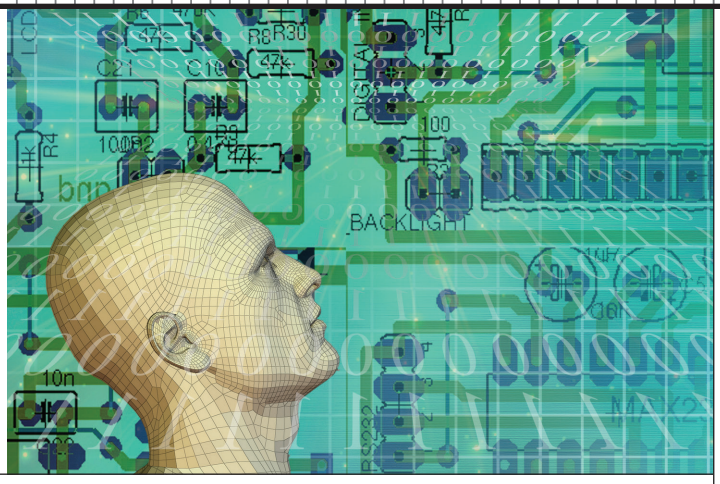
Alan Turing and Bletchley Park

Charles Severance
University of Michigan



This month marks the 100th anniversary of Alan Turing's birth. His ground-breaking work in the 1940s continues to have an impact on computer science as we know it.

Alan Turing is considered by many to be the father of modern computer science. Multiple foundational notions in the field—the Turing test, Turing machine, Turing completeness, and Church-Turing computability—bear his name in acknowledgment of his early breakthroughs and influence.

It's rare that a single genius, working alone, can achieve one great breakthrough, let alone several of them. For the sake of simplicity, historical accounts often remove the details of the rich contexts that create the necessary preconditions for such breakthroughs. But our institutions, colleagues, students, and even the people we have lunch with form a context within which we all operate.

Here, the focus is less on the detail of Turing's particular accomplishments throughout his career, instead examining some of the context in which he achieved his accomplishments. The video associated with this article (www.computer.org/computingconversations) explores some of the activities at Bletchley Park, where Turing did some of his greatest work—in particular, it looks at how Turing was deeply connected to many other brilliant people during and after his time there.

Figure 1 offers an overview of Turing's connection to the work done at Bletchley Park during World War II.

EARLY YEARS AND THE SECOND WORLD WAR

Turing graduated from Princeton in 1938, where he had already proved to be an amazing talent who thought deeply about many topics. After he received his PhD, he returned to Cambridge and started working part time for the Government Code and Cipher School at Bletchley Park. When Britain declared war on Germany in 1939, Turing reported full-time to Bletchley Park and began working on breaking the various cryptography techniques used by Germany during World War II.

Because the stakes were so high for Britain, Bletchley Park was a well-funded operation with more than 10,000 people working at peak capacity, representing a diverse mix of mathematicians, engineers, linguists, and experts in other fields. Women made up two-thirds of its workforce.

Bletchley Park was the ideal place to come up with a theory and watch literally hundreds of people adjust and refine it to get it into production as quickly as possible. Being surrounded by adequate resources and knowing that if you solve the problems you face you'll save thousands of lives generates an intensely creative environment.

The systems developed at Bletchley Park needed to break encrypted messages using whatever technology was available. The decryption devices combined mechanical and electronic computation, but as the war progressed and the cryptography techniques became more sophisticated, the need for faster computations pushed scientists from the primarily mechanical computations of the BOMBE toward the electronic computations of the Colossus.

BUILDING THE BOMBE

At the beginning of World War II, the Germans were able to move troops and other resources very quickly by coordinating those movements using wireless communications. Because their enemies could monitor wireless communications, it was necessary to encrypt any text before it was sent.

The Enigma was one of several machines used to encrypt messages before they were sent in Morse code. It used moving wheels with internal electrical connections as well as a plug board to make it virtually impossible to read the scrambled text without knowing the choice of the encryption wheels' initial settings and plug con-

 Published by the IEEE Computer Society

nections. Each day, all the Engima operators for a particular communication network used a different machine setup known as a key. If the operator could determine the key using one message on a particular day on a particular network, it was a simple matter to decrypt all messages sent by operators on that network for that day.

