Portland State University
PDXScholar

Young Historians Conference | Young Historians Conference 2016

Apr 28th, 9:00 AM - 10:15 AM

# To What Extent Did British Advancements in Cryptanalysis During World War II Influence the Development of Computer Technology?

Hayley A. LeBlanc
*Sunset High School*

Follow this and additional works at: https://pdxscholar.library.pdx.edu/younghistorians

 Part of the European History Commons, and the History of Science, Technology, and Medicine Commons

Let us know how access to this document benefits you.

LeBlanc, Hayley A., "To What Extent Did British Advancements in Cryptanalysis During World War II Influence the Development of Computer Technology?" (2016). *Young Historians Conference*. 1.
https://pdxscholar.library.pdx.edu/younghistorians/2016/oralpres/1

This Event is brought to you for free and open access. It has been accepted for inclusion in Young Historians Conference by an authorized administrator of PDXScholar. Please contact us if we can make this document more accessible: pdxscholar@pdx.edu.

# To what extent did British advancements in cryptanalysis during World War 2 influence the development of computer technology?

---

Hayley LeBlanc
1936 words

**Table of Contents**

**Section A: Plan of Investigation**

This investigation will focus on the advancements made in the field of computing by British codebreakers working on German ciphers during World War 2 (1939-1945). Along with examining the state of code-breaking technology before the war, it will discuss the nature of computing after the war up until the present to determine the impact of the war on computers. It will consider being electronic (rather than electromechanical) as the defining characteristic of modern computers. This investigation will not discuss the cryptanalysis effort by any other country during the war, nor will it consider cryptography-related advancements after the war. However, it will examine the contributions of other countries to code-breaking technology prior to the war when these contributions are relevant to war-time cryptanalysis. It will also consider other countries' contributions to computing after the war. Two sources used in this investigation, Marian Rejewski's *How Polish Mathematicians Deciphered the Enigma* and Simon Singh's *The Code Book,* will be evaluated for their value and limitation.

**Section B: Summary of Evidence**

- Before the war
    - The German Enigma cipher was developed at the end of World War 1 and used for commercial purposes until World War 2.[1]
        - The Enigma was much faster at enciphering messages and its code was much more difficult to break than older ciphers.[2]
    - Polish mathematicians Marian Rejewski, Jerzy Rozycki, and Henryk Zygalski worked on breaking the original Enigma cipher between 1932-1939.[3]
        - Around 1936, the Polish developed an electromechanical[4] device called the cyclometer that sped up the codebreaking process.[5]
        - In 1938, the Polish mathematicians developed electromechanical devices called bombas that further sped up the decryption of messages.[6]
        - In 1939, the Enigma machines were adopted by the German military and became more complex, rendering Polish methods of codebreaking insufficient.[7]
    - In July 1939, the Polish codebreakers gave the British and French intelligence agencies all their code-breaking devices and information.[8]
- During the war
    - The British codebreaking effort was concentrated at the Government Code and Cypher School at Bletchley Park.[9]
    - The British developed two machines to break German codes at Bletchley Park during the war.
        - British electromechanical bombes[10], which were based on Polish bombas developed before the war, helped break the wartime Enigma codes.[11]
            - The British bombes were developed by a group of cryptanalysts at Bletchley Park including Alan Turing and I. J. "Jack" Good.[12]

---

[1] *The Complete Story of Codebreaking*.
[2] Boone, *A Brief History of Cryptology*, 8. See Appendix A for an explanation of how the Enigma machines worked and how they were more secure than prior methods.
[3] Rejewski, *How Polish Mathematicians Deciphered the Enigma*, 214-227.
[4] Electromechanical computers are made of mechanical components like gears and levers that are operated. They are significantly slower than modern electronic computers, which use smaller equipment like transistors and circuits.
[5] Ibid., 224-225.
[6] Woytak, *Ultra-Secret Code in Poland*, 82.
[7] Rejewski, *How Polish Mathematicians Deciphered the Enigma*, 227.
[8] Ibid., 227-228.
[9] Christensen, *Finding Patterns in Enigma Messages*, 247.
[10] Boone, *A Brief History of Cryptology*, 8.
[11] Singh, *The Code Book*, 243.
[12] Dyson, *Turing's Cathedral*, 254-255.

