Compression, Correction, Confidentiality, and Comprehension:
A Modern Look at Telegraph Codebooks

Abstract

Telegraph codes are a more-or-less forgotten part of technological history. In their day, though, they were ubiquitous and sophisticated. They also laid the groundwork for many of today's communications technologies, including encryption, compression, and error correction. Beyond that, reading them provides a snapshot into culture. We look back, describing them in modern terms, and noting some of the tradeoffs considered.

Keywords: telegraph; codebooks; cryptology

1 Introduction

Most cryptologists have heard of telegraph codebooks. Often, though, our knowledge is cursory. We've forgotten what we read in Kahn (1967), and perhaps remember little more than the basic concept: a word, phrase, or sentence is represented by a single codeword. In fact, telegraph codes, from the tiny to the very large (Figure 1), were far more sophisticated, and laid the groundwork for many later, fundamental advances.

Looked at analytically, telegraph codes fulfilled four primary functions: compression, correction, confidentiality, and comprehension. Beyond that, they offer a window into the past: the phrases they can be used to represent give insight into daily lives of the time.

This paper, based to some extent on my own modest collection of codebooks, illustrates some of these points. (The collection has since been donated to the National Cryptologic Museum.)

For typographical simplicity, I have written codewords **LIKE THIS**, while plaintext is written THIS WAY.

2 Compression

Compression was the original goal of telegraph codes. Early trans-Atlantic telegrams were *extremely* expensive—$100 for twenty words in 1866 (Headrick 1991)—so brevity was very important.

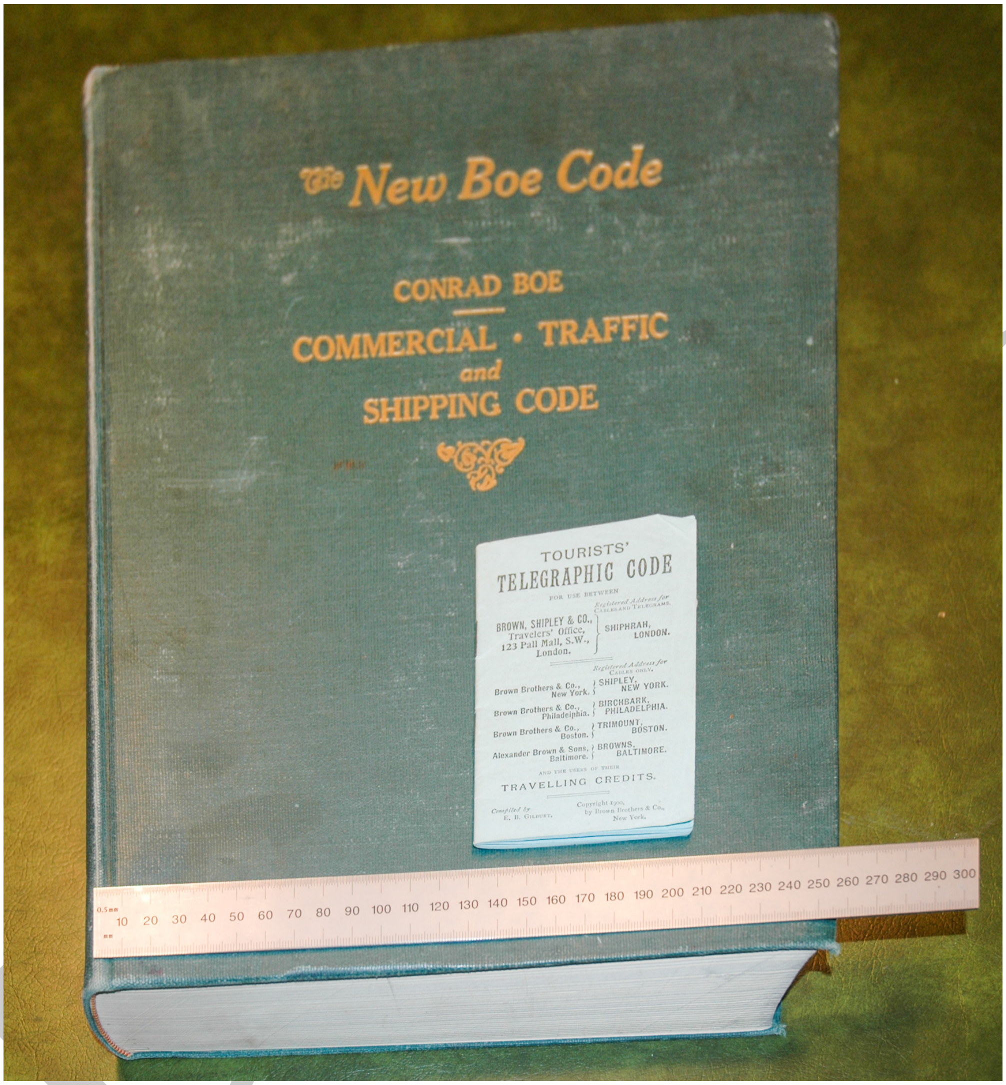
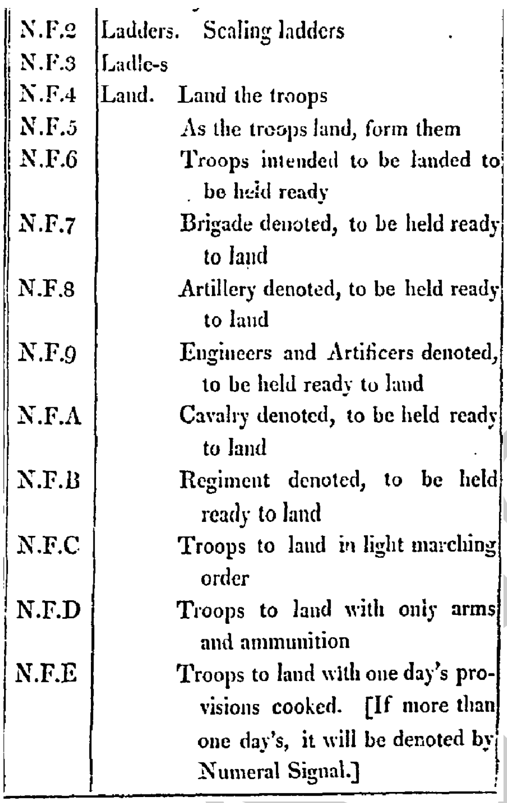


Figure 1: The relative sizes of the New Boe Code (1937) and the Tourists' Telegraphic Code (Gilburt 1900).

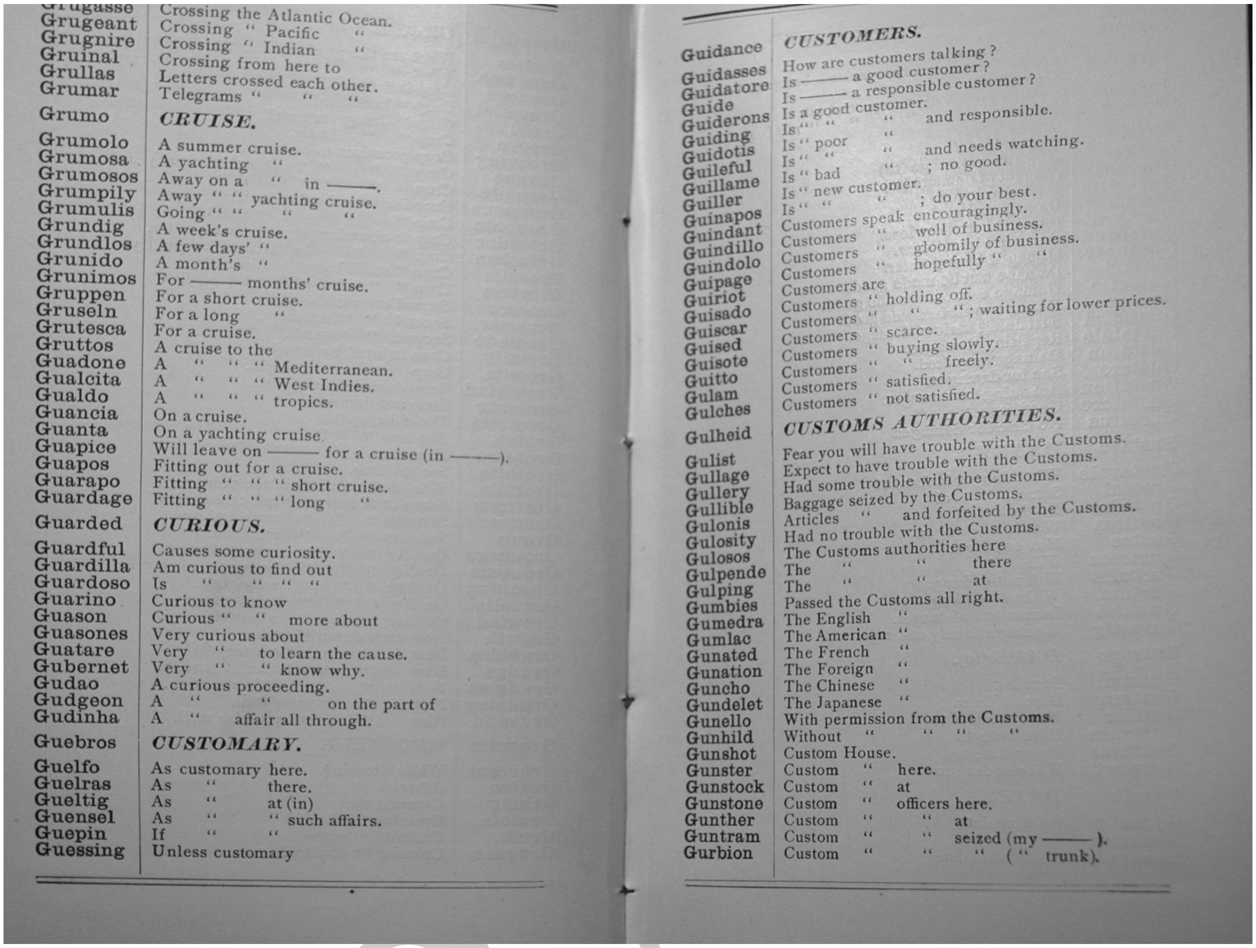


N.F.2	Ladders.	Scaling ladders
N.F.3	Ladle-s	
N.F.4	Land.	Land the troops
N.F.5		As the troops land, form them
N.F.6		Troops intended to be landed to be held ready
N.F.7		Brigade denoted, to be held ready to land
N.F.8		Artillery denoted, to be held ready to land
N.F.9		Engineers and Artificers denoted, 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.]

Figure 2: Popham's naval code.

Early telegraph codes had two ancestors, codes for semaphore networks and naval signaling (Kahn 1967). The constraint in the latter case was not so much cost (though rifling through a collection of flags would not have been quick); rather, the issue was limited space on a ship's rigging for the flags. Early naval codes conveyed meaning by a combination of flag and location. The vocabulary was very limited; it was not possible to send arbitrary messages in such schemes. Later, *numerary codes* were introduced, where a set of flags representing digits were used to indicate an entry in a signal book. The first such system is often attributed to Admiral Bertrand-François Mahé de la Bourdonnais (Great Britain Admiralty 1908; Palmer 2005); however, it was not adopted, possibly because he was of insufficiently noble birth. A number of British admirals adopted and adapted this scheme. Sir Charles Knowles devised a matrix system for indicating digits; a pair of flags, one over the other, would select a matrix cell for a given value. Later, Admiral Richard Lord Howe, probably with the assistance of Captain Richard Kempenfelt (who was familiar with Mahé de la Bourdonnais's work), devised a longer and better signal book. His first version also used a tabular scheme. Amusingly enough from a computer scientist's perspective, he used a 16×16 matrix: bytes!

The most influential early numerary code was devised by Sir Home Popham in 1803 (Great Britain Admiralty 1908; Palmer 2005; Popham 1991; Tunstall 1990); it included concise signals for such phrases as "Troops to land with one day's provisions cooked" (Figure 2). More importantly, it



Grugasse	Crossing the Atlantic Ocean.
Grugeant	Crossing “ Pacific “
Grugnire	Crossing “ Indian “
Gruinal	Crossing from here to
Grullas	Letters crossed each other.
Grumar	Telegrams “ “ “
Grumo	***CRUISE.***
Grumolo	A summer cruise.
Grumosa	A yachting “
Grumosos	Away on a “ in ——.
Grumpily	Away “ “ yachting cruise.
Grumulis	Going “ “ “ “
Grundig	A week's cruise.
Grundlos	A few days' “
Grunido	A month's “
Grunimos	For —— months' cruise.
Gruppen	For a short cruise.
Gruseln	For a long “
Grutesca	For a cruise.
Gruttos	A cruise to the
Guadone	A “ “ “ Mediterranean.
Gualcita	A “ “ “ West Indies.
Gualdo	A “ “ “ tropics.
Guancia	On a cruise.
Guanta	On a yachting cruise.
Guapice	Will leave on —— for a cruise (in ——).
Guapos	Fitting out for a cruise.
Guarapo	Fitting “ “ “ short cruise.
Guardage	Fitting “ “ “ long “
Guarded	***CURIOUS.***
Guardful	Causes some curiosity.
Guardilla	Am curious to find out
Guardoso	Is “ “ “ “
Guarino	Curious to know
Guason	Curious “ “ more about
Guasones	Very curious about
Guatare	Very “ to learn the cause.
Gubernet	Very “ “ know why.
Gudao	A curious proceeding.
Gudgeon	A “ “ on the part of
Gudinha	A “ affair all through.
Guebros	***CUSTOMARY.***
Guelfo	As customary here.
Guelras	As “ there.
Gueltig	As “ at (in)
Guensel	As “ “ such affairs.
Guepin	If “ “
Guessing	Unless customary

Guidance	***CUSTOMERS.***
Guidasses	How are customers talking ?
Guidatore	Is —— a good customer ?
Guide	Is —— a responsible customer ?
Guiderons	Is a good customer.
Guiding	Is “ “ “ and responsible.
Guidotis	Is “ poor “
Guileful	Is “ “ “ and needs watching.
Guillame	Is “ bad “ ; no good.
Guiller	Is “ new customer.
Guinapos	Is “ “ “ ; do your best.
Guindant	Customers speak encouragingly.
Guindillo	Customers “ well of business.
Guindolo	Customers “ gloomily of business.
Guipage	Customers “ hopefully “ “
Guiriot	Customers are
Guisado	Customers “ holding off.
Guiscar	Customers “ “ “ ; waiting for lower prices.
Guised	Customers “ scarce.
Guisote	Customers “ buying slowly.
Guitto	Customers “ “ freely.
Gulam	Customers “ satisfied.
Gulches	Customers “ not satisfied.
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).

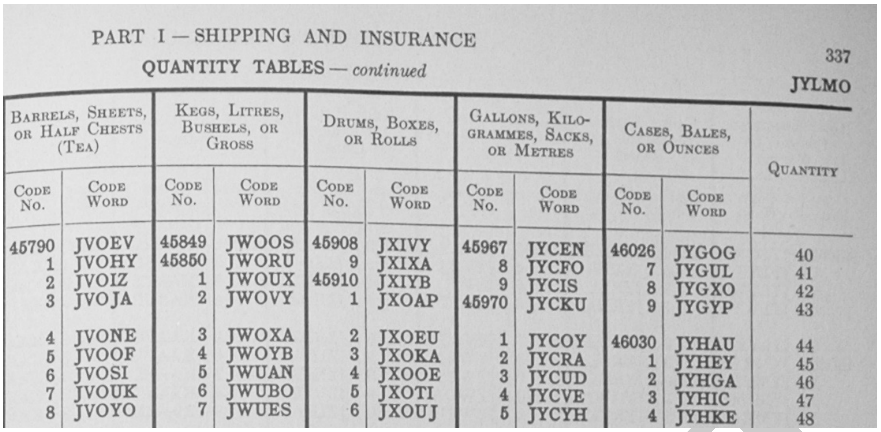
Figure 3: Some sample pages from the *Atlas Universal Travelers' and Business Telegraphic Cipher Code* (Hartfield 1896).

provided signals for various individual parts of speech. (Great Britain Admiralty 1908) likens it to “the step from a “Traveller's Manual of Conversation” to a dictionary of the language”. Popham's code included the concept of parameters; thus, the previous phrase could be modified: “If more than one day's, it will be denoted by Numeral Signal.” Nelson's famous signal “England expects that every man will do his duty” was sent using this's system (Palmer 2005). It was eventually adopted by the Admiralty as the standard signal book (Great Britain Admiralty 1816).

Frederick Marryat produced a *Code of Signals for the Merchant Service* in 1817. It assigned a 4-digit code to each sentence and to each individual merchant ship (Sechrest 2004). By 1828, there was even a codebook for yachts and pleasure boats (Wynne 1828).

Further details on the evolution of naval signals are beyond the scope of this work; those interested should see (Great Britain Admiralty 1908; Palmer 2005; Popham 1991; Tunstall 1990).

