Compression, Correction, Confidentiality, and Comprehension

A Modern Look at Commercial Telegraph Codes

Steven M. Bellovin
smb@cs.columbia.edu
http://www.cs.columbia.edu/~smb
Department of Computer Science
Columbia University

Early Telegraphy

- Early telegraphy, especially overseas, was *very* expensive: $100 for twenty words trans-Atlantic in 1866.
- Messages were no longer sealed; a telegraph operator saw them
- The solution was *code books*
- Precedent: optical semaphore networks; naval signaling flags

Samuel Morse's 1844 telegraph key.

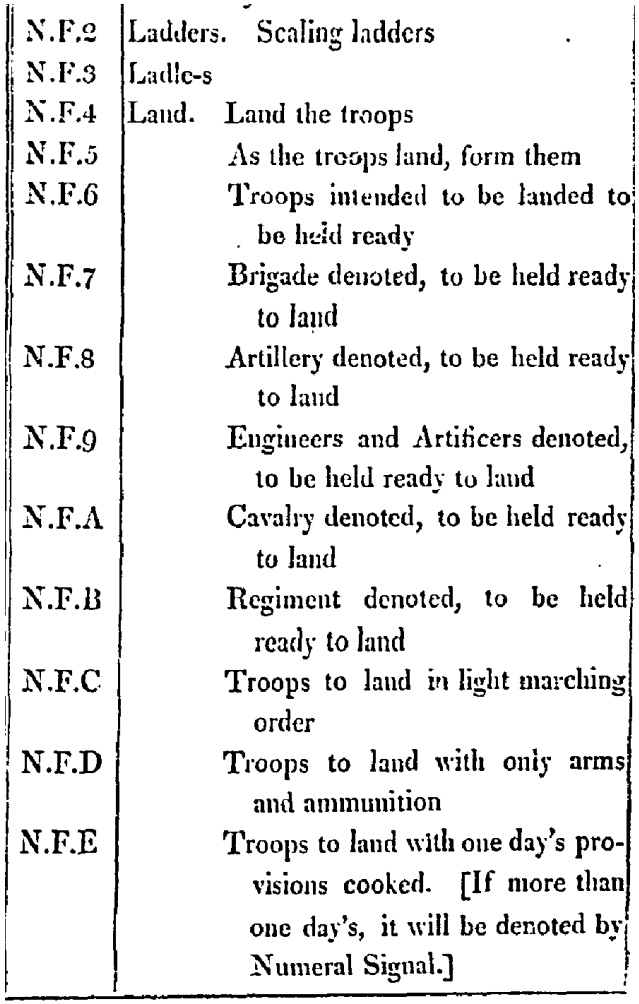
(Alfred Harrell, 1974. ©Smithsonian Institution, `http://www.si.edu`. Image 74-2491. Used by permission.)

Four Focus Areas

- Compression — reducing transmission cost
- Correction — detecting and correcting errors
- Confidentiality — protecting the content of a message
- Comprehension — understanding other cultures, distant in time and space

"England Expects that Every Man Will Do His Duty"

- Sir Home Popham: the first true "conversational" naval code (1803)
- Important common sentences — but also enough words to convey more or less any message
- Note optional parameter
- Nelson's famous signal (1805) was sent using this code
- (Nelson originally said "confides", but that word wasn't in the code book)



N.F.2	Ladders.	Scaling ladders
N.F.3	Ladle-s	
N.F.4	Land.	Land the troops
N.F.5		As the troops land, form them
N.F.6		Troops intended to be landed to be held ready
N.F.7		Brigade denoted, to be held ready to land
N.F.8		Artillery denoted, to be held ready to land
N.F.9		Engineers and Artificers denoted, to be held ready to land
N.F.A		Cavalry denoted, to be held ready to land
N.F.B		Regiment denoted, to be held ready to land
N.F.C		Troops to land in light marching order
N.F.D		Troops to land with only arms and ammunition
N.F.E		Troops to land with one day's provisions cooked. [If more than one day's, it will be denoted by Numeral Signal.]

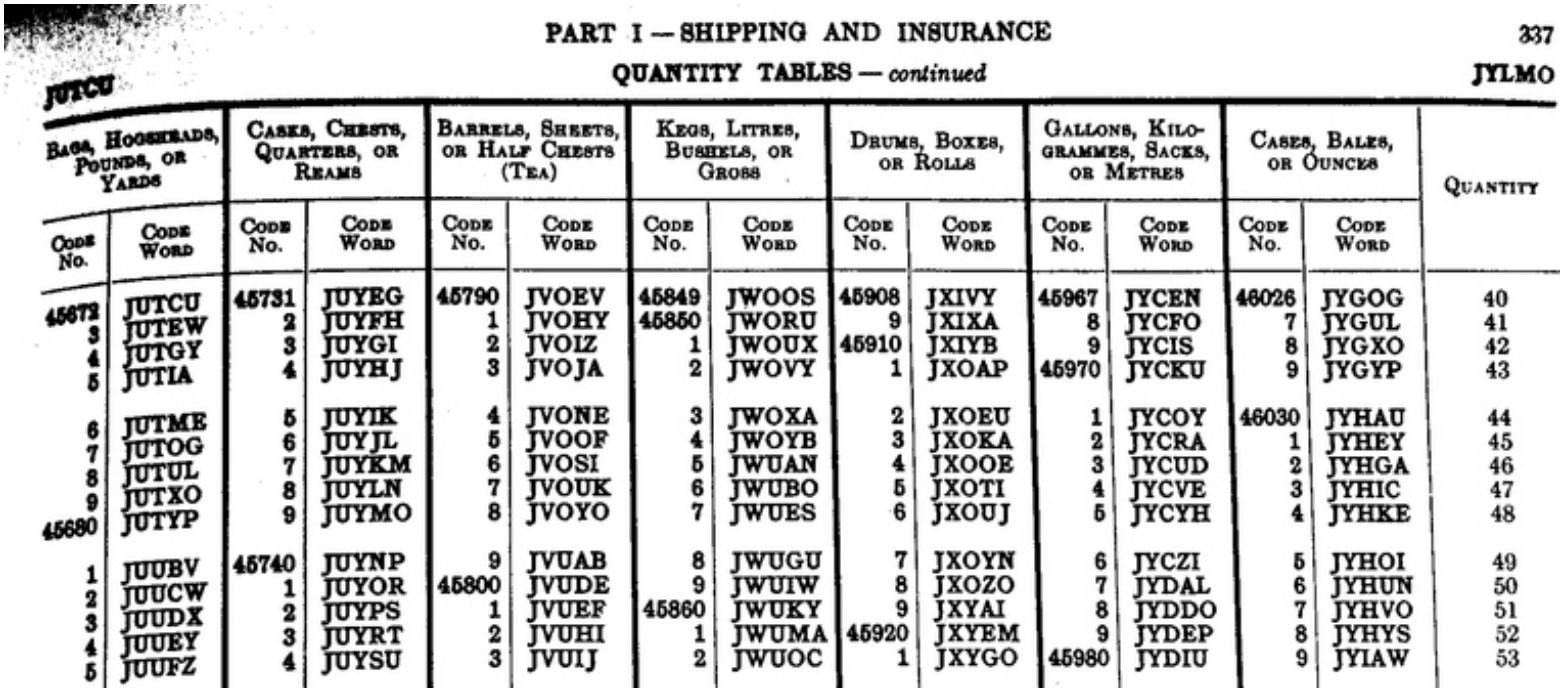
The 1896 Atlas Universal Traveler's and Business Cipher Code

Gulheid	***CUSTOMS AUTHORITIES.***
Gulist	Fear you will have trouble with the Customs.
Gullage	Expect to have trouble with the Customs.
Gullery	Had some trouble with the Customs.
Gullible	Baggage seized by the Customs.
Gulonis	Articles " and forfeited by the Customs.
Gulosity	Had no trouble with the Customs.
Gulosos	The Customs authorities here
Gulpende	The " " there
Gulping	The " " at
Gumbies	Passed the Customs all right.
Gumedra	The English "
Gumlac	The American "
Gunated	The French "
Gunation	The Foreign "
Guncho	The Chinese "
Gundelet	The Japanese "
Gunello	With permission from the Customs.
Gunhild	Without " " " "
Gunshot	Custom House.
Gunster	Custom " here.
Gunstock	Custom " at
Gunstone	Custom " officers here.
Gunther	Custom " " at
Guntram	Custom " " seized (my ———).
Gurbion	Custom " " " (" trunk).

Notable Points

- Codewords are either English words or look more or less like English words
- Plaintext organized into categories, e.g., "Customs Authorities"
- Plaintext and codewords are both in collating sequence order (a "one-part code")
- Specialized areas of discourse, but many variant sentences within each area
- Macro substitution

