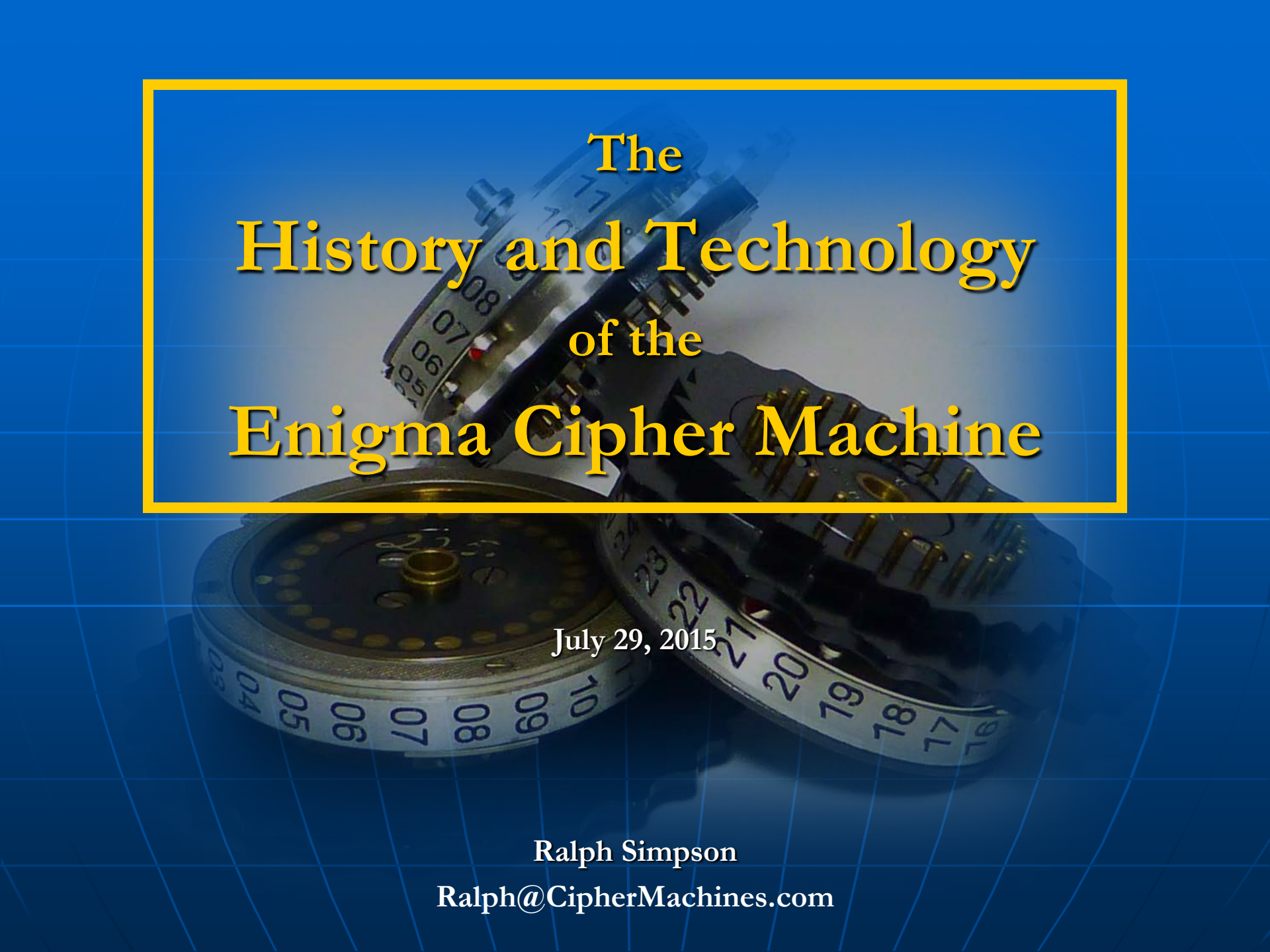


The History and Technology of the Enigma Cipher Machine

July 29, 2015

Ralph Simpson
Ralph@CipherMachines.com

Agenda

- Early history of rotor machines
- Controversy of Enigma invention
- Enigma technology
- Key length of the Enigma
- Shortcomings of the Enigma
- Significance of Enigma in WW2
- Breaking the code
- Beginning of modern computing

WW1 - Radio made most ciphers obsolete

- Proliferation of radios in WW1 highlighted the need for a new cipher technology
- Many ciphers had shortcomings when 100's of messages are captured using the same key
- Cipher technology was manual and error-prone

