Leqi Wang

Professor Hubert Bray

Mathematics of Universe 190s

July 17th 2017

Abstract

Enigma was a ciphering machine widely used by Nazi Germans back in WWII (the second world war). It was a formidable enemy of Allies of World War II. This paper will first focus on the Wehrmacht Enigma (M3, with three rotors working and one plugboard) and then delve deeper into the mechanical structure — how it actually works, and why the codebreakers devoted so much effort to breaking this machine.

I.The birth of Enigma:

figure 1: the Enigma machine.

Enigma was born at the end of the WWI(World War I). It was invented by a German engineer Arthur Scherbius and was most wildly used by Nazi Germans in WWII(World War II) as a protective mechanism of military communication. There were many different versions of Enigma. Still, military Enigma with a plugboard was the most complex version.

II.Why we are studying Enigma.

Though Enigma wasn't the first electronic-mechanical rotor cipher machine in the history and belonged to the defeated nation Nazi German, and it was not as secure as modern encrypting machines, what really surprises us is that it was the first cipher machine broadly put into practice. After the silence in cryptography over a hundred years, the emergence of Enigma prompted the development in encryption machine. It was equipped across German armed forces and was engaged in an actual war; it was the machine that was thoroughly made public and fully explained after the war. It was much accounted of heads of the state. Hitler himself spoke highly of the security of Enigma, he claimed Enigma to be "unbreakable" after he was told about the internal settings; Winston Churchill put breaking Enigma as an "absolute priority"; Dwight Eisenhower gave thank to Polish mathematicians who made contributions on breaking Enigma in person … …

Here is a popular misunderstanding of Enigma's fame or notoriety. Though Enigma itself has nothing to do with the crime Nazi German committed, Enigma is often related to the rise and fall of the whole empire — the unbreakable character of Enigma first made it widely used in every military and government services. Thanks to its brilliant work, the cryptanalysis of the Enigma enabled the western Allies in World War II to read

substantial amounts of secret Morse-coded radio communications of the Axis Powers that had been enciphered using Enigma machines.

III. The Unbreakable machine.

A M3 Enigma machine has a keyboard, a lamp board, one entry wheel, five rotors (a scrambler) , one reflector, and a plugboard.

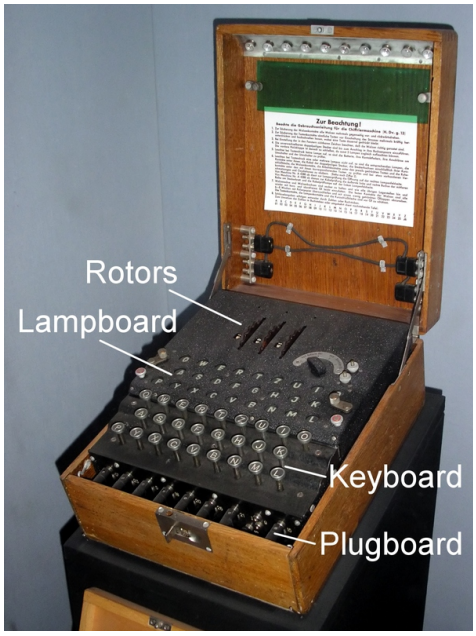

figure2: basic component of Enigma machine

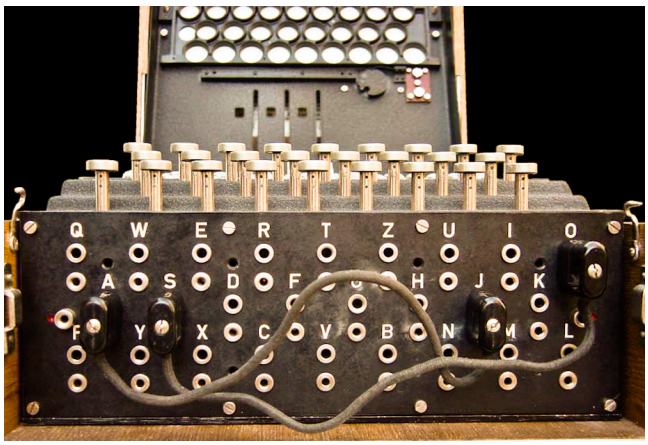

figure3: plugboard of Enigma.

