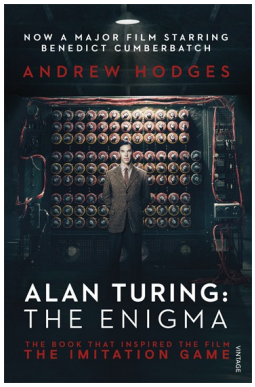
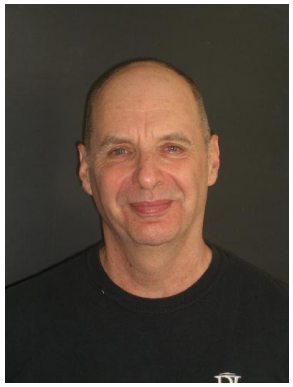
Alan Turing: the enigma by *Andrew Hodges*. Princeton University Press / Vintage, Random House, 2014, ISBN 978-0-6911-6472-4 / 978-1-7847-0008-9 (pbk), 768 pp.

US cover



UK cover



Andrew Hodges

This a practically unaltered pocket edition of *the* biography of Alan Turing that appeared first in 1983. It is published in the UK by Vintage, Random House, and by Princeton University Press in the US. It serves as the basis for the movie *The imitation game* released in 2014 in the US and early 2015 in Europe.

In his foreword, Douglas Hofstadter writes: "Atheist, homosexual, eccentric, marathon-running English mathematician, A.M. Turing was in large part responsible not only for the concept of computers, incisive theorems about their powers, and a clear vision of the possibility of computer minds, but also for the cracking of German ciphers during the Second World War". This one sentence says who Turing was. The biographer Hodges, has an obvious empathy for his subject, being a mathematician himself, working in fundamental physics in Oxford and activist in the gay liberation movement of the seventies. He compiled a well researched biography, and his background allowed him to sketch not only the war history, but also the social situation of English academic life of Turing's lifespan, and to give a clear exposition of Turing's philosophical and scientific ideas concerning mathematics and computer science. He continues promoting Turing and his work in the media and he maintains the website www.turing.uk.org devoted to Turing.

A. Turing at Sherborne

Christopher Morcom

The essentials of the biography has been widespread since the centennial year 2012 (Turing was born 23 June 1912). His father worked for the Indian Civil Service and the parents hopped between England and India, leaving Alan and his elder brother John with a retired couple. During his school days at Sherborne, Alan read Einstein's work at the age of 16 and he has been interested in quantum physics ever since. He lost his faith and became a fervent atheist when his fellow student and dear friend Christopher Morcom died in 1930. During his university studies at King's College, he started his first major work about Turing machines. These theoretical machines were a mechanization for solving Gödel's *Entscheidungsproblem*. His paper was published shortly after the results of Church who obtained the same result via lambda calculus. He showed later that both approaches were equivalent. He visited Church in Princeton where he got his PhD in 1936. The *Institute of Advanced Studies* (IAS) there was a point of attraction for the most prominent mathematicians and physicists of that time like Einstein, Weyl, Von Neumann, Gödel, and Pauli. Several of these were fleeing Europe for the impending Nazi threat. During his US stay, Turing also designed an electro-mechanical binary multiplier and studied cryptanalysis. Back in Cambridge in 1938, Wittgenstein, teaching there on the foundations of mathematics, disagreed with Turing's formalistic approach.

