
COMPUTERS AT WAR
Bob Walker

In honour of tonight's meeting being on Remembrance Day, we'll look at how the development of early computers was brought about by World War Two.

In particular we will be looking at the codebreakers of Bletchley Park like computer pioneers Alan Turing, Gordon Welchman, Tommy Flowers and Max Newman who developed Colossus, the world's first programmable, electronic, digital computer, and used it to break the German Enigma and Lorenz codes and shorten the war.

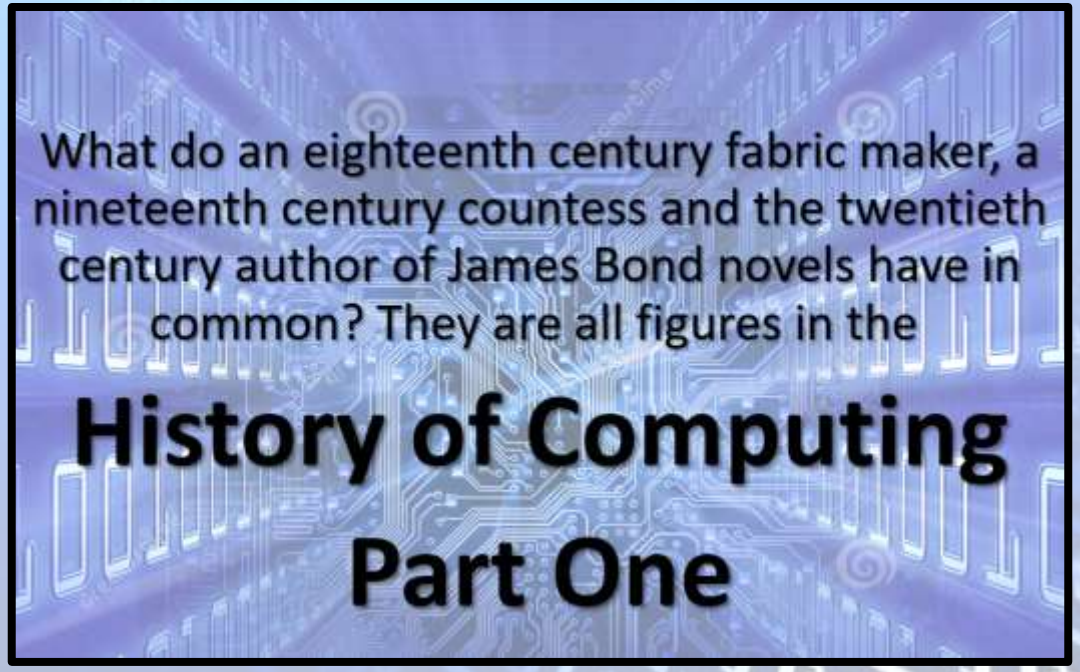
We’re not just going to look at what they did, we’re going to look at why it mattered, why it was so important.

We’ll also look at some of the other computer developments related to the war.

While I will focus on the Bletchley Park story tonight, there is a lot of other information at the end of this presentation deck I may not have time for, but the deck will be available on the OPCUG website.

I briefly covered some of this information in a presentation in February 2015 called *"The History of Computing Part One"* which covered the history of computers from prehistory through to the dawn of the personal computer and the beginning of the digital revolution.

That presentation is available on the OPCUG website in the "Past Presentations" section.



Tonight's presentation encompasses my intersecting interests in history (especially WW2 history) and technology

ZZZ

In 1978 historian and futurist James Burke did a 10 episode series "*Connections*" about how seemingly unrelated events led to major developments in the history of science and technology.

en.wikipedia.org/wiki/Connections_(TV_series)
Some episodes available on YouTube and Netflix

PBS

BBC

TLC
THE LEARNING CHANNEL

As part of this presentation I'm going to look at two different sets of Connections:

- **How events during World War II led to major developments in the world of computers**
- **How I came to do this presentation**

- Near the start of WW2, a bi-plane that was lost and low on gas landed on a prairie farm in southern Manitoba, and a boy showed the pilot where he was and got him some gas.
- In return, the pilot took the boy up for a ride.
- That boy was my father, Stuart Walker.

- When he was old enough to serve, he enlisted in the Royal Canadian Air Force.
- He served most of the rest of the war as a mechanic at the training base near Dauphin, Manitoba working on Tiger Moths, Harvards and Lancasters.
- When the war in Europe ended, he was in a barracks in Halifax waiting for a ship over to Europe.

When I was growing up he gave me lots of books including:

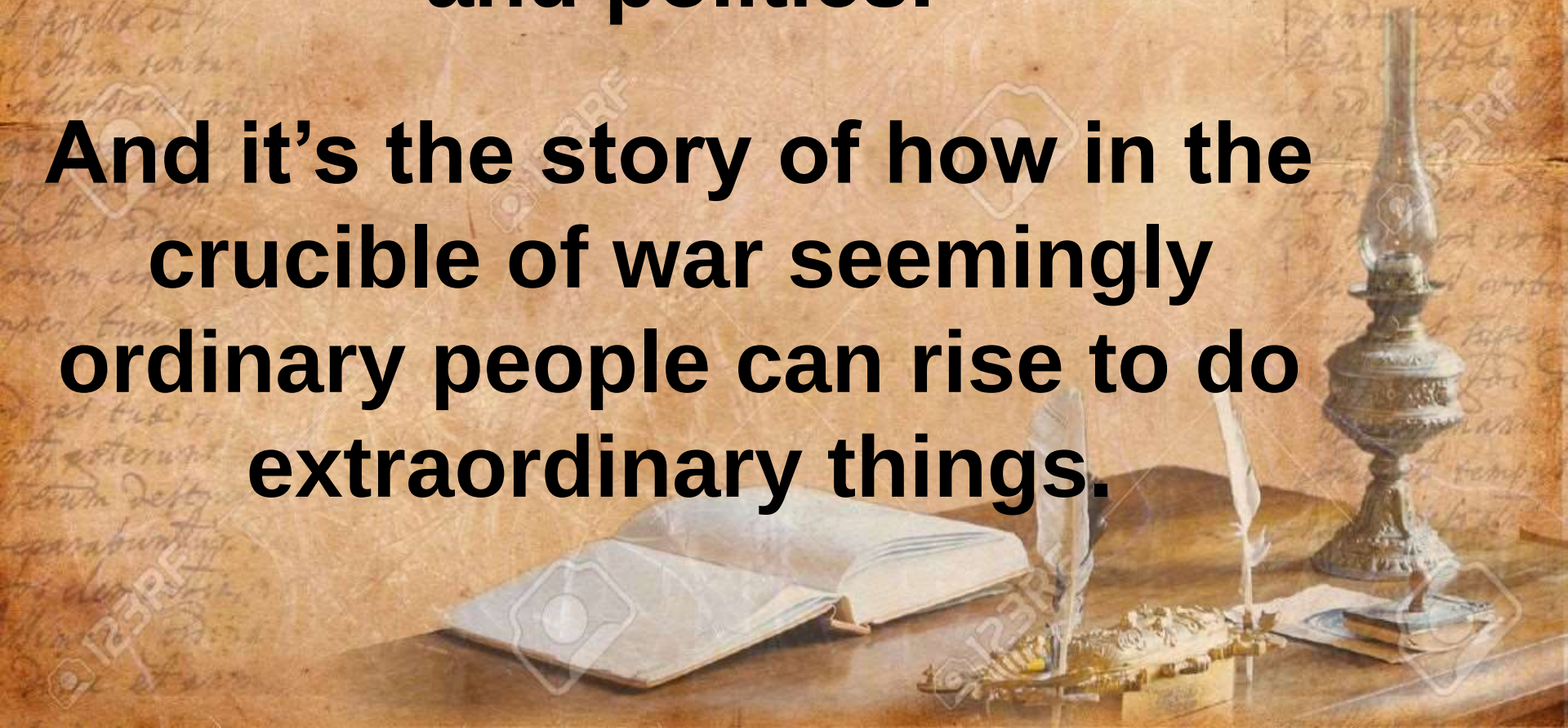
- ***"Knights of the Air: Canadian Aces of World War 1"*** **by John Norman Harris**
- ***"The Dam Busters"*** **by Paul Brickhill**
- ***"Reach for the Sky: The Story of Douglas Bader, Legless Ace of the Battle of Britain"*** **by Paul Brickhill**
- ***"The Great Escape*"*** **by Paul Brickhill**

*** - Paul Brickhill was actually involved in the Great Escape**

As a results of my father, as well as the influence of some excellent teachers, I developed a major interest in history, especially World War 2 history.

History is so much more than dry dates and events. It is the story of people, personalities and politics.

And it's the story of how in the crucible of war seemingly ordinary people can rise to do extraordinary things.



War Mobilizes Science

World War II led to major computer developments on both the Allied and German sides.

The Germans failed to utilize their computers in any effective way.

The British and Americans used theirs to help win the war.

War Mobilizes Science

Practical applications for computers during WWII included:

- **artillery ballistics table calculation,**
- **shipboard gun fire-control systems,**
- **torpedo aiming systems,**
- **bombsights,**

and most especially important,

ENEMY CODE BREAKING

Why Try to Break the Enemy's Codes?

"Winning at poker is not too difficult when you can see your opponent's cards"

- **Herbert Yardley, US Army's top code breaker in WW1 and head of the US Cipher Bureau in the 1920's**

"Gentlemen do not read each other's mail"

- Henry Stimson, Herbert Hoover's Secretary of State who in 1929 shut down Cipher Bureau

During World War 1 and throughout the 1920's and 1930's, military and diplomatic communications were primarily through telephone, telegraph and messengers, including messenger pigeons.

The Zimmermann Telegram

- The Zimmermann Telegram was a secret diplomatic communication from the German Foreign Office in January 1917 that proposed a military alliance between Germany and Mexico. If the United States entered World War 1 against Germany, Mexico would recover Texas, Arizona, and New Mexico. The telegram was intercepted and decoded by British intelligence.
- Revelation of the contents enraged Americans, helping to generate support for the United States' declaration of war on Germany in April.
- The decryption was described as the most significant intelligence triumph for Britain during World War I, and one of the earliest occasions on which a piece of signal intelligence influenced world events.

During the global arms limitation talks in Washington in 1921, the Americans intercepted and decoded telegraphs between the Japanese negotiators and Tokyo, and used the knowledge to gain extra concessions from the Japanese on limiting the size of their navy.

Pre-war German military planning emphasized fast, mobile forces and tactics, later known as blitzkrieg, which depended on radio communication for command and coordination.

Since adversaries would likely intercept radio signals, messages would have to be protected with very secure encryption. The compact and easily portable Enigma machine filled that need.

The Enigma Machine

The Enigma machine was invented in Germany at the end of World War I.

It was originally marketed under the brand name Enigma in 1923 as a tool to protect commercial communications.

It was soon adopted by military and government services of several countries, most notably Nazi Germany before and during World War II.