Telegraph codes drew on this rich history. Many codebooks were aimed at shipping and traveling. Figure 3 shows a typical example of this genre. By the time this particular code was is-



PART I — SHIPPING AND INSURANCE

QUANTITY TABLES — *continued*

337

JYLMO

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	
45790	JVOEV	45849	JWOOS	45908	JXIVY	45967	JYCEN	46026	JYGOG	40
1	JVOHY	45850	JWORU	9	JXIXA	8	JYCFO	7	JYGUL	41
2	JVOIZ	1	JWOUX	45910	JXIYB	9	JYCIS	8	JYGXO	42
3	JVOJA	2	JWOVY	1	JXOAP	45970	JYCKU	9	JYGYP	43
4	JVONE	3	JWOXA	2	JXOEU	1	JYCOY	46030	JYHAU	44
5	JVOOF	4	JWOYB	3	JXOKA	2	JYCRA	1	JYHEY	45
6	JVOSI	5	JWUAN	4	JXOOE	3	JYCUD	2	JYHGA	46
7	JVOUK	6	JWUBO	5	JXOTI	4	JYCVE	3	JYHIC	47
8	JVOYO	7	JWUES	6	JXOUJ	5	JYCYH	4	JYHKE	48

Figure 4: Part of a quantity table from the *A B C Telegraphic Code, Seventh Edition* (Droege 1936).

sued, in 1896, a great deal of effort had gone into specialized phrases. For example, **GULLIBLE** meant BAGGAGE SEIZED BY THE CUSTOMS, while **GURBION** meant CUSTOM HOUSE OFFICERS SEIZED MY TRUNK (Hartfield 1896).

Some codebooks incorporated domain-specific information. Thus, when Charles A. Stoneham & Co., a mining stock brokerage firm, issued its own codebook in 1910, it had words such as **REVERE** meaning WIRES BEING DOWN, YOUR TELEGRAM DID NOT REACH US IN TIME TO TRANSACT ANY BUSINESS TODAY, AND AS YOUR ORDERS ARE GOOD FOR THE WEEK, WE WILL TRY TO EXECUTE TOMORROW (Charles A. Stoneham & Co 1910). There were also specific code words for gold fields, mining companies, etc.

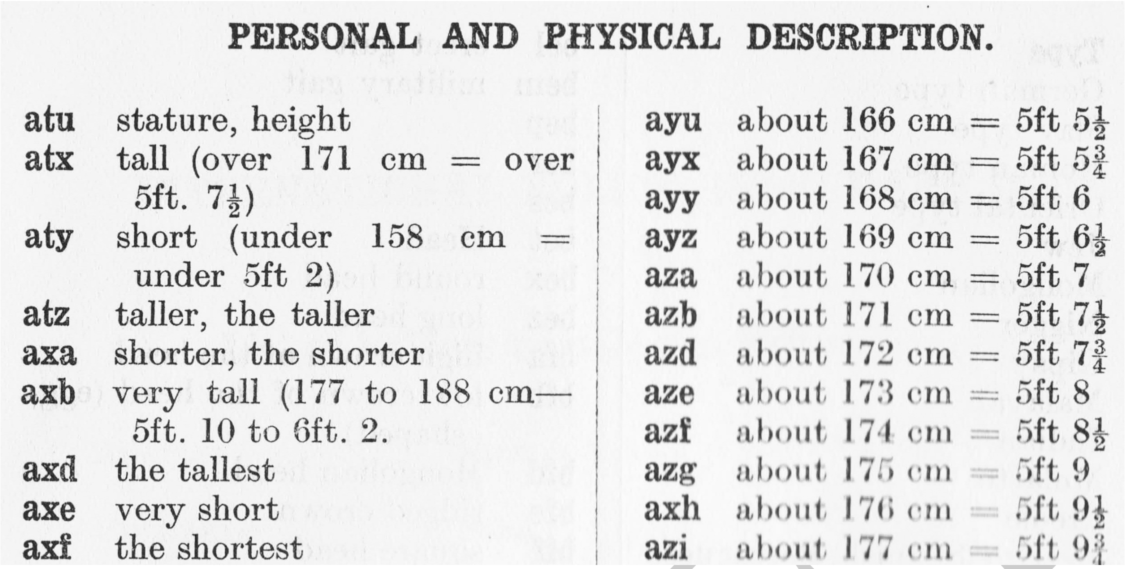
Domain-specific compression is at least as important today. MP3 and JPEG compression of sound and picture files is far more effective than, say, simple Lempel-Ziv compression would be. Informal experiments show that high-quality JPEG images taken from "raw" camera files are 30–40% smaller; simple Lempel-Ziv compression achieved no more than 5% improvement in file size.

Referring back to Figure 3, note that some messages are parameterized. Thus, one might send **GUIDE RICANTI** to ask IS **RICANTI** A RESPONSIBLE CUSTOMER? (Note the potential for confusion: is Ricanti a proper name? In fact, it is the code word for the BANK OF IRELAND. This issue is discussed further in Section 3.)

Sometimes, compression was implicit, as in (Droege 1936). Figure 4 shows that **JYGUL** (or **46027**) could stand for 41 CASES, 41 BALES, or 41 OUNCES. Presumably, the recipient would know what was meant. On the other hand, there were typically distinct code words for amounts of money in dollars, pounds sterling, francs, etc.

Compression could be taken to extremes. One wonders how often users of the 1920 *ABC Telegraphic Code, Sixth Edition* ever sent **ENBET** (CAPTAIN IS INSANE) or **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 (Droege 1920).[1] (We note that the first of these phrases persisted into the 7th Edition (Droege

[1] While I certainly recalled Kahn's reprint (1967, p. 851) of the classic July 28, 1934 *New Yorker* essay on amusing



PERSONAL AND PHYSICAL DESCRIPTION.

atu	stature, height	**ayu**	about 166 cm = 5ft 5½
atx	tall (over 171 cm = over 5ft. 7½)	**ayx**	about 167 cm = 5ft 5¾
aty	short (under 158 cm = under 5ft 2)	**ayy**	about 168 cm = 5ft 6
atz	taller, the taller	**ayz**	about 169 cm = 5ft 6½
axa	shorter, the shorter	**aza**	about 170 cm = 5ft 7
axb	very tall (177 to 188 cm—5ft. 10 to 6ft. 2.	**azb**	about 171 cm = 5ft 7½
axd	the tallest	**azd**	about 172 cm = 5ft 7¾
axe	very short	**aze**	about 173 cm = 5ft 8
axf	the shortest	**azf**	about 174 cm = 5ft 8½
		azg	about 175 cm = 5ft 9
		axh	about 176 cm = 5ft 9½
		azi	about 177 cm = 5ft 9¾

Figure 5: Part of a police code for describing suspects (*International Police Telegraph Code* 1930).

1936), but the second did not. Was there a greater incidence of crazy captains than bad weather?)

As telegraphy evolved, compression efficiency was no longer measured in characters but in money. What was actually charged by the telegraph companies was the important matter, and code compilers were quick to find loopholes. Instead of sending **MAGFD YHFJU** for DELIVERED IN TIME TO SAN FRANCISCO, could one send **MAGFDYHFJU** and thus be charged for a single word? What *is* a word? In 1903, international regulations defined a "word" as ten characters or less "capable of pronunciation according to the usage of one of the folloiwng languages: German, English, Spanish, French, Dutch, Italian, Portuguese, or Latin". This gave rise to things like the 1907 *Pantelegraphy Simplex Translating and Check Card*, which allowed digits or pairs of digits to be encoded as consonant-vowel pairs, with alternate forms in the name of euphony (*Pantelegraphy Simplex Translating & Check Card* 1907). When the regulations loosened in 1929, to eliminate the pronounceability requirement but to impose a vowel density standard, code makers adapted accordingly. The 1953 Western Union tariffs (*Tariff Book No. 77* 1953) described what a word was in great and gory detail. For example, "B&O" was one word—no spaces—while "B & O" was three words. Even then, how to count words was destination-dependent.

3 Correction

Especially towards the end of the codebook period, a tremendous amount of effort went into error detection and correction. Errors could be costly, in time, money, or both, and the encoding process removed a lot of redundancy. Consider the poor constable who typed **AXF** instead of **AXG** in

code words' meanings while I was writing this, I did not, in fact, have it available at the time. I later realized that Kahn misidentified the code as the *Acme*; it's actually the *A B C Sixth Edition*—with some errors!

Figure 5 (*International Police Telegraph Code* 1930), giving a very incorrect description of the suspect. Also note that **F** and **G** are adjacent on the keyboard, though it isn't clear that it ever would have been typed as opposed to being hand-written and sent in Morse code. (This code was rather late for such errors. It authors were apparently more concerned with economy: three codewords could be combined into a single telegraph word for billing purposes.)

A number of different techniques were used. *Mutilation tables* are perhaps the most interesting. A chart from (Boe 1937) (Figure 6) shows the possible middle letters of a codeword, indexed by the initial two and final two letters that can produce that letter. Consider the chart shown, and a received code word **ZNBAB**. This is an impossible value; if the first two letters are **ZN** and the last two **AB**, the middle letter must be **N**. The error could be in any of the three sections, leading to five possible correct values; the instructions suggest looking at the semantics of the decoded value to reconstruct the proper plaintext.

As a complement to mutilation tables, terminal indices were sometimes provided. These were indices alphabetized by the last two letters of the codeword, and were used when it was suspected that the beginning of the word had been corrupted in transmission.

Numerical data was particularly sensitive. The semantic difference between, say, "1,000" and "9,000' is small, so it is harder to recognize errors from context; nevertheless, the business difference can be great. Accordingly, code makers adopted check digits or letters (Figure 7). These are what today would be known as checksums over the plaintext, and provide at least error detection. One code (Telling 1929) had a separate set of mutilation tables for numeric data. (In fact, that understates the cleverness of their solution: numeric data was a special case of "subsidiary tables", which were used to encode not just numbers of various types (currency, dimensions, etc.) but also things like repeated dates and markings: **CD** or **AX** might mean best possible shipment January, **CM** or **BU** best possible shipment August, etc., all concatenated into a single codeword, and followed by a check letter.)

Check letters are notable because they operate on the plaintext, and thus can help with encoding errors. More common techniques dealt with transmission errors. Thus, the *A B C 6th Edition* stated that it was "built on the principle of at least a two-letter difference in each five-letter codeword". The compiler also tried to deal with transposition errors, though admittedly imperfectly; by contrast, the 1923 *Acme Commodity and Phrase Code* (Meisenbach 1923) proudly stated

> This Code consists of one hundred thousand five-letter code ciphers with at least two-letter difference between each and every word. No transposition of any two adjoining letters will make another word in the book, and we assert that it is the first time this feat has been fully accomplished for 100,000 words.

They did not quite succeed; see Figure 8 for some errors in it and in *Bentley's Complete Phrasebook* (Bentley 1909). Today, of course, we lump things like the two-letter differential into the general class of Hamming distance (Hamming 1950); codebooks, though, used the concept several decades before it was formalized.

In later years, the two-letter difference was considered insufficient. A Czech code (Cipl 1961) used three-letter differences. This provided error *correction*, not just detection, similar to the difference between today's simple parity checks versus error-correcting codes. The delivery time in

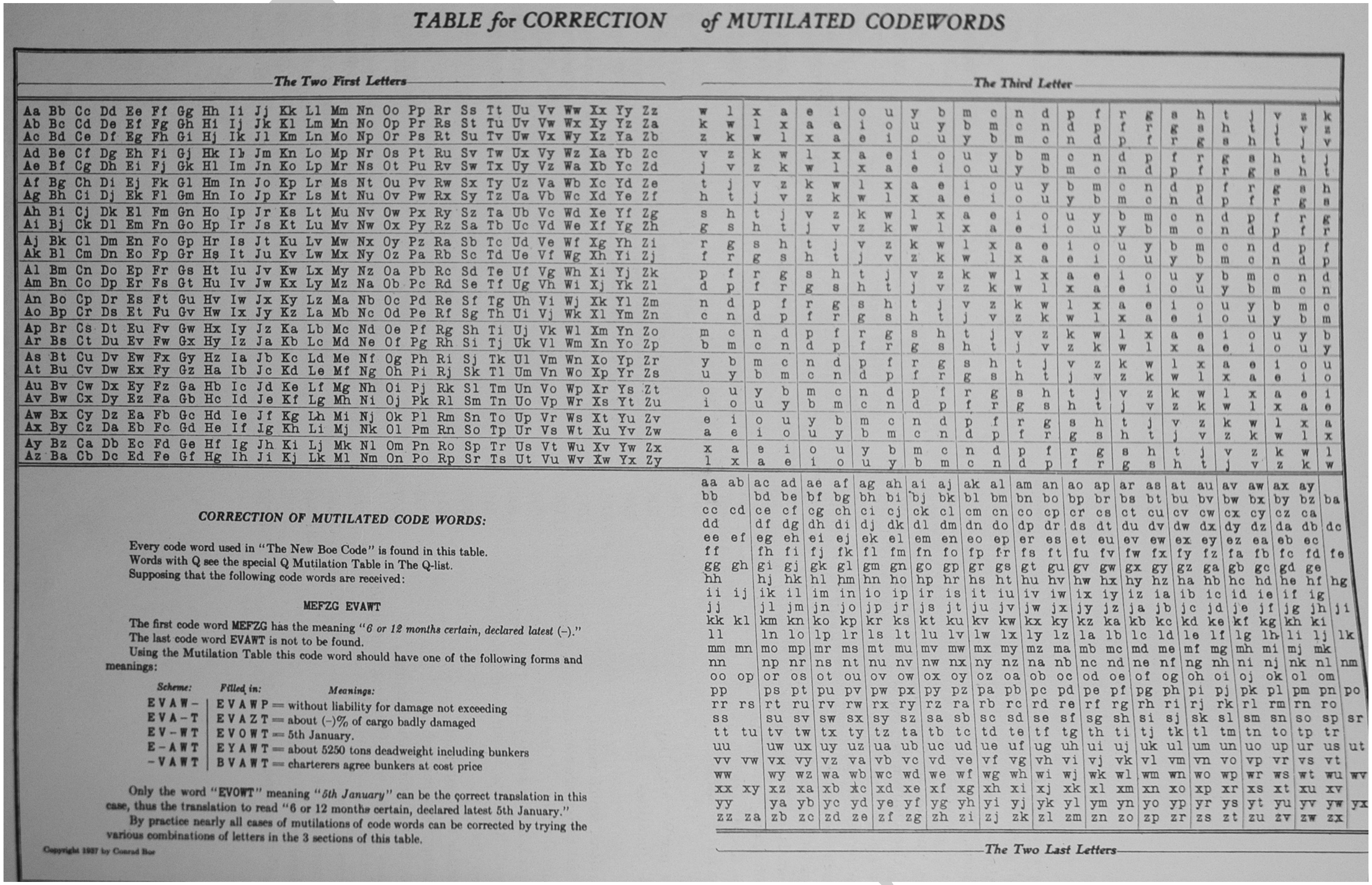


TABLE for CORRECTION of MUTILATED CODEWORDS

The Two First Letters

Aa	Bb	Cc	Dd	Ee	Ff	Gg	Hh	Ii	Jj	Kk	Ll	Mm	Nn	Oo	Pp	Rr	Ss	Tt	Uu	Vv	Ww	Xx	Yy	Zz
Ab	Bc	Cd	De	Ef	Fg	Gh	Hi	Ij	Jk	Kl	Lm	Mn	No	Op	Pr	Rs	St	Tu	Uv	Vw	Wx	Xy	Yz	Za
Ac	Bd	Ce	Df	Eg	Fh	Gi	Hj	Ik	Jl	Km	Ln	Mo	Np	Or	Ps	Rt	Su	Tv	Uw	Vx	Wy	Xz	Ya	Zb
Ad	Be	Cf	Dg	Eh	Fi	Gj	Hk	Il	Jm	Kn	Lo	Mp	Nr	Os	Pt	Ru	Sv	Tw	Ux	Vy	Wz	Xa	Yb	Zc
Ae	Bf	Cg	Dh	Ei	Fj	Gk	Hl	Im	Jn	Ko	Lp	Mr	Ns	Ot	Pu	Rv	Sw	Tx	Uy	Vz	Wa	Xb	Yc	Zd
Af	Bg	Ch	Di	Ej	Fk	Gl	Hm	In	Jo	Kp	Lr	Ms	Nt	Ou	Pv	Rw	Sx	Ty	Uz	Va	Wb	Xc	Yd	Ze
Ag	Bh	Ci	Dj	Ek	Fl	Gm	Hn	Io	Jp	Kr	Ls	Mt	Nu	Ov	Pw	Rx	Sy	Tz	Ua	Vb	Wc	Xd	Ye	Zf
Ah	Bi	Cj	Dk	El	Fm	Gn	Ho	Ip	Jr	Ks	Lt	Mu	Nv	Ow	Px	Ry	Sz	Ta	Ub	Vc	Wd	Xe	Yf	Zg
Ai	Bj	Ck	Dl	Em	Fn	Go	Hp	Ir	Js	Kt	Lu	Mv	Nw	Ox	Py	Rz	Sa	Tb	Uc	Vd	We	Xf	Yg	Zh
Aj	Bk	Cl	Dm	En	Fo	Gp	Hr	Is	Jt	Ku	Lv	Mw	Nx	Oy	Pz	Ra	Sb	Tc	Ud	Ve	Wf	Xg	Yh	Zi
Ak	Bl	Cm	Dn	Eo	Fp	Gr	Hs	It	Ju	Kv	Lw	Mx	Ny	Oz	Pa	Rb	Sc	Td	Ue	Vf	Wg	Xh	Yi	Zj
Al	Bm	Cn	Do	Ep	Fr	Gs	Ht	Iu	Jv	Kw	Lx	My	Nz	Oa	Pb	Rc	Sd	Te	Uf	Vg	Wh	Xi	Yj	Zk
Am	Bn	Co	Dp	Er	Fs	Gt	Hu	Iv	Jw	Kx	Ly	Mz	Na	Ob	Pc	Rd	Se	Tf	Ug	Vh	Wi	Xj	Yk	Zl
An	Bo	Cp	Dr	Es	Ft	Gu	Hv	Iw	Jx	Ky	Lz	Ma	Nb	Oc	Pd	Re	Sf	Tg	Uh	Vi	Wj	Xk	Yl	Zm
Ao	Bp	Cr	Ds	Et	Fu	Gv	Hw	Ix	Jy	Kz	La	Mb	Nc	Od	Pe	Rf	Sg	Th	Ui	Vj	Wk	Xl	Ym	Zn
Ap	Br	Cs	Dt	Eu	Fv	Gw	Hx	Iy	Jz	Ka	Lb	Mc	Nd	Oe	Pf	Rg	Sh	Ti	Uj	Vk	Wl	Xm	Yn	Zo
Ar	Bs	Ct	Du	Ev	Fw	Gx	Hy	Iz	Ja	Kb	Lc	Md	Ne	Of	Pg	Rh	Si	Tj	Uk	Vl	Wm	Xn	Yo	Zp
As	Bt	Cu	Dv	Ew	Fx	Gy	Hz	Ia	Jb	Kc	Ld	Me	Nf	Og	Ph	Ri	Sj	Tk	Ul	Vm	Wn	Xo	Yp	Zr
At	Bu	Cv	Dw	Ex	Fy	Gz	Ha	Ib	Jc	Kd	Le	Mf	Ng	Oh	Pi	Rj	Sk	Tl	Um	Vn	Wo	Xp	Yr	Zs
Au	Bv	Cw	Dx	Ey	Fz	Ga	Hb	Ic	Jd	Ke	Lf	Mg	Nh	Oi	Pj	Rk	Sl	Tm	Un	Vo	Wp	Xr	Ys	Zt
Av	Bw	Cx	Dy	Ez	Fa	Gb	Hc	Id	Je	Kf	Lg	Mh	Ni	Oj	Pk	Rl	Sm	Tn	Uo	Vp	Wr	Xs	Yt	Zu
Aw	Bx	Cy	Dz	Ea	Fb	Gc	Hd	Ie	Jf	Kg	Lh	Mi	Nj	Ok	Pl	Rm	Sn	To	Up	Vr	Ws	Xt	Yu	Zv
Ax	By	Cz	Da	Eb	Fc	Gd	He	If	Jg	Kh	Li	Mj	Nk	Ol	Pm	Rn	So	Tp	Ur	Vs	Wt	Xu	Yv	Zw
Ay	Bz	Ca	Db	Ec	Fd	Ge	Hf	Ig	Jh	Ki	Lj	Mk	Nl	Om	Pn	Ro	Sp	Tr	Us	Vt	Wu	Xv	Yw	Zx
Az	Ba	Cb	Dc	Ed	Fe	Gf	Hg	Ih	Ji	Kj	Lk	Ml	Nm	On	Po	Rp	Sr	Ts	Ut	Vu	Wv	Xw	Yx	Zy

