

COMPSCI 790

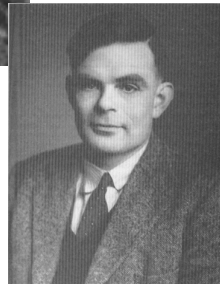
History of Computing and Computers

Assignment 2

The Computing Projects of World War II



Zuse [GILOI 1997]



Turing [SINGH1999]

World War II saw dramatic progress in the computer science. The advances made led to the construction of the first working general-purpose computers. Projects in Germany, England and the United States of America were involved. These projects were carried out independently and to a great extent for different reasons.

To understand why the War brought about such progress, it is first necessary to understand the need for high-speed numerical computation that the machines of war required.

Electronic weapons were not yet invented, and without heat-seeking and radar-guided weapons armies depended entirely upon the accurate aiming of artillery shells. The gunners used “firing tables” to make the necessary calculations to set and then adjust the trajectory of shells being fired. The elevation of the gun, the density and temperature of the air, the wind, the dimensions of the shell and the muzzle-velocity affected the trajectory. The rotation of the Earth also affected longer flights. These calculations were so complex that it required:

“...an average of two eight-hour days to compute the path of a single trajectory” [POLACHEK 1997]

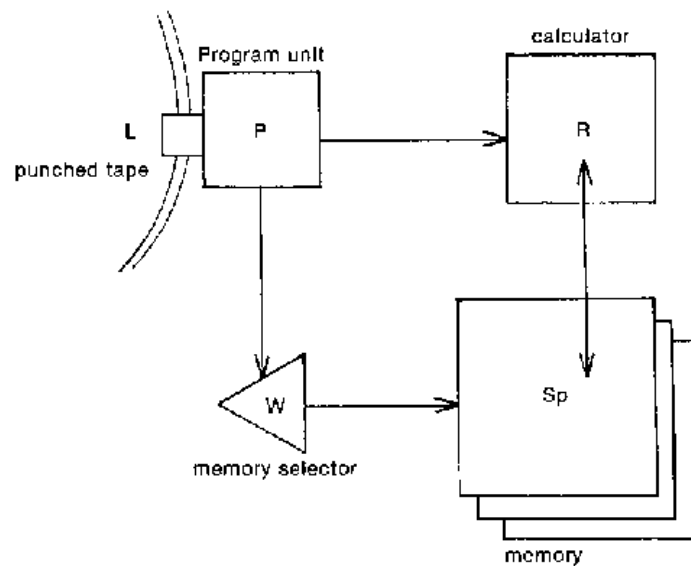
It was the need for faster and better computation of these tables that led to the funding and development of America’s first working electronic computer.

The other major computation requirement was that which cryptography demanded. For thousands of years encryption has been used to protect messages being passed between armies and leaders, armies and armies, and leaders and leaders. Mary Queen of Scots was executed largely because her cipher was vulnerable enough to be broken by Queen Elizabeth’s code-breaker, and the text of the letter intercepted was sufficient to incriminate her [SINGH 1999]. The Germans used cryptography in the form of the “Enigma” machine from the mid-1930s for communication between and within the divisions of its armed forces. The Enigma was an adaptation of a 1923 design by Arthur Scherbius of Berlin [LEE 2000]. The allied forces in World War II desperately needed a way to decrypt and read the secret communications of the enemy.

The German contribution to wartime computing was made by Konrad Zuse, a civil engineer born in Berlin-Wilmersdorf in 1910 [WEISS 1996]. The machines that play a significant role in the history of computing are those nick-named the Z1, Z2, Z3 and Z4: digital computing automatons. Zuse’s standard response to questions on his

motivation for creating these machines was “laziness”. He was troubled by the tedious calculations necessary to civil engineering that were carried out by hand at the time and wanted a machine to do them for him. Zuse also designed and built two special-purpose computers for computing wing corrections needed when building HS293 flying bombs at the German Aeronautics Research Institute (DVL) [GILOI 1997].