Numerical Tables



PART I — SHIPPING AND INSURANCE 337

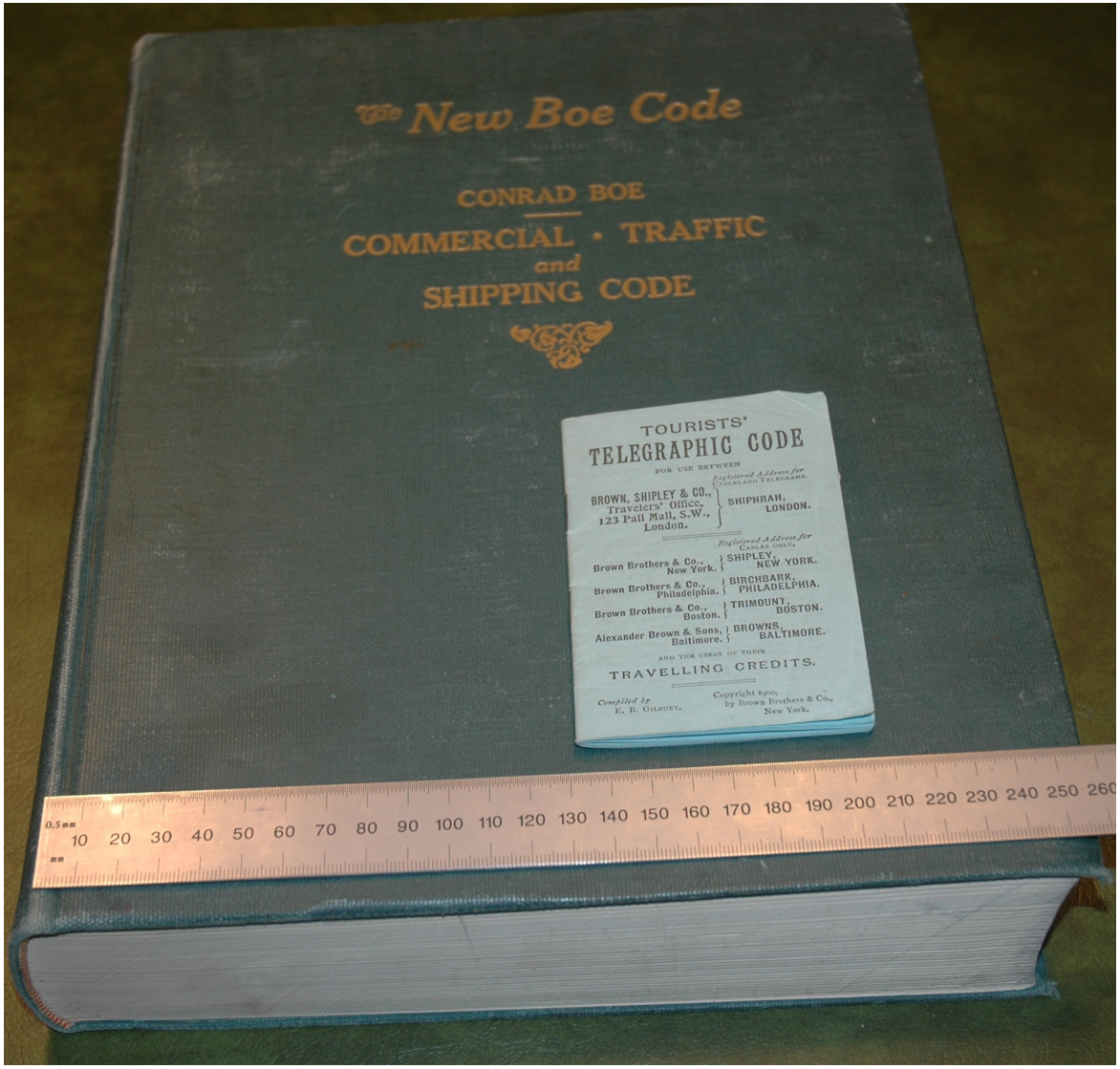
QUANTITY TABLES — *continued* JYLMO

JUTCU

Bags, Hogsheads, Pounds, or Yards		Casks, Chests, Quarters, or Reams		Barrels, Sheets, or Half Chests (Tea)		Kegs, Litres, Bushels, or Gross		Drums, Boxes, or Rolls		Gallons, Kilogrammes, Sacks, or Metres		Cases, Bales, or Ounces		Quantity
Code No.	Code Word	Code No.	Code Word	Code No.	Code Word	Code No.	Code Word	Code No.	Code Word	Code No.	Code Word	Code No.	Code Word	
45672	JUTCU	45731	JUYEG	45790	JVOEV	45849	JWOOS	45908	JXIVY	45967	JYCEN	46026	JYGOG	40
3	JUTEW	2	JUYFH	1	JVOHY	45850	JWORU	9	JXIXA	8	JYCFO	7	JYGUL	41
4	JUTGY	3	JUYGI	2	JVOIZ	1	JWOUX	45910	JXIYB	9	JYCIS	8	JYGXO	42
5	JUTIA	4	JUYHJ	3	JVOJA	2	JWOVY	1	JXOAP	45970	JYCKU	9	JYGYP	43
6	JUTME	5	JUYIK	4	JVONE	3	JWOXA	2	JXOEU	1	JYCOY	46030	JYHAU	44
7	JUTOG	6	JUYJL	5	JVOOF	4	JWOYB	3	JXOKA	2	JYCRA	1	JYHEY	45
8	JUTUL	7	JUYKM	6	JVOSI	5	JWUAN	4	JXOOE	3	JYCUD	2	JYHGA	46
9	JUTXO	8	JUYLN	7	JVOUK	6	JWUBO	5	JXOTI	4	JYCVE	3	JYHIC	47
45680	JUTYP	9	JUYMO	8	JVOYO	7	JWUES	6	JXOUJ	5	JYCYH	4	JYHKE	48
1	JUUBV	45740	JUYNP	9	JVUAB	8	JWUGU	7	JXOYN	6	JYCZI	5	JYHOI	49
2	JUUCW	1	JUYOR	45800	JVUDE	9	JWUIW	8	JXOZO	7	JYDAL	6	JYHUN	50
3	JUUDX	2	JUYPS	1	JVUEF	45860	JWUKY	9	JXYAI	8	JYDDO	7	JYHVO	51
4	JUUEY	3	JUYRT	2	JVUHI	1	JWUMA	45920	JXYEM	9	JYDEP	8	JYHYS	52
5	JUUFZ	4	JUYSU	3	JVUIJ	2	JWUOC	1	JXYGO	45980	JYDIU	9	JYIAW	53

Tables were used for dates, quantities, etc. Note the ambiguity in units: `JYCFO` could be `41 gallons`, `41 kilogrammes`, `41 sacks`, or `41 metres`

Size Matters Not



Domain-Specific Compression

- Many professions had their own code books
- Even explosives manufacturers had their own code
- Example: in the *The Theatrical Cipher Code*, `DISORB` meant `do not want drunkards` and `FILIATION` meant `chorus girls who are shapely and good looking`
- We still use domain-specific compression: Lempel-Ziv does not work nearly as well as JPEG and MP3 on pictures or audio files

The Theatrical Cipher Code (1905)

Filacer.....An opera company
Filament.....Are they willing to appear in tights
Filander..... Are you willing to appear in tights
Filar.....Ballet girls
Filaria.....Burlesque opera
Filature.....Burlesque opera company
File.....Burlesque people
Filefish..... Chorus girl
Filial..... Chorus girls
Filially..... Chorus girls who are
Filiation..... Chorus girls who are shapely and good looking
Filibuster..... Chorus girls who are shapely, good looking and can sing
Filicoid..... Chorus girls who can sing
Filiform.....Chorus man
Filigree.....Chorus men
Filing.....Chorus men who can sing
Fillet..... Chorus people
Fillip..... Chorus people who can sing
Filly.....Comic opera
Film.....Comic Opera Company
Filter.....Comic Opera people
Filtering.....Desirable chorus girl

Too Many Phrases?

- In the *ABC Code, Sixth Edition*, there were some very unusual phrases. . .
- `ENBET`: `Captain is insane`
- `PAASG`: `Arrived here (at ---), encountered a severe gale and heavy seas, which carried away boats and wheel, stanchions and bulwarks, broke mast and jib-boom, all sails gone`
- `ENIMP`: `Captured by pirates` (21 different code words dealing with captures; two whole pages on arrests!)
- In the 1930 *International Police Telegraph Code*, `IOL` is `Wishes to join Foreign Legion`

Compression Metrics

- The goal was not to minimize characters sent, it was to minimize *cost*
- Cost was affected by telegraph company tariffs and international regulations
- Permissible "words" changed over time: words in the local language, words in one of several languages, pseudo-words that were "pronounceable", ten letters with a certain vowel density — and ultimately, any five-letter sequence

Correction

Error Correction

- What about errors during transmission?
- In the police code, `SUB` is Vienna, but `SYB` is Jerusalem — and `U` and `Y` are adjacent on the keyboard
- Morse code had its own errors: `..-.` (`F`) could easily be received as `IN` (`.. -.`), `ER` (`. .-.`), or `UR` (`..- .`)

A U.S. Supreme Court Case

The plaintiff wanted this sent:

DESPOT AM EXCEEDINGLY BUSY BAY ALL KINDS QUO PERHAPS
BRACKEN HALF OF IT MINCE MOMENT PROMPTLY OF PURCHASES

It was received as

DESTROY AM EXCEEDINGLY BUSY BUY ALL KINDS QUO PERHAPS
BRACKEN HALF OF IT MINCE MOMENT PROMPTLY OF PURCHASE

What was meant? Who is liable?

Issues

- The message was mixed plaintext and code
- `BAY` was a code word; `buy` is plaintext. The two differ by a single dot ("_... ._ _.__" versus "_... ..._ _.__")
- As a result, the plaintiff's agent bought unwanted goods, resulting in a large loss
- The plaintiff had not requested reverse transmission as an error-check

Techniques

- Terminal indices
- Mutilation Tables
- Check digits
- Two-letter differences
- Avoidance of common words

Mutilation Tables

UK	QG	GW	XN	FV	SI	LB	VL	TJ	ND	HX
UN	QJ	GZ	XQ	FY	SL	LE	VO	TM	NG	HA
UR	QN	GD	XU	FC	SP	LI	VS	TQ	NK	HE
UX	QT	GJ	XA	FI	SV	LO	VY	TW	NQ	HK
UY	QU	GK	XB	FJ	SW	LP	VZ	TX	NR	HL
UU	QQ	GG	XX	FF	SS	LL	VV	TT	NN	HH
UB	QX	GN	XE	FM	SZ	LS	VC	TA	NU	HO
UZ	QV	GL	XC	FK	SX	LQ	VA	TY	NS	HM

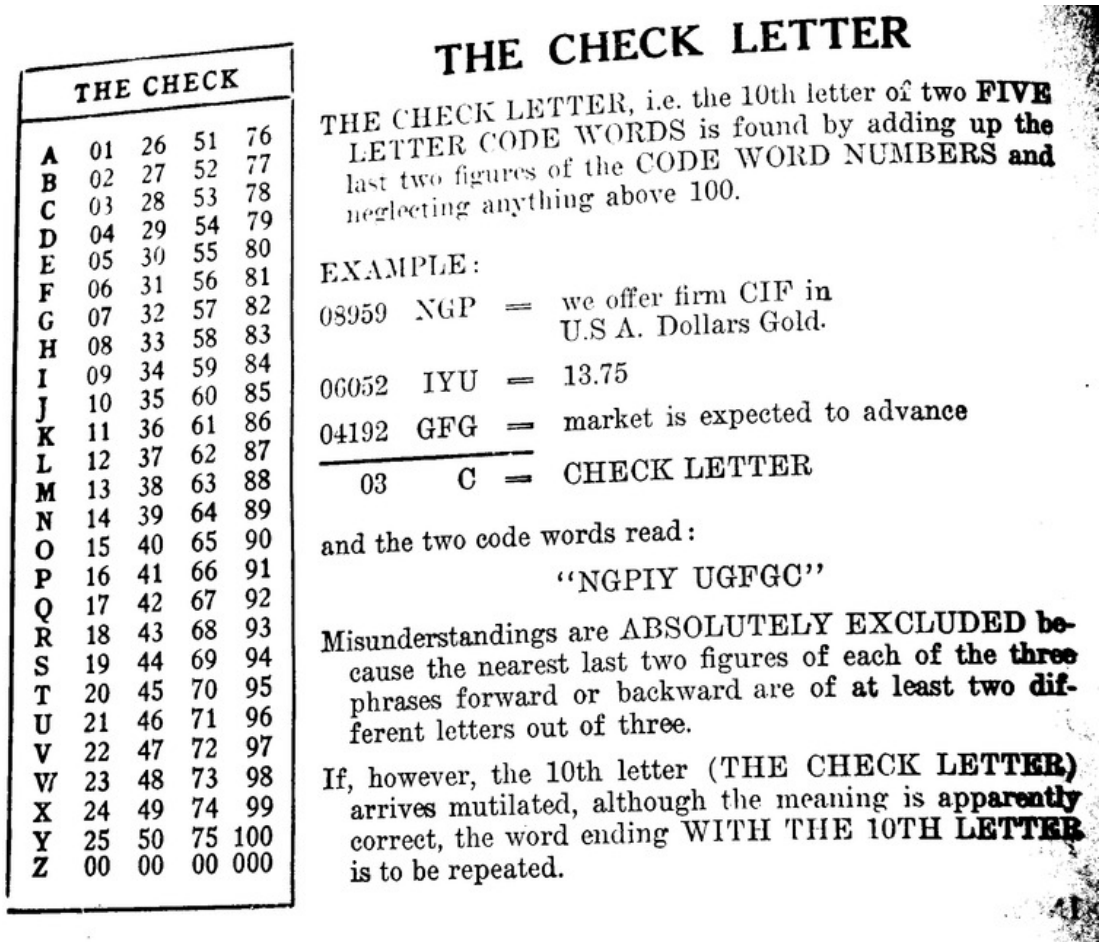
K	D	F	O	V	M	P	I	U	G	J	W
Q	J	L	U	A	S	V	O	B	M	P	D
Y	R	T	D	I	B	C	W	J	U	X	L
L	C	E	P	U	N	O	J	V	H	I	X
N	E	G	R	W	P	Q	L	X	J	K	Z
F	X	Z	J	O	H	I	D	P	B	C	R
T	K	M	X	D	V	W	R	C	P	Q	E
P	G	I	T	Y	R	S	N	Z	L	M	A

