# ISC

(BTech III Jan-April 2024)
Week#6 – Feb 9, 2024

Dhiren Patel

# One Time Pad - Vernam

- One time pad (of ASCII text) can be easily extended to binary data by using a one-time pad of key bits and XOR operation  (same as Vernam cipher – with non repeating random key).
- To decrypt, XOR the cipher-text with a string from an equivalent copy of the one-time pad. Everything else remains the same and security is just as perfect as there are no patterns or regularities that a cryptanalyst can use to attack.
- Problems associated with key generation (truly random), key distribution, and perfect synchronization between the sender and receiver(s).

# Book cipher (WW I – British)

- A simple version of such a cipher would use a specific book as the key, and would replace each word of the plaintext by a number that gives the position where that word occurs in that book.
- For example, if the chosen key is H. G. Wells's novel The War of the Worlds,
- the plaintext "all plans failed, coming back tomorrow"
- could be encoded as "335 219 881, 5600 853 9315"
- since the 335th word of the novel is "all", the 219th is "plans", etc.
- This method requires that the sender and receiver are using the exact same edition of the key book.
- King James Bible was extensively used

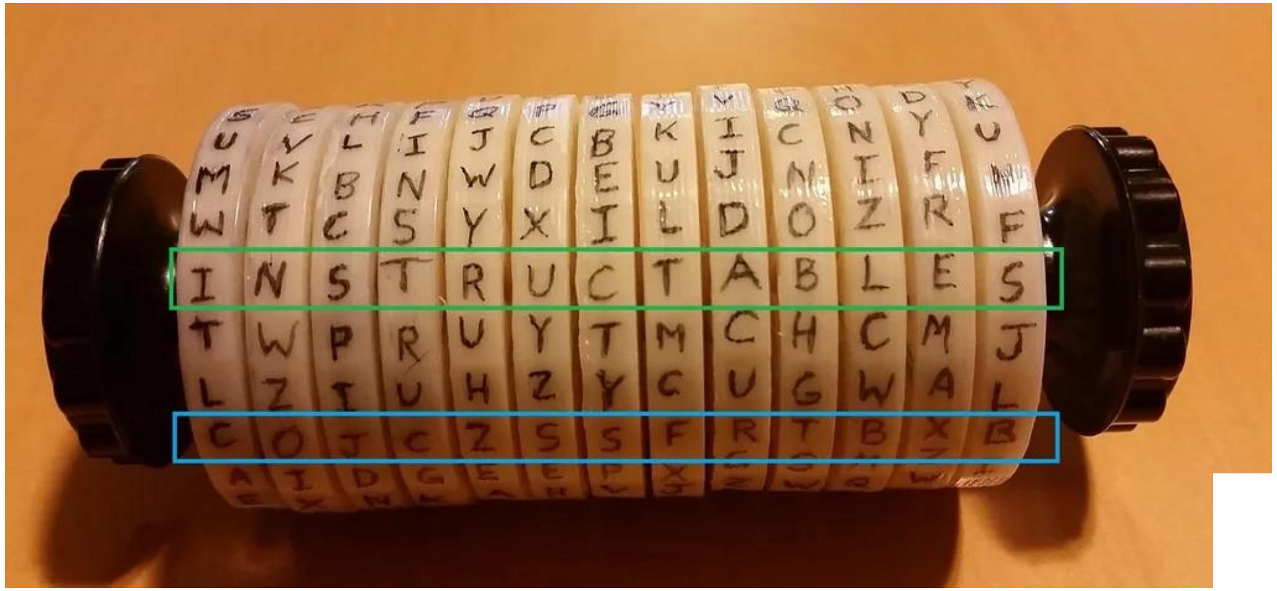
# Machine ciphers (next slide)

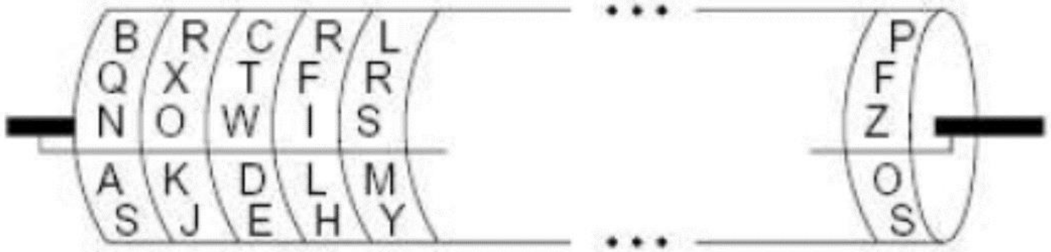
Book cipher - Curious people – Google “Beale ciphers”