The Third Letter

w	l	x	a	e	i	o	u	y	b	m	c	n	d	p	f	r	g	s	h	t	j	v	z	k
k	w	l	x	a	e	i	o	u	y	b	m	c	n	d	p	f	r	g	s	h	t	j	v	z
z	k	w	l	x	a	e	i	o	u	y	b	m	c	n	d	p	f	r	g	s	h	t	j	v
v	z	k	w	l	x	a	e	i	o	u	y	b	m	c	n	d	p	f	r	g	s	h	t	j
j	v	z	k	w	l	x	a	e	i	o	u	y	b	m	c	n	d	p	f	r	g	s	h	t
t	j	v	z	k	w	l	x	a	e	i	o	u	y	b	m	c	n	d	p	f	r	g	s	h
h	t	j	v	z	k	w	l	x	a	e	i	o	u	y	b	m	c	n	d	p	f	r	g	s
s	h	t	j	v	z	k	w	l	x	a	e	i	o	u	y	b	m	c	n	d	p	f	r	g
g	s	h	t	j	v	z	k	w	l	x	a	e	i	o	u	y	b	m	c	n	d	p	f	r
r	g	s	h	t	j	v	z	k	w	l	x	a	e	i	o	u	y	b	m	c	n	d	p	f
f	r	g	s	h	t	j	v	z	k	w	l	x	a	e	i	o	u	y	b	m	c	n	d	p
p	f	r	g	s	h	t	j	v	z	k	w	l	x	a	e	i	o	u	y	b	m	c	n	d
d	p	f	r	g	s	h	t	j	v	z	k	w	l	x	a	e	i	o	u	y	b	m	c	n
n	d	p	f	r	g	s	h	t	j	v	z	k	w	l	x	a	e	i	o	u	y	b	m	c
c	n	d	p	f	r	g	s	h	t	j	v	z	k	w	l	x	a	e	i	o	u	y	b	m
m	c	n	d	p	f	r	g	s	h	t	j	v	z	k	w	l	x	a	e	i	o	u	y	b
b	m	c	n	d	p	f	r	g	s	h	t	j	v	z	k	w	l	x	a	e	i	o	u	y
y	b	m	c	n	d	p	f	r	g	s	h	t	j	v	z	k	w	l	x	a	e	i	o	u
u	y	b	m	c	n	d	p	f	r	g	s	h	t	j	v	z	k	w	l	x	a	e	i	o
o	u	y	b	m	c	n	d	p	f	r	g	s	h	t	j	v	z	k	w	l	x	a	e	i
i	o	u	y	b	m	c	n	d	p	f	r	g	s	h	t	j	v	z	k	w	l	x	a	e
e	i	o	u	y	b	m	c	n	d	p	f	r	g	s	h	t	j	v	z	k	w	l	x	a
a	e	i	o	u	y	b	m	c	n	d	p	f	r	g	s	h	t	j	v	z	k	w	l	x
x	a	e	i	o	u	y	b	m	c	n	d	p	f	r	g	s	h	t	j	v	z	k	w	l
l	x	a	e	i	o	u	y	b	m	c	n	d	p	f	r	g	s	h	t	j	v	z	k	w

aa	ab	ac	ad	ae	af	ag	ah	ai	aj	ak	al	am	an	ao	ap	ar	as	at	au	av	aw	ax	ay	
bb		bd	be	bf	bg	bh	bi	bj	bk	bl	bm	bn	bo	bp	br	bs	bt	bu	bv	bw	bx	by	bz	ba
cc	cd	ce	cf	cg	ch	ci	cj	ck	cl	cm	cn	co	cp	cr	cs	ct	cu	cv	cw	cx	cy	cz	ca	
dd		df	dg	dh	di	dj	dk	dl	dm	dn	do	dp	dr	ds	dt	du	dv	dw	dx	dy	dz	da	db	dc
ee	ef	eg	eh	ei	ej	ek	el	em	en	eo	ep	er	es	et	eu	ev	ew	ex	ey	ez	ea	eb	ec	
ff		fh	fi	fj	fk	fl	fm	fn	fo	fp	fr	fs	ft	fu	fv	fw	fx	fy	fz	fa	fb	fc	fd	fe
gg	gh	gi	gj	gk	gl	gm	gn	go	gp	gr	gs	gt	gu	gv	gw	gx	gy	gz	ga	gb	gc	gd	ge	
hh		hj	hk	hl	hm	hn	ho	hp	hr	hs	ht	hu	hv	hw	hx	hy	hz	ha	hb	hc	hd	he	hf	hg
ii	ij	ik	il	im	in	io	ip	ir	is	it	iu	iv	iw	ix	iy	iz	ia	ib	ic	id	ie	if	ig	
jj		jl	jm	jn	jo	jp	jr	js	jt	ju	jv	jw	jx	jy	jz	ja	jb	jc	jd	je	jf	jg	jh	ji
kk	kl	km	kn	ko	kp	kr	ks	kt	ku	kv	kw	kx	ky	kz	ka	kb	kc	kd	ke	kf	kg	kh	ki	
ll		ln	lo	lp	lr	ls	lt	lu	lv	lw	lx	ly	lz	la	lb	lc	ld	le	lf	lg	lh	li	lj	lk
mm	mn	mo	mp	mr	ms	mt	mu	mv	mw	mx	my	mz	ma	mb	mc	md	me	mf	mg	mh	mi	mj	mk	
nn		np	nr	ns	nt	nu	nv	nw	nx	ny	nz	na	nb	nc	nd	ne	nf	ng	nh	ni	nj	nk	nl	nm
oo	op	or	os	ot	ou	ov	ow	ox	oy	oz	oa	ob	oc	od	oe	of	og	oh	oi	oj	ok	ol	om	
pp		ps	pt	pu	pv	pw	px	py	pz	pa	pb	pc	pd	pe	pf	pg	ph	pi	pj	pk	pl	pm	pn	po
rr	rs	rt	ru	rv	rw	rx	ry	rz	ra	rb	rc	rd	re	rf	rg	rh	ri	rj	rk	rl	rm	rn	ro	
ss		su	sv	sw	sx	sy	sz	sa	sb	sc	sd	se	sf	sg	sh	si	sj	sk	sl	sm	sn	so	sp	sr
tt	tu	tv	tw	tx	ty	tz	ta	tb	tc	td	te	tf	tg	th	ti	tj	tk	tl	tm	tn	to	tp	tr	
uu		uw	ux	uy	uz	ua	ub	uc	ud	ue	uf	ug	uh	ui	uj	uk	ul	um	un	uo	up	ur	us	ut
vv	vw	vx	vy	vz	va	vb	vc	vd	ve	vf	vg	vh	vi	vj	vk	vl	vm	vn	vo	vp	vr	vs	vt	
ww		wy	wz	wa	wb	wc	wd	we	wf	wg	wh	wi	wj	wk	wl	wm	wn	wo	wp	wr	ws	wt	wu	wv
xx	xy	xz	xa	xb	xc	xd	xe	xf	xg	xh	xi	xj	xk	xl	xm	xn	xo	xp	xr	xs	xt	xu	xv	
yy		ya	yb	yc	yd	ye	yf	yg	yh	yi	yj	yk	yl	ym	yn	yo	yp	yr	ys	yt	yu	yv	yw	yx
zz	za	zb	zc	zd	ze	zf	zg	zh	zi	zj	zk	zl	zm	zn	zo	zp	zr	zs	zt	zu	zv	zw	zx	

The Two Last Letters

CORRECTION OF MUTILATED CODE WORDS:

Every code word used in "The New Boe Code" is found in this table.
Words with Q see the special Q Mutilation Table in The Q-list.
Supposing that the following code words are received:

MEFZG EVAWT

The first code word **MEFZG** has the meaning *"6 or 12 months certain, declared latest* (–)."
The last code word **EVAWT** is not to be found.

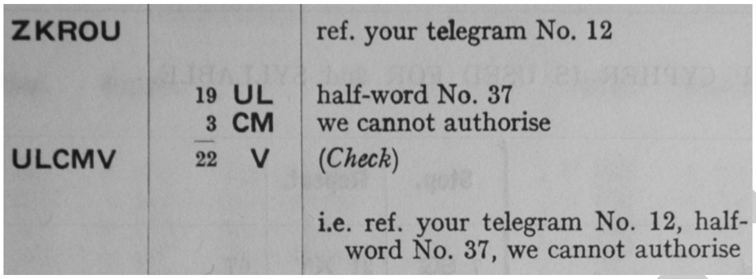
Using the Mutilation Table this code word should have one of the following forms and meanings:

Scheme:	*Filled in:*	*Meanings:*
E V A W –	E V A W P	= without liability for damage not exceeding
E V A – T	E V A Z T	= about (–)% of cargo badly damaged
E V – W T	E V O W T	= 5th January.
E – A W T	E Y A W T	= about 5250 tons deadweight including bunkers
– V A W T	B V A W T	= charterers agree bunkers at cost price

Only the word "**EVOWT**" meaning "*5th January*" can be the çorrect translation in this case, thus the translation to read "6 or 12 months certain, declared latest 5th January."

By practice nearly all cases of mutilations of code words can be corrected by trying the various combinations of letters in the 3 sections of this table.

Figure 6: A "mutilation table" for error correction.



ZKROU		ref. your telegram No. 12
	19 UL	half-word No. 37
	3 CM	we cannot authorise
ULCMV	22 V	(*Check*)
		i.e. ref. your telegram No. 12, half-word No. 37, we cannot authorise

Figure 7: Check digits for numerical data, from the 1929 *New Standard Code*.

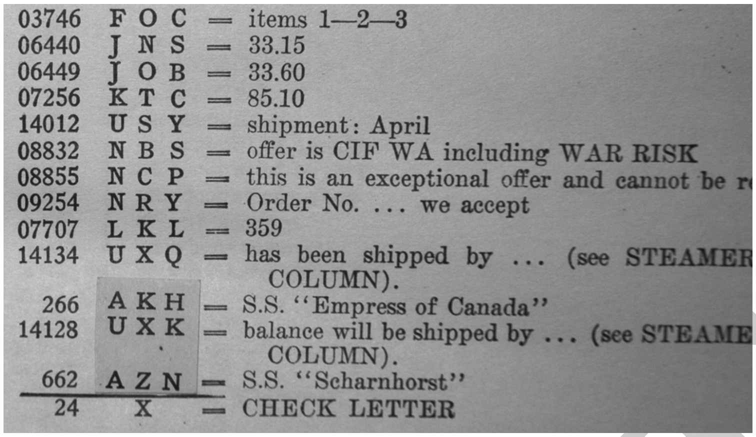
HALAN	HAALN
IBLAN	IBALN
LELAN	LEALN
OGLAN	OGALN
QILAN	QIALN
UMLAN	UMALN
WOLAN	WOALN
ATLAN	ATALN
BULAN	BUALN
EXLAN	EXALN
FYLAN	FYALN

(a) Acme codebook pairs that do not protect against transposition errors.

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

(b) Bentley codebook pairs that are only one character apart.

Figure 8: Codebook compilers did not always succeed in their error-detecting goals. Here we see codeword pairs from the Acme codebook that are not immune to transposition error and pairs from Bentley's code (Bentley 1909) that are only a single letter apart. (Data supplied by J. Reeds.)



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 r
09254	N R Y	=	Order No. . . . we accept
07707	L K L	=	359
14134	U X Q	=	has been shipped by . . . (see STEAMER COLUMN).
266	A K H	=	S.S. ''Empress of Canada''
14128	U X K	=	balance will be shipped by . . . (see STEAME COLUMN).
662	A Z N	=	S.S. ''Scharnhorst''
24	X	=	CHECK LETTER

Figure 9: Correction of errors in the codebook. 1936 *Cosmos Trading Code*.

1961—this code was often used for "postal telegrams", i.e., those delivered by the postal service—was much longer than for telegrams at the peak of the telegraph era, meaning that a request for retransmission would have required several days before a corrected version could be received.

It is worth noting that the check characters used were not as effective against transposition errors as one might want: they generally operated on a $\bmod 10$ basis. On the other hand, as a rule two digits were generally encoded at a time, thus providing some protection. Further protection could be gained by ensuring that the second letter of the encoded digraphs could never be the first letter of a numeric code.

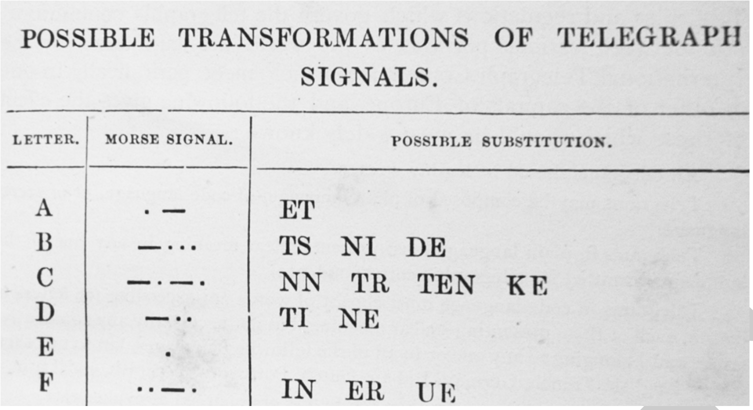
That said, hand-calculation of check characters was itself error-prone. Consider the complex process outlined in (Eckelman 1936), which used a "Three-Letter System". Groups of three letters were combined, with a check letter, into a single telegraph word. But the example supplied in the codebook, Figure 9, appears to have a correction glued over the last three code entries. Imagine the error rate in production use!

Unencoded numbers were especially subject to corruption during transmission. The 1931 *Swift & Company Private Telegraphic Code* (*Private Telegraphic Code of Swift & Company* 1931), after setting a requirement that telegrams of ten words or more should be coded, says

> As a protection against mutilation, phrases, numbers, etc., should be coded if possible, even though the message contains ten words or less. This applies especially to prices and amounts.

Transposition errors are more likely in typed text; in the context of telegrams, this meant when teletypes were used, rather than Morse code. Morse code had its own distinctive errors. Not only could a single dot or dash be omitted, timing variations during transmission could result in a single letter being received as two. Thus, Figure 10 (*Unicode* 1886) shows how F, which should be transmitted as . . _ . could be received as IN (. .   _ .), ER (.   . _ .), or UE (. . _   .).

All of this could be exacerbated by some users' habits of only partially encoding a message. One such instance reached the U.S. Supreme Court, in *Primrose v. Western Union Tel. Co.*, 154 U.S. 1 (1894). Primrose sent the message



POSSIBLE TRANSFORMATIONS OF TELEGRAPH SIGNALS.