1.input&output

The operator of Enigma will presses the key on the keyboard to implement input. The corresponding encrypted letter will be shown on the lamp board.

figure4: keyboard

figure 5: lamp board

2.Encryption.

-Rotors

In every M3 machine, there are 5 rotors in total but only 3 of which put into usage. Every time the operator types a letter into Enigma, the letter will first enter the rotors on the right. And every time the operator taps, the 3rd rotor rotates 1/26 to the next letter and changes the settings of Enigma:

$$rotor3 <-- rotor2 <-- rotor1$$

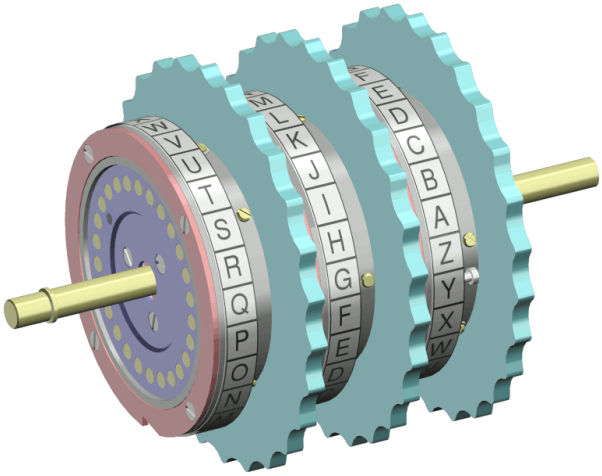

figure6: a scrambler comprising of 3 rotors

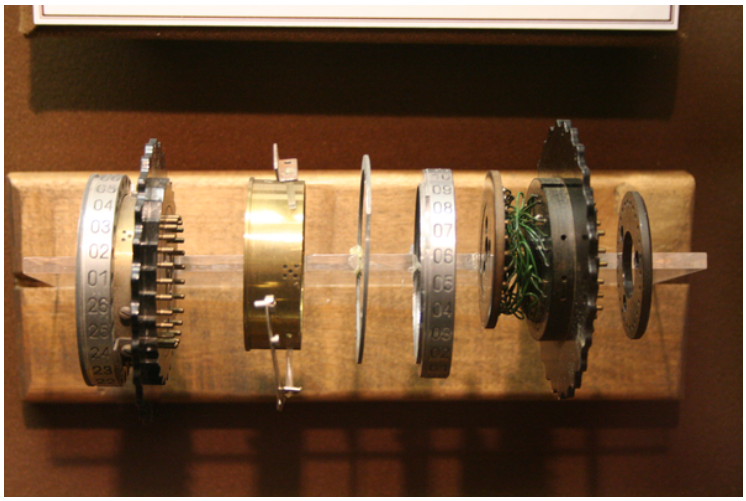

figure7: inside the rotor

On the opposite side of every rotor, correspondingly, it has 26 electrical contact on the left side, 26 pin contact on the right side.

figure8: electrical contact(left)

figure9: pin contact (right)

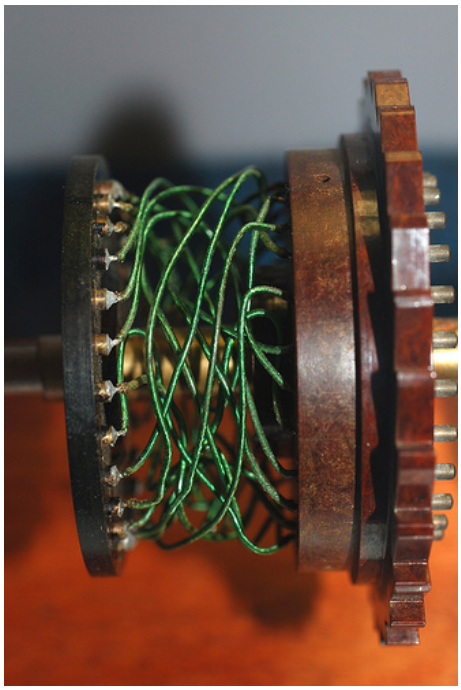

figure10: one-on-one connection between electrical and pin contact.