Enigma machines were electro-mechanical rotor cipher machines used primarily for enciphering and deciphering secret messages.

Breaking the Codes

Although Enigma and the later Lorenz did have some cryptographic weaknesses, properly used they should have been virtually unbreakable.

In practice it was German procedural flaws, operator mistakes, laziness, failure to systematically introduce changes in encipherment procedures, and the Allied capture of key tables and hardware that enabled Allied cryptologists to succeed in breaking the codes.

The Polish Contribution

- Poland recognized early on that Hitler's Germany was a major threat.
- In 1929 the Polish Cipher Bureau began trying to break the Enigma ciphers.
- In late 1932, Marian Rejewski, a Polish mathematician and cryptanalyst, managed to break the message keys of the Enigma machine.
- Rejewski did this without any knowledge of the wiring of the machine, so the result did not allow the Poles to decrypt actual messages.

The Polish Contribution

- French spy Hans-Thilo Schmidt obtained access to German cipher materials that included the daily keys used in September and October 1932. The French passed the material to the Poles, and Rejewski used some of that material and the message traffic in September and October to reverse engineer the unknown rotor wiring.
- After that the Poles were able to build their own Enigma machines and the Cipher Bureau was able to read German Enigma messages starting from January 1933.
- The Poles built six electro-mechanical cryptologic 'bomba' to search for rotor settings, but in 1938 the Germans added two more rotors, requiring ten times as many bomba devices and the Poles did not have the resources to build them.

The Polish Contribution

- **In July 1939, suspecting that a German attack was immanent, the Poles invited French and British military intelligence representatives to Poland to share their work on Enigma with them.**
- **The demonstration represented a vital basis for the later British continuation and effort.**
- **In September 1939, after the Germans invaded, the British smuggled some of the Poles through Europe to Britain.**

Meanwhile in 1937

In 1937 new approaches , technologies, and theories began to emerge, exactly a hundred years after Charles Babbage first published his paper on the Analytical Engine.

1937 would become an Annus Mirabilis (Year of Wonders) of the computer age.

The result would be the emergence of the '*Four Properties*' that would define modern computing.

1937 and the ‘Four Properties’

- **DIGITAL** (discrete vs continuous, digital not analog)
- **BINARY** (‘0’s and ‘1’s)
- **ELECTRONIC** (not mechanical)
- **GENERAL PURPOSE** (able to do many things vs a mechanical computer that can do only one thing)

Bletchley Park

During World War II the Brits established the British Government Code and Cypher School (GC&CS) at Bletchley Park northwest of London

Bletchley's Location

- In 1938, Admiral Sir Hugh Sinclair, head of the Secret Intelligence Service (SIS or MI6) and his colleagues scouted the site under the cover of "Captain Ridley's shooting party".
- Sinclair bought the Bletchley mansion and 58 acres (23 ha) of surrounding land for £6,000 (£386,000 today) for use by GC&CS and SIS in the event of war. He used his own money as the Government said they did not have the budget to do so.
- A key advantage was Bletchley's geographical centrality. It had:
  - Railway connections to London and the rest of Britain, and to Oxford and Cambridge - whose universities were expected to supply many of the code-breakers.
  - Road connections to London and the northwest of England.
  - High-volume communication links were available at the telegraph and telephone repeater station in nearby Fenny Stratford.

The Site

The original manor and outbuildings were added to extensively during the war, including the famous ‘huts’ where most of the work was done.

The Manor

Hut Six

Bletchley's Alias'

- Bletchley Park was known as "B.P." to those who worked there.
- Cover names used during the war included "Station X", "London Signals Intelligence Centre" and "Government Communications Headquarters".
- The formal posting of the many "Wrens" (members of the Women's Royal Naval Service) working there was to HMS Pembroke.
- Royal Air Force names of Bletchley Park and its outstations included RAF Eastcote, RAF Lime Grove and RAF Church Green.
- The postal address that staff had to use was "Room 47, Foreign Office" in London.

Bletchley's People

- **Key GC&CS cryptanalysts were moved from London to Bletchley Park.**
- **Recruitment of new talent included:**
  - **linguists,**
  - **chess champions,**
  - **papyrologists (the study of ancient manuscripts, including deciphering ancient hieroglyphs),**
  - **top solvers of cryptic crossword puzzles,**
  - **historians,**
  - **experts in Morse and other codes**
  - **German language and culture experts**
  - **mathematicians like Alan Turing and Gordon Welchman.**

Bletchley's People

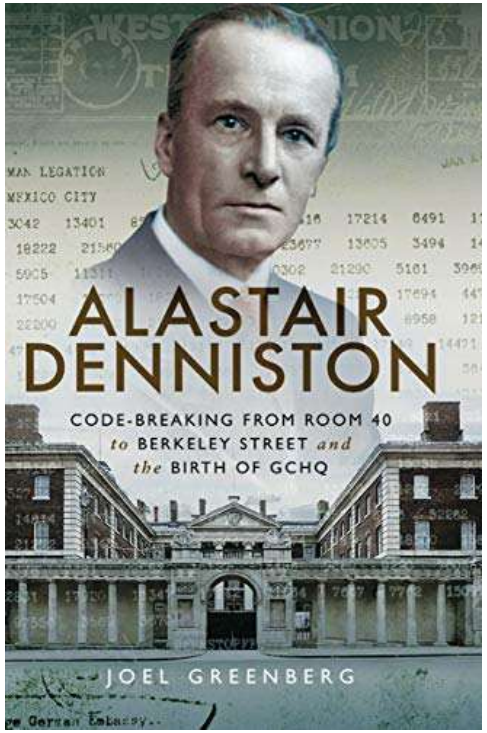
In January 1945, at the peak of codebreaking efforts, nearly 10,000 personnel were working at Bletchley and its outstations.

The Women of Bletchley

About three-quarters of the people at Bletchley were women. Many of the women held degrees in the areas of mathematics, physics and engineering; they were given chance due to the lack of men, who had been sent to war. They performed calculations and coding and hence were integral to the decryption processes. Many of the women had backgrounds in languages, particularly French, German and Italian.

Bletchley's Leadership

- Alastair Denniston was initially in charge of Bletchley.
- Despite his knowledge of the success of the Polish cryptologists against Enigma, Denniston was pessimistic about the prospects of breaking the more complex German Naval Enigma encryption.
- There was also a personality clash between Denniston and Stewart Menzies, the Director of the Government Code and Cypher School and the head of the Secret Intelligence Service.
- Under Denniston there were ongoing and unresolved management problems at Bletchley.



The Wicked Uncle's Letter to Churchill

- **In October 1941 four senior cryptanalysts (later known as the 'Wicked Uncles') Alan Turing, Gordon Welchman, Hugh Alexander, and Stuart Milner-Barry wrote directly to Churchill over the head of Denniston to alert Churchill to the fact that a shortage of staff at Bletchley Park and other problems were preventing them from deciphering many messages, to the detriment of the war effort.**
- **In the letter, there was praise for the *"energy and foresight"* of Commander Edward Travis, Denniston's second in command.**
- **Churchill reacted to the letter immediately, ordering *"Action this day make sure they have all they want on extreme priority and report to me that this has been done."* Resources were transferred as fast as possible.**

Bletchley's Leadership

In February 1942, GC&CS was reorganised. Travis succeeded Denniston at Bletchley Park, although both were listed as "co-directors".

When Travis took over, he *"presided over an administrative revolution which at last brought the management of Intelligence into line with its mode of production".*

Commander Edward Travis

Secrecy at Bletchley

- **All staff signed the Official Secrets Act (1939) and security warnings emphasised the importance of discretion even within Bletchley itself:**

  "Do not talk at meals. Do not talk in the transport. Do not talk travelling. Do not talk in the billet. Do not talk by your own fireside. Be careful even in your Hut."

- **Nevertheless, there were security leaks. Jock Colville, the Assistant Private Secretary to Winston Churchill, recorded in his diary on 31 July 1941, that the newspaper proprietor Lord Camrose had discovered Ultra and that security leaks *"increase in number and seriousness"*.**

Secrecy at Bletchley

- After the United States joined the war, a number of American cryptographers were posted to Hut 3, and there was very close co-operation between British and American intelligence.
- In contrast, Stalin and the Soviet Union was never officially told of Bletchley Park and its activities – a reflection of Churchill's distrust of the Soviets. However, Bletchley Park had been infiltrated by John Cairncross, the notorious Soviet mole and member of the Cambridge Spy Ring, who leaked much of the decrypted material to Moscow.
- All of the German spies in Britain were either turned into double agents working for the British or executed.

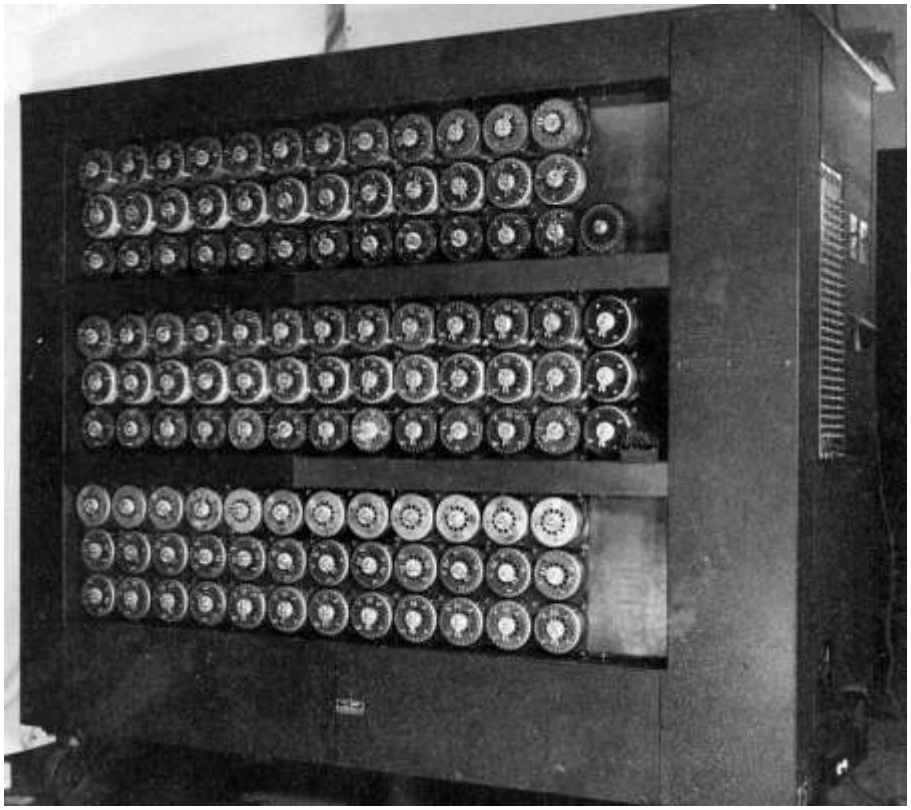
The ‘Bombes’

- **The bombes were electro-mechanical devices used by the British cryptologists to help decipher German Enigma encrypted secret messages during World War II.**
- **The British bombes were developed from the Polish bomba’s.**
- **The US Navy and US Army each developed their own bombes based on the Polish and British bombes, and shared them with the British.**

The Turing Bombe

Alan Turing had developed a decryption technique that became know as "Banburismus". The initial design of the British bombe in 1939 was done by Alan Turing to mechanize his technique.

