ENIGMA CRYPTOGRAPHY

ABSTRACT:

In this paper you will be reading about enigma cryptography. You will learn how the machine is assembled and how the signal travels through the enigma machine, including the machines 6 steps through the journey. We will go in depth with enigma cryptography and how the machine is able to encrypt the signal messages. To gain better understanding, you will read about WWII and how this enigma cryptography impacted, and contributed to this war.

Karyliz R. Daniel G. Chevon A.

COM 416-Introduction to Information Security

10/3/2017

Dr. Nguyen

Enigma Cryptography

Introduction:

On August 5 of 1857, a cable was laid out across the Atlantic Ocean to allow quicker and better communications between the United States of America and the British. The cable allowed machines to communicate across the continents through electrical impulses. This form of communication stood for a while as a onetime path for communication. It was not until World War II that the forms of communication changed.

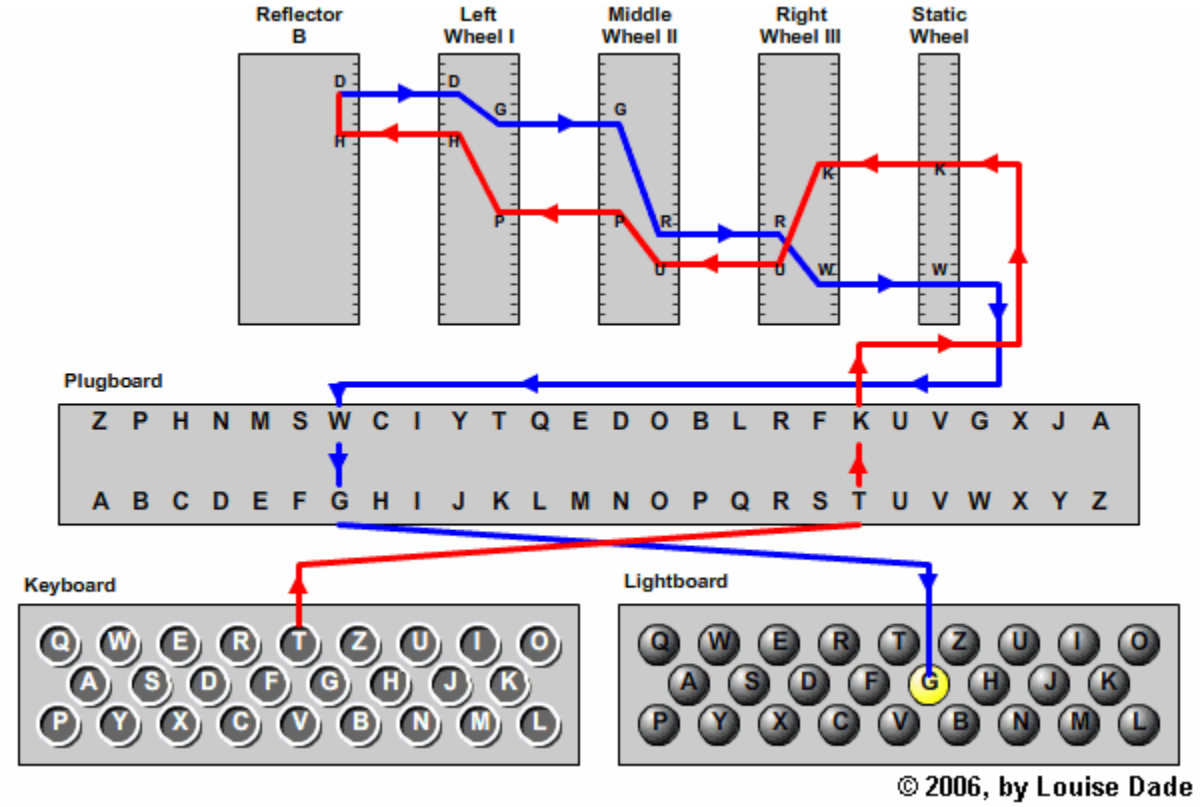
The German and their alliances were outnumbered by a lot, so instead of increasing their numbers in men, they decided to come up with new technology. This technology, at the time refer to as the rotor encryption machine allowed to send encrypted messages by using sequence of scrambled numbers that would translate into one letter of the alphabet that would subsequently stand for another letter of the alphabet. To be successful in what is now a two-way encrypted communication they would require same machine, agree on an initial position (which is defined as the key setting), align the machine to the same position, which then would circle through identical operations to achieve identical operations to achieve the same sequence. They used an odometer to scramble the numbers that was the key part that made a sent the message from one end to the other.

