The Enigma

Hadi Bohsali

August 2024

The Enigma

Part 1: The Machine

Throughout human history there has been perhaps no machine more influential or cynically important than the Enigma Machine. Originally developed for commercial use, it was invented in 1918 by Arthur Scherbius, a German engineer. However, by the beginning of the 1930s, the machine was adopted as the Nazi Germany military's main encryption mechanism and was used throughout the second World War. There were several variants produced for different services such as the government, navy, and military, with slight differences. For example, the Enigma used by the military had a plugboard (an extra padding of encryption-more on that later). Although the machine's code was cracked in 1941, the Enigma remained in use until the end of the war in 1945, with the Germans desperately trying to innovate and add further encryption to the machine, although to not much avail. After the war, the Enigma was discontinued in favor of more secure and mechanized encryption mechanisms, and the captured machines were sold to developing countries.

The machine itself looks quite simple on the outside, about the size of a typewriter, with a keyboard containing the 26 letters of the alphabet, and a lampboard mirroring it.

Let us imagine we are in a battle in the Second World War. We have two German officers: Sam (the sender) and Ron (the receiver). Sam wants to inform Ronald about the time of a planned ambush. Sam types the message on the keyboard and the ciphertext appears on the lampboard. The ciphertext is then broadcasted through the radio in morse code. Ron would then write down the ciphertext, and assuming the settings on Ron's Enigma machine were the same as the ones on Sam's, when Ron types the ciphertext on his Enigma machine, Sam's message containing the time of the ambush should appear on the lampboard.

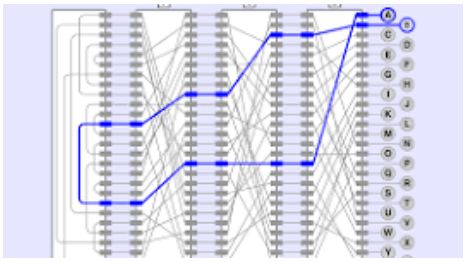
The Enigma machine is fundamentally a complicated circuit, containing a battery, wires, and light switches. When a letter is pressed on the keyboard, it connects a circuit, turning on the lightbulb under the lampboard, illuminating the letter directly under it. Simple, right? However, although this may seem like a basic substitution cipher, rather than one letter corresponding to another, a letter can be encoded as any letter in the alphabet other than itself, multiple times as well. This is possible due to the three rotors in the machine: each rotor

has the numbers 1-26 in order, corresponding to the position of the letter in the alphabet (1=A, 2=B, C=3...26=Z).

When a letter on the keyboard is pressed, electricity flows through the circuit, travelling through wires, eventually reaching the rotors. Every time electricity passes through the rotor, the letter is changed once, corresponding to the position of the rotor. For example, if the letter A on the keyboard is pressed, and the rotor position is on the number 5, the A will be changed to an E. The electricity then flows to the next rotor via metal contacts between each rotor, and the letter is changed again. When this happens for a third time, the current flows into a reflector, which connects letters in pairs. The current then flows back through the three rotors, changing the letter three more times, and illuminates the letter under the lampboard. This means that the original input letter is changed minimum seven times before it is returned. However, the military had another layer of encryption: the plugboard, which paired 2 letters together on the keyboard. There could be up to 20 paired letters on the plugboard, adding extra security into the cipher. This leaves us with a monoalphabetic substitution cipher, or simply, a substitution cipher where the letters are changed multiple times.

Part 2: The Inner System

Let's bring back our friends Sam and Ron. For simplicity, let's assume that neither Sam nor Ron have matched any pairs on the plugboard. Sam wants to encrypt the word ALLAN, the codename of an undercover enemy agent, and send it to Ron. He types the letter A on the keyboard. Let's assume the first rotor is on the number 16, so A is changed to P in the first rotor. The second rotor is on the number 20 (could be paired with any number), and the letter remains the same. The last rotor is on the number 2, so the letter is once again changed from P to T. On the reflector, T is matched with L. L is then matched with I on the third rotor, and I is changed to C in the third rotor, then C is



changed back to B in the first rotor, so the electrical current flows into the lightbulb under the letter B in the lampboard and illuminates it

When Ron receives the message, assuming his rotors are in the same starting position as Sam's, if he types in the letter B, the same process should occur, but in reverse order, with B turning into C, C into I, and so on, until P is changed into A in the first rotor and illuminates A under Ron's lampboard. It is important to note that every time a letter passes through the circuit, the first rotor's position moves up by one number. For example, in this case after the letter A is converted into B on Sam's lampboard, the rotor will automatically switch from the number 16 to 17, meaning that the pressing A again will most likely yield an entirely different letter, hence the second A in ALLAN would likely be coded as a different letter, differentiating the Enigma from a simple substitution cipher.

