International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Breaking the Unbreakable

Ayush Singh Sagar

Sem-01, MSc. Mathematics

When we hear about World War 2, it is natural that the first thought about it a person has in his/her mind is of mass destruction and murder of innocent Jews. However, among these extremes there lies inexplicable countless stories of bravery, love and sheer intelligence of the human mind.

World War 2 started with the invasion of Poland by Nazi Germany under the leadership of the then Fuhrer Adolf Hitler in 1939. Which rained down havoc on the world but the main highlight of it is the resistance against these acts of cruelty against humans.

I must say Resistance to fascism was the fight to breathe under a suffocating closed room filled with poisonous gases. Which came in many forms like resistance groups, guerilla warfare, execution of German officers, Operation Valkyrie, all-out War, spying and then there were mathematicians cracking the unbreakable German code-**THE ENIGMA**.

One such genius among men was Alan Turing. Let us know about the man behind winning a crucial battle for Britain over Nazi Germany and saved millions of lives using not guns but Mathematics.

Some of you may know him by chance about what I am going to discuss about further but other of you who does not have a clue about this. Do not worry I got your back.

The first question is what is an enigma? (In relation with the World War 2)

In literary terms, ***Enigma*** means something, which is difficult to understand and is mysterious or another meaning can be something, which is next to impossible to understand. Now, let us enter the world of "world war 2" and relate enigma to it.

During World War 2, Nazi Germany's military command mainly used to encode strategic messages before and during World War 2. What we know as the technique of cryptography. The technique of converting a readable message into an unreadable form and sending it to the trusted party avoiding the risk of disclosure to the third party. Which is synonymous to encryption and decryption of a code. The formulation of such messages and regular transmission was the daily need of the hour during the war.

What kind of code they had sent?

Why was it important to decode them?

I can mention one incident where if the code have had been decoded it could have saved lives that mattered.

The innocent and affected Londoners in the 20th century were very less aware of what was waiting for them with the onset of war. Germany had already invaded Poland at the dawn of 1 September 1939. The poles were quite unprepared for what was going to happen and were dumbstruck by the new ***blitzkrieg*** form of warfare used by German military on the poles. By 16 September, they reached the Poland's capital and by 27September, it had fallen to Nazi Germany. Now Britain was at war with Nazi Germany officially. The war officially broke out between the two countries on July 10, 1940 with the attack of 120 German aircraft sent by the German Airforce-the *Luftwaffe (1).* When the *Luftwaffe* found it difficult to raid in the day, they began to raid at nights. Every night the Londoners dreaded the night bombing such was the atmosphere of paranoia. One such incident where no intelligence could prevent the destruction was at the Coventry. Three main forces of bombers streamed in over 439 of them in total. British Intelligence decoded the German signals and even found the code name-*Mondlichtsonate (German), which* is "moonlight sonata" *(2).* The Enigma Coded messaged did reveal that the target was the factory at Coventry but it was too late to figure it out. The bombers dropped more than 1000 incendiaries that led to 60,000 damaged buildings, 111 factories, 600 shops, 28 hotels and all of cities railway lines. The raid killed 568 people and injured were 1256, which became atomic level of German brutality as more was to follow.

Lest the British were able to break the code completely, the damage could have been reduced or completely avoided.
The unbreakable German enigma code was the one of the very things that was giving the allies a tough fight. The first break of deciphering the German Enigma code came in 1932 when a polish mathematician and cryptologistMarian Adam Rejewski. The techniques developed by the polish cryptologist were later shared with the British, which they tweaked, and modified to their convenience and cracked the unbreakable enigma code of the Germans.

The breakthrough of cracking the enigma for the British at the Bletchley Park where Government code and cypher school (GC&CS) was housed during the World War 2. The GC&CS code breaker team included **Alan Turing**, Gordon Welchman, Hugh Alexander, Bill Tutte, and Stuart Milner-Barry.

One of them was Alan Turing who played the key role in successfully dismantling the German Enigma and saving millions of lives.

The Question of the hour is what kind of German Enigma machine was? What made it so impossible to break? How Alan Turing was able to break the unbreakable?

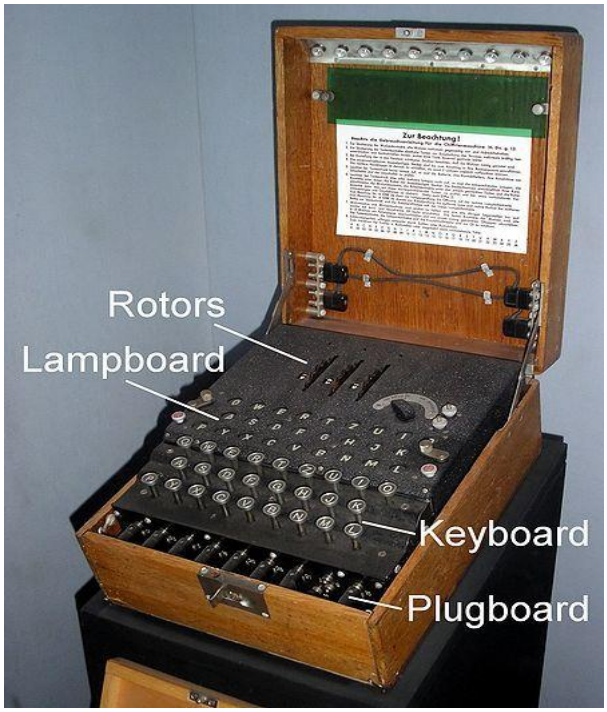
Let us address the first question that is,

Whatis an Enigma Machine?

