University of Technology

Office for International Study Programs

Alan Turing and the Engima cipher

Introduce to Computing

Submitted by:

Nguyen Le Phu Hoa

Doan Anh Tien

Lecturer: Mai Duc Trung

April 13, 2019

1 Preface

Despite of the fact that a minority of people in the previous years conscious of his achievements, it is only a slight exaggeration to say that the British mathematician Alan Turing (1912-1954) saved millions lives during the WWII, invented the artificial intelligence, and anticipated homosexual liberation throughout the decades.

Alan Turing's electronic design - Bombe - was directly related to his leading role in breaking the German Engima cipher, a scientific triumph which was a greatest threat to the Allied's cryptogram cracking process. Simultaneously with the event, this was also a beginning of the tragic life of Turing who, despite of his contribution, was arrested and forced to suffer a humiliating treatment program, leading to his suicide at age forty-one.

I would recommend you to have a look on The Imitation Game (2014) movie, a gripping story of mathematics, computers, cryptography, and homosexual persecution; perhaps after reading our report/presentation. Therefore, you would be able to comprehend both the inner and outer drama of Turing's life while getting know an outlook of how the Enigma cipher working.

Figure 1: *Alan Turing (played by Benedict Cumberbatch in The Imitation Game)*

Contents

2 Enigma

Enigma German machine was supplied with 26 buttons indicating all alphabetical signs and used a scheme that was quite similar to what we call QWERTY.

Figure 2: *Close look at Enigma Machine*

Inside the box, the system is built around three physical rotors. Each takes in a letter and outputs it as a different one. That letter passes through all three rotors, bounces off a "reflector" at the end, and passes back through all three rotors in the other direction.

When the first rotor has turned through all 26 positions, the second rotor clicks round, and when that's made it round all the way, the third does the same, leading to more than 17,000 different combinations before the encryption process repeats itself.

