

In Search of the World's Oldest Surviving Cipher Devices



May 1, 2020



Ralph Simpson

Ralph@CipherHistory.com

Copyright © 2022
CC Attribution 4.0 International

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

Definition

- A “cipher device” will be defined as an apparatus, mechanism, tool, or instrument that performs a cryptographic function
 - Popular and accepted use of the word “device”
 - A Vigenère table, one-time pad, Playfair matrix, code book are not devices
 - Vigenère disk, Cardano grille, skytale are considered cipher devices

The Quest...

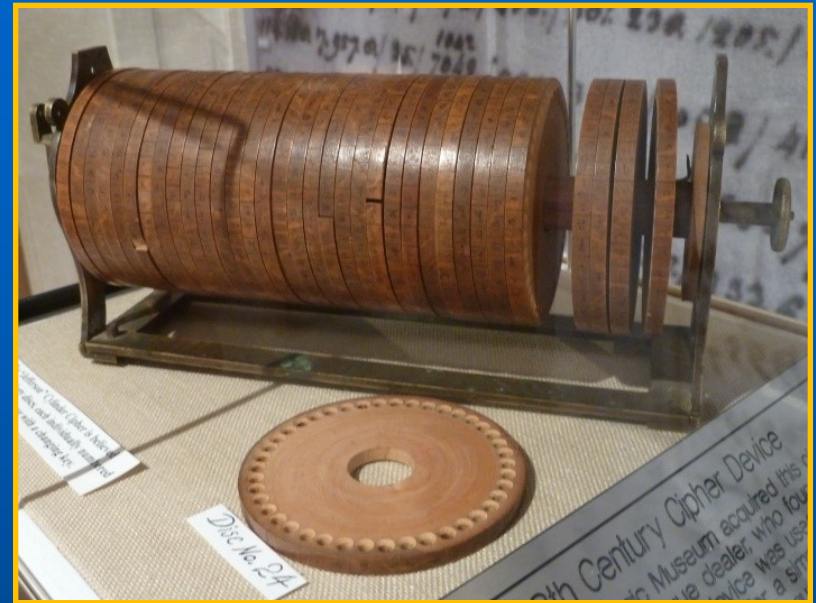
- **A systematic and global search for the world's oldest surviving cipher devices**
 - **No previous searches have been found**
 - **Seems like a fool's errand**

...and the Problem

- **Cryptologic tradition is to keep all devices & methods secret**
 - Only portion of one Japanese Purple cipher from WW2 exists
 - 360 out of 40,000 Enigma machines exist
 - 5 Confederate cipher disks exist
 - 1 Jefferson Wheel Cypher exists
 - German WW1 invisible ink recipes finally disclosed by CIA in 2011
- **Old cipher devices may be mis-identified or discarded**
- **Oldest devices saw limited use, by kings, military leaders, ambassadors, etc., so few were made and kept secret**

Oldest Device at NSA?

- Thomas Jefferson invented his “Wheel Cypher” in about 1795
- Reinvented twice, used by US until WW2
- Only one existing example, in the NSA Museum in Ft. Meade, MD
- NSA claim: "the oldest true cipher device in existence in the world"



18th Century Cipher Device

The National Cryptologic Museum acquired this cipher device from a West Virginia antique dealer, who found it in a home near Monticello. This cipher device was used to encipher the French language. A description for a simplified version of the device to be used for the English language has been found in Jefferson's papers and has become known as the "Jefferson Cipher Wheel". Although Jefferson may have used it while Ambassador to France, a direct connection to Jefferson of the device exhibited here remains unproven.

This particular artifact is thought to be the oldest true cipher device in existence in the world.

Nicholas Bion Cipher Disk



- Found and owned by Nick Gessler
- Vigenère cipher disk originally invented in 1466-7
- Disk above made by Nicholas Bion (1652-1733) of France
- Bion was instrument maker for King Louis XIV (1638-1715)
- This device is likely from 1680-1715, 100 years older than NSA's Jefferson Wheel Cypher