The pin and electrical contacts are one-on-one linked by electrical circuit to make things go faster and more complex(shown in figure 10). For example, if we input letter A to the scrambler, the current will first get to the pin that represents A. Let's assume that this pin is connected with the electrical area that represents P. When the letter comes out from the first rotor, A has already become P. So all the letter has to do is to repeat this process for 3 times.

And how this will work out is indicated in the window:

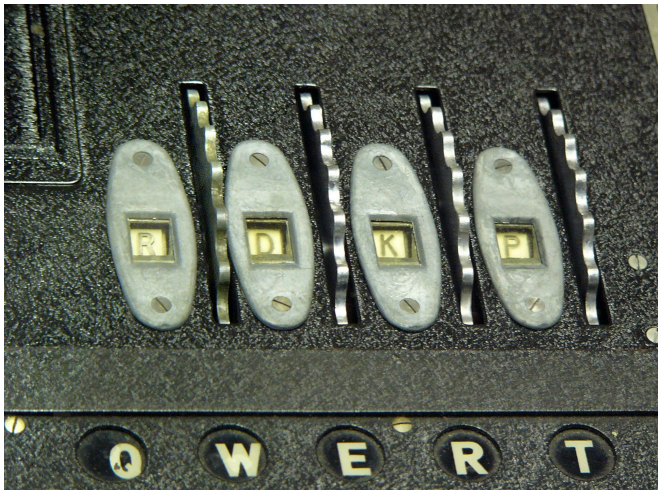

figure11: rotor windows of M4 machine of navy

Still, the settings eventually depend on the internal electrical circuit of Enigma.

-reflector

figure12: reflector

The reflector is sitting behind the last rotor. It has 26 pin contact areas connected with their electrical counterpart on the third rotor. And inside every reflector, the pins are connected by pairs. If one letter enters the reflector, it'll come out from the other side as another letter. And the letter it becomes will go back into the rotors and come out from the first rotor, enter the plugboard, and eventually shown on the lamp board.

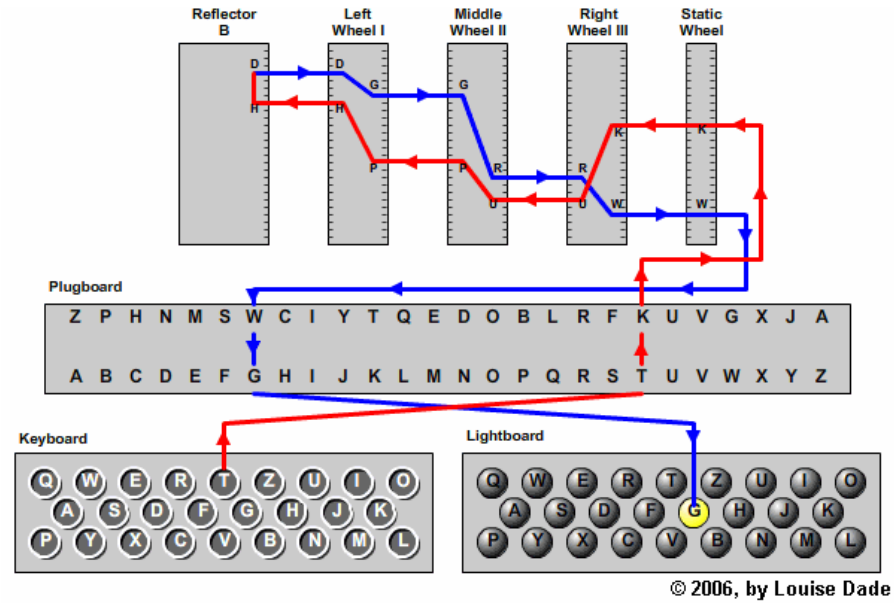

figure13:How Enigma works in general

Generally speaking, the reflector is a mirror, but it does not reflect the same things as input. For example, If I input the first letter into Enigma.

A—>first rotor—>B
B—>second rotor—>C
C—>third rotor —>D

and here is the problem, when D enters the reflector, it'll become something else.

D—>reflector—>E

Therefore, we can safely say that whatever goes into Enigma machine, when it comes out, it cannot be itself. This feature becomes the most important flaw of Enigma. And the codebreakers of the Allies finally beat Enigma by this flaw. And I will go back into this problem in my next paper.