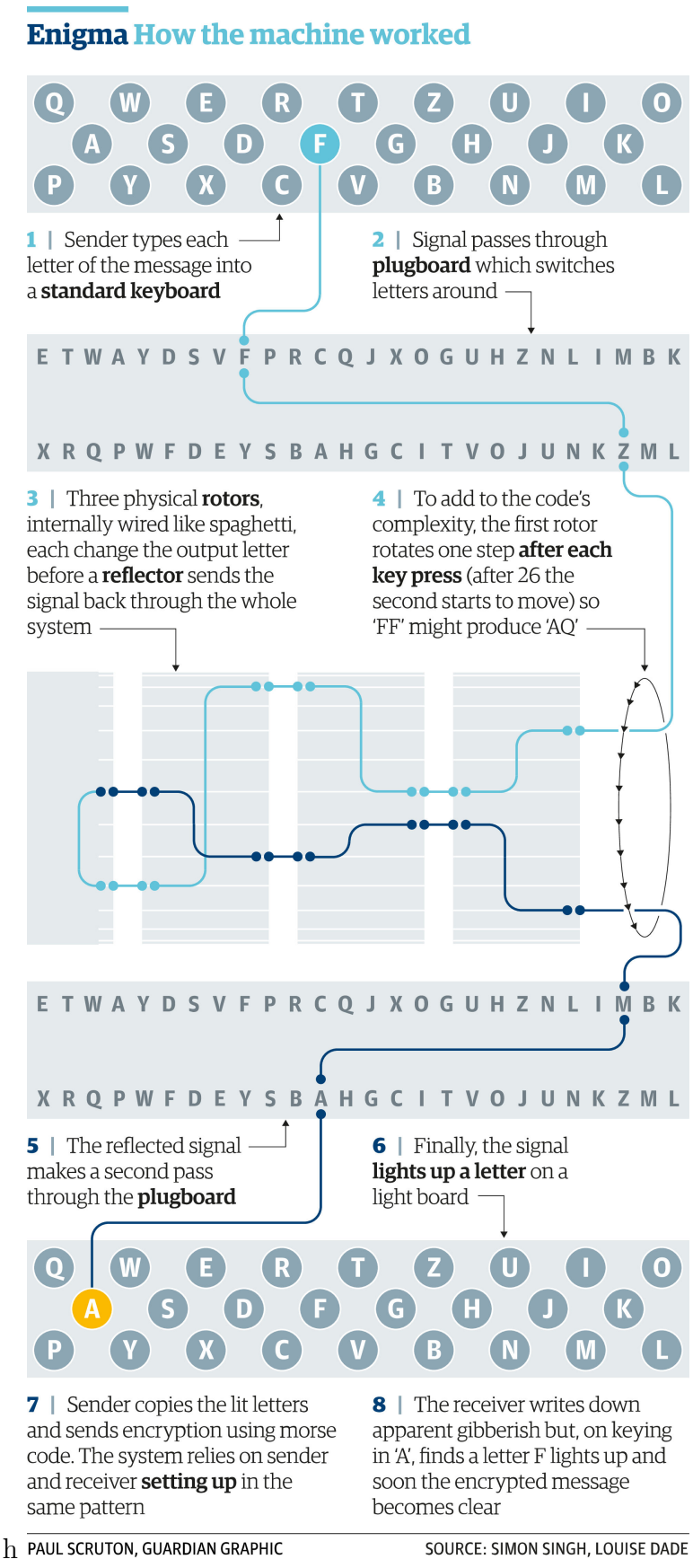

Figure 3: *Mechanic of Enigma*

3 Alan Turing

Alan Turing, in full **Alan Mathison Turing** (born June 23, 1912, London, England—died June 7, 1954, Wilmslow, Cheshire) is an mathematician and logician, who made major contributions to the victory of **Allied** against **Nazis** during WWII, the area of mathematics, cryptanalysis, logic, philosophy and also the new ones later known as computer science, cognitive science and artificial intelligence.[1]

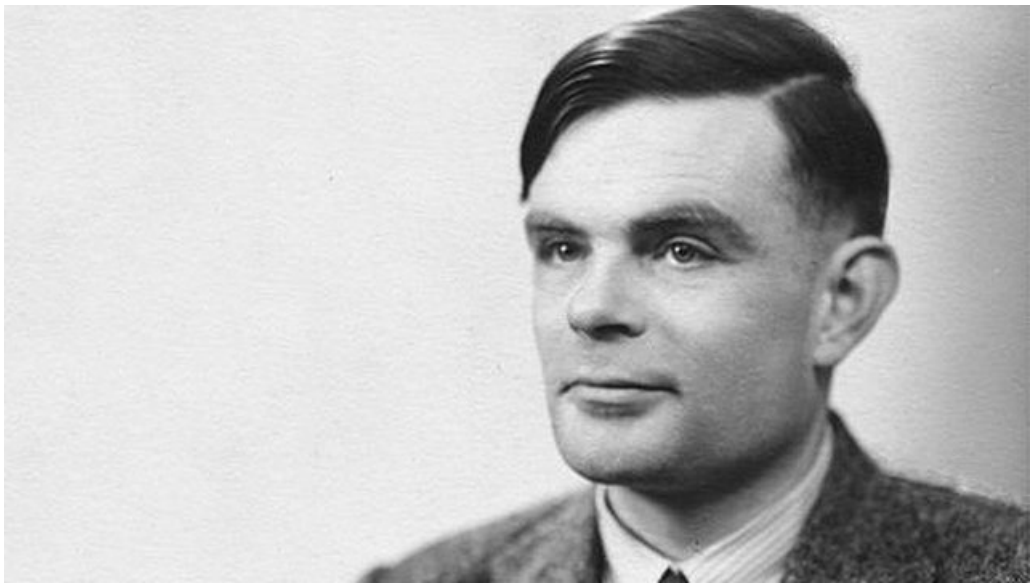

Figure 4: *Alan Turing - a British mathematician*

Alan Turing had a dramatic ambition in acquiring knowledge which paved a way for him to study advanced modern scientific ideas, such as relativity, on his own, running far ahead of the school syllabus. Turing later won a scholarship to King's College, Cambridge, and took the Mathematics degree with distinction in 1935.

After two years at Princeton, developing ideas about secret ciphers, Turing returned to Britain and joined the government's code-breaking department, **Bletchley Park**.

4 Breaking the Enigma

Germany's Army, Air Force and Navy transmitted many thousands of coded messages each day during World War II.
These ranged from top-level signals, such as detailed situation reports prepared by generals at the battle fronts, and orders signed by Hitler himself, down to the important minutiae of war like weather reports and inventories of the contents of supply ships

4.1 Bletchey Code-breaking Team

On the first day of war, at the beginning of September 1939, Turing took up residence at Bletchley Park, the ugly mansion that served as the wartime HQ of Britain's top codebreakers. There he was being treated as a burdensome freak at first but later then became a key player in the battle to decrypt the coded messages generated by Enigma, the German military's typewriter-like cipher machine.

