Cracking the Enigma:

the Secret Battlefield of WW2

Cipher History Museum

October 15, 2022

Ralph Simpson

Ralph@CipherHistory.com

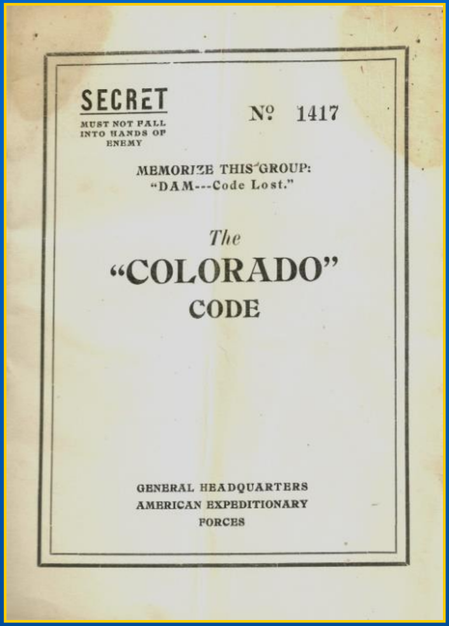
All images and cipher devices in this presentation are from the collection of CipherHistory.com, unless otherwise noted

WW1 - first time radio was used in war

WW1 US Army portable radio station in Germany

Photo credit: US Army

US Army
Code Book
1918



SECRET
MUST NOT FALL INTO HANDS OF ENEMY

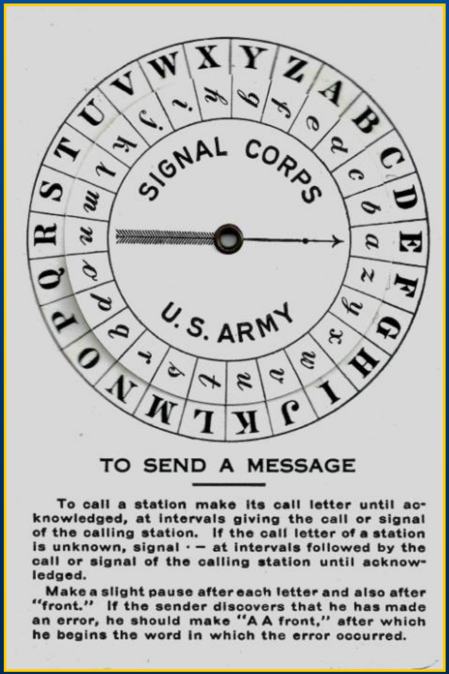
Nº 1417

MEMORIZE THIS GROUP:
"DAM---Code Lost."

The
"COLORADO"
CODE

GENERAL HEADQUARTERS
AMERICAN EXPEDITIONARY
FORCES

US Army
Vigenère Disk
1912



TO SEND A MESSAGE

To call a station make its call letter until acknowledged, at intervals giving the call or signal of the calling station. If the call letter of a station is unknown, signal · — at intervals followed by the call or signal of the calling station until acknowledged.

Make a slight pause after each letter and also after "front." If the sender discovers that he has made an error, he should make "A A front," after which he begins the word in which the error occurred.

- Radio radically transformed battlefield strategy, but the enemy can now intercept all messages
- Cipher technology was not up to the task
- Ciphers were manual, error-prone, 450 years old… and all were broken!

Birth of crypto warfare

- Explosion of new cipher technology during WW1:
  - One-time teletype tape
  - Cipher wheel
  - Strip cipher
  - Burst encoder
  - 4 electro-mechanical rotor machines:

Edward Hebern USA 1917	Arthur Scherbius Germany 1918	Hugo Koch Holland 1919	Arvid Damm Sweden 1919

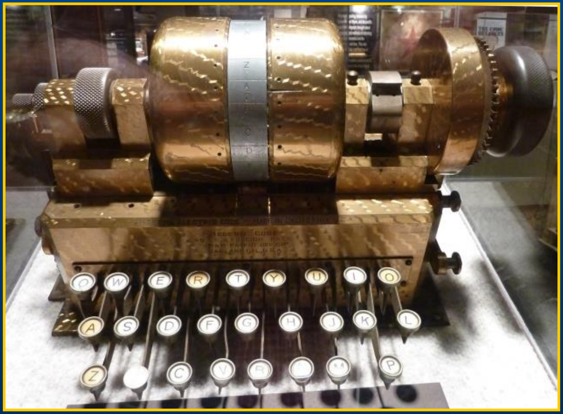


Photo credit: Ralph Simpson, device at NCM. Ft. Meade, MD

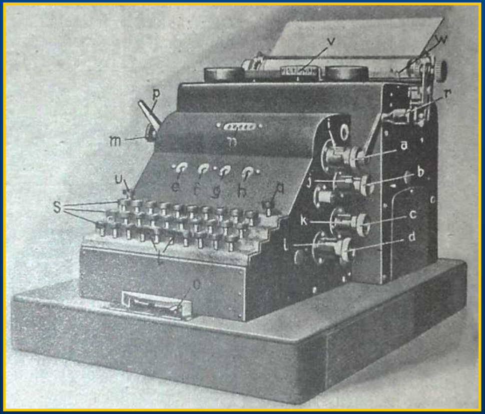
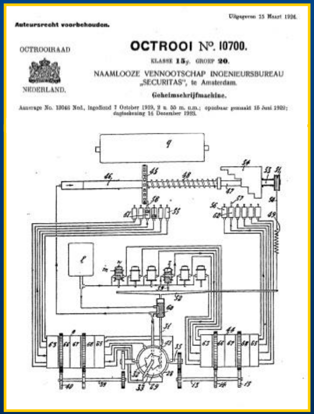


Photo credit: 1923 book, Technit, neue Apparate, Maschinen, Bauwerte



Uitgegeven 15 Maart 1924.

Auteursrecht voorbehouden.

OCTROOIRAAD

NEDERLAND.

OCTROOI No. 10700.

KLASSE 15g. GROEP 20.

NAAMLOOZE VENNOOTSCHAP INGENIEURSBUREAU „SECURITAS", te Amsterdam.

Geheimschrijfmachine.

Aanvrage No. 13046 Ned., ingediend 7 October 1919, 2 u. 55 m. n.m.; openbaar gemaakt 15 Juni 1922; dagteekening 14 December 1923.

Photo credit: Bureau voor Industriele Eigendom

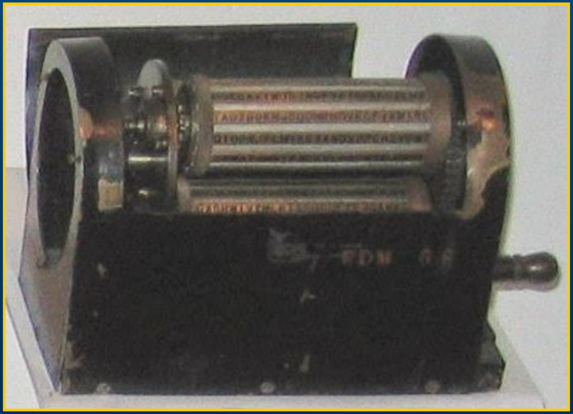


Photo credit: Austin Mills, device in NCM, Ft. Meade, MD

Enigma invention - the classic story

Arthur Scherbius
Germany
(1878-1929)

Photo credit:
Scherbius family

Hugo Koch
Holland
(1870-1928)

Photo credit:
Koch family

- Scherbius / Koch collaborated on Enigma, filed separate patents
- German Navy began testing Scherbius Enigma in 1926
- In 1927, Scherbius “curiously” bought the rights to Koch’s patent, paid 600 Dutch guilders (~$350)
- “Curious” because Scherbius owned the identical German patent
- Koch died in 1928; Scherbius in 1929 in a horse carriage accident
- Neither knew the role their invention would have in history

History rewritten in 2003

Theo van Hengel
(1875-1939)

Photo credit: Instituut voor
Maritieme Historie, Den Haag

- 2003 bombshell: two Dutch naval officers invented the rotor cipher in 1915
- Patent attorney hired, but Dutch Navy suppressed patent during WW1
- Nov. 1919, Dutch Navy allowed naval officers patent, but Koch filed his patent 3 weeks earlier

Rudolf P.C. Spengler
(1875-1955)

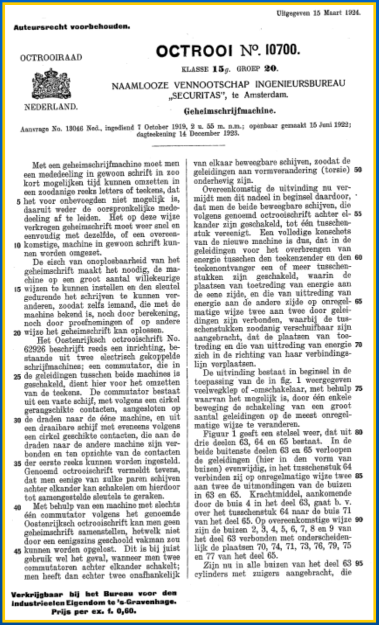
Photo credit: Spengler family

- Naval officers filed lawsuit against Koch, but lost…
  - They didn't know their patent attorney was Koch's brother-in-law!
  - Judge was ex-Navy Minister who suppressed the patent in WW1!
- Now van Hengel and Spengler are recognized as the true inventors of the rotor cipher and the Enigma machine

Dutch and German patents are exact copies

Dutch patent NL10700
filed 10/7/1919

- Dutch patent never built
- German patent was early version of Enigma
- Scherbius bought Dutch patent on 1/28/1927



Uitgegeven 15 Maart 1924.