Enigma machine

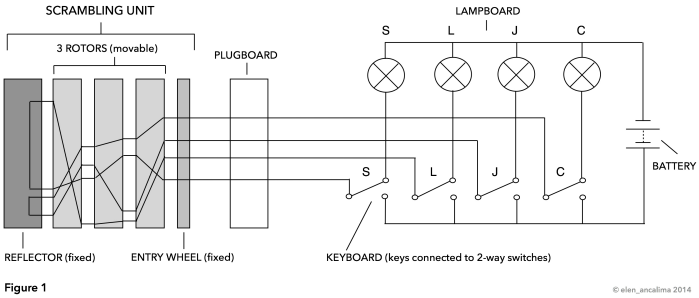
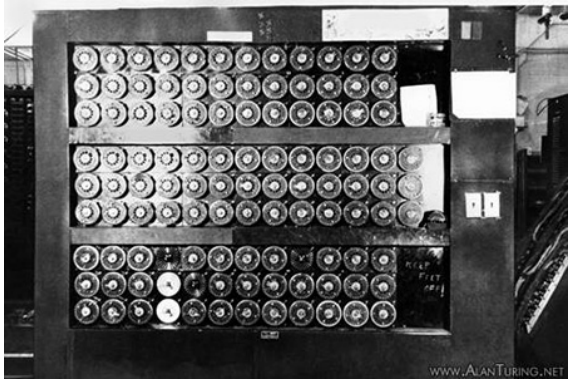


Figure 1

Enigma rotors

Codebreakers at Bletchley Park



The Bombe

Turing's knowledge of cryptanalysis was very useful when he was recruited by the *Government Code and Cypher School* (GC&CS) soon after. The primary goal was to decode the German messages during the war that were encoded via the *Enigma* typewriters by varying the positioning of rotors and the dashboard wirings. The Poles brought some elementary knowledge of this machine and Turing joining an army of code breakers at *Bletchley Park*[1] could automate the process which resulted in the *bombe* an electro-mechanization machine simulating the different settings of the rotors and wirings. Turing was essential for the design of this machine and improvements in subsequent devices like the different versions of the *Colossus*, developed later by Tommy Fowles to analyze the Lorentz cipher. Its design relied on a statistical analysis that went well beyond the bombe that could only make yes or no decisions. It was basically the first programmable digital computer.

Joan Clarke

Joan Murray

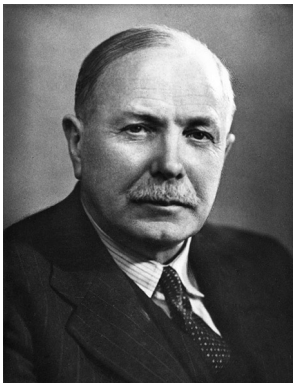
Turing's reports on code breaking were only released by the British secret service in 2012. During this period he developed a passion for long distance running. His mother did not know about his secret work and considered him a bit eccentric. His colleagues experienced him as non-conformist and somewhat on his own. That might be related to him struggling with his homosexual orientation. Nevertheless, he was for a short period engaged to Joan Clarke[2]. In 1942 Alan traveled to Princeton for a year to collaborate with the US Navy on cryptanalysis, and he also visited the people building the first computing machines and he met Nyquist and Shannon at *Bell Labs* who were working on speech processing. After his return

[1] Can be virtually visited at www.bletchleypark.org.uk.

[2] Later Joan Murray after her marriage with colonel John Murray.

he exchanged Bletchley Park for *Hanslope Park* where he designed a device to scramble voice communication (code name *Delilah*).

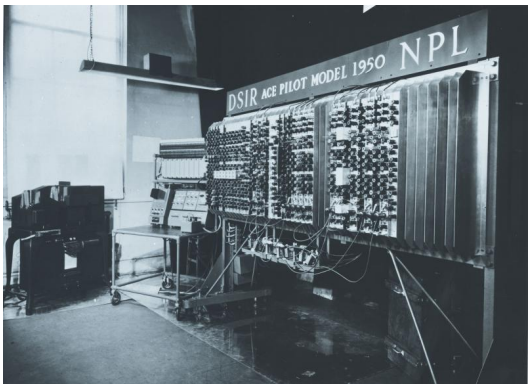
After the war, he joined the *National Physical Laboratory* (NPL) in Teddington, run by the grandson of Charles Darwin. There he worked on the *Automatic Computing Engine* (ACE) project and he produced a report in 1946 for a computer, which contained not only the data but also the instructions to process it, a blueprint for the modern computer. To some extent it was a realization of ideas already present in his abstract Turing machine. His report was well superior to the report of Von Neumann on the EDVAC project. But the pressure and priorities imposed by the war removed and Churchill who had been very supportive of the code breakers being replaced, the ACE project resulted in a working test run only in 1950. In 1948 he was appointed reader at the *University of Manchester* where he continued working on abstract mathematics trying to simulate the human mind. It was then that he proposed the Turing test in an attempt to identify intelligence in a man or a machine. While trying to understand the brain, he started research on the chemical basis of morphogenesis.