Alan Turing designed a machine at Bletchley Park called the BOMBE that would mechanically help determine the daily key used by a particular group of Enigma operators by trying many different possible key combinations very quickly. The BOMBE had its roots in the BOMBA, an earlier mechanical code-breaking device developed in Poland by Marian Rejewski, Jerzy Różycki, and Henryk Zygalski of the Polish Cypher Bureau. The Polish team shared the design with Turing and others at Bletchley Park five weeks before the German invasion of their country in 1939. As described by Paul Kellar of Bletchley Park,

> [The Poles] told Turing and the people here everything they had done for which we are and should be very grateful, but they also proved that it was possible and that was the spur that kicked the Brits into actually doing something about it.

The Polish approach to breaking the Enigma depended on the way the message header was added at the beginning of each message. But in early May 1940, the Germans changed their method for adding headers.

Turing's solution was based on the fact that many military messages are routine and use identical phrases day after day, such as "Nothing to report" or "Weather forecast for today is …" If the researchers had the encrypted text and the guessed plaintext (the "crib"), it was only a matter of time before they could compute the wheel settings used to encrypt the message.

The BOMBE was a mechanical device that simulated 36 Enigmas, repeatedly testing possible settings for the wheels and stopping when it found a possible correct setting. More than 200 BOMBE machines were built for use at Bletchley Park.

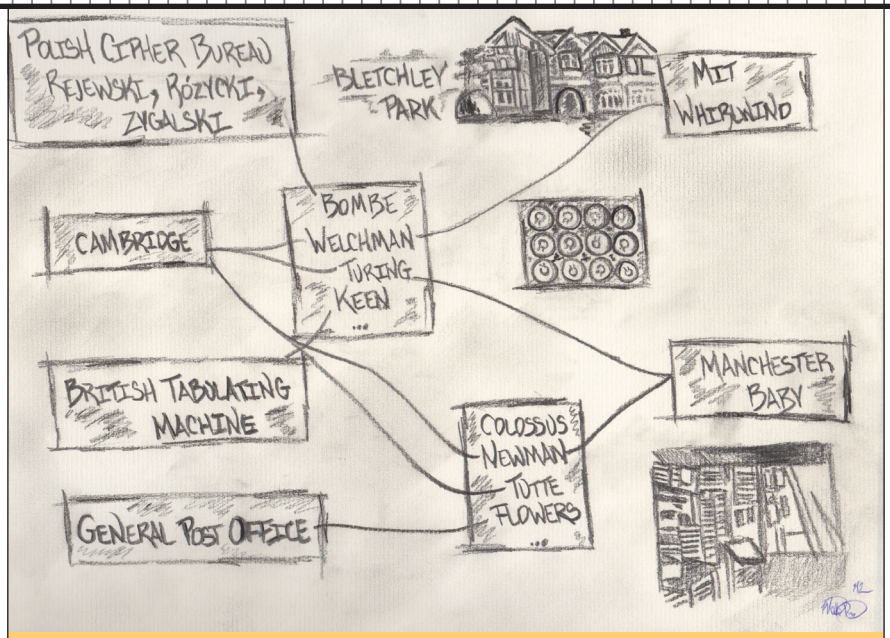


Figure 1. From Polish Bomba to the birth of the digital age: Alan Turing's work at Bletchley Park. Artist's rendering by Matt Pinter.

Although Turing designed the BOMBE's algorithm, the machine was engineered and built by a team at the British Tabulating Machine Company, led by Harold (Doc) Keen. Gordon Welchman, also from Cambridge, added the Diagonal Board concept, which dramatically reduced the number of random or incorrect stops. All in all, developing the BOMBE was very much a team effort.

BUILDING THE COLOSSUS

Later in the war, Germany started using much more sophisticated encryption devices, including the Lorenz SZ42. The SZ42 had 12 wheels and sent encrypted data using five-bit teleprinter codes rather than Morse code. Hitler and his generals used it for longer, more strategic messages. Manual decryption of a single message took nearly six weeks, so the Allies needed an automated solution.

Turing was involved in developing some of the approaches used to crack new messages encoded with the SZ42, but he wasn't involved in the Colossus computer's development.

There was no possible way to build a mechanical code-breaking machine for this new encryption technique, so engineers at Bletchley Park started building electronic computers to implement faster code-breaking algorithms. After testing an earlier version (the Mark I), the Colossus Mark II emerged—it could help break an encrypted high-command message in roughly six hours. The first Colossus Mark II was up and running at Bletchley Park on 1 June 1944 and helped decrypt strategic traffic in time to inform the D-Day invasion on 6 June 1944.

