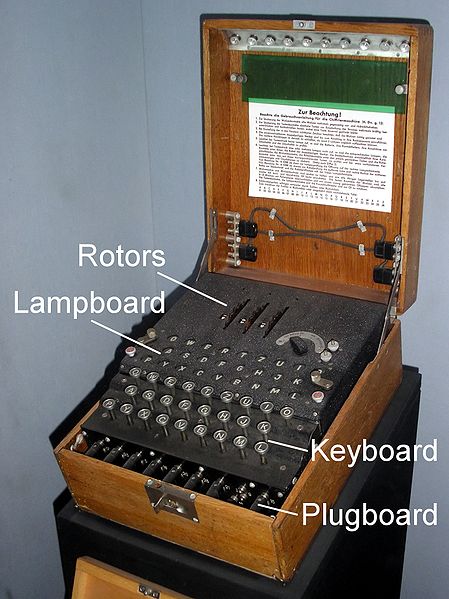
Author of the Essay: Sarang Kharche (150740395)

Word Count: 1712

**The Enigma Machine**

In this essay, the information will be analytically presented which includes the brief history, technology used, flaws, shortcomings and impact of human behaviour on the Enigma machine . The Enigma machine is a crypto device hardware which was invented by the Germans and used by British codebreakers as a way to decipher German communication during WW2. Several types of Enigma machines were developed before and during WW2, each one with added complexity, of all the army segments the German Navy used the most complex machine. The machine was developed by a German engineer Arthur Scherbius. This device allowed the operator to type in a message, then scatter it using 3 to 4 rotors which then displayed different (cipher) letter of the alphabet. On the other hand, the receiver needed to know same settings of the rotors in order to get the correct message. The basic operating was simple, to send an encrypted message the operator set the electric (plug wiring) and mechanical setting (rotor wheels) to a pre-decided combination which is known to himself and the operator on the other side.

[[1]](#footnote-1)

To send the message the sender typed the text message on the machine’s keyboard, for each typed letter a different ciphered letter was lit in the upper board bulb panel. These lit letters were written down by the sender, after finishing the original message on the Enigma machine the sender would have some random cypher text for example “YTWHSHKSD” which was the enigma encrypted message. The sender of the message then transmitted the encrypted message with a standard Morse code transmitter, upon receiving the message the receiver wrote the encrypted message down, set his Enigma message to the same pre-decided combination and then type the message on to the machine's keyboard, which the machine then would decipher and display message using the same upper board bulb panel.

What made this cipher machine special was the typewriter style design which was easy to use and a major advance in cryptologic strength. The innovation of the electromechanical rotors gave the machine more cryptographic strength, as the rotors turned in odometer style and gave new cypher algorithm for each letter in the message. The electric pathway of the signal goes from Keyboard -> Plugboard -> Rotors -> Reflectors -> Rotors -> Plugboard and finally the letter was lit up on the blub panel (A keyboard in QWERTZ format with a backlight under each letter to get the ciphertext). Despite the advances of the machine, there was no printing capability hence the message must be written down by hand.

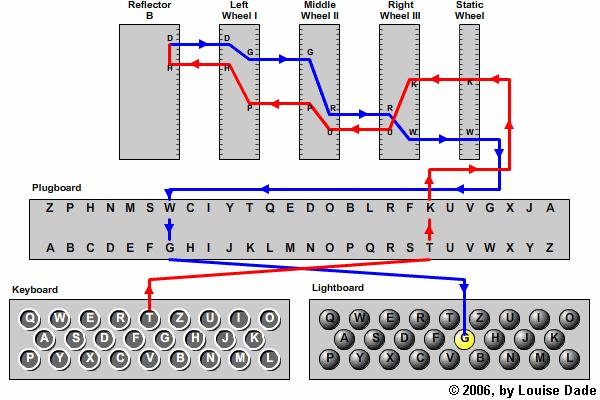
The vital parts of the Enigma machine are rotors and reflectors, the interwiring of the rotors and the rotors reflector controlled the enciphering of the Enigma machine. The technology used in the making of this machine is advanced and a legend in the world of cryptography let's discuss more about the important pieces of the Enigma and the technologies used.