Auteursrecht voorbehouden.

OCTROOIRAAD

NEDERLAND.

OCTROOI Nº. 10700.

KLASSE **15***g*. GROEP **20**.

NAAMLOOZE VENNOOTSCHAP INGENIEURSBUREAU „SECURITAS", te Amsterdam.

Geheimschrijfmachine.

Aanvrage No. 13046 Ned., ingediend 7 October 1919, 2 u. 55 m. n.m.; openbaar gemaakt 15 Juni 1922; dagteekening 14 December 1923.

Met een geheimschrijfmachine moet men een mededeeling in gewoon schrift in zoo kort mogelijken tijd kunnen omzetten in een zoodanige reeks letters of teekens, dat het voor onbevoegden niet mogelijk is, daaruit weder de oorspronkelijke mededeeling af te leiden. Het op deze wijze verkregen geheimschrift moet weer snel en eenvoudig met dezelfde, of een overeenkomstige, machine in gewoon schrift kunnen worden omgezet.

De eisch van onoplosbaarheid van het geheimschrift maakt het noodig, de machine op een groot aantal willekeurige wijzen te kunnen instellen en den sleutel gedurende het schrijven te kunnen veranderen, zoodat zelfs iemand, die met de machine bekend is, noch door berekening, noch door proefnemingen of op andere wijze het geheimschrift kan oplossen.

Het Oostenrijksch octrooischrift No. 62926 beschrijft reeds een inrichting, bestaande uit twee electrisch gekoppelde schrijfmachines; een commutator, die in de geleidingen tusschen beide machines is geschakeld, dient hier voor het omzetten van de teekens. De commutator bestaat uit een vaste schijf, met volgens een cirkel gerangschikte contacten, aangesloten op de draden naar de éène machine, en uit een draaibare schijf met eveneens volgens een cirkel geschikte contacten, die aan de draden naar de andere machine zijn verbonden en ten opzichte van de contacten der eerste reeks kunnen worden ingesteld. Genoemd octrooischrift vermeldt tevens, dat men eenige van zulke paren schijven achter elkander kan schakelen om hierdoor tot samengestelde sleutels te geraken.

Met behulp van een machine met slechts één commutator volgens het genoemde Oostenrijksch octrooischrift kan men geen geheimschrift samenstellen, hetwelk niet door een eenigszins geschoold vakman zou kunnen worden opgelost. Dit is bij juist gebruik wel het geval, wanneer men twee commutatoren achter elkander schakelt; men heeft dan echter twee onafhankelijk van elkaar beweegbare schijven, zoodat de geleidingen aan vormverandering (torsie) onderhevig zijn.

Overeenkomstig de uitvinding nu vermijdt men dit nadeel in beginsel daardoor, dat men de beide beweegbare schijven, die volgens genoemd octrooischrift achter elkander zijn geschakeld, tot één tusschenstuk vereenigt. Een volledige kenschets van de nieuwe machine is dus, dat in de geleidingen voor het overbrengen van energie tusschen den teekenzender en den teekenontvanger een of meer tusschenstukken zijn geschakeld, waarin de plaatsen van toetreding van energie aan de eene zijde, en die van uittreding van energie aan de andere zijde op onregelmatige wijze twee aan twee door geleidingen zijn verbonden, waarbij de tusschenstukken zoodanig verschuifbaar zijn aangebracht, dat de plaatsen van toetreding en die van uittreding van energie zich in de richting van haar verbindingslijn verplaatsen.

De uitvinding bestaat in beginsel in de toepassing van de in fig. 1 weergegeven veelwegklep of -omschakelaar, met behulp waarvan het mogelijk is, door één enkele beweging de schakeling van een groot aantal geleidingen op de meest onregelmatige wijze te veranderen.

Figuur 1 geeft een stelsel weer, dat uit drie deelen 63, 64 en 65 bestaat. In de beide buitenste deelen 63 en 65 verloopen de geleidingen (hier in den vorm van buizen) evenwijdig, in het tusschenstuk 64 verbinden zij op onregelmatige wijze twee aan twee de uitmondingen van de buizen in 63 en 65. Krachtmiddel, aankomende door de buis 4 in het deel 63, gaat b. v. over het tusschenstuk 64 naar de buis 71 van het deel 65. Op overeenkomstige wijze zijn de buizen 2, 3, 4, 5, 6, 7, 8 en 9 van het deel 63 verbonden met onderscheidenlijk de plaatsen 70, 74, 71, 73, 76, 79, 75 en 77 van het deel 65.

Zijn nu in alle buizen van het deel 63 cylinders met zuigers aangebracht, die

Verkrijgbaar bij het Bureau voor den industrieelen Eigendom te 's-Gravenhage.
Prijs per ex. f. 0,60.

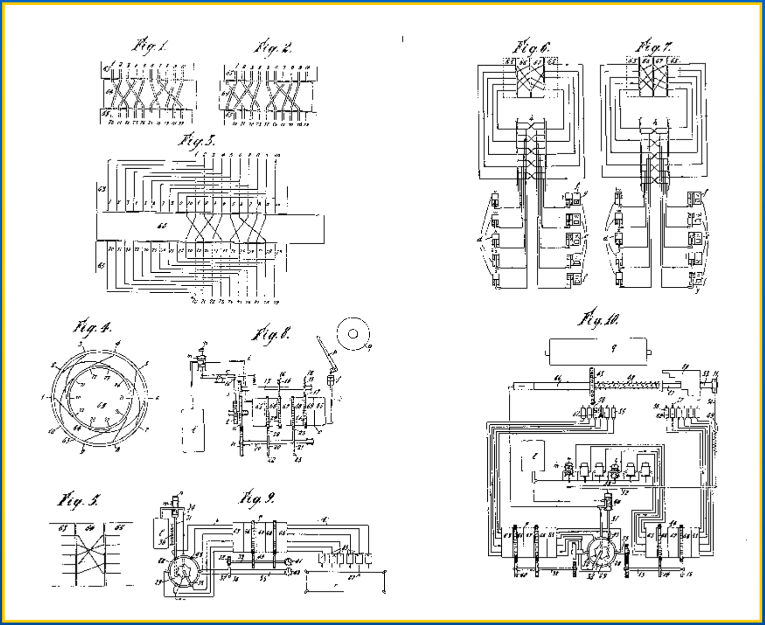
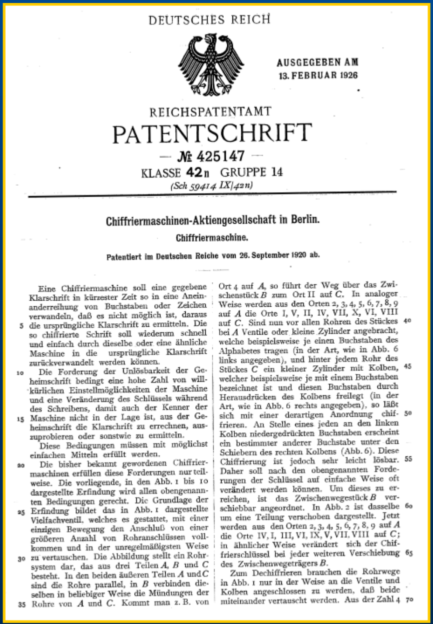


Photo credit: Bureau voor Industriele Eigendom

German patent
DE425147
filed 9/26/1920



DEUTSCHES REICH

AUSGEGEBEN AM
13. FEBRUAR 1926

REICHSPATENTAMT

PATENTSCHRIFT

— № 425147 —

KLASSE **42**n GRUPPE 14

(Sch 59414 IX/42n)

Chiffriermaschinen-Aktiengesellschaft in Berlin.