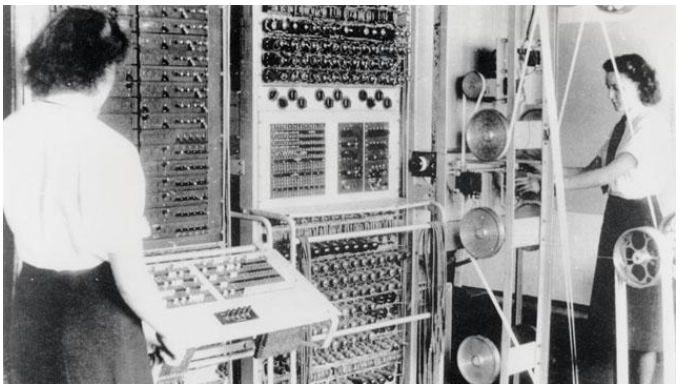
C. Darwin NPL

J. Von Neumann IAS

When he and the much younger working class lad Arnold Murray engaged in a sexual relationship, things went terribly wrong. This "gross indecency" was accidentally detected when the police was investigating a burglary at Turing's house. Turing was condemned in 1952 to hormonal treatment which made him impotent. Two years later, on 7 June 1954, totally unexpected, he was found dead in his home, an apple half eaten nearby and cyanide in the room. The investigation concluded it was suicide.

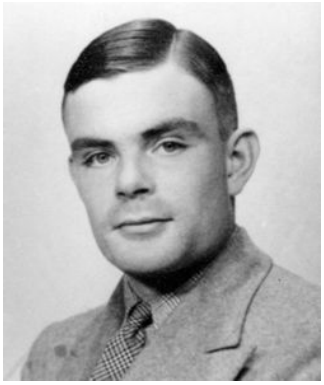


Ace project 1950

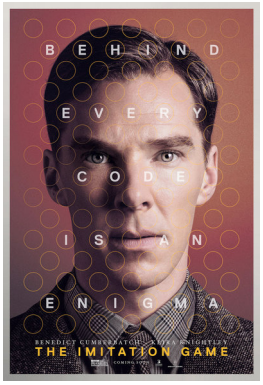


Colossus

Turing was always interested in the theoretical aspects and the possible (abstract) generalizations. For example, these computers could break a code, but he was also thinking of these machines computing the zeros of the zeta function to verify the Riemann hypothesis, an aborted project from his student years at King's College. The practical applications were almost fortunate side effects. He also never considered himself as the leading figure on top of the ladder. He was uncomfortable when people depended on him. Somewhat unorganized, a clumsy negotiator, and politically eccentric, he preferred to work on his own most of the time. With many quotations from letters, reports and testimonies by people who have known Turing, Hodges could give a very clear picture of Turing's character, his mind, and how he arrived at his results. Although his contributions seem quite diverse, in the end they are all rather closely related and very logically connected. It is indeed the ultimate biography of Alan Turing. It will bring you as close as possible to his enigmatic personality.

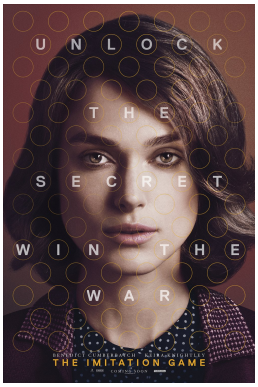


Alan Turing



Benedict Cumberbatch

Joan Clarke



Keira Knightley

The imitation game by *Morten Tyldum* Black Bear Pictures, 2014, 114 min.
Enigma by *Michael Apted.* Jagged Films, 2001, 119 min.
U-571 by *Jonathan Mostow.* Dino De Laurentiis Company, 2000, 116 min.