-plugboard(figure3)

The essence of plugboard is working on the principle of Mono-alphabetic substitution, which means the plaintext and ciphertext have the same amount of letters and these letters are also corresponding. This relationship is shown in figure13. If letter A is encrypted into E, then the plaintext of E must be A.

So, how many combinations can be brought by plugboard?

First, two letters are connected by one wire, which means every wire concatenates// connects 2 letters. Once one wire is plugged in, the available letters left will reduce by 2. The total number left is

$$2n - 2$$

And the total possibility of plugboard is actually the product of these processes.

We choose 2n letters from 26 as the number of letters we want to change, we have:

$$\frac{26!}{(26-2n)! \cdot (2n)!}$$

kinds of situations.

Second,

$$(2n-1)*(2n-3)*\ldots\ \ldots*1$$

is the number of pairs these 2n letters can become.

Therefore, the total number of variation is the product of these two formula, which turns out to be:

$$\frac{26!}{(26-2n)! \cdot 2^n \cdot n!}$$

So this is the possibility of plugging on **n** wires on the plugboard:

n = 0, Possibility = 1
n = 1, P = 325
n = 2, P = 44,850
n = 3, P = 3,453,450
n = 4, P = 164,038,875
n = 5, P = 5,019,589,575
n = 6, P = 100,391,791,500
n = 7, P = 1,305,093,289,500
n = 8, P = 10,767.019,638,375
n = 9, P = 58,835.098,191,875
n = 10, P = 150,738,274,937,250

n = 11, P = 205,552,193,096,250 （MAX)
n = 12, P = 102,776,096,548,125
n = 13,P = 7,905,853,580,625

The possibility will come to maximum when there are 11 wires plugged in, meaning 22 letters paired up. But in the real M3 settings, German made only 20 jacks and that's 150,738,274,937,250 settings at most.

-The number of combinations in Enigma

Since Every rotor has 26 independent circuit connection from each pin to each electrical contact. And each connection corresponds with one conversion of a letter, which means, one rotor will have 26 starting points, 26 different possibilities.（ Since the second rotor is influenced by the marching problem, its period only contains 25 possibilities, but we'll dismiss this difference.）Every time the typer input one letter, the rotor on the right side will rotate to next letter(1/26). So there are

$$26*26*26 = 17576$$

total possible starting point configurations.

And since there are 5 rotors in total and only three at word, we have to randomly pick up 3 rotors from 5 possible rotors. So there are

$$\frac{5!}{(5-3)!} = 60$$

possible combinations(The possibilities in Enigma is actually less than 17567 but only 16900, since the second rotor only has 25 starting points other than 26, so the formula should be 26*25*26).

As a result, there are

$$17576*60 = 1054560$$

possible settings in a M3 scrambler.

In 1930, the German army introduced the plugboard that further secure the machine from brute-force attack to Enigma machine. And inside the plugboard, there are 10 pairs of alphabets being connected. Two letters in one pair can be swapped over. This level of scrambling only appears in military Enigma machine and adds the most combinations in to Enigma settings. So there are 26 letters in alphabets, and we have

$$26!$$

different ways to arrange these letters. However, we don't have to get every combination of these 26 letters because in Enigma there are only 10 pairs of letters, 20 letters in total, being swapped over. Therefore we have to divide 26! by 6! so that we can dismiss the combination of those 6 letters we don't care about. And the formula becomes

$$26!/6!$$

possibilities. After that, since we don't know about the arrangement of these 10 pairs of letters, we don't care about them. Therefore, we can divided by 10!:

$$26!/6!/10!$$

There is the last factor we have to divide by: since there are two letters in a pair, the order of these letters does not matter because they will be swapped over anyhow(B and A is the

same as A and B). So each pair can divided by 2, and there are 10 pairs , so we divide by 2^10:[1]

$$\frac{26!}{(26-20)!\cdot 2^{10}\cdot 10!} = 150{,}738{,}274{,}937{,}250$$

So there are 150738274937250 possible ways of setting up in a plugboard.

And in total, there are

$$\frac{5!}{(5-3)!}\cdot 26^3\cdot\frac{26!}{(26-20)!\cdot 2^{10}\cdot 10!} = 158{,}962{,}555{,}217{,}826{,}360{,}000$$

kinds of Enigma M3 combinations, approximately 159 with 18 zeros behind.