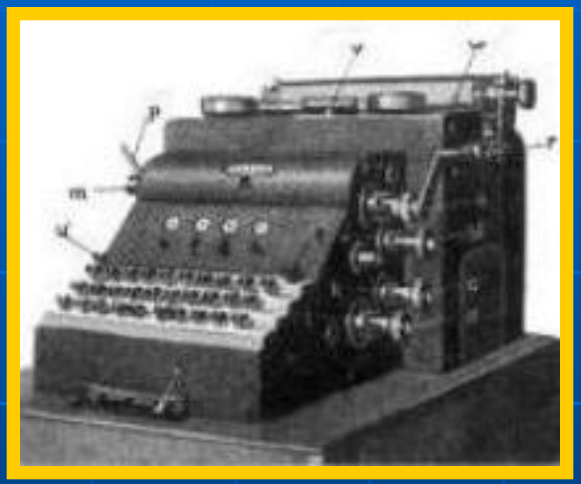
Confederate
Vigenère Wheel

US Army
M-94 Cipher Wheel

Invention of Rotor-Based Cipher Machines

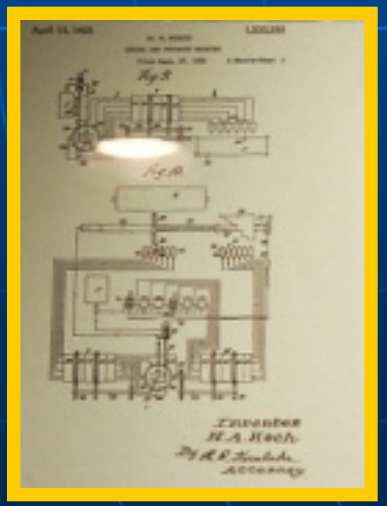
- Enigma was one of four cipher machines with electro-mechanical rotors invented in 4 different countries between 1917-1919

Edward Hebern USA 1917



Arthur Scherbius Germany 1918

Hugo Koch Holland 1919



Arvid Damm Sweden 1919

Enigma Invention

Arthur Scherbius
Germany

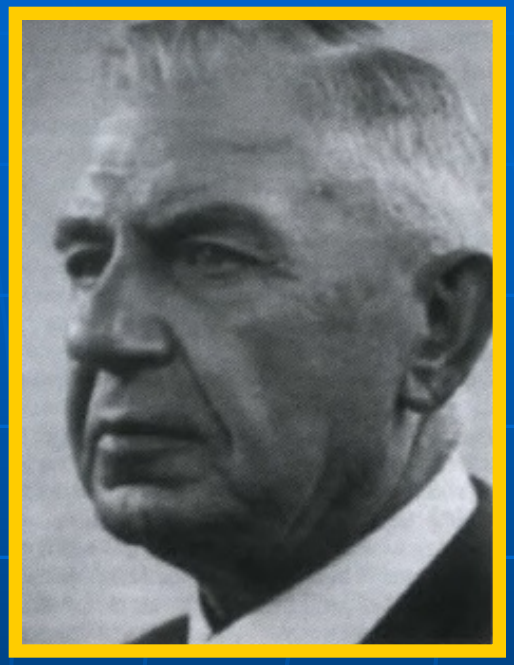
Hugo Koch
Holland

- German Navy bought Enigma in 1926, Army in 1928
- In 1927, Enigma inventor Scherbius curiously bought the rights to Koch's patent, paid 600 Dutch guilders (~$350)
- Scherbius had the earlier and almost identical patent
- Koch died in 1928
- Scherbius died in 1929 in a horse carriage accident, not knowing the role his invention would have in history

History Rewritten in 2003

Theo van Hengel

- 2003 discovery: electro-mechanical rotor cipher was invented in 1915 by 2 Dutch naval officers
- Dutch Navy suppressed this patent until Nov. 1919, weeks after Koch's patent was granted



RPC Spengler

- The patent attorney for the 2 Dutch naval officers was the brother-in-law of Hugo Koch!
- Koch collaborated with Scherbius, and their patent drawings were identical to the Dutch naval officer's
- Now it is recognized that van Hengel and Spengler were the true inventors of the Enigma machine

Enigma Technology

- Typewriter style cipher machine was a major advance in ease of use and cryptologic strength
- Innovation was the electro-mechanical rotors to encipher / decipher messages
- Pressing a key causes the rotors to turn, giving a new cipher algorithm for each letter in a message
- Electric pathway goes from keyboard→ plugboard→ rotors→ reflector→ rotors→ plugboard, then it lights up a bulb
- There is no printing capability, so the message must be written down

