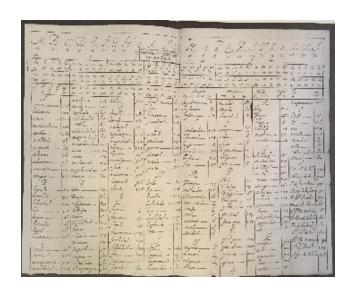
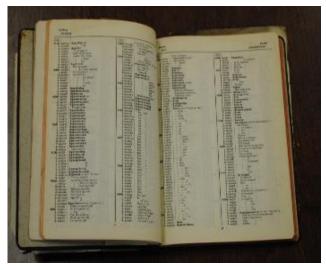
### Codes and Nomenclators

### A Systematic View





Klaus Schmeh (www.schmeh.org)
HistoCrypt 2018 Uppsala





#### The Top 50 unsolved encrypted messages: 34. Unsolved nomenclator messages

For centuries nomenclators were the most popular kind of encryption. Still today messages enciphered with a welldesigned nomenclator are hard or even impossible to break.

Von Klaus Schmeh / 24. April 2017 / 5 Kommentare / Weiterlesen



#### Nomenclator encryptions: centuries old, but still hard to solve

The British National Archive has published an encrypted letter from the 17th century. The solution is known, but many other encrypted notes of the same kind still wait to be

broken.

Von Klaus Schmeh / 13. August 2016 / 4 Kommentare / Weiterlesen

## If you have an unsolved encrypted text, I will be happy to publish it on my blog.

### Agenda

- 1. Basics: scope, terminology, classification
- 2. How to detect a code
- 3. How to cryptanalyze a code
- 4. Open research questions
- 5. A few solved code cryptograms
- 6. A few unsolved code cryptograms

#### **Code facts**

Please correct, if wrong

Codes are not used any more today. So, the topic is only of historical interest.

No specialist for deciphering code cryptograms currently exists.

Stephen Bellovin currently seems to be the most renowned codebook expert.



#### **Terminology**

Please check the following website for the current version of the terminology discussed at the workshop and afterwards:

http://scienceblogs.de/klausis-krypto-kolumne/2018/07/09/a-terminology-for-codes-and-nomenclators/