<Treasure Hunt of tons of Gold and Silver in USA>

# Wheel Cypher (Cipher)

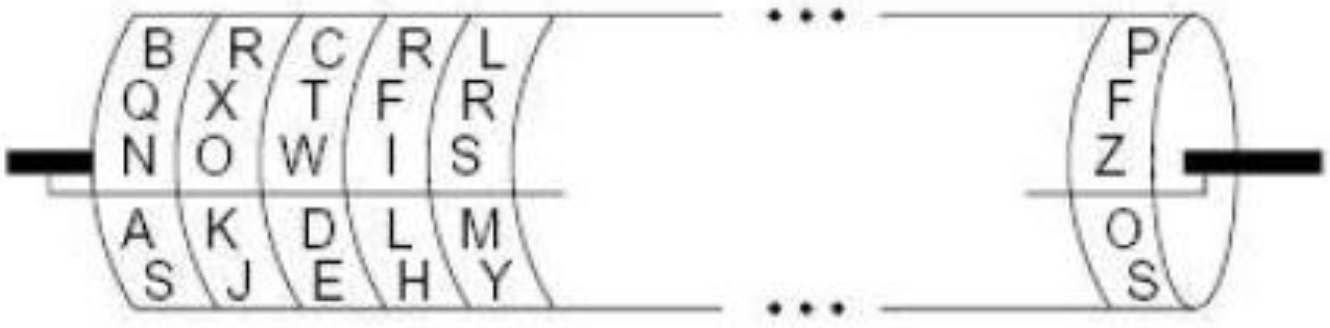
- The Jefferson disk, also called the Bazeries Cylinder or wheel cypher as named by Thomas Jefferson (1743-1826) – 3rd POTUS 1801-1809





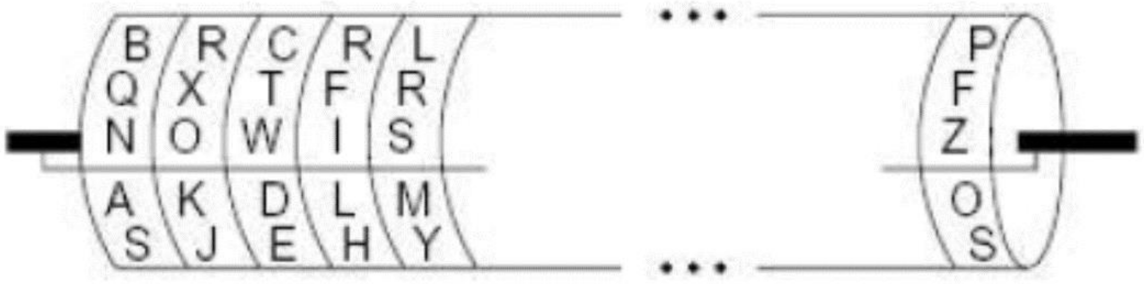
# Machine cipher (Mechanical)

- The *Jefferson cylinder* implements a poly-alphabetic substitution cipher while avoiding complex machinery, extensive user computations, and Vigenère table.
- A solid cylinder 6 inches long is sliced into 36 disks. A rod inserted through the cylinder axis allows the disks to rotate. The periphery of each disk is divided into 26 parts.



# Jefferson Cylinder

- On each disk, the letters A–Z are inscribed in a (different) random ordering.
- Plaintext messages are encrypted in 36-character blocks.
- A reference bar is placed along the cylinder's length.
- Each of the 36 wheels is individually rotated to bring the appropriate character (matching the plaintext block) into position along the reference line.
- The 25 other parallel reference positions then each define a ciphertext, from which, one is selected as the ciphertext to transmit.

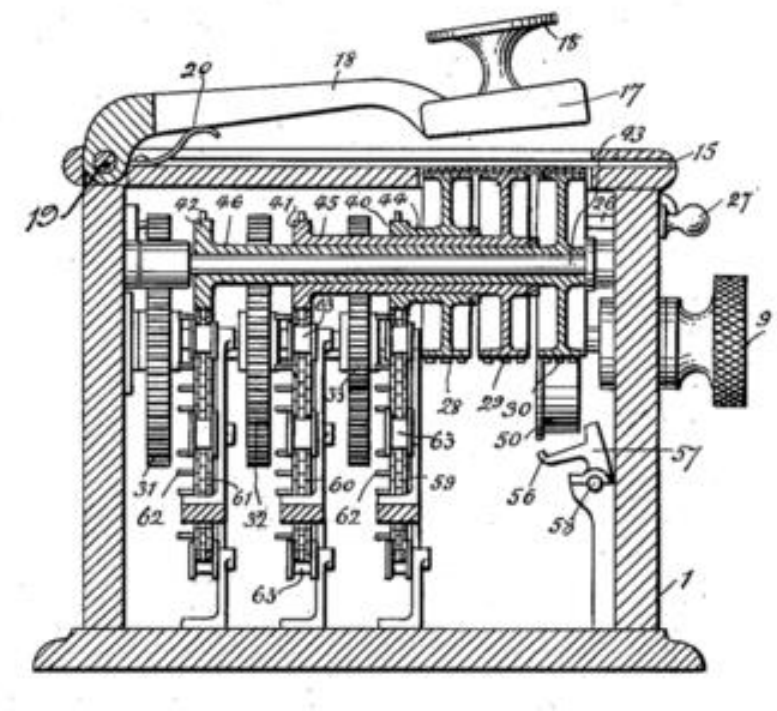


# Jefferson cylinder

- The ciphertext is decrypted by rotating each of the 36 disks to obtain characters along a fixed reference line matching the ciphertext.
- The other 25 reference positions are examined for a recognizable plaintext.
- Reordering disks (1 through 36) alters the polyalphabetic substitution key.
- The number of possible orderings is 36! ≈ 3.72 x $10^{41}$
- Both parties may agree beforehand on an index 1 through 25 specifying the offset between plaintext and ciphertext lines (or use additional shift cipher) to defeat an enemy with identical cylinder.