Systematic Search

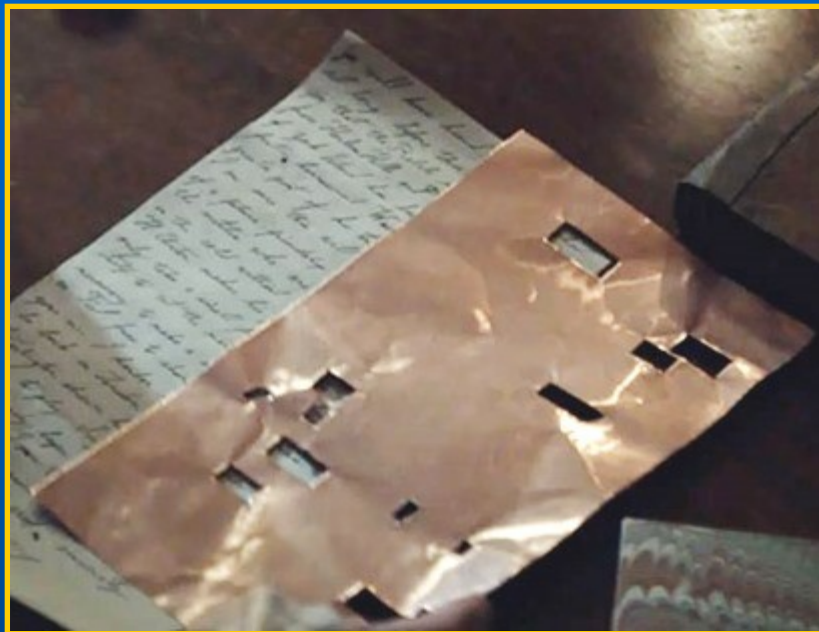
- **What are the earliest types of cipher devices?**
 - **Scytale**
 - **Cardano grille**
 - **Cipher disks**
- **Global search**
 - **China, Japan use thousands of characters, not compatible with cipher devices**
 - **India used ciphers, transposition and steganography**
 - **Arabic world discovered letter frequency analysis in 800s CE and used astrolabs, but no writings of early cipher disks**
 - **Africa left no evidence of cryptology outside Egypt, Arabic areas**
 - **Europe likely is the area of focus**

Scytale

- Stick or cylinder with ribbon of parchment wrapped around it
- Message written along length of stick in rows
- Receiver needs same size stick to read the message
- Transposition cipher
- First mention of scytale from 7th century BCE in Greece
- Since they would not appear to have significance, no early artifacts exist in our museums



Cardano Grille



- Invented by Girolamo Cardano (1501-1576) in 1550
- Holes cut in metal or paper sheet to write in a secret message
- Rest of page is filled in with ordinary looking letter
- Combination of transposition cipher and steganography
- Grilles carefully protected, no early examples known to exist

Cipher Disks

- Astrolabes invented over 2000 years ago
- Disks used to calculate motion of heavenly bodies
- Antikythera mechanism has 30 meshed gears for calculating motion of sun, moon, planets c.250-100 BCE

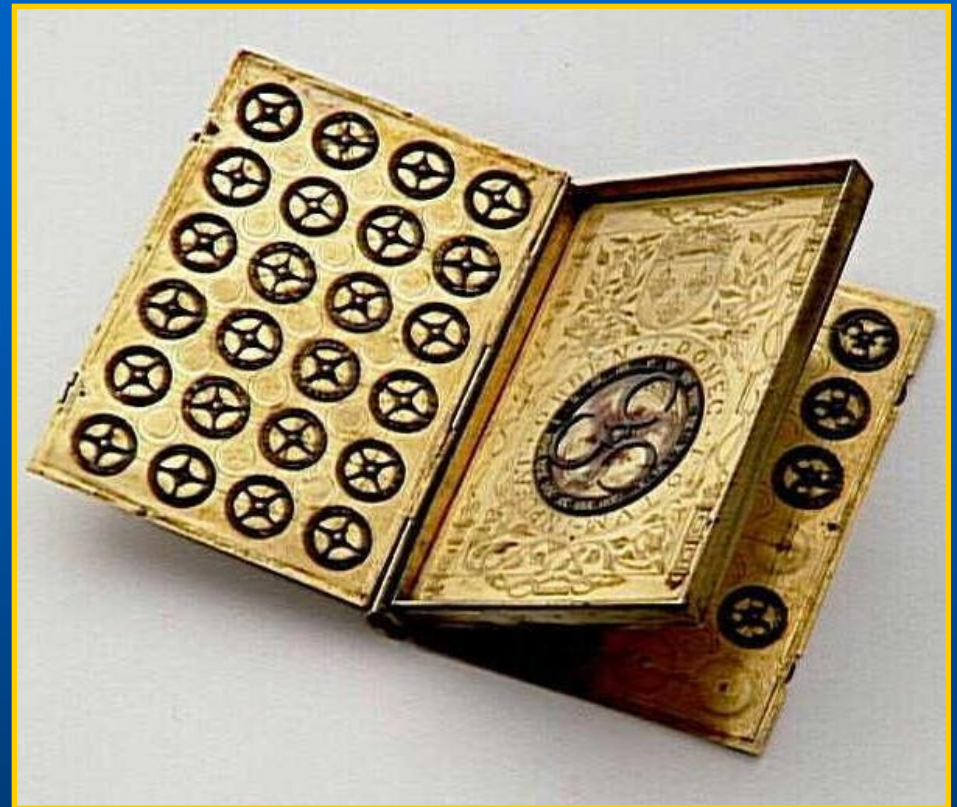
Alberti disk from 1466 document



- Ramón Llull (c.1232 - c.1316) introduced volvelle from Arabic world in 1274
- First disk to have evidence of use as a cipher device was 1466 invention of Alberti disk

