# 0x101 – Security in History
# Basic Ciphers

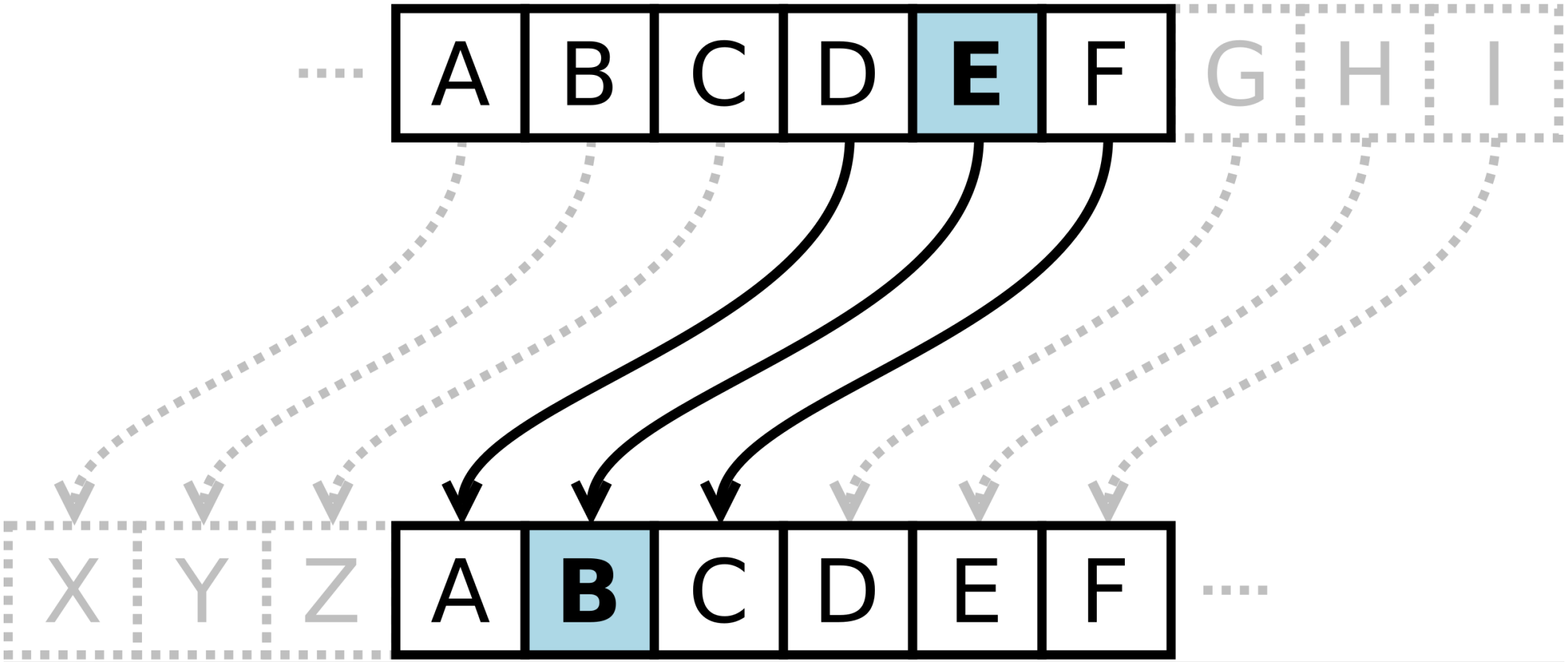
**ECED4406 – Computer Security**


**Dr. Colin O'Flynn**
**Dalhousie University.**

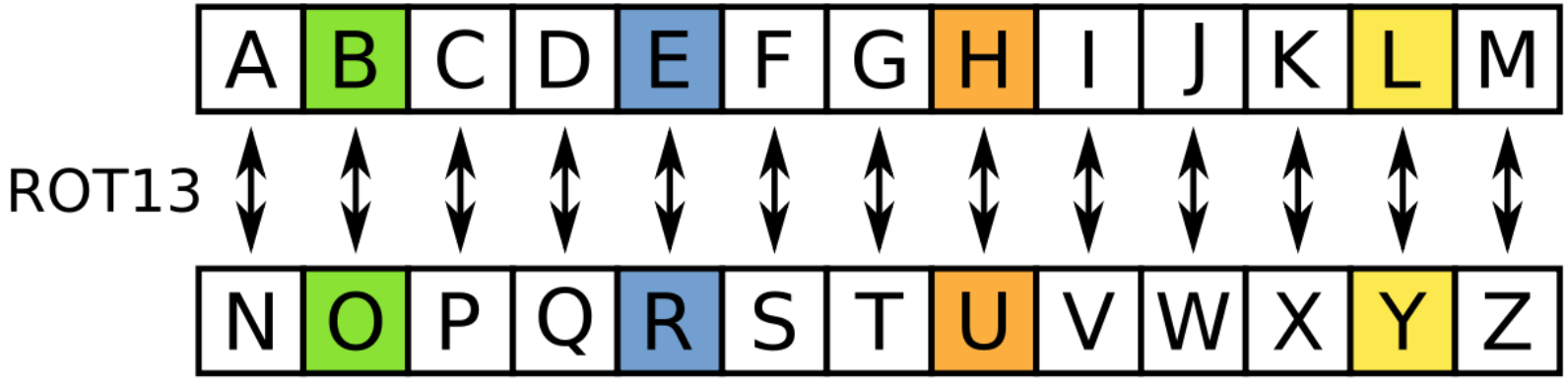
# War

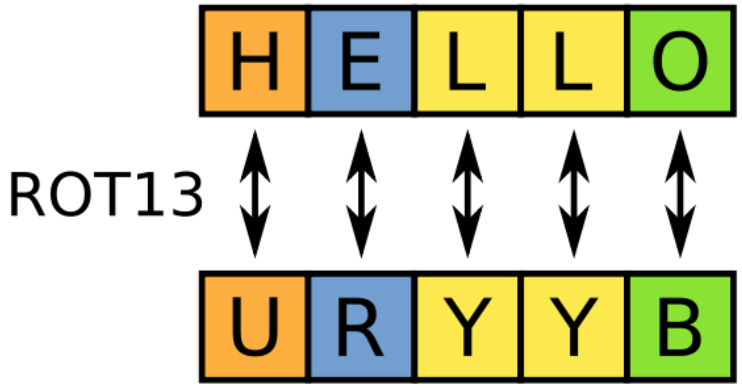
# Scytale Cipher

# Caesar Cipher



# Example: Rotate by 13 places (ROT-13)



# …but that's old right???

## *United States v. Elcom Ltd.*

From Wikipedia, the free encyclopedia

***United States v. ElcomSoft and Dmitry Sklyarov*** was a 2001–2002 criminal case in which Dmitry Sklyarov and his employer ElcomSoft were charged with alleged violation of the DMCA. The case raised some concerns of civil rights and legal process in the United States, and ended in the charges against Sklyarov dropped and Elcomsoft ruled not guilty under the applicable jurisdiction.

Charges laid in the case were trafficking in, and offering to the public, a software program that could circumvent technological protections on copyrighted material, in violation of Section 1201(b)(1)(A)&(C) of Title 17 of the United States Code (the Copyright Acts, including most of the Digital Millennium Copyright Act), as well as Sections 2 (Aiding and Abetting) and 371 (Conspiracy) of Title 18, Part I, of the United States Code (the Federal Criminal Code).