And then there are the films related to Turing and the code breaking. The most recent is *The imitation game* with Benedict Cumberbatch as Alan Turing and Keira Knightley as Joan Clarke. It is based on Hodges' biography.

No mathematics in the film, except for some senseless scribbled formulas you can see in passing. Only the idea of the Turing test is explained at some point. Turing is portrayed as a 'math professor' with a sympathetic arrogance and a prejudicial degree of autism (people tend to consider all mathematicians and certainly logicians as weird). The former places him immediately in a conflict situation with his boss Denniston. He is mainly shown as an engineer designing and constructing the Bombe with his own hands backed up by Churchill and against Denniston's will.

The director is Norwegian, but the film has a strong American flavor. It collects the most emotive elements of Turing's life: the death of Christopher Morcom, Alan being caught as a homosexual and the subsequent chemical castration, the moment when a convoy had to be sacrificed to keep it a secret for the Germans that Enigma was cracked, and most of all, his relation with Joan Clarke which supports the whole film. Add to this the combination of typical British stiff upper lip kind of humor in combination with the 'extreme logical' reactions by Turing, and of course the suspense element of the drive to break the Enigma code, culminating in the hallelujah moment when they finally succeed. This is in strong contrast with the dramatic ending when Joan visits him, wrecked by his hormone treatment, all underscored by swelling and tear welling music.

Hodges finds the emphasis on the affair between Alan and Joan over-emphasized, although it was not uncommon in British upper class circles of the 1940s that a homosexual man married a women just to meet social demands.

Benedict Cumberbatch does a marvelous job in evoking Turing, as a socially clumsy but brilliant mind. It is difficult not to feel sympathy for this character. There are many historical flaws that geeks will certainly publish on their web sites in due time. However one should take the fim for what it is: entertainment based on historical facts, but entertainment in the first place rather than a documentary.

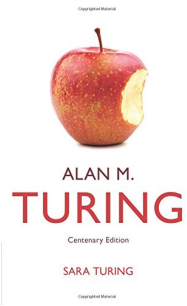
Tom Jericho (Dougray Scott) and
Hester Wallace (Kate Winslet) in Enigma

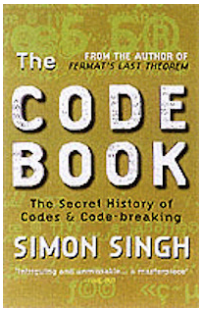
The 2001 film *Enigma* is loosely inspired by Turing's work during the war but is largely fictional. The Turing-like character is called Tom Jericho and is working on decrypting the German codes in 1943. His lover Claire steals some messages and disappears mysteriously. Jericho and Claire's house mate Hester succeed in decrypting the stolen message to find out that it is a cover-up by the British government of the Katyn massacre where Polish nationalists were murdered by the Russians. Claire had revealed this to a colleague who's brother was killed in Katyn and he decides to sell secrets to the Germans as a revenge, which was prevented, and Hester and Tom marry and live happily ever after. The film was co-produced by Mick Jagger who lent his own Enigma machine to be used during the filming.

During the decryption of the Enigma code Germans added more rotors to their machine making the decoding more demanding to break. Decoding would take much more time, possibly producing a plain message only when it was too late. It was of great help that the message from the German U-boats started with a weather message which helped the decryption. However capturing the German Enigma machines and possibly the code book that defined the position of the rotors and the wiring was of utmost importance. And indeed several of such captures have taken place. The one of U-110 in 1940 was inspirational for the action thriller movie *U-571* from 2000. The plot is simple. The German submarine U-571 is damaged and is waiting for help, but the US Navy, arrives first in a German submarine pretending to be the repair team. They can capture U-571, but have to deal with the true help arriving shortly after. Somewhat later they can sink a German destroyer after surviving barely the depth charges. They abandon the sinking U-571 in a life boat saving the Enigma machine and the code books and they are picked up by the Navy.