Later on, in the years around 1918, some electrical engineers had founded a firm and had created basic cypher machines and they wanted to make that firm associate with the German Navy and make them add in their cypher machine and put it to good use. The naval staff ended up using this machine and had thought that it was absolutely amazing and wanted to put it to great use. This machine enabled people to have what is called a Cipher mechanism and this lead to a great discovery for the Enigma machine. The first enigma machine comprised of a progression of rotors through which electrical current could go in a way that relied upon the relative introduction of the rotors. The path is taken by the current associated an input image to a yield framework. After each key press, the rotors experienced a venturing movement that changed the utilitarian relationship between input and output for the keys that followed. A sender and recipient who arranged their machines utilizing a similar starting setting, dictated by the catchphrase, could then trade scrambled messages. Soon this enigma machine became a major part of the world helping people to all kinds of things and make it a lot easier for people to type, input an image and even more.

Enigma A which was made in 1923 and was the first machine to put its output directly on a piece of paper. This was only one of the many different kinds of enigma systems that made a major impact on Germany's military. There are many other different kinds of enigma machines that changed the way the Germans communicated with one another, interacted with one another, and how they dealt with allies and enemies.

The components of the Enigma machine:

The enigma machines are very well known but does anyone really know how it works? Like stated before, the enigma main idea was to be write a sort of like a secret language that it is stated to mean another letter, which then was really a to substitute another letter.



The enigma machine was, well is an electro-magnetic device. Apparently, the enigma begins with sending a signal which is then, sent to different areas of the of the machined (followed a path) which went on a one-way path to another enigma which is then received and then the pattern goes on and on.

To get a little more familiar of the enigma machine we should begin by know its key parts and as well, know how does different contribute to what enigma cryptography communication. The main parts of the enigmas machine messages include, Keyboard,

plugboard, static rotor, scramblers (more rotors), reflector, reverse journey, and lastly the lamp board.

For the message to first be formed we would need to input the message in to the machine, which would be done by applying the message into the keyboard.

After the message is the imputed, the plugboard will be the messages the second stop in the journey. The plugboard is where the wiring that is causes the electrical signal which is imputed into the keyboard is now transferred to it connected cyphered letter.

This then leads us to, the static rotor. The static rotor has nothing to do with the static itself. The static rotor does more with just wires into contacts. Then, when the contacts touch they allow for the signal to pass through.

Then our signal passes through out rotor/scramblers. Scramblers do exactly what they are name after and that is to scramble the signal. For example, when you input letter “R” when the signal is the passes through the scramblers now the letter is then converted to letter “K”. In the machine there are five of these rotors that can be place in the either the left, middle, or right positions. It is important to know that each of these rotors contain an inner and out ring; these rings sole purpose is to scramble the signal it is given. Rings are often rotated or traded/substituted to provide more alternative scrambled signal. The rotors itself is also rotated. This constant rotating relates to the fact that when the letter itself are scrambled and not displayed in the same order that they we placed on the machine. Then the signal is then reflected.

Once the signal is reflected, it goes back to the rotors which is all part of the reverse journey. As the signal passes through the rotors it changes the letters a couple of more times depending on the rotation of rotors which then it’s taken back to the

plugboard. In the plugboard in there is no actual plug the letter stays the same however if there is a plug the letter in the redirected to its original state.

Finally, we are directed into out lamp board. The lamp board is works so if the letter is “R”, the letter “R” in the lamp board lights up.