**Contents** [hide]



### Details [ edit ]

Dmitry Sklyarov, a Russian citizen employed by the Russian company ElcomSoft, visited the U.S. to give a presentation called "eBook's Security – Theory and Practice" at the DEF CON convention in Las Vegas, Nevada. On July 16, 2001, as he was about to return to Moscow, Sklyarov was arrested by the FBI and jailed for allegedly violating the United States' Digital Millennium Copyright Act (of 1998) by writing ElcomSoft's Advanced eBook Processor software.[1]

The original issue came to the attention of prosecutors when Adobe Systems, a U.S. company, complained that copy protection arrangements in its e-book file format were being illegally circumvented by ElcomSoft's product. Adobe withdrew its complaint, but United States Department of Justice prosecutors (under the authority of local U.S. Attorney Robert S. Mueller, future Director of the FBI) declined to likewise drop the charges. ElcomSoft's product, and thus presumably the efforts of its employees including Sklyarov, were entirely legal in Russia. Sklyarov was eventually released on bail, but forced to remain in California, separated from his family, until his case concluded.

The day after his arrest several web sites, coordinated from the website *freesklyarov.org*, and mailing lists started to organize protests against his arrest, many of them under the slogan "Free Dmitry" or "Free Sklyarov". The main point of these campaigns was that no DMCA violations were committed at DEF CON, and the DMCA does not apply in Russia, so Sklyarov was being arrested for something that was perfectly legal in his jurisdiction. A campaign to boycott Adobe products was also launched.

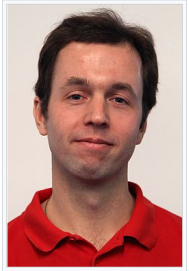
On July 19, 2001, the Association of American Publishers issued a press release announcing their support of his arrest.

After Sklyarov was arrested he was held briefly at the North Las Vegas Detention Center; then he was held in the Oklahoma City Federal Prisoner Transfer Center until August 3, 2001, when he was transferred to the Federal building in San Jose, California. On August 6, 2001, Sklyarov was released on a US $50,000 bail and was not allowed to leave Northern California.

The U.S. government agreed to drop all charges filed against Sklyarov, provided that he testify at the trial of his company. He was permitted to return to Russia on December 13. 2001.

***U.S. v. ElcomSoft and Dmitry Sklyarov***

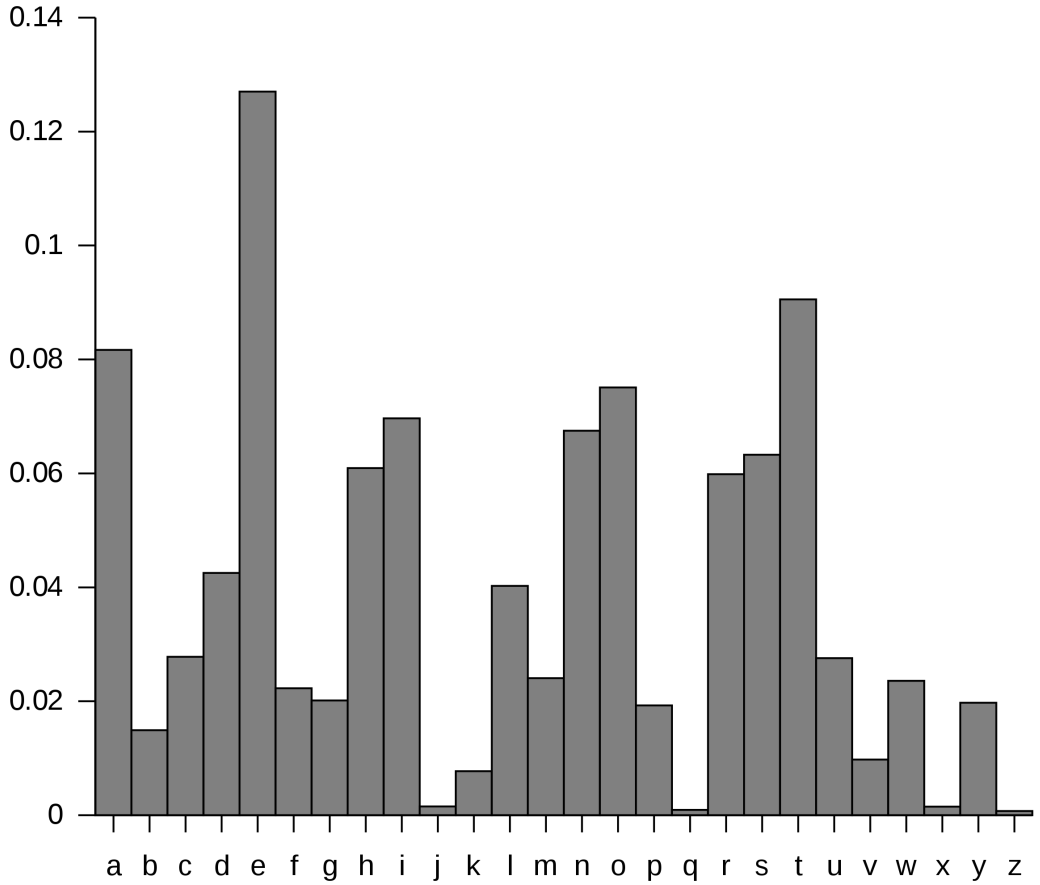
| | |
|---|---|
| **Court** | U.S. District Court for the Northern District of California, San Jose Division |
| **Full case name** | *United States of America* versus *Elcom Ltd., also known as ElcomSoft Co. Ltd., and Dmitry Sklyarov* |
| **Decided** | ElcomSoft acquitted by a federal jury on December 17, 2002 |
| **Case history** | |
| **Prior action(s)** | Dmitry Sklyarov dropped from prosecution in exchange for agreeing to testify and to leave the U.S. |