If we had ten people checking one setting a minute for 24 hours a day and 7 days a week, it'll take

$$20 Million Years$$

to work out all settings in Enigma.

-Turning Point

Though Enigma machine seemed unbreakable, the brilliant mind in the Allied country solved this hard puzzle by combining their effort: the Polish mathematicians used permutation matrix and a machine called "Bomba" worked out the settings of 3-rotor Enigma machine. And after the German-Soviet invasion to Poland, British

mathematicians, Dilly Knox, Alan Turing and Gordon Welchman, gradually made effort to completely decipher all versions of Enigma machines.

Throughout the second world war, though there were only three kinds of ciphering machines: Enigma, Lorenz SZ40/SZ42 and SIEMENS AG T43/T52. And Enigma was the most widely used across the both on map and the timeline — nineteen years. But this immoderate use eventually made Nazi Germans lose the entire war, and this was, and still is, the greatest flaw in the Unitary Security System. "The first weakness, the machine design itself, was a minor one. When Enigma enciphered a letter, it was guaranteed that the resulting enciphered letter would not be the same letter. For example, 'A' could be translated into any letter other than 'A', 'B' would never be enciphered as 'B', etc. By itself would not have allowed the Allies to read Enigma ciphertext but it did assist cryptographers in finding the human errors. The more important weakness was the human one. The mistakes made by the Enigma operators and the poor procedures put into place by the German military were legion; without them the Poles and the British would have had no hope of cracking them. Gordon Welchman, one of the officers in the British program, said 'the machine as it was would have been impregnable if it had been used properly' but pointed out twelve serious errors in procedure that, if corrected, would 'have stopped us cold.'"

Conclusion

In the world of cryptography, Enigma is absolutely a huge breakthrough. Its contribution should be counted as two mileposts: one for inventing this machine, which is a huge intelligence challenge put on Allies of WWII and on the whole human race.

"Breaking Enigma, the historian estimated, shortened the war by more than two years, saving over 14 million lives."

Another mileposts is for the difference Enigma made in science by studying and solving it, which generated an entire new scientific field — computer science.

Reference

Yanfeng Zhao. (2008).Legends of Enigma. Beijing, China: Science publishing house.

Andrew Hodge. Counting the Possible Plugboard Settings.https://www.codesandciphers.org.uk/enigma/steckercount.htm(Accessed July17th, 2017)

Cryptanalysis of the Enigma.(2017, July 13). In Wikipedia, the free encyclopedia. Retrieved July 17th, 2017, from https://en.wikipedia.org/wiki/Cryptanalysis_of_the_Enigma

Enigma machine.(July 2nd, 2017).In Wikipedia, the free encyclopedia. Retrieved July 17th, 2017, from https://zh.wikipedia.org/wiki/%E6%81%A9%E5%B0%BC%E6%A0%BC%E7%8E%9B%E5%AF%86%E7%A0%81%E6%9C%BA#.E5.8F.8D.E5.B0.84.E5.99.A8

Enigma Machine. (July 13th, 2017).In Wikipedia, the free encyclopedia. Retrieved July 17th, 2017, from https://en.wikipedia.org/wiki/Enigma_machine#Basic_operation

How did Alan Turing break Enigma in the film the Imitation Game? https://www.zhihu.com/question/28397034 (Accessed July 17th, 2017)

How to break enigma？ https://movie.douban.com/subject/10463953/questions/34393/ (Accessed July 16th, 2017)

Cracking the Enigma code: How Turing's Bombe turned the tide of WWII http://home.bt.com/tech-gadgets/cracking-the-enigma-code-how-turings-bombe-turned-the-tide-of-wwii-11363990654704 (Accessed July 16th, 2017)

Numberphile.(2013, Jan 10). 158,962,555,217,826,360,000 (Enigma Machine) - Numberphile [video file]Retrieved from https://youtu.be/G2_Q9FoD-oQ

Chris Christensen.Machine Ciphers. http://www.nku.edu/~christensen/section%2017%20machine%20ciphers.pdf(Accessed July 17th, 2017)

How many possible Enigma machine settings? https://crypto.stackexchange.com/questions/33628/how-many-possible-enigma-machine-settings (Accessed July 16th, 2017)