Zuse had no formal training in electronics, and he was not familiar with the technology used in mechanical calculators. This gave him a unique viewpoint, and years before John von Neumann mooted the idea Zuse wrote that his calculating machine should have the storage separated from the calculation module. It is not thought that Zuse knew of Babbage’s work on this very subject at the time (Babbage proposed the same basic design for his Analytical Engine). Zuse did find out about Babbage’s work when his patent application was rejected in 1939. Zuse’s machine used binary numbers – this Babbage did not consider. Zuse made use of Leibniz’s work on binary arithmetic [Ceruzzi 1983].



A sketch of Zuse’s architecture c.1937 [CERUZZI 1983]

Zuse completed the memory for his first machine in 1936, instead of using gears as Babbage did, he implemented it using metal rods that slid between two positions giving the binary 0 and 1. A few months later he built the processor. All this construction was performed with the help of his friends in the living room of his parents’ apartment. Given that the machine was the size of a pool table, his parents

must have been very supportive. This machine – the Z1 – worked, but was never reliable [ROJAS 1997].

Zuse's friend Helmut Schreyer suggested that he use electromechanical telephone system relays rather than purely mechanical components. The Z2 followed: it consisted of a relay-based processor coupled with the mechanical memory. Zuse demonstrated the Z2 to the DVL in 1940. They were sufficiently impressed to give him a contract to build the Z3. According to Zuse this demonstration was the only time the Z2 ever worked [WEISS 1996]!

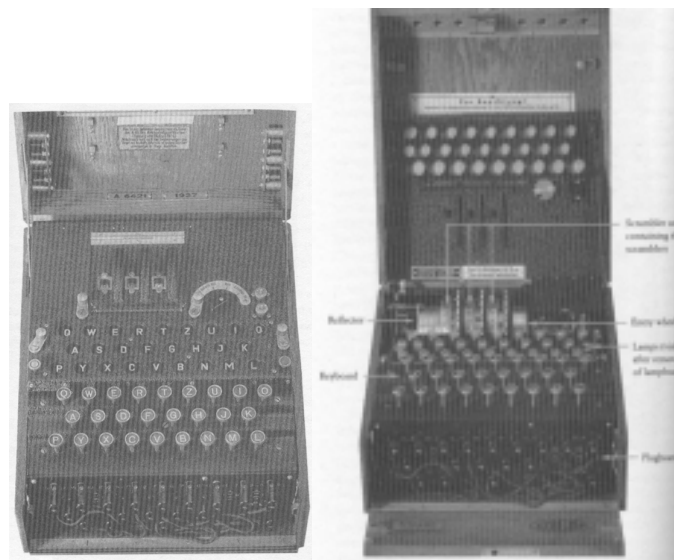
The Z3 had the same logical structure as the Z1, but was built entirely out of relays and far more complex. The Z3 used punched celluloid film as its input – discarded film was much cheaper than paper and more readily available in wartime [CERUZZI 1983]. The Z3 used what Zuse called “semilogarithmic” notation: what it now called floating-point representation. It is interesting to note that the other early machines did not do this. If the Z3 had not been missing an “if” statement it could have been the first general-purpose computer, but it was instead the first programmable calculating machine [ROJAS 1997]. With the Z4 Zuse returned to using a mechanical store, the partially completed Z4 was the only of Zuse's machines to survive the war [RANDELL 1976].

Zuse's other remarkable achievement was the creation of a high-level programming language that he called “*Plankalkül*” – plan calculus – for use with his machines. Zuse presented the concepts of the language in a monograph in 1945. The language featured input variables, intermediate variables and output variables. Data structures could be specified in a binary representation and programs had names that could be invoked in the same manner as a subroutine in a modern language. The language also specified constructs for conditional execution of an equation, and for repetition. The *Plankalkül* seems to have been a forerunner of modern algorithmic programming languages [GILOI 1997].

Unfortunately, due to Zuse's intellectual and social isolation from Britain and the United States during the war, he had no influence over the early projects there.