#### **Terminology**

Please correct, if wrong

**Cipher**: encryption method that operates at the level of individual letters

Code: encryption method that operates at level of meaning

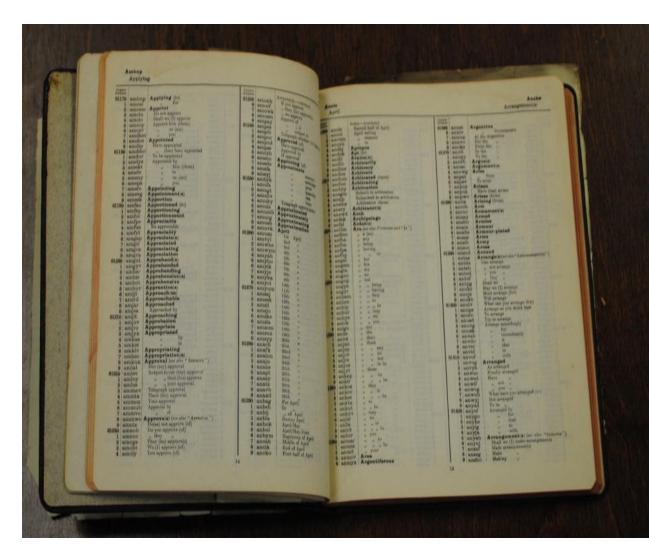
**Nomenclator**: small code

Codebook: big code

#### **Nomenclator**

10 10 10																
	10		000	,	200	, .		_								
	M. B.	6	00 2	1	4. It.	1	K. P.	CNA	10 0	(	700		0711	~	V ~ 11	7
	18 20	19	1) 14	16	15 12	13/1	culvue an 3	John .		1	G. K	,0	. J. Y.	1	1. 4. de	
	m		9			1	DE DELGIQUE	HIM .	4 5	8	. 21 22	7	5 26 27	29 2	28 39 36	
1	ba be bi bo	bu	sa ce ci co		Da De Di De	du	for to his			001	Sa Se Sir So	1	3/a 2/e 2/i 3/0	7.1	1. 1. 1. 1. 1	+ 1
1	65 66 65 68	69	va ve vi vo	vw.		cu	rasre hi no	ne	ga ge gi go	tu	pa pe si po			·mil	la le le lo la	
	Za Ze Zi zo	Zu	no ne ne no no 45 46 47 48	nu 49	pa pe pi po		1 / /	ru		No.	Ja de di lo.	Jul	ta te ti to	tu !	con che chi cho de	1 0
	al el el ol	ul	as es is or	w	a. e. i. c.	u,		fu!	ga ge gi go	gu.	30 31 32 33	34	Ta ye Ti Ye	3/4	an en in on un	
	la le li lo	lu	na ne ni no	nu	75 76 >> 78		104.	007	finale		Mumeros			uplia	lla que	T
	A		conclusion_	119	Oicsa	fur		Sun	impedimento-	,	nouedad -	90	0	-	for second will	7
	aputamiento-	106	concluyr-	120	é		fuerca	141	Inolationa_	1		20	Lev -	mue	temperamento ril	
	avistencia	10>	my dado	bat	Opana	4	frontera	142	11.	151	4	0	Reyna		lexa rol	
	auro	108	catholico -	bet bit	estado -	131	facultad_	143	0		0		religion	165	My rue	· 1000
	autsoridas -	109	oritianismo-		Embajada-	132	9		Lombardia -	153	occarion -	9	rebelde	166	Om 17.	4
	audiencia _	ale	coneponderia		esperanza.	133	grande	144	11	154		9	resolucion -	/	Varallo 17	1000
	artillería	els	conceniencia_	121	experiencia-	134	gouierno -	145	lucao -		oficio -	21	rendimienso-		veandad le	
	armada	ile	Coneo	122	empresa	135	диета	3'at	licencia	156	ocupación _	5	5	1	Villa lli	100000
	aleman	olt	Carta	123	exerceto	gal	general -	L'et	Condres	153	obligación -	7	Su Mag :-	nat	Union - Ula	
	aduntenca'_	celo	conferencia	124		gel	10	Wit Yes	Sorena	158	openion -		su Ala	net nit .	d of	
	amutad	110	confidencia -	125		,	gente -	100	M		9		su ex	mat	T. D. Me. de Arus gu	ia la
	amigo	# \$\$	Consejo	Dan	execution_	901	-71	01	-4		Paris	×	Jecreto	10000	Duys de Hora gu	a
	barallo		2,50		Emperador -	gul	Secso -	Yut	pocuorque	159	Principe -	Z	siempre	1000	de funsatione go	u
	beneficio		Dios	den	clecuon	136	1.	146	mediación -	160	Portugal_	K	Jaris facion-		Marg de la purce 9	ue
	bruedad		Duque -	Din	J.		Sombre -	(4)	Mazarini -	20	Portugues;	161	rezuucio -	1	Ofer de sole - gr	200
	bien_		Oiligencia -	Oun	francia	^	Sabrendo -	149	1.	8	pretexto-	162	1 /	1	Mons- de Sionne - Si	14
	bueno	115	Dano -		frances -	9	Sonra	150	Milan -	0	puntual_	163	sinceridad -		Alde Carden -	11
	Bruelas_	cel	Dificultad	127	14	137	Sostilidad -	lar	materia -	100	para que -	164		pen	Min de Salaro	or
	basel	cil	Dinero -	128	flandes -	138		Cer	mueso	1	é		Jenior -	Jul	Mary de lang -	= 0
	bartimento _	col	Diversion -	129	flamenco -	139	Sager		Madrid -	2		1	T.	1	D for de cont "	Ret
	C		Oiscurso -	1130	faulidad -	140	1	1	19	10.	qualquera-	1	himpo -	pin	AC. B. Cansacero	136
	Conde	cul	Despacso	fan	felicidad_	San	Italia	#	,	- 2		mes	todo-	por	che de Penanda	>>
	Cardenal -	116	serpus	fer	forma	Sen	Imperio -	100	necessario -	12	quenta -	met	fregue -	Y ,	Argo de Bles - 1	1)8
-	consequencia -	11)	Ouposicion -	for	fortuna -	Sin	importancia-	lur	ninguna	12	guen -	mos	trato -	ral		
	consideration	118	Dungungus-	for	rencaon —	Son	instruccion -	lor	nucua	1=	6		fanto -	rei		
STATE OF	AND DESCRIPTION OF THE PERSON NAMED IN	TO SHOW SHAPE	CONTRACTOR OF THE PARTY OF THE	THE REAL PROPERTY.	The state of the s	and the same	and the	-	and the second	-		Can		-		and the local division in which the local division in the local division in which the local division in