SECTION (SECCIÓN - SECÇ

TI	TR	TS	TK	TA	TJ	TX	TG	TN	TH	TU	TO
WL	WU	WV	WN	WD	WM	WA	WJ	WQ	WK	WX	WR
PE	PN	PO	PG	PW	PF	PT	PC	PJ	PD	PQ	PK
CR	CA	CB	CT	CJ	CS	CG	CQ	CW	CP	CD	CX
OD	OM	ON	OF	OV	OE	OS	OB	OI	OC	OP	OJ
XM	XV	XW	XO	XE	XN	XB	XK	XR	XL	XY	XS
FU	FD	FE	FW	FM	FV	FJ	FT	FZ	FS	FG	FA
SH	SQ	SR	SJ	SZ	SI	SW	SF	SM	SQ	ST	SN
DS	DB	DC	DU	DK	DT	DH	DR	DX	DQ	DE	DY

Look up the first two letters in the upper left, move across to the middle letter, move down to the lower table. Context often permits disambiguation of the possible original words from the five possibilities.

Check Digits



THE CHECK				
A	01	26	51	76
B	02	27	52	77
C	03	28	53	78
D	04	29	54	79
E	05	30	55	80
F	06	31	56	81
G	07	32	57	82
H	08	33	58	83
I	09	34	59	84
J	10	35	60	85
K	11	36	61	86
L	12	37	62	87
M	13	38	63	88
N	14	39	64	89
O	15	40	65	90
P	16	41	66	91
Q	17	42	67	92
R	18	43	68	93
S	19	44	69	94
T	20	45	70	95
U	21	46	71	96
V	22	47	72	97
W	23	48	73	98
X	24	49	74	99
Y	25	50	75	100
Z	00	00	00	000

THE CHECK LETTER

THE CHECK LETTER, i.e. the 10th letter of two **FIVE** LETTER CODE WORDS is found by adding up the last two figures of the CODE WORD NUMBERS and neglecting anything above 100.

EXAMPLE:

08959 NGP = we offer firm CIF in U.S A. Dollars Gold.

06052 IYU = 13.75

04192 GFG = market is expected to advance

03 C = CHECK LETTER

and the two code words read:

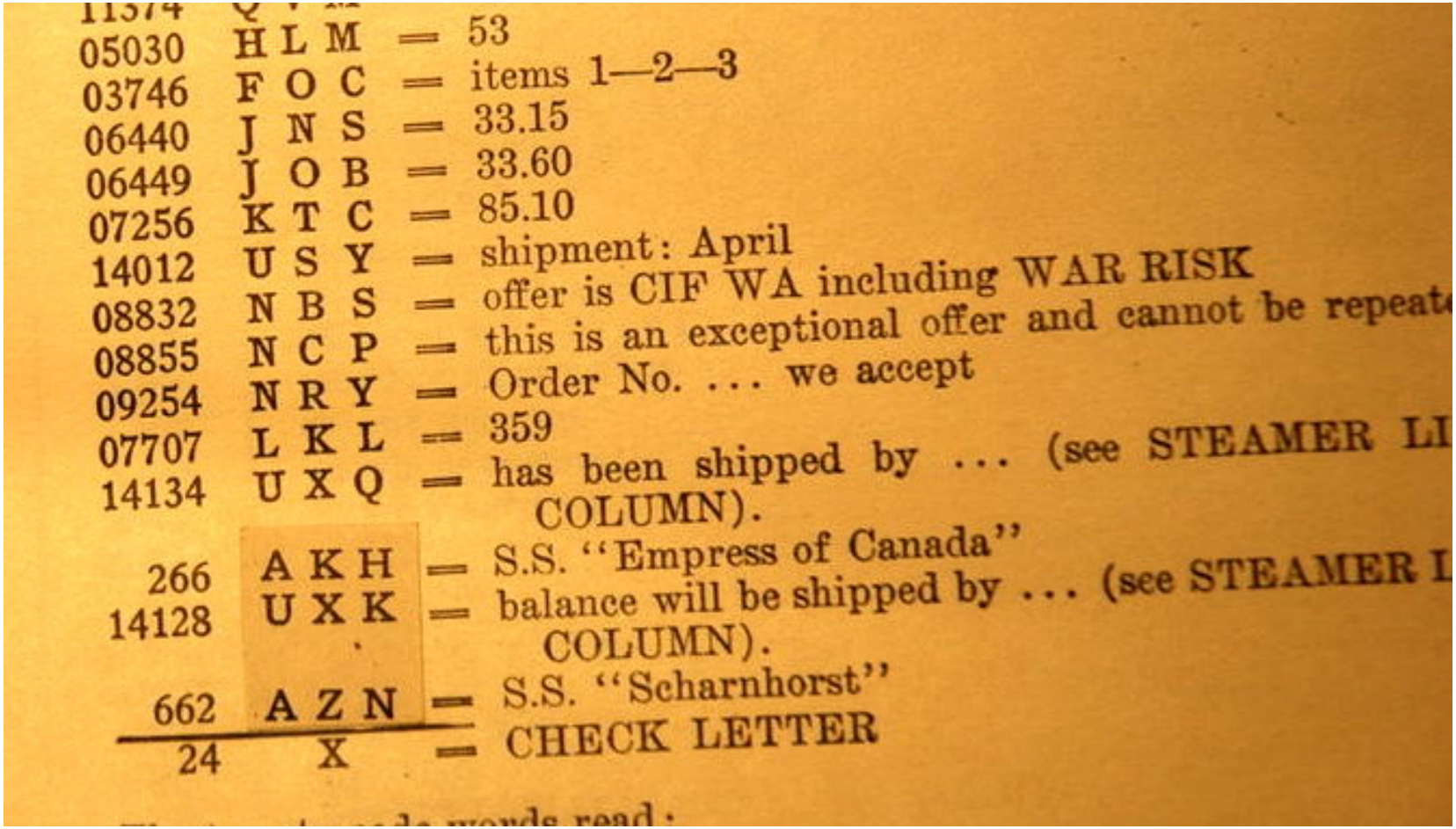
"NGPIY UGFGC"

Misunderstandings are ABSOLUTELY EXCLUDED because the nearest last two figures of each of the three phrases forward or backward are of at least two different letters out of three.

If, however, the 10th letter (THE CHECK LETTER) arrives mutilated, although the meaning is apparently correct, the word ending WITH THE 10TH LETTER is to be repeated.

Checksum calculations in the 1936 *Cosmos Trading Code*

Checksum Calculations Are Hard. . .



11374 Q [illegible]
05030 H L M = 53
03746 F O C = items 1—2—3
06440 J N S = 33.15
06449 J O B = 33.60
07256 K T C = 85.10
14012 U S Y = shipment: April
08832 N B S = offer is CIF WA including WAR RISK
08855 N C P = this is an exceptional offer and cannot be repeat
09254 N R Y = Order No. ... we accept
07707 L K L = 359
14134 U X Q = has been shipped by ... (see STEAMER LI
COLUMN).
266 A K H = S.S. "Empress of Canada"
14128 U X K = balance will be shipped by ... (see STEAMER L
COLUMN).
662 A Z N = S.S. "Scharnhorst"
24 X = CHECK LETTER
[illegible] words read:

Note the paste-over in the example.

Building a Vocabulary is Hard

Transposition	
HALAN	HAALN
IBLAN	IBALN
LELAN	LEALN
OGLAN	OGALN
QILAN	QIALN
UMLAN	UMALN
WOLAN	WOALN
ATLAN	ATALN
BULAN	BUALN
EXLAN	EXALN
FYLAN	FYALN

Letter Distance	
BEBPY	BEEPY
CIBPY	CIEPY
DOBPY	DOEPY
FUBPY	FUEPY
GABPY	GAEPY
TAUMY	TAZMY
WIUMY	WIZMY
YOUMY	YOZMY

Errors are in the Acme and Bentley code books. (Data from Jim Reeds.)

Common Words

- Many people mixed plaintext and codewords
- Better-designed codes avoided codewords that could be confused with plaintext in that field of discourse
- Not everyone got it right: the 1900 *Tourist's Telegraphic Code* did use `SUBWAY`, `REVOLT`, and `SAVAGERY`
- Perhaps their class of tourist didn't encounter such things. . .

Confidentiality

Confidentiality

- Paper letters were sealed, and thus were (theoretically) secure from sender to receiver
- Telegrams were handled by an intermediary, who could read them
- Many people perceived a need for encryption

The Secret Corresponding Vocabulary (1845)

C 1750.

1550		1600		1650		1700		1750	
1501	Chlorotic	1551	Chorus	1601	Chronological	1651	Churlish	1701	Ciphering
2	Chock	2	Chose	2	ally	2	ishly	2	key
3	Chocolate	3	en	3	Chronometer	3	ishness	3	Circassian
4	nut	4	Chouse	4	ric	4	ly	4	Circeon
5	Choice	5	ed	5	rical	5	Churn	5	Circle
6	less	6	ing	6	etry	6	ed	6	ed
7	ly	7	Chowder	7	Chrysalis	7	ing	7	er
8	ness	8	Christ	8	Chrysography	8	staff	8	et
9	Choir	9	less	9	Chrysolite	9	Chyle	9	ing
1510	service	1560	Christen	1610	Chub	1660	ifaction	1710	Circuit
1	Choke	1	dom	1	bed	1	ifactive	1	eer
2	cherry	2	ed	2	by	2	iferous	2	ous
3	ed	3	ing	3	faced	3	ous	3	ously

Encode to a letter/number pair. Encrypt by adding or subtracting a prearranged value from the number. For greater security, apply a monoalphabetic substitution to the letter.