LETTER.	MORSE SIGNAL.	POSSIBLE SUBSTITUTION.
A	· —	ET
B	— · · ·	TS NI DE
C	— · — ·	NN TR TEN KE
D	— · ·	TI NE
E	·	
F	· · — ·	IN ER UE

Figure 10: A table of likely Morse code errors, from the 1886 *Unicode* book.

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

Three errors occurred during transmission. "Despot" was received as "Destroy", "bay" was received as "buy", and "purchases" was received in the singular. The second error—a single dot in transmission—was crucial.

Primrose's message was partially encoded. **DESPOT** meant Yours of the 15th received; **DESTROY** meant Yours of the 17th received. That error was inconsequential. But **BAY** was a codeword which meant I have bought; the recipient interpreted **BUY** as the plaintext instruction to purchase some more—and the remainder of the message indicated that 300,000 pounds of wool was the desired quantity. . . . Primrose lost $20,000 and sued; he lost because of the disclaimer on the back of the telegraph form. Perhaps he could have sued the code compiler—but in fact, it was a private code he and his agent had devised. (More details may be found in (Kahn 1967)[p. 840] or in the Court's opinion.)

The odd appearance of encoded telegrams has had amusing consequences. Once, a New York brokerage firm received an unsigned radiogram reading **ONE LEOPARD AND SEVENTY MONKEYS PERMIT OTHO**. Attempts to decode it using a variety of codebooks failed. The cashier was concerned that a vital trade would be missed, because the market was closing, so he circulated it among the staff. One person finally understood it as plaintext: his son was arriving from Africa on the steamship *Otho* and wanted assistance getting an import permit for a leopard and a large number of monkeys (Maloney 1935).

Imposing patterns on codewords, such as a minimum two-letter difference, obviously reduces the size of the space available to compilers. The inclusion of a minimum vowel density requirement reduced it further. An analysis of the actual effect of these constraints was done by Friedman (yes, that Friedman) and Mendelsohn (1932).

High-end code makers were aware of such problems, and responded by avoiding use of common words (and especially common commercial words) in their tables. Thus, the 1901 *A B C Telegraphic Code, 5th Edition, Improved* has codewords like **MAELSTROM** and **THEORY**, but not **PURCHASE** or **SELL** (Clausen-Thue 1915). (The 5th Edition was originally published in

1901; the 1915 Improved Edition added five letter codewords but did not change or delete the existing codewords.) Not everyone was as careful. The *Tourists' Telegraphic Code* (Gilburt 1900) includes such codewords as **SUBWAY**, **REVOLT**, and **SAVAGERY**. Perhaps well-bred tourists did not encounter the plaintext equivalents!

It is instructive to consider these problems in the light of modern technology and terminology. The usual sequence of operations today is compression (either generic or domain-specific), encryption, checksum or MAC on the ciphertext, and medium-specific encoding. Each operation is done separately, by a different component, though in some high-performance cryptosystems encryption and MACcing are done in a single pass. In addition, there is generally a checksum at various points during transmission, such as the TCP checksum (Postel 1981) or the Ethernet CRC. Sound design would suggest an application-level checksum on the plaintext (Saltzer, Reed, and Clark 1984); this is rarely done in most systems.

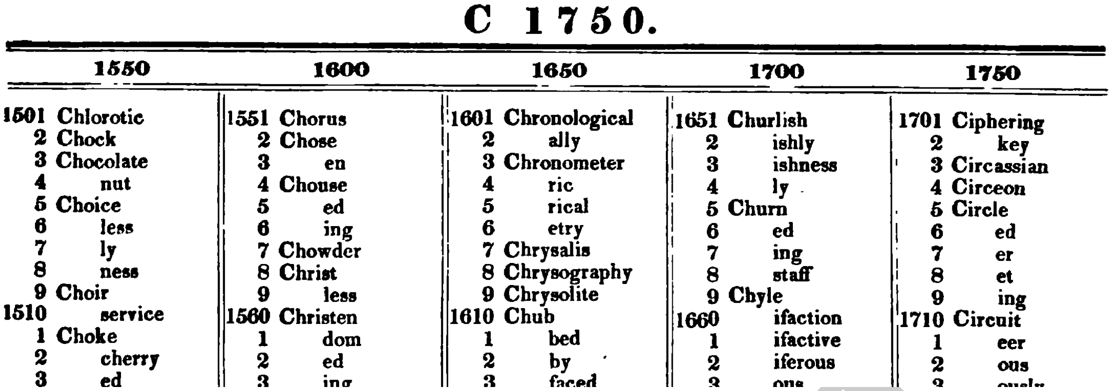
In telegraph codes, compression was the primary step. The encoding was an integral part of the compression process; more precisely, a separate encoding step was composed with compression, to avoid an extra, expensive, and error-prone pass over the data. Furthermore, the encodings were chosen with particular transmission characteristics in mind. This is not unreasonable—checksums need to be tuned to the medium (Stone and Partridge 2000)—but it required changes in encoding (and hence in codebooks) when transmission characteristics changed.

As today, confidentiality was implemented via a transform on the compressed text. This posed a problem, though: since the compression output was already optimally encoded for transmission, a modern-style cipher or even early mechanized encryptors (Enigma, the Hagelin machine, etc.) would have destroyed properties such as two-letter differences. Accordingly, the confidentiality systems of the era (see the following section) were effectively a mapping from the codeword space to the codeword space. Today, we seek indistinguishability of a cipher's output from a uniformly distributed random bit string; for telegraph codes, the proper comparison would be a uniformly random selection of codewords.

4 Confidentiality

Although compression was the primary goal of commercial telegraph codes, confidentiality was a concern as well. To be sure, as Kahn has noted, though the opacity of an ordinary code book was often sufficient, many telegraph users required more. That said, the very first telegraph codebook, Smith's *Secret Corresponding Vocabulary* (1845), though it mentions cost-savings, was intended for confidentiality:

> As the tariff of expense chargeable to correspondents, who shall have recourse to the Telegraph, in order to be equal, can only be based upon the quantity of matter communicated, and as that can only be measured by the number of words transmitted, it is obvious that, in a system where *signs* are employed to represent the letters which form words, whatever will tend to lessen the requisite number of those signs to communicate any given number of words, will add to the despatch of the correspondence, and indirectly, at least, cheapen its transmission.



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

Figure 11: Part of a page from the *Secret Corresponding Vocabulary* (1845). The compiler, Francis O.J. Smith, was Samuel Morse's business partner in the first commercial deployments of the telegraph. (Image taken from the Google Books digitization of the work.)

> But, SECRECY in correspondence, is far the most important consideration to be secured. And the crowning desideratum, in the use of the Telegraph, consists in its adaption to this end, by means of the compilation now presented.

The book (Figure 11) contained a list of about 56,000 words. The user would denote a word by its first letter and the index of the word in that section; thus, CIPHERING would be sent as **C.1701**. For confidentiality, a prearranged value was to be added to or subtracted from the index number. Thus, one might send **C.1710** instead if the sender's offset were 9. For more security, a set of different offsets could be used in sequence and a monoalphabetic substitution applied to the letters:

> The complexity of this mode of writing, may be very much increased, so as to render all experiments to decypher communications, utterly hopeless.

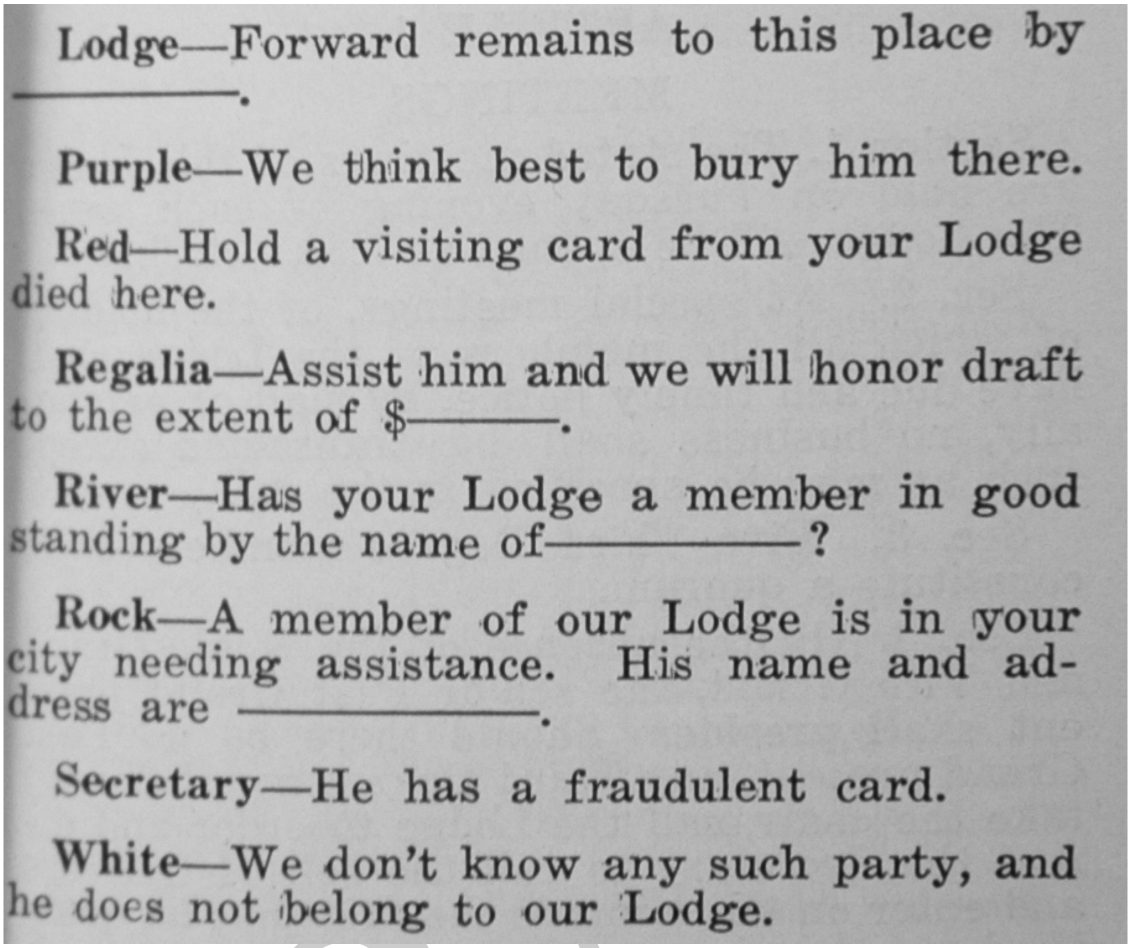
Sometimes, though, even for data that might be deemed sensitive, protection against causual readers was deemed sufficient. The (*International Police Telegraph Code* 1930) notes that

> By its nature the Code renders superfluous the translation of an incoming telegram, and so saves valuable police time, while offering a certain guarantee of secrecy.

The recognition of the limitations is itself gratifying.

Needless to say, commercial code confidentiality does not live up to the standards of military or governmental codes. Serious confidentiality codes are "two-part"—separate books or sections are used for encoding and decoding. This removes the requirement, clearly shown in these examples, that the plaintext and the code words be in the same order. Other measures commonly taken include multiple ciphertext symbols for common plaintext phrases and superencipherment of the codewords. Only the latter was commonly used commercially, and rarely well.

For simple uses, secrecy of the code words was employed. A fraternal group, the Independent Order of Odd Fellows, published a 1931 constitution and bylaws booklet that included some pages of a 1908 "Telegraph Cipher and Key" (Figure 12).



Lodge—Forward remains to this place by ————.

Purple—We think best to bury him there.

Red—Hold a visiting card from your Lodge died here.

Regalia—Assist him and we will honor draft to the extent of $————.

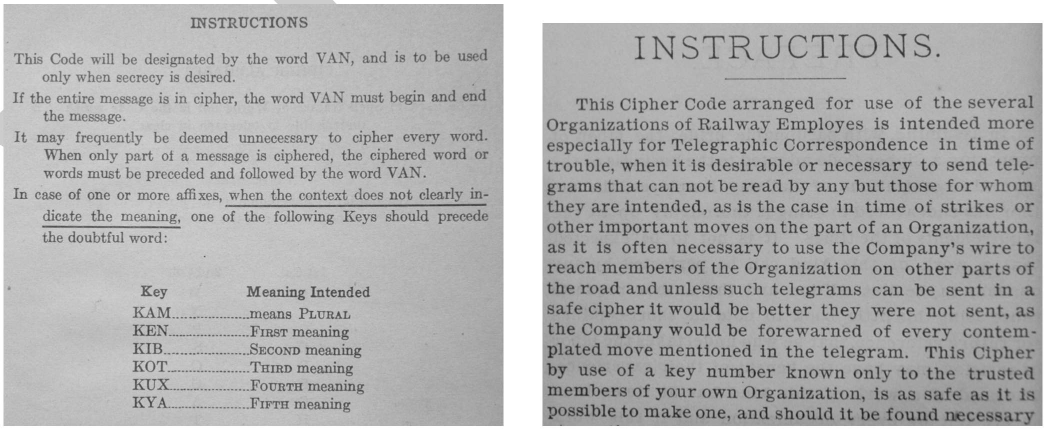
River—Has your Lodge a member in good standing by the name of————?

Rock—A member of our Lodge is in your city needing assistance. His name and address are ————.

Secretary—He has a fraudulent card.

White—We don't know any such party, and he does not belong to our Lodge.

Figure 12: A few secrecy code words used by the Independent Order of Odd Fellows, 1931.



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.

In case of one or more affixes, when the context does not clearly indicate the meaning, one of the following Keys should precede the doubtful word:

Key	Meaning Intended
KAM	means PLURAL
KEN	FIRST meaning
KIB	SECOND meaning
KOT	THIRD meaning
KUX	FOURTH meaning
KYA	FIFTH meaning

(a) A management codebook

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 road and unless such telegrams can be sent in a safe cipher it would be better they were not sent, as the Company would be forewarned of every contemplated move mentioned in the telegram. This Cipher by use of a key number known only to the trusted members of your own Organization, is as safe as it is possible to make one, and should it be found necessary

(b) A union codebook

Figure 13: Secrecy codebooks for railroad use.

The normal approach for confidentiality of widely distributed codebooks was superencipherment. An amusing pair is the *New York Central Lines VAN Code* (1923), which for management is “to be used only when secrecy is desired” (Figure 13(a)) and the union’s code (Figure 13(b)) (Sheahan 1892)

> “for use of the several Organizations of Railway Employes [sic] . . . 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 . . . as it is often necessary to use the Company’s wire.

Of the two, labor employed better techniques. The key was an integer added to the code number; the code word corresponding to the new code number was to be sent. Thus, if the key were 3 and someone wanted to send the word STRUGGLE, 3 would be added to **5592** and PRODUCTION would be transmitted in its place. Users were cautioned never to mix plaintext and ciphertext.

The most intriguing part of the scheme was the deliberate omission of numbers (and hence superencipherment) for times and dates, for fear of known plaintext attacks:

> This plan was adopted after careful study and deliberation, as a safeguard for the reason that a telegram giving a number a name, or in reference to anything that occurred on a certain day would, if the same key number applied to the entire book, be a clew [sic] that would lead to the discovery of your key number. Therefore, I have used numbers only where I believed it was safe to do so.

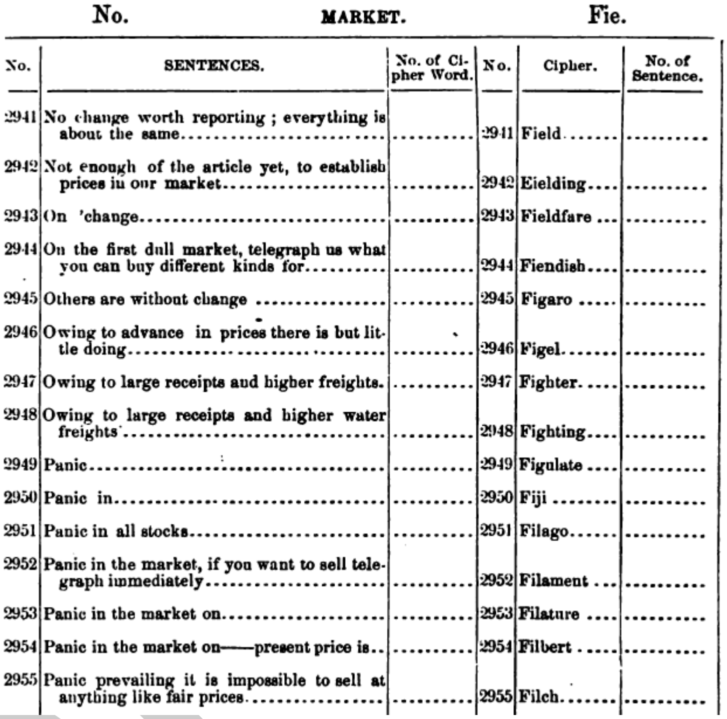
It is unclear how successful this book was, organizationally or cryptographically; however, it was reissued at least as late as 1938, well after the Railway Labor Act (45 U.S.C. §151 *et seq*), which regulated relations between unions and management, was enacted.

Management showed much less sophistication. Mixed ciphertext and plaintext was expressly supported, and keying was a choice of either sending “the word opposite” or the “Arbitrary Word to the left” of the desired word.

