Enigma Summary (from Code Book by Simon Singh)

The Enigma machine was invented by Arthur Scherbius in 1918, utilizing the idea of the cipher disk, coupled with modern electrical technology. The rough idea is as follows:

The machine has three disks, called rotors, that are divided into 26 parts. So, think about a clock dial with 26 notches, instead of 12. You can label the notches 'A' to 'Z'. When you press a plaintext key to be encrypted, there is a wire that connects it to one of the notches in the first disk. The first and second disk are wired which connections that represent a random permutation. So for example, slot 3 on disk one might have a wire that connects it to slot 17 on disk two. Similar connections are between disk 2 and disk 3. Thus, we can envision a signal being sent through the three disks (all together, these are called the "scrambler") and outputting a letter. By itself, this is nothing more than a substitution cipher. But, the disks weren't fixed in space.

What's interesting is that the disks can rotate, and the corresponding connections rotate with them. Thus, if we rotate disk 3 by one notch, and then send the same plaintext letter through the circuit, the wire that it follows in its last step will be a different one, resulting in a potentially different ciphertext letter. In fact, any of the three disks could be in any of 26 positions. Changing any disk position changed the overall "substitution" performed. Thus, with just three disks, there were a total of 26^3 possible substitution "tables" so to speak, that could be implemented.

Now, there were more parts to the machine than just the three disks in the scrambler, but for now, let's just consider how these were used before describing the other complexities of the machine.

Each time a letter was encrypted, the third scrambler disk would move one position. After the third scrambler disk returned to its original position in 26 steps, the second disk would rotate one step, so after each letter was encrypted, a new "substitution" table would be used. In total, there were 26^3 substitution alphabets ready to use.

In the Vigenere cipher, we use k separate shift ciphers and then repeat them. Thus, effectively speaking, an Enigma message less than $26^3 = 17{,}536$ letters would never encrypt a letter the same exact way. Thus, a huge "cycle length" is achieve through combining fairly simple tools.

We can think of the disk settings on the scrambler as going from AAA to ZZZ, as all possible three letter strings in alphabetical order.

A depiction of the machine is given in the handouts posted online from the Code Book. (It's too hard for me to draw them here.)

But, the three scrambler disks isn't all the Enigma had. Once the signal gets through the 3 scramblers, it hits a reflector that sends the signal back through the scrambler (in reverse order). (This is so that a letter could never encrypt to itself.)

Finally, once the signal bounced all the way back through all of the disks, it hits the plugboard. The plugboard allowed for up to 10 pairs of letters to be swapped, right before the final output of

the cipher text letter. As you can see, this machine was **a huge step up** from the ADFGVX cipher used in WWI.

How the Engima was Used by the Germans

If all messages were encrypted with the same starting setting of the rotors, then if 1000 messages were encrypted, the first letter of those messages would all be encrypted using the same substitution cipher and some frequency information could be gleaned. Thus, the Germans wanted to make sure the initial setting of the rotors (AQW, etc.) would be different from message to message. Here is how they did it:

1. A book of day codes was published. So for example, for 3/25/1932 perhaps the daycode was "LWS".

2. If you were an Engima operator sending a message, you look up that day's day code and set the disks to that particular setting.

3. Pick a random message code, any three letters. For example, "JYW".

4. Set the machine to the day code and encrypt the message code, written twice. So, in our example set the machine to "LWS" and then send the plaintext "JYWJYW". It was sent twice to detect errors in transmission.

5. Set the disks to the message code, in this case "JYW", and then from THAT setting, encrypt the plaintext message you want to send.

Enigma Blueprints

The German military started using the machine sometime in the 1920s. At that point, the French were interested in what the Germans were saying, but had no idea how their messages were being encrypted. To try to find out, they decided to use a little old fashioned spying. A secret French agent looked to see if he could bribe a German official to show up the Enigma blueprint. He found a perfect candidate in Hans-Thilo Schmidt, a disaffected worker who had gotten a job, courtesy of his brother, Rudolph, who was head of secret communications for Germany. The secret agent, code named Rex, met Hans-Thilo on November 8, 1931, and paid him 10,000 marks to take pictures of what was essentially the blueprints to the Engima machine.

The French looked at the plans and realized they had no idea how they might break the code, even given how the machine was built. But, the French and the Polish had a peace time military cooperation pact, so the French shared with the Poles the pictures they had of the Engima plans. The Polish decided to start working on breaking the machine, using intercepted messages.