#### Codebook



#### **Terminology**

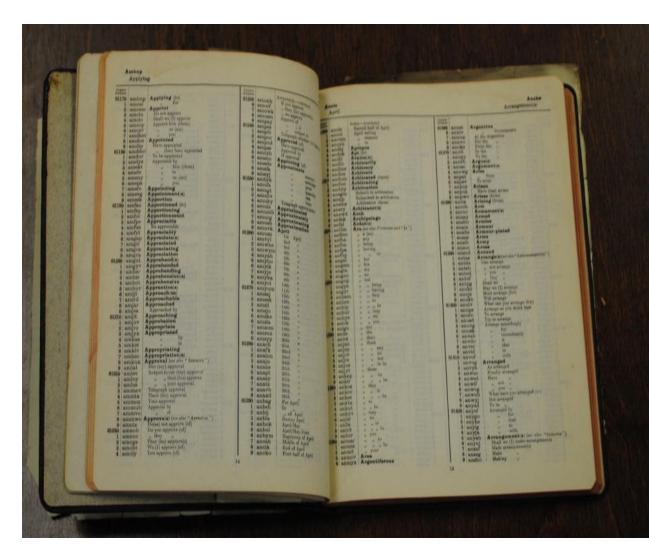
Please correct, if wrong

- **Codegroup**: smallest unit of a code, may consist of several letters/numbers
- Null: meaningless codegroup
- Nullifyer: makes the previous codegroup meaningless
- Homophones: several codegroups with the same meaning
- Wordgroup: Codegroup that refers to a word
- Lettergroup: analog