Bloomer (1874) showed more cryptographic sophistication than many. In addition to the usual additives, it suggested transposition of code words. The practical effect of that would often be minimal, especially on short messages—**ABUKIR FILAGO EVACUATE** (ADVICE FROM NEW YORK; PANIC IN ALL STOCKS; MARKET AFFECTED BY GENERAL CAUSES) would be nearly as intelligible if rendered as MARKET AFFECTED BY GENERAL CAUSES; PANIC IN ALL STOCKS; ADVICE FROM NEW YORK. The scheme would do considerably better if different additives were used for successive words, a technique that is also described.

More interestingly, Bloomer appears to have understood the benefit of two-part codes. The codebook (Figure 14) provided extra spaces for each code word and code sentence, with the following advice:

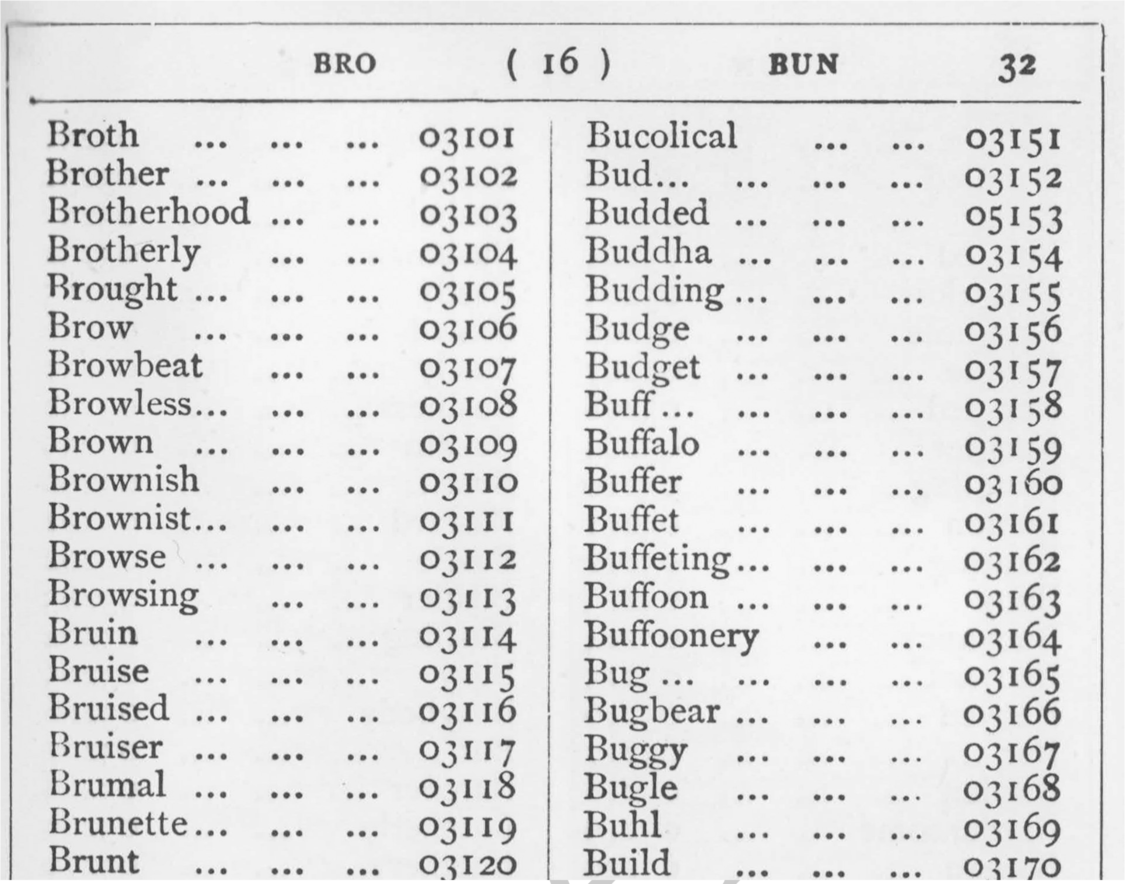
> 5th.—Double Index—A permanent cryptograph may he made in the third and sixth columns by selecting cipher words indiscriminately from the fifth column, and entering the numbers of such words in the third column, opposite the sentences which the cipher words are intended to represent, and entering the numbers of such sentences in the sixth column, opposite the cipher words selected. Thus, if 2228 be written in the



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.......	....

Figure 14: An excerpt from Bloomer's Commercial Cryptograph. Note the blank spaces for writing in variant code numbers.



BRO (16) BUN 32

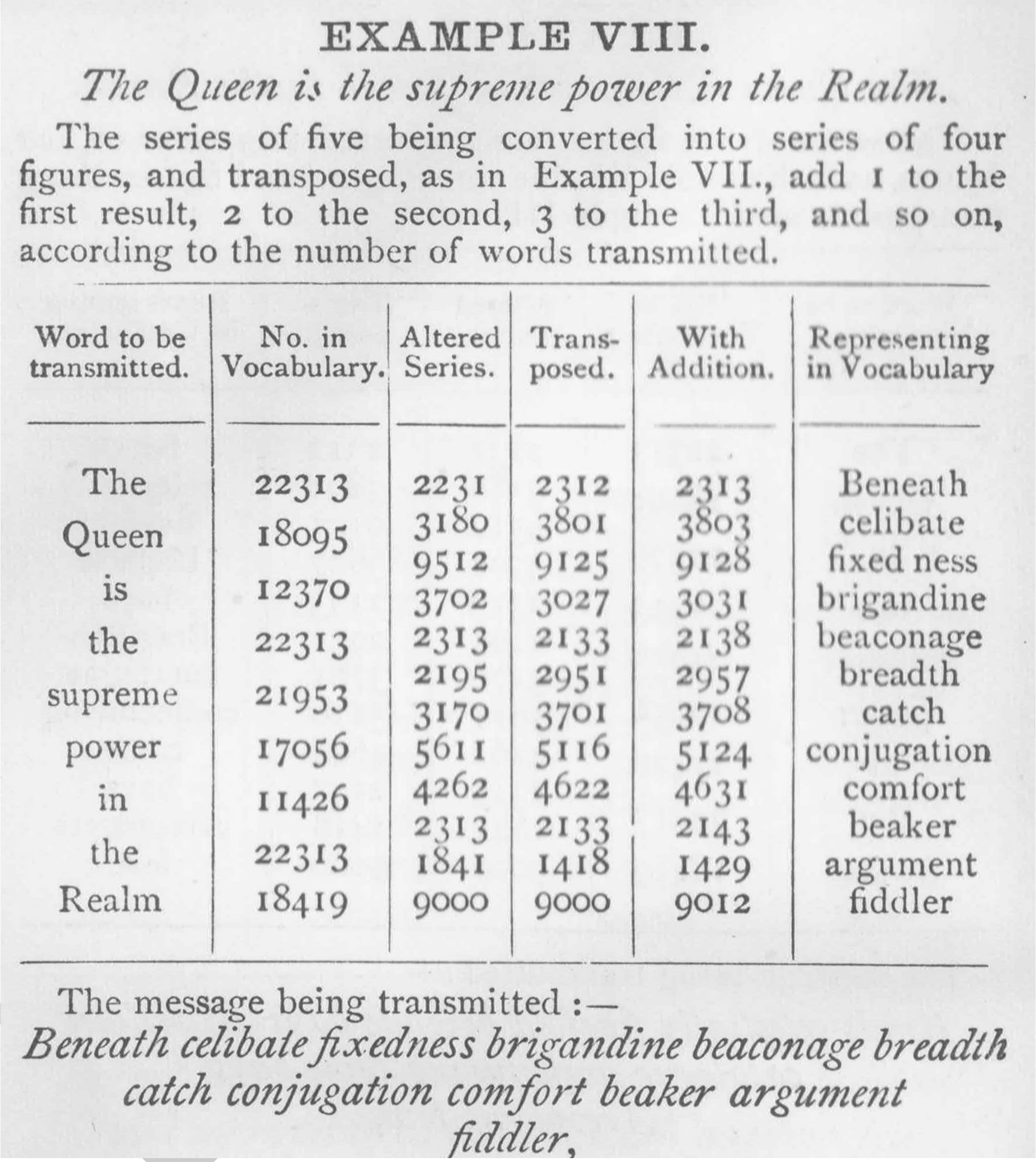
Broth	03101	Bucolical	03151
Brother	03102	Bud...	03152
Brotherhood	03103	Budded	05153
Brotherly	03104	Buddha	03154
Brought	03105	Budding	03155
Brow	03106	Budge	03156
Browbeat	03107	Budget	03157
Browless...	03108	Buff	03158
Brown	03109	Buffalo	03159
Brownish	03110	Buffer	03160
Brownist...	03111	Buffet	03161
Browse	03112	Buffeting...	03162
Browsing	03113	Buffoon	03163
Bruin	03114	Buffoonery	03164
Bruise	03115	Bug	03165
Bruised	03116	Bugbear	03166
Bruiser	03117	Buggy	03167
Brumal	03118	Bugle	03168
Brunette...	03119	Buhl	03169
Brunt	03120	Build	03170

Figure 15: Code numbers for Slater's secrecy code.

> third column, opposite numher 2175, "Buy at seller's option," and 2175 in the sixth column, opposite the cipher word "Doctor," the party desiring to telegraph the above sentence will find the numher 2228. By turning to the printed number 2228, the cipher word will he found to be "Doctor," which being telegraphed, the receiver finds opposite "Doctor," 2175, the number of the original sentence. In this case it will he necessary for correspondents to have the exact copy of the numbers written in both volumes.

In other words, users of the code were instructed to create their own two-part equivalences, pair by pair, and distribute them to their correspondents. This is a laborious process, and of dubious utility unless many such pairs were created. It may safely be assumed that very few users actually carried out this process to any noticeable extent.

Most of the commercial codebooks offer add-ons that promise "absolute secrecy". These tend to be simple transforms of the codeword or code number, or monoalphabetic transformations of the individual characters of the code word. There is one, though, that stands out: Slater's, since it was intended solely for secrecy and provided no compression or correction (1870). Conventional



EXAMPLE VIII.

The Queen is the supreme power in the Realm.

The series of five being converted into series of four figures, and transposed, as in Example VII., add I to the first result, 2 to the second, 3 to the third, and so on, according to the number of words transmitted.

Word to be transmitted.	No. in Vocabulary.	Altered Series.	Trans-posed.	With Addition.	Representing in Vocabulary
The	22313	2231	2312	2313	Beneath
Queen	18095	3180	3801	3803	celibate
is	12370	9512	9125	9128	fixed ness
		3702	3027	3031	brigandine
the	22313	2313	2133	2138	beaconage
supreme	21953	2195	2951	2957	breadth
		3170	3701	3708	catch
power	17056	5611	5116	5124	conjugation
in	11426	4262	4622	4631	comfort
the	22313	2313	2133	2143	beaker
		1841	1418	1429	argument
Realm	18419	9000	9000	9012	fiddler

The message being transmitted :—

Beneath celibate fixedness brigandine beaconage breadth catch conjugation comfort beaker argument fiddler,

Figure 16: Some suggested transformations of code numbers.

wisdom has it that there was never a market for commercial secrecy; this codebook, though, lasted from about 1870 until at least 1938 (Slater 1938), from a variety of publishers. The threat model was interesting as well:

> 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. Now in large or small communities (particularly perhaps in the latter) there are always to be found prying spirits, curious as to the affairs of their neighbours, which they think they can manage so much better than the parties chiefly interested, and proverbially inclined to gossip.

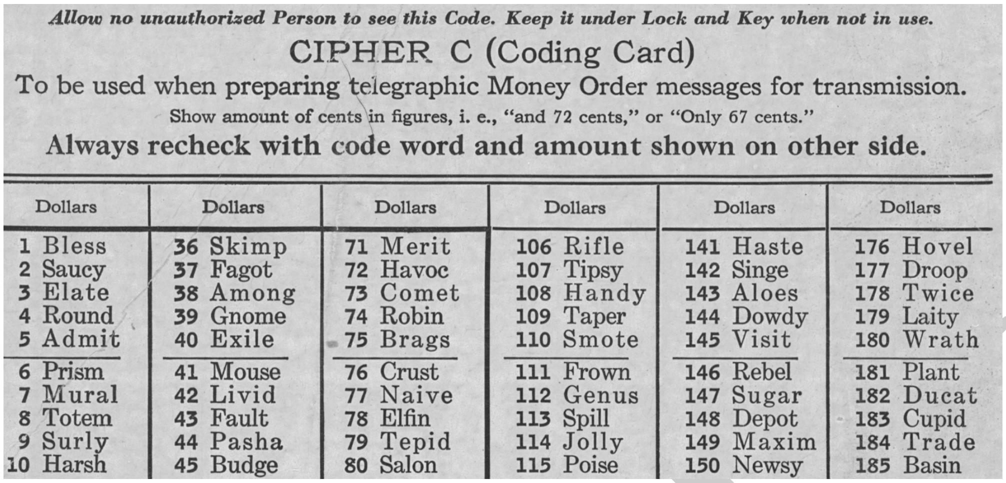
((Darhan 1912) appears to be a Spanish version of the same codebook.)

To start, a message was converted to code numbers via the book (Figure 15). Next, some transform was applied to the sequence of code numbers. Several types are suggested: simple addition or subtraction of a key number, transposition of some of the ciphertext digits, and regrouping into four-character sections instead of five. Combinations also suggested. Of particular interest is the realization by the compiler that with regrouping, minor changes in plaintext can result in very large changes of ciphertext—always a good thing in an encryption scheme (Figure 16). More generally, by combining code groups before superencryption, it flattens the frequency distribution, much as the Playfair cipher does by encrypting letter pairs rather than single letters (Kahn 1967).

One remarkable confidentiality code stands out even more. It was devised by a California banker named Frank Miller (1882). In a nutshell, Miller invented the one-time pad, more than 35 years before it was reinvented by Vernam and Mauborgne (Bellovin 2011). Most of the codebook was a fairly typical domain-specific codebook, though not a great one; there was too little compression. But his superencipherment relied on additives whose differences "*must not be regular*"—emphasis in the original!—and which, once used, "must be erased from the list *and not used again*" (again, emphasis in the original) . Miller also gave a weak provision for authenticity checks, called "test words"; however, these were not really linked to the message itself. Slater, in a another of his codebooks, gives a stronger authenticity scheme, though by modern standards still not well-tied to the actual message (Slater 1876).

Later codebooks used more sophisticted authentication algorithms. For example, National City Bank's code (1938) prescribed an algorithm involving adding up all numerical quantities plus another value for the date of the transfer, and using other code letters to denote the direction of the messsage. They relied on the confidentiality of the codebook: "This Code is Strictly Confidential and the Correspondent receiving it should safeguard it by keeping it inaccessible to persons not authorized to use it. The National City Bank of New York disclaims any responsibility in circumstances which may arise through the failure of a Correspondent to observe such precautions."

At least as late as 1953, Western Union used a code card to encrypt transmission of money orders (*Tariff Book No. 77* 1953), though this appears to have been more for authenticity than con-



Allow no unauthorized Person to see this Code. Keep it under Lock and Key when not in use.

CIPHER C (Coding Card)

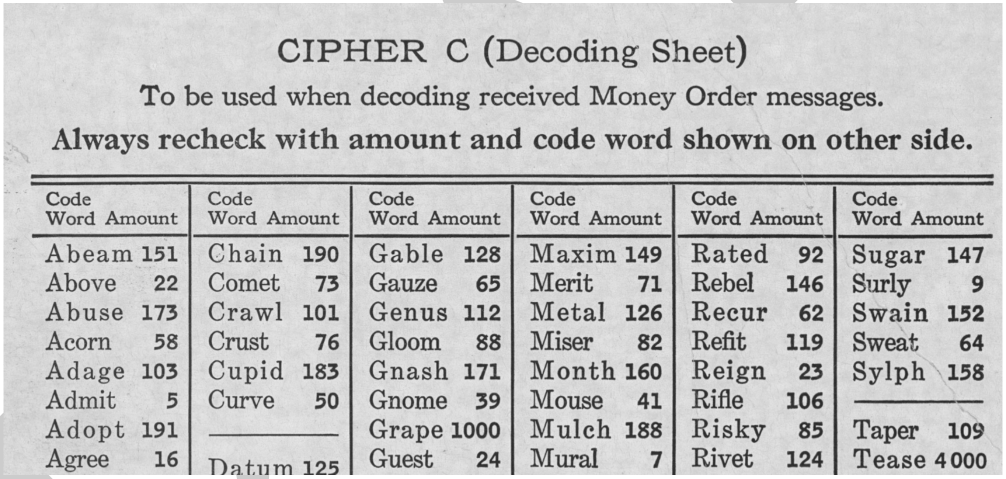
To be used when preparing telegraphic Money Order messages for transmission.

Show amount of cents in figures, i. e., "and 72 cents," or "Only 67 cents."

Always recheck with code word and amount shown on other side.

Dollars	Dollars	Dollars	Dollars	Dollars	Dollars
1 Bless	36 Skimp	71 Merit	106 Rifle	141 Haste	176 Hovel
2 Saucy	37 Fagot	72 Havoc	107 Tipsy	142 Singe	177 Droop
3 Elate	38 Among	73 Comet	108 Handy	143 Aloes	178 Twice
4 Round	39 Gnome	74 Robin	109 Taper	144 Dowdy	179 Laity
5 Admit	40 Exile	75 Brags	110 Smote	145 Visit	180 Wrath
6 Prism	41 Mouse	76 Crust	111 Frown	146 Rebel	181 Plant
7 Mural	42 Livid	77 Naive	112 Genus	147 Sugar	182 Ducat
8 Totem	43 Fault	78 Elfin	113 Spill	148 Depot	183 Cupid
9 Surly	44 Pasha	79 Tepid	114 Jolly	149 Maxim	184 Trade
10 Harsh	45 Budge	80 Salon	115 Poise	150 Newsy	185 Basin

(a)



CIPHER C (Decoding Sheet)

To be used when decoding received Money Order messages.