        - The Colossus computers were used to break the German Lorenz ciphers.[13]
            - The Lorenz ciphers were much more difficult to break than the Enigma ciphers.[14]
            - The Colossi were electronic and built with 1,500 lightbulb-like valves that made them programmable[15] and much faster than the electromechanical bombes.[16]
            - The Colossi implemented a branch of mathematics known as Boolean algebra in its hardware.[17]
            - The Colossi were developed by a group at Bletchley Park that included Max Newman and Tommy Flowers known as the "Newmanry."[18]
- After the war
    - Some mathematicians and scientists who had worked at Bletchley Park during the war, such as Alan Turing and Max Newman,[19] continued to work on electronic computers after World War 2.[20]
    - Due to the British Official Secrets Act, none of the cryptanalysts from Bletchley Park could share any information about their wartime work until the 1970s.[21]
        - All the developments made by Bletchley Park, including blueprints for the Colossus machines and most of the machines themselves, were destroyed after the war.[22]
    - In 1945, American mathematicians created ENIAC (Electronic Numerical Integrator And Calculator).[23]
        - ENIAC was very similar to Colossus in that it used electronic valves and was plug programmable, but the two computers were developed independently of one another.[24]
        - ENIAC is widely believed to be the first electronic computer.[25]

---

[13] Singh, *The Code Book*, 244.
[14] Copeland et al., *Bletchley Park's Code-Breaking Computers*, 36.
[15] Ibid., 62.
[16] Singh, *The Code Book*, 244.
[17] Boone, *A Brief History of Cryptology*, 65.
[18] Copeland et al., *Bletchley Park's Code-Breaking Computers*, 61.
[19] Dyson, *Turing's Cathedral*, 334.
[20] Ibid., 257.
[21] Copeland et al., *Bletchley Park's Code-Breaking Computers*, 2.
[22] Singh, *The Code Book*, 244.
[23] Ibid.
[24] Ibid.
[25] Burks and Hofstadter, *Who Invented The Computer?*, 316.

**Section C: Evaluation of Sources**

*How Polish Mathematicians Deciphered the Enigma* by Marian Rejewski

Marian Rejewski is one of the Polish mathematicians who helped break the German Enigma code before World War 2. His paper is a primary source, so it is valuable to this investigation. Rejewski is very knowledgeable about the pre-war Enigma cipher and the methods used to crack it. He also has first-hand information about British codebreaking during the war. However, the paper was published nearly 50 years after Rejewski worked on the Enigma, so he was writing from memory and may have forgotten some details. The paper's purpose is valuable in that it explains in detail how the pre-war Enigma worked and the methods used to break it. It also discusses the devices invented to help the cryptanalysts, like the bombe and cyclometer, which provides useful information about pre-war cryptographic techniques. However, the paper only discusses code breaking before the war, which is not the main focus of this investigation. The paper provides useful background knowledge that can be used to judge the level of technological advancement that happened in Britain during the war, but it doesn't provide any information that contributes to conclusions about the impact of World War 2 technologies on today's computers.

*The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography* by Simon Singh

Simon Singh is a British author who has worked on several books and television shows about mathematics, science, and technology. He is well-versed in topics relating to cryptography, making *The Code Book* a valuable resource. However, he is not specifically a cryptology expert, so he may not be as credible as someone who has studied the field for many years. *The Code Book* is also not a primary resource, as many of the developments happened before Singh's birth and he was not involved with those that were made while he was alive. Singh's book is meant to cover all of cryptographic history, so while it includes valuable information about cryptanalysis during World War 2, the book also contains a large amount of information that is not relevant to this investigation. The book also focuses solely on cryptography and no other advancements to the world of computing, limiting the value of its purpose.

