater than 50% chance that one has the daily key (minus the plugboard) for that day! The Poles spent several months creating a catalog that would list which daily keys corresponded to which cycle structures.

Factoring Permutations

Again, for more mathematical detail on factoring permutations refer to (Bauer, 2013) and (Christensen, 2007). When teaching this to students, one can avoid much of the abstract notation and use the "Finger Theorem". The Finger Theorem may be a bit cumbersome to describe in writing but it can quickly be described in a classroom (or on Zoom!) and students have little trouble mastering its use.

Suppose we wish to factor

DA = (AYKRBXHFSWDC) (EZGIOPNUQJTM)(L)(V).

Start by identifying two cycles of the same length (we will pick the two twelve-cycles). Place a finger from your left-hand on the A in the first cycle and a finger from your right hand on the M on the second cycle:

DA = (AYKRBXHFSWDC) (EZGIOPNUQJTM) (L)(V)

Left finger

Right finger

This tells us that permutation A sends $A \rightarrow M$, which we will write as the two-cycle (AM).

Now, move your left finger to the right and your right finger to the left:

DA = (AYKRBXHFSWDC) (EZGIOPNUQJTM) (L)(V)

Left finger

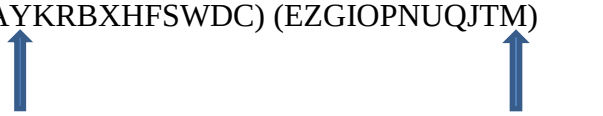
Right finger

This gives us another two-cycle (YT). Continue in this manner until one's fingers run through all the pairings in the two twelve-cycles. Repeat this process for the two one-cycles. The resulting two-cycles form permutation A:

$$A = (AM)(YT)(KJ) \ldots (CE)\ (LV).$$

To get permutation D, start with your original finger configuration, except move your left finger one position to the right:

DA = (AYKRBXHFSWDC) (EZGIOPNUQJTM) (L)(V)



Left finger Right finger

This yields the two-cycle (YM). As before, start moving your left finger to the right and your right finger to the left to recover the rest of permutation D:

$$D = (YM)(KT)(RJ) \ldots (AE)\ (LV).$$

If your finger ever gets to the "end" of a cycle, just move it back to the beginning of the cycle when it needs to be moved again.

At this point, one can check that the composition of A and D, as written above, agrees with DA. For example, under A, $A \to M$ and under D, $M \to Y$. Thus, under DA, $A \to Y$, which agrees with what we found earlier. Unfortunately, as with factoring integers, other factorizations are also possible. Essentially, one can apply the Finger Theorem with one's fingers in any starting position and produce a correct factorization. Thus, there are actually 11 different ways to factor DA in such a way that A and D are legitimate Enigma permutations (permutations which swap 13 pairs of letters). Similarly, since FC is composed of pairs of seven-, three-, two-, and one-cycles, there are $7 \times 3 \times 2 \times 1 = 42$ ways to factor FC. In terms of factoring DA, EB, and FC, this is about as far as mathematics will take us. One now has to use what Bauer (2013, 261) refers to as the "psychological method".

The cryptographic flaw in the German's Indicator Method was encrypting the randomly chosen session key a second time. The human flaw in this method is asking a

soldier to pick three random letters every time he needs to send a message! If time was of the essence, this task would be even harder. "It is well known that a human being gifted with consciousness and memory does not have the ability to imitate chance in a faultless manner" (Rejewski, 1981, 219). While all humans are bad at picking random letters, it appears that some are worse than others. There are many stories of Enigma operators picking letters grouped together on the keyboard or, perhaps, initials of loved ones. In many cases, operators would just pick the same letter three times! If an operator picks YYY as his session key and Enigma encrypts it as, say, GCK, one can understand how that looks pretty random! Rejewski (1981, 219) mentions that "it is the task of a cryptologist to uncover and suitably make use of these deviations from chance."

Intel Report: We have information that the message keys WWW, AAA, and QQQ were used among this batch of 47. But, we don't know which operators were responsible for these lapses.