#### **Nomenclator**

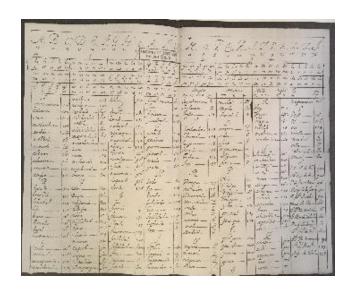
10 10 10																
	10		000	,	200	, .		_								
	M. B.	6	00 2	1	4. It.	1	K. P.	CNA	10 0	(	700		0711	~	V ~ 11	7
	18 20	19	1) 14	16	15 12	13/1	culvue an 3	John .		1	G. K	,0	. J. Y.	1	1. 4. de	
	m		9			1	DE DELGIQUE	HIM .	4 5	8	. 21 22	7	5 26 27	29 2	28 39 36	
1	ba be bi bo	bu	sa ce ci co		Da De Di De	du	for to his			001	Sa Se Sir So	1	3/a 2/e 2/: 3/0	7.1	1. 1. 1. 1. 1	+ 1
1	65 66 65 68	69	va ve vi vo	vw.		cu	rasre hi no	ne	ga ge gi go	tu	pa pe si po			·mil	la le le lo la	
	Za Ze Zi zo	Zu	no ne ne no no 45 46 47 48	nu 49	pa pe pi po		1 / /	ru		No.	Ja de di lo.	Jul	ta te ti to	tu !	con che chi cho de	1 0
	al el el ol	ul	as es is or	w	a. e. i. c.	u,		fu!	ga ge gi go	gu.	30 31 32 33	34	Ta ye Ti Ye	3/4	an en in on un	
	la le li lo	lu	na ne ni no	nu	75 76 >> 78		104.	007	finale		Mumeros			uplia	lla que	T
	A		conclusion_	119	Oicsa	fur		Sun	impedimento-	,	nouedad -	90	0	-	for second will	7
	aputamiento-	106	concluyr-	120	é		fuerca	141	Inolationa_	1		20	Lev -	mue	temperamento ril	
	avistencia	10>	my dado	bat	Opana	4	frontera	142	11.	151	4	0	Reyna		lex rol	
	auro	108	catholico -	bet bit	estado -	131	facultad_	143	0		0		religion	165	My rue	· 1000
	autsoridas -	109	oritianismo-		Embajada-	132	9		Lombardia -	153	occarion -	9	rebelde	166	Om 17.	4
	audiencia _	ale	coneponderia		esperanza.	133	grande	144	11	154		6	resolucion -	/	Varallo 17	1000
	artillería	els	conceniencia_	121	experiencia-	134	gouierno -	145	lucao -		oficio -	21	rendimienso-		veandad le	
	armada	ile	Coneo	122	empresa	135	диета	3'at	licencia	156	ocupación _	5	5	1	Villa lli	100000
	aleman	olt	Carta	123	exerceto	gal	general -	L'et	Condres	153	obligación -	7	Su Mag :-	nat	Union - Ula	
	aduntenca'_	celo	conferencia	124		gel	10	Wit Yes	Sorena	158	openion -		su Ala	net nit .	d of	
	amutad	110	confidencia -	125		,	gente -	100	M		9		su ex	mat	T. D. Me. de Arus gu	ia la
	amigo	# \$\$	Consejo	Dan	execution_	901	-71	01	-4		Paris	×	Jecreto	10000	Duys de Hora gu	a
	barallo		2,50		Emperador -	gul	Secso -	Yut	pocuorque	159	Principe -	Z	siempre	1000	de funsatione go	u
	beneficio		Dios	den	clecuon	136	1.	146	mediación -	160	Portugal_	K	Jaris facion-		Marg de la purce 9	ue
	bruedad		Duque -	Din	J.		Sombre -	(4)	Mazarini -	20	Portugues;	161	rezuucio -	1	Ofer de sole - gr	200
	bien_		Oiligencia -	Oun	francia	^	Sabrendo -	149	1.	8	pretexto-	162	1 /	1	Mons- de Sionne - Si	14
	bueno	115	Dano -		frances -	9	Sonra	150	Milan -	0	puntual_	163	sinceridad -		Alde Carden -	11
	Bruelas_	cel	Dificultad	127	14	137	Sostilidad -	lar	materia -	10	para que -	164		pen	Min de Salaro	or
	basel	cil	Dinero -	128	flandes -	138		Cer	mueso	1	é		Jenior -	Jul	Mary de lang -	= 0
	bartimento _	col	Diversion -	129	flamenco -	139	Sager		Madrid -	2		1	T.	1	D for de cont "	Ret
	C		Oiscurso -	1130	faulidad -	140	1	1	19	10.	qualquera-	1	himpo -	pin	AC. B. Cansacero	136
	Conde	cul	Despacso	fan	felicidad_	San	Italia	#	,	- 2		mes	todo-	por	che de Penanda	>>
	Cardenal -	116	serpus	fer	forma	Sen	Imperio -	100	necessario -	12	quenta -	met	frequa -	Y ,	Argo de Bles - 1	1)8
-	consequencia -	11)	Ouposicion -	for	fortuna -	Sin	importancia-	lur	ninguna	12	guen -	mos	trato -	ral		
	consideration	118	Dungungus-	for	rencaon —	Son	instruccion -	lor	nucua	1=	6		fanto -	rei		
STATE OF	AND DESCRIPTION OF THE PERSON NAMED IN	TO SHOW SHAPE	CONTRACTOR OF THE PARTY OF THE	THE REAL PROPERTY.	The state of the s	and the same	and the	-	and the second	-		Can		-		and the local division in which the local division in the local division in which the local division in

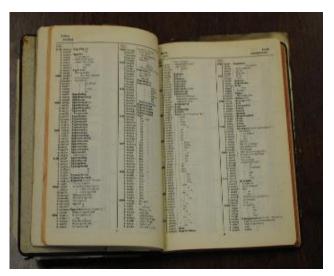
#### Codebook



#### Questions

What exactly is the difference between a nomenclator and a codebook?





Is there a better word for "code" ("code" has different meanings in cryptography and in other contexts)?

## What about dictionary codes?

Dictionary code: a dictionary is used. Each word is referenced by its page and position.