Threat Models

"On the 1st February, 1870, the telegraph system throughout the United Kingdom passes into the hands of the Government, who will work the lines by Post Office officials. In other words, those who have hitherto so judiciously and satisfactorily managed the delivery of our sealed letters will in future be entrusted also with the transmission and delivery of our open letters in the shape of telegraphic communications, which will thus be exposed not only to the gaze of public officials, but from the necessity of the case must be read by them."

Slater's Telegraphic Code

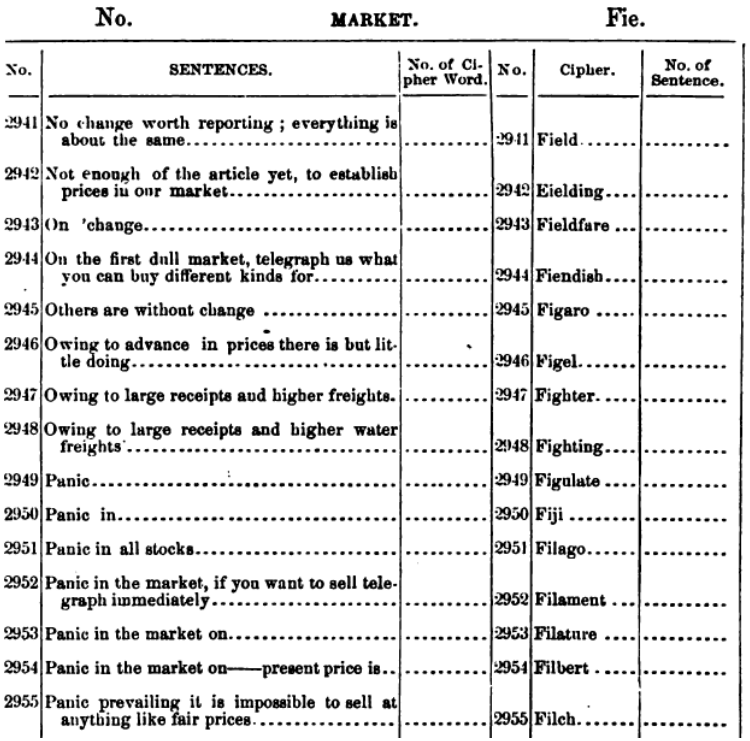
Slater's Code Book

- Long-lived: 1870–1939
- Encode to 5-digit numbers
- Use additives, transpositions, or combinations
- Map the resulting numbers to other code words
- Note: the resulting message was quite expensive: there was no error detection or compression, and the code words were expensive under later tariffs. But the code lasted for almost 70 years.

Bloomer's Commercial Cryptograph: A Telegraph Code and Double Index—Holocryptic Cipher (1874)

- Holocryptic: "wholly hidden or secret; spec. of a cipher incapable of being read except by those who have the key" (OED)
- Standard code words, code numbers, and phrases
- Suggestions for additives, transposition of code words, and user-generated two-part code variant
- Different additives could be used for different words (the holocryptic part)
- Room for user-created two-part codes

Room for a Two-Part Code



No. MARKET. Fie.

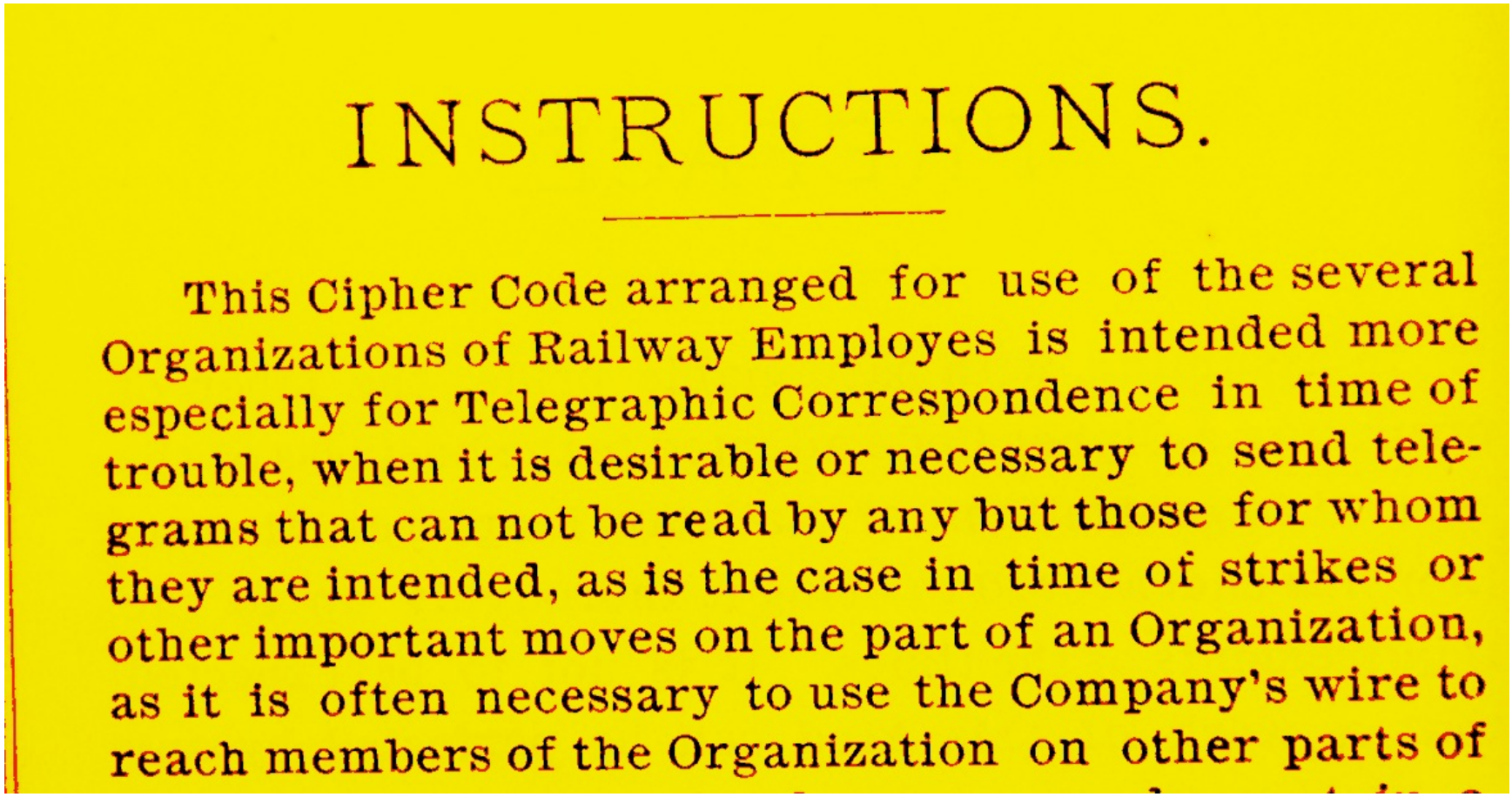
No.	SENTENCES.	No. of Cipher Word.	No.	Cipher.	No. of Sentence.
2941	No change worth reporting ; everything is about the same		2941	Field	
2942	Not enough of the article yet, to establish prices in our market		2942	Eielding	
2943	On 'change		2943	Fieldfare	
2944	On the first dull market, telegraph us what you can buy different kinds for		2944	Fiendish	
2945	Others are without change		2945	Figaro	
2946	Owing to advance in prices there is but little doing		2946	Figel	
2947	Owing to large receipts and higher freights.		2947	Fighter.	
2948	Owing to large receipts and higher water freights		2948	Fighting	
2949	Panic		2949	Figulate	
2950	Panic in		2950	Fiji	
2951	Panic in all stocks		2951	Filago	
2952	Panic in the market, if you want to sell telegraph immediately		2952	Filament	
2953	Panic in the market on		2953	Filature	
2954	Panic in the market on——present price is		2954	Filbert	
2955	Panic prevailing it is impossible to sell at anything like fair prices		2955	Filch	

Users were instructed to write their own numbers for codewords in column 3, and the corresponding decoding number for plaintext sentences in column 6 (the double-index technique).

Labor versus Management

- Railway workers had their own code, sometimes used to arrange strikes via the railway's own telegraph wires
- Management had its own secrecy codes
- From the examples I have, labor did a better job with their cryptography. . .

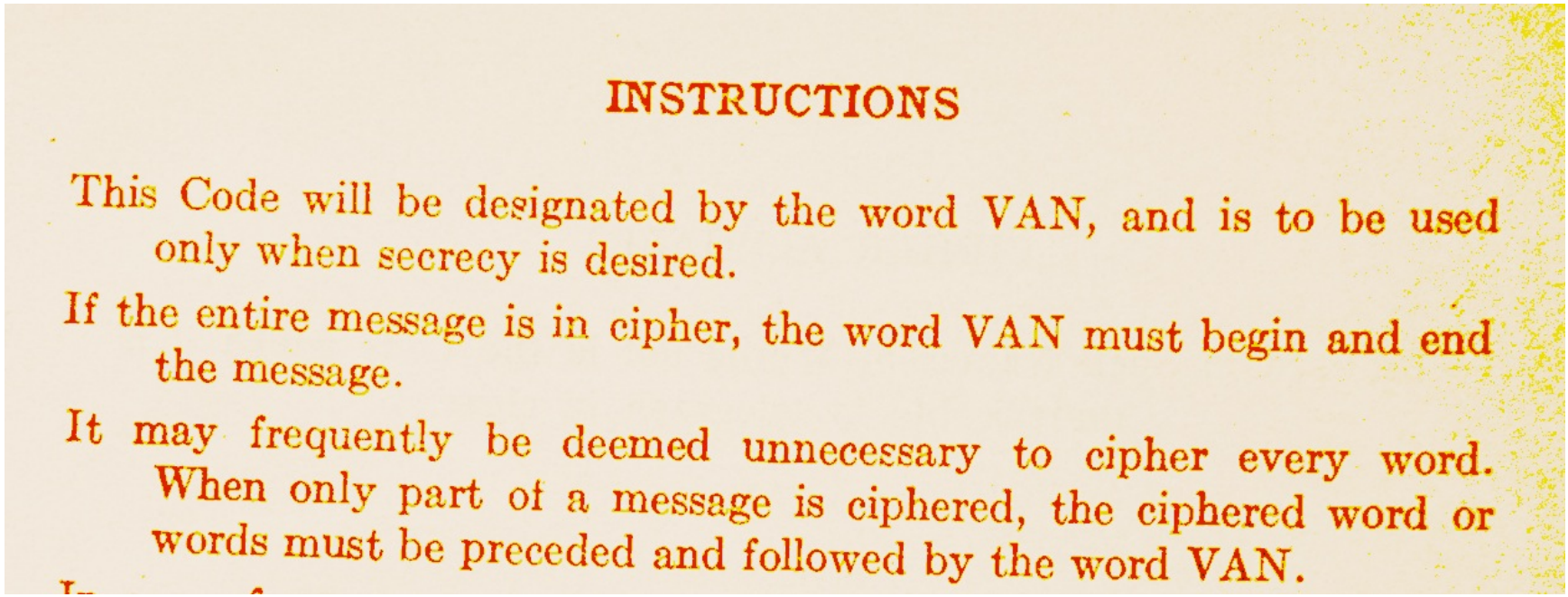
Sheahan's Code



INSTRUCTIONS.