Complete messages:

Op1: IVI ORA RINXJ PANCL BYNDT CMBHK OJDEG TBVYF IRCTA FCAWX VTFDU QXWXN MSLZL MZNGF CFAHS XKBDD

Intel Report: This operator always sends a weather report shortly after midnight and typically begins the message with "weather report is as follows"

Op13: FVO SRT FZHUN BMCNL HMXWD DIYJC CNRRO OYXDB NNPTG SFMNM RQUAD HFHCQ GUIDI GRTGK

Intel Report: This message originated from German high command and is believed to contain important information on future troop movements. We need this decrypted with the UTMOST URGENCY.

Figure 2: Second half of the Intelligence Briefing.

At this point, one might have to make a few educated guesses about likely session keys chosen by operators. Or, maybe it is known that certain operators tend to

use some of the same poorly chosen session keys day after day. In the Enigma Project, we assume we have some additional intelligence which tells us that three of the 47 operators used the session keys WWW, AAA, and QQQ. The second half of the Intelligence Briefing in the Enigma Project contains this additional information as well as some additional information that will be used later (see Figure 2). Of course, if this was not known, one could try to check certain triple letter session keys or keys such as QWE or ASD. Rejewski (1981, 218) comments on guessing such session keys: "When I first assumed that there would be many keys of the sort *aaa*, *bbb*, etc. it was only a hypothesis that luckily turned out to be true." It turns out that one can often tell from examining the 47 six-letter encrypted session keys whether a given session key was chosen or not and, if it was chosen, which operator chose it!

For example, let us assume that one operator chose WWW for his session key. Since

EB = (ASUGKHC)(DFYTZVR) (EOJM) (IQLX) (B) (N) (P) (W),

the Finger Theorem would tell us to put one finger on W and one finger on either B, N, or P. That tells us that under permutation B, W must be sent to B, N, or P. Similarly, examining

FC = (BNQRFES) (GKHPLMY) (CWJ) (OTV) (DU) (AI) (X) (Z),

one concludes that under permutation C, W must get sent to O, T, or V. Thus, we are looking for an operator whose encrypted session key has a B, N, or P as the second letter and an O, T, or V as the third letter. Operator 12 is the only candidate! Furthermore, this also tells us that under permutation A, $W \rightarrow N$. This means that when we factor DA, we want to start with our fingers on W and N. We can now uniquely factor DA. One can similarly deduce which operators typed AAA and QQQ as their

session keys. The resulting information allows one to uniquely factor EB and FC and decrypt **all** of the 47 session keys!

Let us pause and review where we are. To break Enigma on any given day, we start by examining a bunch of encrypted session keys (six-letter snippets). This allows us to form the products DA, EB, and FC. Thanks to the work of the early polish codebreakers in building their catalog, the cycle structure of these three products may yield the daily key (minus the plugboard settings) or give us a few possible daily keys to try. Using a little extra intelligence or some educated guesswork, the Finger Theorem and the psychological method will allow us to factor the three products and uniquely determine the six permutations A, B, C, D, E, F as well as the unencrypted session keys. In order to read any Enigma message for the day, one needs two additional items: 1) the plugboard settings and 2) a working Enigma machine.

Before attacking Enigma on a daily basis, Marian Rejewski used the flaws in the Indicator Method that have already been pointed out, some recovered codebooks with daily keys, and the mathematics of permutations to set up a system of equations which, when solved, yielded the internal wirings of the Enigma rotors. This allowed the Poles to construct their own working Enigma machine. While the Pringle can Enigma is wonderful for teaching about Enigma (Franklin Heath Ltd, 2021), for this project students may wish to use an online simulator. Care should be taken when choosing a simulator as not all of them are accurate! This author recommends students use the simulator written by Daniel Palloks (Palloks, 2021). For this project, if you are using Palloks' simulator, keep the default Enigma model set at "M3 (Army; Navy)".

Plugboard Settings

As with many puzzles, there is no one right way to break a cipher. In Cryptanalysis there are often many paths that lead to a successful break. While there may be several

interesting ways to recover the plugboard settings for the daily key, the Enigma Project is designed to make use of cribs, which accurately reflects the historical break of Enigma. In the Enigma Project, students are given a very long crib. Also, to make this project go a little faster, students are also told where the crib should be placed. Alternatively, since Enigma never encrypts a letter to itself, one can employ the process of "crib dragging" to help determine the correct placement of a crib. However, this extra step was not required during the Spring 2021 implementation of this project.