In 1940 Gordon Welchman added the 'Diagonal Board', which made the Bombe immensely more powerful.



The Turing Bombe

The first bombe (code-named Victory) was operational in March 1940 while the second version (Agnus Dei or Agnes) incorporating Welchman's 'Diagonal Board', was operational by August 1940.

The U-Boat War

- The over-centralised command structure of German Navy and its insistence on micro-managing every aspect of U-boat operations. The resulting endless flow of signals provided the British with enormous intelligence. The sheer volume of radio traffic compromised the German ciphers by giving the British more messages to work with.
- Furthermore, transmissions from the boats enabled the Allies to use radio direction finding (HF/DF, called "Huff-Duff") to locate a U-boat that was using its radio, and then track it and attack it.
- Through the decrypts the British were able to identify individual boats, their commanders, location, operational readiness, damage reports, type, speed, endurance, etc.

The Capture of An Enigma Machine

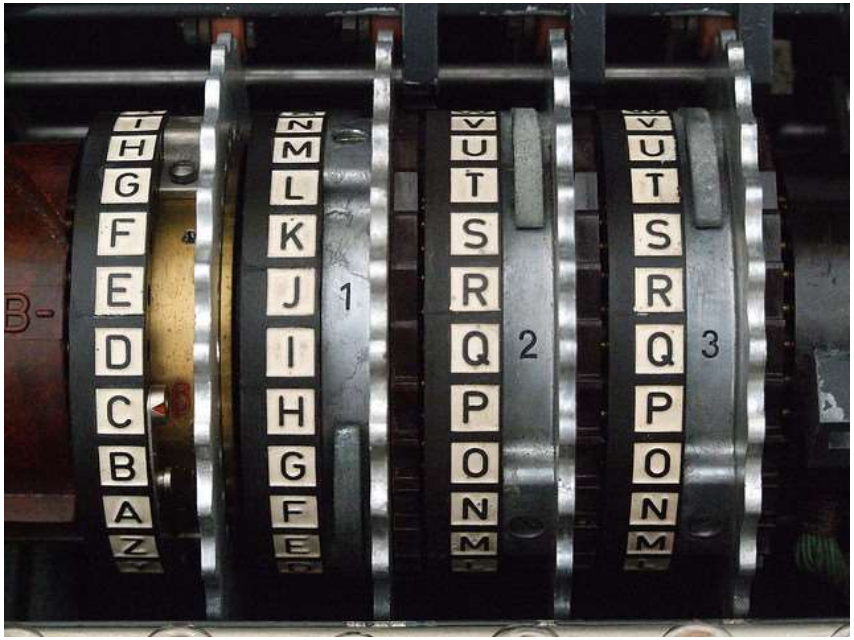
- In May 1941 U-110 was depth-charged near Iceland and forcing to the surface. While its crew was abandoning the boat, Sub-Lieutenant David Balme of the destroyer HMS Bulldog led a boarding party that removed the Enigma coding machine and various codebooks.
- The machine and code books were of great value at Bletchley, but it was an older three rotor machine, not a four rotor.
- The 2000 film “U-571” starring Matthew McConaughey about American submariners boarding a German submarine and capturing her Enigma machine is a total Hollywood fantasy and has absolutely NO basis in reality.

Capturing German Code Books

- Capturing secret code books was one of the keys to breaking German codes. The codebooks were used to determine the settings on the cipher machines.
- In 1940 the crew of a captured German ship threw their code books overboard, but the British Royal Navy managed to recover some of them.
- In 1942 British sailors recovered code books from a sinking U-boat in the Mediterranean Ocean.

The Fourth Rotor Problem

In February 1942 the German Navy introduced an Enigma version with a fourth rotor for its U-boats, resulting in a prolonged period when these messages could not be decrypted.



Note: It took the German Navy almost a year to swap out all the 3 rotor machines.

The Dieppe Raid

- The introduction of a 4th rotor in 1942 was preventing cryptanalysis of the German naval Enigma, and led to a strong resurgence in German U-Boat attacks on the vital Atlantic convoys coming from North America.
- Thus the Brits were eager to get their hands on one to discover and exploit any weaknesses in the new system.

Note: The resurgence was also due to the large number of U-boats the Germans were producing. Over 1,100 were made by the end of the war.

The Dieppe Raid

A raid on Dieppe, France was carried out in August 1942 as cover for a 'pinch' mission overseen by Ian Fleming (best known later as author of the James Bond action espionage books) to steal one of the new German 4-rotor Enigma code machines, plus the associated code books and rotor setting sheets, from the German Naval station there.

The Dieppe Raid

- The August 1942 raid was a failure and no machine was obtained.
- The new German naval Enigma code was not cracked until December of that year.
- The raid provided valuable lessons for the eventual D-Day Invasion

The Dieppe Raid

- **Of the nearly 5,000-strong Canadian contingent, 3,367 were killed, wounded or taken prisoner, an exceptional casualty rate of 68%.**
- **The 1,000 British Commandos lost 247 men.**
- **The Royal Navy lost one destroyer (HMS Berkeley) and 33 landing craft, suffering 550 dead and wounded.**
- **The RAF lost 106 aircraft vs the 48 lost by the Luftwaffe.**
- **The German Army had 591 casualties.**

The Fourth Rotor Problem Solved

With the capture of relevant cipher keys from other sources, and the use of much faster US Navy Bombes, the regular rapid reading of U-boat messages resumed in December 1942.

By the end of 1942, the Brits were reading up to 4,000 Enigma messages a day.

Lorenz

- Early in the war the Germans introduced the Lorenz cipher machines.
- The much simpler and more portable Enigma was used for operational level messages in the German navy, army and air force.
- The Lorenz was used for encrypted high-level messages between the German High Command (OKW) and their army commands throughout occupied Europe.
- Information on the Lorenz machines was not declassified until 2002.

Lorenz

- **The Enigma had three or four rotors, the Lorenz had twelve.**
- **The Lorenz was a teleprinter machine that encrypted/decrypted teletype messages.**
- **British cryptanalysts deduced the Lorenz's logical structure three years before they saw the machine.**

The Heath Robinson

Although the British were able to decrypt intercepted Lorenz messages using a manual method developed by William Tutte, the decoding procedure involved trying so many possibilities that it was impractical to do by hand in the volumes required.

That's where the Heath Robinson comes into the picture.

The Heath Robinson

- **Mathematician Max Newman persuaded his superiors at Bletchley that Tutte's method for breaking Lorenz codes could be mechanized, and he was assigned to develop a suitable machine in December 1942.**
- **Tommy Flowers and Frank Morrell from the telecommunications branch of the General Post Office (GPO) at Dollis Hill worked with Newman and designed the Heath Robinson.**

The Heath Robinson

- **The first prototype was delivered in June 1943. The Wrens nicknamed the machine the "Heath Robinson", after the cartoonist of the same name who drew humorous drawings of absurd mechanical devices.**
- **The Heath Robinson used electro-mechanical switches, and while it was much faster than the manual methods it was still too slow, and so the Colossus was developed.**
- **Despite the success of Colossus, the Heath Robinson approach was still valuable for solving certain problems. The final development of the concept was a machine called Super Robinson that was also designed by Tommy Flowers.**

Colossus

- Colossus was a set of computers developed in the years 1943-1945 to help in the cryptanalysis of the Enigma and Lorenz ciphers.
- Colossus used vacuum tubes instead of electro-mechanical switches to perform its operations.
- Colossus is thus regarded as the world's first programmable, electronic, digital computer.

Colossus

- Colossus was designed by Tommy Flowers to solve the problem posed by Max Newman. Alan Turing's use of probability in cryptanalysis ("Banburismus") contributed to its design.
- It has sometimes been erroneously stated that Turing designed Colossus. Turing's machine was the electromechanical Turing Bombe, not Colossus.

Colossus

- The prototype Colossus Mark 1 was working in December 1943 and was in use at Bletchley Park by early 1944.
- An improved Colossus Mark 2 that used shift registers to quintuple the processing speed, first worked on 1 June 1944, just in time for the Normandy landings on D-Day.

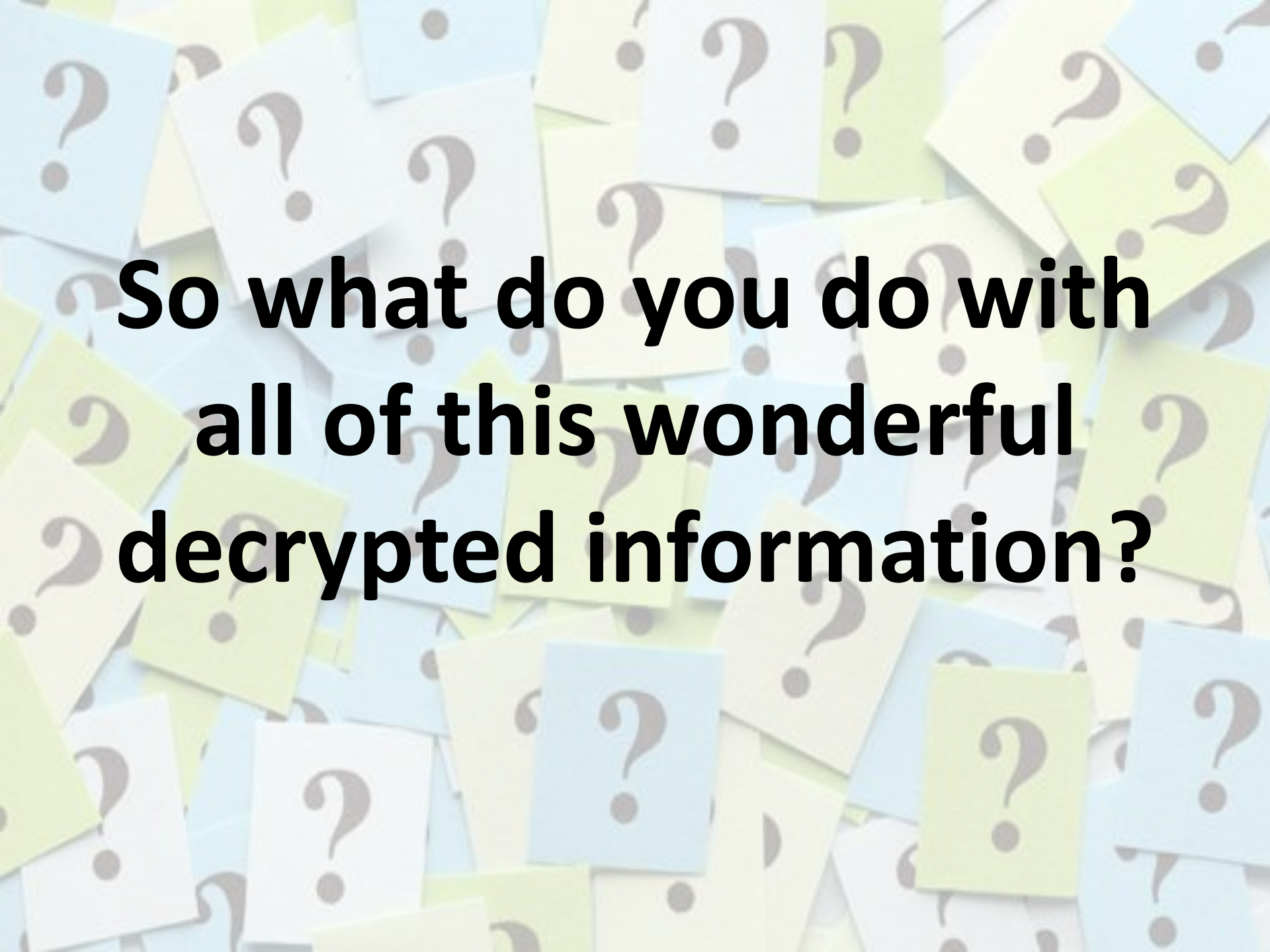
Colossus

Ten Colossi were in use by the end of the war and an eleventh was being commissioned.