Chiffriermaschine.

Patentiert im Deutschen Reiche vom 26. September 1920 ab.

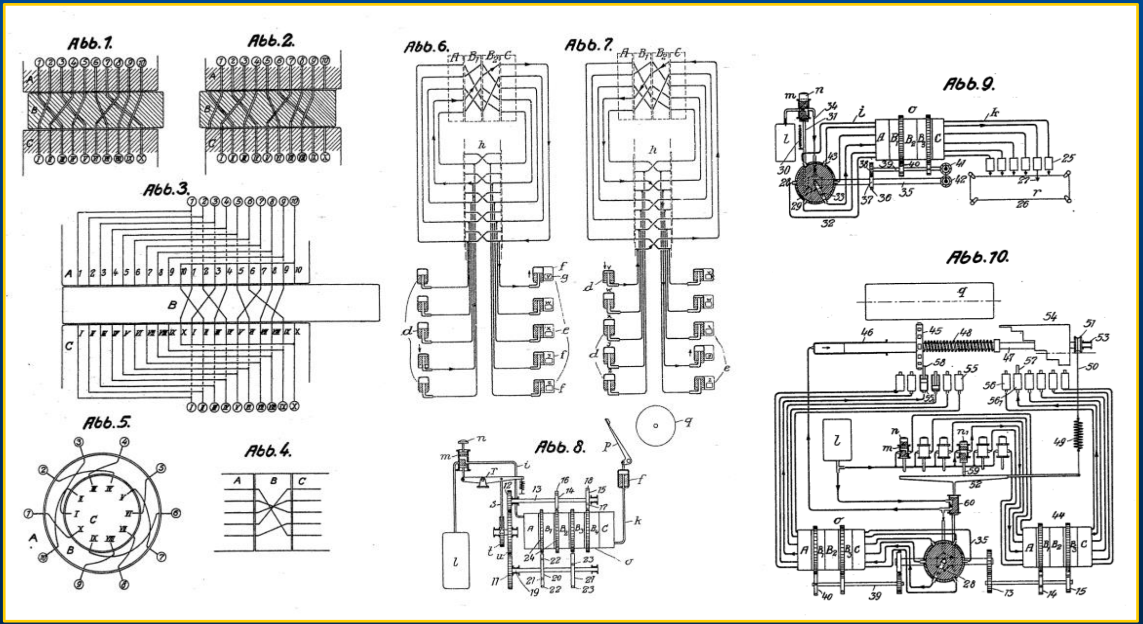
Eine Chiffriermaschine soll eine gegebene Klarschrift in kürzester Zeit so in eine Aneinanderreihung von Buchstaben oder Zeichen verwandeln, daß es nicht möglich ist, daraus die ursprüngliche Klarschrift zu ermitteln. Die so chiffrierte Schrift soll wiederum schnell und einfach durch dieselbe oder eine ähnliche Maschine in die ursprüngliche Klarschrift zurückverwandelt werden können.

Die Forderung der Unlösbarkeit der Geheimschrift bedingt eine hohe Zahl von willkürlichen Einstellmöglichkeiten der Maschine und eine Veränderung des Schlüssels während des Schreibens, damit auch der Kenner der Maschine nicht in der Lage ist, aus der Geheimschrift die Klarschrift zu errechnen, auszuprobieren oder sonstwie zu ermitteln.

Diese Bedingungen müssen mit möglichst einfachen Mitteln erfüllt werden.

Die bisher bekannt gewordenen Chiffriermaschinen erfüllen diese Forderungen nur teilweise. Die vorliegende, in den Abb. 1 bis 10 dargestellte Erfindung wird allen obengenannten Bedingungen gerecht. Die Grundlage der Erfindung bildet das in Abb. 1 dargestellte Vielfachventil, welches es gestattet, mit einer einzigen Bewegung den Anschluß von einer größeren Anzahl von Rohranschlüssen vollkommen und in der unregelmäßigsten Weise zu vertauschen. Die Abbildung stellt ein Rohrsystem dar, das aus drei Teilen *A*, *B* und *C* besteht. In den beiden äußeren Teilen *A* und *C* sind die Rohre parallel, in *B* verbinden dieselben in beliebiger Weise die Mündungen der Rohre von *A* und *C*. Kommt man z. B. von Ort 4 auf *A*, so führt der Weg über das Zwischenstück *B* zum Ort II auf *C*. In analoger Weise werden aus den Orten 2, 3, 4, 5, 6, 7, 8, 9 auf *A* die Orte I, V, II, IV, VII, X, VI, VIII auf *C*. Sind nun vor allen Rohren des Stückes bei *A* Ventile oder kleine Zylinder angebracht, welche beispielsweise je einen Buchstaben des Alphabetes tragen (in der Art, wie in Abb. 6 links angegeben), und hinter jedem Rohr des Stückes *C* ein kleiner Zylinder mit Kolben, welcher beispielsweise je mit einem Buchstaben bezeichnet ist und diesen Buchstaben durch Herausdrücken des Kolbens freilegt (in der Art, wie in Abb. 6 rechts angegeben), so läßt sich mit einer derartigen Anordnung chiffrieren. An Stelle eines jeden an den linken Kolben niedergedrückten Buchstaben erscheint ein bestimmter anderer Buchstabe unter den Schiebern des rechten Kolbens (Abb. 6). Diese Chiffrierung ist jedoch sehr leicht lösbar. Daher soll nach den obengenannten Forderungen der Schlüssel auf einfache Weise oft verändert werden können. Um dieses zu erreichen, ist das Zwischenwegestück *B* verschiebbar angeordnet. In Abb. 2 ist dasselbe um eine Teilung verschoben dargestellt. Jetzt werden aus den Orten 2, 3, 4, 5, 6, 7, 8, 9 auf *A* die Orte IV, I, III, VI, IX, V, VII. VIII auf *C*; in ähnlicher Weise verändert sich der Chiffrierschlüssel bei jeder weiteren Verschiebung des Zwischenwegeträgers *B*.

Zum Dechiffrieren brauchen die Rohrwege in Abb. 1 nur in der Weise an die Ventile und Kolben angeschlossen zu werden, daß beide miteinander vertauscht werden. Aus der Zahl 4

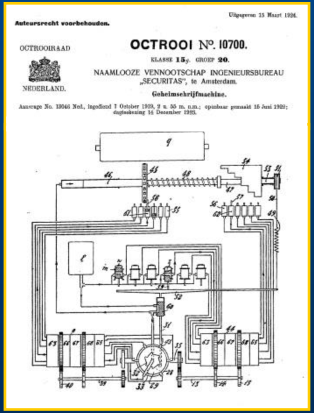


Birth of crypto warfare

- Explosion of new cipher technology during WW1:
  - One-time teletype tape
  - Cipher wheel
  - Strip cipher
  - Burst encoder
  - Now 3 electro-mechanical rotor machines:

UPDATED BY 2003 REVELATIONS

Theo van Hengel
Rudolf P.C. Spengler
Holland
1915



Uitgegeven 15 Maart 1924.

Auteursrecht voorbehouden.

OCTROOIRAAD

NEDERLAND.

OCTROOI N°. 10700.

KLASSE 15g. GROEP 20.

NAAMLOOZE VENNOOTSCHAP INGENIEURSBUREAU „SECURITAS", te Amsterdam.

Geheimschrijfmachine.

Aanvrage No. 13046 Ned., ingediend 7 October 1919, 2 u. 55 m. n.m.; openbaar gemaakt 15 Juni 1922; dagteekening 14 December 1923.