The Enigma machine was a cipher machine used extensively by the German *Wehrmacht* (Nazi German Military) for the purpose of transmitting their messages and maintaining secrecy and privacy.

GERMAN ENIGMA MACHINE 1937-1938
SERIAL NUMBER- A6551
Image Courtesy:
https://simonsingh.net/cryptography/enigma-photos/

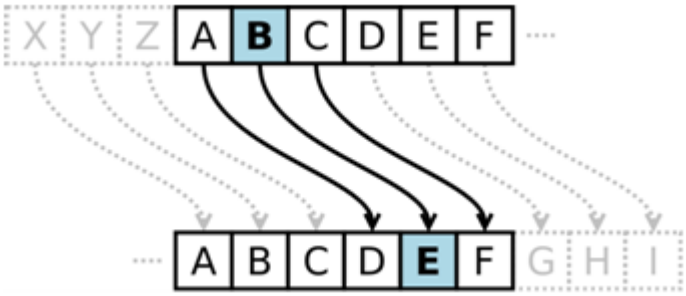
Working of the Enigma Machine:
An enigma machine had a keyboard, a lamp board, rotors/drums, a plug board and an internal electronic circuitry that made the whole machine work.



Enigma Machine at the Imperial War Museum, London

There are several ways of encryption where this machine used substitution form of encryption. A simple example of it is Caesar cipher, which is very easy to understand.

Below is an image of Caesar Cipher with the shift of 3.



So if you were to encode “Mathematics” using Caesar Cipher with the shift of 5.

a	b	c	d	e	f	g	h	i	j	K	l	m	n	O	p	q	r	s	t	u	v	w	x	y	z
f	g	h	i	j	k	l	m	n	o	P	q	r	s	T	u	v	w	x	y	z	a	b	c	d	e

It would be encrypted as “rfymjrfynhx” , which is gibberish for the layman but easy to understand for a decipherer.(you can also try your name)

The above example is quite straightforward and the encoded message is quite vulnerable. Here, the enigma machine came to rescue.

In the machine, when a key on the keyboard is pressed, one or more rotors move to form a new rotor configuration, which will encode one letter as another. Current flows through the machine and lights up one display lamp on the lamp board, which shows the output letter. Therefore, if the "K" key is pressed, and the Enigma machine encodes that letter as a "A," the "A" would light up on the lamp board.

The extraordinary thing about the machine is the encoding of a single alphabet is not repeated. For instance, Considering the above mentioned example the letter “K” was encoded to letter “A” as it was once encoded “A”. Again pressing the letter K on the keyboard would never reflect A on the lamp board. Which provided the complexity of the machine.

There were 3 slots available for rotors in each machine and each rotor had 26 numbers/letters on it. The operator had to choose any of the possible combination of 3 rotors from 5 available rotors.

In the first slot, there are 5 rotors to pick from, in the second there are 4 rotors to pick from, and in the third slot there are 3 rotors to pick from. So there are

Total combinations of rotors would be
5×4×3=60

And each rotor had 26 starting positions, so there are
26×26×26=17,576
Choices for initial configurations of the rotors' numbers/letters.

Since there are 26 letters in the alphabet, there are 26! Ways to arrange the letters, but the plug board can only make 10 pairs, so there are 20 letters involved with the pairings, and 6 leftover that must be divided out. Furthermore, there are 10 pairs of letters, and it does not matter what order the pairs are in, so divide also by 10!, and the order of the letters in the pair does not matter, so divide also by 2^10.

The resulting number of combinations yielded by the plug board is as follows:
26! /6! ×10! ×2^10=150,738,274,937,250.

All of the components put together yields:
60 * 17576 * 150,738,274,937,250 = 158,962,555,217,826,360,000

Total number of ways to set a military-grade Enigma machine.

Each month, Enigma operators received codebooks, which specified which settings the machine would use each day. Every morning the code would change. So now, one can understand why a single code or message was next to impossible to break.

Cracking the Enigma

Impossible is nothing for the one who is determined towards the task. So proved by Alan Turing and his teammates at Bletchley Park. They cracked the enigma using their own machine, which was called Bombe Machine.

Which accomplished its task to break the enigma using electric circuits under 20 minutes. The machine would try to determine the settings and the arrangement of the rotor and plug board as to crack the enigma it was necessary.

However, even after cracking enigma they lost battles for winning the war. Even the cracking of enigma posed a problem as they cannot tackle every attack of the German, which will alert the Germans and may lead them to change the settings of the Enigma Machine and they have to repeat the mammoth task of cracking it again.

Alan Turing's contribution in the war led the allies win the war of Atlantic. But his contribution did not stopped there. He went on to make contributions after the war like designing Automatic Computing Engine (ACE) , The Manchester Computers and even contributed in Mathematical Biology.

Absolutely, He is regarded as the father of theoretical computer science and artificial intelligence.

Despair shadows a person when he/she gets to know the man of such caliber was not recognized and mistreated in his own country. He was charged for Homosexuality and died by cyanide by poisoning on 7th June, 1954. He was posthumously pardoned by Queen Elizabeth the 2nd in 2013.

References

[1] World at war- Reader's Digest
[2] Enigma Machine- Karlegh Moore, Ethan W, Ejun Dean
[3] Alan Turing by B.J. Copeland
[4] How Alan Turing Cracked The Enigma Code at iwm.org.uk.
[5] Alan Turing by Jacob Aron