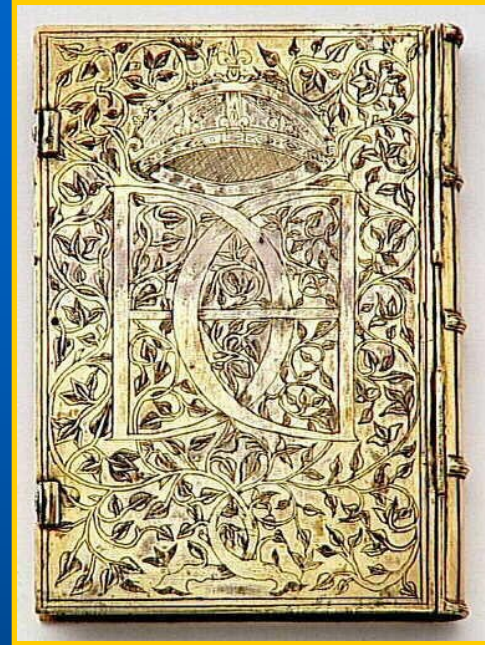
King Henry II Cipher Device

- French King Henry II (1519-1559)
- Engraved brass cipher device in shape of 4 page book with 50 cipher disks
- Henry II reign 1547-59
- Polyalphabetic cipher, but not of the Alberti style
- In French museums for 180 years, but mis-identified as an astronomic device until 2014
- Now identified as the world's oldest cipher device!



Pages 1&2, similar to pages 3&4

King Henry II Cipher Device

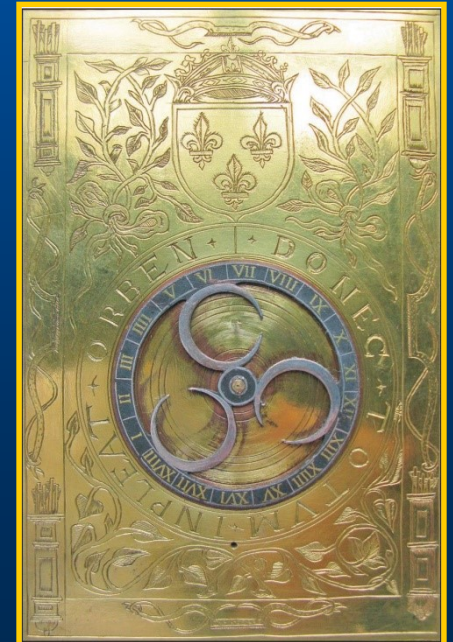


Front & back covers



Pages 3&4

Page 2 details,
with larger
wheel,
numbered I-
XVIII



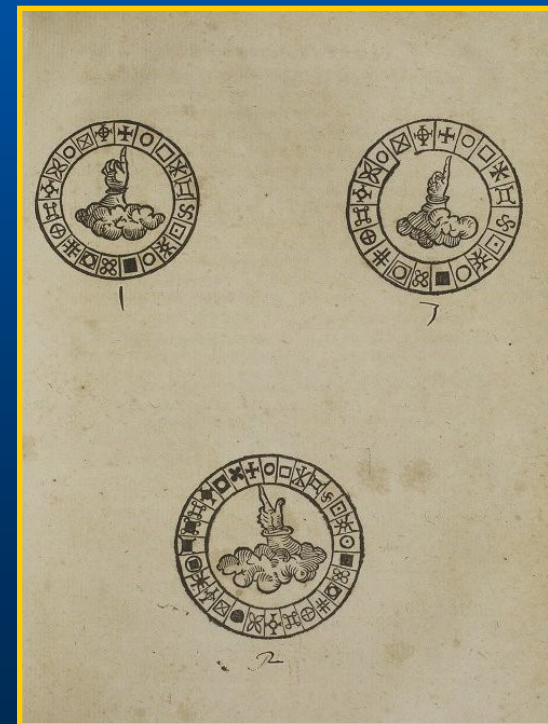
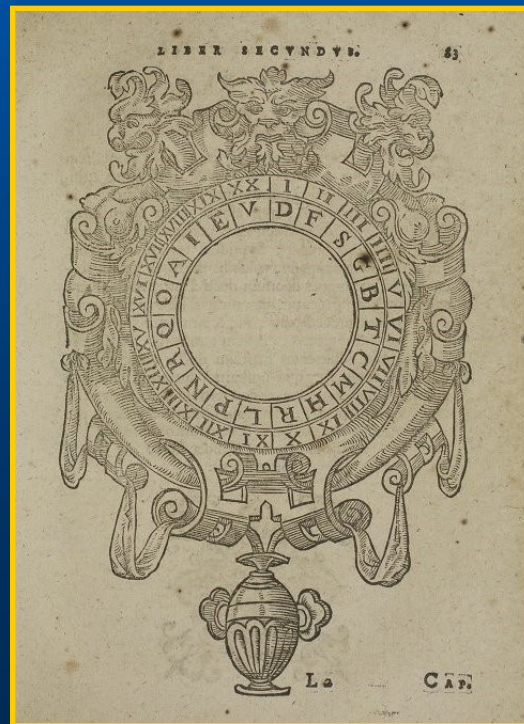
Details of
smaller wheels,
alternate wheels
numbered I-XII
and A-Z plus U