Always recheck with amount and code word shown on other side.

Code Word	Amount	Code Word	Amount	Code Word	Amount	Code Word	Amount	Code Word	Amount	Code Word	Amount
Abeam	151	Chain	190	Gable	128	Maxim	149	Rated	92	Sugar	147
Above	22	Comet	73	Gauze	65	Merit	71	Rebel	146	Surly	9
Abuse	173	Crawl	101	Genus	112	Metal	126	Recur	62	Swain	152
Acorn	58	Crust	76	Gloom	88	Miser	82	Refit	119	Sweat	64
Adage	103	Cupid	183	Gnash	171	Month	160	Reign	23	Sylph	158
Admit	5	Curve	50	Gnome	39	Mouse	41	Rifle	106		
Adopt	191			Grape	1000	Mulch	188	Risky	85	Taper	109
Agree	16	Datum	125	Guest	24	Mural	7	Rivet	124	Tease	4000

(b)

Figure 17: The encoding and decoding parts of the Western Union money transfer code. Note in particular the entries for 7 (**MURAL**) and 9 (**SURLY**).

fidentiality. The January 1952 card was a two-part code (Figure 17). There were strict injunctions, on both the card and in the tariff book, that the card should be strictly guarded; clearly, the integrity of the system depended on that card rather than on any superencipherment: “The code cards are strictly confidential. They must be kept out of sight, carefully guarded, and made accessible only to bonded employees authorized to use them in the performance of the service.” The tariff book has a lot of discussion of how to authenticate the recipient, though it notes that the “inability of the payee to produce documentary or other tangible evidence of identity does not necessarily preclude payment—particularly in the case of women payees who frequently have difficulty producing such evidence—provided the paying clerk has no reason to suspect that the person applying for payment is other than the payee named in the order.” (But monogrammed clothing and jewelry were considered useful forms of identification.) Senders can include “test questions” that the recipient must answer correctly to receive the money.

It is tempting to laugh at the cryptanalytic naïveté of most of these code compilers. At least in the U.S., the military did no better back then. In 1899, the War Department published a supplement to the Western Union code book (1900) until their own full code could be compiled (*War Department Telegraphic Code* 1899–1904) five years later. Although economy was the primary concern, “it is also to be used as a cipher code in important and confidential messages where secrecy is desired” (Greely 1899). The suggested scheme? “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.” The codeword corresponding to the new number was then used. Kahn calls this “probably the most secure and advanced code system of the day” (1967, p. 252).

The 1899 U.S. Navy (Moody 1904) felt the same way about mixing plaintext and ciphertext:

> In order to eliminate as far as possible errors in transmission due to mistakes of telegraphic operators in telegraphing words strange to them, it is hereby directed that in using the cipher code only that part of the communication which is of a confidential nature be put in cipher, except in cases where the cipher code is used to shorten the message in order that the telegraphic cost may be materially lessened.

Arguably, the State Department was even worse. They were much more concerned with economy than confidentiality (Weber 1979, 2013), and their codes reflected that. Superencryption schemes, similar to Bloomer’s, were provided as an appendix; given diplomats’ penchant for sending mixed plaintext and codewords, one can assume that these schemes were seldom used. Not surprisingly, other countries were frequently able to read U.S. diplomatic traffic. Indeed, in a note that Roosevelt sent to Japan pleading for peace on December 6, 1941, he specified that a known-insecure code be used because

> . . . he did not mind if the dispatch was “picked up”, and also that the code “saves time”. (Weber 1979).

When Roosevelt wanted security, he had the Navy transmit his messages (Kahn 1967).

Even addresses were considered sensitive sometimes, though no solution was propounded. Companies could register short addresses with their telegraph companies, much as domain names are used today. New York, unlike many cities, had a central list serving all companies. They had had separate lists, but “in 1917, the State Department, fearing spies, abolished all existing lists and set up a uniform one for everybody” (Coates 1934).

Full names were important as well. In the Bahamas during World War II, people were required to sign their full names on telegrams, even those going to family members (Ross 1940).

There are places one would have expected more attention to confidentiality but it was not provided. A Cold War-era Czech code (Cipl 1961)—the name “Unicode” appears to bear no relation to (*Unicode* 1886)—was intended for international commerce, including within the Soviet bloc, but had no provision for confidentiality. This is despite the long history of intelligence agencies spying on commercial traffic; see the following section.

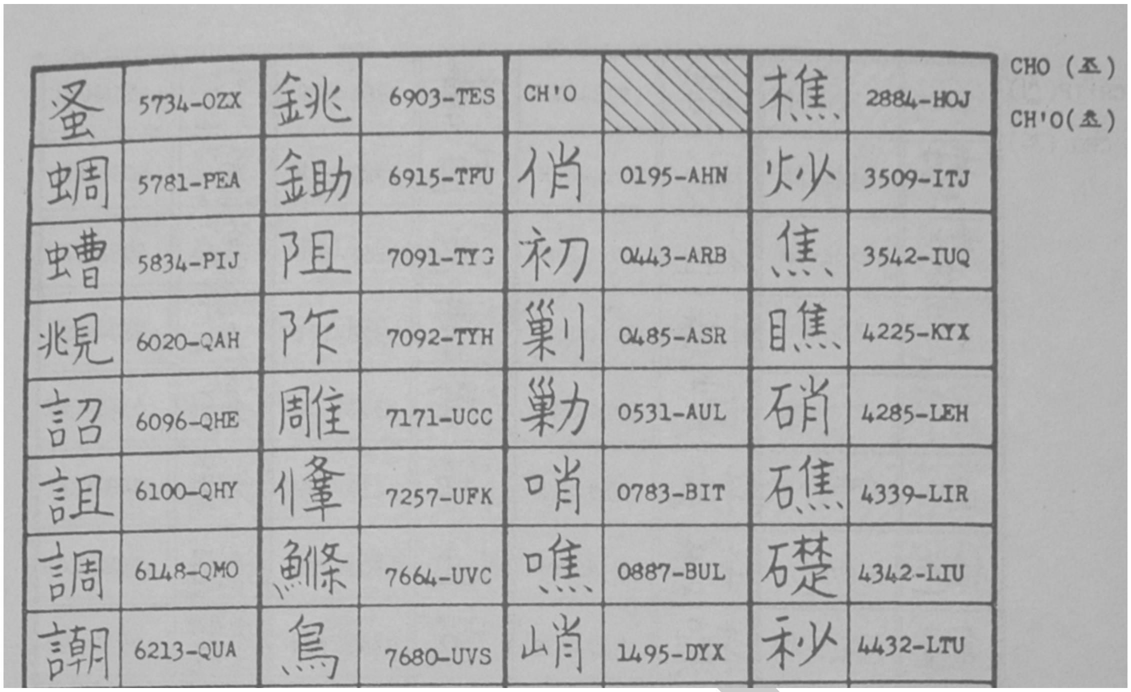
Some organizations that one would expect to embrace confidentiality seemed to rely entirely on the secrecy of the codebook. One effort, intended primarily for administrative use between government, police, and military agencies in the U.K. and its colonies (*Government Telegraph Code* 1908), was described as useful for confidential (but not “highly confidential” traffic) without any mention of or provision for superencipherment. The U.S. Federal Reserve didn’t place any restrictions on use of its code (McDougal et al. 1921), save for physical security of the codebook.

Several war time Japanese codebooks show the same curious blindness (Japanese Ministry of Telecommunications 1943; *Japanese Special Code Book* 1943; *Mitsui Bussan Japanese Code Book* 1941). This is especially surprising for (*Japanese Special Code Book* 1943), which made explicit mention of the war: “With the outbreak of the Greater East Asian War, we have added a considerable number of new terms that have become necessary due to changes in the economic structure, and we have also improved the content.” Either they assumed that the U.S. could not intercept their traffic or they didn’t understand the importance of commercial intelligence, which is very odd for a steamship company. A comprehensive online history of Japanese telegraph codes (Satoshi 2019) shows the same blindness to the need for confidentiality. Indeed, the only mention of the war in the codebooks of that era that the page cites shows a nationalistic issue: “The preface explains motivation of compiling the code by deploring there are no match for British Bentley’s Second Phrase Code and American Acme Code in Japan and regretting the situation of ‘relying on British and American codebooks of the enemy nations’.”

5 Comprehension

This title of this section refers many forms of comprehension. Under this heading I’ve lumped linguistic issues, coding issues, and—most important—what we learn of other cultures, removed in time from ours.

The simplest issue was character set suitability. Any alphabetic script, whether Latin, Greek, Cyrillic, or Hebrew, can be transmitted rather easily. Ideographic languages, such as Chinese, Japanese, and Korean, pose serious issues for the telegraph operator. The primary purpose of such a codebook, e.g., Figure 18 ((*Korean Telegraphic Code Book* 1950?)), is simply encoding into an alphabetic form, often on a per-word basis. (The book isn’t dated; however, it says it uses the McCune-Reischauer romanization system, which was first published in 1939 (McCune and Reischauer 1939). The Library of Congress catalog lists 1950, 1952, and 1978 code books of this

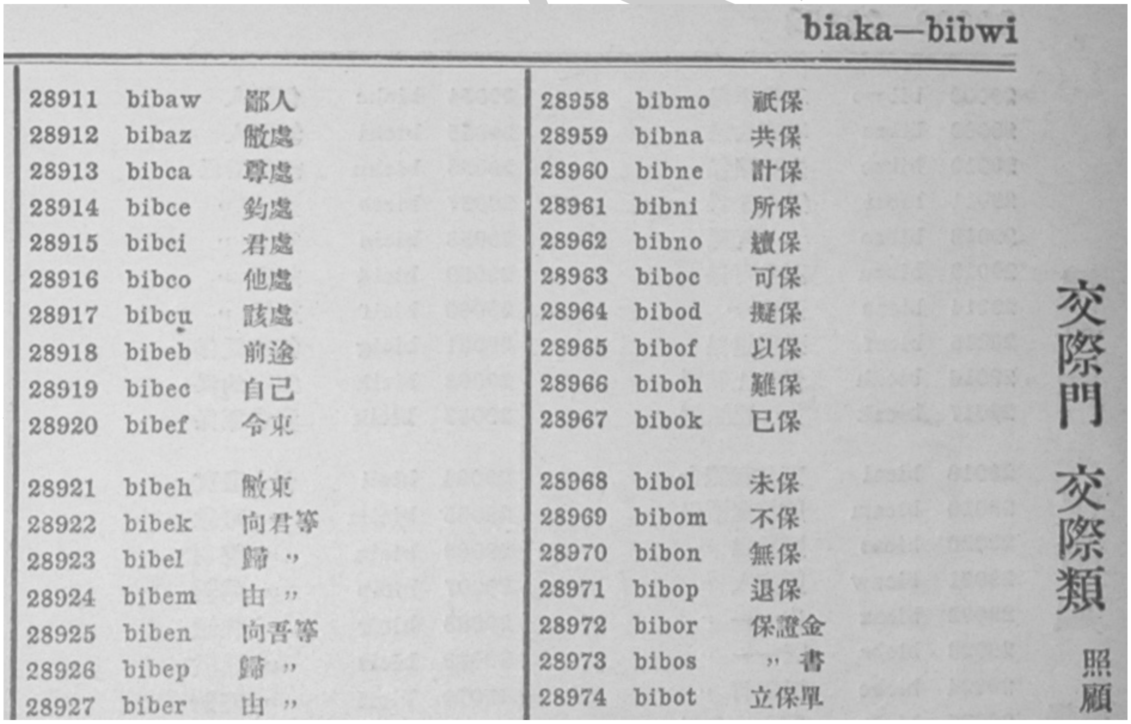


蚤	5734-OZX	銚	6903-TES	CH'O	▨	樵	2884-HOJ
蜩	5781-PEA	鋤	6915-TFU	俏	0195-AHN	炒	3509-ITJ
螬	5834-PIJ	阻	7091-TYG	初	0443-ARB	焦	3542-IUQ
覜	6020-QAH	阼	7092-TYH	剿	0485-ASR	瞧	4225-KYX
詔	6096-QHE	雕	7171-UCC	勦	0531-AUL	硝	4285-LEH
詛	6100-QHY	[illegible]	7257-UFK	哨	0783-BIT	礁	4339-LIR
調	6148-QMO	鰷	7664-UVC	噍	0887-BUL	礎	4342-LIU
謿	6213-QUA	鳥	7680-UVS	峭	1495-DYX	秒	4432-LTU

CHO (조)

CH'O(초)

Figure 18: The *Korean Telegraphic Code*.

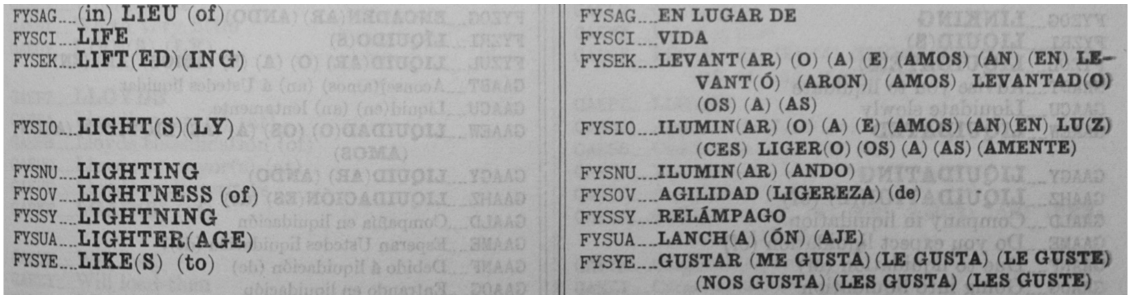


biaka—bibwi

28911	bibaw	鄙人	28958	bibmo	祇保
28912	bibaz	敝處	28959	bibna	共保
28913	bibca	尊處	28960	bibne	計保
28914	bibce	鈞處	28961	bibni	所保
28915	bibci	君處	28962	bibno	續保
28916	bibco	他處	28963	biboc	可保
28917	bibcu	該處	28964	bibod	擬保
28918	bibeb	前途	28965	bibof	以保
28919	bibec	自己	28966	biboh	難保
28920	bibef	令東	28967	bibok	已保
28921	bibeh	敝東	28968	bibol	未保
28922	bibek	向君等	28969	bibom	不保
28923	bibel	歸 „	28970	bibon	無保
28924	bibem	由 „	28971	bibop	退保
28925	biben	向吾等	28972	bibor	保證金
28926	bibep	歸 „	28973	bibos	„ 書
28927	biber	由 „	28974	bibot	立保單

交際門　交際類　照顧

Figure 19: The 1915 *China Republican Telegraphic Code*.



FYSAG	(in) LIEU (of)
FYSCI	LIFE
FYSEK	LIFT(ED)(ING)
FYSIO	LIGHT(S)(LY)
FYSNU	LIGHTING
FYSOV	LIGHTNESS (of)
FYSSY	LIGHTNING
FYSUA	LIGHTER(AGE)
FYSYE	LIKE(S) (to)

FYSAG	EN LUGAR DE
FYSCI	VIDA
FYSEK	LEVANT(AR) (O) (A) (E) (AMOS) (AN) (EN) LEVANT(Ó) (ARON) (AMOS) LEVANTAD(O) (OS) (A) (AS)
FYSIO	ILUMIN(AR) (O) (A) (E) (AMOS) (AN)(EN) LU(Z) (CES) LIGER(O) (OS) (A) (AS) (AMENTE)
FYSNU	ILUMIN(AR) (ANDO)
FYSOV	AGILIDAD (LIGEREZA) (de)
FYSSY	RELÁMPAGO
FYSUA	LANCH(A) (ÓN) (AJE)
FYSYE	GUSTAR (ME GUSTA) (LE GUSTA) (LE GUSTE) (NOS GUSTA) (LES GUSTA) (LES GUSTE)

Figure 20: The 1923 *Peterson International Code, 2nd Edition* with both English and Spanish plaintexts (Peterson 1923).

name.) On top of that, phrase compression and substitution could be added (Figure 19, (*China Republican Code Book* 1915)).

The need for such encodings has not vanished. Telegrams were popular in China until around 2000, when they were displaced by email and a variety of text message systems. The codebook used—typically, one with a 4-digit encoding for each ideograph—was originally developed in the 1870s. Although telegraph usage has dropped off sharply in recent years, as mobile phones have become extremely common, the codebooks are still used for spelling names in certain circumstances, such as when applying for a passport. Many Chinese characters are very similar-looking; this form of encoding is less ambiguous and dialect-independent (Zhao 2009). Its use is often recommended for police use, to avoid errors from transliteration: a name's sound (and hence its transliteration) are dialect-dependent; ideographs are not (Daye 1997). The same set of code points are used for other purposes, such as machine translation. However, the evolution of the Chinese language over time—new words, and hence new ideographs, and the switch to simplified ideographs that the government of the People's Republic of China started in the mid-1950s—has resulted in a more complex code (Chennault 1962; Lamb and Martin 1963), with newer entries not in their nominally-correct place.

More sophisticated codes were multilingual, where the codeword provided the mapping between languages. Thus, in Peterson (1923), **FYSAG** is rendered as both IN LIEU OF and EN LUGAR DE. Kahn describes codebooks that encompassed nine languages.