As mentioned earlier, the German military had been using the Enigma machine since the 30s. The Enigma works by a sophisticated method of character substitution. For every plain language character pressed on its keyboard, a lamp-board displays the

enciphered character. Enigma's main purpose was to protect radio communications, so the radio operator and the Enigma operator would work together, with the radio operator delivering or receiving the enciphered results via Morse code and the Enigma operator encoding or decoding to and from plain text. The press of a key on the keyboard sends a current through a series of rotors – each of which provides a wiring pattern delivering the current from a contact on one side to a contact in a different position on the other side. The current was then reflected back through the rotors to the lamp board. The substitution pattern could be changed by changing the positions of the rotors – i.e. rotating them by a certain amount – or by changing a pattern of patch cables on a plug board at the front, or by changing the ordering of the removable rotors themselves. The ingenuity of the system is that for each character entered, the rotors move forward one position, thereby changing the substitution pattern for every letter. The pattern is of course dependent on the starting position of the rotors, so the sender and receiver had to know which starting position they were using. The starting positions were exchanged by means of “code books”. The Enigma was further enhanced when the rotors were selected from a library of a larger number of rotors, this provided around 10^{23} different encipherings for a three-rotor machine [LEE 2000].



Views of the Enigma closed (left) and open with the rotors visible [SINGH 1999]

Thanks to traditional methods of espionage by the French and the Poles, the Poles under threat of invasion from Germany managed to obtain documents describing the operation of the Enigma machine, and eventually gained access to an actual machine.

The Polish secret service invited twenty young mathematicians to a course on cryptography [SINGH 1999]. These were whittled down to three: Rejewski, Rozycki and Zyglaski [TEE 2001]. Rejewski employed mathematical logic to create a system where by analysing an encrypted message and working through a catalogue of possible chains of encryption that he and the bureau had compiled, the arrangement of rotors could be deduced. It was then just a matter of using “cribs” – recognisable sequences of characters – and other techniques to work out any plug-board settings that had been made. Once that day’s settings had been obtained, any messages on the day could be deciphered. From 1932 the Poles could read all of Germany’s secret communications. When the Germans adjusted Enigma to make it more complex, Rejewski developed a machine nick-named the “Bombe”. The Bombes were mechanised versions of his system of cracking Enigma keys, they analysed messages on a paper tape loop, testing it for feasible keys [SINGH 1999].

In 1939 when the invasion of Poland was inevitable, a meeting was held between the secret services of Britain, France and Poland. The British found it hard at first to believe that Enigma had been cracked, but they took information on the methods employed back to Britain. The Bombes in Poland were destroyed and the mathematicians were evacuated to France, and then later to England [TEE 2001].

The British set up a special code-breaking centre at Bletchley Park, an estate outside London. They gathered together crossword experts, chess masters, linguists, engineers, physicists, mathematicians, logicians and intelligence analysts to form one of the most important intelligence centres of World War II. Amongst the people called to work at Bletchley were Max Newman and Alan Turing [RANDELL 1977].

Alan Turing was born in India in 1912. At the age of 26 Turing published a paper that became the foundation of modern computing, “On Computable Numbers With an Application to the *Entscheidungs-problem*”. Turing set out to construct a universal method for “decide-ability” as challenged by the mathematician Hilbert. Turing invented what is now known as the “Universal Turing Machine”, a theoretical computer based on a tape and a reading/recording head [SINGH 1999]. In doing so he created a solid theoretical basis for computation, demonstrating previously un-realised potential for mechanical computation, that there is a:

“universal automaton which can perform any calculation that any special single-purpose automaton can”
[RANDELL 1977].

Turing was one of the few people at the time that realised the importance of and was influenced by Charles Babbage's work on the difference and analytical engines [TEE 2001].

Thousands of people worked at Bletchley Park, using paper and pencil to decipher enemy radio messages on a daily basis. British versions of the Bombes worked to discover the daily settings of the Enigma machines. Newman set up a section of specialists to create electronic solutions to some of these problems [LEE 1995]. Turing worked with this group between 1939 and 1942. Their first efforts were a series of machines known as the "Robinsons" after the cartoonist Heath Robinson. The machines read two paper tapes at an astounding speed of up to 2000 characters a second, processing Boolean functions on the two inputs and printing decimal output [RANDELL 1977].

In 1942 the German High Command ceased to use the Enigma for their communications, and switched to a new group of ciphers that became known as the "Fish", using a machine known as the Geheimschreiber. Newman posited that only electrons could move fast enough to solve the Fish ciphers [TEE 2001]. With Jack Good and Donald Michie, Turing and Newman conceived the ideas for a series of "Colossus" machines [LEE 1995]. The machines were built by a group of engineers – Tommy Flowers, S.W. Broadhurst and W.W. Chandler at the Telecommunications Research Establishment at Dollis Hill [TEE 1987].