Dmitry Sklyarov in 2010

https://en.wikipedia.org/wiki/United_States_v._Elcom_Ltd.

# Cipher Security?

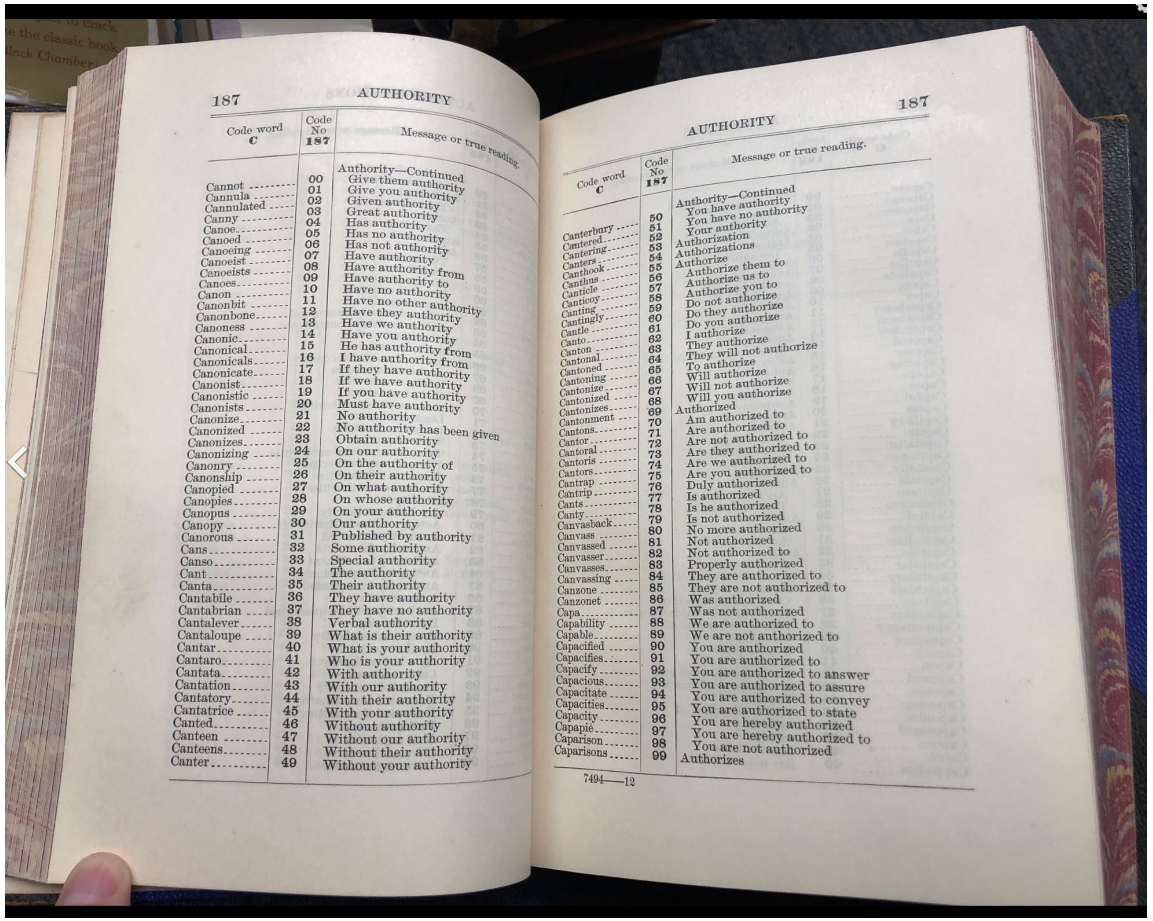


# Example of Cipher Decryption

**Olssv LJLK Jshzz Mvby Mvby Glyv Zpe**

https://www.dcode.fr/caesar-cipher

# Code Book



187 AUTHORITY

| Code word C | Code No 187 | Message or true reading. |
|---|---|---|
| | | Authority—Continued |
| Cannot | 00 | Give them authority |
| Cannula | 01 | Give you authority |
| Cannulated | 02 | Given authority |
| Canny | 03 | Great authority |
| Canoe | 04 | Has authority |
| Canoed | 05 | Has no authority |
| Canoeing | 06 | Has not authority |
| Canoeist | 07 | Have authority |
| Canoeists | 08 | Have authority from |
| Canoes | 09 | Have authority to |
| Canon | 10 | Have no authority |
| Canonbit | 11 | Have no other authority |
| Canonbone | 12 | Have they authority |
| Canoness | 13 | Have we authority |
| Canonic | 14 | Have you authority |
| Canonical | 15 | He has authority from |
| Canonicals | 16 | I have authority from |
| Canonicate | 17 | If they have authority |
| Canonist | 18 | If we have authority |
| Canonistic | 19 | If you have authority |
| Canonists | 20 | Must have authority |
| Canonize | 21 | No authority |
| Canonized | 22 | No authority has been given |
| Canonizes | 23 | Obtain authority |
| Canonizing | 24 | On our authority |
| Canonry | 25 | On the authority of |
| Canonship | 26 | On their authority |
| Canopied | 27 | On what authority |
| Canopies | 28 | On whose authority |
| Canopus | 29 | On your authority |
| Canopy | 30 | Our authority |
| Canorous | 31 | Published by authority |
| Cans | 32 | Some authority |
| Canso | 33 | Special authority |
| Cant | 34 | The authority |
| Canta | 35 | Their authority |
| Cantabile | 36 | They have authority |
| Cantabrian | 37 | They have no authority |
| Cantalever | 38 | Verbal authority |
| Cantaloupe | 39 | What is their authority |
| Cantar | 40 | What is your authority |
| Cantaro | 41 | Who is your authority |
| Cantata | 42 | With authority |
| Cantation | 43 | With our authority |
| Cantatory | 44 | With their authority |
| Cantatrice | 45 | With your authority |
| Canted | 46 | Without authority |
| Canteen | 47 | Without our authority |
| Canteens | 48 | Without their authority |
| Canter | 49 | Without your authority |