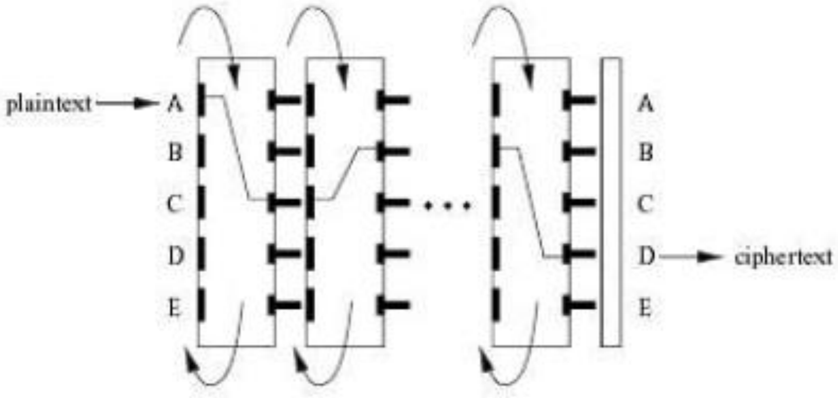
# Caesar cipher and Hill Machine cipher

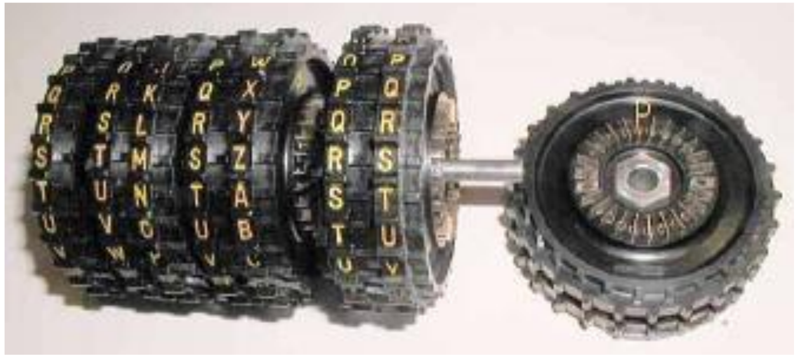
- Patented "Hill-Cipher Machine" in 1931, which performed matrix multiplication using gears and chains



# Rotor machines

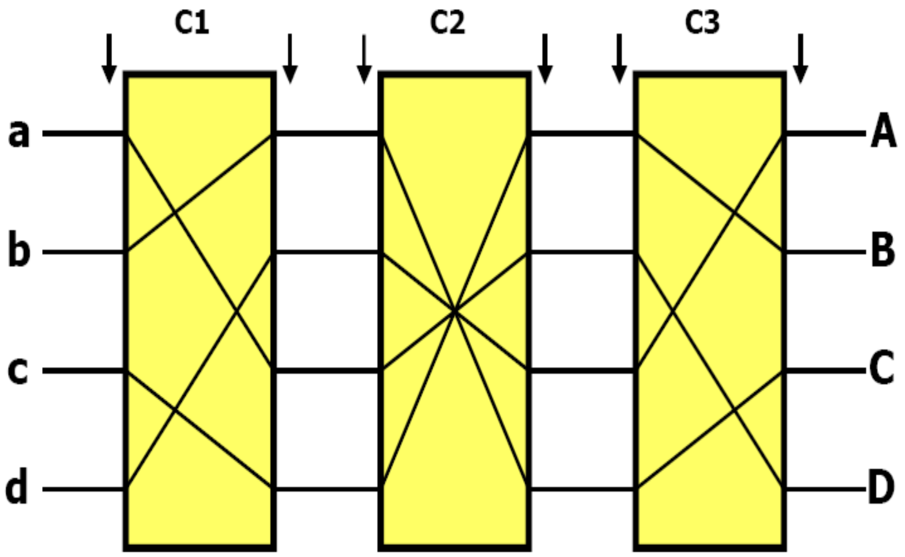
- a disk with electrical contacts on either side, known today as a rotor
- A plaintext character input to the first rotor generates an output which is input to the second rotor, and so on, until the final ciphertext character emerges from the last.
- A generic rotor machine consists of a number of *rotors* (*wired codewheels* through which electric pulses can flow) each implementing a different fixed mono-alphabetic substitution



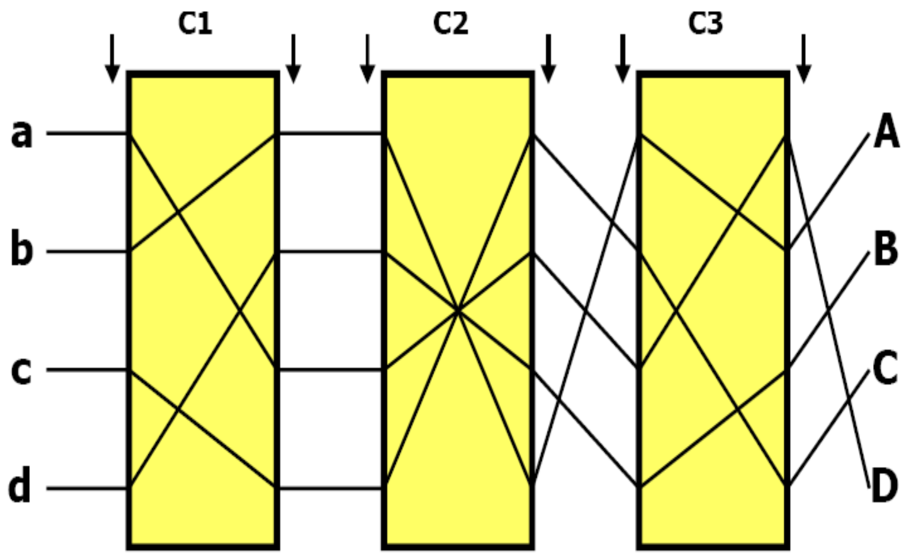


# Rotor machines

- provide polyalphabetic substitution
- Internal cross-connections, providing a substitution using a continuously changing alphabet
- The cipher key is defined by the fixed wheel wirings and initial rotor positions
- Two properties desirable for security are: (1) long periods; and (2) state changes (concerns the motion of rotors relative to each other).