Bletchley Park's use of these machines allowed the Allies to obtain a vast amount of high-level military intelligence from intercepted messages between the German High Command and their army commands and military units throughout occupied Europe.

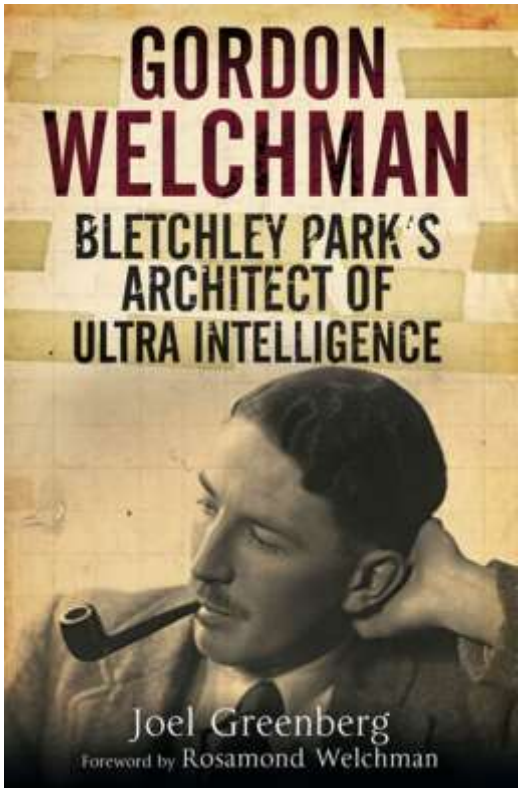
Colossus

- The existence of the Colossus machines was kept secret until the mid-1970's.
- The machines and the plans for building them were destroyed in the 1960s as part of the effort to maintain the secrecy of the project.
- This deprived most of those involved with Colossus of the credit for pioneering electronic digital computing during their lifetimes.
- A functioning rebuild of a Mark 2 Colossus was completed in 2008 by Tony Sale and some volunteers; it is on display at The National Museum of Computing at Bletchley Park.


So what do you do with all of this wonderful decrypted information?

Traffic Analysis

- **Gordon Welchman became head of Hut Six, the section at BP responsible for breaking German Army and Air Force Enigma ciphers.**
- **As well as important contributions to the Turing Bombe and to various decryption techniques, Welchman developed the concept of 'Traffic Analysis' of encrypted German communications.**



Traffic Analysis

- **Traffic Analysis was the collection and analysis of data about which enemy units sent and received messages, including where and when.**
- **Such metadata analysis can reveal a lot about enemy organization, movements, and activities, even when the context of the original message was unknown.**
- **Through Traffic Analysis the British knew where almost every German panzer, submarine, plane, infantry battalion, etc. was located, what officers were stationed where, and what their orders were.**

Traffic Analysis

Nowadays we would enter the information for Traffic Analysis into a computer database.

In WW2 it was all on index cards, with 'hyperlinking' notes on each card linking it to other cards.

Traffic Analysis

It took hundreds of clerks to keep updating existing cards and adding new ones, and huts full of analysts to make sense of the information.

BLETCHLEY PARK AND THE ULTRA SECRET

The ‘ULTRA’ Secret

The British knew the German vulnerabilities could have been remedied by relatively simple improvements in enemy procedures and practices, and such changes would certainly be implemented had Germany had ANY hint of Bletchley's success.

Thus the intelligence Bletchley produced was considered wartime Britain's ‘Ultra Secret’ - higher even than the normally highest classification Most Secret - and security was absolutely paramount.

The ‘ULTRA’ Secret

Any commander in the field receiving Ultra intelligence was fed a cover story crediting a non-Ultra source.

At times sham scouting missions or reconnaissance plane patrols that were intentionally visible to the Germans were dispatched to ‘discover’ German positions that in fact were already known from Ultra.

In some cases it was impossible to act on Ultra intelligence at all because to do so might suggest to the enemy that their communications had been penetrated.

The ‘ULTRA’ Secret

- **The code name Boniface was used as a cover for Ultra. In order to ensure that the successful code-breaking did not become apparent to the Germans, British intelligence created a fictional master spy “Boniface”, who controlled a fictional network of agents throughout Germany.**
- **Information obtained through code-breaking was often attributed to the human intelligence from the Boniface network.**
- **The fictional Boniface radio traffic was transmitted using cypher codes the British knew through Ultra that the Germans had broken.**
- **The Germans were never able to track down any of the Boniface spy network.**

The ‘ULTRA’ Secret

Public information about ULTRA did not even start being declassified until the 1970’s, and even today some information is still secret.

The full ULTRA story is still being pieced together by historians cross-referencing hundreds of thousands of documents, since most of those originally involved are dead or still won’t talk.

The ‘ULTRA’ Secret

The revelation of the Ultra secrets and Enigma in the 1970’s has led to massive rewriting of the history of the war in Europe.

The rewriting is ongoing as additional details still continue to be declassified.

It is conceivable that some of Ultra’s deepest secrets will never be revealed.

The ‘ULTRA’ Secret

Some historians have credited the Ultra information with ending the war one to four years earlier than it would have ended otherwise. However, this ignores two realities:

- **After defeating the Germans in the Battles of Stalingrad and Kursk, the Russians were inexorably pushing the Germans back by the sheer might of overwhelming numbers of troops, tanks and planes, and would have ended up in Berlin in 1945 anyways.**
- **With the first use of the atomic bomb in August 1945 against Japan, it also would inevitably have been used against Germany by the end of 1945 if Germany hadn’t already been defeated or close to defeat.**

A Few Examples of Ultra Successes

- **Winston Churchill wrote that, *"the only thing that ever really frightened me during the war was the U-boat peril"*. In saying this, he correctly identified the critical importance of the threat posed during the war by German submarines to Britain's Atlantic lifeline.**
- **The knowledge gained through Ultra of the whereabout of U-boats and their Wolf Packs enabled many more of them to be sunk than otherwise possible. Ultra also revealed the rendezvous points of the U-boats with their 'milch-cow' supply submarines.**
- **Convoys were routed away from known Wolf Pack locations, and then ships and planes were sent to hunt them down.**
- **648 U-boats were lost, 429 with no survivors. Of these, 215 were lost on their first patrol. Around 30,000 of the 40,000 men to serve in U-boats perished.**

A Few Examples of Ultra Successes

- **Numerous decrypts showed Germany had been completely taken in by Operation Bodyguard, the deception operation to protect Operation Overlord, the D-Day invasion. They revealed the Germans did not anticipate the Normandy landings and even after D-Day still believed Normandy was only a feint, with the main invasion still to be in the Pas de Calais.**
- **One of the very first decrypts from the Mark 2 Colossus was handed to Eisenhower on 5 June, confirming that Hitler wanted no additional troops moved to Normandy because he was convinced that the target was the Pas de Calais and any preparations for Normandy were a diversion. After reading it, Eisenhower announced to his staff *"We go tomorrow"*.**
- **Even after the start of the invasion, Hitler was so convinced that it was a diversion that he delayed sending reinforcements from the Pas de Calais region for nearly seven weeks.**
- **Another decrypt revealed that one of the sites chosen as the drop site for a US parachute division was the base for a German tank division and the site was changed at the last minute.**

A Bit of Associated Historical Trivia

- The irony is that Hitler was initially convinced the landings would take place in Normandy and wanted the Normandy beaches reinforced as early as 1942.
- It was military intelligence who convinced him the landings would most likely take place in the Pas de Calais and that that part of the Atlantic Wall should be reinforced first.
- They made such a convincing case for the Pas de Calais that even after the landings Hitler remained convinced Normandy was a diversion.

A Few Examples of Ultra Successes

- During the campaigns in North Africa, Ultra kept British General Bernard Montgomery informed of German General Erwin Rommel's (the Desert Fox) order of battle and, in some cases, of his actual plans.
- It also enabled the British to know when supply ships would sail from Italy and to sink them, thus eventually starving Rommel of vital fuel and supplies.
- Rommel lost the battle for North Africa.

A Few Examples of Ultra Successes

- Initial Allied air raids on Germany concentrated on airplane and other munitions production facilities, with very limited success. Ultra decrypts of German reports of the damage caused by the raids and their impact revealed that the damage was minimal and the Germans were quickly back in production. However, they also realized that Germany's BIG vulnerability was its fuel and oil production. For most of the rest of the war Germany's oil production became a major target.
- Fuel shortages soon prevented the Germans from training a new generation of pilots to replace those who were lost in the air battles. By summer 1944 German fuel production was down over 50%, severely limiting military operations.
- Whenever Ultra decrypts revealed Germany getting any facility back on line, the bombers returned.

A Few Examples of Ultra Successes

This incident should serve to underline the high price of German carelessness where security discipline was concerned.

- **After sinking the British battle cruiser HMS Hood, the German battleship Bismarck managed to slip away from shadowing British cruisers.**
- **The pursuing British admiral finally figured that the German battleship might be making for safe harbour in Brest. Within an hour, he had confirmation of that hunch through a Luftwaffe, not Kriegsmarine, intercept.**
- **Luftwaffe authorities had radioed their chief of staff, then visiting Athens during the German invasion of Crete, that Bismarck was heading for Brest.**
- **The Bismarck was found, intercepted and sunk.**

Having great information on the enemy is of no value if you don't understand it and take the appropriate action.