Rotor wheels play a significant role in the machine, around 3-4 rotors are used in each machine. For example, if 3 rotors are used it would work in this way: 1st rotor rotates each time a character is an input, the 2nd rotor rotates once each time the 1st rotor makes one full turn, the 3rd rotor rotates once each time the 2nd rotor makes one full turn. The internal wiring of each rotor could be constructed in 26! Different combinations hence 26! \* 3 for 3 rotors which gives exceptionally big number of combinations. Each of the 3 rotors could initially also be set to any letter: 26\*26\*26 = 17,576.

Plugboard in front of the machine were added later to increase cryptographic strength, the way this worked was simple, the machine had several cables with a plug at each end that could be used to plug pairs of letters together. For example, If X were plugged to Z, then on typing the letter X the electric current would follows the path that was assigned with Z and vice versa. This function increased the complexity and added 1000,000,000,000 different possibilities.

Light bulb panel is one of the most important part of the Enigma as it displays the cipher text and the decrypted text as well. This board uses the QWERTZ format without any spaces or symbols, it’s output method for the machine. Working of this light panel is simple, small light bulbs light up each letter which must be written down, and the whole thing is powered with a 4.5v battery.

[[2]](#footnote-2)



Below more the issues, flaws and shortcomings involved with the Enigma Machine will be illustrated analytically. Enigma code which was considered unbreakable by many cryptographers, mathematicians and scientists around the word was indeed on of the most cryptic way of communication in WW2 for the Nazis. What made Enigma code so special? The quality of the code is measured in terms of the number of possibilities one must go through to get the right answer. Enigma was seemingly unbreakable because on must go through 15 million million million possibilities to get the correct answer.

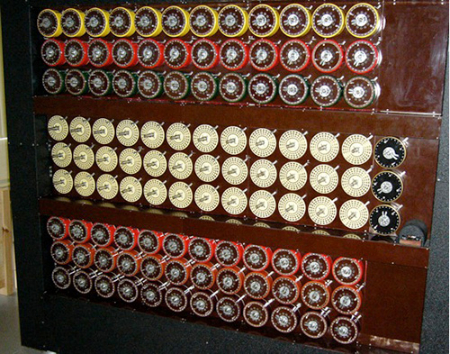
The important flaw and most weak link in the Enigma machine led to the success of Alan Turing, he discovered this flaw that could help to decipher every single encrypted Enigma text. The flaw is explained below in technical depth:

For example, if we want to encrypt a message that contained a total of three words “Queen Mary University”. The first word of the message is Queen, now the first letter that we want to encrypt is Q, when we press the Q on the keyboard of Enigma machine, a process is started where an electric signal is generated and it sent through the wires, rotors, plugboards and ends on the light panel as K. The idea is to encrypt letters differently than they actually were, in this case QUEEN MARY UNIVERSITY could be example ESOJB JAJM IDUWHFCHAJ.

Turing noticed that every letter was encrypted as a letter that was different than itself, not even once it occurred that a letter was encrypted as itself. So, when the Q was typed it could be encrypted as any 1 letter of A to Z, any of the 26 letters but not Q, Q would never be encrypted as Q, this was the signal flaw in the Enigma machine. When this fact was discovered that a letter can be encrypted as any letter by itself, suddenly the total number of possible settings decreased. Now to help this theory Turing needed a word that Germans would use more often in the enigma code and the word that Turing was positive about was ‘Heil Hitler’. Who could have guessed that the most popular and proud upon phrase would give up most important clue in the code breaking.

The rest of the shortcomings came from the poor operating practices and human behaviour. Marian Rejewski who discovered flaws in the Enigma machine and observed the pattern in cipher code is considered to be the true genius behind the defeat of the Enigma machine, he observed German’s major procedural weaknesses of specifying a single indicator setting for all of the messages on a network for a day, also that the operator’s chosen message key in the encrypted 6 letter indicator. This mistake helped Rejewski to decipher the message without knowing any of the machine’s wiring. Even without knowing the rotor wiring or plugboard settings Rejewski reduced the number of possible substitution cipher to a significantly small number. Many factors helped in this for example laziness of the cipher clerk (Human behavioural error), scores of messages were enciphered by a team of clerks but some those messages would have the same encrypted indicator, this meant some clerks happened to coincidently choose the same three letter starting position. These cases were rare and random but lazy clerks often choose starting positions such as AAA, BBB, CCC, DDD, this was a security mistake and helped code breaker to solve each of the 6 permutations used to encipher the indicator.