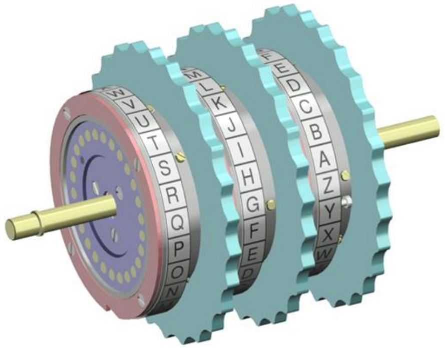


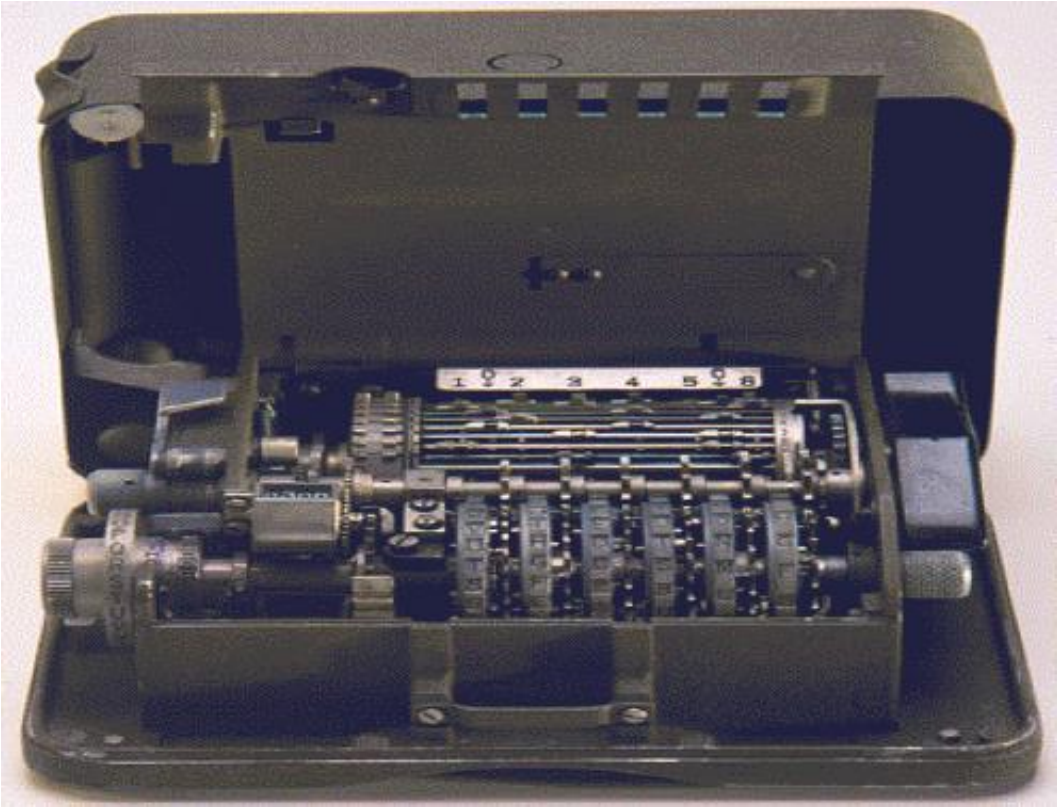
This setting maps: a→D, b→C, c→B, d→A



This setting maps: a→D, b→A, c→C, d→B

# Enigma and M209 Cipher





# Enigma

- The Enigma machine is a cipher device developed and used in the early-to mid-20th century to protect commercial, diplomatic, and military communication.
- invented by German engineer **Arthur Scherbius** in 1918.
- It was employed extensively by Nazi Germany during World War II, in all branches of the German military.

# Enigma Design

- Three rotors: These were the heart of the Enigma, each with 26 electrical contacts representing letters. As characters were typed, the rotors rotated, scrambling the electrical path and substituting the letter.
- Reflector: After passing through rotors, the signal hit the reflector, changing its direction and sending it back through the rotors in a different order, further increasing complexity.
- Plugboard: Additional scrambling could be achieved by manually plugging pairs of letters, swapping their encodings before entering the rotors.

# Enigma operations

- Key settings: Each message required unique settings for the initial rotor positions, rotor order, and plugboard connections. These settings, determined by codebooks, dictated the specific scrambling applied.
- Message encryption: Each keystroke sent an electrical signal through the rotors, transforming the letter based on the current rotor positions. The scrambled signal then passed through the reflector and back through the rotors, resulting in the ciphertext letter displayed on the machine.
- Message decryption: The same key settings were used to reverse the process, recovering the original plaintext message.