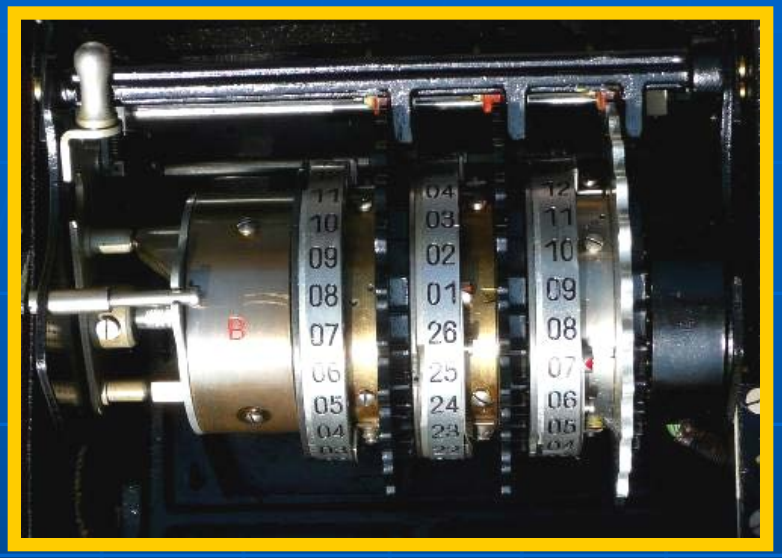
Keyboard

- QWERTZ keyboard with only 26 letters - no numbers, space bar, etc.
- Pressing key first rotates 1 to 3 rotors then lights up a bulb
- Each letter is encrypted 7 to 9 times, the key changes for each letter
- Note the serial # plate below the “V”

Plugboard

- German military added the plugboard to commercial Enigma in 1930, greatly increasing cryptologic strength
- In WW2, Germans always used 10 cables, switching 20 of 26 letters instead of varying # of cables from 0-13
- Reduced key length by a factor of 4, but simplified operations

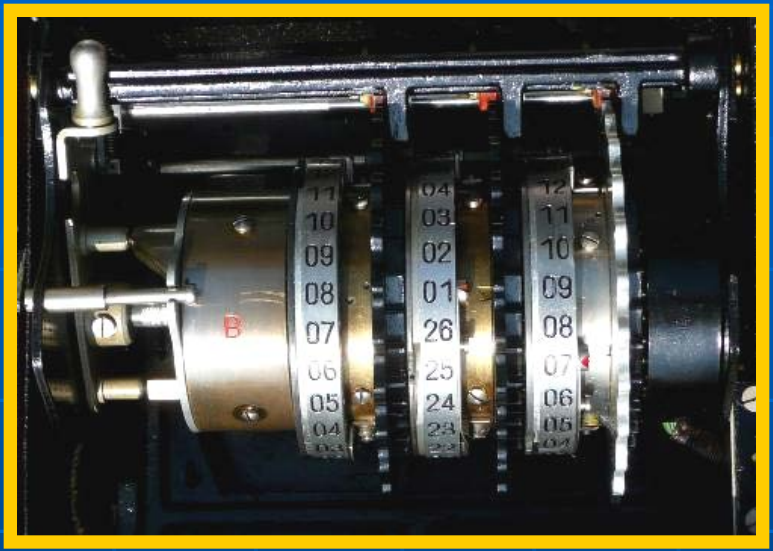
Rotors



Notch by "04" causes the rotor to its left to turn

- 3 rotors out of 5 available are changed daily, giving 5 X 4 X 3 = 60 possible positions for the 3 rotors
- Each rotor is set to a beginning alphabetic character, giving 26^3 = 17,576 possible settings
- Notch on each rotor sets turnover point for the rotor to its left, giving 26^2 = 676 possibilities (notch on leftmost rotor has no effect)
- Later in WW2, the German Navy developed a 4 rotor Enigma and added 3 new rotors to the 5 available