**Section D: Analysis**

Today's computers are electronic, not electromechanical. Before World War 2, there were no electronic computers. Polish cryptanalysts working on early versions of the German Enigma machine developed several electromechanical devices - the cyclometer and the bomba - that historian Richard Woytak describes as "the first modern computers."[26] Although these machines were very useful in breaking the early Enigma codes, they should not be considered modern because they are not electronic. Several months before the beginning of World War 2, after Germany enhanced the complexity of their ciphers, the Polish government gave Britain and France all the information they had gathered on the Enigma.[27] After this, Britain became one of the most important centers of cryptanalysis during the war, breaking several German ciphers over the course of the war.

At the British Government Code and Cypher School in Bletchley Park, two main devices were developed to aid the effort to break German codes. The first, the bombe, was developed by a group that included Alan Turing and "was used to analyze Enigma ciphertext and recover key settings of the machine."[28] This bombe was based on the earlier Polish bombas and was still electromechanical.[29] Although the bombe machines are arguably a huge part of how the Allies won World War 2, they still cannot be considered to be truly modern computers due to their electromechanical nature.

The second device, and the one that is arguably more important to this investigation, is the Colossus computer. The Colossi were developed to break the German Lorenz cipher.[30] The Lorenz was significantly more complicated than the Enigma, and the preexisting bombes were not advanced enough to break the code.[31] It was also developed at Bletchley Park, by a group known as the "Newmanry" for their leader Max Newman.[32] The computer was Newman's idea, but a Newmanry engineer named Tommy Flowers built it over about ten months with about 1,500 electronic valves that used Boolean algebra to solve problems.[33] Unlike the bombes, the Colossi were electronic and programmable, although this programming mainly involved figuring out how to configure the hardware of the machine to solve problems.[34] Many historians and computer scientists believe that Colossus was the first modern computer. Stephen Budiansky says that the Colossi helped "[usher] in the age of the digital, general purpose, stored program

[26] Woytak, *Ultra-Secret Code in Poland*, 82.
[27] Rejewski, *How Polish Mathematicians Deciphered the Enigma*, 227-228.
[28] Boone, *A Brief History of Cryptology*, 8.
[29] Rejewski, *How Polish Mathematicians Deciphered the Enigma*, 233.
[30] Singh, *The Code Book*, 244.
[31] Ibid.
[32] Copeland et al., *Bletchley Park's Code-Breaking Computers*, 61.
[33] Boone, *A Brief History of Cryptology*, 63-65.
[34] Copeland et al., *Bletchley Park's Code-Breaking Computers*, 62.

electronic computer,"[35] and Simon Singh says that the Colossus was "the precursor to the modern digital computer."[36]

Like the Colossi, today's computers are programmable, and their hardware and software is still based on Boolean algebra. Some integral aspects of the Colossi are still used in today's computers, about 75 years later. However, although the Colossi may have set the basic foundation for modern computing, they still lacked many features. They could not store programs in their memory, so each algorithm had to be recreated and reprogrammed in whenever the cryptanalysts wanted to use it. The Colossi were also only meant for one specific purpose - breaking the Lorenz codes - and were not advanced enough to do other operations.[37] Today's computers, on the other hand, store hundred of programs and can do a wide variety of operations.

There is another reason why the Colossi may not have been particularly influential on modern computing. Britain's Official Secrets Act effectively prevented the spread of any information about the Colossus, bombes, or any other wartime cryptology advancements for nearly 40 years.[38] Tommy Flowers says he was "naturally disappointed" when he learned that Colossus was to be kept secret after the war,[39] but destroyed the computers and their blueprints regardless.[40] Shortly after the end of World War 2, American researchers at the University of Pennsylvania unveiled their ENIAC (Electronic Numerical Integrator And Calculator) computer. Today, most people believe that ENIAC was the first modern programmable computer. Donald Michie, a mathematician who worked on Colossus during the war, says that "the fact that those of us who worked with the Colossus range were inhibited until the 1970s by wartime secrecy from mentioning their existence explains the widespread persistence… of the false belief that the ENIAC was the first electronic computer."[41] Even though Colossus came before ENIAC, it did not directly influence any of the computing advancements that took place between World War 2 and the 1970s because very few people knew about it. By the time information about the Colossi was made public, computing had advanced too much for any additional impact to be made.