This Cipher Code arranged for use of the several Organizations of Railway Employes is intended more especially for Telegraphic Correspondence in time of trouble, when it is desirable or necessary to send telegrams that can not be read by any but those for whom they are intended, as is the case in time of strikes or other important moves on the part of an Organization, as it is often necessary to use the Company's wire to reach members of the Organization on other parts of

The New York Central's Code



INSTRUCTIONS

This Code will be designated by the word VAN, and is to be used only when secrecy is desired.

If the entire message is in cipher, the word VAN must begin and end the message.

It may frequently be deemed unnecessary to cipher every word. When only part of a message is ciphered, the ciphered word or words must be preceded and followed by the word VAN.

A Cryptanalytic Assessment

- Few approached Slater's or Bloomer's sophistication
- Most commercial codes used a constant additive, then mapped back to code word space
- Governments were often no better:

  > "When a single key number is used, the number may be alternately added and subtracted. Other methods will readily occur. The use of 50 or 100, while easy to remember, should be avoided."

  (U.S. War Department, 1904)

Why Map to Code Word Space?

- Code words were cheaper than numeric groups
- Code words had error-detecting and error-correcting properties

Comprehension

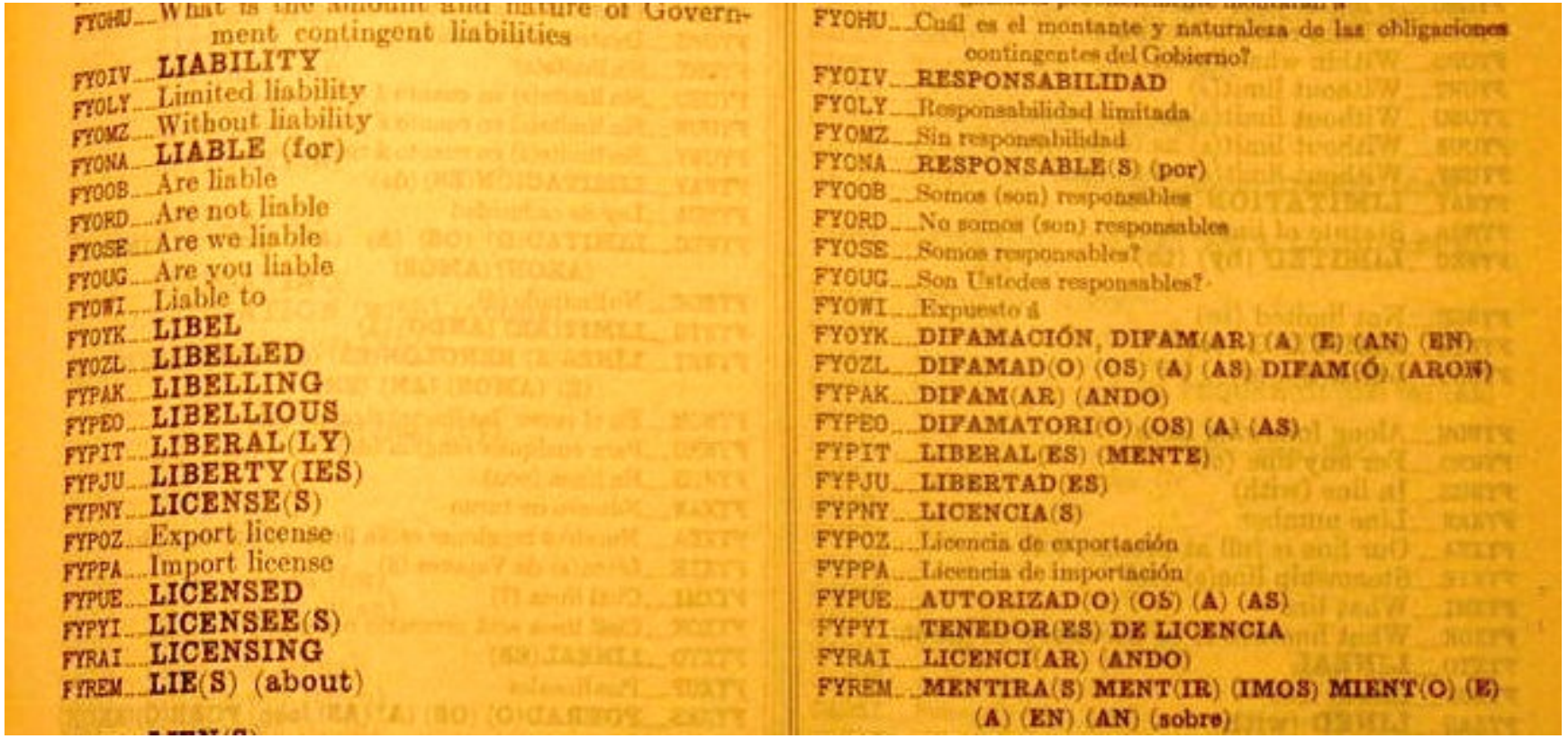
Comprehension

- "A code reflects the world at a particular instant, and as the world moves on it outmodes the code. New products, new ways of doing things, new political or economic facts begin to make its vocabulary old-fashioned." (Kahn)
- Code books present a picture of a given era
- Code books could also be used for translation

A Bygone Age

- `NASUM: Marriage has been arranged between ____` (*Unicode*, 1897)
- `MORDAX: Will lunch with you today` (*Unicode*)
- 23697: `Roman Catholic intrigue` (*China Inland Mission Private Telegraph Code*, 1907)
- `N.O.M.: Send women on shore to wash` (Popham's Naval Signal Code, under "Military and Technical Terms", 1816)
- Professions: `HKO` (`castle-keeper`) and `HKZ` (`boy`) (*International Police Telegraph Code*, 1930)

Translations

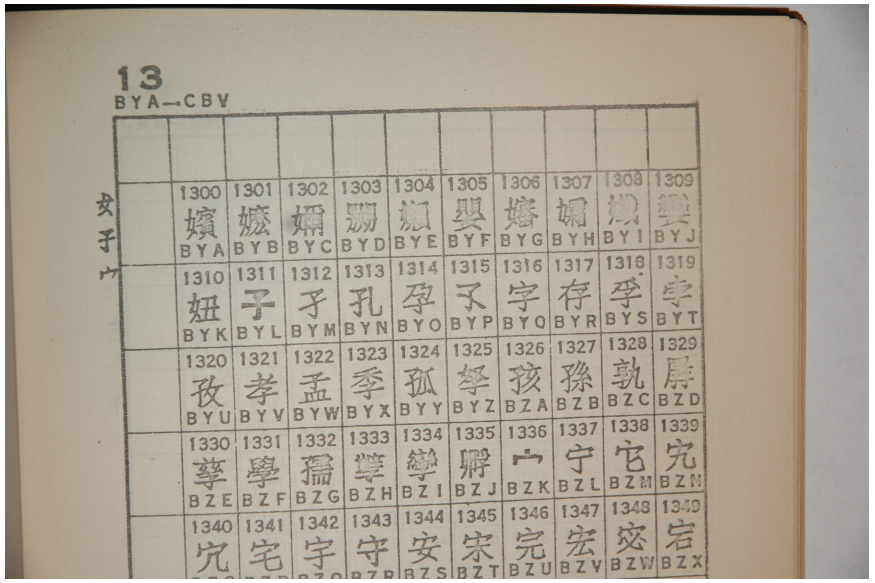


FYOHU What is the amount and nature of Government contingent liabilities
FYOIV LIABILITY
FYOLY Limited liability
FYOMZ Without liability
FYONA LIABLE (for)
FYOOB Are liable
FYORD Are not liable
FYOSE Are we liable
FYOUG Are you liable
FYOWI Liable to
FYOYK LIBEL
FYOZL LIBELLED
FYPAK LIBELLING
FYPEO LIBELLIOUS
FYPIT LIBERAL(LY)
FYPJU LIBERTY(IES)
FYPNY LICENSE(S)
FYPOZ Export license
FYPPA Import license
FYPUE LICENSED
FYPYI LICENSEE(S)
FYRAI LICENSING
FYREM LIE(S) (about)

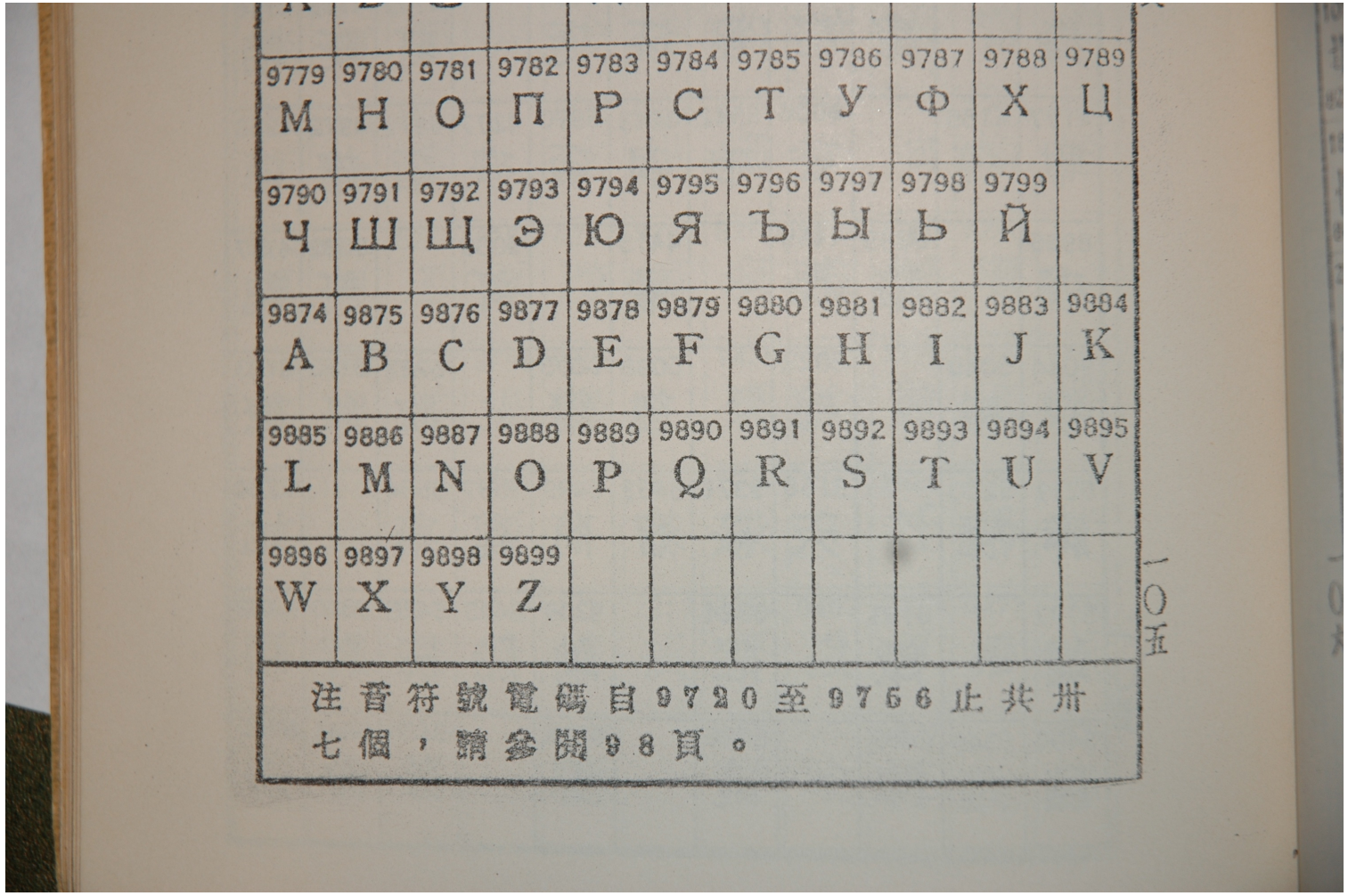
FYOHU Cuál es el montante y naturaleza de las obligaciones contingentes del Gobierno?
FYOIV RESPONSABILIDAD
FYOLY Responsabilidad limitada
FYOMZ Sin responsabilidad
FYONA RESPONSABLE(S) (por)
FYOOB Somos (son) responsables
FYORD No somos (son) responsables
FYOSE Somos responsables?
FYOUG Son Ustedes responsables?
FYOWI Expuesto á
FYOYK DIFAMACIÓN, DIFAM(AR) (A) (E) (AN) (EN)
FYOZL DIFAMAD(O) (OS) (A) (AS) DIFAM(Ó) (ARON)
FYPAK DIFAM(AR) (ANDO)
FYPEO DIFAMATORI(O) (OS) (A) (AS)
FYPIT LIBERAL(ES) (MENTE)
FYPJU LIBERTAD(ES)
FYPNY LICENCIA(S)
FYPOZ Licencia de exportación
FYPPA Licencia de importación
FYPUE AUTORIZAD(O) (OS) (A) (AS)
FYPYI TENEDOR(ES) DE LICENCIA
FYRAI LICENCI(AR) (ANDO)
FYREM MENTIRA(S) MENT(IR) (IMOS) MIENT(O) (E) (A) (EN) (AN) (sobre)