Mick Jagger's Enigma on the U-571

Alan M. Turing. Centenary edition by *Sara Turing* Cambridge University Press, 2012, ISBN 978-11075-2422-4 (hbk), 194 pp.
The code book by *Simon Singh*. Fourth Estate, 1999, ISBN 978-1-107-02058-0 (pbk), 416 pp.





The mythical figure of Alan Turing and the secret code breaking at Bletchley Park has triggered many other authors to write a book. In fact, shortly after Alan's death his mother, turning 70 at that time, published a small biographical booklet. It got a centenary edition in 2012[3] with an addition by John Turing, Alan's brother. Sara Turing never understood her son very well, and considered him eccentric, and she never knew about his secret work during the war. She never mentions his homosexuality and considered his death to be an accident. In 2012 Sara had passed away, allowing John to be more realistic to place her account into a proper perspective.

[3]For a more detailed review see this Newsletter issue 90, November 2012.

If you want to know more on code breaking and cryptanalysis in general, you could (among many others) consult Simon Singh's *Code book*. He sketches the history of cryptography from Caesar, over Mary Queen of Scots, to the *chiffre indéchiffrable* attributed to de Vigenère (1523-1596). A Caesarean code just shifts the letters of the alphabet, and the Vigenère code is a sequence of Caesarean codes with different shifts. It resisted 3 centuries but was finally cracked in 1863. Of course a major part is devoted to the Enigma code breaking efforts during WW II. Singh also discusses the translation of forgotten languages like the Egyptian hieroglyphs and the Mycenaean linear B. The puzzle is very similar to code breaking. Finding a "Rosetta stone" or a piece of it definitely helps. In fact one of the "codes" that were never cracked during WW II, was an old Navajo language only spoken by a specific tribe that had not been exposed to foreign (read German) infiltration. Navajo code talkers were recruited for secret communication. Singh also explained the post-war evolution with public-key cryptography, in particular RSA code (published in 1971 by Rivest, Shamir, and Adleman) and the PGP protocol (Pretty Good Privacy, by Zimmermann in 1991). Practical public-key cryptography depends on the fact that prime number factorization for very large numbers takes too much time to do with the current state of the technology. In simple terms: Alice publishes her public key which is the product of two large primes and keeps one of the primes as her private key. If Bob wants to send a message to Alice, he encrypts her message with her public key and Alice can decrypt it because she has her private key. The original ideas were developed early 1970 inside de British GCHQ (*Government Communications Headquarters*) which was the new name of the GC&CS used since 1946. However, this material was classified and was only released in 1996. So it was the RSA team at MIT that published their work in 1978 and got all the credits. This kind of cryptography is used a zillion times a day in secure internet communication or in digital signatures. It is ironic that G.H. Hardy took a pacifist point of view by studying number theory, because he said, it was the only part of mathematics that had no practical applications, and thus could not be used in a malicious way. Clearly this type of encryption is only safe as long as it will take too long to compute the prime number factorization. Singh therefore also give a glimpse on quantum computing which would be able to crack this major security guard. He even explains what quantum cryptography could be like.

Linear B 1450 BC

Navajo code talkers WW II

The nice thing about Singh's approach is that he confronts the reader with a problem that seems impossible to solve, and then takes him along on the steps, often corresponding to the historical steps taken, to eventually solve the problem and break the code. At the end of the first edition he offered a Cipher Challenge of 10 code puzzles for the reader to break. A prize of 10,000 pounds was offered for the first one to solve them. It was won in 2000[4]. Singh has a PhD in physics and has authored several popular books dealing with mathematics such as Fermat's Last Theorem, the Big Bang, etc.

A. Bultheel

[4]I read the 2000 edition where that was announced, but you can also read about it on the author's web page `simonsingh.net`.