The Intelligence Report (see Figure 2) gives the complete message sent by Operator 1: `IVI ORA RINXJ PANCL BYNDT CMBHK OJDEG TBVYF IRCTA FCAWX VTFDU QXWXN MSLZL MZNGF CFAHS XKBDD.` Using what we know about permutations A, B, C, D, E, and F, we can decrypt the first six letters: ASD ASD to recover Operator 1's session key. The Poles would use the cycle structure of DA, EB, and FC together with the catalogue to, hopefully, determine that the daily key consisted of placing rotors III, I, II (left to right) in the machine. (For the purpose of this classroom project, and this discussion, we are simplifying the situation by assuming the ring settings are A,A,A. We are also assuming that reflector B was being used.) For this project, the instructor can play the role of the "catalog". Any students who correctly determine the cycle structure of the three product permutations are given the correct rotor order (and ring settings). One can now set the rotors to the session key ASD and type in the known plaintext: "weather report is as follows". This produces the ciphertext: `RTDKJ PSNMG BYUHO NBBHW SJDD.` This does not match the ciphertext that Operator 1 sent, because we do not have the correct plugboard settings. If we compare the two ciphertexts we might get some clues as to the correct plugboard settings:

Our CT: `RTDKJ PSNMG BYUHO NBBHW SJDD`

OP1 CT: RINXJ PANCL BYNDT CMBHK OJDE

While the first letters agree the second letters do not (as well as many others). Perhaps these do no match up because T and I should be connected on the plugboard. If we connect T and I and re-encrypt our plaintext we get:

Our CT: RIDXJ PSNMG BYNDO NBBHW SJDD

OP1 CT: RINXJ PANCL BYNDT CMBHK OJDE

This looks better and suggests that we might try connecting D and N. If we do this, we get:

Our CT: RINXJ PSDMG BYDNO DBBHW SJNN

OP1 CT: RINXJ PANCL BYNDT CMBHK OJDE

Again, this is looking better. Let's connect A and S:

Our CT: RIDXJ PADMG BYDNT MCBHW AJNE

OP1 CT: RINXJ PANCL BYNDT CMBHK OJDE

Now it looks like we want to remove the D→N connection and add an M→C connection. This results in:

Our CT: RINXJ PANCG BYNDT CMBHW AJDE

OP1 CT: RINXJ PANCL BYNDT CMBHK OJDE

Using a final plugboard setting of I→T, A→S, M→C, and G→L we get:

Our CT: RINXJ PANCL BYNDT CMBHK OJDE

OP1 CT: RINXJ PANCL BYNDT CMBHK OJDE

A perfect match!

We are now in a position to decrypt any Enigma traffic for the day. As we did with Operator 1, we can determine Operator 13's session key, use the correct plugboard settings, and decrypt the final message on the Intelligence Briefing (exercise left to the reader).

Project Logistics

Once the techniques of the Polish Codebreakers has been taught in class, one may use the Intelligence Briefing as a final culminating project to assess all of these cryptanalytic skills. All of the necessary information is included in the Intelligence Briefing, but one may tailor the difficulty level of the assignment by providing students with additional scaffolding and/or prompts. This project was used in Spring 2021 in a 10-week seminar (ten 50-minute meetings on Zoom) on the Polish breaking of Enigma. For that class, the project was broken up into four Canvas assignments, due a week apart. While readers are welcome to contact the author for the specific wording of the prompts used, the four assignments were essentially:

(1) Determine the three product permutations and their cycle structure. If this is done correctly, the instructor will respond with the correct rotor order and ring positions for the daily key.
(2) Determine the six permutations A, B, C, D, E, and F. Decrypt the session keys of Operators 1 and 2. Do these seem like random session keys?
(3) What are the plugboard settings and what is the complete message that Operator 1 sent?
(4) Decrypt Operator 13's message.