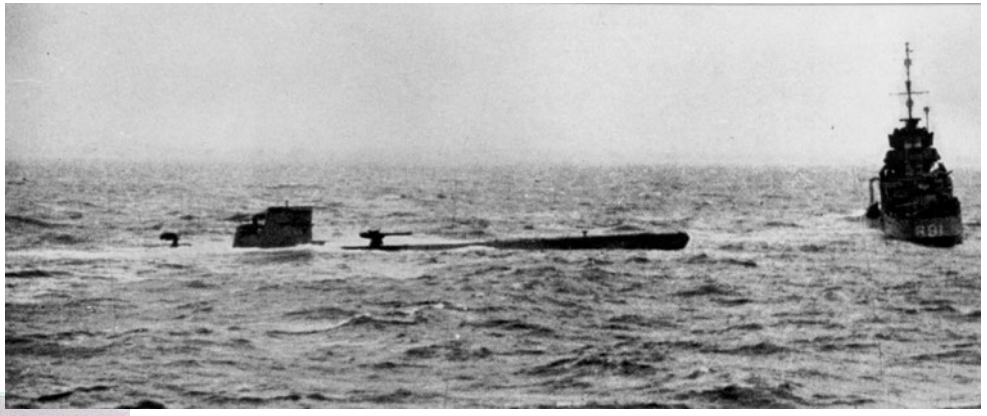
AUTHORITY 187

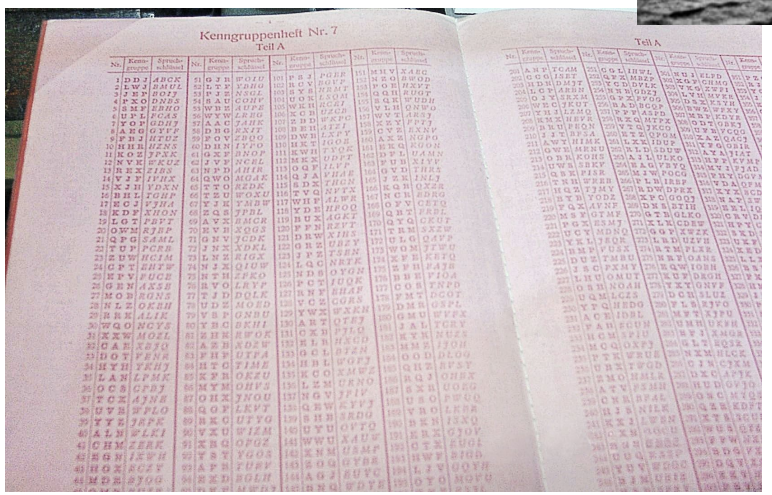
| Code word C | Code No 187 | Message or true reading. |
|---|---|---|
| | | Authority—Continued |
| Canterbury | 50 | You have authority |
| Cantered | 51 | You have no authority |
| Cantering | 52 | Your authority |
| Canters | 53 | Authorization |
| Canthook | 54 | Authorizations |
| Canthus | 55 | Authorize |
| Canticle | 56 | Authorize them to |
| Canticoy | 57 | Authorize us to |
| Canting | 58 | Authorize you to |
| Cantingly | 59 | Do not authorize |
| Cantle | 60 | Do they authorize |
| Canto | 61 | Do you authorize |
| Canton | 62 | I authorize |
| Cantonal | 63 | They authorize |
| Cantoned | 64 | They will not authorize |
| Cantoning | 65 | To authorize |
| Cantonize | 66 | Will authorize |
| Cantonized | 67 | Will not authorize |
| Cantonizes | 68 | Will you authorize |
| Cantonment | 69 | Authorized |
| Cantons | 70 | Am authorized to |
| Cantor | 71 | Are authorized to |
| Cantoral | 72 | Are not authorized to |
| Cantoris | 73 | Are they authorized to |
| Cantors | 74 | Are we authorized to |
| Cantrap | 75 | Are you authorized to |
| Cantrip | 76 | Duly authorized |
| Cants | 77 | Is authorized |
| Canty | 78 | Is he authorized |
| Canvasback | 79 | Is not authorized |
| Canvass | 80 | No more authorized |
| Canvassed | 81 | Not authorized |
| Canvasser | 82 | Not authorized to |
| Canvasses | 83 | Properly authorized |
| Canvassing | 84 | They are authorized to |
| Canzone | 85 | They are not authorized to |
| Canzonet | 86 | Was authorized |
| Capa | 87 | Was not authorized |
| Capability | 88 | We are authorized to |
| Capable | 89 | We are not authorized to |
| Capacified | 90 | You are authorized |
| Capacifies | 91 | You are authorized to |
| Capacify | 92 | You are authorized to answer |
| Capacious | 93 | You are authorized to assure |
| Capacitate | 94 | You are authorized to convey |
| Capacities | 95 | You are authorized to state |
| Capacity | 96 | You are hereby authorized |
| Capaple | 97 | You are hereby authorized to |
| Caparison | 98 | You are not authorized |
| Caparisons | 99 | Authorizes |