9
46
45
48
54
53
52
47
58
57

Photo credit: Bureau voor Industriele Eigendom

Edward Hebern
USA
1917

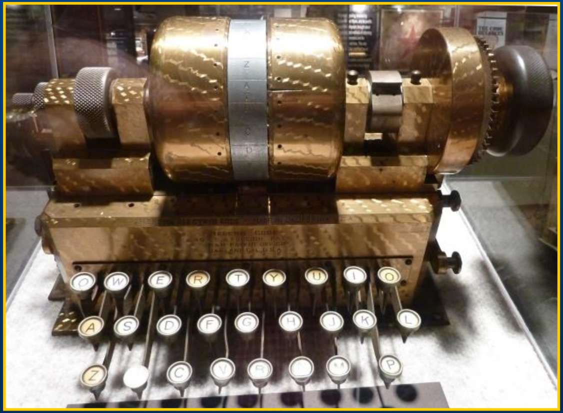


Photo credit: Ralph Simpson, device in NCM. Ft. Meade, MD

Arvid Damm
Sweden
1919

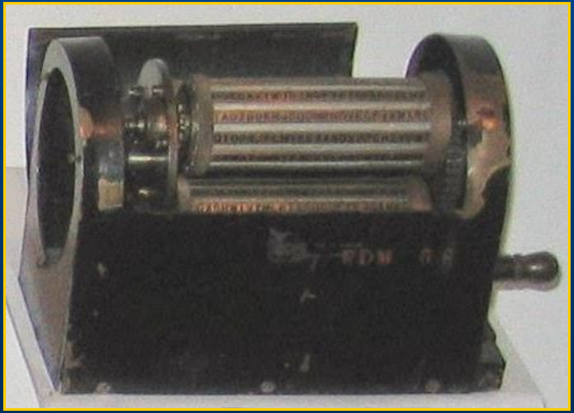
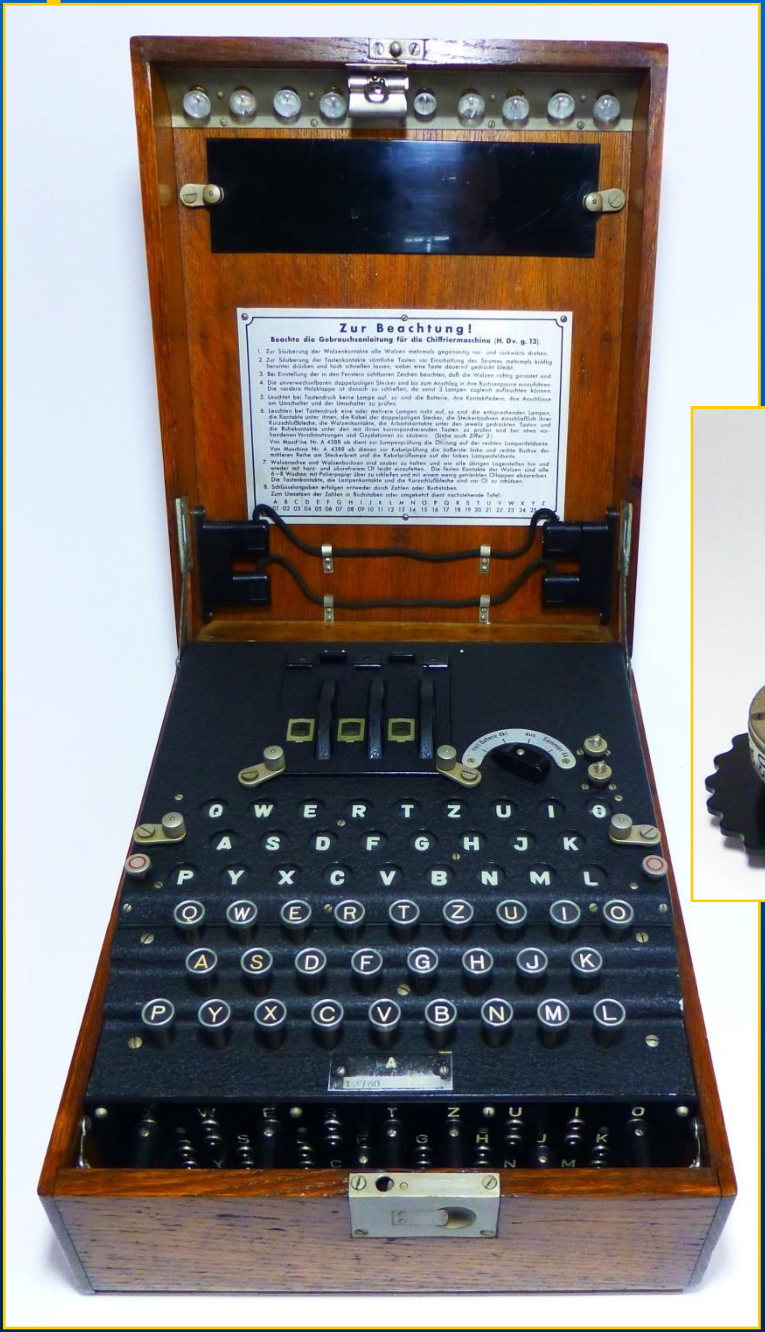
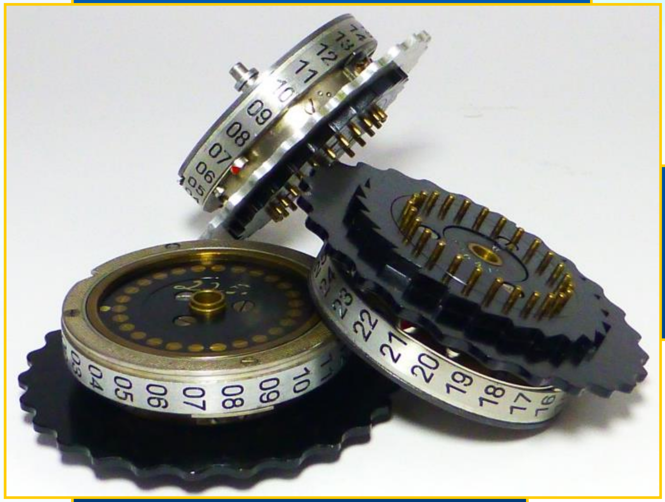


Photo credit: Austin Mills, device in NCM, Ft. Meade, MD

Enigma machine



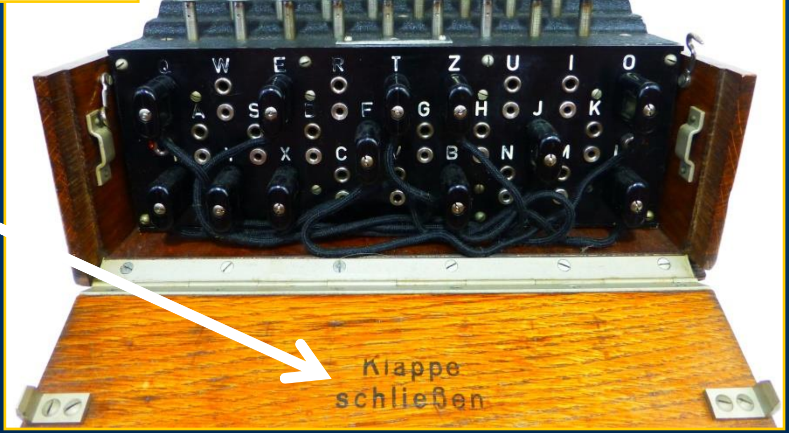
Enigma means puzzle or mystery in German & most European languages