Cryptography’s Overview, and Its Impact:

The use of Cryptography has been used for over a thousand years to hide secret messages and almost in a way communicate with people or things but remain secretive. As far as we know Cryptography was used around 1900 BC inside underground tunnels or tombs and would be a secret communication that used symbols and things such as object figures and each would mean something particular. Egypt as you can see was the main birthplace of this fine secret language and would continue to evolve over the years. Soon it began to spread all over the middle east to places like India and Indonesia. They would use Cryptography over in these countries to pass on secret messages to spies in secret writing. This was a great way to communicate with each other and not be known whatsoever to the public. Later on, around 100 BC the famous Julius Caesar even used a form of encryption so that he could communicate with his soldiers and even his Army generals that were all over the place at one time. You never wanted an enemy knowing what was going on because if that happen your whole operation could go straight to the ground. Later on, people started to discover how to not just speak secretively but began to start actually creating cyphers. These cyphers sometimes would have an actual encrypted key and to be able to get into it certain steps would have to be repeated as much as 15 times.

Around the 19th century Cryptography became a lot easier to understand and in a way, was easier to use. They became electric, and it turned into a machine that had a single rotor and the secrets or anything that you wanted to keep a secret would be in a rotating disc. When the disc would rotate, a different table would be used meaning that a different message was used to or was transmitted. After this was discovered Cryptography spread all over the globe because people were figuring out how to send messages not only where no one knew what it was but because you could do it long distance. This was great for the military because it helped send strategy's and strategic ways to take down enemies and attack their weak points.

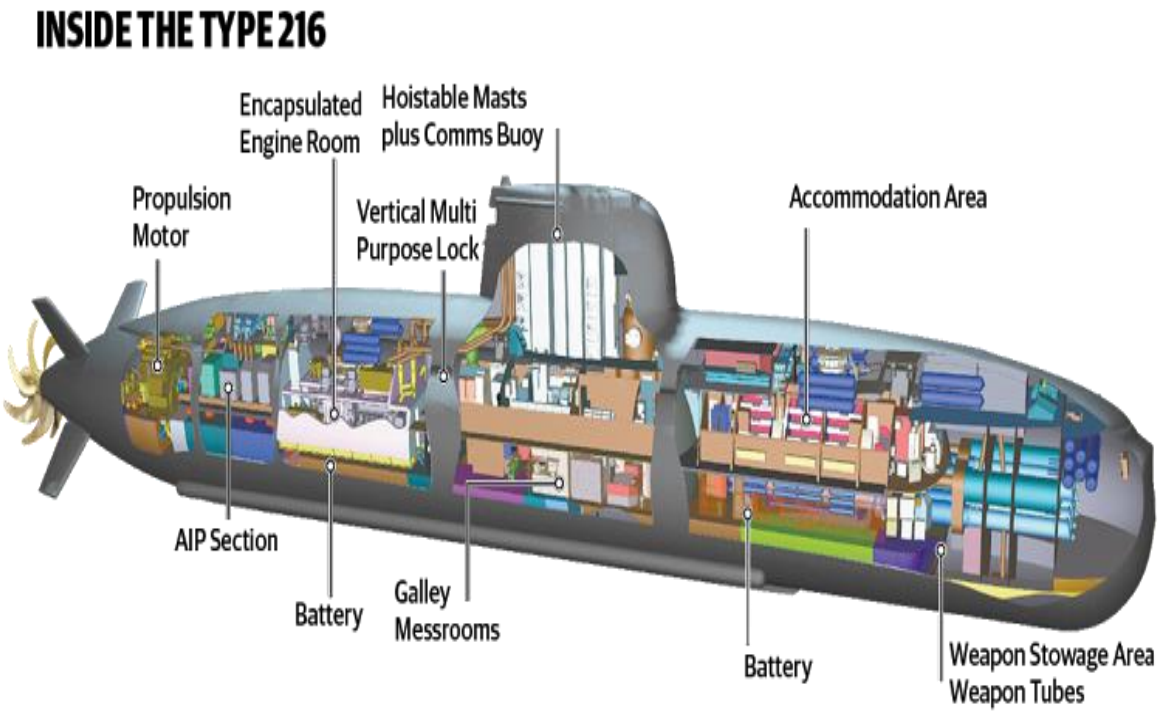
Soon one of the biggest things that the Germany Military had was the making of a machine called the Enigma machine as you can see from the picture above. This

