**Important figure in Cryptography-Alan Turing**

Alan Mathison Turing – Perhaps the most famous Cryptographer from recent history. Known for his work in Hut 8 of Bletchley Park during World War two to crack the seemingly unbreakable “Enigma Code” used by the German’s as a commercial and military encryption tool.

Born in London on the 23rd of June 1912 Alan Turing made significant contributions to mathematics, cryptanalysis, philosophy, logic, biology and in fields later known as computer science, cognitive science, artificial intelligence and artificial life.

Alan Turing attended a top Private school called Sherborne at age thirteen where he became particularly interested in science and mathematics.

After Sherborne, Turing enrolled at King's College (University of Cambridge), studying there from 1931 to 1934 where he received an M.A. upon his graduation. While there he was awarded a Smith’s prize for his work on probability theory in 1936. As a result of his dissertation at King’s College, in which he proved the central limit theorem. Turing was elected a fellow at the school. In 1936 Alan presented a paper "On Computable Numbers, with an Application to the Entscheidungsproblem," in which he presented the notion of a universal machine (later called the “Universal Turing Machine," and then the "Turing machine") capable of computing anything that is computable. This seminal paper was recommended by an American logician, Alonzo Church, who had published a paper of their own that reached the same conclusion as Turing using a different method. (*Stanford Encyclopaedia of Philosophy, 2013*)  
Alan Turing’s proposal of the “Universal Turing Machine” is considered to be the precursor to the modern computer.

Alan then moved to Princeton University, New Jersey, for the next two years to study for his Ph.D in Mathematics and cryptography under the direction of Alonzo Church.

Returning to his fellowship at King’s College in 1938 Alan Turing went to join the Government Code and Cypher school for a part time position. (*Copland, 2020*) Once the war started in September of 1939 Alan was moved to organise the wartime headquarters at Bletchley Park, Buckinghamshire. Primarily working in Hut 8 to break the German Naval cipher.

Five weeks before the beginning of the war the Polish government had given the British and French details of their success against the Enigma cipher used by the German military to encrypt their communication.

A small Polish team led by Marian Rejewski had deduced the internal wiring of the Enigma machine as early as 1932 and by 1938 the Polish team had created a code breaking machine that was called the Bomba. In 1940 German cypher procedures changed, making the Bomba useless by adding new rotors to the Enigma machine. (*Copland, 2020*)

During the autumn of 1939 and the spring of 1940, Turing and the team in Hut 8 at Bletchley Park designed a machine similar to the Bomba. The Enigma code-breaking machine called the “Bombe” in ode to the Polish design before it. The Bombe used rows of rotors similar to the Enigma rotors to find the most likely pathways used to encrypt the message. The Bombe reduced the amount of time it took for the teams in Bletchley Park to decrypt messages they intercepted but had a few flaws, in that there was only one machine available and multiple Huts were in need of it. This issue was quickly fixed and the design plans were also shared with American code breaking teams.  
Turing’s contribution to the effort was not just the overseeing of the team in Hut 8 or the assistance in the design of the Bombe. According to the GCHQ (Government Communications Headquarters) which at the time was the Code and Cypher School, Alan also wrote two papers on a mathematical approach to code-breaking which were extremely valuable and such an important asset that they were kept hidden until 2012 when the GCHQ released them to the National Archives of the United Kingdom. (*The Papers of Alan Mathison Turing | The National Archives, n.d.)*

Over the course of the war the Allies used these Bombe machines to decipher large quantities of military intelligence. By early 1942 Alan Turing's team in Bletchley Park were decoding approximately 39,000 intercepted messages each month. This figure rose substantially to more than 84,000 per month. Approximately two messages every minute, day and night.

After the war Alan Turing worked with the National Physical Laboratory in London to create an electronic computer. Alan was the first to submit a complete specification for his Automatic Computing Engine (ACE). Alan Turing’s design was considered too difficult by his colleagues at NPL to engineer and a smaller design was favoured, the Pilot Model ACE (1950). However, had Alan’s design been constructed as he planned it would have vastly more memory than any other early computer and would be faster. However, the Royal Society Computing Machine Laboratory at the University of Manchester created their own computer in June of 1948. Discouraged by the NPL Turing moved to take the position of Deputy Director at the University of Manchester where his earlier theoretical concept of the Universal Turing Machine had been a fundamental influence. Now working in the University of Manchester Alan Turing designed an input-output system and a programming system. He also wrote the first ever programming manual and this system was used in the first marketable electronic digital computer in 1951, the Ferranti Mark I. (*Copland, 2020*)

Alan also established the foundations of artificial intelligence and cognitive science in the year 1950 with his “Turing Test.”

Elected a fellow of the Royal Society of London in March 1951 Alan Turing’s success rapidly turned the next year. In March of 1952 Alan Turing was convicted of “Gross Indecency” for his homosexuality, which was a crime in Britain at the time. Alan was given the choice of imprisonment or twelve months of hormone therapy. Choosing the later Alan Turing, now with a criminal record, was stripped of his security clearance and was barred from his position in the GCHQ.  (*Alan Turing, 2019*)

Alan spent the next two years in Manchester where he was appointed to a specially created readership in the theory of in May 1953 and since 1951 Alan was working on what is now known as artificial life and published “The Chemical Basis of Morphogenesis” in 1952.(*Copland, 2020*)  
Amidst this ground-breaking work Alan Turing was discovered dead in his bed by cyanide poisoning. The Inquest in 1954 determined the death to be a suicide but no motive was found. Alan had taken to his Hormone treatment with what his close friend Peter Hilton referred to as “Amused fortitude,” and there was nothing to suggest a chemical imbalance as the treatment had ended a year earlier. Assassination by a secret service could not be ruled out and Alan Turing’s death could have been an accident as he had a small laboratory adjacent to his bedroom that contained experiments with cyanide. (*Alan Turing, 2019*)  
Alan Turing’s death was recognised as a great tragedy and in 2009 Gordon Brown, the British Prime Minister at the time, issued a public apology on behalf of the British government on how Alan Turing was treated. In 2013 Queen Elizabeth II granted Alan Turing a posthumous Royal Pardon of all crimes he was accused of and in 2016 “Turing’s Law” was announced to posthumously pardon thousands of homosexuals and bisexual men who were convicted unfairly. (*Alan Turing, 2019*)

## **References**

*Biography.com. 2019. Alan Turing. [online] Available at: <https://www.biography.com/scientist/alan-turing> [Accessed 10 May 2020].*

*Copeland, B., 2019. Alan Turing | Biography, Facts, & Education. [online] Encyclopedia Britannica. Available at: <https://www.britannica.com/biography/Alan-Turing> [Accessed 9 May 2020].*

*Discovery.nationalarchives.gov.uk. n.d. The Papers Of Alan Mathison Turing | The National Archives. [online] Available at: <https://discovery.nationalarchives.gov.uk/details/r/3a9b1600-921c-4200-98cf-20b8c8617ce4> [Accessed 10 May 2020].*

*Plato.stanford.edu. 2013. Alan Turing (Stanford Encyclopedia Of Philosophy). [online] Available at: <https://plato.stanford.edu/entries/turing/> [Accessed 10 May 2020].*