klappe schließen

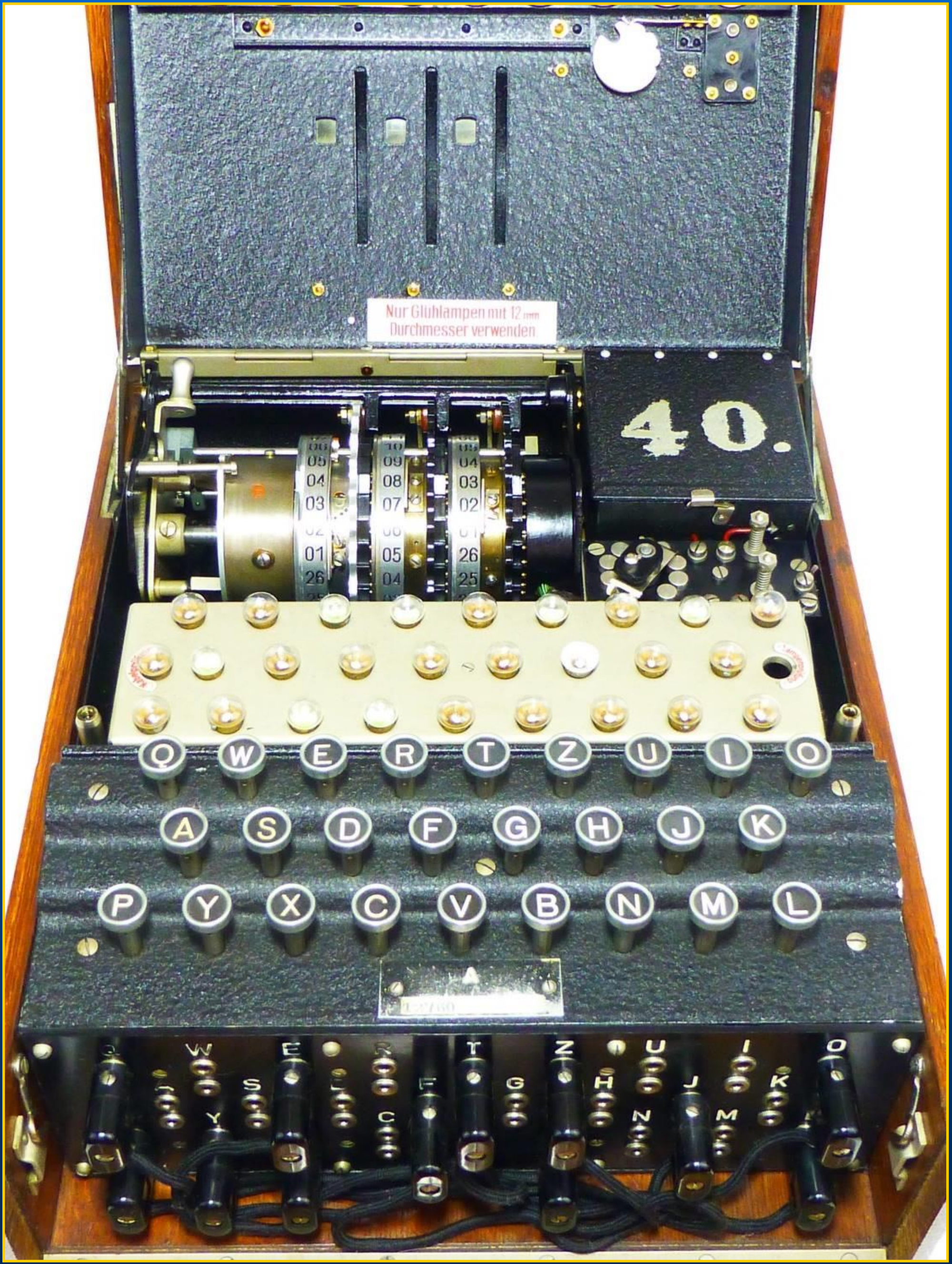
=

close your the flap



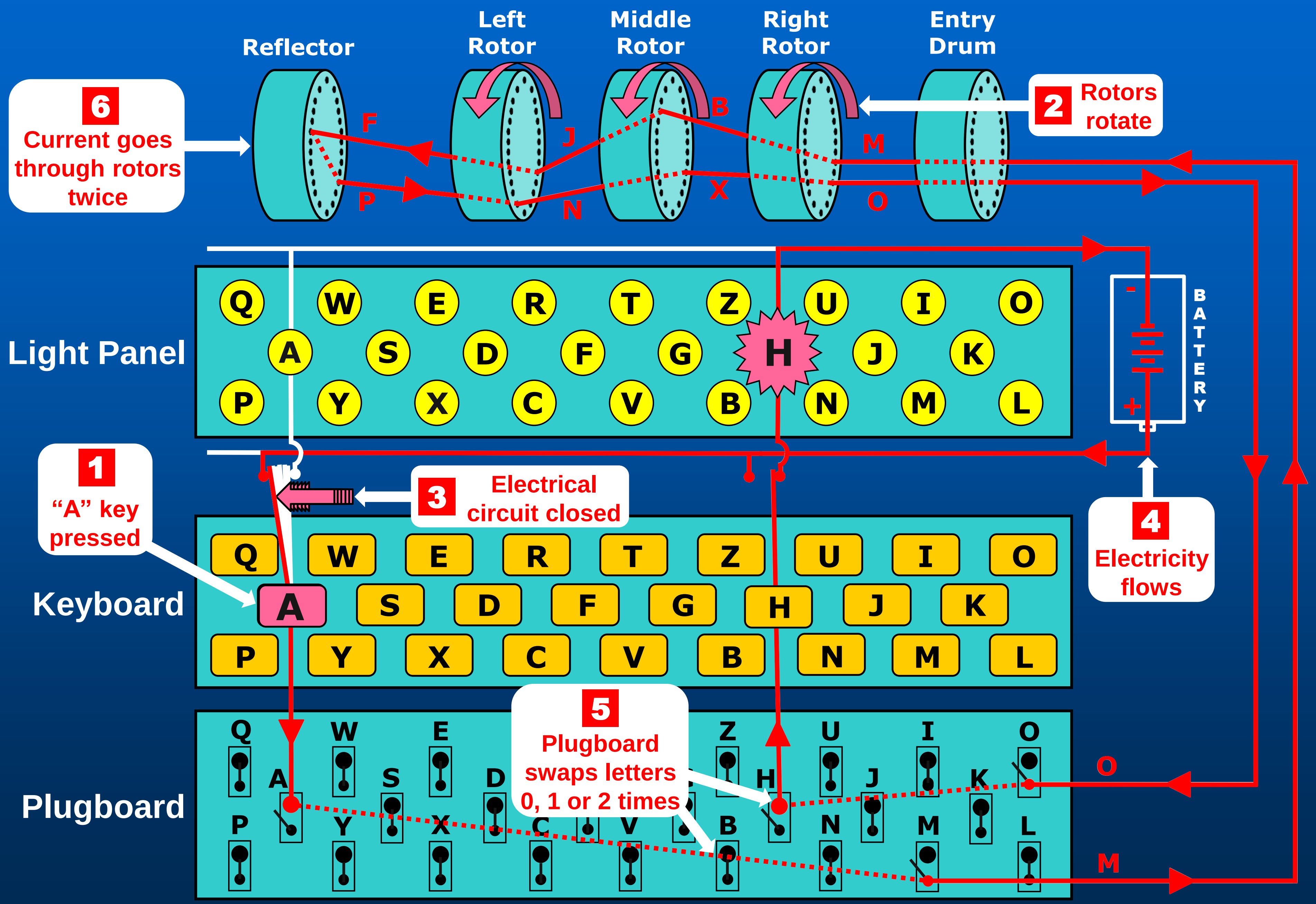
Enigma machine - under the covers

- Typewriter style cipher machine, with light bulbs instead of printer
- Electro-mechanical rotors was the key innovation
- Rotors turn odometer style, so every letter in a message uses a different algorithm
- Reflector gives reciprocal encryption / decryption
- German military added plugboard



Enigma wiring - animated!

example: "A" enciphers / deciphers to "H"



1 "A" key pressed

2 Rotors rotate

3 Electrical circuit closed

4 Electricity flows

5 Plugboard swaps letters 0, 1 or 2 times

6 Current goes through rotors twice

Cryptographic strength of Enigma

- Theoretical maximum # of Enigma settings is 3 X 10^{114} (# atoms in universe = 10^{80})
- If an enemy captures the Enigma, the # settings is still astronomical - 10^{23}
- 10^{23} is equal to a 76 bit key, far better than the 56 bit DES standard, used until 2001
- A 76 bit key means:

Webb Space Telescope view of cartwheel and spiral galaxies

Photo credit: NASA, ESA, CSA, STScI

If 100,000 Enigma operators could each check one key setting every second, 24X7…

It would take twice the age of the universe to break the code!

Enigma Weaknesses

Photo credit: Deutsches Bundesarchiv, colored by Lopatin V.