7494—12

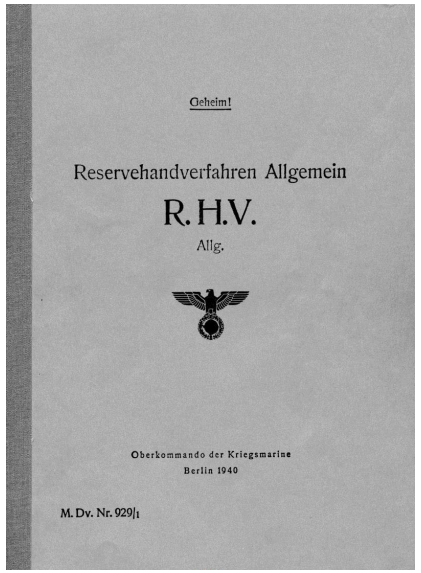
- Theoretically unbreakable! Random words assigned to other words or numbers.
- You need the corresponding code book to decode it.
- …you need a secure channel for the code book. Need many updates to them during a war.

# Example – Various Ciphers from U110 Capture






https://en.wikipedia.org/wiki/Kurzsignale




https://en.wikipedia.org/wiki/Reservehandverfahren

Documentary on U110: https://www.youtube.com/watch?v=K6R52Xhh0_I
https://en.wikipedia.org/wiki/German_submarine_U-110_(1940)

# On Bording Party (from Wikipedia)

“Bulldog's boarding party, led by sub-lieutenant David Balme, got onto U-110 and stripped it of everything portable, including her Kurzsignale code book and Enigma machine.[5] William Stewart Pollock, a former radio operator in the Royal Navy and on loan to Bulldog, was on the second boat to board U-110. He **retrieved the Enigma machine and books as they looked out of place in the radio room**. U-110 was taken in tow back toward Britain, but sank en route to Iceland.”

# Number Stations

- Example of good usage of code books – “number stations” transmit words in the clear to *everyone*. Only agents with codebook can understand.

Example of https://www.youtube.com/watch?v=GNnPPQU9c-c&t=47s

## Very famous & interesting one is UVB-76

- See https://en.wikipedia.org/wiki/UVB-76
- Running since 1973, still running today.
- Mostly beeps / buzzes (that change).
- Sometimes talking has been broadcast.
- Often number/letter sequence (as recently as August 24 / 2020).

Listen to it live: https://www.youtube.com/watch?v=LegzZZRIqj4

# Historical Ciphers

- Normally based on substitutions, code books, etc.
- Easy to break with computers (luckily those didn’t exist then).
- Reasonable to break even with humans however often…
- Usage of code books made them high suspectable to capture of the code book

  → Once one book captured, system could be lost!