# Enigma - Security and Weaknesses

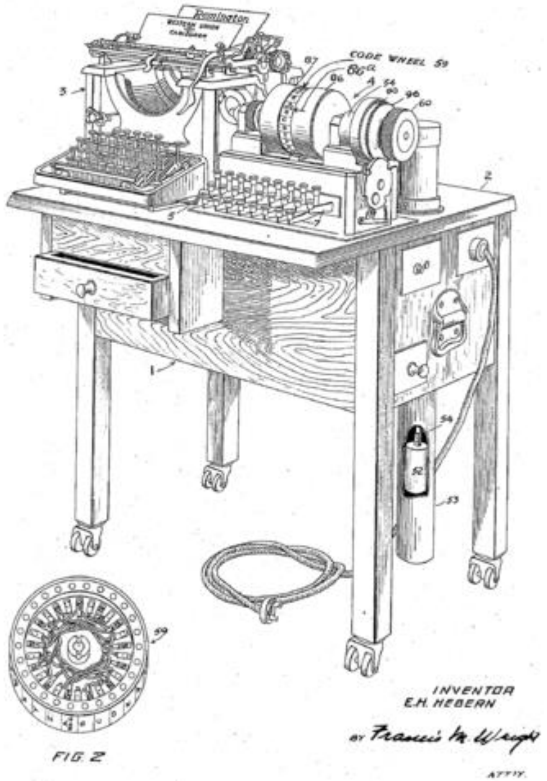
- Polyalphabetic substitution: Enigma used a different substitution for each letter based on constantly changing rotor positions, making it much harder to crack.
- Weaknesses: Despite its complexity, the Enigma had vulnerabilities. Repetitive use of certain indicators, operator errors, and limited rotor combinations (compared to theoretical possibilities) provided opportunities for codebreakers.
- Polish and British efforts: Polish mathematicians first broke the Enigma in the 1930s, sharing their insights with the British. Alan Turing and his team at Bletchley Park further developed cryptanalysis techniques, ultimately enabling them to decipher vast amounts of German communication.

# Imitation Game (movie 2014)

- 1939, Alan Turing travels to Bletchley Park UK. Under the direction of Commander Alastair Denniston, he joins the cryptography team. The team analyze the Enigma machine, which the Nazis use to send coded messages.
- They could successfully decrypted 2 msgs per minute.
- Breaking Enigma played a huge role in ending the World war II.

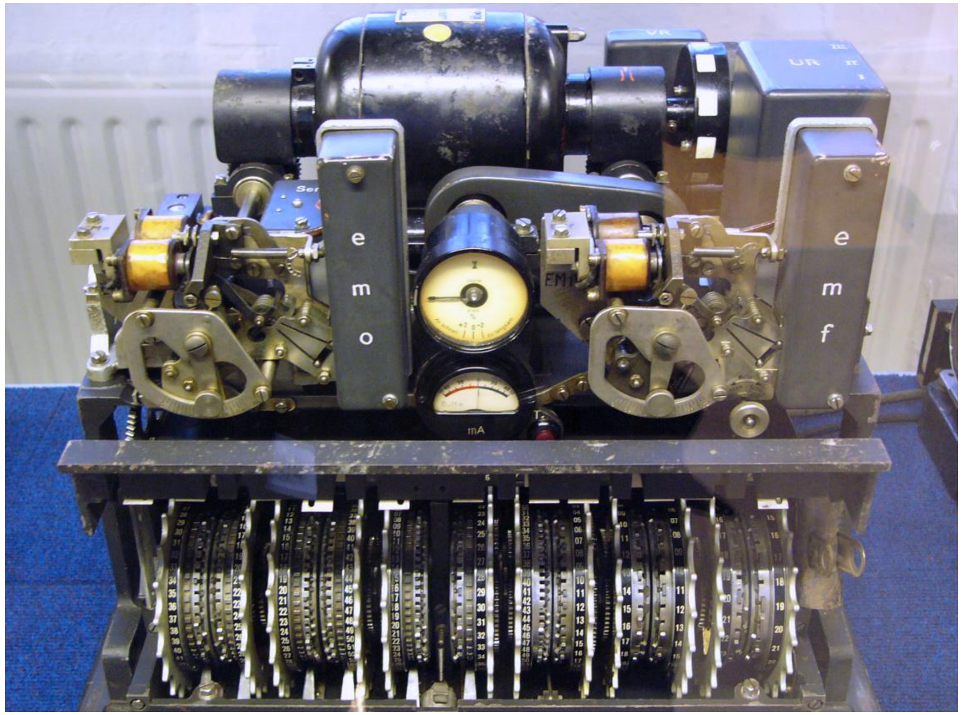
# The Hebern Rotor Machine (USA) (Edward Hebern - 1917)

- The Hebern Rotor Machine was an electro-mechanical encryption machine built by combining the mechanical parts of a standard typewriter with the electrical parts of an electric typewriter, connecting the two through a scrambler.