Reflector



Reflector is *to the left of the rotors (with red "B")*

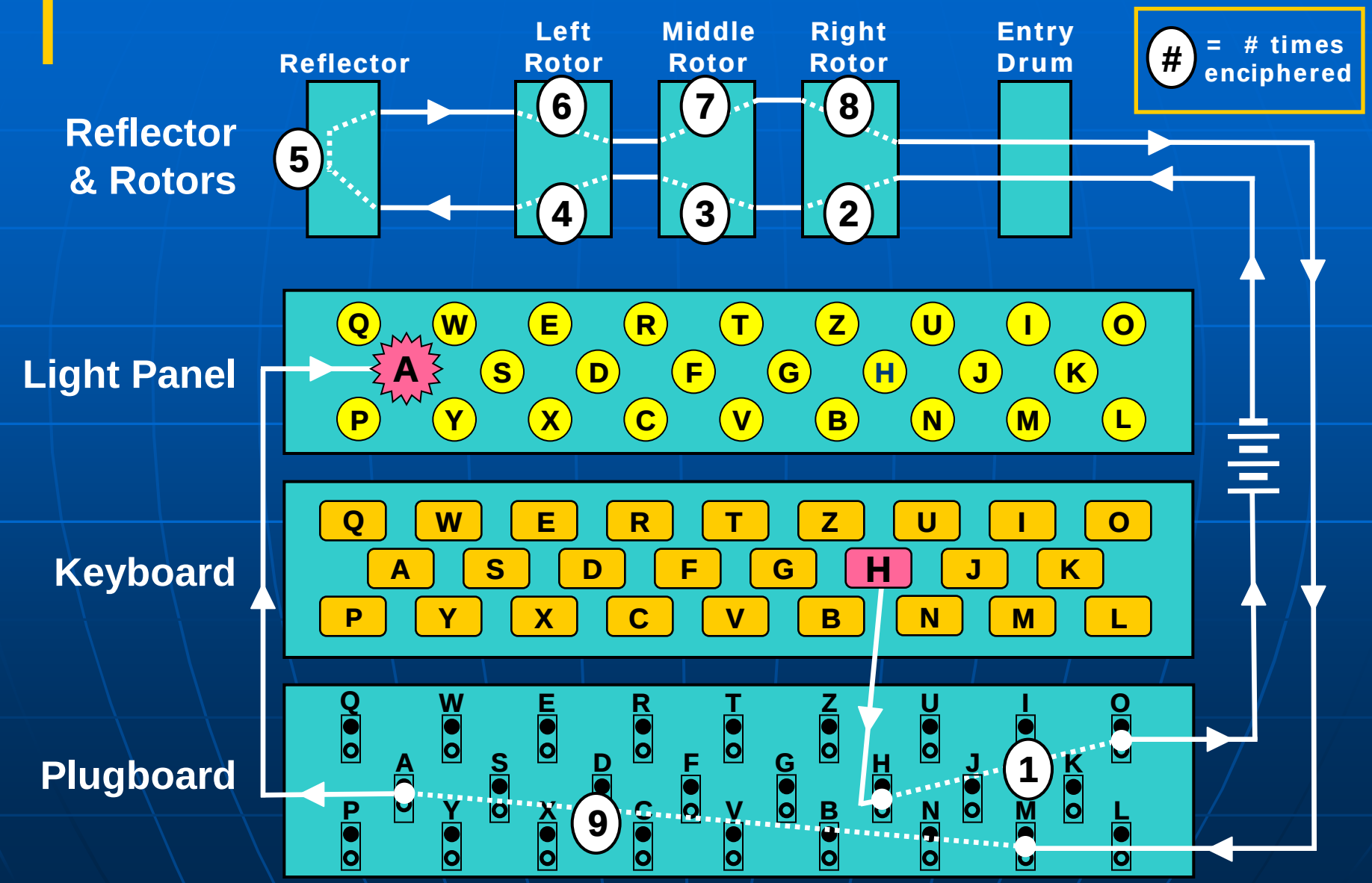
- Reflector swaps pairs of letters
- If "A" was enciphered to a "G", then "G" was enciphered as "A"
- The electrical signal goes through the 3 rotors, then the reflector and back again through the 3 rotors
- Reflector enables Enigma to encrypt / decrypt with the same key settings

- Reflector design meant no plaintext letter could encrypt to itself
- This was a major design flaw and was exploited by the Allies
- Finding cribs (expected words in an enciphered message) was aided by German military precision and the reflector design

Light Bulb Panel

- Keyboard, plugboard and light panel all follow QWERTZ format
- Only method of output - no printing capability
- Small light bulbs light up a letter, which must be written down
- Latches hold plastic filter for use in sunlight
- Operated by 4.5 volt battery or transformer from 220V plug

Wiring Diagram



Key Length of the Enigma

- Enigma has theoretical maximum number of settings (or keys) of 3 X 10^{114}, far more than the number of atoms in the universe (10^{80})
- Germans accepted operational tradeoffs which reduced the key length to the still astronomical number of 10^{23}
- A key length of 10^{23} is equivalent to a 77 bit key, better than the 56 bit DES standard of 1976-2002
- A key length of 10^{23} means 100,000 operators, each checking one key setting every second would take twice the age of the universe to break the code

Nazi Procedures for the Enigma

- Daily keys (settings for rotors and plugboard cables) were sent in a code book each month (longer for U-boats)
- Using the daily key, operators first sent a new key, then the text of the message in this new key – nullifying letter frequency analysis
- The new key specified the 3 rotor positions, and was sent TWICE
- Some operators used the same keys for each message, such as girlfriends initials, giving clues to solve the code
- Polish code-breakers exploited this shortcoming until 1939, when the Nazis sent the key only once