Note the difficulty that one-part codes have when multilingual: the plaintext alphabetization cannot be consistent. Word indices were provided, generally for all languages, to help with that problem.

Kahn notes that "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." Consider the many types of household staff members described in the *International Police Telegraph Code* (1930)). How many of those entries were relevant even five years later, given onset of the Great Depression? "BOOTS"? "LACKEY"? "CASTLE-KEEPER"?

Specialized professions had their own codes. The theater world had one (Theatrical Code Publishing Co. 1905); it included many variants on phrases like **DISORB**, which meant DO NOT WANT

DRUNKARDS. Some phrases would probably not appear in a modern equivalent, such as **DORIAN** for JEW COMEDIAN. **FILIATION**, CHORUS GIRLS WHO ARE SHAPELY AND GOOD LOOKING, might appear today, though I suspect that **FILIBUSTER**—CHORUS GIRLS WHO ARE SHAPELY, GOOD LOOKING, AND CAN SING might displace it. Then and now, though, the large section on "Financial Straits" is probably appropriate.

The old naval codes are just as illuminating. The section for "Person's Names" in (Wynne 1828), for example, includes EARL OF * *. No other titles of nobility except QUEEN are listed; presumably, LORD and LADY are expected to suffice. Popham (Great Britain Admiralty 1816) has a signal for SEND WOMEN ON SHORE TO WASH.

A more light-hearted example may be seen in (*Unicode* 1886), where **NASUM** is A MARRIAGE HAS BEEN ARRANGED BETWEEN ———. How often, today, does one speak of a marriage being arranged between two parties? (Of course, that is a culture-centric statement, too; in many parts of the world, arranged marriages are still not uncommon.) Surprisingly modern concepts can show up; the (1930) police code did include *living together with* in the same grouping as marriages.

The Unicode book suggests that telegrams were a very rapid means of communication: there is a code word (**MORDAX**) used for scheduling a lunch that same day. Think of the steps necesssary: the message must be composed, encoded, delivered to a telegraph office for transmission, delivered to the recipient, and decoded. Email is much simpler!

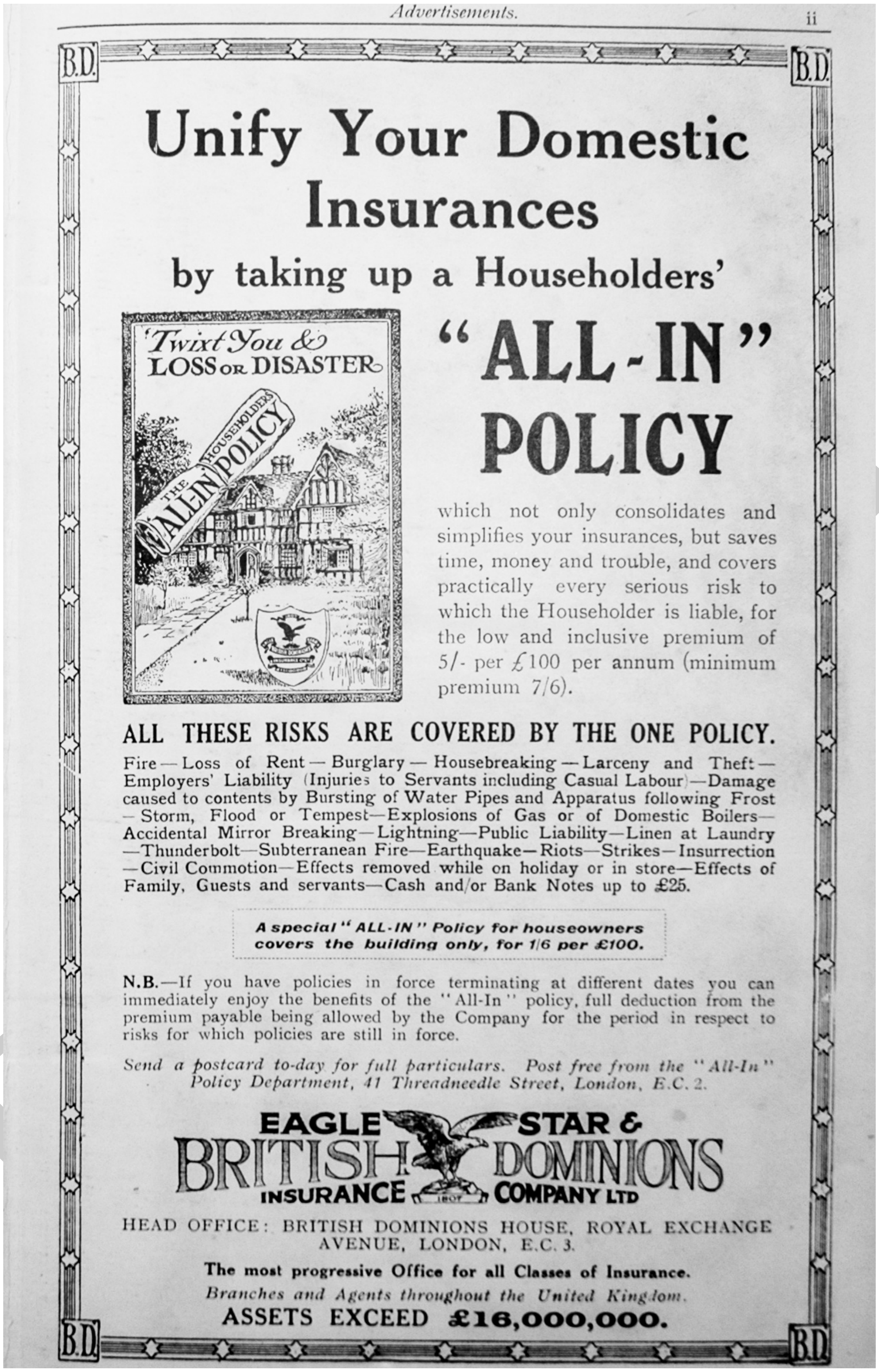
One of the most fascinating codes, from a perspective of revealing attitudes, is the codebook for the China Inland Mission (1907, 1913, 1917). It is replete with many references to "natives": **19316** is THE NATIVES IN THE DISTRICT ARE VERY TROUBLESOME), many phrases about the addressee's wife but none about husbands, etc. There were, of course, codewords concerning Scripture and prayer. It was a turbulent era in China; the Boxer Rebellion had just ended and the Revolution of 1912 was about to start. Not surprisingly, there are many phrases concerning disturbances, riots, rebellions, and revolutions. The most fascinating phrases, though, are **23697** and **23699**, about the Roman Catholic "competition": the former is ROMAN CATHOLIC INTRIGUE and the latter is THE UPRISING WAS CAUSED BY *or* DIRECTED AGAINST THE ROMAN CATHOLICS.

The necessity of using the telegraph was reflected throughout society. Indeed, there are those who argue that relatively speaking, the telegraph had far more effect in its day than the Internet has had today (Standage 1998). Today, printed catalogs frequently contain URLs. The Norton Company's catalog included code words for each product or option: **MATRIX** is NO. 19 ALUNDUM.

Codebooks were expensive. The 1896 *Atlas Universal Travelers' and Business Telegraphic Cipher Code* sold for $5.00 only a few years before New York's Biltmore Hotel, in an ad on the outside cover of the *A B C Telegraphic Code, 5th Edition* (Clausen-Thue 1915) offered rooms starting at $2.50. (The ad also noted that 950 of their 1000 rooms had baths. Perhaps the $2.50 rooms were in the lower 5%...)

The cost of many of the codebooks was indeed defrayed by advertising. Figure 21 shows an ad in (Droege 1920). Most of the ads were, as to be expected, aimed at businesses or at least business travelers, but—as shown here—there were exceptions.

In an eerie parallel with today's controversies, communications intelligence gleaned from telegraphed messages was quite important. Kahn tells much of this story, but the geopolitical aspects are even more fascinating. The U.K. was the center of the world's cable lines; a very high percent-



Advertisements. ii

B.D. B.D.

Unify Your Domestic Insurances

by taking up a Householders'

'Twixt You &
LOSS or DISASTER
THE ALL-IN HOUSEHOLDERS POLICY

"ALL-IN" POLICY

which not only consolidates and simplifies your insurances, but saves time, money and trouble, and covers practically every serious risk to which the Householder is liable, for the low and inclusive premium of 5/- per £100 per annum (minimum premium 7/6).

ALL THESE RISKS ARE COVERED BY THE ONE POLICY.

Fire — Loss of Rent — Burglary — Housebreaking — Larceny and Theft — Employers' Liability (Injuries to Servants including Casual Labour)—Damage caused to contents by Bursting of Water Pipes and Apparatus following Frost — Storm, Flood or Tempest—Explosions of Gas or of Domestic Boilers— Accidental Mirror Breaking—Lightning—Public Liability—Linen at Laundry —Thunderbolt—Subterranean Fire—Earthquake—Riots—Strikes—Insurrection —Civil Commotion—Effects removed while on holiday or in store—Effects of Family, Guests and servants—Cash and/or Bank Notes up to £25.

A special "ALL-IN" Policy for houseowners covers the building only, for 1/6 per £100.

N.B.—If you have policies in force terminating at different dates you can immediately enjoy the benefits of the "All-In" policy, full deduction from the premium payable being allowed by the Company for the period in respect to risks for which policies are still in force.

Send a postcard to-day for full particulars. Post free from the "All-In" Policy Department, 41 Threadneedle Street, London, E.C. 2.

EAGLE STAR & BRITISH DOMINIONS INSURANCE COMPANY LTD

HEAD OFFICE: BRITISH DOMINIONS HOUSE, ROYAL EXCHANGE AVENUE, LONDON, E.C. 3.

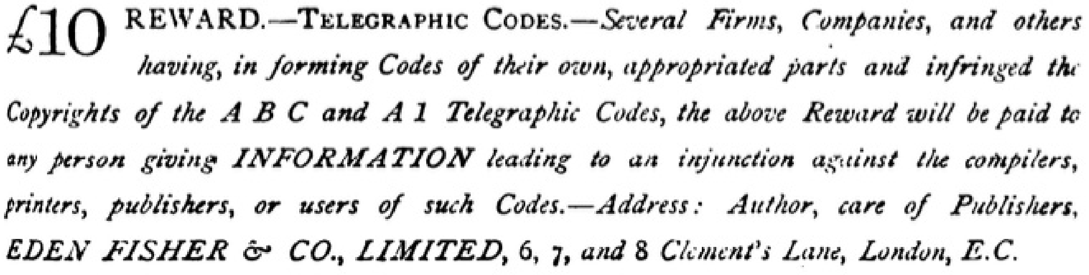
The most progressive Office for all Classes of Insurance.

Branches and Agents throughout the United Kingdom.

ASSETS EXCEED £16,000,000.

B.D. B.D.

Figure 21: An ad in the *A B C 6th Edition* codebook (Droege 1920).



£10 REWARD.—TELEGRAPHIC CODES.—*Several Firms, Companies, and others having, in forming Codes of their own, appropriated parts and infringed the Copyrights of the A B C and A 1 Telegraphic Codes, the above Reward will be paid to any person giving INFORMATION leading to an injunction against the compilers, printers, publishers, or users of such Codes.—Address: Author, care of Publishers, EDEN FISHER & CO., LIMITED,* 6, 7, *and* 8 *Clement's Lane, London, E.C.*

Figure 22: A copyright warning.

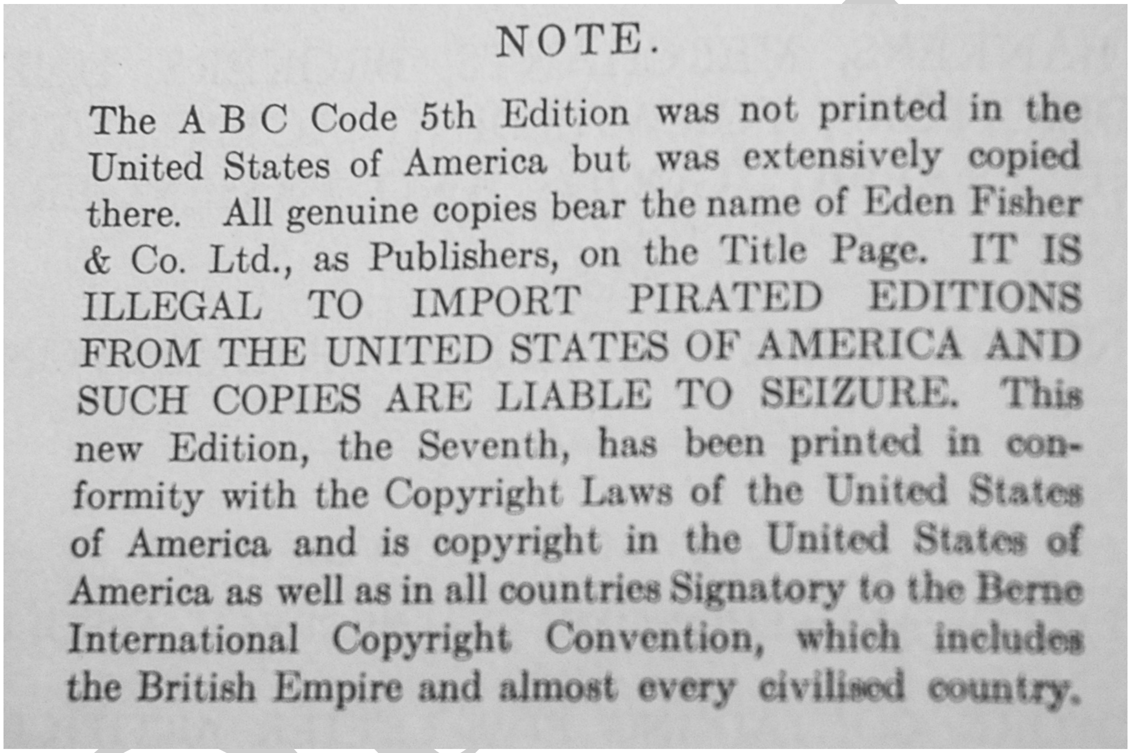
age of international messages flowed through Britain or or one of its colonies (Headrick 1991). This was by design. Not only were "All-red routes"—so-called because that was the map color used for territories of the British Empire—preferred to protect domestic traffic, the Official Secrets Act of 1920 required cable companies to turn over to the government copies of all international telegrams. One U.S. executive tried to explain away the problem in some Senate hearings:

> The messages were then placed in large bags, sealed I believe, and put in wagons. These wagons were driven away under the custody of the Admiralty and lodged overnight in a storehouse and returned to the cable offices the next morning. So that they were kept—they had actual custody of the messages but for a few hours, and so far as the United States messages were concerned, only as a matter of form to make the custom uniform for all countries. We have further investigated and are satisfied that during that period not a single message, commercial, diplomatic, or otherwise, has been actually handled by the Naval Intelligence Bureau, and that their contents are unknown to the British Government because of that fact.

Headrick goes on to wonder if he was "the most naive person ever to testify before Congress, or the most deceitful".

The military importance of civilian telegraph codes continued. During World War II, the Army's Signals Intelligence Service had a Commercial Code Unit in the Code Recovery Section of the Cryptanalytic Branch (Williams 2024). The data they obtained provided insight into economic conditions in various countries, as well as providing trade and travel data.

Finally, we note another important point of commonality with that era: intellectual property rights were a battleground then, too. (Clausen-Thue 1915) offered a reward for information about infringers (Figure 22). Perhaps more significantly, different legal standards in different countries led to problems. For protectionist reasons, U.S. copyright law of the time did not protect books unless they were printed within the country; this could and did lead to piracy. The wording of the warning in Figure 23 (Droege 1936) suggests that perhaps the U.S. was not a civilised [sic] country then. . .



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.

Figure 23: Was the U.S. civilised then?

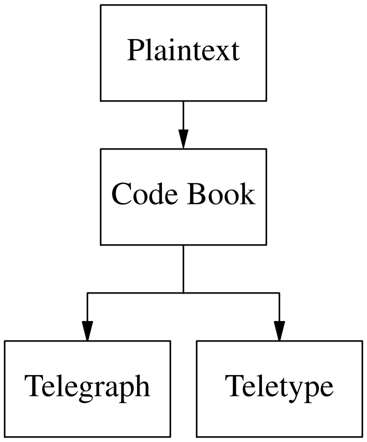


Figure 24: A stack architecture for communications.

6 The Transmission Stack

Figure 24 shows the system architecture as a network stack. Three of our concepts—confidentiality, compression, and correction—can be applied at any of the layers.

At first blush, this seems odd; at the plaintext layer, there would appear to be little room for any of it. Indeed, we now realize that for information-theoretic reasons, we cannot compress encrypted text; applying any sort of confidentiality transform before using the code books would seem impossible. Perhaps more to the point, given the semantic nature of the codes, compression would seem unlikely as well. Still, it can be done, by operating at the semantic level. In *McNeill's Code, 1908 Edition* (1908), users desiring secrecy are told to combine certain numeric fields based on semantic knowledge. Thus, a day of the month—two digits—and the maximum daily output of a stamping mill (asserted to be three digits at most)—can be combined into a single five-digit number, for which there is a code word equivalent. This reduces the number of groups by one; it also makes life harder for an enemy cryptanalyst.

The vocabulary of codebooks can force the user to do other types of compression. Nelson, for example, originally asked that the signal be sent as "England confides that every man will do his duty". Upon being informed that "confides" was not in the codebook and hence would have to be spelled out, he agreed to use "expects" instead.