- Easier to set up than codebook
- Less secure than a (well-made) codebook
- Different cryptanalysis approaches
- Many examples of usage known
- Related to book codes

#### Classifications of codes

**Purpose** 

Codes used for encryption

Codes used for compression

Codes used for avoiding errors

**Alphabet** 

Code numbers

Code words

Code symbols

**Number of parts** 

One-part codes

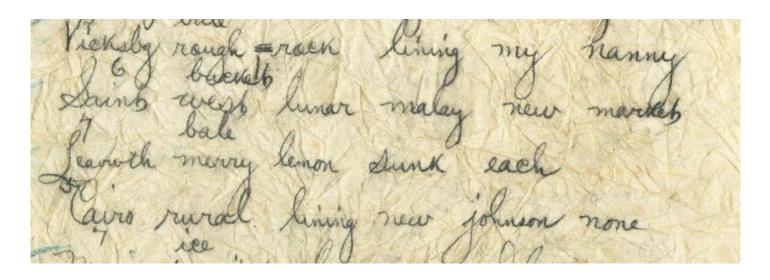
Two-part codes

### Agenda

- 1. Basics: scope, terminology, classification
- 2. How to detect a code
- 3. How to cryptanalyze a code
- 4. Open research questions
- 5. A few solved code cryptograms
- 6. A few unsolved code cryptograms

I received your Letter dated Sept 2. and should not have delayed so long sending an answer to it had Jany thing very material fo communicate 3693: 2517. 65: 3423.576.1100. 97. 1765. 3000. 259. 3032. 57. 66. 1795. 19. 211. 46. 1038. 1637. 970. 2609. 3369. 696. 3696. 427. 118. 3364. 1362. 456. 111. 566, 77. 1551. 2961. 1504. 1437. 3560. 1453. 2053. 1555. 1834. 1406. 9. 2044. 2694. 3423. 678. 1359. 493. 809. 1094. 956. 636. 1618. 61. 1437. 1369. 2316.497. 314.684. 1205. 193.685. 2072. 65,39. 3459. 3937. 2108. 2615. 1359. 766. 2450. 880.1291.

An alphabet with hundreds of letters (e.g., numbers with several digits) is typical for a code.



CRAQUEREZ REFRENANS VIJFVOETIG IMPAZZAVA

PRENSABERE INTRUSIVE REGENBUL EDIFLERS

RETAPLEZ DECRUSAMES IMPAVIDEZ RIBOTIEZ

GOLDKRAUT RIONORAL SANSCRITO FLEMINGS

BRAMIDO SUPERFICIE GALEFFAVA BOWLINE

Pseudo-meaningful words are typical for a code.

Was nvlvaft by
aakat txpxsck upbk
txphn ohay ybtx cpt
mxhg wae sxfp zavfz
ack there first
txlk week wayx za
with thx

Cleartext words in an encrypted message are typical for a code.

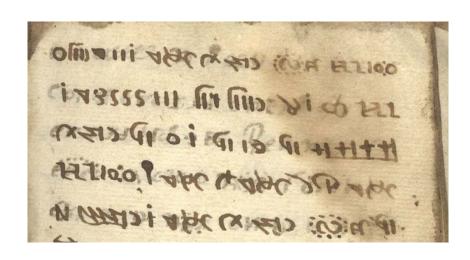
#### Sometimes it's easy

I received your Letter dated Sept 2. and should not have delayed so long sending an anower to it, had sany thing very material to communicate 3693: 2517. 65: 3423.576.1100. 97. 1765. 3000. 259. 3032. 57. 66. 1795. 19. 211. 46. 1038. 1637. 970. 2609. 3369. 696. 3696. 427. 118. 3364. 1362. 456. 111. 566. 77. 1551. 29 61. 1504. 1437. 3560. 1453. 2053. 1555. 1834. 1406. 9. 2044. 2694. 3423. 678. 1359. 493. 809. 1094. 956. 636. 1618. 61. 1637. 1369. 2316. 497. 314. 684. 1205. 193. 685. 2072.