Ultra Failures

- **Operation Market Garden was a massive failed operation fought in the Netherlands in September 1944. The objective was to create a 64 mile bulge into German territory and capture a bridgehead over the River Rhine, creating an Allied invasion route into northern Germany. Despite some successes, it failed to secure the sought for bridgehead.**
- **Ultra intelligence indicated that at the very time when the operation was moving forward, some of Germany's best panzer divisions would be refitting in the town selected as the operation's final objective on the Rhine, Arnhem.**
- **Putting this information together with intelligence from the Dutch underground that the SS panzer units were refitting in the neighborhood of Arnhem, Allied commanders should have recognized that Operation Market-Garden had little prospect of success.**
- **Unfortunately, officers at the highest level at Field Marshal Montgomery's headquarters who had access to all this information failed to draw the correct conclusions and proceeded with the operation as planned.**
- **Operation Market Garden was immortalized in the movie *"A Bridge Too Far"*.**

Ultra Failures

- In late 1944 the Germans were massing large amounts of men, tanks and other material north of the Ardennes for a final major offensive that would come to be known as the Battle of the Bulge.
- Although the Germans suspected their security had been compromised and undertook a series of unprecedented measures to hide the attack, there were still many indications in the Ultra decrypts of what the Germans were up to. Since it was known through Ultra that the Germans were desperately low on such materiel, the allocations of that many resources could only portend major operations to come in the Ardennes. Lack of effective Allied aerial reconnaissance due to bad weather limited the ability to confirm the information.
- The Allied high command, especially General Omar Bradley at the front, dismissed the info in the belief the war was almost over and the Germans could not possibly launch a major offensive.
- The Germans achieved a total surprise attack on the morning of 16 December 1944. Bradley's American forces bore the brunt of the attack and the US incurred their highest casualties of any operation during the war. The Germans made major progress before finally being stopped by a combination of good weather that allowed Allied air support operations, and thrusts by Montgomery from the north-west and Patton from the south-east.

More Connections

- After the war, my father took advantage of the veterans training programs to get a degree in Electrical Engineering.
- In the mid-1950's he joined a then small company known as IBM.
- He was a database project manager before he retired.
- During Y2K I moved from Hi Tech manufacturing to become a Senior IT Project Manager specializing in database application development.

More Connections

- I didn't have any interest in computers when I was younger, but I finally developed an interest in computers when I was at Mitel and got to use a MacIntosh Classic and an IBM PC-XT.
- When I finally decided to get my own computer I was helped out by my brother-in law and friend Chris Taylor, who's now President and System Admin of OPCUG.
- Chris got me to join the group, and a while later got me to join the Board of Directors.
- And so here I am now doing this presentation on 'Computers At War' for OPCUG's Remembrance Day meeting.

Let’s look at some of the people of Bletchley Park

Alan Turing

- **Alan Turing, OBE , FRS (1912 – 1954) was a British pioneering computer scientist, mathematician, logician, cryptanalyst, philosopher, mathematical biologist, and marathon and ultra distance runner.**
- **He was highly influential in the development of the emerging field of computer science, providing a formalization of the concepts of "algorithm" and "computation" with the Turing Machine, which can be considered a model of a general purpose computer.**
- **Turing is widely considered to be the father of theoretical computer science and of artificial intelligence.**

The Turing Machine

A Turing machine is a hypothetical device that manipulates symbols according to a table of rules. A Turing machine can be adapted to simulate the logic of any computer algorithm.

In essence, it can do anything that's computable.

Turing Complete

‘Turing Complete’ is a term used in computability theory to describe an abstract machine. The machine is considered Turing Complete if it can be used to emulate a Turing Machine.

Most modern programming languages are Turing Complete.

The Turing Test

- **In 1950 Turing published a paper that addressed the problem of artificial intelligence, and proposed an experiment which became known as the Turing Test, in an attempt to define a standard for a machine to be called "intelligent".**
- **The idea was that a computer could be said to "think" if a human interrogator could not tell it apart, through conversation, from a human being.**
- **Turing suggested that rather than building a program to simulate the adult mind, it would be better rather to produce a simpler one to simulate a child's mind and then to subject it to a course of education, which is essentially how some modern artificial intelligence works*.**

*** - I covered Artificial Intelligence and the concept of teaching the computer in more detail in my December 2017 presentation *"Where Are Self-Flying Planes and Self-Driving Cars Taking Us"*.**

“Lady Lovelace's Objection”

Ada Lovelace (1815 – 1852) is credited as being the world's first computer programmer. She stated that computers are incapable of originality. This is largely because, according to her, machines are incapable of independent learning.

"The Analytical Engine has no pretensions whatever to originate anything. It can do whatever we know how to order it to perform. It can follow analysis; but it has no power of anticipating any analytical relations or truths.“

Turing suggests that Lovelace's objection can be reduced to the assertion that computers "can never take us by surprise" and argues that, to the contrary, computers could still surprise humans, in particular where the consequences of different facts are not immediately recognizable. Turing also argues that Lady Lovelace was hampered by the context from which she wrote, and if exposed to more contemporary scientific knowledge, it would become evident that the brain's storage is quite similar to that of a computer.

Alan Turing

- **Turing was prosecuted in 1952 for homosexual acts when such behaviour was still criminalized in the UK.**
- **He accepted treatment with oestrogen injections (chemical castration) as an alternative to prison.**
- **Turing died in 1954, 16 days before his 42nd birthday, from cyanide poisoning. There is still controversy as to whether it was accident or suicide.**

Alan Turing

In 2009 British Prime Minister Gordon Brown made an official public apology on behalf of the British government for *"the appalling way he was treated"*.

Queen Elizabeth II granted him a posthumous pardon in 2013.

The Imitation Game

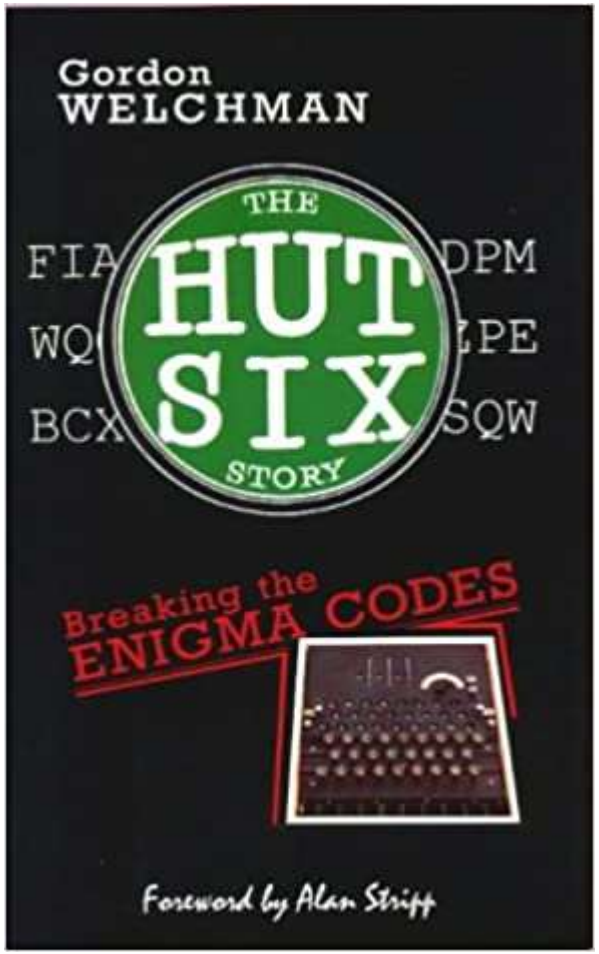
- "***The Imitation Game***" is a 2014 historical drama film based on the 1983 biography "***Alan Turing: The Enigma***" by Andrew Hodges. The title of the film quotes the name of the game Alan Turing proposed for answering the question "***Can machines think?***", in his 1950 seminal paper "***Computing Machinery and Intelligence***".
- The film has a great many historical inaccuracies.

Gordon Welchman

- **Welchman was one of the four early recruits to Bletchley Park who became known as the "wicked uncles”. Their letter to Churchill resulted in more resources and major changes at Bletchley.**
- **Much of Welchman's work at Bletchley was in "traffic analysis" of encrypted German communications. However, his main contributions were to the process of breaking the German Enigma machine cipher, including his invention of the ‘Diagonal Board’.**
- **Welchman became head of Hut Six, the section at BP responsible for breaking German Army and Air Force Enigma ciphers.**

Gordon Welchman

- **After the end of the war Welchman stayed in the intelligence technology field.**
- **In 1951 he taught the first computer programming course at the Massachusetts Institute of Technology.**
- **His book *"The Hut Six Story"* was published in 1982. The book was not banned, but as a result of it, Welchman lost his security clearance and therefore his livelihood, and was forbidden to discuss either the book or his wartime work.**
- **The impact on Welchman of the withdrawal of his security clearance was devastating. He died in 1985.**



Tommy Flowers

Tommy Flowers (BSc, DSc, MBE, 1905 - 1998) worked for the telecommunications branch of the General Post Office (GPO) at Dollis Hill From 1935 onward, he explored the use of electronics for telephone exchanges. This background in switching electronics would prove crucial for his computer designs.

Flowers was put in touch with Alan Turing at Bletchley in February 1941. Turing wanted Flowers to build a decoder for the relay-based Turing Bombe. The decoder project was abandoned but Turing was impressed with Flowers's work, and in February 1943 introduced him to Max Newman who was leading the effort to automate part of the cryptanalysis of the Lorenz cipher. The decoding procedure involved trying so many possibilities that it was impractical to do by hand.

Tommy Flowers

- **Flowers and Frank Morrell (also from the GPO) designed the Heath Robinson to automate the cryptanalysis of the Lorenz. The Heath Robinson used electro-mechanical switches. Flowers proposed a more sophisticated alternative, using an electronic system with vacuum tubes.**
- **Flowers's team at Dollis Hill built the first machine in eleven months. It was immediately dubbed 'Colossus' by the Bletchley Park staff for its immense proportions. The Mark 1 Colossus operated five times faster and was more flexible than the Heath Robinson. The first Mark 1, with 1500 vacuum tubes, first ran in November 1943 and was delivered to Bletchley Park in January 1944. began operation in early February.**
- **Colossus proved to be efficient and quick against the twelve-rotor Lorenz cipher machine.**

Tommy Flowers

- **Flowers then designed the Colossus Mark 2 which used 2,400 vacuum tubes. The first Mark 2 went into service at Bletchley Park on 1 June 1944, and immediately produced vital information for the imminent D-Day landings.**
- **Despite the success of Colossus, the Heath Robinson approach was still valuable for solving certain problems. The final development of the concept was a machine called Super Robinson that was designed by Tommy Flowers. This one could run four tapes and was used for running depths and "cribs" or known-plaintext attack runs.**

Tommy Flowers

- **After the war, Flowers received little recognition for his contribution. He applied for a loan from the Bank of England to build another machine like Colossus but was denied the loan because the bank did not believe that such a machine could work. He could not argue that he had already designed and built many of these machines because his work on Colossus was covered by the Official Secrets Act.**
- **It was not until the 1970s that Flowers' work in computing was fully acknowledged. His family had known only that he had done some 'secret and important' work.**
- **He remained at the Post Office Research Station where he was Head of the Switching Division. He and his group pioneered work on all-electronic telephone exchanges.**
- **He was also involved in the development of ERNIE, a hardware random number generator used to generate the winning numbers in British government lotteries starting in 1957.**
- **In 1964, he became head of the advanced development at Standard Telephones and Cables Ltd., where he continued to develop electronic telephone switching including a pulse amplitude modulation exchange, retiring in 1969.**