Figure 5: *Bletchley Park (today), Buckinghamshire, England*

A secret code-breaking team, known as **Ultra**, had been founded and operated by Alan Turing and his fellow - Britain's most valuable code-breakers

4.2 Struggles against German Enigma

The Enigma was a type of enciphering machine used by the German armed forces to send messages securely. Although Polish mathematicians had worked out how to read Enigma messages and had shared this information with the British, the Germans increased its security at the outbreak of war by changing the cipher system daily. This made the task of understanding the code even more difficult.[2]

Figure 6: *The German enciphering machine - Enigma*

It was just before the war started when Poles decided to share their 8-year work achievements with united nations - copies of Engima. Each delegation was given a photocopy of full documentation and one replica of Enigma. Machines were immediately sent to Paris and London where local scientists quickly researched their construction and settings.

Although Allied disposed money in huge numbers, they were not able to decipher Enigma. What is more, they could not even get close to breaking the code used by Germans.

On the 1^{st} of September German Army crossed the Polish borders giving a sign to start World War II, the biggest conflict in the human history.

5 Bombe

In May 1940, Germans changed the indicator system and made all the perforated sheets useless, leading the British to develop new solutions. At this time Turing had already started constructing the bombe which completely changed the course of war.
To decipher Enigma message codebreakers needed four factors – rotors, Ringstellung, plugboard connections, indicator-setting. Turing was not able to face his problem so he was helped by experienced constructors.

"The bombe weighed about one ton, was housed in a bronze-coloured metal cabinet about 7 feet wide, 6 feet 6 inches tall and 2 feet deep and was mounted on castors. Protruding from the front of the cabinet there were 108 shafts (more in some models, fewer in the two prototypes) arranged in three 12 x 3 arrays on which drums were mounted" - Graham Ellsbury.[3]

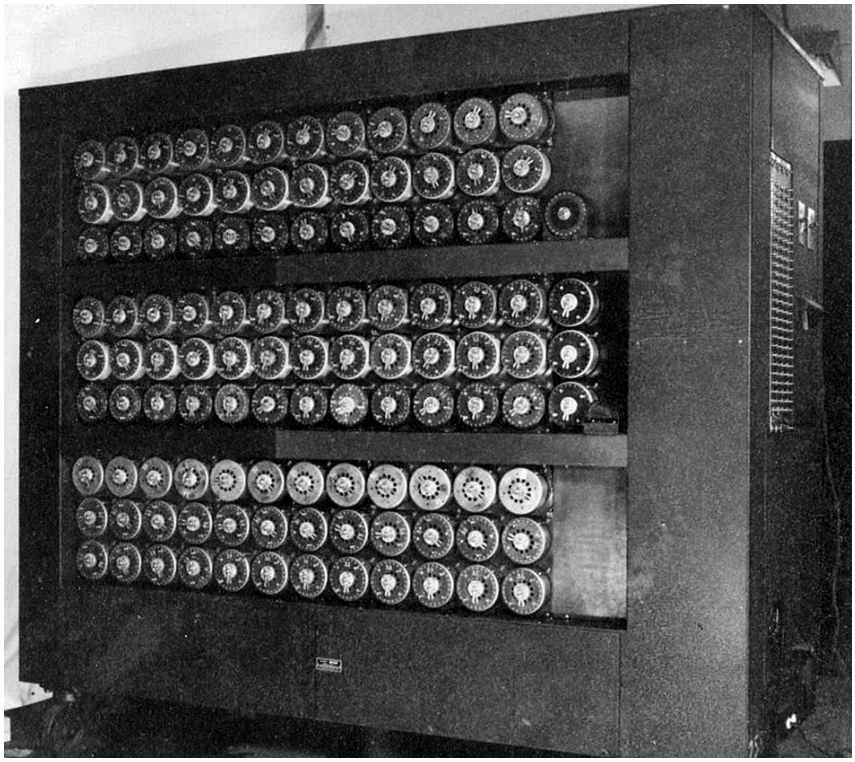

Figure 7: *Wartime picture of Bletchley Park Bombe machine named Victory*

The theoretical background of the bombe idea needs specific mathematic knowledge, that is why it will be skipped and we just need to know that the electro-mechanical system can reconstructed original settings of Enigma.