Using Enigma in the field

Shortcomings of the Enigma

- The reflector design allowed encryption and decryption with the same setting, but also ensured no letter encoded to itself
- Rotors had regular “odometer” movement
- Multiple notches used to make odometer stepping more complex was used on naval Enigma only
- Greatest shortcomings were lax operator procedures
- Strength of Enigma design gave Germans complete confidence in its security, even when faced with evidence of compromise

“Panzer General” Heinz Güderian on communications truck with Enigma machine

German Secrets of the Enigma

- Notice anything unusual about this Enigma?

Enlargement of Enigma from previous slide

Another Nazi propaganda picture of Enigma

- White cover over the plugboard
- Germans wanted to keep secret the military addition of a plugboard
- Even German allies, Italy and Japan, received Enigma machines without the plugboard

Polish Success in Decoding Enigma

- In 1932, Polish cryptologists reverse engineered the Enigma
- Enigma code was still not broken until the French bribed a German official to get keys
- German official, Hans-Thilo Schmidt, was later caught and executed
- Polish code-breakers could now exploit the double sending of the key – breaking the code in March 1933

Marian Rejewski
Polish cryptographer

- Poles made the Bomba – 6 Enigma machines in series to speed the checking of codes for the 6 combinations of 3 rotors
- Poles successfully decoded Enigma messages until 1939, when the Germans quit sending the key twice and added 2 new rotors
- Poles finally disclosed their code-breaking success to Britain and France just before Germany invaded Poland on Sept. 1, 1939

British Effort in Breaking the Code

- In 1939, UK began a major decoding effort in Bletchley Park, employing 11,000 people
- Effort led by Alan Turing, who built the Bombe - 36 Enigmas in series to check settings

Bletchley Park Mansion

- Many settings were manually eliminated and only the remaining settings checked by the Bombe – brute force wouldn't work
- Army and Luftwaffe messages were routinely decoded, the Naval Enigma was the greatest challenge
- British only acted on intelligence that could be uncovered from traditional sources (spies, direction finding, radar, traffic analysis)

U-Boat Peril

- Before the US entered the war, U-boats decimated Allied shipping, sinking about 60 ships per month
- U-boats roamed freely throughout Atlantic, forming “wolfpacks” to efficiently destroy convoys of supply ships for the UK
- Nazi strategy was to blockade the UK, expecting a quick surrender
- Naval Enigma was initially the same as the Army, but later more complex versions were used with more rigorous procedures
- Naval Enigma messages were completely secure until May, 1941

“The only thing that ever really frightened me during the war was the U-boat peril”

- Winston Churchill

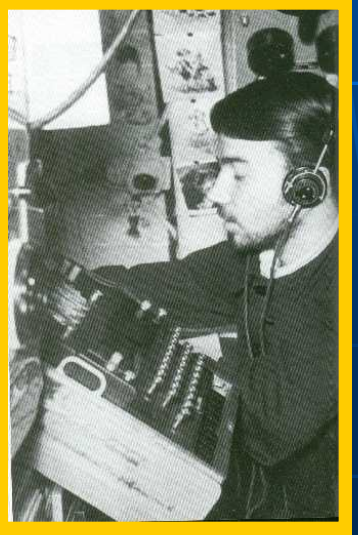
U-Boat

U-110

Sinking of U-110

- The first U-boat boarded and code books recovered was from U-110 in May 1941
- Captain died scuttling U-boat
- U-110 was sunk by British so Germans didn't realize their codes were compromised
- This single act was the turning point in the Battle of the Atlantic