Max Newman

- **Mathematician Max Newman (FRS, 1897 - 1984) arrived at Bletchley Park in August 1942 and joined the group working on the "Tunny" Lorenz ciphers.**
- **He persuaded his superiors at Bletchley that Tutte's method for breaking Lorenz codes could be mechanised, and he was assigned to develop a suitable machine in December 1942.**
- **Newman's new section, termed the "Newmanry", was housed initially in Hut 11, and initially staffed by himself, Donald Michie, two engineers, and 16 Wrens (Womens Royal Naval Service).**

Max Newman

- **The first prototype was delivered in June 1943. The Wrens nicknamed the machine the "Heath Robinson", after the cartoonist of the same name who drew humorous drawings of absurd mechanical devices.**
- **The Heath Robinson used electro-mechanical switches and while being much faster than the previous methods was still too slow, and so the Colossus was developed.**
- **Despite the success of Colossus, the Heath Robinson approach was still valuable for solving certain problems. The final development of the concept was a machine called Super Robinson that was designed by Tommy Flowers. This one could run four tapes and was used for running depths and "cribs" or known-plaintext attack runs.**

There are a great many more people at Bletchley Park and other locations in Britain and the United States that made very significant contributions to the success of ‘Ultra’ and the American ‘Magic’. Most of them received little or no recognition for their work until decades after the war ended, and very many of them are still unknown.

The End, Sort Of

Due to time limitations I'm going to end tonight's presentation here, but there is a lot of other info to go and the presentation deck will be available on the OPCUG website.

Still To Go

- Arlington Hall, America's version of Bletchley Park
- The 55 ton SIGSALY telephone scrambler that allowed secure conversations between Churchill, Roosevelt, Eisenhauer and other top war leaders.
- The American SIGABA, described as "Enigma on steroids", whose codes were never broken during its service lifetime.
- The story of how American codebreaking allowed the major victory over the Japanese at the pivotal Battle of Midway.
- How breaking of the Japanese 'Purple' diplomatic code revealed crucial information about Germany.
- How breaking the Japanese JN25 military code led to the death of Japanese Admiral Isoroku Yamamoto, the architect of the attacks on Pearl Harbor and Midway, and considered the most important military commander the Japanese had.
- A look at the mechanical and electro-mechanical computers used for torpedo aiming systems, shipboard gun fire-control systems, artillery ballistics table calculation and bombsights.
- The pre-war electromechanical analog computer designed by MIT engineering professor Vannevar Bush that would be used during the war for churning out artillery firing tables, and in training and inspiring the next generation of computer pioneers.
- The story of Grace Hopper, the American computer scientist and US Navy rear admiral who invented the first compiler for computer programming languages and who led in the development of COBOL, one of the first high-level machine independent programming languages.

Arlington Hall

The United States had their own version of Bletchley Park at Arlington Hall.

Arlington Hall concentrated its efforts on the Japanese systems (including PURPLE) while Bletchley Park concentrated on European combatants.

The American version of the ULTRA secret was called MAGIC.

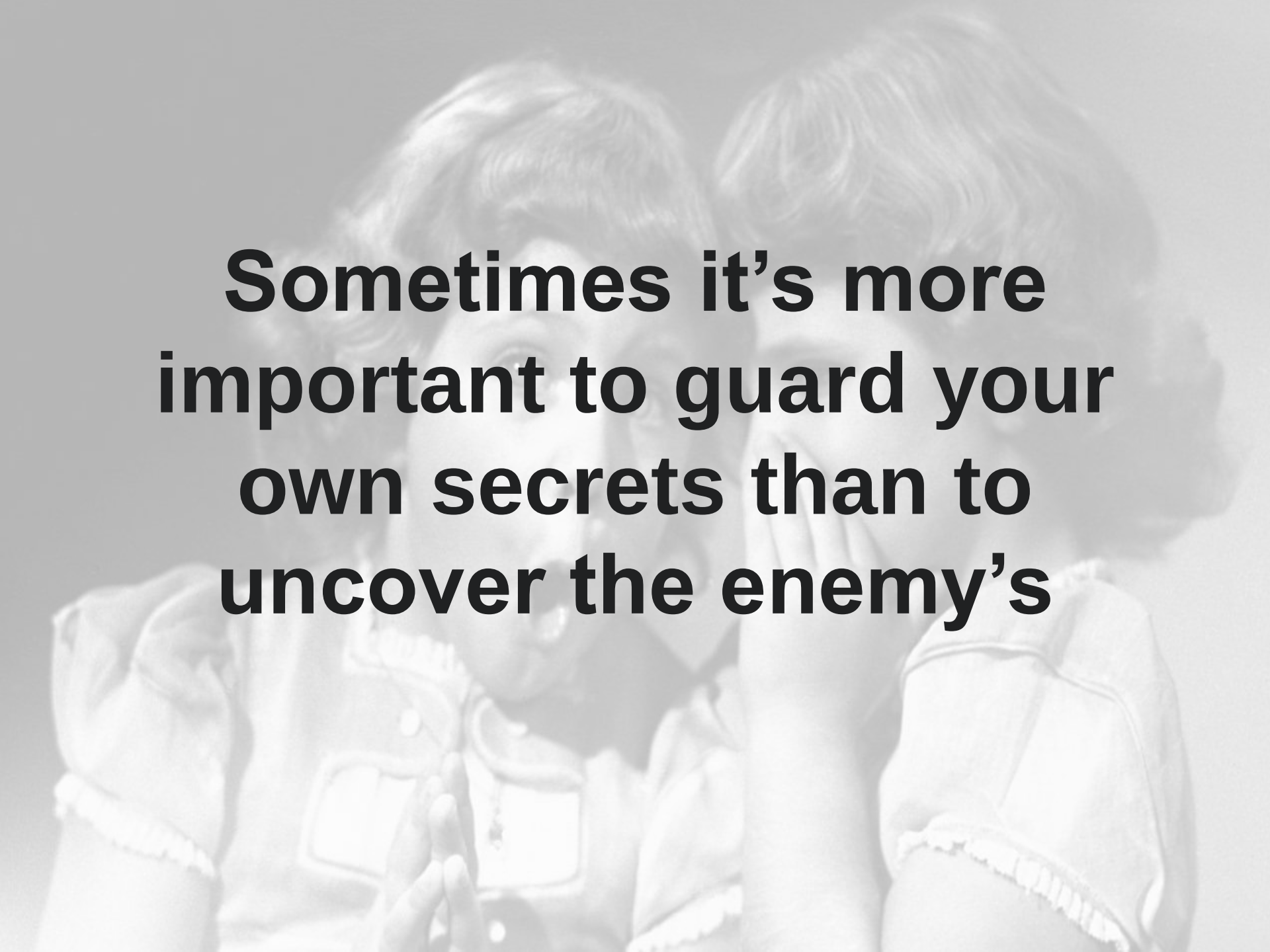
War Mobilizes Science

- 1941 - Konrad Zuse completed the 'Z3', the world's first operational programmable computer. The Germans never appreciated the value of computers and when the Z3 was destroyed in 1943 during an Allied bombardment of Berlin, it was not rebuilt. After the war Zuse continued to be a pioneer in the development of computers.

- 1944 - The IBM Automatic Sequence Controlled Calculator was turned over to Harvard University, which called it the Harvard Mark I. It was designed by Howard Aiken and his team, financed and built by IBM. It became the second program controlled machine (after Konrad Zuse's). Used to create ballistics tables for the US Navy.

War Mobilizes Science

- Other computers started development during the war but weren't ready for use until after the war ended.
- Post-war computer development really got rolling with:
  - The invention of the transistor in 1947.
  - The development of compilers for computer programming languages.
  - The development of machine-independent programming languages.
  - The development of practical business applications.



Sometimes it's more important to guard your own secrets than to uncover the enemy's

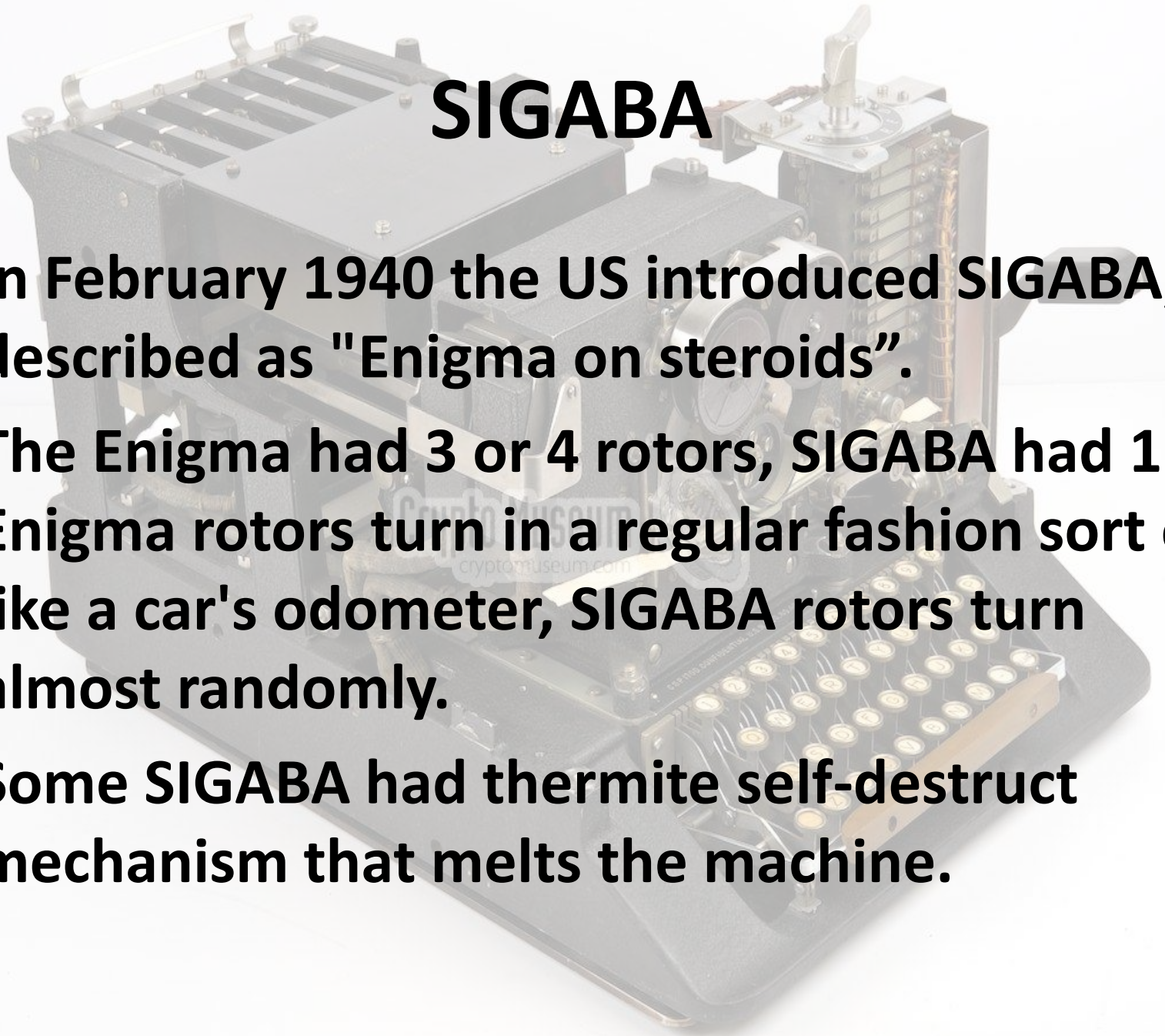
SIGSALY

- Although telephone scramblers were used by both sides in World War II, they were not very secure, and both sides often cracked the scrambled conversations of the other, so the Americans developed SIGSALY.
- SIGSALY was a secure speech system used in World War II for the highest-level Allied communications such as conversations between Roosevelt and Churchill.
- Eisenhauer took one with him to France. The machine weighed 55 tons, so it couldn't be used in transit but was set up whenever he set up a new headquarters.