In fact, the first step was to limit these possible settings to manageable number and find the proper one. Bombe "searched all the settings and disregarded those that were incorrect. For example, if the assumed letter was G and the corresponding cipher letter was L, Turing's test register ignored any results that did not allow the electrical current to pass from G to L. By disproving thousands of rotor settings, those left were possible correct settings". That process was called "Banburismus".[4]

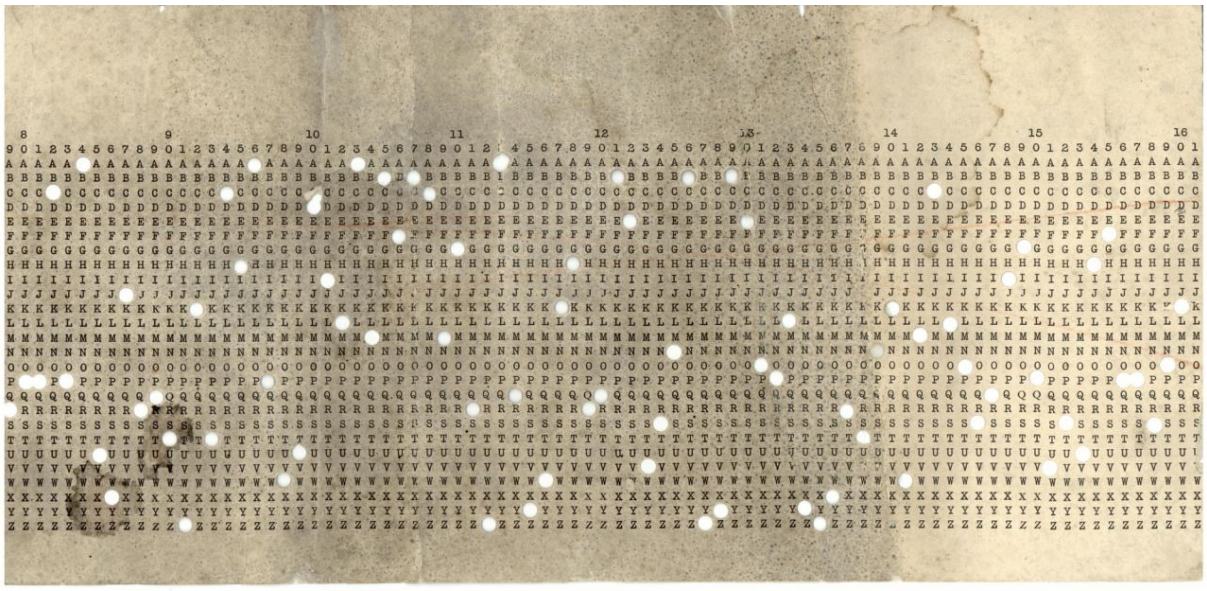

Figure 8: *"Banbury Sheet" from World War II (recreated)*

The process of "Banburismus" appeared to be the best way of constructing new electro-mechanical devices. The results were shocking – from the second half 1943 till the end of the war Bletchley Park was able to decipher 84 000 German Enigma messages per month103. The numbers are extremely high but it should not be forgotten that operation engaged almost 9000 people grouped in many teams. The operation Ultra became one of the most secret missions in the history of World War II.

Type	**Number of Enigma-equivalents**	**Mechanism**	**Number built**
Original standard	36	3-rotor Enigma-equivalents	73
Jumbo	36	3-rotor Enigma-equivalents plus an additional mechanism to check each stop and print the results	14
Mammoth	36	4-rotor Enigma-equivalents with high-speed relays to sense stops	57
Cobra	36	4-rotor Enigma-equivalents with an electronic sensing unit designed by C.E. Wynn-Williams and Tommy Flowers' team at the GPO Research Station (this machine was unreliable)	12
New standard	36	3-rotor Enigma-equivalents (with high-speed Siemens-type sense relays)	68

Table 1: *Main British (BTM) bombe types* [5]

6 Results

In February 1946 (Turing post-war life), he presented paper on designing Automatic Computer Engine. It was not the end of his researches. Although his project was not executed he had a huge impact on worldwide scientific approaches.

He suggested the experiment called "Turing's test" that could prove or not whether machines could think or not. The Turing's test was based on convincing independent human judge by machine that machine is a human being. The imitation game was later a source of Turing's different discoveries that led him to creation of the chess program.