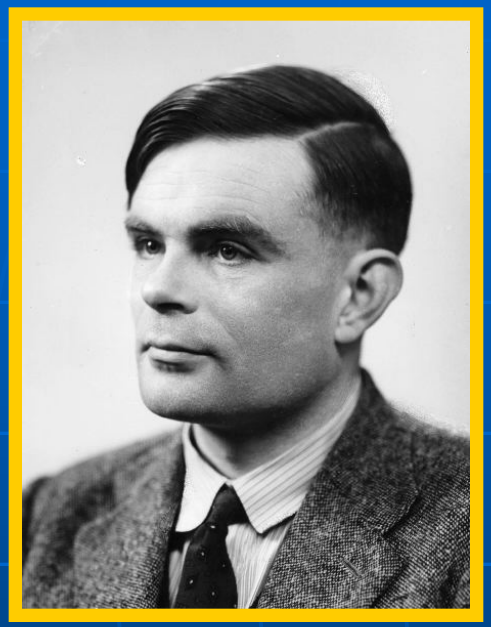
Captain of U-110
Fritz Julius Lemp



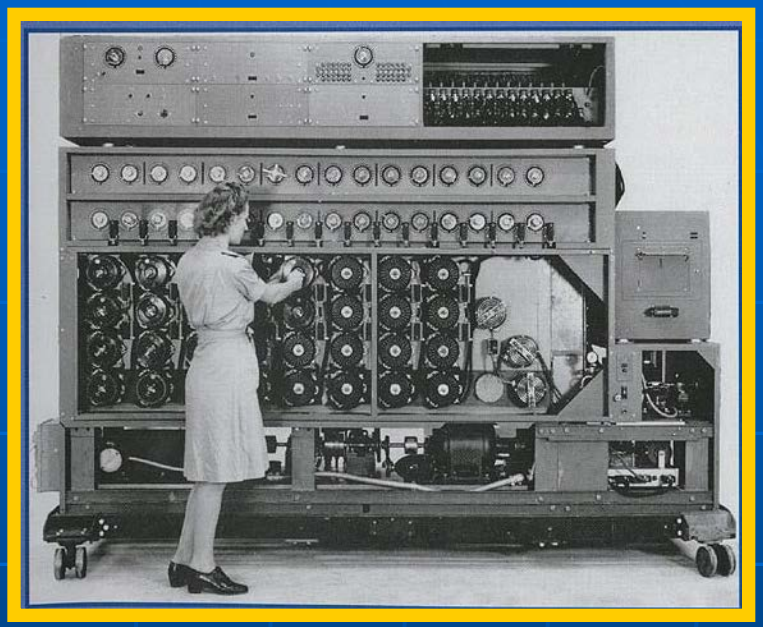
Enigma operator in U-110

HMS Bulldog – British destroyer captured U-110

Bombe – the Beginning of Computing



Alan Turing: Father of Computing

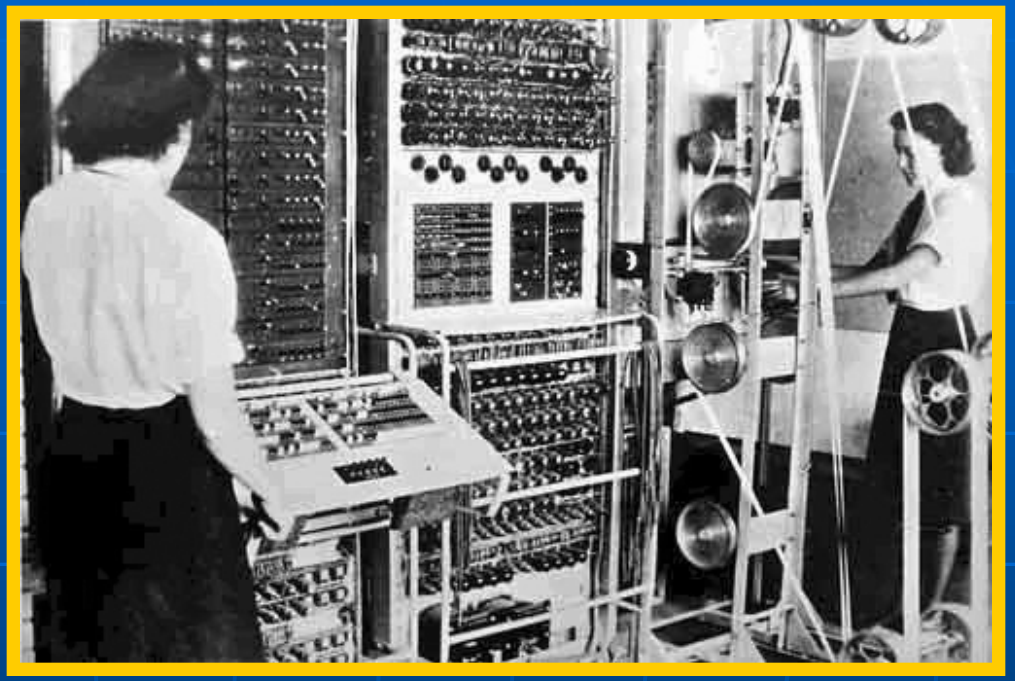


US Bombe

- Polish cryptoanalysts named their electro-mechanical codebreaker the Bomba for an ice cream treat, British called it a Bombe
- 210 Bombes were built in the UK, all were destroyed after WW2
- US employed NCR to build a faster version of the Bombe to decode the 4 rotor naval Enigma – 121 were built
- By the end of the war, the naval code was deciphered within 12 hours and the rest of the day's messages were read in real time