SIGSALY

- SIGSALY was the first transmission of digitized speech.
- The voice was split into 12 separate channels, 10 for the speech and two to control tone. Each channel encrypted 50 times a second by random tones.
- SIGSALY converted analog voices into digital signals and scrambled them by adding tones from a 78 RPM record. An identical device on the other end descrambled the message by removing the tone using an identical record synchronized to within a fiftieth of a second.
- About 30 patents that weren't declassified until 1976. The 78 RPM records are the only remaining artifacts left.

SIGABA

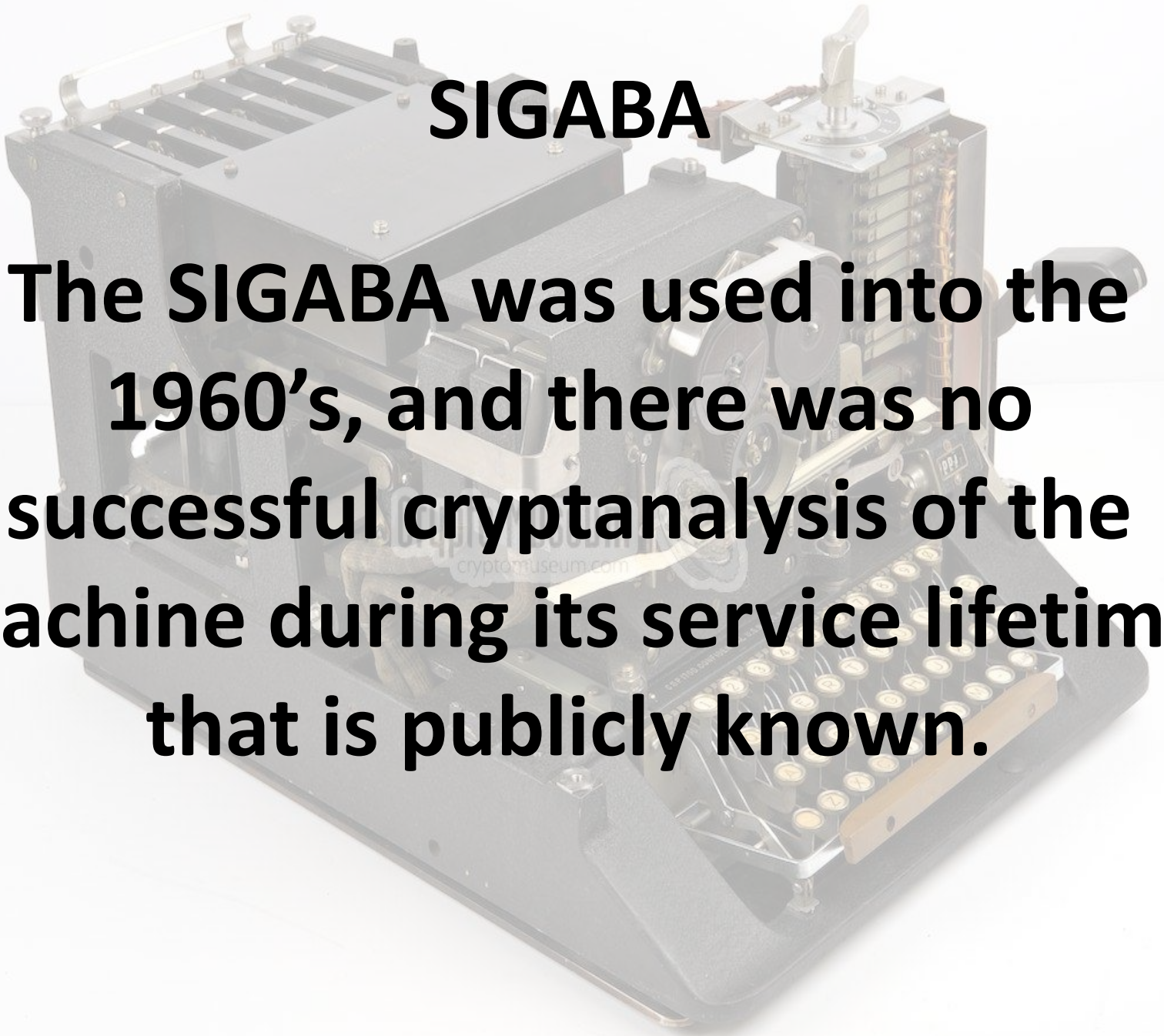


- In February 1940 the US introduced SIGABA, described as "Enigma on steroids”.
- The Enigma had 3 or 4 rotors, SIGABA had 15, Enigma rotors turn in a regular fashion sort of like a car's odometer, SIGABA rotors turn almost randomly.
- Some SIGABA had thermite self-destruct mechanism that melts the machine.

SIGABA

- SIGABA systems were closely guarded at all times, with separate safes for the system base and the code-wheel assembly, but there was one incident where a unit was lost for a time.
- On February 3, 1945, a truck carrying a SIGABA system in three safes was stolen while its guards were visiting a brothel in recently-liberated Colmar, France.
- General Eisenhower ordered an extensive search, which finally discovered the safes six weeks later in a nearby river.

SIGABA



The SIGABA was used into the 1960's, and there was no successful cryptanalysis of the machine during its service lifetime that is publicly known.

In the Pacific

- The Imperial Japanese Navy code was called JN-25 by the Americans. By early 1942 considerable progress had been made in decrypting these messages.
- US cryptanalysts under Commander Joseph Rochefort decrypted Japanese plans to attack Midway Island.
- As a result, the Americans had a good picture of where, when, and in what strength the Japanese would appear, and so the Americans were in the right place at the right time with the right stuff to deal the Japanese a serious defeat by sinking four of their aircraft carriers.

Japan, Purple, JN25 and Magic

- The Japanese cipher machine dubbed "Purple" by the Americans, was used for highest-level Japanese diplomatic traffic. It was cracked by the US Army's Signal Intelligence Service and disseminated under the codeword MAGIC.
- Some Purple decrypts also proved useful against Germany. Detailed reports by Japan's ambassador to Germany included:
  - Reviews of Germany's assessments of the military situation
  - Reviews of strategy and intentions,
  - Reports on direct inspections (in one case, of Normandy beach defenses) by the ambassador, and
  - Reports of long interviews with Hitler.

Japan, Purple, JN25 and Magic

- Japanese Admiral Isoroku Yamamoto planned the attacks on Pearl Harbor and Midway, and was considered the most important military commander the Japanese had.
- He was killed when American code breakers identified his flight plans, enabling American fighters to intercept and shoot down his plane in April 1943.
- His death was a major blow to Japanese military morale during World War II.

War Mobilizes Science

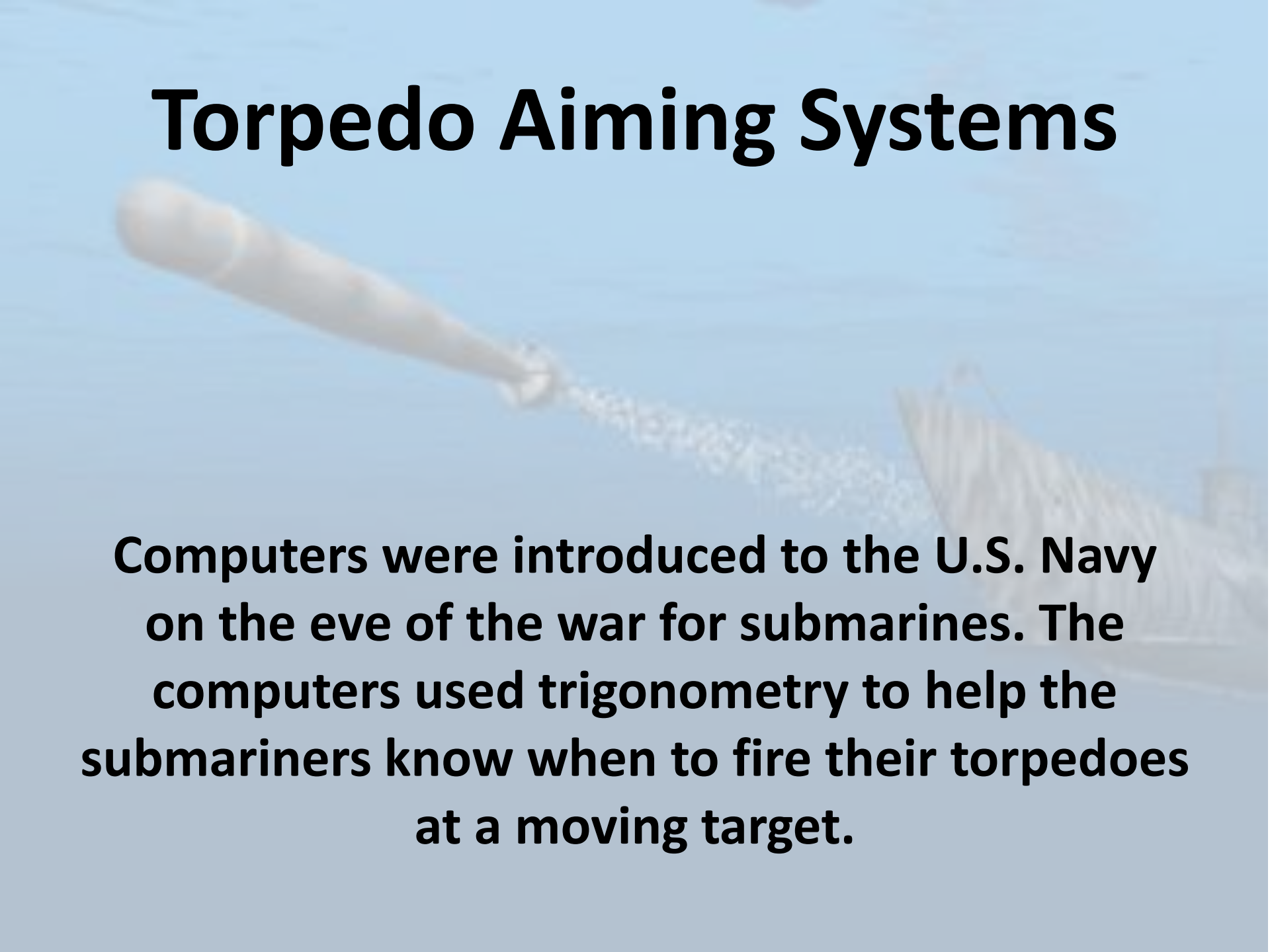
As well as code breaking, practical applications for computers during WWII also included:

- torpedo aiming systems
- shipboard gun fire-control systems
- artillery ballistics table calculation
- bombsights

War Mobilizes Science

Most of these computers were mechanical or electro-mechanical, and most were analog as opposed to digital.