Most of the students found the project reasonably challenging and some students were given additional hints to help them with the "psychological method" portion of the assignment. For example, one could tell students which operators typed "WWW", "AAA", and/or "QQQ" to make the project less difficult. To make the project more challenging, there are also a variety of options:

(1) An instructor could just hand out the Intelligence Report and ask for a decrypt of Operator 13's message. Students would need to identify the correct cryptanalytic steps to take in order to break Enigma.

(2) One could reduce the number of message keys given to the students and let them try to guess some of the more likely ones. In addition to the message keys of "WWW", "AAA", and "QQQ", many of them are three consecutive letters on the keyboard, like: "ASD", "QWE", "ZXC", "DFG", "POI", "LKJ", etc. Working in groups and sharing information might allow students to deduce some of the message keys and allow them to uniquely factor the product permutations.

(3) One could not disclose the exact placement of the crib in Operator 1's message. However, if one uses this modification to the project, one might adjust the crib. As written, there are quite a few possible places it could appear in the message if one is simply using the fact that Enigma never encrypts a letter to itself.

The Story Continues

The preceding paragraphs detailed some of the steps taken by the Polish codebreakers on a daily basis in breaking Enigma. In early 1938, the Poles were reading 75% of all Enigma traffic! Moreover, Rejewski believes this could have been as high as 90% if they had been given a slight increase in personnel (Rejewski, 1981). However, the story of breaking Enigma continues long after the first successful breaks by the Poles. The Poles had to rebuild their catalogue of daily keys after the Germans started using a different reflector on November 2, 1937. More devastating though, on September 15, 1938, the Germans stopped using the indicator method, which the above work is based on. At the same time, the Germans introduced a fourth and fifth rotor, thereby increasing the number of daily keys tenfold. The Poles developed new techniques

including Zygalski sheets, Różycki's "Clock Method" and the building of the bomba to continue their breaks into Enigma. Of course, Germany invaded Poland in September of 1939 disrupting the work of the Polish Cipher Bureau and causing the Polish codebreakers to begin a series of dangerous trips across Europe and North Africa in attempts to continue their cryptanaytic work and simultaneously safeguard the valuable secret of their break into Enigma. Advances in the Enigma machine continued throughout World War II and the codebreakers of Bletchley Park picked up the battle so courageously and deftly begun by Rejewski in 1932.

Conclusion

The wonderful world of secret writing, codes, and ciphers can hold the interest of many students. College instructors with an interest in cryptology should take advantage of this interest and challenge themselves to bring this subject to a wider audience by weaving in exciting stories like the Polish codebreakers and personal privacy. Instructors could offer courses in innovative formats (e.g. seminars) or to students outside the typical domains of mathematics and computer science. Cryptology is inherently nestled in a context that is naturally exciting, intriguing, and thought provoking. It would be great to see colleges and universities regularly offering cryptology courses.

References

Bauer, C.P. 2013. *Secret History: The Story of Cryptology*. CRC Press.

Christensen, C. 2007. Polish Mathematicians Finding Patterns in Enigma Messages. *Mathematics Magazine*, 80 (4): 247 - 273.

Franklin Heath Ltd, Enigma/Paper Enigma. Accessed September 14, 2021. http://wiki.franklinheath.co.uk/index.php/Enigma/Paper_Enigma

Kahn, D. 2012. *Seizing the Enigma: The Race to Break the German U-Boat Codes, 1939 – 1943*. Frontline Books.

Palloks, D. Universal Enigma – Simulator by dp. Accessed September 14, 2021. http://people.physik.hu-berlin.de/~palloks/js/enigma/enigma-u_v25_en.html

Rejewski, M. 1981. How Polish Mathematicians Deciphered the Enigma. *Annals of the History of Computing*, 3 (3): 213 – 234.—

Sebag-Montefiore, H. 2000. *Enigma: The Battle for the Code*. Hoboken, New Jersey: John Wiley & Sons, Inc.

Taylor and Francis. Cryptologia Aims & Scope. Accessed September 14, 2021. https://www.tandfonline.com/action/journalInformation?show=aimsScope&journalCode=ucry20