1. Greatest vulnerability was lax operator procedures
2. Reflector was reciprocal, so no letter encoded to itself
3. Rotors had regular, odometer movement
4. Ironically, brute strength of the Enigma gave Germans too much confidence in its security

Panzer General Heinz Guderian on communications truck with Enigma (1940)

Poland was first to break Enigma

Marian Rejewski (1905-1980), in UK c.1943/44

Photo credit: Public domain, unknown photographer

- In 1932, German spy Hans-Thilo Schmidt sold Enigma keys to Allies
- Marian Rejewski used mathematics to recreate & break Enigma, in Dec. 1932
- Breakthrough was breaking of rotors and plugboard separately, so now…
  - 100,000 operators can break Enigma in 2 hours vs “twice age of universe”!
- Poles made “Bomba,” 6 Enigmas in series, to quickly break daily key (Bomba = Eureka in Polish)
- Polish codebreaking success kept secret for 7 years
- Poles finally disclosed Enigma secrets to UK and France just 5 weeks before Germany invaded Poland on Sept. 1, 1939

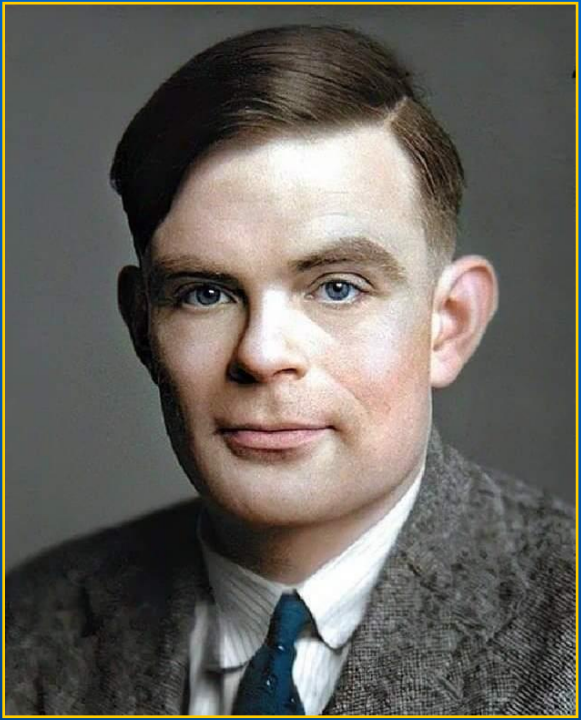
British effort in breaking the Enigma

Bletchley Park Mansion

Photo credit: Standardissuemagazine.com

- In 1939, UK began a major decoding effort at Bletchley Park, employing 11,000
- Effort led by Alan Turing, who built the Bombe: 36 Enigmas in series to find possible rotor settings
- After the Bombe found rotor settings, plugboard cables were solved manually

Bombe - the beginning of computing



Alan Turing (1912-1954)

"Father of Computing"

Photo credit: Godrey Argent Studio, via The Royal Society

US Bombe

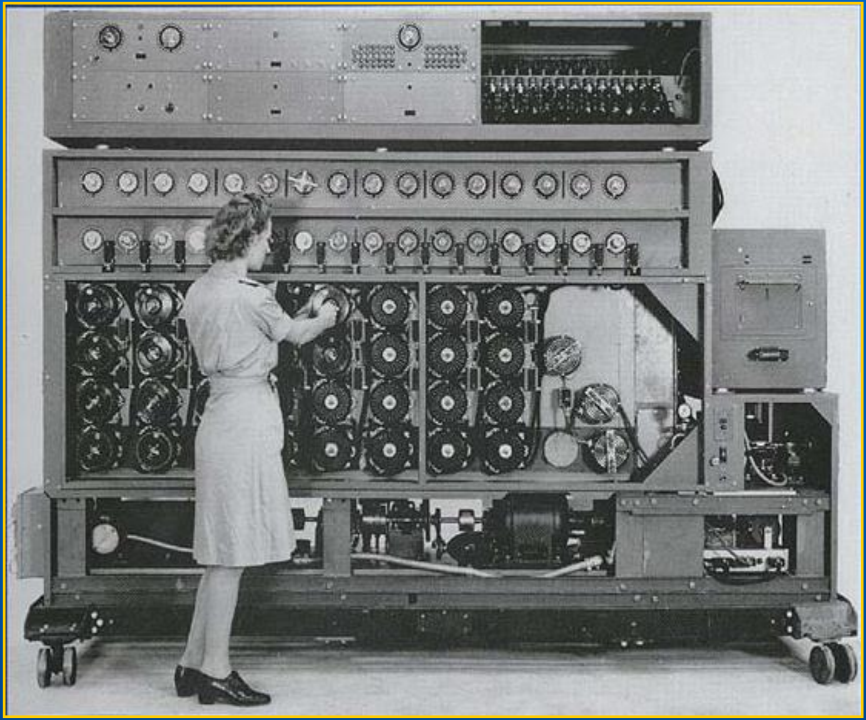


Photo credit: NCM, Ft. Meade, "Solving the Enigma"

- Poles named their electro-mechanical codebreaker "Bomba," British used "Bombe" in honor of Polish contribution
- British exploited cribs vs Poles exploit of double message key
- 211 UK Bombes were built, most 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

Colossus computer

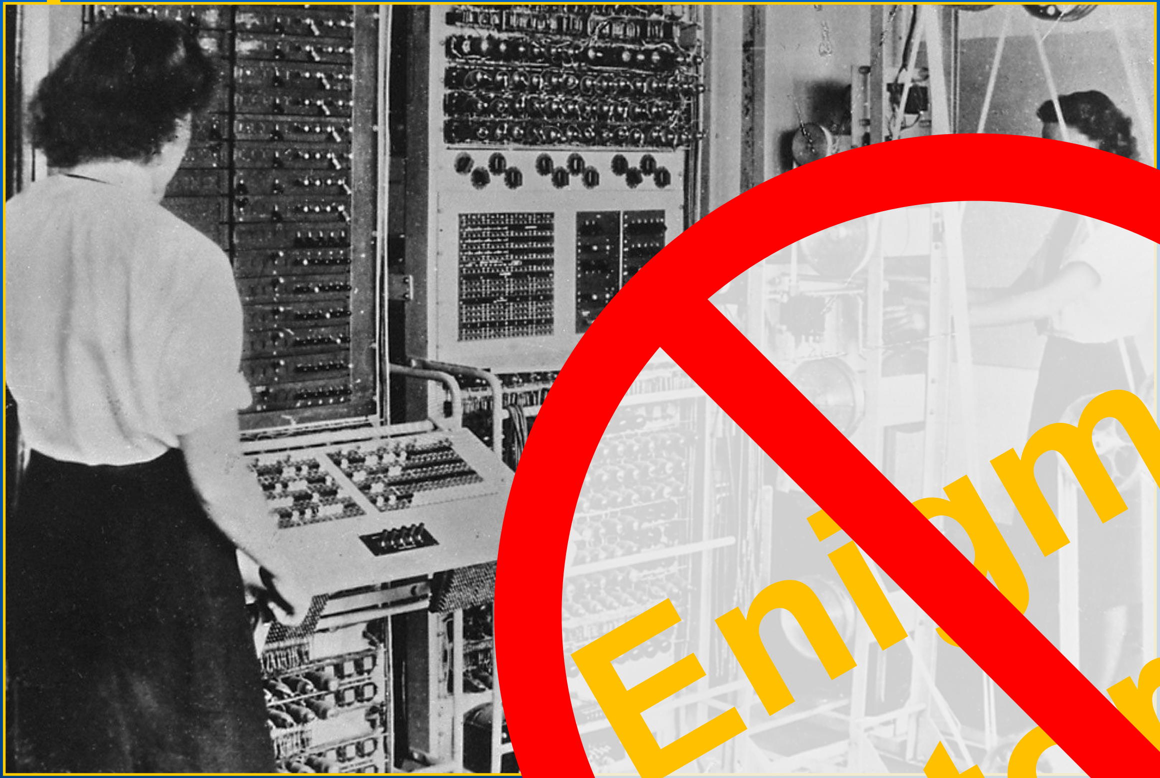


Photo credit: [illegible]tional Archives

Lorenz SZ-42 cipher

Photo credit: Ralph Simpson,
device at NCM, Ft. Meade, MD

- Colossus world's first electronic, programmable, digital computer
- Uses 2400 vacuum and [illegible]
- Colossus breaks Lorenz teletype cipher, not Enigma
- Lorenz cipher used for high level messages

U-boat peril

- Before the US entered the war, U-boats sank 60 ships / month
- U-boats roamed freely, then formed “wolfpacks” to sink convoys efficiently
- Nazis expected a UK blockade to result in a quick surrender
- Naval Enigma was initially the same as the Army, but later a 4-rotor version was used with more rigorous procedures
- Naval Enigma messages were secure until May 1941

> *“The only thing that ever really frightened me during the war was the U-boat peril.”*
>
> **- Winston Churchill**