Part 3: The Combination

Let's take a look at the possible combinations of codes on the Enigma. Most Enigma machines used by the German military had a box of five different rotors, of which three could be picked. In the first slot, you have a choice of five rotors. In the second, you have a choice of four, and in the third, you have a choice of three:

$5 \cdot 4 \cdot 3 = 60$.

Each rotor has twenty-six possible starting positions, and we have three rotors:

$26 \cdot 26 \cdot 26 = 17576$

The plugboard allows up to twenty letters to be connected in pairs. There are twenty-six letters in the alphabet, which can be arranged in 26! Ways. However, there are still six letters that are not paired and therefore, are not part of the calculation, therefore we can divide by 6!. As well as that, the order of the pairs on the plugboard is irrelevant, so we can also divide by 10!. Finally, the order of letters in pairs also do not affect the permutation, so we can divide by 2*10:

26! / (6! · 2*10), which gives us: 150 738 274 937 250

Multiplying everything together gives us:

$60 \cdot 17576 \cdot 150\,738\,274\,927\,250 = 158\,962\,555\,217\,826\,360\,000$

158 962 555 217 826 360 000 possible combinations is perhaps why the Germans thought the code to be unbreakable. Let us look at the relation between symmetric groups and the Enigma's encryption to understand this better:

A symmetric group Sn is the group of all permutations of n elements. For example, the symmetric group S4 consist of all possible arrangements of four objects. The order (number of elements in a group) of a symmetric group Sn is n! Therefore in the group S4, the order would be 4!, or 24, which is also the amount of permutations in the group.

We can apply this information to understand how the Enigma works as a permutation device. Let's start with the rotors: every rotor is a permutation of the alphabet, scrambling letters according to its internal wiring, which creates a specific permutation.

The combination of different rotors also serves as a permutation group: the product of the transformation of a letter when passed through multiple rotors is a sum of the individual permutations performed by each rotor. If each rotor performs a permutation of the twenty-six letters, the number of different permutations possible with three rotors is a product of the possible configurations and the twenty-six possible positions for each rotor.

In addition, the plugboard implements a permutation by swapping pairs of letters, which adds another element to the symmetric group. The number of ways to swap 10 pairs of letters from 26 possible can be described by the binomial coefficient (26 2) for each pair, significantly increasing the total number of possible permutations.

Therefore, the operations of the Enigma Machine can be summarized as performing a series of permutations on the letters of the alphabet, where each individual component performs a separate permutation, and the combination of all the permutations is equivalent to one large permutation, explaining the complexity of the Enigma, and how hard is was to crack.

Part 4: The cracks in the invincibility

Although the Enigma was an incredibly secure encrypting system, there were a few noticeable weaknesses in the code which were capitalized on by the allies, and eventually led to the cracking of the Enigma code. It is crucial that we understand these weaknesses before we delve into how the code was broken.

A major weakness of the Enigma code is that it is impossible for a letter to be encrypted as itself. This is due to the reflector, which pairs 2 letters together at the end of the third rotor. This means that the allies knew a letter could never be encrypted as itself, reducing the number of possible combinations. For example, if the ciphertext read VNBT and NBT had been deciphered as 'ast', the cryptographers could be sure that the word was not 'vast'.

Another fault with the reflector is that it always performed the same permutation. For example, regardless of the order of the rotors, if the letter C was paired with the letter Y, C would always encrypt as Y, and Y would always encrypt with C. This was a major disadvantage as it allowed the allies to identify patterns and relationships between different permutations.