Now that the flaws were known, the cryptographers have to develop a machine which will seek the proper combination of the rotors between all possible combinations, Polish scientists invented techniques and machines called ‘Bomba’ to automate the search for the initial settings. Turing and Gordon Welchman a fellow Cambridge mathematician set to improve the Polish machine. Many improvements in design and speed, reduced time to decrypt the code to just a few hours instead of days making the recovered message more valuable, this machine developed under the supervision of Alan Turing was called ‘Bombe’. At the Bletchley Park where a team of scientists, mathematicians and cryptographers were attempting to break the Enigma code, Alan Turing was the head of the crypto team where he devised a number of statistical tests to reduce the number of initial settings checked by bombes, this made the decryption of the code easier and faster.

[[3]](#endnote-1)

To conclude on this one of a kind machine, which have a significant impact in the past and will serve as an example for future, the technical advances of the machine were commendable and unbreakable theoretically due to N number of possible combinations, the number of combinations in which Enigma machine could be set is more than the number of atoms in the universe 3.28 \* 10114. For example, a key length of 1023 means 100,000 operators, each checking one key setting every second would take twice the age of the universe to break the code (research supported by <http://www.bletchleypark.org.uk/>)

The factors that helped the code breakers are listed to conclude in brief below:

* No letter could be enciphered to itself, it meant that some possible solutions could quickly be eliminated because of the same letter appearing in the same place in both the ciphertext and in piece of plaintext.
* Laziness of the operators who would use same settings more often.
* Poor practices on part of some operators who only changed shift key settings by a bit rather than making a complete new setting.
* Poor procedural practices to use well know good and bad words.
* Human error by using the names of the wife, girlfriend or town name.
* And last but not the least, the acceptance of Germans that the machine was unbreakable.

# References

*Enigma*. (2014). Retrieved from Nationalarchives: http://www.nationalarchives.gov.uk/spies/ciphers/enigma/default.htm

Ludlow, D. (2011, January 20). *How Bletchley Park broke the German Enigma code.* Retrieved from Expertreviews: http://www.expertreviews.co.uk/technology/7857/how-bletchley-park-broke-the-german-enigma-code

Miller, D. A. (2012). *The Cryptographic Mathematics of Enigma.* CreateSpace Independent Publishing Platform.

Numberphile. (2013, Janurary 10). *158,962,555,217,826,360,000 Enigma Machine.* Retrieved from Youtube: https://www.youtube.com/watch?time\_continue=711&v=G2\_Q9FoD-oQ

Numberphile. (2013, January 14). *Flaw in the Enigma Code - Numberphile.* Retrieved from Youtube: https://www.youtube.com/watch?time\_continue=1&v=V4V2bpZlqx8

Raj, A. (2016, September 19). *enigma cipher machine.* Retrieved from Slideshare: https://www.slideshare.net/Tapeshtapeshvatsa/enigma-cipher-machine?qid=42b916e9-3914-44e0-b507-a2fd340e529a&v=&b=&from\_search=1

Stubblj. (2014, October 22). *Fatal Flaws.* Retrieved from derekbruff.org: https://derekbruff.org/blogs/fywscrypto/2014/10/22/fatal-flaws/

Thimbleby, H. (2015, 19 October). *Human factors and missed solutions to Enigma design weaknesses.* Retrieved from Tandfonline: https://www.tandfonline.com/doi/full/10.1080/01611194.2015.1028680

1. https://en.wikipedia.org/wiki/File:EnigmaMachineLabeled.jpg [↑](#footnote-ref-1)
2. http://enigma.louisedade.co.uk/howitworks.html [↑](#footnote-ref-2)
3. https://bletchleypark.org.uk/whats-on/hut-11a-the-bombe-breakthrough [↑](#endnote-ref-1)