Breaking Enigma

A mathematician named Marian Rejewski was ultimately successful in breaking the Engima. In order to do so, he had to use information about how the Engima was used. In particular, since the bulk of each message was encrypted at different "points" of the cycles of the rotors, it was difficult to glean meaningful information that way. But, the first six characters of each message were always encrypted with the same day code (for a single day), so many messages collected from the same day could have valuable information in their first six characters, since these six characters were encrypted under the same machine settings.

It turns out that Rejewski discovered a rather obscure pattern based on these six letters. Recall that the six letters were guaranteed to be a set of three letters repeated, the message code. He focused on the first ciphertext letter and the fourth ciphertext letter, since this represented the encryption of the same letter. For example, if the first ciphertext letter was 'P' and the fourth ciphertext letter was 'B', then Rejewski would write down a table (like a substitution table), where the input was 'P' and the output was 'B'. As more messages came in, he would use these two letters of ciphertext to build a full table. (This could also be done for the 2^{nd}+5^{th} letters and 3^{rd} and 6^{th} letters of the ciphertext.) As an example, imagine an alphabet of size 8 (A through H) and having the following table built:

1^{st} letter	A	B	C	D	E	F	G	H
4^{th} letter	F	E	A	H	B	C	D	G

Another way we can express this table is to write down the chains we get by writing arrows moving from the first row to the second:

A → F → C → A
B → E → B
D → H → G → D

It turns out that if you just follow these steps (go from input letter to output letter, then use that output letter as the next input letter), you'll always form some cycles. (See if you can intuitively convince yourself of this!) What's even more shocking is that Rejewski realized that for all of the $6 \times 26^3 = 102{,}576$ settings of the rotors (which rotation each of the three are and the order of the three in the machine), that **the list of cycle lengths** was unique for each!!!

So, the fundamental way in which Rejewski broke Enigma was by using the blue print he had, he built a machine. Then, for each of the 102,576 settings of the rotors, he encrypted different day codes, so that he could generate the matching cycle information for each possible setting. This work was very, very tedious and took a full year.

Once this table was built, then, after intercepting enough messages within a single day, the mapping chart between letters 1 and 4 of the ciphertext could be created, and from this, the cycle lengths deduced. Finally, the set of cycle lengths were arranged so that they were easy to look up into the book as the setting for that day. Once the day code was known, then the message could be decrypted, since plugging that into the machine revealed the message code, and then that could be used to decrypt the message.

Enigma Change – 1939

In 1939, to increase the difficulty of Enigma, 2 new rotors were added. Now, instead of the rotors being organized in 6 possible orders ([1,2,3], [1,3,2], [2,1,3], [2,3,1], [3,1,2], [3,2,1]), there were 5 x 4 x 3 = 60 possible orders for the rotors. The rationale here is that there are five choices for which rotor goes in the first slot, four choices for which rotor goes in the second slot, and three choices for which rotor goes in the third slot.

Now, instead of Rejewski needing 6×26^3 look up charts, he would need 60×26^3 look up charts, which is ten times as many. If he went at the rate it took him to make the first set of charts (6×26^3 settings in one year), then it would have taken him nine years to make the look up books for all the new settings introduced my just adding 2 rotors.

If you think about it, this is really quite ingenious. Since the early 1920s, the infrastructure of the regular Enigma machine existed. The rotors had always been interchangeable, and it was possible to generate many rotor designs (ultimately, these are just wired permutations). Thus, at relatively low cost (no need to make new machines), the possible machine settings was multiplied by 10 just be adding two new rotors, which could separately be distributed to everyone who had the old Enigma machine.

Enter the British and Turing

In 1940, when the Polish were no longer able to reliably read Enigma messages, they shared their work with the British, who were stunned with just how successful the Polish had been for years in reading Enigma messages. All of the information that Rejewski had ascertained (the signature cyclic behavior of the repeated encryption of the message codes in particular), were passed onto the British and known by Alan Turing, who gained previous fame for the Church-Turing Thesis.

Turing helped further mechanize the process of figuring out the cycle characteristics of all of the new Enigma settings. With the greater resources of the British government, he was able to finish in about a year's time, the rest of the entries needed to help the Allies start decrypting Enigma encrypted messages on a regular basis.

In the details of the process, here are some other factors that helped the Allied forces:

1) Certain Enigma machine operators would pick the same message code (say their girlfriend's initials) over and over again. On occasion, specific operators could be identified by their "fist", the way in which they sent morse code. Thus, lucky guesses (hey, this message was send by this one person who always seems to use "LPR" for his message code) greatly expedited the process of discovering the day key!

2) The Germans always sent out a weather report at the exact same time of day, each day. The format of this report was fixed and the German word for weather appeared in the exact same character indexes each day.

3) The Enigma never allowed a letter to encrypt to itself. Thus, when put together with other clues, this aided the decryption process.