There were also common human errors that plagued the security of the code. An example of this is that the three-letter sequence for the rotors would be sent twice at the start of each message. For example, if the sequence for the rotors was (2,1,4) the letters BAD (corresponding to the numbers and their sequence in the alphabet) would be sent twice, so BADBAD. As any cryptographer knows,

frequencies and repetitions are a major threat to the security of the code, and the allies analyzed the intercepted messages to determine the purpose of the key. This was a major asset as it eliminated the possible permutations performed by the position of the rotors.

The allies also focused on repetitive phrases known as 'cribs'. Messages containing names, weather, and time were commonly prefixed with the same phrase. Again, this helped the allies understand the internal workings on the enigma better and deduce the overall message.

There were numerous other weaknesses in the Enigma, such as the German's overdependence on a sole method of encryption as they were confident nobody would be able to break the code. However, the code was still incredibly hard to break; even after the allies had captured several machines and intercepted the key for the positioning of the rotors, the additional defense layers such as the plugboard served as a thick skin behind the armor. It would take a herculean effort for the Enigma code to crack.

Part 5: The Bombe

The effort to crack the Enigma code was first made almost a decade before it was solved. In the early 1930s, the Polish became suspicious of Nazi Germany's aggressive actions and orchestrated an effort to crack the code to anticipate a possible attack. A team led by mathematician Marian Rejewski made a big lead on how the rotors and internal wiring worked by analyzing how the Germans sent the key for the positioning of the rotors twice in every message. Rejewski was able to deduce the internal wiring through the theory of permutations, which was an incredible accomplishment.

In 1938, a year before the Germans invaded Poland, Rejewski and his team designed a device to try break the code. Nicknamed 'Bomba', the machine ran through different rotor positions and tried to deduce the configurations of the letters. Although numerous Bombas were required to deduce the rotor positions, it narrowed it down greatly and laid the foundations for future adaptations to the machine that would make it more effective.

A year later, after escalating tensions and war in Europe looking inevitable, the Polish held a meeting with British cryptanalysts. All progress that Rejewski and his team had made was shared with the British, as well as a prototype of the Bomba and models of the Enigma. This meeting proved vital in cracking the code as it gave the mathematicians at Bletchley Park a large base to build on. However, the Germans had recently modified and improved the Enigma, adding two new possible rotors and increasing the plugs on the plugboard from six pairs to ten. It would still be no pushover for the British to decipher the code.

Alan Turing was a young and extremely intelligent Cambridge graduate. He is perhaps the most well-known codebreaker of all time due to his massive contribution in breaking the Enigma code. He was put in charge of the team of codebreakers at Bletchley Park and inheriting a great amount of information and technology from the polish, was tasked to figure out how to crack the impenetrable fortress of the Enigma. Turing's first initiative was to improve on the polish Bomba and adapt it to the newly bolstered Enigma machine. The newly

constructed and anglicized 'Bombe' consisted of thirty-six Enigma machines wired together, which had the ability to simulate several Enigma machines running at once, which helped to determine the order of the plugboard and rotors. Turing would then make educated guesses on the pairs on the plugboard and easily deduced the pairing on the reflector. This was major progress for the allies.

Turing also had a precise method to isolate separate parts of the code. He focused on the cribs (see part 4) of the messages and frequently ran them through the Bombe to see if a logical plaintext was produced. He was also aided by the discovery that the Enigma would never encrypt a letter as itself, which helped him deduce specific phrases that could logically contain many letters but could never be the same as the ciphertext. When the ciphertext was completely decrypted by the Bombe, the machine would stop. The codebreakers would then record the settings and run the full message through, successfully decrypting it.

By 1941, Turing and his team at Bletchley Park had become incredibly adept at intercepting and deciphering the Enigma code. The further development of the Enigma meant that messages could be deciphered in as little as twenty minutes, providing the British with a monumental advantage that changed the tide of the war. Vital information such as the position of German troops, planned ambushes, and German U-Boat communications were ceded to the British, which led to further information on the Enigma. Allied troops were able to raid German outposts and, on many occasions, recovered Enigma machines and codebooks. The Germans tried to further complicate and obscure the Enigma, but to no great avail. Finally, after Germany's surrender and the end of the Second World War, the death of Enigma was imminent; weakened considerably by British intelligence and blown up by the Bombe, the Enigma was put out of use.