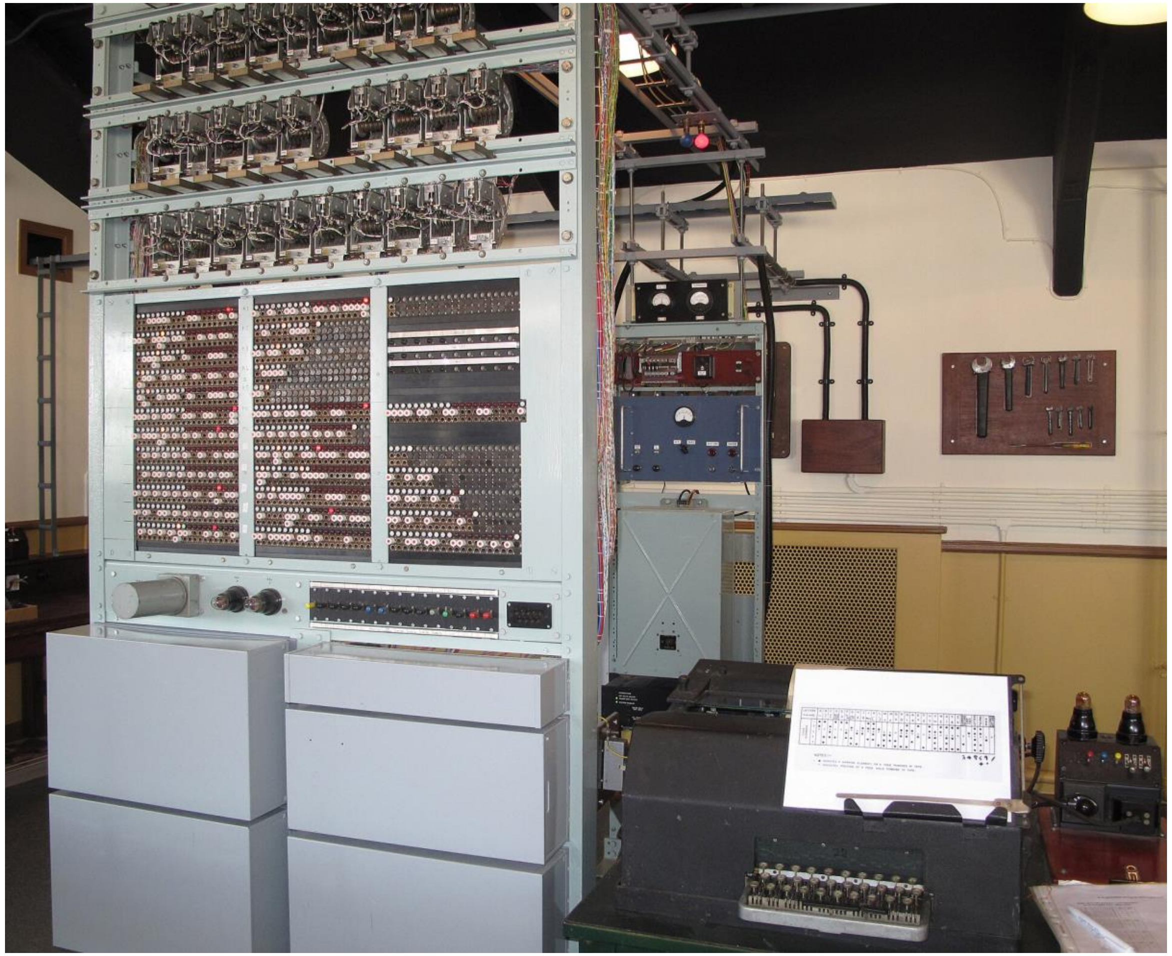
# Lorenz SZ 42 Rotor machine
(C. Lorenz AG in Berlin during World War II)

- Unlike the Enigma, which used rotors for substitution, the SZ 42 implemented a stream cipher using complex clockwork mechanisms. This offered greater theoretical security but also increased mechanical complexity.