Sending Chinese Characters

- 4-digit/3-letter link-layer encoding for each Chinese character
- Widely used in China until about 10 years ago — faxes and cell phones have taken over
- Code points are still used today to enter names on official forms: dialect-independent, unambiguous, etc.



Code Points for Other Alphabets



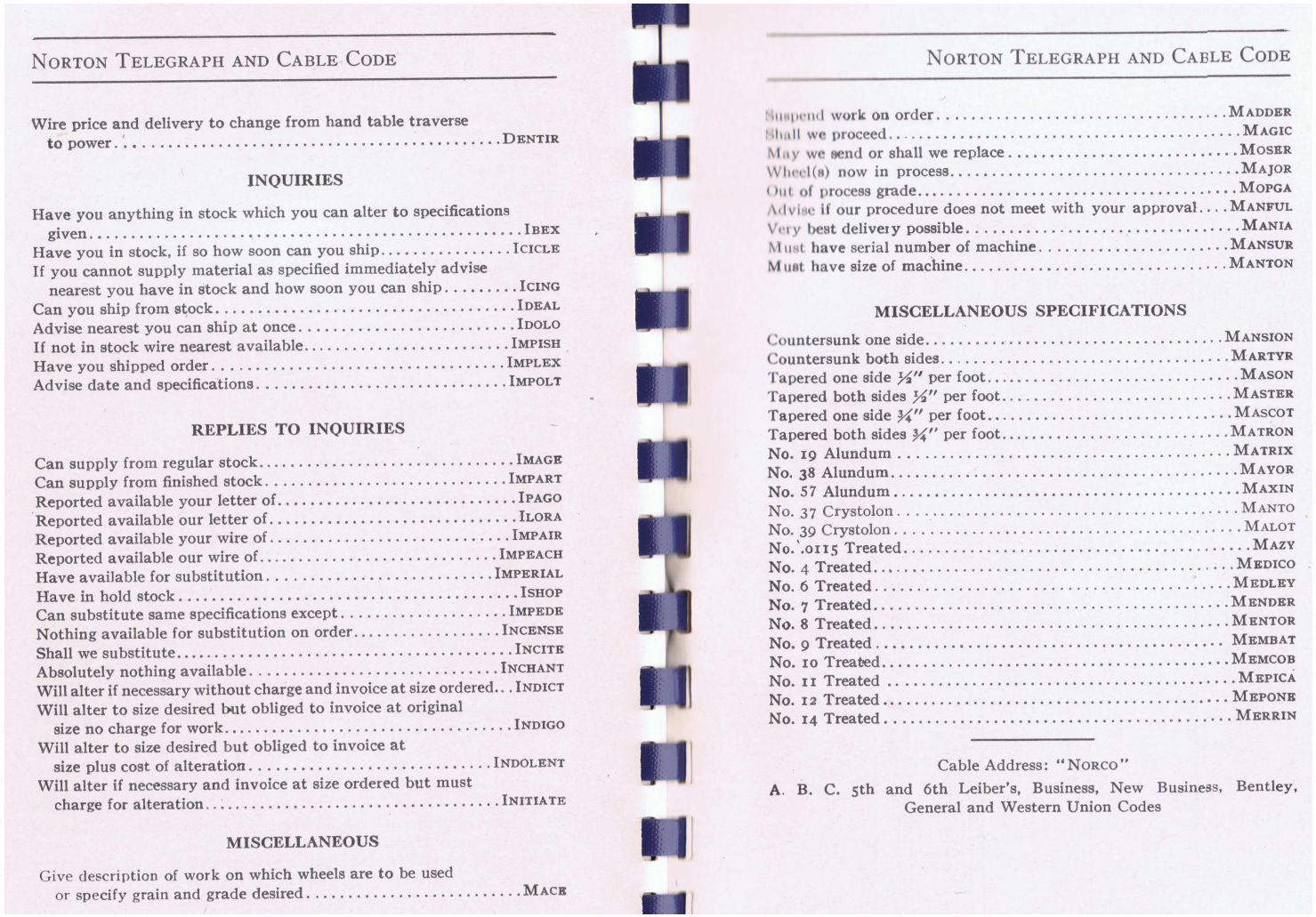
9779 М	9780 Н	9781 О	9782 П	9783 Р	9784 С	9785 Т	9786 У	9787 Ф	9788 Х	9789 Ц
9790 Ч	9791 Ш	9792 Щ	9793 Э	9794 Ю	9795 Я	9796 Ъ	9797 Ы	9798 Ь	9799 Й	
9874 A	9875 B	9876 C	9877 D	9878 E	9879 F	9880 G	9881 H	9882 I	9883 J	9884 K
9885 L	9886 M	9887 N	9888 O	9889 P	9890 Q	9891 R	9892 S	9893 T	9894 U	9895 V
9896 W	9897 X	9898 Y	9899 Z							

注音符號電碼自9720至9756止共卅七個，請參閱98頁。

Cultural Norms: A Woodblock Tibetan Codebook (1949/1985)

Cultural Norms: An Illuminated Persian Government Codebook (1901)

Pervasive Codes: Catalogs



NORTON TELEGRAPH AND CABLE CODE

Wire price and delivery to change from hand table traverse to power ..... DENTIR

INQUIRIES

Have you anything in stock which you can alter to specifications given ..... IBEX
Have you in stock, if so how soon can you ship ..... ICICLE
If you cannot supply material as specified immediately advise nearest you have in stock and how soon you can ship ..... ICING
Can you ship from stock ..... IDEAL
Advise nearest you can ship at once ..... IDOLO
If not in stock wire nearest available ..... IMPISH
Have you shipped order ..... IMPLEX
Advise date and specifications ..... IMPOLT

REPLIES TO INQUIRIES

Can supply from regular stock ..... IMAGE
Can supply from finished stock ..... IMPART
Reported available your letter of ..... IPAGO
Reported available our letter of ..... ILORA
Reported available your wire of ..... IMPAIR
Reported available our wire of ..... IMPEACH
Have available for substitution ..... IMPERIAL
Have in hold stock ..... ISHOP
Can substitute same specifications except ..... IMPEDE
Nothing available for substitution on order ..... INCENSE
Shall we substitute ..... INCITE
Absolutely nothing available ..... INCHANT
Will alter if necessary without charge and invoice at size ordered ..... INDICT
Will alter to size desired but obliged to invoice at original size no charge for work ..... INDIGO
Will alter to size desired but obliged to invoice at size plus cost of alteration ..... INDOLENT
Will alter if necessary and invoice at size ordered but must charge for alteration ..... INITIATE

MISCELLANEOUS

Give description of work on which wheels are to be used or specify grain and grade desired ..... MACE

NORTON TELEGRAPH AND CABLE CODE

Suspend work on order ..... MADDER
Shall we proceed ..... MAGIC
May we send or shall we replace ..... MOSER
Wheel(s) now in process ..... MAJOR
Out of process grade ..... MOPGA
Advise if our procedure does not meet with your approval ..... MANFUL
Very best delivery possible ..... MANIA
Must have serial number of machine ..... MANSUR
Must have size of machine ..... MANTON

MISCELLANEOUS SPECIFICATIONS

Countersunk one side ..... MANSION
Countersunk both sides ..... MARTYR
Tapered one side ½" per foot ..... MASON
Tapered both sides ½" per foot ..... MASTER
Tapered one side ¾" per foot ..... MASCOT
Tapered both sides ¾" per foot ..... MATRON
No. 19 Alundum ..... MATRIX
No. 38 Alundum ..... MAYOR
No. 57 Alundum ..... MAXIN
No. 37 Crystolon ..... MANTO
No. 39 Crystolon ..... MALOT
No. .0115 Treated ..... MAZY
No. 4 Treated ..... MEDICO
No. 6 Treated ..... MEDLEY
No. 7 Treated ..... MENDER
No. 8 Treated ..... MENTOR
No. 9 Treated ..... MEMBAT
No. 10 Treated ..... MEMCOB
No. 11 Treated ..... MEPICA
No. 12 Treated ..... MEPONE
No. 14 Treated ..... MERRIN

Cable Address: "NORCO"

A. B. C. 5th and 6th Leiber's, Business, New Business, Bentley, General and Western Union Codes

Code Books Were Expensive

- Some code books contained advertisements
- Usually, these were business-oriented; some, though, were aimed at households
- An 1896 code book cost $5.00; in 1915, a room at the Biltmore Hotel in New York could cost $2.50.
- (Note: about 5% of their rooms didn't have private baths. . .)