Volvelles

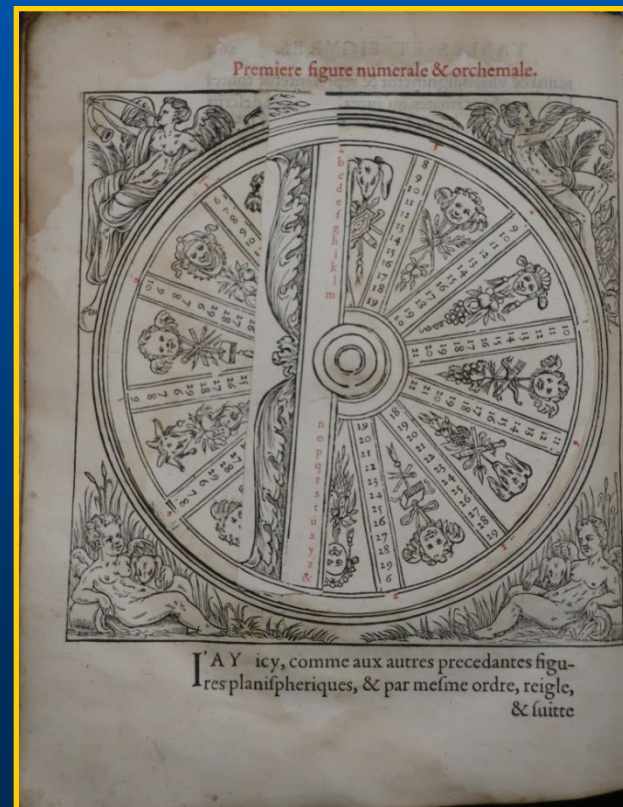
- Paper volvelles were known to be printed in medieval books
- Search through the first printed books on cryptography shows:
 - “Polygraphia” by Johannes Trithemius in 1518
 - “Opus Novum” by Jacopo Silvestri in 1526
 - “*De furtivis Literarum Notis*” by Giambattista della Porta in 1563

della Porta's book has 3 volvelles. The smaller disks would be cut out by the book owner and attached to larger disk by thread



Polygraphia

- “Polygraphia” was first printed book on cryptography, but did not contain volvelles
- Gabriel Collange translated French edition in 1561, contained 13 volvelles, with spokes!
- Later French editions printed in 1571, 1620, 1625



World's Oldest Surviving Cipher Devices

1. 1547-1559 - King Henry II brass cipher device
2. 1561 - "Polygraphia" – 1st French translation
3. 1563 - "De furtivis Literarum Notis"
4. 1571 - "Polygraphia" – 2nd French edition
5. 1591 - "De furtivis Literarum Notis" – pirated edition (false 1563 date)
6. 1593 - "De furtivis Literarum Notis" 2nd edition
7. 1602 - "De furtivis Literarum Notis" 3rd edition
8. 1620 - "Polygraphia" – 3rd French edition
9. 1625 - "Polygraphia" – 4th French edition
10. 1680-1715 - Nicholas Bion silver cipher disk
11. c.1795 - Thomas Jefferson Wheel Cypher

Download this Presentation

Slides: CipherHistory.com/slides/oldestciphers.pptx

Video: CipherHistory.com/video/oldestciphers.mp4

Article: CipherHistory.com/oldestciphers.html