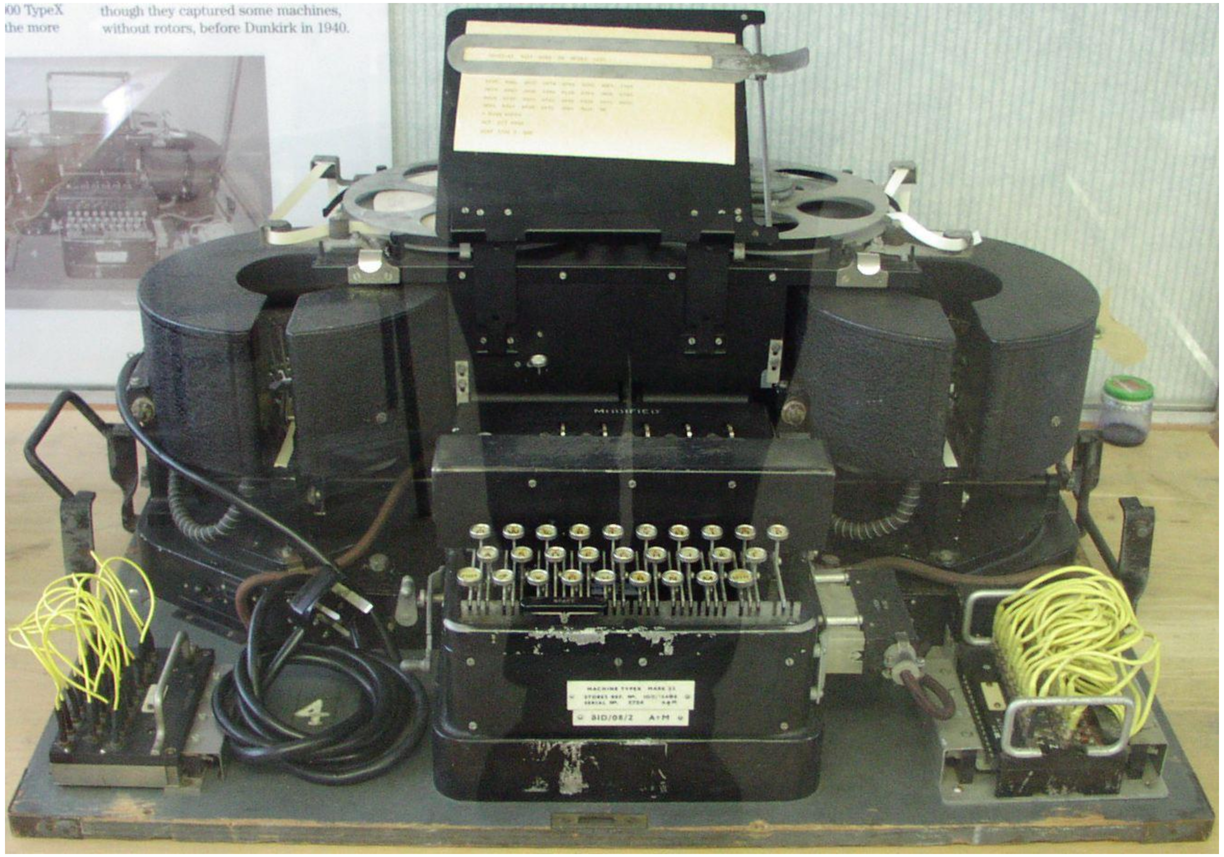
# Lorenz SZ Breaker – Bletchley Park UK

- emulated the functions of the Lorenz SZ40/42, producing printed cleartext from ciphertext input



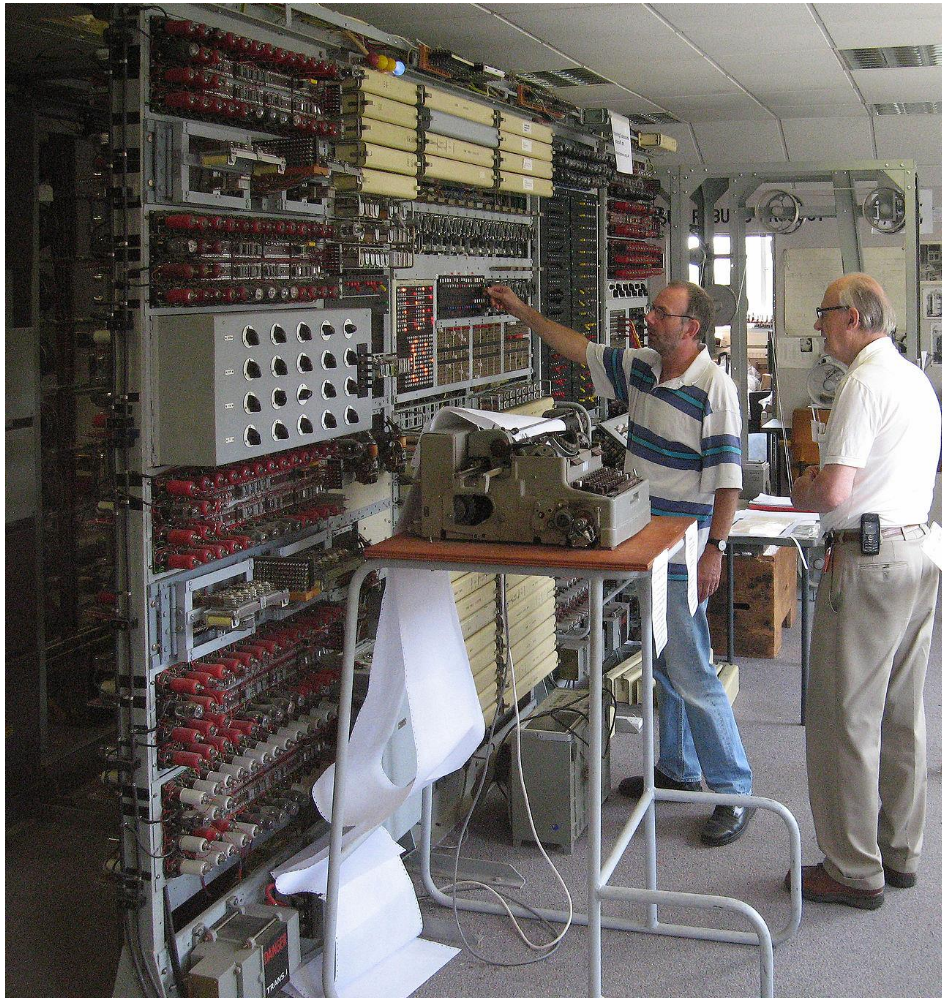
# Typex ERC (Enigma Replacement Cipher) 1937 (Designed by the British during World War II)

- It was an adaptation of the commercial German Enigma with a number of enhancements that greatly increased its security.
- Increased security features like five rotors and a plugboard with more connections. However, it also suffered from its share of mechanical complexities.