In his seminar work he asked a question "whether there are imaginable computers which would do well (in playing against humans). The answer, what Turing proved with his concepts of machines, was simple – they could. In fact, Turing predicted "that machines will eventually compete with men in all purely intellectual fields.

In the next few years Turing worked at mathematical biology and in 1952 he published "The Chemical Basis of Morphogenesis" dealing with some Fibonacci's theories, including his famous sequences present in the natural environment.[6]

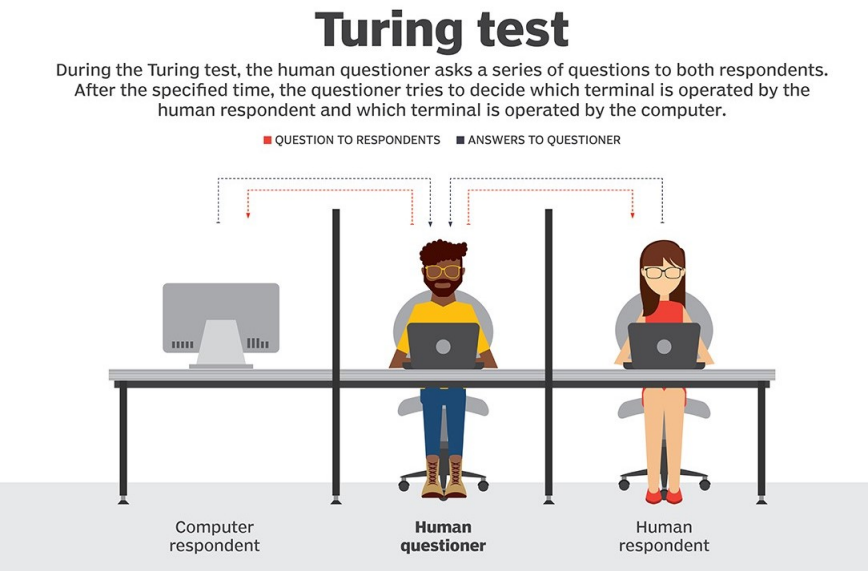

Figure 9: *Turing test*

7 Discussion and Outlook

The history of Enigma operation for many years could not be openly told. Many efforts of many nations were not wasted – their involvement, devotion (usually underestimated) laid a groundwork for the allies' victory. It could not have been achieved without researches conducted by Polish Cipher Bureau commanded by Gwido Langer, without many years of organizational work of Maksymilian Cieżki, without genius brains of Rejewski, Zygalski, Różycki and many less prominent scientists who anonymously worked behind the scene although they also were crucial part of the codebreaking team.

It is not appropriate way of describing Polish success although underestimating or devaluating significance of Polish researches and their influence on Turing's works is evident bias or even changing the course of history. All nations engaged in the process of codebreaking had their own moments of triumph and they built a way to the final victory with constructing Ultra system and regular deciphering of German messages.

In 1952, Alan Turing was arrested for homosexuality – which was then illegal in Britain. He was found guilty of 'gross indecency' (this conviction was overturned in 2013) but avoided a prison sentence by accepting chemical castration. In 1954, he was found dead from cyanide poisoning. An inquest ruled that it was suicide.

The legacy of Alan Turing's life and work did not fully come to light until long after his death. His impact on computer science has been widely acknowledged: the annual 'Turing Award' has been the highest accolade in that industry since 1966. But the work of Bletchley Park – and Turing's role there in cracking the Enigma code – was kept secret until the 1970s, and the full story was not known until the 1990s. It has been estimated that the efforts of Turing and his fellow code-breakers shortened the war by several years. What is certain is that they saved countless lives and helped to determine the course and outcome of the conflict.

List of Figures

List of Tables

References

[1] B.J. Copeland and Michael Dear. Alan Turing - British Mathematician and Logician. *Encyclopedia Britannica*, 1999.

[2] IWM Staff. ENIGMA AND THE BOMBE. *IWM*, 2018.

[3] Graham Ellsbury. The Turing Bombe: What it was and how it worked. 1998.

[4] Wilcox E.Jenifer. Solving the Enigma: History of the Cryptanalytic Bombe. 2001.

[5] John Harper. Bombe Types. *The British Bombe CANTAB*, 2007.

[6] Mateusz Łabuz. The Great Expectations - Allied Codebreakers against German Enigma. *Pedagogical University of Cracow Faculty of Humanities- Thesis*, 2012.