machine had a couple key components on it including rotors at the very top, and these would spin when someone was typing something. Next, we have the lamp board and the keyboard that both acted as typing mechanisms for when someone wanted to send out a message. And last but not least the plug board for any electrical uses. This machine was used throughout World War 2 for inputting secret military information. This form of Cryptography was one of the most highly used ever and gave Germany a big advantage. One of the down sides to having this machine was that other country's or even other companies in general wanted this machine and would try to steel the copyrights and all the key information that would be with stowed in it. Groups such as foundations started to make their own encrypting, making it to the best of their ability then it started to become a competition between everyone.

Now a days Cryptography has a different way of being displayed and transported to other places. Now we use algorithms to solve equations, messages, and even encrypt secret data to where you can only get access through a higher up or even government agency. To get into encrypted systems and bypass them is literally almost impossible now a day's. Systems, machines, and a whole bunch more have certain password and keys where there can be anywhere from 100 – 100 billion different possible password or keys to be able to get into the system. Today, we use Cryptography every day. Whenever we buy something and swipe our card our information is going to a secure database, or even when we buy something online, that also is secured by either a key or encrypted so our info doesn't get released out there.

How the enigma machine was used during WWII

The U boat was considered unsinkable due to the enigma machine. The U boats of Germany used the enigma as a weapon where they would send encrypted code of the location of the allies' ship. When the u boat gets the code from the enigma, they would go and sink the ship. This was a big problem for the allies because this would mean that Germany would own the sea.



The U-boat can work submerged just for brief periods at once. For the U-boat compel, it was considered as a torpedo watercraft, with the uncommon capacity to submerge for assault or as a protective measure – thus offering to ascend to the name Undersea Boat or U-pontoon. All things considered, a U-boat is an exceedingly modern vessel of war, with many accuracy controls and a 45-man team to work.

On the U-boat, the conning tower rises amidships. Whenever surfaced, the U-boat is guided from the highest point of the conning tower. Whenever submerged, it is

worked from a control room specifically underneath the conning tower. Inside the weight structure, weight entryways separate the watertight bulkheads into compartments, which contain the apparatus, combat hardware, stores and living quarters.

So, the U-boat can see the surface action without being spotted, it is fitted with periscopes. Some U-boat is equipped with two periscopes, an assault periscope for watching and focusing on surface boats and a perception periscope for filtering the skyline for flying machine. These are further fitted with amplification focal points which zoom mode could be flipped like a camera's zoom focal point.

Conclusion:

To finalize, the enigma was one of the earliest revolutionary forms of communication. It begun like every new technology begins, with war. From a one-way communication physical cable stretching from coast to coast. To later, that cable being used to be able to morph into a two-way communication, by sending out signals from one machine to the other. That is the main reason why these machines were placed on U-boats. This enabled for the enigma machine be one of the fastest and most effective ways of communication during World war II. A simple machine with six main steps (from the keyboard to the lampboard), which allows for encrypted messages to be displayed in a light-up board. This allowed to avoid any unwanted interference from enemies, and the encryption in each messaged allowed only wanted parties to read the message without their enemies being able to see, read, or established their next move. In simple terms, war during this time was of such high hostility, that lead to the governments being so paranoid. This paranoia ignited creation which lead new ways of

communication that in one way assisted the evolution of communication and technology in the longs run.

References

http://www.idt.mdh.se/~gdc/work/TURING-SEMINAR/TURING-NATURE/DawnOfComputing.pdf

https://link.springer.com/chapter/10.1007/978-1-349-07234-7_7