Colossus

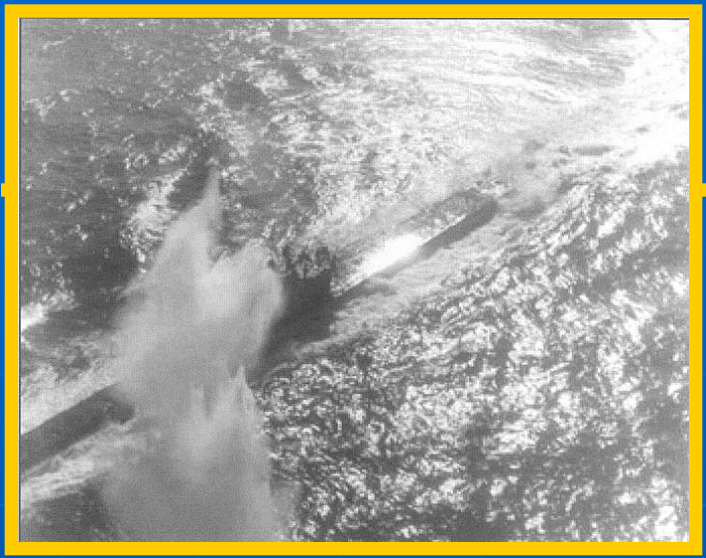
- Colossus – world's first programmable digital computer
- Named because of its overwhelming size, including 1600 vacuum tubes
- Designed by Tommy Flowers with help from Alan Turing in 1943



Colossus – note paper tape reels on right

- Colossus was used to break Nazi Lorenz teletype cipher, not the Enigma machine
- Total of 11 Colossi were built, all destroyed after the war
- CHM has tape pulley from an original Colossus

Battle of the Atlantic



US bombing of U-117 – Aug. 1943

- After breaking the Naval Enigma code, British selectively protected some ships
- British knew when U-boats would surface for supplies, so they pretended to "accidentally" find and destroy them
- In 1942, a 4th rotor was added to the Naval Enigma and 8 rotors were issued instead of 5 - making it more difficult to decipher
- An operator mistakenly sent the same message using old and new Enigmas, giving valuable clues to the new rotors and reflector
- It was discovered that unarmed weather trawlers carried the Enigma and codes, an easy target for additional code books
- Early U-boat success turned to failure, 725 of 1155 U-boats and 82% of 35,000 sailors never returned from sea
- Some estimate breaking the Enigma shortened WW2 by 2 years

Enigma After WW2

- Code-breaking success was not revealed until 1974, despite 11,000 people working on the effort in Bletchley Park, plus thousands more in the US
- US and UK encouraged use of Enigmas by other countries, including allies, reading their secrets for 3 decades
- Some Bombes were not destroyed, to decipher messages from countries still using Enigmas
- About 40,000 German Enigmas were manufactured, most were destroyed during or just after the war
- Today, fewer than 300 Enigmas are known to exist, up to 200 more are suspected to be in hidden collections
- Record prices at auction:
  - $269K for a 3-rotor Enigma at Bonhams on 4/13/15
  - $365K for a 4-rotor Enigma at Christies on 12/3/14

Download this Presentation

CipherMachines.com/enigma.ppt

Addendum

Calculations showing the maximum number of settings both theoretically and as practiced by the Nazis

Plugboard Settings

The # of possible plugboard settings is a function of 3 variables:

1. **# plugboard cables, p, can be from 0 to 13**
2. **# of groupings of possible letters (2p letters out of 26)**
3. **# interconnections of p cables within the group of letters chosen**

1. # plugboard cables	2. # groupings of letters 26! / ((2p!) X (26-2p)!)	3. # interconnections (2p-1) X (2p-3) X (2p-5) X …X 1	Total # possible settings (Column 2) X (Column 3)
0	1	1	1
1	325	1	325
2	14,950	3	44,850
3	230,230	15	3,453,450
4	1,562,275	105	164,038,875
5	5,311,735	945	5,019,589,575
6	9,657,700	10,395	100,391,791,500
7	9,657,700	135,135	1,305,093,289,500
8	5,311,735	2,027,025	10,767,019,638,375
9	1,562,275	34,459,425	53,835,098,191,875
10	230,230	654,729,075	150,738,274,937,250
11	14,950	13,749,310,575	205,552,193,096,250
12	325	316,234,143,225	102,776,096,548,125
13	1	7,905,853,580,625	7,905,853,580,625
Total			532,985,208,200,576