Even though the bombe and Colossus machines built during World War 2 could not impact the development of electronic computers, to say that British cryptanalysts did not affect the field would be inaccurate. Alan Turing worked with Max Newman at the University of Manchester after the war, continuing where they left off on the Colossus.[42] Turing's work over his own lifetime - before, during, and after the war - became incredibly influential in the field of computing. After the war, he made especially important contributions to the concept of artificial

---

[35] Ibid., 52.
[36] Singh, *The Code Book*, 244.
[37] Copeland et al., *Bletchley Park's Code-Breaking Computers*, 62. One mathematician who worked on Colossus designed a program that would allow the computers to do base-10 multiplication (the type best known to us) but it was deemed to be too advanced for Colossus' processors.
[38] Ibid., 2.
[39] Ibid., 82.
[40] Singh, *The Code Book*, 244.
[41] Burk and Hofstadter, *Who Invented the Computer?*, 316.
[42] Dyson, *Turing's Cathedral*, 334.

intelligence.[43] Other former cryptanalysts of Bletchley Park created the first stored-program computer in 1948 and continued to contribute to the development of computer memory for years.[44] By the end of World War 2, there were still many developments to be made before today's computers could be built, but the work of British cryptanalysts set the stage for modern computing.

[43] Ibid., 259-261.
[44] Ibid., 257.

**Section E: Conclusion**

Despite the great improvements made on pre-war computational technology, British cryptanalysis during World War 2 did not have a particularly large impact on future computing. British engineers created the first electronic computer in the world, the Colossus, but due to the Official Secrets Act all information about the Colossi was kept secret for decades. The other devices built by British cryptanalysts - the bombes - were not similar enough to modern electronic computers to be considered influential. The only way that the British codebreaking effort truly contributed to the field of computer science was through the work of former cryptanalysts following up on their wartime work after 1945.

**Section F: List of Sources**

"Battle of Wits: The Complete Story of Codebreaking in World War II." n.d. Accessed November 17, 2015. http://practicalcryptography.com/ciphers/enigma-cipher/.

Boone, J. V. *A Brief History of Cryptology*. United States: US Naval Institute Press, 2005.

Burks, Alice Rowe and Douglas R. Hofstadter. *Who Invented the Computer? The Legal Battle That Changed Computing History*. New York: Prometheus Books, 2003.

Christensen, Chris. "Polish Mathematicians Finding Patterns in Enigma Messages." *Mathematics Magazine* 80, no. 4 (August 2007). http://0-www.jstor.org.catalog.multcolib.org/stable/27643040?Search=yes&resultItemClick=true&searchText=enigma&searchText=machine&searchUri=%2Faction%2FdoBasicSearch%3FQuery%3Denigma%2Bmachine%26amp%3Bprq%3Dhistory%2Bof%2Bcryptography%26amp%3Bgroup%3Dnone%26amp%3Bhp%3D25%26amp%3Bacc%3Don%26amp%3Bfc%3Doff%26amp%3Bwc%3Don%26amp%3Bso%3Drel&seq=3#page_scan_tab_contents.

Copeland, Jack, ed. *Colossus: The Secrets of Bletchley Park's Code-Breaking Computers*. United States: Oxford University Press, UK, 2010.

Dade, Louise. "How Enigma Machines Work." n.d. Accessed November 18, 2015. http://enigma.louisedade.co.uk/howitworks.html.

Dyson, George. *Turing's Cathedral: The Origins of the Digital Universe*. New York: Pantheon Books, 2012.

Rejewski, Marian. "How Polish Mathematicians Deciphered the Enigma." 2006. Accessed November 7, 2015. http://chc60.fgcu.edu/images/articles/rejewski.pdf.

Singh, Simon. *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. United States: Knopf Doubleday Publishing Group, 2000.

