Reconstruction of Codes

Karl de Leeuw & Hans van der Meer

14-05-2018

Overview

- How to start the reconstruction
- Paths of entry
- Assigning meaning to code groups
- Special situations

How to start

- Finding the structure of the code
- The crucial step is the first entry
- If nothing else “guesswork” and/or “frequencies”
- If lucky the adversary will be of help
  two examples follow
- Simpler one part code easies the hard work

What is a codegroup?

CYTVW UEYNY IUWUE YBETY MUIUF OWCWI CYTEW RXAVU LUYIX ULFMU IUZEN
MJYYF DURVZ ENMWO GBWOI DBEBG HIRAD IFMRE ATJYY FDURV ZENMW OGBXI
IFDIF MJYYF DURVZ ENMWO GBFYY CXIIF DIFMB ETYKO MWJYY FDURV ZENMW
OGBMI VIDIF MKOZK JYYFD URVNO GWWOG BXITQ DIFMF AFPJY YFDUR VNOGU
WOGBK EER

CYTVW UEYNY IUWUE YCYTV MUIUX EUSKU WFWUE YMUIU PEBSQ OTITU XPXAV
UWIGC CAZGQ IQGRO WNCYT VHAWH MYYIK OZKKI QBLAW LKUWF BETYT OGZMU
IUCAR YTOQI XYTND IDKBI EICYT VCAZG QIQGR OWNTO QIQEU MXYMF NYCOM
EBQLU RBZEA ZDUQU RUWMX ULF

US Army - Zendia Exercise

Groups of 4 are obvious

CYTVW UEYNY IUWUE YBETY MUIUF OWCWI CYTEW RXAVU LUYIX ULFMU IUZEN

MJYYF DURVZ ENMWO GBWOI DBEBG HIRAD IFMRE ATJYY FDURV ZENMW OGBXI

IFDIF MJYYF DURVZ ENMWO GBFYY CXIIF DIFMB ETYKO MWJYY FDURV ZENMW

OGBMI VIDIF MKOZK JYYFD URVNO GWWOG BXITQ DIFMF AFPJY YFDUR VNOGU

WOGBK EER

CYTVW UEYNY IUWUE YCYTV MUIUX EUSKU WFWUE YMUIU PEBSQ OTITU XPXAV

UWIGC CAZGQ IQGRO WNCYT VHAWH MYYIK OZKKI QBLAW LKUWF BETYT OGZMU

IUCAR YTOQI XYTND IDKBI EICYT VCAZG QIQGR OWNTO QIQEU MXYMF NYCOM

EBQLU RBZEA ZDUQU RUWMX ULF

Rewrite in groups of 4

CYTV WUEY NYIU WUEY BETY MUIU FOWC WICY TEWR XAVU LUYI XULF MUIU
ZENM JYYF DURV ZENM WOGB WOID BEBG HIRA DIFM REAT JYYF DURV ZENM
WOGB XIIF DIFM JYYF DURV ZENM WOGB FYYC XIIF DIFM BETY KOMW JYYF
DURV ZENM WOGB MIVI DIFM KOZK JYYF DURV NOGW WOGB XITQ DIFM FAFP
JYYF DURV NOGU WOGB KEER

CYTV WUEY NYIU WUEY CYTV MUIU XEUS KUWF WUEY MUIU PEBS QOTI TUXP
XAVU WIGC CAZG QIQG ROWN CYTV HAWH MYYI KOZK KIQB LAWL KUWF BETY
TOGZ MUIU CARY TOQI XYTN DIDK BIEI CYTV CAZG QIQG ROWN TOQI QEUM
XYMF NYCO MEBQ LURB ZEAZ DUQU RUWM XULF

Patterns become visible

```
CYTV WUEY NYIU WUEY BETY MUIU FOWC WICY TEWR XAVU LUYI XULF MUIU
ZENM JYYF DURV ZENM WOGB WOID BEBG HIRA DIFM REAT JYYF DURV ZENM
WOGB XIIF DIFM JYYF DURV ZENM WOGB FYYC XIIF DIFM BETY KOMW JYYF
DURV ZENM WOGB MIVI DIFM KOZK JYYF DURV NOGW WOGB XITQ DIFM FAFP
JYYF DURV NOGU WOGB KEER
```

```
CYTV WUEY NYIU WUEY CYTV MUIU XEUS KUWF WUEY MUIU PEBS QOTI TUXP
XAVU WIGC CAZG QIQG ROWN CYTV HAWH MYYI KOZK KIQB LAWL KUWF BETY
TOGZ MUIU CARY TOQI XYTN DIDK BIEI CYTV CAZG QIQG ROWN TOQI QEUM
XYMF NYCO MEBQ LURB ZEAZ DUQU RUWM XULF
```

part message part # stop

Enemy mistake: isolog

isolog = same content in two different systems

March 11, 1918 listening post Souilly intercepts three messages at 00:40 12:52 and 12:57 hours