Rotor Settings

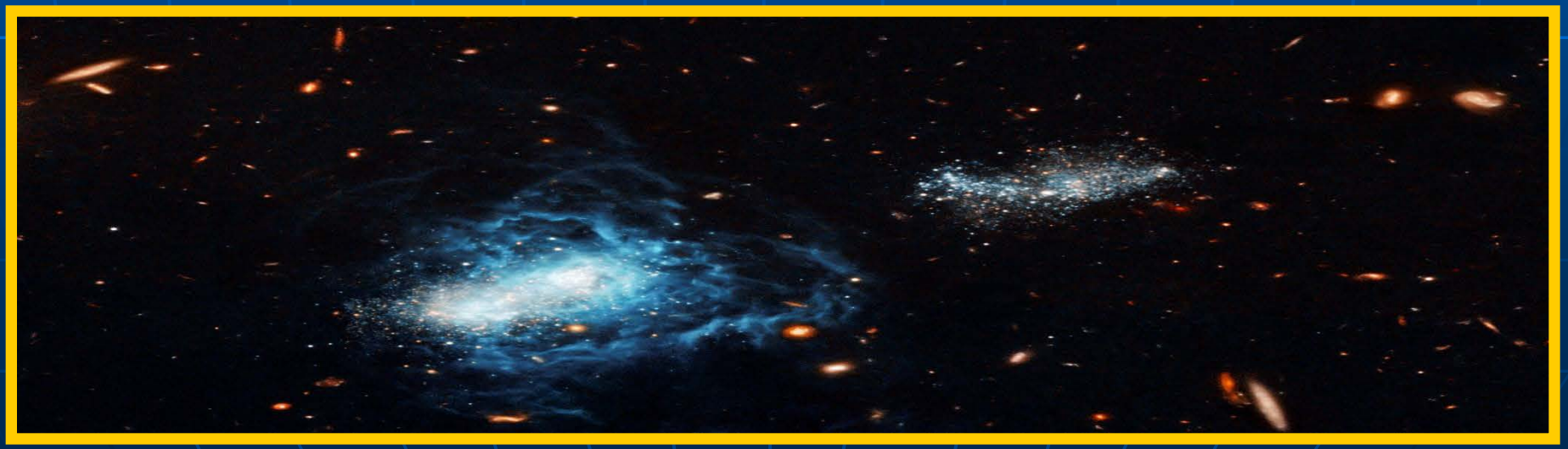
- The internal wiring of each rotor could be constructed in 26! different combinations. Since 3 rotors are used, the number of combinations when selecting 3 rotors out of 26! are:
  - 26! X (26!-1) X (26!-2) = 65,592,937,459,144, 468,297,405,473,480,371,753,615,896,841,298, 988,710,328,553,805,190,043,271,168,000,000
- Each of the 3 rotors could initially be set to any letter:
  - 26 X 26 X 26 = 17,576
- The right-most rotor advances one letter after each key is pressed, the second and third rotors advance one letter after a full revolution of the rotor to its right. The setting for the notch to enable this was also changeable to any letter of the alphabet:
  - 26 X 26 = 676 (Note: notch on left-most rotor has no effect)

Reflector Settings

- The reflector scrambled the letters in pairs so it could encrypt and decrypt
- The letter “A” could be switched to any of the 25 remaining letters, the next letter could be switched to any of the 23 remaining letters, and so on.
- Notice this result is the same as using 13 plugboard cables, since all letters are paired (see chart on page 22)
  - 25 X 23 X 21 X … X 1 = 7,905,853,580,625

Total Theoretical Number of Settings

- The total theoretical number of Enigma settings is thus the product of the 5 items on the previous 3 slides, or…
  - 3,283,883,513,796,974,198,700,882,069,882,752,878, 379,955,261,095,623,685,444,055,315,226,006,433,615, 627,409,666,933,182,371,154,802,769,920,000,000,000
  - Or 3.28×10^{114}
- This number is far greater than the total number of atoms in the observable universe (10^{80})



Theory vs. Practice

- The theoretical number of Enigma settings was not achieved in practice by the Germans, the number of settings the Allied Forces encountered for the standard 3 rotor enigma:
  - 10 plugboard cables were always used, reducing errors and the possible combinations to 150,738,274,937,250
  - Only 5 of 26! possible rotors were issued and known by Allies, so selecting 3 out of 5 is 5 X 4 X 3 = 60
  - The initial settings of the rotors and the positions of the notches remain the same at 17,576 and 676
  - Reflector setting was known and remained unchanged = 1
  - The product of the above numbers is: 107,458,687,327,250,619,360,000 or 1.07×10^{23}
- To test 10^{23} key settings, 100,000 operators each checking one setting every second would take twice the age of the universe to break the code