Tommy Flowers, a telecommunications engineer with the British Post Office, built the Colossus. According to Kevin Murrell of the National Museum of Computing at Bletchley Park:

> Tommy came up with the idea to use electronics to do this [solve the Lorenz encryption]. At the time, the idea of using more than half-dozen valves in a circuit was never considered. Valves had a bad reputation; people had valves in their radios at home, and they failed when they switched the radios

> on. The idea of using 2,500 [valves] was simply phenomenal. But Tommy understood that it was almost certainly the thermal shock that kills valves in the first place. So if you leave the machine on and don't subject it to that shock, you won't have the problem.

Ultimately, the engineers at the British Post Office built 10 Colossus computers, and they were never powered off except when there was a failure. Using this technique, the valves turned out to be quite reliable, and some of the vacuum tubes in the rebuilt Colossus machine that runs today at the National Museum of Computing at Bletchley Park date back to the 1940s.

AFTER THE WAR

All of the technology developed at Bletchley Park remained top secret long after the war. But the knowledge that it was possible to build a fast, reliable electronic computer remained in the minds of those who had worked on the technology. According to Joel Greenberg of Bletchley Park,

> At the end of the war, Turing went to work at the National Physics Laboratory, then he went to the University of Manchester, where Max Newman, who had run the department where the Colossus computers had been located at Bletchley Park ended up as the head of mathematics. At that point, Turing became involved in the very early computer developments in Britain … like the Manchester Baby and Ferranti Mark I. Gordon Welchman immigrated to the United States in 1948 and became involved in many of the early American computing developments, like Project Whirlwind. Welchman worked at MIT and taught the first course in computing science at MIT.

Interestingly, the time pressures of immediate wartime needs at Bletchley Park kept Turing and his colleagues from building more general-purpose computers, but it also meant that they could afford to take big risks on untried technologies, decide to try more than one approach simultaneously, and quickly work out the engineering details on new technologies. Once the war was over and the pressure was off, Turing, Welchman, Newman, and others went back into academia; with more time to reflect, they adapted electronic technologies to build general-purpose electronic computers.

BLETCHLEY PARK TODAY

As a computer scientist, you owe it to yourself to visit Bletchley Park; it's a necessary pilgrimage that helps you fully understand the foundations of our field. What's particularly striking is the juxtaposition of the BOMBE as a highly developed mechanical computing device and the first generation of electronic computing machines in the form of the Colossus. Between the two devices, you can see the seeds of the electronic computing age. It's like comparing a highly refined horse-drawn carriage to the earliest automobile.

One of the goals of Bletchley Park's curators is to make sure the historical systems actually run. When you visit, you can see and feel a rebuilt BOMBE actually running; the Colossus is in daily production as if it were still World War II. As you walk by it, you can watch and hear paper tape whizzing by at 30 miles per hour and feel the heat radiating from the tubes.

Until you can visit in person, watch the video of my visit to Bletchley Park and the National Museum of Computing. I got an up close and personal tour of a running BOMBE and Colossus and spent some time in Alan Turing's office in Hut 8.

Turing was arguably one of the most brilliant mathematicians at Bletchley Park during World War II. He designed or influenced virtually every technology developed there, and whenever a new challenge presented itself, he threw himself into finding a solution.

However, Turing wouldn't have progressed as quickly as he did without the help of other mathematicians, linguists, scientists, and engineers who could quickly validate his ideas and improve on them, and then build hardware that put the ideas into successful production. The quick turnaround on each idea and the need to solve increasingly complex cryptanalysis problems moved computational thinking forward very quickly during that time period.

Sometimes, Turing was at the center of the design of something like the BOMBE and at other times, he was on the periphery, such as in the Colossus's development. As Joel Greenberg says,

> They threw together the smartest people in Britain, and said, "Here is the budget, this is the end game." That is why they [the people at Bletchley Park] invented some of these technologies that probably would not have [otherwise] been invented for years.

The fact that Turing never had to worry about funding his research or even publishing the results in journals (since they were top secret) let him focus on moving his thinking forward as quickly as possible, unfettered with academic minutiae—at least during his years at Bletchley Park.

Acknowledgments

I thank the Bletchley Park Trust, the National Museum of Computing, Joel Greenberg, Paul Kellar, and Kevin Murrell; I also greatly appreciate the insightful comments from the reviewers of the video and article.

***Charles Severance**, Computing Conversations column editor and* Computer*'s multimedia editor, is a clinical associate professor and teaches in the School of Information at the University of Michigan. You can follow him on Twitter @drchuck or contact him at csev@umich.edu.*