U-boat sinks an English freighter, from a German book published during WWII

Photo credit: Naval History and Heritage Command

Capture of U-110

U-110 Captain Fritz-Julius Lemp

Photo credit: reibert.info

- First code books captured from a U-boat was on May 9, 1941
- Captain died trying to scuttle U-110
- Germans didn’t know 3 months of codes were stolen, by Lt. Balme
- 5 ships, from 1 Enigma message, were sunk on June 3 & 4, 1941
- U-110 capture was the turning point in the Battle of the Atlantic

Lt. David Balme on deck of HMS Bulldog

Photo credit: forces.net

Balme leads boarding party to captured U-110

Photo credit: uboatarchive.net

UK sailors on deck of U-110

Photo credit: uboatarchive.net

Battle of the Atlantic

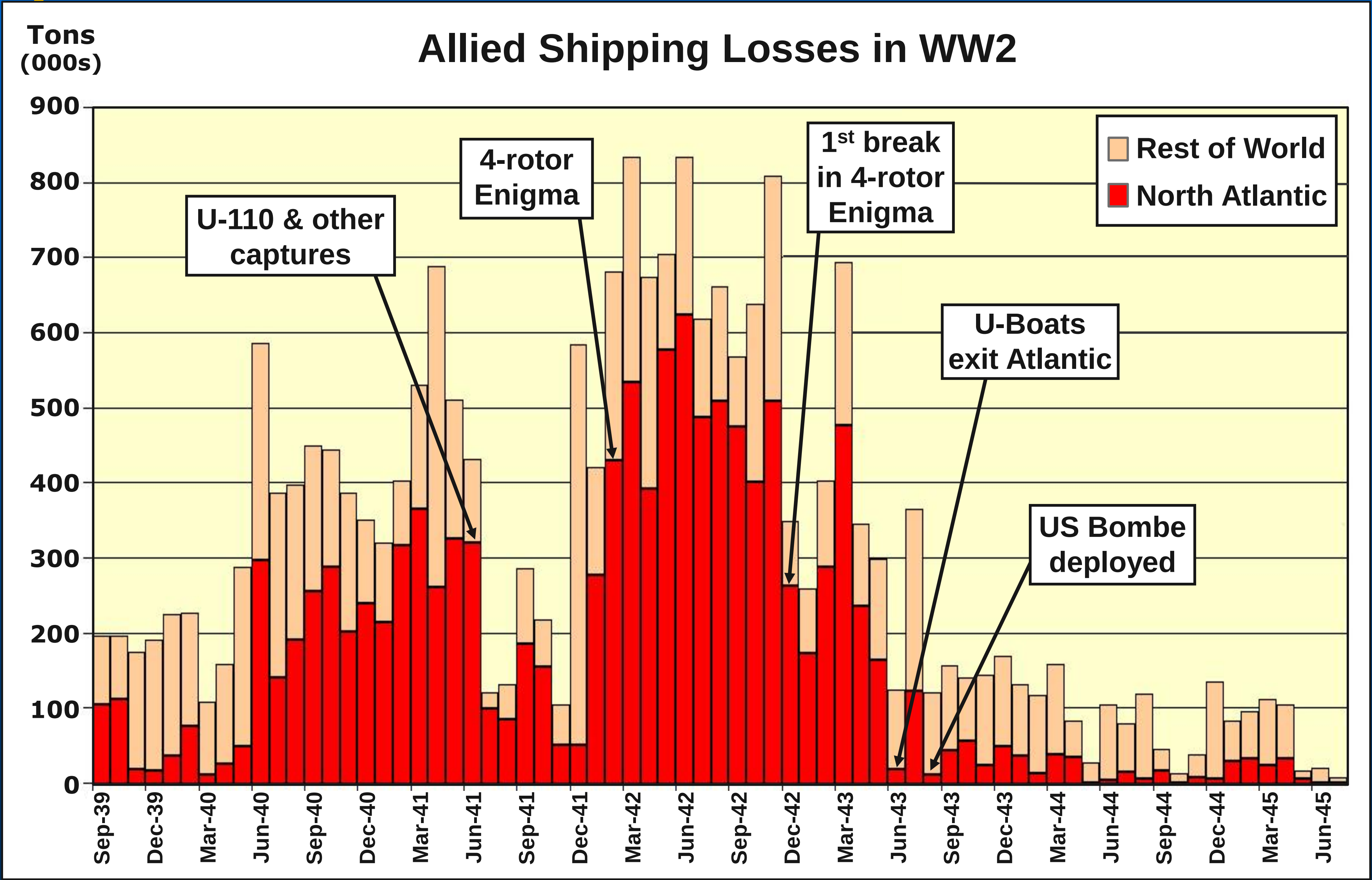
- After breaking Naval Enigma, the British continuously re-routed convoys to avoid U-boats
- Unarmed weather trawlers carried Enigma, a recurring target for more code books
- British targeted supply ships and mother U-boats
- Early U-boat success turned to failure, 725 of 1155 U-boats and 82% of 35,000 sailors never returned from sea

US bombing of U-117 – Aug. 1943

Photo credit: US National Archives

- Some estimate breaking the Enigma shortened WW2 by 2 years

Allied shipping losses vs codebreaking



Did Germans know Enigma was broken?

- Allies only exploited Enigma messages after deception of traditional sources: (spotter planes, spies, etc.)
- But, Allied codebreaking should have been suspected:
  - 5 ships, from one Enigma message, all sunk in 2 days!
  - Supply convoy for Gen. Rommel in Africa found and sunk, despite continuous cloud cover from Naples to Africa
- Was 4-rotor Enigma designed to counter UK codebreaking?
  - No, more likely security from other Nazi military or spies
  - Confirmed in interview with Admiral Dönitz in 1974

Admiral Dönitz inspects U-boat at Saint-Nazaire, France

Photo credit: Bundesarchiv

Enigma after WW2

- Codebreaking success was kept secret for 41 years, until 1974, despite thousands who knew the secret in the US and UK
- US and UK encouraged use of Enigma by other countries, including Allies, reading their secret messages for 3 decades
- About 35,000 Enigmas were manufactured
- Today, about 380 Enigma machines are known to exist, half in museums, half in private collections

Photo credit: US Navy release

David Hatch, NSA Historian, tells story of US Navy missile test, sinking "pallets" of Enigma machines

(pallet = 150 Enigmas = 2 tons)

Enigma prices

Enigma prices doubled after release of movie, “The Imitation Game” on Christmas, 2014

Benedict Cumberbatch operates Enigma from movie, “The Imitation Game”

Photo credit: StudioCanal

- In June 2017, a professor of cryptology found a “typewriter” in a Romanian flea market
- He knew it was an Enigma and bought it for 100 Euros
- Immediately sold on Romanian auction site for 45,000 Euros
- Sold 4 months later in US by Rau Antiques for $245,000
- Rarity plus interest generate record prices at auction:
  - $441K for a 3-rotor Enigma at Sothebys on 4/30/21
  - $860K for a 4-rotor Enigma at Sothebys on 12/17/19

Download this presentation

CipherHistory.com/enigma.pptx

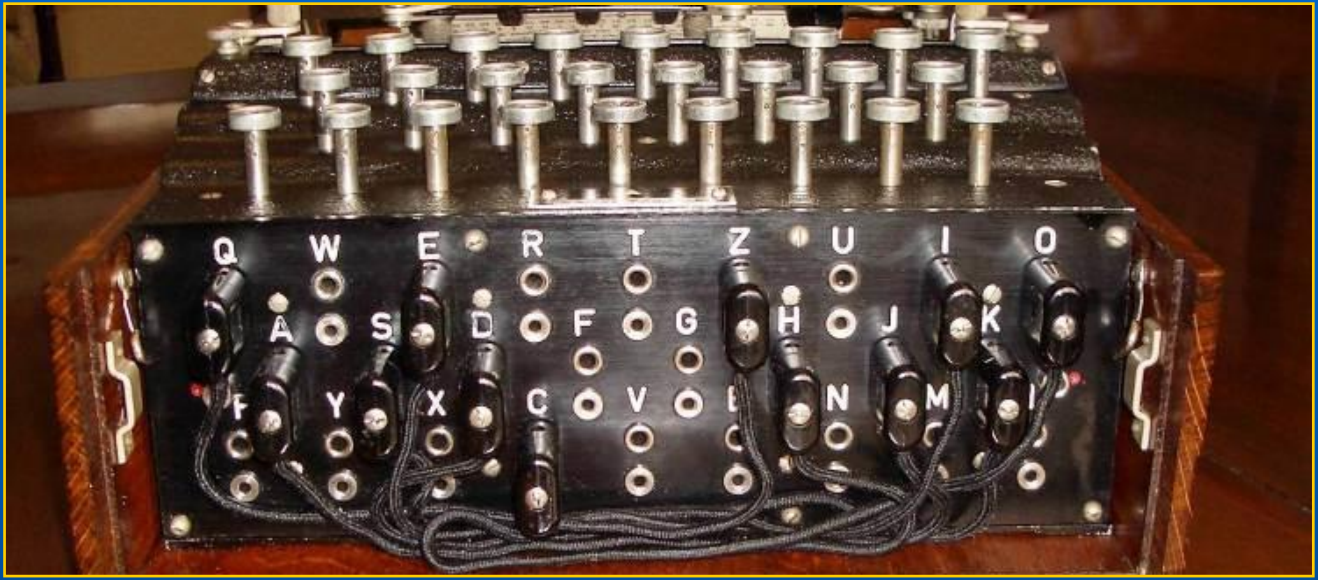
Cipher History Museum

Addendum

The following pages show the mathematics of the Enigma key space, both theoretically and as implemented by the Nazis