00:40 X2 an AN 00:25 CHI-13 845 422 373 792 240 245 068 652 781 245 659 659 504

12:52 AN an X2 CHI-13 OS RGV KZD

12:57 X2 an AN 00:25 CHI-14 UYC REM KUL RHI KWZ RLF RNQ KRD RVJ UOB KUU UQX UFQ RQK

Code change at midnight

March 11, 1918 at 00:00 KRU-code → Schlüßelheft

KRU-code: OS = Ohne Sinn RGV = alte
OS RGV KZD =?= Ohne Sinn alte Kode

Note: message X2 an AN 00:40 timegroup = 00:25
Note: message X2 an AN 12:57 timegroup = 00:25

RLF	RNQ	KRD	RVJ	UOB	KUU	UQX	UFQ		RQK
H	I	R	SCH		W	I	TT		E
240	245	068	652		781	245	659	659	504

Lazy coders

June 15, 1918: On the Austrian-Italian front new Austrian code of 1000 groups of 3 digits appears

Luigi Sacco: messages of radiostation on Col della Guardia Conegliano show small number of groups very often

June 20, two telegrams end identically

```
492 073 065 834 729 589 255 073 255 834 729 264

492 073 065 834 729 589 255 073 255 834 729 264
 R   A   D   I   O   S   T   A   T   I   O   N
```

Alphabetical groups only: monoalphabetic substitution
Partial deciphering then fill gaps by guessing
Effect of lazy coder: within 6 days code completely broken

One-part code lets interpolate meanings

0 ?	130 Cromwell	280 keep	370 ?
1 null	131 Culpepper	281 King	371 Parliament
2 e	132 e	282 kingdom	372 Pembroke
3 a	133 can	283 know	373 Pendennis
4 i	134 cannot	284 Lancashire	374 Plymouth
5 o	135 ?	285 L...? (naam)	375 ?
6 u,v	136 care	286 ?	376 party
7 w	137 ?	287 ?	377 pass
8 y	138 cause	288 ?	378 ?
9 a	139 city	289 London	379 per

The real gold

Corresponding

Ciphertext-Plaintext

Historical setting

- Reports of ambassador in Sweden R. de Haeften to Dutch stadholder Willem V during 1775-1776
- Serious reports but also news and scandals from the Swedish court, why?
- King Gustave III of Sweden is married to the sister of Wilhelmina van Pruisen who is Dutch stadholders spouse
- Archives contain original message and decipherment by the private secretary
- Thus first partial reconstruction of the codebook possible

Text besides the code

contraires à la presente forme	3317 648 6 96 510 2146 2591 1814 1108 1428 1608 1476 1094
sans aucune forme de proces	2769 326 952 110 1814 1108 2348
cette forme de gouvernement renfermoit	3000 941 1814 101 1428 1608 1276 2160
donnee elle même la presente forme de gouvernement elle sauroit aussi le mieux	568 796 975 893 1075 1792 2146 2591 1814 1696 1428 1502 1476 975 604 2170 2021 428 604 1179

Note corresponding texts

contraires à la presente forme	3317 648 6 96 510 2146 2591 1814 1108 1428 1608 1476 1094
sans aucune forme de proces	2769 326 952 110 1814 1108 2348
cette forme de gouvernement renfermoit	3000 941 1814 101 1428 1608 1276 2160
donnee elle même la presente forme de gouvernement elle sauroit aussi le mieux	568 796 975 893 1075 1792 2146 2591 1814 1696 1428 1502 1476 975 604 2170 2021 428 604 1179

Spot corresponding codegroups

contraires à la presente forme	3317 648 6 96 510 2146 2591 1814 1108 1428 1608 1476 1094
sans aucune forme de proces	2769 326 952 110 1814 1108 2348
cette forme de gouvernement renfermoit	3000 941 1814 101 1428 1608 1276 2160
donnee elle même la presente forme de gouvernement elle sauroit aussi le mieux	568 796 975 893 1075 1792 2146 2591 1814 1696 1428 1502 1476 975 604 2170 2021 428 604 1179