Woytak, Richard A. "The Origins of The Ultra-Secret Code in Poland, 1937-1938." *The Polish*

*Review* 23, no. 3 (1978). http://0-www.jstor.org.catalog.multcolib.org/stable/25777589?Search=yes&resultItemClick=true&searchText=the&searchText=origins&searchText=of&searchText=the&searchText=ultra&searchText=secret&searchText=code&searchText=in&searchText=poland&searchUri=%2Faction%2FdoBasicSearch%3FQuery%3Dthe%2Borigins%2Bof%2Bthe%2Bultra%2Bsecret%2Bcode%2Bin%2Bpoland%26amp%3Bprq%3Dcolossus%2Bcomputer%26amp%3Bgroup%3Dnone%26amp%3Bfc%3Doff%26amp%3Bwc%3Don%26amp%3Bhp%3D25%26amp%3Bacc%3Don%26amp%3Bso%3Drel&seq=1#page_scan_tab_contents.

## Appendix 1: Explanation of The Enigma Machine[45]

The underlying principle of an Enigma machine cipher is that of *letter substitution*, meaning that each letter of our plaintext (undeciphered message) is substituted by another letter.

## The Journey Of A Single Letter

The Enigma machine is an electro-mechanical device. It is mechanically operated, with an electric signal passed through wires and various mechanical parts. The easiest way to explain the mechanics is to follow the journey of a single letter from keyboard to lampboard.

The diagram below (figure 1) shows the path the signal takes from pressing the letter 'T' on the keyboard to the 'G' lamp lighting up.

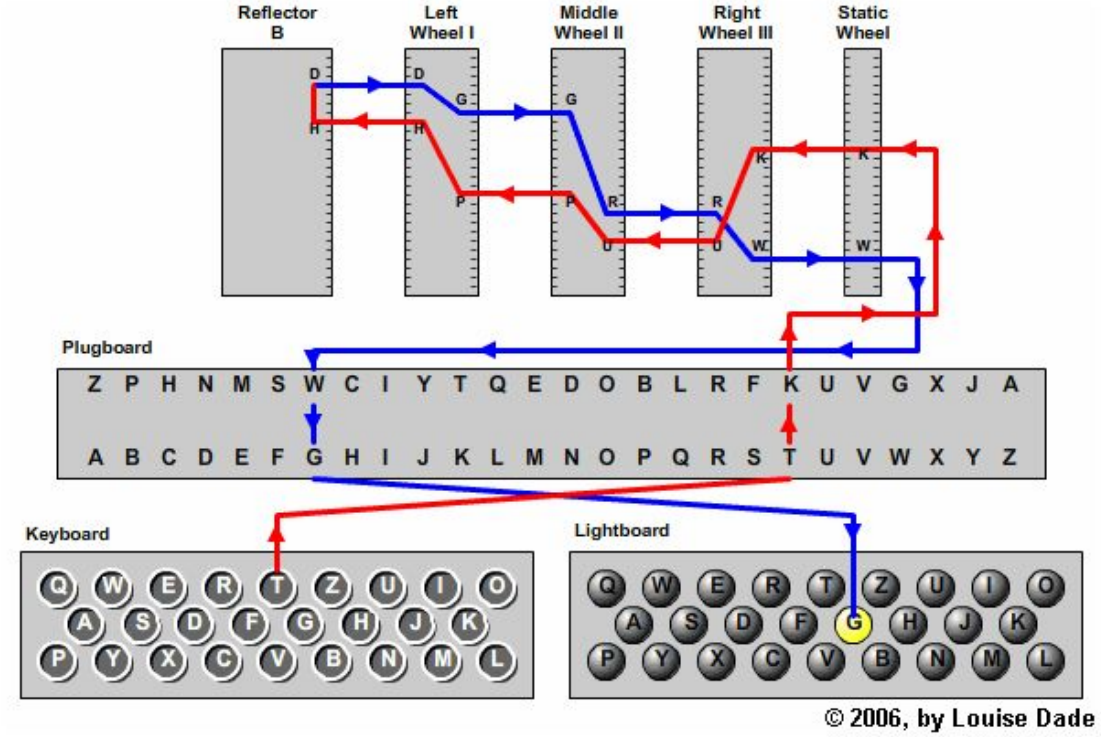


*Figure 1: How one letter is changed into another letter at each stage as it passes through an Enigma machine.*

## Keyboard

When the operator presses the letter 'T' on the keyboard it creates an electric signal that begins the journey through the Enigma machine wiring that will end with a lamp flashing on the lampboard.