00 TypeX
the more
though they captured some machines,
without rotors, before Dunkirk in 1940.
4

# Colossus (Mark II) at Bletchley Park

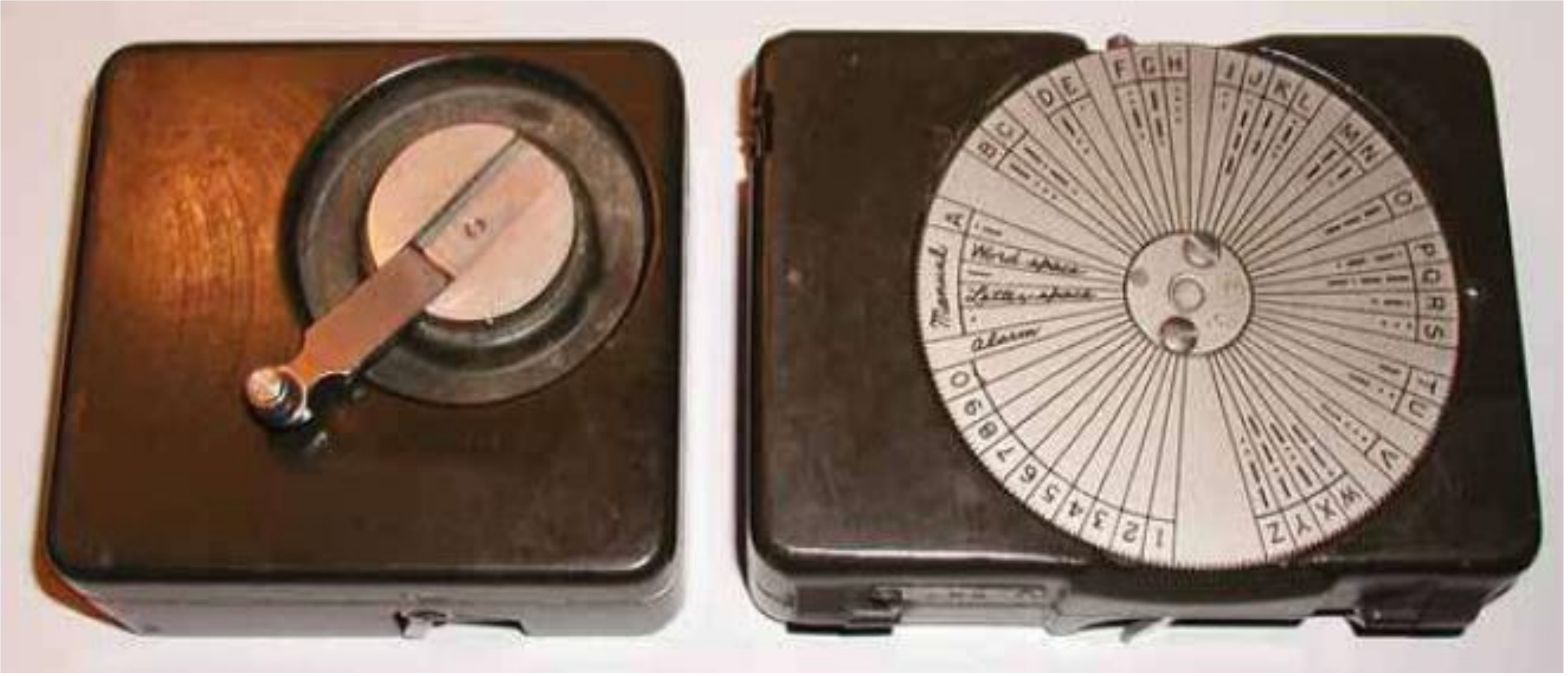
- Code breaker computer



# Rotor Machines

1. In *indicating machines*, ciphertext output characters are indicated by means such as lighted lamps or displayed characters in output apertures.
2. In *printing machines*, ciphertext is printed or typewritten onto an output medium such as paper.
3. With *on-line machines*, output characters are produced in electronic form suitable for direct transmission over telecommunications media.

# Pocket code breaker (with Morse code)



# Security of One Time Pad

- A random key sequence “added” to a nonrandom plaintext message produces a completely random cipher-text message and no amount of computing power can break that.
- Conditional security v/s un-conditional security
- Two time pad – Same key used twice!
- ASCII txt – MSB is always 0 for all printable characters (8 bit)
- Assignment – find out pairs of ciphertext encrypted using the same key
- (output cipher txt is generally written as hex – i.e. for every ASCII plain txt character; there are two hex characters in ciphertext)
- Check MSB of every odd hex characters – this is the key output

# Cyber Threat Hunting

- Cyber threat hunting is a proactive security strategy that seeks to identify and eliminate cybersecurity threats on the network before they cause any obvious signs of a breach.
- Traditional security methodologies and solutions reactively detect threats, often by comparing threat indicators (like the execution of unknown code or an unauthorized registry change) to a signature database of known threats.

# Cyber Threat Hunting

- Examples of threat hunting techniques include:
- Searching for insider threats, such as employees, contractors or vendors.
- Proactively identifying and patching vulnerabilities on the network.
- Hunting for known threats, such as high-profile advanced persistent threats (APTs).
- Establishing and executing incident response plans to neutralize cyber threats.

# Why?

- Traditional, reactive cybersecurity strategies focus primarily on creating a perimeter of automated threat detection tools, assuming that anything that makes it through these defenses is safe.
- If an attacker slips through this perimeter unnoticed, perhaps by stealing authorized user credentials through social engineering, they could spend months moving around the network and exfiltrating data.
- Unless their activity matches a known threat signature, reactive threat detection tools like antivirus software and firewalls won’t detect them.