Was nvlvaft by aakat txpxsck upbk txphn ohay ybtx cpt mxhg wae sxfp zavfz ack there first txlk week wayx za with thx

277. 409. 50. 24. 428. 82. 326. 13. 101. 308. 393. 409.
335. 102. 106. 251. 30. 3. 393. 291. 359. 262. 85. 160.
329. 136. 84. 43. 166. 50. 14. 184. 201. 226, 152. 129.
162. 350. 122. 13. 295. 409. 188. 168. 28. 43. 50. 78. 396.
326. 56. 138. 30. 22. 20. 50. 84. 66. 100. 344. 202. 369.
129. 81. 22. 8. 85. 286. 28. 328. 30. 56. 84. 50. 126.
138. 17. 14. 247. 35. 17. 200. 33. 84. 3. 8. 50. 275. 54.
8. 77. 62. 282. 260. 198. 393. 28. 169. 65. 50. 37. 59. 11.

#### Sometimes not



| 80CH | J2 6 L  | B 50 U  | 2 R E H |
|------|---------|---------|---------|
| DYTM | NRLF    | DUTN    | D R S K |
| nyAT | 2 M N T | 2 % 4 D | BycY    |
| PDUR | BONR    | RYEL    | 1205    |

### Agenda

- 1. Basics: scope, terminology, classification
- 2. How to detect a code
- 3. How to cryptanalyze a code
- 4. Open research questions
- 5. A few solved code cryptograms
- 6. A few unsolved code cryptograms

#### How to break a code?

#### Solution approaches:

- Find the codebook/nomenclator
- Frequency analysis, text statistics
- Word guessing

Weakly constructed codes may be helpful

### Agenda

- 1. Basics: scope, terminology, classification
- 2. How to detect a code
- 3. How to cryptanalyze a code
- 4. Open research questions
- 5. A few solved code cryptograms
- 6. A few unsolved code cryptograms

## Analysing tool applying text statistics

Number of entries

Letters, sylables, words, expressions

Homophones
Nulls
Nullifiers

Superencipherment

#### **Code creation software**

Software that creates a code based on parameters:

- language
- number of codegroups
- number of homophones
- number of nulls
- ...

#### **Code database**

I would be helpful to have a searchable database containing all codes known.

### Agenda

- 1. Basics: scope, terminology, classification
- 2. How to detect a code
- 3. How to cryptanalyze a code
- 4. Open research questions
- 5. A few solved code cryptograms
- 6. A few unsolved code cryptograms



This form must accompany any enquiry respecting this telegram:

ايب ان يرسل هذا النموذج مع كله لام بخصوص هذه البرتية

את הטופס הוה צריך לצרף לכל. ירה הנערכת בנידון המכרק הוה. Published by Karsten Hansky
John McVey, a design professor and codebook expert
from Massachusetts recognized the codebook

(Peterson's International Code (3rd edition, 1929)).

TEL BANGETTIN

vizl38 idz 1646 r4993 jw931 cde Newyork 271/159

4 1930

7

GOVIT MEMISRAEL TELAVIV

91

147 FOLLOWING TRANSMITTED FROM LONDON FOR GENEVANA QUOTE CABLE NAMBER 36 LE\_RZY YUBRB BIKUG NEYBH FIFOD XADAT OLUZA DYELN AMIAW LFYWI AHCRU KOXXE EGBFA IOGBU ODVYE OJCEK KEWOF ONRIU AMIIM OIWXN AMJYZ CDVYE IOGVU ARLEJ DYRVY GIFYK FUPAR VERTIALLY ITTYA FUPAR CYTUV OSYLO OTRVO KKM YUBRB BIKUG NEYBH FIFOD XADAT OLUZA DYELN AWIAW LEYWI HCRU XX KOXXE KOXXE EGBFA IOGBU ODVYE OJCEK KEWOF ONRIU AMIIM OTWXN AHJYZ ODVYE IOGVU ARLEJ DYRVY GIFYK FUPAR VERTICALLY ITTYA FUPAR CYTUV OSYLO OTRVO ALHDE IOGBU FIFOD COYSV ODHMU MOIEX HSOIG KFIYS GIFYK NFIGU IUXBX OYHLI HDYIZ ITOXH IYVIR FLAAF GKATU IOXYJ ALEFM OUDNK LRZIC AYBGV ODVYE FUPUK LMBOA AZMUV ALEFA EFZXU ITYHZ OWYRC AFGNE LZGOE ANMNI FDYAV CYUWV ODVYE AWIAW JESSA IXDYN ANGEVINEX AHOEV UPHY IOGBU

## 16th century nomenclator broken by Albert Leighton

Message sent from Poland to the Vatican in 1573 (excerpt):

```
608 53 17 11 75 17 55 25 77 75 29 97 41 77 13 79 11 77 15 59 19 79 15 79 17 39 19 79 15 59 13 79 99 58 99 11 17 59 13 67 79 15 77 17 99 15 15 83 54 97 41 57 15 77 75 15 59 26 99 15 37 15 38 34 17 37 57 19 79
```

...