"Colossus had 1500 thermionic valves, and it read paper tape at 5000 characters per second! (When the reader was tested at 9700 characters per second, shreds of paper tape got embedded in the walls of the hut containing Colossus.)" [TEE 1987]

Colossus was working in December 1943 and began producing plain text from the Fish ciphers immediately. Colossus has almost certainly has the place in history of the first working electronic computer [TEE 2001].

It is worth noting that much of the detail about Colossus is still secret. A report on the machine was finally made public in 1999, but the first leaked information on what exactly was going on at Bletchley Park was not available until 1974 [TEE 2001].

At the start of World War II in the United States of America there were three Differential Analysers operational. The analysers were analogue computing devices based on the wheel and disc integrator invented by Vannevar Bush in 1931. An analyser could produce a shell trajectory in around 15 to 30 minutes, but it was not as

accurate as the equivalent hand calculations due to the friction-based action at its heart. The analyser was “programmed” by physically altering the machine with spanners and screwdrivers and so it took a day or more to prepare it for a new trajectory. Even when the “programming” was improved later in the war, a human had to participate in the input of data while the analyser was in operation. Although the U.S. had not yet entered the war, the potential need for the faster generation of artillery firing tables was apparent [POLACHEK 1997].

J. Presper Eckert had entered the Moore School of Electrical Engineering in his home state of Pennsylvania in 1937, when his mother couldn't bear the thought of her only child leaving home early and pursuing his dream to go to the Massachusetts Institute of Technology. The Moore School had been founded in 1923 and Harold Pender, formerly of MIT had as Dean raised the school to a respectable centre of research. When Eckert graduated in 1941 he was made three very lucrative job-offers, but instead accepted a research scholarship to stay at the Moore School [ECKSTEIN 1996].

Eckert served as a teaching assistant in a summer workshop that John W. Mauchly attended. Mauchly was the one-man physics department at Ursinus College in Collegeville. Mauchly was doing meteorological research that required extremely fast counting and calculation – he was convinced that thermionic valve technology would help him but he had encountered much scepticism about using hundreds of valves in one machine. Mauchly found that the idea did not bother Eckert at all and the two spent much time talking together. When a position came up on the teaching staff at the Moore School Mauchly took it [ECKSTEIN 1996][POLACHEK 1997].

Eckert worked part time on radar research in the year following and proposed using mercury in storage delay-lines. Later this became a very important technology for the post-war computers. He built a model of such a delay-line for the Harvard radar researchers [ECKSTEIN 1996].

Eckert and Mauchly spent a lot of time discussing how to make a more electronic differential analyser; they decided that getting rid of all the mechanical components was the only way to do it. In August 1942 Mauchly wrote a memo to the head of research at Moore School arguing for an electronic machine, but it was ignored until Herman Goldstine heard of it. Moore School was working on improvements for the

differential analyser under contract from the army's Ballistics Research Laboratory at Aberdeen. Goldstine was the representative at Moore School from the laboratory. The original memo had been lost, but the secretary who took the dictation still had her shorthand notes and was able to recreate it for Goldstine [ECKSTEIN 1996]. Aberdeen requested a full proposal in March 1943 and Eckert and Mauchly prepared one, it was accepted:

"Eckert would be chief engineer in charge of planning the work and getting it done. Mauchly would continue teaching but serve as principal consultant, and Goldstine would serve on site as liaison from Aberdeen." [ECKSTEIN 1996]

Eckert went to RCA laboratories and enquired as to how thousands of thermionic valves could be kept operating without intolerable numbers of blowouts. He was advised to reduce power levels and turn them off as seldom and slowly as possible. This would reduce the thermal expansion damage that electronic components suffer from when heated and cooled often [ECKSTEIN 1996].

The Electronic Numerical Integrator and Computer (ENIAC) containing 18000 valves and 1500 relays was not completed until the end of 1945 and so was too late to clear the firing table bottleneck, but was a great success and had:

"...evolved into a general-purpose computer with conditional branching facility, and with potentially unlimited capacity available through punched cards (as Babbage had envisaged)." [TEE 1987]

One of ENIAC's first uses was for the Manhattan Project, testing the feasibility of the first hydrogen bomb [CERUZZI 1983].

