Important figures Draft

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.

To understand the importance of Alan Turing’s work and the reason for his fame we first need to understand the Enigma Machine and its implementation during the war.  
  
The Enigma Machine was considered unbreakable at the time due to the sheer number of permutations that were possible and the apparent randomness of the encrypted messages.   
The machine appeared much like a typewriter but through a series of ten plugs mapping pairs of letters, three of eight rotors marked with the numbers one through twenty-six and a reflector. The Enigma Machine scrambled every letter almost randomly every time a key was pressed. The encryption was used in three different ways with varying difficulty in the decryption process.

Used commercially the Enigma Machine featured only the three rotators and reflector. First the message that was to be encrypted would be written out and the start positions of the rotors noted. Upon pressing a key, the right most rotor would turn one position and an electrical signal sent through the rotors. The internal wiring of the rotors assigned an input “Stud” with an output “Stud” representing the letter entering the mechanism and the assigned output which in turn would enter the second rotor and repeat. Exiting the third rotor the signal would be reflected back through the rotors on the opposite side, upon passing through all three rotors a second time the output would then be displayed on a lamp board to show the encrypted letter. This encrypted letter would be noted and the process was repeated for each letter in the message and for every full revolution of the first rotor, the second would turn one position and so on for the third.

The first military use of the Enigma Machine was for the army and air force of Germany and it was considerably harder to break the cypher due to the addition of two exchangeable rotors and the plug sockets at the front of the machine. Functionally similar to the commercial version this enhanced form was much more secure.   
When a key was pressed on this military version the rotation of the first rotor was the same however the electrical input signal was redirected from the letter pressed, through the plug to the assigned pair, thus changing the input to the rotors. The rotors functionally identical to the commercial version however with the introduction of the two extra rotors with completely different wiring made it very difficult to track which were used and what position they were in. The governed starting position for the machine was given to radio operators and communication centres at the start of each month. Outlining all setting the machine would have for each day. The rotors name, which were roman numerals, in order of use. Then the starting positions and the letter pairing of the socket plugs.  
This means that not only did the Enigma Code change daily but no two months were the same.

Finally, the German Navy version of the Enigma Machine was the most complicated of them all. For fleet ships three new rotors were introduced, these three new rotors when in position two or three in the Enigma Machine would rotate every thirteen letters instead of once each revolution. Submarines were valuable to the German navy and as a security measure the messages sent to and from them would use a modified machine that used four of the now eight rotors. Admiral Karl Dönitz enforced this change as he feared that the German codes had been at least partially broken

Alan Turing worked alongside many notable people in Hut 8 such as Conel Hugh O’Donel Alexander. The work of the team in Hut 8 of Bletchley Park was set up by the Polish at the beginning of the war. With the assistance of a German spy who seceded by the name of Hans-Thilo Schmidtthe Polish Cipher Bureau managed to break the original Enigma code used in the German military. Using a machine known as the “Bomba” along with punctured sheets of paper they were able to decipher the early code used by the German army and air force. Sending their information to the French and British the Polish team under Marian Adam Rejewski provided the groundwork for those at Bletchley Park. However, the method could not be used once the two extra rotors were introduced and the information was shared with the Allies five weeks before the German invasion of Poland as such the Polish research was halted.

On May 9th 1941 the allies captured a German U-boat, U110 in the northern Atlantic with a complete enigma machine and the key for that month allowing the allies to intercept encoded messages for a few weeks. The teams at Bletchley Park were given the materials and the task of breaking the Enigma code. Hut 8 was among those assigned to the task. For the early periods of the war it seemed impossible, however, Alan Turing discovered the major flaws of the Enigma code towards the end of 1942. As a Mathematician and a Statistician, he noted two key features of the cypher. First, was that any letter entered into the Enigma Machine never produced itself as an output. Second was the change in when the machine was given pairs of letters such as the two l’s in ‘Hello’. With these traits known all that was needed was a reliable, repeated word encrypted through the Enigma Machine. Thankfully, every morning at six o’clock a weather report was sent in Germany using the Enigma code. “Wetterbericht” being the German for the weather report provided a good start for the decryption teams to start decrypting the message and to find some of the settings used. The repeating “t” helped to discern where in a string of code the word might be, as a letter is never mapped with itself and is changed immediately. The multiple “e” in the phrase helped deduce which right most rotor was used and which position it started in based on the internal wire mapping. This deduction bled into the second rotor where after one full rotation the output would change and expose the second rotor and onto the third if the word count was sufficient enough. This process was dubbed Banburismus and shortened the length of time needed to decrypt a message. Banburismus was a development on the work of Jerzy Witold Różycki, a colleague of Marian Rejewski who worked on the Bomba.  
Hugh Alexander and I.J. Good were the most skilled in this Banburismus method in Hut 8.  
However, this method was laborious and time consuming to do by hand. So, Alan assisted in the construction of a decryption machine that when fed the encrypted message, using modified versions of the Enigma rotors, would search the pathway used in that day’s code. The machine was named the Bombe, in ode to the Bomba it followed. With this machine the Enigma code could be broken in twenty minutes every morning.  
The work of Alan Turing and all that assisted the team in Hut 8 was crucial in the outcome of the Second World war and is said to have shortened the conflict substantially.