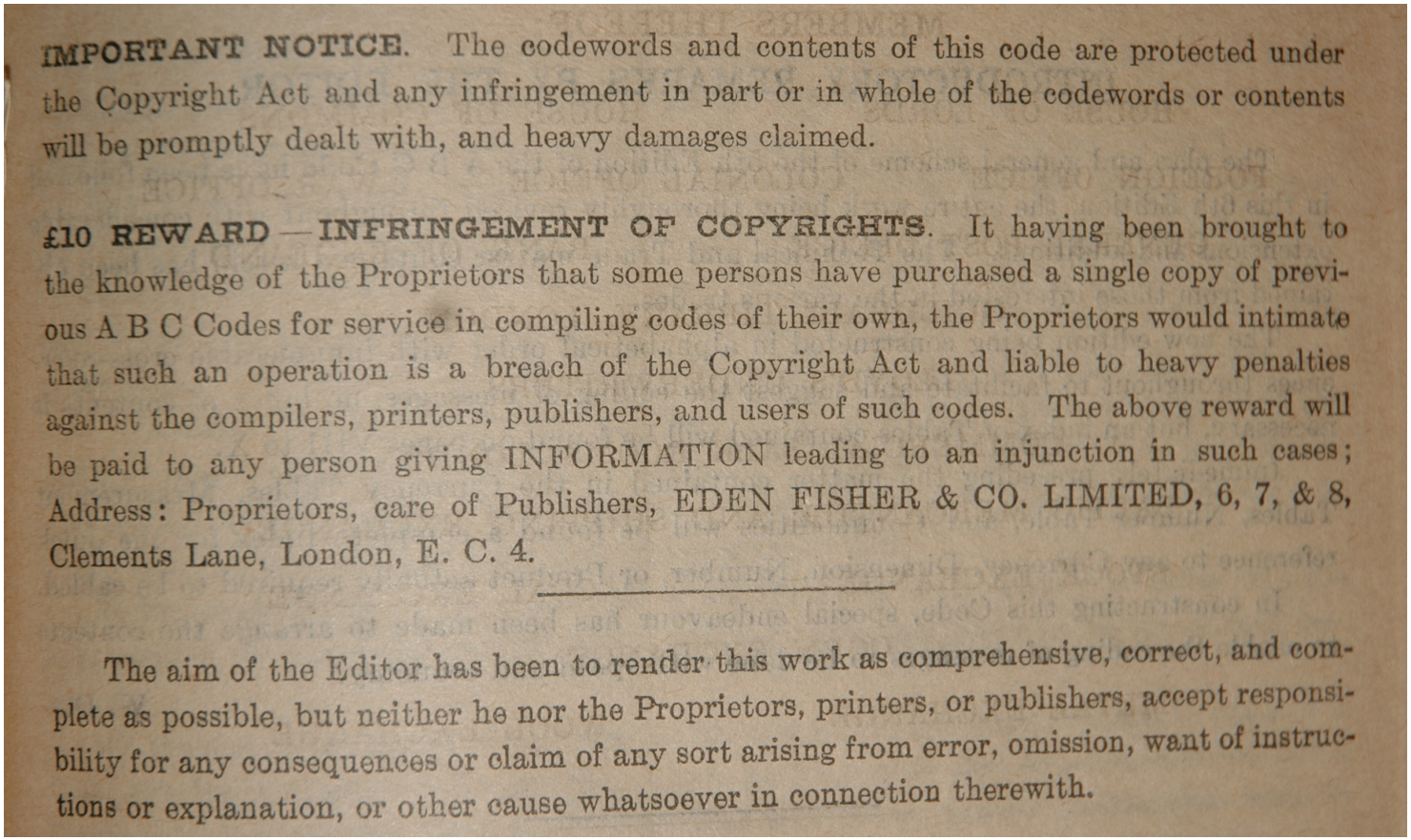
There Was a Confidentiality Threat!

- The Official Secrets Act (1920) required British cable companies to turn over copies of all international telegrams
- (An American executive — of a company with strong British ties — assured Congress that it was all for show. . .)
- To protect its own traffic, Britain strove to expand the "All-Red Route"

Copyright

- Under U.S. law of the time, books were not protected by copyright unless they were first printed in the U.S. (The U.S. didn't sign the Berne Convention until 1976.)
- The ABC Code was (legally) reprinted within the US
- The code words were used to build other codes
- But — importation of U.S. editions into the British Empire was illegal
- British publishers sometimes printed first in the U.S., just to protect copyright

Compiling Your Own Code?

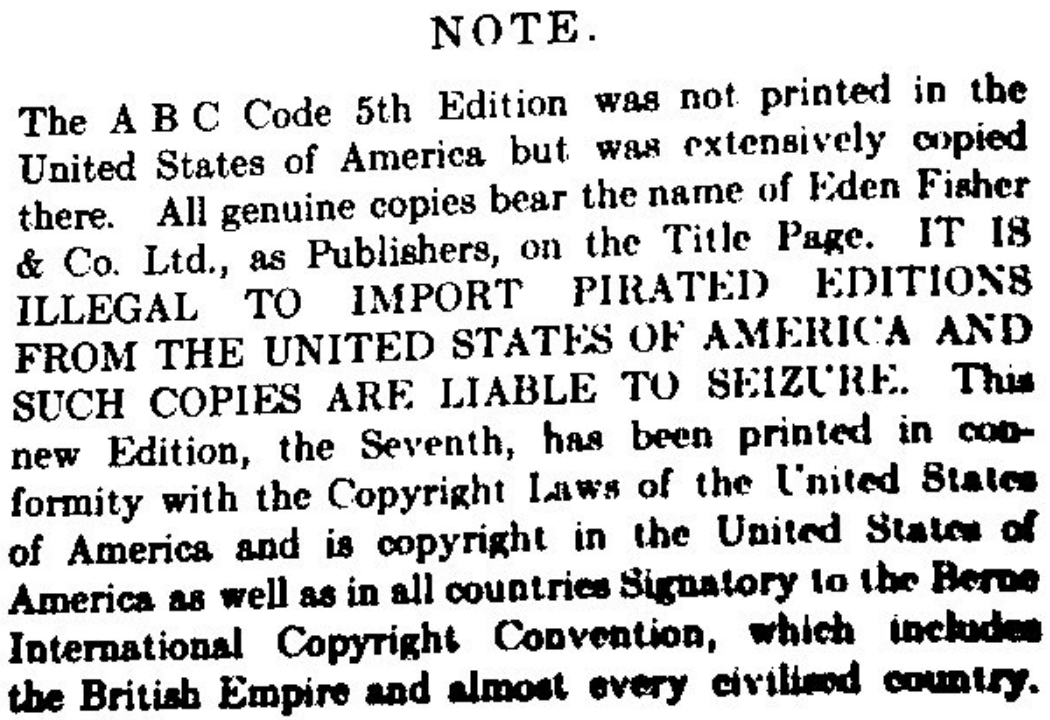


IMPORTANT NOTICE. The codewords and contents of this code are protected under the Copyright Act and any infringement in part or in whole of the codewords or contents will be promptly dealt with, and heavy damages claimed.

£10 REWARD — INFRINGEMENT OF COPYRIGHTS. It having been brought to the knowledge of the Proprietors that some persons have purchased a single copy of previous A B C Codes for service in compiling codes of their own, the Proprietors would intimate that such an operation is a breach of the Copyright Act and liable to heavy penalties against the compilers, printers, publishers, and users of such codes. The above reward will be paid to any person giving INFORMATION leading to an injunction in such cases; Address: Proprietors, care of Publishers, EDEN FISHER & CO. LIMITED, 6, 7, & 8, Clements Lane, London, E. C. 4.

The aim of the Editor has been to render this work as comprehensive, correct, and complete as possible, but neither he nor the Proprietors, printers, or publishers, accept responsibility for any consequences or claim of any sort arising from error, omission, want of instructions or explanation, or other cause whatsoever in connection therewith.

Copyright Infringement Without the Internet



NOTE.

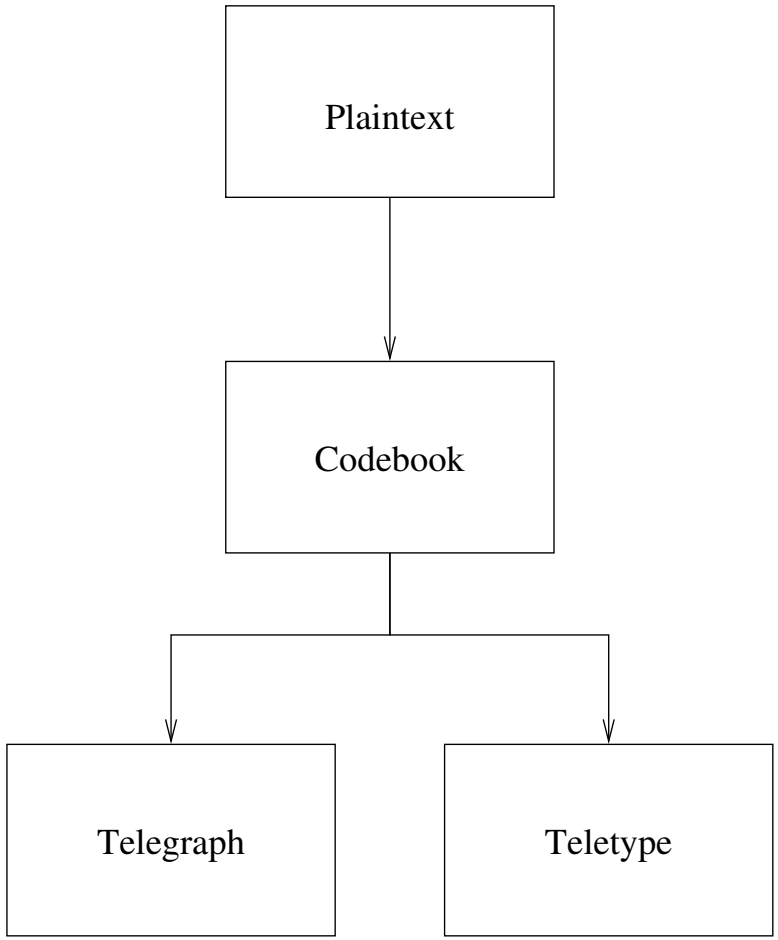
The A B C Code 5th Edition was not printed in the United States of America but was extensively copied there. All genuine copies bear the name of Eden Fisher & Co. Ltd., as Publishers, on the Title Page. IT IS ILLEGAL TO IMPORT PIRATED EDITIONS FROM THE UNITED STATES OF AMERICA AND SUCH COPIES ARE LIABLE TO SEIZURE. This new Edition, the Seventh, has been printed in conformity with the Copyright Laws of the United States of America and is copyright in the United States of America as well as in all countries Signatory to the Berne International Copyright Convention, which includes the British Empire and almost every civilised country.

Was the U.S. considered "civilised" then?