The ENIAC was not the only wartime American project. A commander in the U.S. Naval Reserve and a Professor of Applied Mathematics at Harvard named Howard H. Aiken was the man behind the machine that became known as the Harvard Mark I.

The Mark I was originally called the "Automatic Sequence Controlled Calculator", and the reasons for building it were very much the same as for the ENIAC: numerical integration for military purposes. The navy provided most of the funding for the project, and it is thought that the machine was used for ballistics, ship design and lens design. Aiken wrote the proposal for his machine when he was still a graduate student in 1937. He was inspired by Babbage, and proposed a machine whereby intermediate results of calculations were passed from one module to another – each module carrying out a different operation – hence the "sequence" in the machine's name [CERUZZI 1983].

The paper-tape driven machine was completed in 1943. IBM supplied the other part of its funding and it was built at the IBM premises using its skilled engineers. IBM distrusted electronic components and the machine was entirely electro-mechanical. Despite Babbage's influence the machine did not have conditional branching [CERUZZI 1983]. This was pointed out to Aiken by the New Zealand born Leslie Comrie and corrected at a later stage [TEE 2001].

World War II no doubt ended the lives of many potential pioneers in computing, but it also redirected funds and resources in unprecedented levels into numerical computation and analysis by machines. It is a pity that the shrouds and secrecy of military activities have hidden the accomplishments of so many people for so many years.

The audaciousness of Eckert and of the engineers of the British Telecommunications Research Establishment in using numbers of thermionic valves never used before, the genius of Zuse in recognizing the power of the binary system, the genius of Turing in recognizing the power of computing itself and the drive and determination of Mauchly, Aiken and others laid the foundations for computing as we know it today. The wartime projects in the U.S.A., Britain and Germany were begun for different purposes but all arrived at more-or-less the same place, more-or-less independently. That place was the birth of the first working general-purpose computers.

References

Ceruzzi, Paul E. **Reckoners : the prehistory of the digital computer, from relays to the stored program concept, 1935-1945.** Greenwood Press, Westport, Connecticut, 1983.

Eckstein, Peter. **J. Presper Eckert.** IEEE Annals of the History of Computing. Vol. 18, No.1 1996.

Giloi, Wolfgang K. **Konrad Zuse's Plankalkül: The First High-Level, "non von Neumann" Programming Language.** IEEE Annals of the History of Computing. Vol. 19, No.2 1997.

Lee, John A.N. Burke, Colin. Anderson, Deborah. **The US Bombes, NCR, Joseph Desch, and 600 WAVES: The First Reunion of the US Naval Computing Machine Laboratory.** IEEE Annals of the History of Computing. July-September 2000. pp 27-41.

Lee, John A.N. Holtzman, Golde. **50 Years After Breaking the Codes: Interviews with Two of the Bletchley Park Scientists.** IEEE Annals of the History of Computing. Vol. 17, No. 1, 1995. pp 32-43.

Polacheck, Harry. **Before the ENIAC.** IEEE Annals of the History of Computing. Vol. 19, No.2, 1997. pp 25-30.

Randell, B. **Colossus: Godfather of the Computer.** New Scientist, 73, 1037, February 1977. pp 346-348.

Randell, B. **The History of Digital Computers.** The Institute of Mathematics and its Applications, November/December 1976. pp 335-346.

Rojas, Raúl. **Konrad Zuse's Legacy: The Architecture of the Z1 and Z3.** IEEE Annals of the History of Computing. Vol. 19, No.2, 1997. pp 5-16.

Singh, Simon. **The Code Book (The Secret History of Codes & Code-breaking).** Fourth Estate. London, 1999.

Tee, G.J. **The Early History of Computing,** Search. Vol. 18, No.6, 1987.

Tee, G.J. **Lectures in "The History of Computing and Computers",** University of Auckland, First Semester, 2001.

Weiss, Eric. **Obituary for Konrad Zuse.** IEEE Annals of the History of Computing.
Vol. 18, No.2, 1996. pp 3-5.