Plugboard settings

- The German military addition of the plugboard added more key space than the rotors



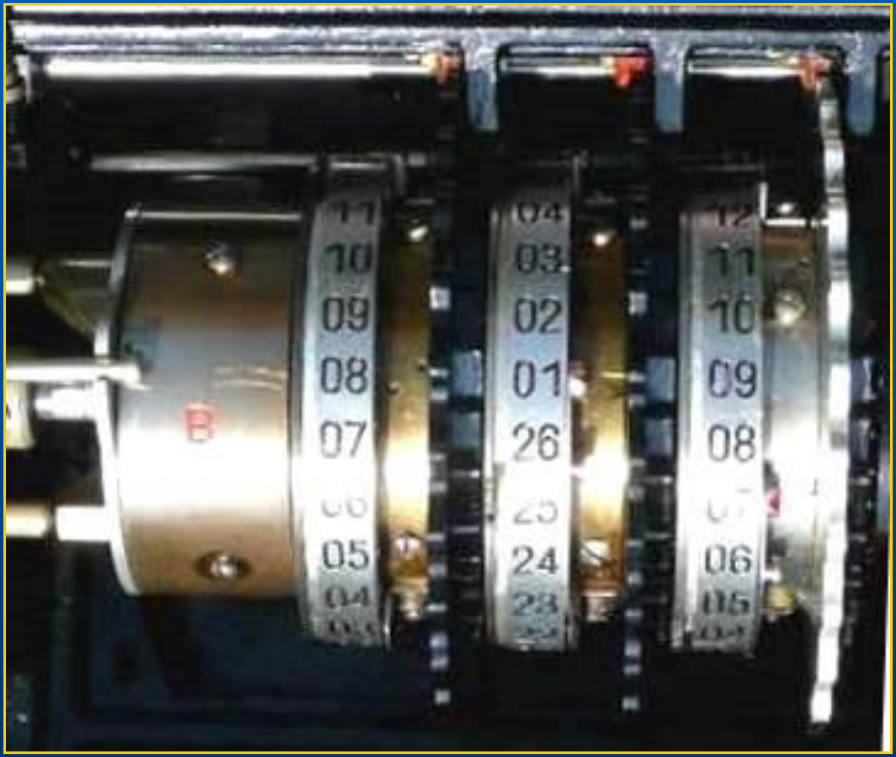
- The # of possible plugboard settings is a function of 3 variables:
    1. # plugboard cables, p, can be from 0 to 13
    2. # of groupings of possible plugged letters (2p letters out of 26) = 26! / ((2p!) X (26-2p)!)
    3. # interconnections of letters within each group of plugged letters chosen from #2 = (2p-1) X (2p-3) X (2p-5) X …X 1
- The 3 items above are calculated on the next slide

Plugboard settings

1. # plugboard cables	2. # groupings of plugged letters 26! / ((2p!) X (26-2p)!)	3. # interconnections for each set of plugged letters (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

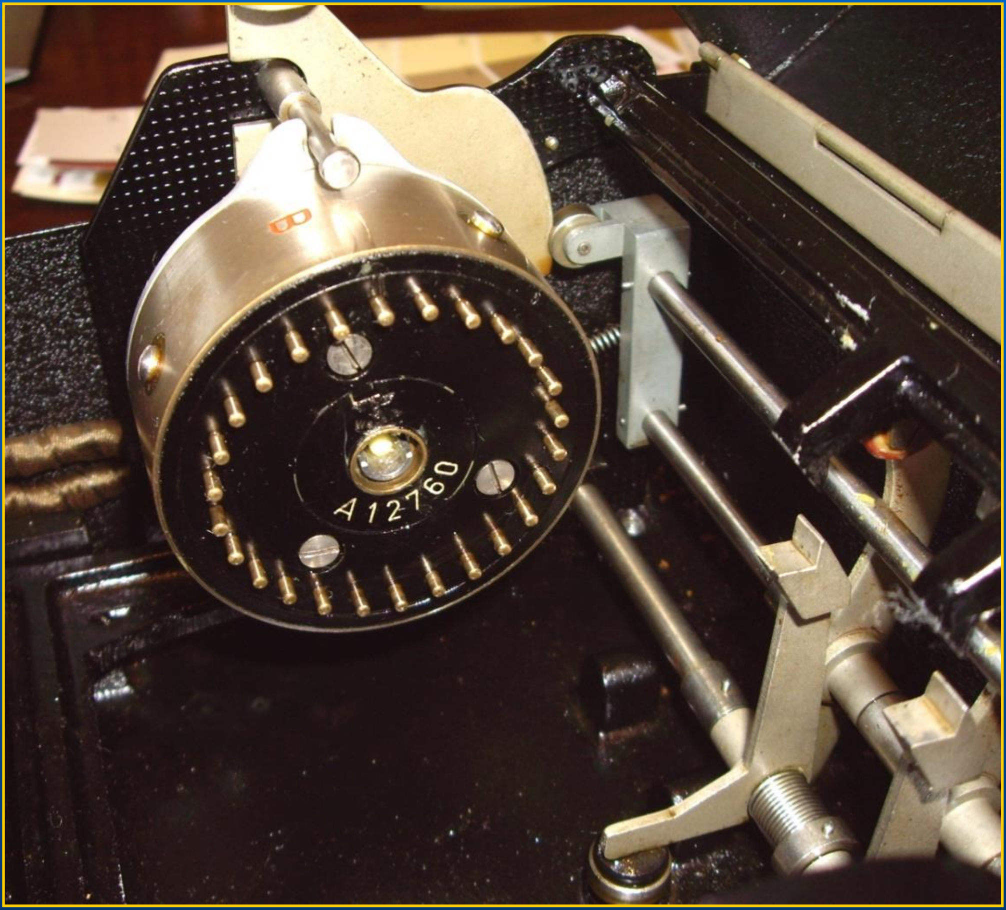
Rotor settings

- The internal wiring of each rotor could be arranged in 26! different combinations. Since only 3 rotors are used, the number of combinations when selecting 3 unique rotors out of 26! is:
  - 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 be set to any letter:
  - 26 X 26 X 26 = 17,576



- The rotors advance like an odometer, the setting to enable this is a notch set to any letter of the alphabet:
  - 26 X 26 = 676 (Note: notch on left-most rotor has no effect)

Reflector settings



- The reflector scrambles the letters in pairs so it could encrypt or decrypt with the same setting
- 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 23)
  - 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 X 10^{114}
- This number is far greater than the total number of atoms in the observable universe (10^{80})

Webb Space Telescope view of cartwheel and spiral galaxies

Photo credit: NASA, ESA, CSA, STScI

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 fixed rotors were issued out of 26! possibilities. Since the wiring was known, 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 X 10^{23}
  - 1.07 X 10^{23} is equivalent to a 76 bit key, better than 56 bit DES, the first PC standard in use until 2001

Enigma codebreaking example

- Germans considered the Enigma to be unbreakable
- Before computers, a brute force attack was impossible:
  - To test 10^{23} key settings:

If 100,000 Enigma operators could each check
one key setting every second, 24X7…

It would take twice the age of the universe to break the code!

- Each U-boat, Air Force, and Army unit had separate keys, which changed daily!
- The British Bombe did not perform brute force attacks but searched for possible cribs to decode the rotors only
- The plugboard, which gave more key space than the rotors, was manually, and easily, decoded