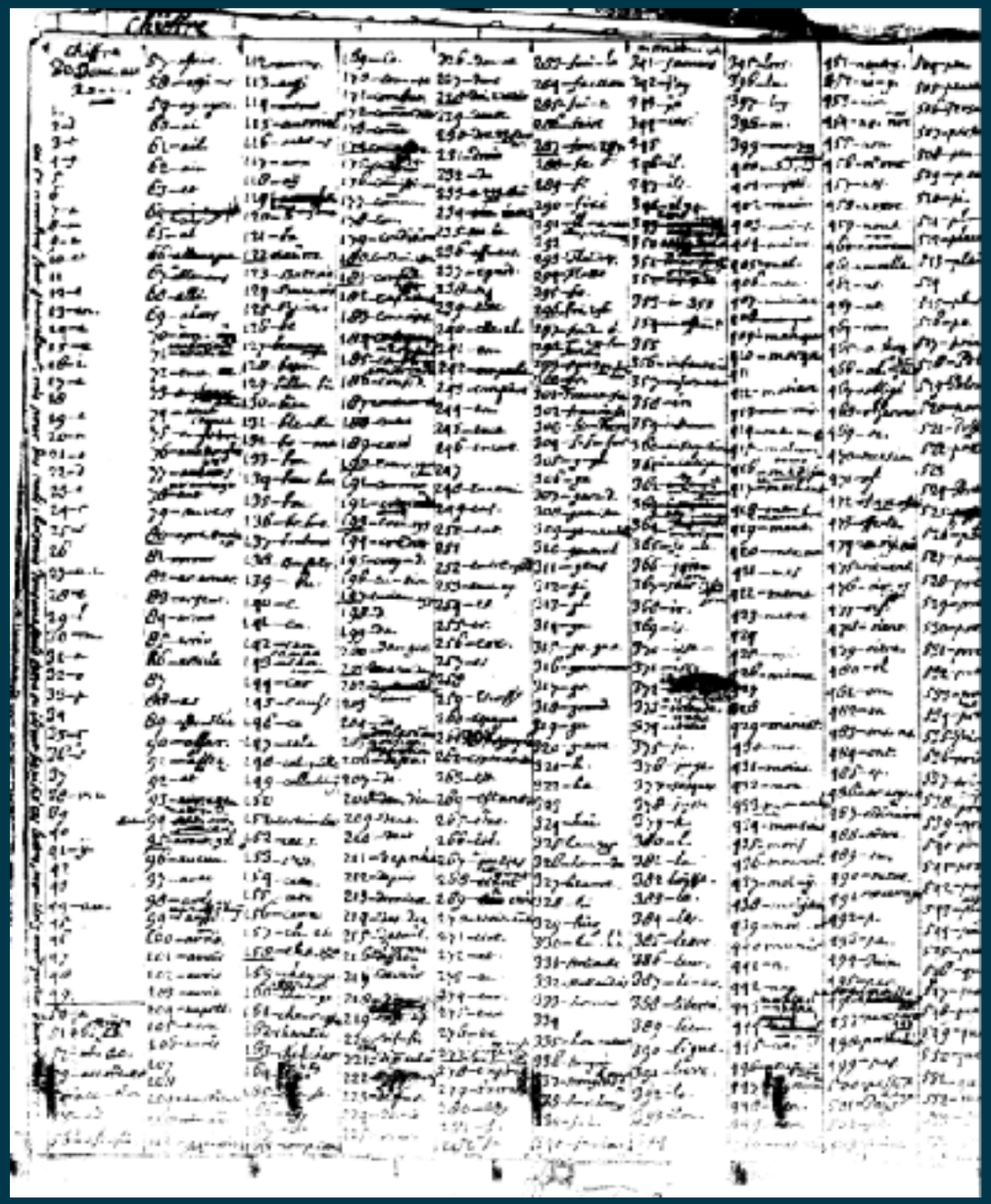
Combine groups to words spot homophones

contraires à la presente forme	3317 648 6 96 510 2146 2591 1814 1108 1428 1608 1476 1094
sans aucune forme de proces	2769 326 952 110 1814 1108 2348
cette forme de gouvernement renfermoit	3000 941 1814 101 1428 1608 1276 2160
donnee elle même la presente forme de gouvernement elle sauroit aussi le mieux	568 796 975 893 1075 1792 2146 2591 1814 1696 1428 1502 1476 975 604 2170 2021 428 604 1179

Delineate words and groups

contraires à la presente forme	3317 648 6 96 510 2146 2591 1814 1108 1428 1608 1476 1094
sans aucune forme de proces	2769 326 952 110 1814 1108 2348
cette forme de gouvernement renfermoit	3000 941 1814 101 1428 1608 1276 2160
donnee elle même la presente forme de gouvernement elle sauroit aussi le mieux	568 796 975 893 1075 1792 2146 2591 1814 1696 1428 1502 1476 975 604 2170 2021 428 604 1179

Codebreaking match: guess who wins



Abel Tasien d’Alonne

William Blencowe