#### Albert Leigthton's assumptions:

- unmarked two-digit numbers: letter
- marked two-digit numbers, three-digit numbers: word
- numbers starting with 1 or 2 are vowels
- 77, the most frequent non-vowel stands for N

This information was sufficient to decipher most of the cryptogram.

### Agenda

- 1. Basics: scope, terminology, classification
- 2. How to detect a code
- 3. How to cryptanalyze a code
- 4. Open research questions
- 5. A few solved code cryptograms
- 6. A few unsolved code cryptograms

WW2 Telegram



Manchester Cryptogram

Sir

I received your Letter dated Sept 2 and should not have delayed so long sending an answer to it had Jany thing very material to communicate 3693: 2517. 65. 3423.576.1100. 97. 1765. 3000. 259. 3032. 57. 66. 1795. 19. 211. 46. 1038. 1637. 970. 2609. 3369. 696. 3696. 427. 118. 3364. 1362. 456. 111. 566. 77. 1551. 2961. 1504. 1437. 3560. 1453. 2053. 1555. 1834. 1406. 9. 2044. 2694. 3423. 678. 1359. 493. 809. 1094. 956. 636. 1618. 61. 1437. 1369. 2316.497. 314. 684. 1205. 193. 685. 2072. 65,39. 3459. 3937. 2108. 2615. 1359. 766.2450. 880.1291. 647. 3339. 1175. 3714. 809. 184. 564. 2101. 1581. 566. 2323. 2066. 823. 665.2401.1692.3560.1444.2734.970.830. 3601. 3263. 1612. 8000. 1291. 2000. 1936. 3056. 3278.1618. 2894. 3438. 233. 2424. 3137. 3928. 1501. 3364.434.492. 566.1498.2450. 3560. 1603. 3905. 3082.1504.1242. 1624.987.2615. 1306.350.1245. 1504.1145.9.3658.

J. John Stepney Faster

2622.

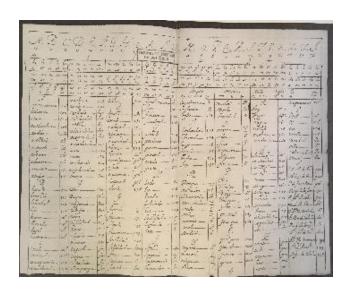
Ohio Cryptogram

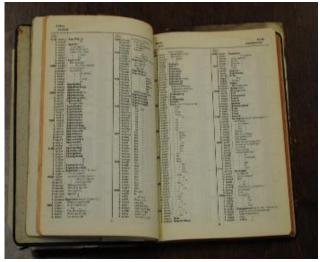
WAS NVKVAFT BY AAKAT TXPXSCK UPBK TXPHN OHAY YBTX CPT MXHG WAE SXFP ZAVFZ ACK THERE FIRST TXLK WEEK WAYX ZA WITH THX.

Van Gelder Cryptogram

1194 239 62 893 2395 1568 226 980 1382 929 800 75 2482 497 1195 211 560 511 475 524 680 228 1007 804 1696 35 331 4 39 356 2538 1049 564 934 416 748 601 577 179 2740 742 710 75 900 539 1341 805 420 561 2891 679 1632 1034 1171 8264 1294 332 508 707 1789 75 2655 632 189 473 1128 624 1194 2913 103 894 1193 850 227 93 657 1567 298 1300 948 255 1700 1576 816 735 609 547 189 2898 467 713 519 1567 2486 792 147 680 805 1843 21 2731 935 831 112 771 791 185 1343 1523 1413 2920 241 799 1097 699 613 795 15 1528 186 607 894 135 510 1388 1710 804 618 949 524 211 1413

## **END**





Klaus Schmeh (www.schmeh.org)