[45] Dade, *How Enigma Machines Work.*

## Plugboard

The first stop on the journey is the plugboard. Here the signal is connected to the 'T' input on the plugboard. Some of the letters on the plugboard will be wired up to other letters (the plugs), causing the signal to be diverted. If the 'T' input is not plugged to another letter then our signal will pass straight to the 'T output. In our case, though the 'T' is plugged to the 'K', so the signal is diverted to a new path, the letter is now 'K'.

## Static Rotor

The next stop is the static rotor, which as the name suggests does nothing to the signal it simply turns wires into contacts (the signal only passes when the contacts touch). So our signal is still the letter 'K'. The static rotor output is connected to the input of the right rotor. This is where things get more complicated.

## Rotors (Scramblers)

There are five possible rotors that can be used in any order for the three rotor positions: right, middle, left. Each rotor has an inner ring of contacts and an outer ring of contacts and their purpose is to scramble the signal. The outer ring contacts connect each rotor to the next rotor (or the static rotor / reflector) as well as its own inner ring. The inner ring contacts can be rotated relative to the outer ring which results in even more possible connections (and therefore, letter substitutions). The whole rotor itself can be rotated relative to the static rotor, so that the static rotor 'A' output is not connected to 'A' input on the rotating rotor.

Furthermore, as each letter is entered the rotors rotate by one position, so that the same letters are never connected together in the same message. To add further complication, each rotor has a notches (different rotors have the notch in different positions) which when reached, causes the next rotor to its left to step forward too. In the case of the middle rotor, it causes the left rotor to step *as well as itself* (the infamous double stepping mechanism).

In our example, we are using rotor III in the right-hand position.

## Reflector

The reflector takes the input and reflects back the electrical signal for its return journey through the rotors. There are two possible reflectors, each of which is wired up differently so that the input letter is transformed to a different letter when reflected back. In our example, we are using 'Reflector B', which turns our input letter 'H' into output letter 'D'.

It is important that the signal is scrambled when reflected, because of the way the Enigma machine is designed -- if you enter the cipher text you get back the clear text. So if the reflector output is the same letter as its input when the signal passes back through the rotors they will just *unscramble* what was already scrambled and you would get your original letter back again unencrypted!

## Reverse Journey

The reflected signal now passes back through the rotors, which work in exactly the same way in reverse. So our letter 'D' passes through the left rotor and becomes 'G', which then passes through the middle rotor and becomes 'R', which then passes through the right rotor and becomes 'W'. The signal remains unchanged as it passes through the static rotor again (connecting contacts to wires), before it passes through the plugboard - here the signal is again left as it is if there is no plug, or changed if the letter 'W' is plugged to another letter. In our case the 'W' is plugged to the letter 'G', so our plugboard output is 'G'.

## Lampboard

The final stop is the lampboard, where the plugboard output is connected to the corresponding lamp for that letter. In our example, the letter 'G' lights up meaning the original letter 'T' is encrypted as 'G'.

The Enigma machine operator notes down the output letter and then enters the next letter in the message, and so on for every letter in the message.

**Appendix B: Glossary of Cryptology Terms**[46]

**Boolean algebra:** A field of mathematics based on values of true and false.

**Cipher:** Any general system for hiding the meaning of a message by replacing each letter in the original message with another letter. The system should have some built-in flexibility, known as the key.

**Ciphertext:** The message (or plaintext) after encipherment.

**Code:** A system for hiding the meaning of a message by replacing each word or phrase in the original message with another character or set of characters. The list of replacements is contained in a codebook.

**Cryptanalysis:** The science of deducing the plaintext from a ciphertext, without knowledge of the key.

**Cryptography:** The science of encrypting a message, or the science of concealing the meaning of a message. Sometimes the term is used more generally to mean the science of anything concerned with ciphers, and is an alternative to the term cryptology.

**Cryptology:** The science of secret writing in all its forms, covering both cryptography and cryptanalysis.

**Plaintext:** The original message before encryption.

[46] Selected definitions from Singh, *The Code Book*, 391-393.