Torpedo Aiming Systems



Computers were introduced to the U.S. Navy on the eve of the war for submarines. The computers used trigonometry to help the submariners know when to fire their torpedoes at a moving target.

Shipboard Gun Fire-control Systems

- The American Mark 1 fire control system electronically linked gun mounts to the electronic gun director (mounted high on the ship) and to the watertight armored plotting room deep in a ship's superstructure.
- The analog computer in the plotting room weighed 3,000 pounds.
- It took into account the muzzle velocity, the type of projectile and its weight, wind, distance, roll and pitch of the ship, the magnus effect (the projectile's spin), parallax (the different locations of the ship's guns) and other factors.
- The information was electronically transmitted to the gunners and could produce continuous fire control solutions during combat.
- The Mark 1's and 1A's remained in service until 1969, when digital fire control solutions replaced it.

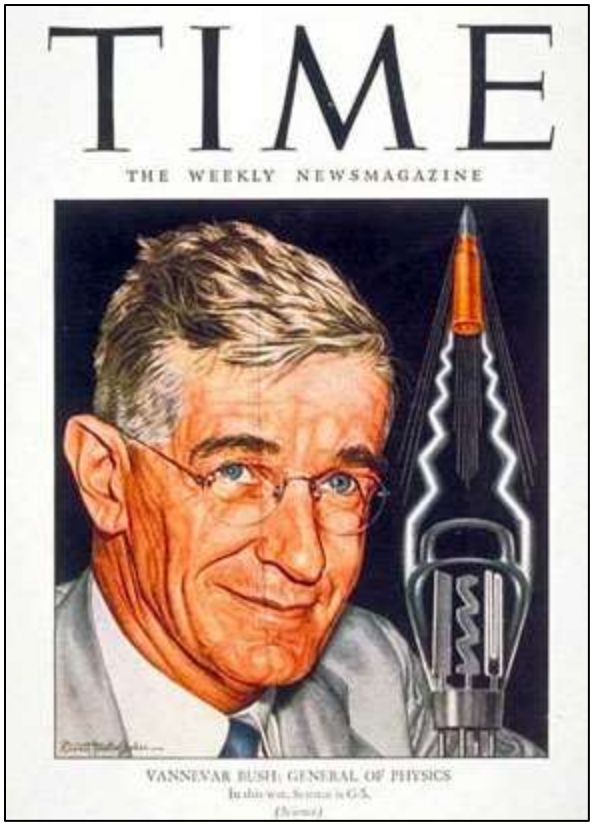
Shipboard Gun Fire-control Systems

British, German and Japanese ships had their own fire control systems, although not as sophisticated as the American Mark 1.

Bombsites

- A bombsight is a device used by military aircraft to drop their bombs accurately. The bombs are affected by forces including gravity, air drag, air density and wind. Accuracy is also affected by how close to flat and level the aircraft is flying. The danger to the bombers from ground-based defences is reduced by bombing from a high altitude, but this also reduces the accuracy of the bombing. That has led to a series of increasingly sophisticated bombsight designs, dedicated to high-altitude level bombing.
- In the 1930s, mechanical computers with the performance needed to "solve" the equations of motion started to be incorporated into the new gyroscopic bombsights, the most famous of which is the Norden. Although bombsights like the American Norden, British SABS and German Lotfernrohr 7 performed well in testing, their accuracy in combat conditions was disappointing, with most of the bombs hitting outside a 5 mile radius of the target.
- Later in the war radar bombsights were developed which allowed targeted bombing at night, but the accuracy was still disappointing. Radio guided bombing was used as well ("the battle of the beams") with slightly better results.

Vannevar Bush

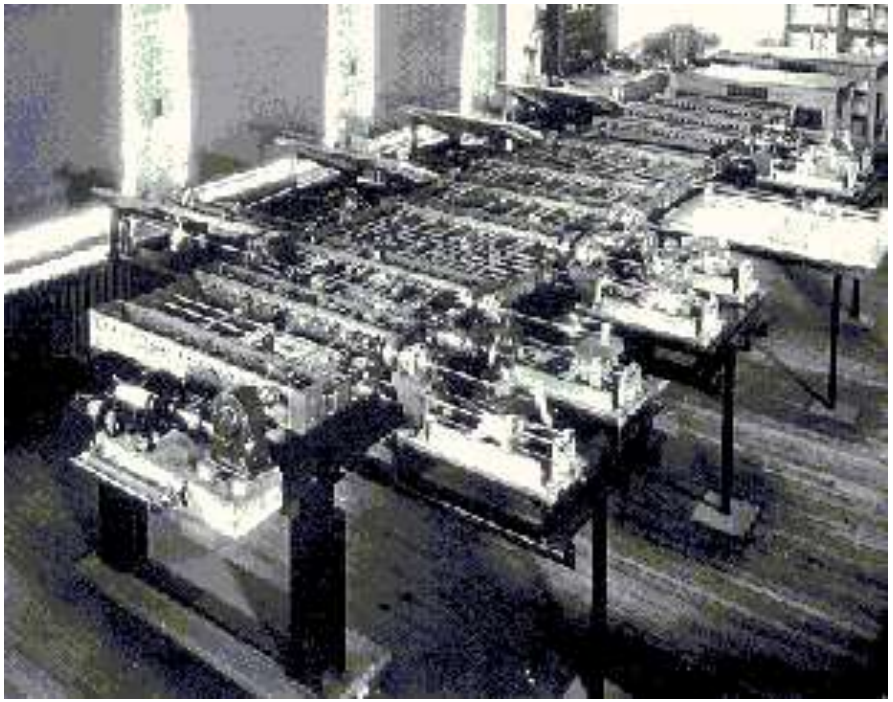


In 1931 MIT engineering professor Vannevar Bush was able to build the world's first analog electrical-mechanical computer. He dubbed his machine a **'Differential Analyzer'**.

Vannevar Bush

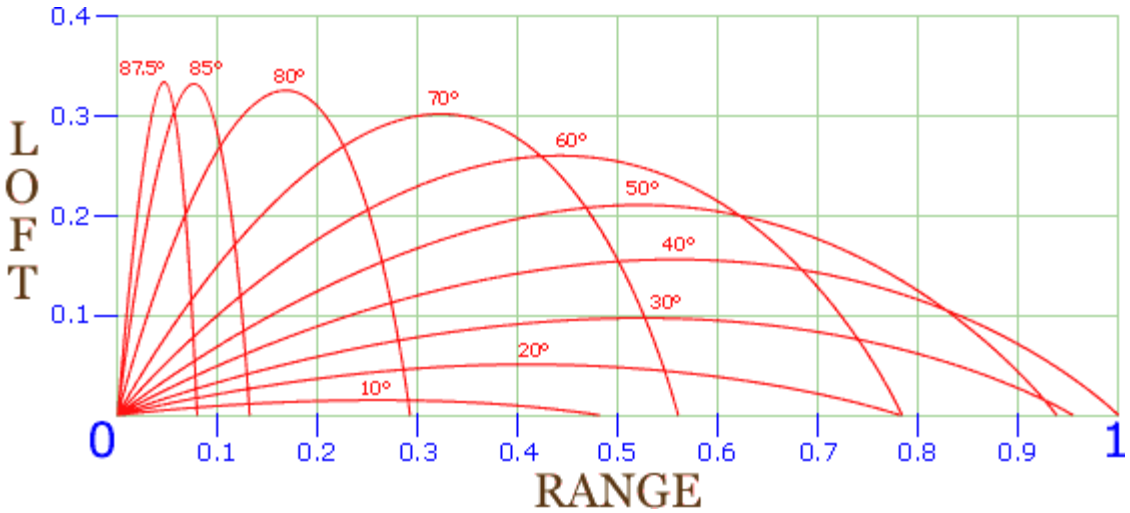
It consisted of six wheel-and-disk integrators connected by an array of gears, pulleys, and shafts rotated by electric motors.

It helped that Bush was at MIT; there were a lot of people around who could assemble and calibrate complex contraptions.



Vannevar Bush

It proved particularly useful in churning out artillery firing tables— and in training and inspiring the next generation of computer pioneers.



Vannevar Bush's Differential Analyzer was the last major Analog Computer.

An analog computer does not use discrete values (e.g. '0's and '1's) but rather continuous values (e.g. a sound wave, an artillery trajectory). The processes cannot be reliably repeated with exact equivalence, as they can with digital computers.

Analog computers can have a very wide range of complexity. Slide rules and nomographs are the simplest, while naval gunfire control computers and large hybrid digital/analog computers were among the most complicated.

The advent of digital computing made analog computers largely obsolete in 1950s and 1960s, though they remain in use in some specific applications, like the flight computer in aircraft.

Vannevar Bush

- **An offshoot of Vannevar Bush's work on the Differential Analyzer was some of the original work on digital circuit design theory.**
- **Bush invented the Memex, an adjustable microfilm viewer with a hyperlink structure analogous to that of the World Wide Web.**
- **Bush became Vice President of MIT and Dean of the MIT School of Engineering in 1932, and president of the Carnegie Institution of Washington in 1938.**
- **Bush was as head of the U.S. Office of Scientific Research and Development (OSRD) during World War II, through which almost all wartime military R&D was carried out, including initiation and early administration of the Manhattan Project.**
- **He founded Raytheon Corporation.**

Grace Hopper

Grace Hopper (1906 - 1992) was an American computer scientist and United States Navy rear admiral

She was one of the first programmers of the Harvard Mark I computer, and invented the first compiler for a computer programming language.

She popularized the idea of machine-independent programming languages, which led to the development of COBOL, one of the first high-level programming languages.

She is credited with popularizing the term "debugging" for fixing computer glitches (inspired by an actual moth removed from the computer).

(So Far)