The Telegraph Stack

Different Layers

- Codes were used for compression, confidentiality, and compression
- There were different layers — and each function could be done at each layer
- There were different tradeoffs



The Plaintext Layer

- Compression: Restricted word choice; stylized sentences; sentence fragments that will be concatenated
- Semantic confidentiality — combine numerical fields based on knowledge of ranges
- Encode numbers via code book even if not otherwise needed, because words are easier to transmit correctly

The Link Layer

- Confidentiality: avoid exposed links (radio; links not on the All-Red Route)
- Correction: different links have different error properties
- Compression metrics

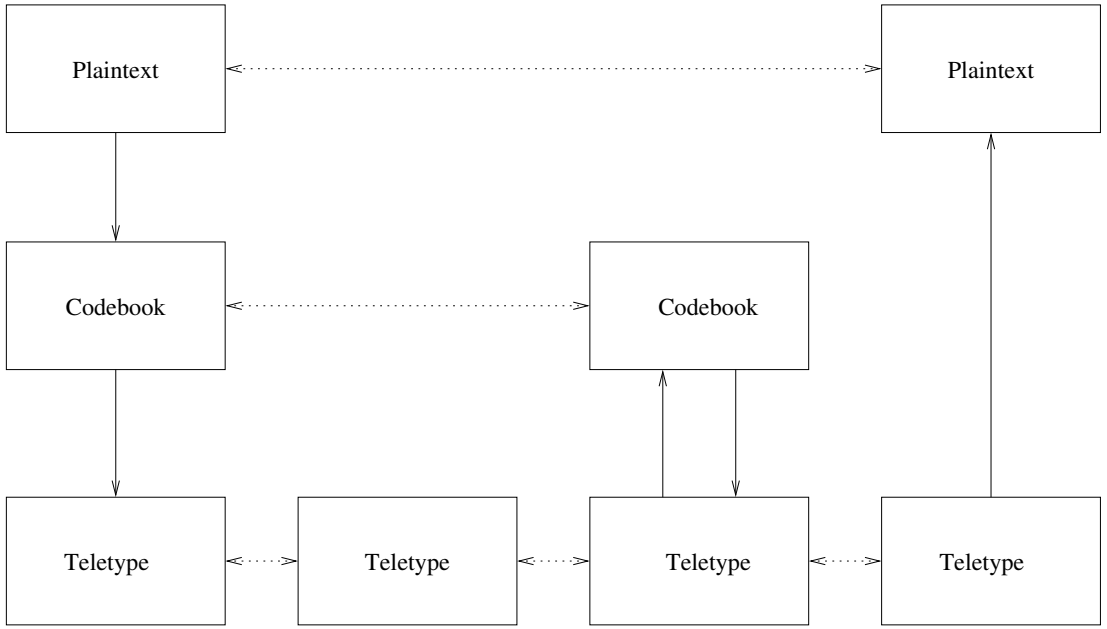
(What's a Teletype?)

(Picture courtesy of Perry Metzger; taken at Bletchley Park)

Compression Metrics

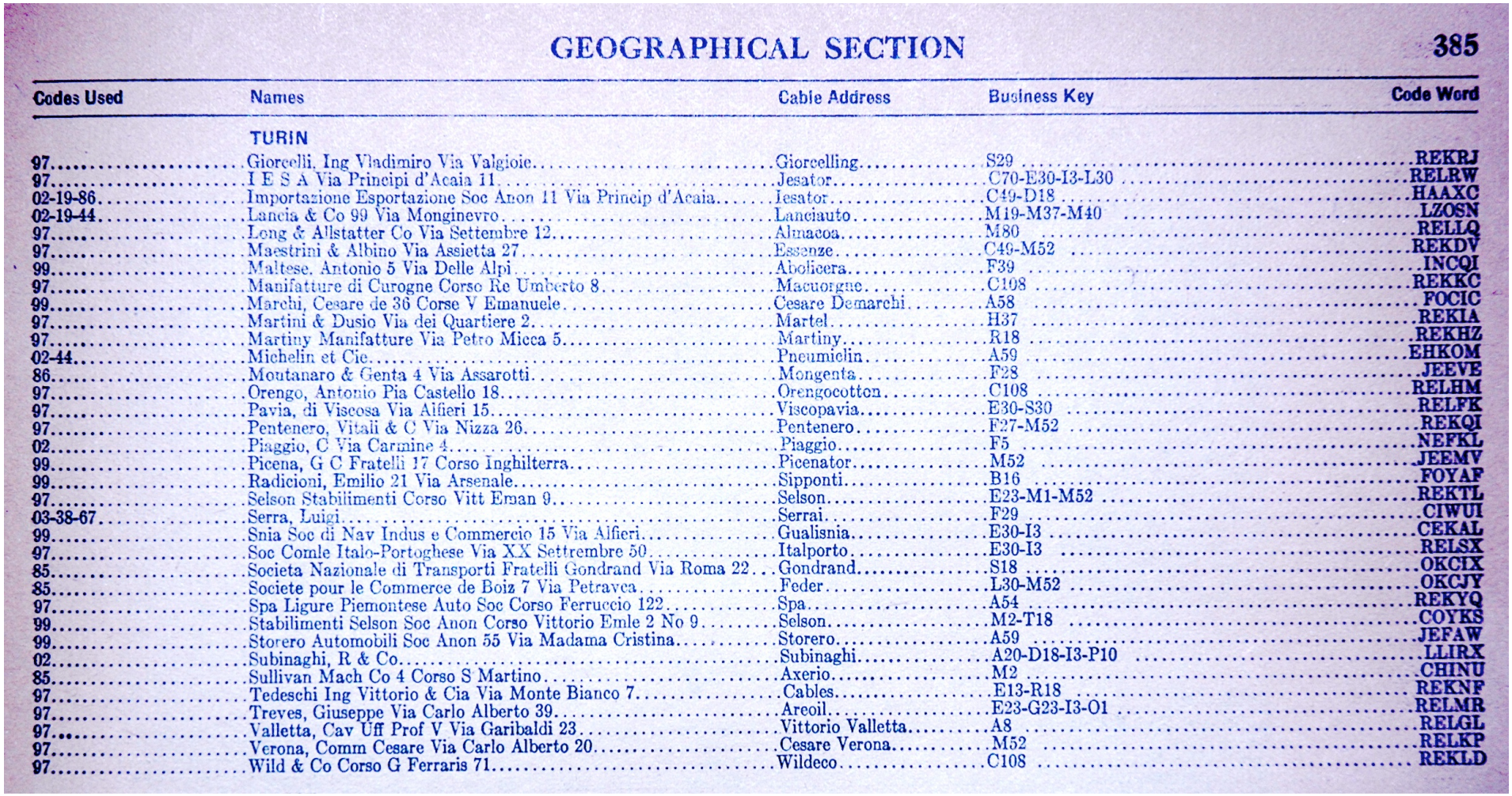
- Optimize cost, not transmission time
- Codebooks evolved as tariffs evolved
- An adversarial process between code compilers and telegraph companies
- This is a security interaction!

End-to-End vs. Hop-by-Hop



Telegrams were often sent via multiple hops, and sometimes to a decoding service. Confidentiality at a lower layer protected that layer, or perhaps even that hop, but not the end-to-end message. VPNs often have that problem today.

A DNS Analog



GEOGRAPHICAL SECTION 385

Codes Used	Names	Cable Address	Business Key	Code Word
	TURIN			
97	Giorcelli, Ing Vladimiro Via Valgioie	Giorcelling	S29	REKRJ
97	I E S A Via Principi d'Acaia 11	Jesator	C70-E30-I3-L30	RELRW
02-19-86	Importazione Esportazione Soc Anon 11 Via Princip d'Acaia	Jesator	C49-D18	HAAXC
02-19-44	Lancia & Co 99 Via Monginevro	Lanciauto	M19-M37-M40	LZOSN
97	Long & Allstatter Co Via Settembre 12	Almacoa	M80	RELLQ
97	Maestrini & Albino Via Assietta 27	Essenze	C49-M52	REKDV
99	Maltese, Antonio 5 Via Delle Alpi	Abolicera	F39	INCQI
97	Manifatture di Curogne Corso Re Umberto 8	Macuorgne	C108	REKKC
99	Marchi, Cesare de 36 Corse V Emanuele	Cesare Demarchi	A58	FOCIC
97	Martini & Dusio Via dei Quartiere 2	Martel	H37	REKIA
97	Martiny Manifatture Via Petro Micca 5	Martiny	R18	REKHZ
02-44	Michelin et Cie	Pneumiclin	A59	EHKOM
86	Moutanaro & Genta 4 Via Assarotti	Mongenta	F28	JEEVE
97	Orengo, Antonio Pia Castello 18	Orengocotton	C108	RELHM
97	Pavia, di Viscosa Via Alfieri 15	Viscopavia	E30-S30	RELFK
97	Pentenero, Vitali & C Via Nizza 26	Pentenero	F27-M52	REKQI
02	Piaggio, C Via Carmine 4	Piaggio	F5	NEFKL
99	Picena, G C Fratelli 17 Corso Inghilterra	Picenator	M52	JEEMV
99	Radicioni, Emilio 21 Via Arsenale	Sipponti	B16	FOYAF
97	Selson Stabilimenti Corso Vitt Eman 9	Selson	E23-M1-M52	REKTL
03-38-67	Serra, Luigi	Serrai	F29	CIWUI
99	Snia Soc di Nav Indus e Commercio 15 Via Alfieri	Gualisnia	E30-I3	CEKAL
97	Soc Comle Italo-Portoghese Via XX Settrembre 50	Italporto	E30-I3	RELSX
85	Societa Nazionale di Transporti Fratelli Gondrand Via Roma 22	Gondrand	S18	OKCIX
85	Societe pour le Commerce de Boiz 7 Via Petravca	Feder	L30-M52	OKCJY
97	Spa Ligure Piemontese Auto Soc Corso Ferruccio 122	Spa	A54	REKYQ
99	Stabilimenti Selson Soc Anon Corso Vittorio Emle 2 No 9	Selson	M2-T18	COYKS
99	Storero Automobili Soc Anon 55 Via Madama Cristina	Storero	A59	JEFAW
02	Subinaghi, R & Co	Subinaghi	A20-D18-I3-P10	LLIRX
85	Sullivan Mach Co 4 Corso S Martino	Axerio	M2	CHINU
97	Tedeschi Ing Vittorio & Cia Via Monte Bianco 7	Cables	E13-R18	REKNF
97	Treves, Giuseppe Via Carlo Alberto 39	Arcoil	E23-G23-I3-O1	RELMR
97	Valletta, Cav Uff Prof V Via Garibaldi 23	Vittorio Valletta	A8	RELGL
97	Verona, Comm Cesare Via Carlo Alberto 20	Cesare Verona	M52	RELKP
97	Wild & Co Corso G Ferraris 71	Wildeco	C108	REKLD

Parting Thoughts

- Telegraph codebooks were used in Australia until at least 1972, and China until around 2000
- What we do today is the evolution of what was done then
- Huffman didn't invent compression; Hamming didn't invent error correction; NIST didn't invent encryption

Thanks to. . .

- Jim Reeds
- Hang Zhao, Seung Geol Choi Evelyn Guzman, Malek Ben Salem, Arezu Moghadam, and Ted Lemon
- The research libraries and librarians of the world
- Google Books

Draft paper at papers/codebooks.pdf on my web page.