Finally, the structure of the code may itself force compression. In (Brooke 1926), correspondents are instructed to use a particular stylized form for routine reports of disease outbreak: the date, the port or location, a list of disease-number pairs, a list of ports followed by **UB** to indicate no plague, cholera, smallpox, or yellow fever, and the title of the person filing the report.

(McCutcheon 1885), rather than being a code book per se, is an algorithm and a set of tables for code construction and use. The user is instructed to compile a list of stylized phrases, perhaps of the form subjects, verbs, and objects. Each list entry is denoted by a letter or number; to decode a triplet, the reader would look up each letter in the appropriate list. Many such sets of lists are possible; an indicator word is sent first to denote in what order the sets should be consulted.

Error-handling is more of a stretch; still, one can note the rules given in (*Private Telegraphic Code of Swift & Company* 1931):

```
 b     a    n    e     f     u     l
-...   .-   -.   .   ..-.   ..-   .-..
----------------------------------------
 d     u    t    i     f     u     l
-..   ..-   -    ..  ..-.   ..-   .-..
```

Figure 25: Friedman (1928) shows how the movement of two dots between adjacent letters can completely change the appearance of a word.

> Care must be exercised in copying words from the Code.
>
> Each code word should begin with a capital letter and should be written distinctly (typewritten, if possible) to prevent errors in transmission.

Perhaps more to the point, code words, especially for numerical quantities were much less error-prone than the actual plaintext. The same book thus instructs:

> As a protection against mutilation, phrases, numbers, etc., should be coded if possible, even though the message contains ten words or less. This applies especially to prices and amounts.

It is obvious how all three functions are accomplished via codebooks; we will not belabor the point further. It is, though, worth noting that Kahn (2004) asserts that well before the middle of the 20th century, advances in cryptanalysis had doomed the use of codebooks for protection against sophisticated enemies. Commercial codebooks, even if enciphered, would offer no protection at all.

During the era of telegraph code books, little specific was done to provide link-level confidentiality, at least for commercial messages. Indeed, confidential diplomatic messages were sent by the same means. Compression and error protection were important, but in a non-obvious way. That said, Friedman notes “certain firms … at the present time prefer to use wire and cable telegraphy exclusively [as opposed to radio] and must, for purposes of secrecy, as is the case with banks and brokerage house, use code” (1928). In other words, link selection was done in part to increase confidentiality, because the available, economical, technical mechanisms were perceived to be inadequate.

Compression must always be done against some metric. Today, we are concerned with net bits per second, perhaps with a tradeoff against latency or computational power. The primary metric then was cost—what the telegraph companies would charge for a given message—with error rates the primary tradeoff. Usually, the charge was per word; that, however, rests on the definition of “word”. Internationally, at least, this was a matter of treaties and regulations; these changed over time. (See (Friedman 1928) for details of the issues.) When the rules permitted words in any of fifty or so languages, code compilers used many such dictionaries. When the rules permitted words that were “pronounceable” according to the rules of eight different languages, code makers adapted to that. In one example, (Brooke 1926) specified that the letter **A** should be freely inserted into

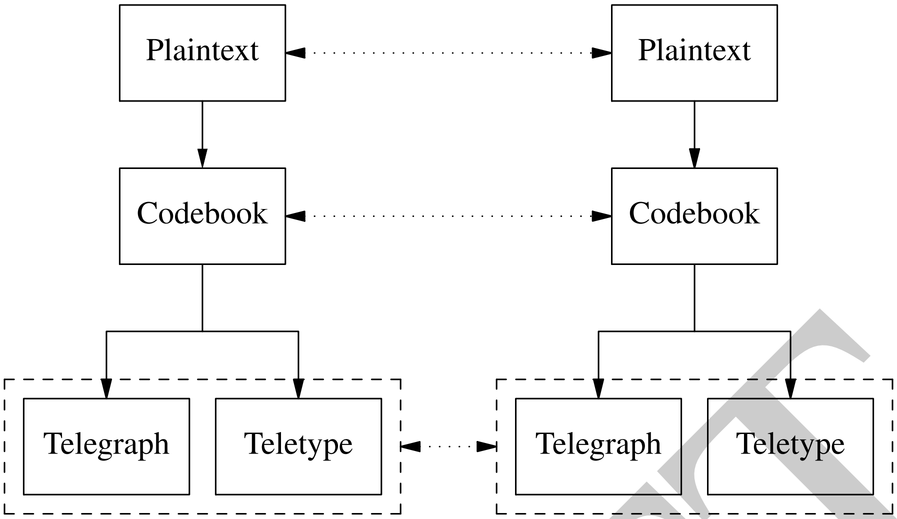


Figure 26: Communication between entities at different levels.

code words to make them pronounceable, and should be deleted on receipt. More commonly, code books were often designed so that two or more code groups could be combined into one chargeable word. Not surprisingly, error characteristics are heavily affected by link characteristics. Figure 25 shows how the appearance of a word can be completely changed by common Morse code mistakes. Clearly, the switch to teletypes would completely eliminate that sort of error. On the other hand, new types of errors, such as accidentally hitting an adjacent letter on the keyboard, could occur. Error-correcting mechanisms needed to be redesigned accordingly.

Another way to look at the situation is to realize that stack components communicate with their peers. Their properties—or failures—in confidentiality, compression, or correction are first manifested at that layer. More importantly, lower layer behavior does not change such results. An early, unencoded telegram differed from a traditional sealed letter in that the plaintext was exposed at the transmission layer. Security at that lower layer—for example, selection of a link not easily tapped—did nothing to protect the message from the eyes of the telegraph operator. We see the same thing today with wireless networking: encrypting a single network hop—say, from a laptop to an access point—does nothing to protect the traffic from being intercepted on another hop: there is no end-to-end protection.

It is worth noting that telegrams were also sent via multiple hops. Security protection on one hop, even if perfect, did nothing to protect other hops. Even codebooks were not always end-to-end. Some code companies offered a decoding service. Senders could address their messages to the decoding center; it would produce plaintext and retransmit to the actual recipient (Figure 27). Such a service was useful for transoceanic messages, where the cost of that hop dominated the total cost of the message. Note the peer associations: if encryption is done at the codebook layer, there is no protection against eavesdropping on the link between the decoding station and the recipient. This is analogous to today's virtual private networks (VPN), where traffic from a laptop is encrypted to the VPN provider but not thereafter.

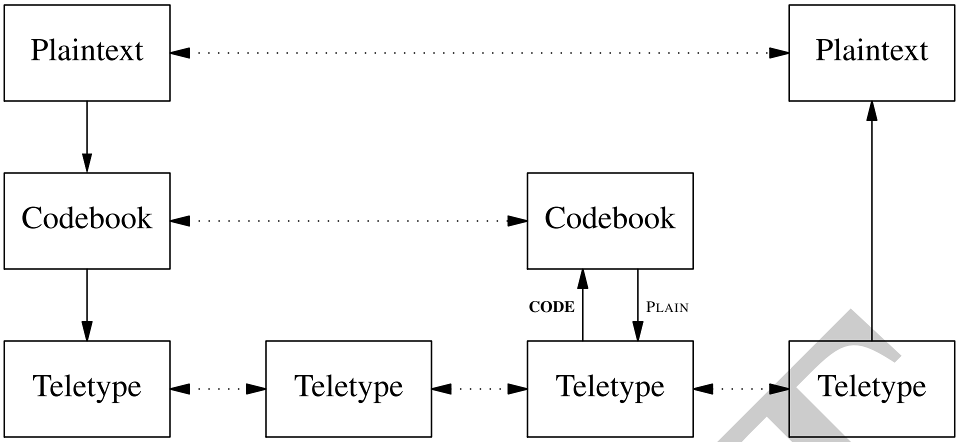


Figure 27: Multi-hop telegram with en route decoding.

7 Parting Thoughts

The era of telegraph codes has largely passed. That said, they persisted in some form much longer than is commonly supposed. The Australian Postmaster-General issued a postal banking codebook in (1968), and the Victorian Railways issued an operational codebook in (1972). As noted earlier, some types of codebooks are still in use in China for special purposes. The *Manual for Use in Sending Tibetan Telegraphic Wireless Messages* was reprinted at least as recently as (1985).

It is unlikely that we will glean new technical insights by studying these tomes. What they excelled at has been mathematicized and optimized. That said, the picture painted of the times is still valuable.

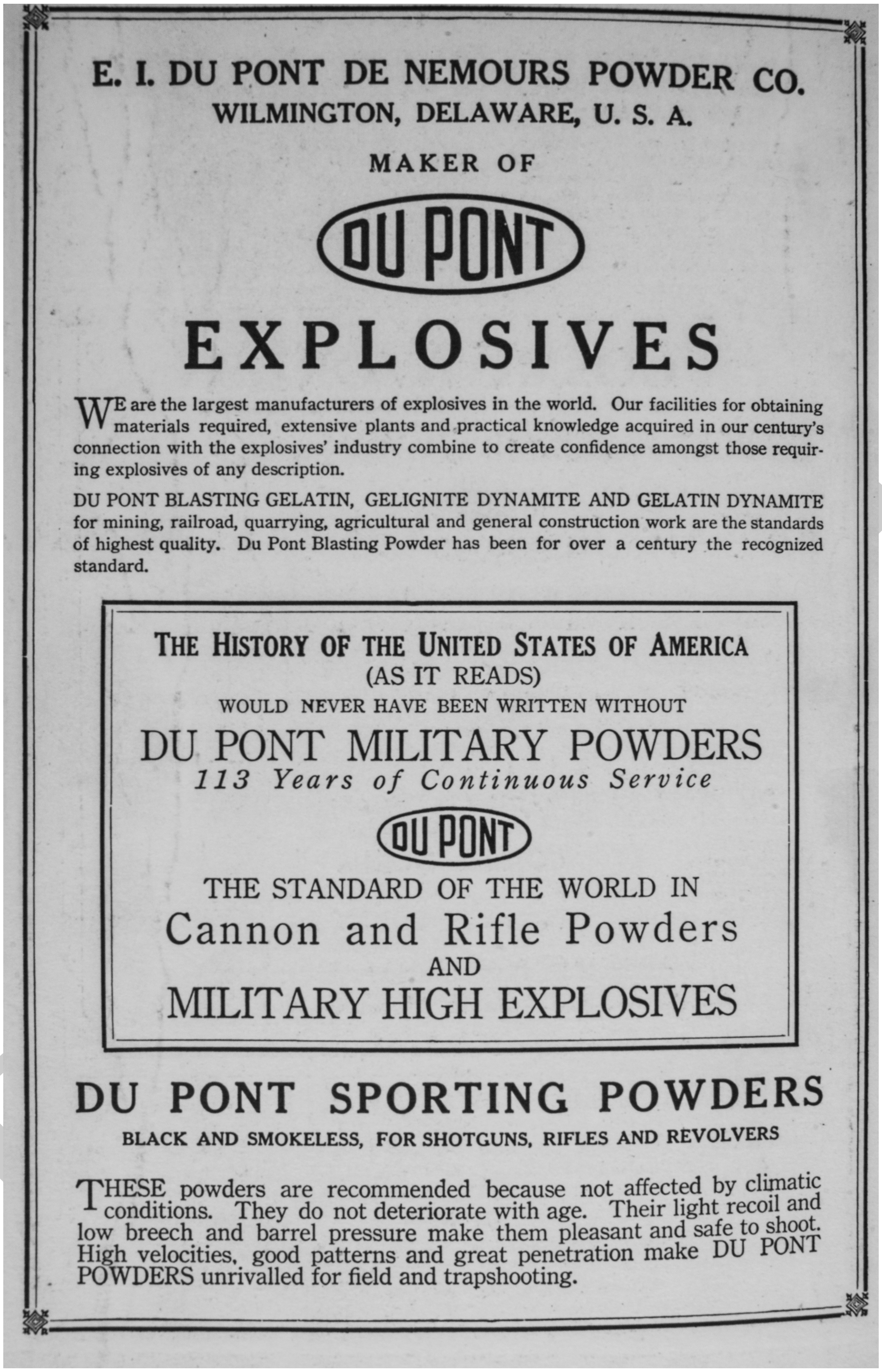
I close with one final similarity. Today, cryptography is sometimes regulated as a munition. Figure 28, an ad from more than 100 years ago (Clausen-Thue 1915), shows that perhaps the linkage has long been there.

Acknowledgments

A paper like this is made immeasurably easier if one has access to a research library, and Columbia University has a superb one. I thank not just the institution but also the librarians and other individuals who have collected and saved obscure works over decades and centuries, against the chance that someone would need them. Robert Simpson of the National Cryptologic Museum Library was also very helpful.

I'd also like to thank Jim Reeds. He first showed me commercial codebooks when I started getting interested in the subject. He also made many useful comments on a draft of this paper, and supplied the error data shown in Figure 8.

Hang Zhao supplied information on modern codebook usage in China and helped with other questions on Chinese codebooks; she and Seung Geol Choi advised me on the Korean Telegraph Code. Ted Lemon provided useful insights on the Tibetan code book. Evelyn Guzman translated the introductory material in (Dobal 1986). Malek Ben Salem and especially Arezu Moghadam



E. I. DU PONT DE NEMOURS POWDER CO.
WILMINGTON, DELAWARE, U. S. A.

MAKER OF

DU PONT

EXPLOSIVES

WE are the largest manufacturers of explosives in the world. Our facilities for obtaining materials required, extensive plants and practical knowledge acquired in our century's connection with the explosives' industry combine to create confidence amongst those requiring explosives of any description.

DU PONT BLASTING GELATIN, GELIGNITE DYNAMITE AND GELATIN DYNAMITE for mining, railroad, quarrying, agricultural and general construction work are the standards of highest quality. Du Pont Blasting Powder has been for over a century the recognized standard.

THE HISTORY OF THE UNITED STATES OF AMERICA
(AS IT READS)
WOULD NEVER HAVE BEEN WRITTEN WITHOUT
DU PONT MILITARY POWDERS
113 Years of Continuous Service
DU PONT
THE STANDARD OF THE WORLD IN
Cannon and Rifle Powders
AND
MILITARY HIGH EXPLOSIVES

DU PONT SPORTING POWDERS

BLACK AND SMOKELESS, FOR SHOTGUNS, RIFLES AND REVOLVERS

THESE powders are recommended because not affected by climatic conditions. They do not deteriorate with age. Their light recoil and low breech and barrel pressure make them pleasant and safe to shoot. High velocities, good patterns and great penetration make DU PONT POWDERS unrivalled for field and trapshooting.

s

Figure 28: Cryptography and explosives…

helped with Persian codebooks. Matsuzaki Yoshinobu provided the Japanese translations. Michal Bryxí and Josef Sipek provided the Czech translations.

References

Bellovin, Steven M. (July 2011). "Frank Miller: Inventor of the One-Time Pad". In: *Cryptologia* 35.3. An earlier version is available as technical report CUCS-009-11, pp. 203–222. URL: https://dx.doi.org/10.1080/01611194.2011.583711.

Chennault, Anne (1962). *Dictionary of New Simplified Chinese Characters*. Georgetown University. URL: https://hdl.handle.net/2027/uva.x000501566.

Coates, Robert M. (May 26, 1934). "Talk of the town: Rebebureau". In: *New Yorker*, pp. 16–17. URL: https://www.newyorker.com/archive/1934/05/26/1934_05_26_016_TNY_CARDS_000237372.

Daye, Douglas D. (1997). *A Law Enforcement Sourcebook of Asian Crime and Cultures: Tactics and Mindsets*. Boca Raton, FL: CRC Press.

Friedman, William F. (1928). "The History of the Use of Codes and Code Language, the International Telegraph Regulations Pertaining Thereto, and the Bearing of this History on the Cortina Report". In: *International Radiotelegraph Conference of Washington: 1927*. Washington: United States Government Printing Office.

Friedman, William F. and Charles J. Mendelsohn (1932). "Notes on Code Words". In: *The American Mathematical Monthly* 39.7, pp. 394–409. ISSN: 00029890. URL: https://www.jstor.org/stable/2300386.

Great Britain Admiralty (1908). *Nelson's Signals: The Evolution of the Signal Flags*. Naval Intelligence Division Historical, No. 1. London: Printed for His Majesty's Stationery Office by Eyre and Spottiswoode.

Hamming, Richard W. (1950). "Error Detecting and Error Correcting Codes". In: *Bell System Technical Journal* 26.2, pp. 147–160.

Headrick, Daniel R. (1991). *The Invisible Weapon: Telecommunications and International Politics, 1851–1945*. New York: Oxford University Press. ISBN: 0195062736.

Kahn, David (1967). *The Codebreakers*. New York: Macmillan.

— (2004). *The Reader of Gentlemen's Mail: Herbert O. Yardley and the Birth of American Codebreaking*. New Haven: Yale University Press.

Lamb, Sydney M. and Samuel E. Martin (1963). *Chinese Character Indexes*. Berkeley: University of California Press.

Maloney, Russell (Nov. 23, 1935). "Talk of the town: Financial crisis". In: *New Yorker*, pp. 11–12. URL: https://www.newyorker.com/archive/1935/11/23/1935_11_23_011_TNY_CARDS_000161388.

McCune, G.M. and E.O. Reischauer (1939). "The Romanization of the Korean Language, Based Upon its Phonetic Structure". In: *Transactions of the Korea Branch of the Royal Asiatic Society* XXXIX, pp. 1–55. URL: http://anthony.sogang.ac.kr/transactions/VOL29/KORS0749D_VOL29.pdf.

Moody, W.H. (1904). *Order on Use of Cipher Code in Navy Telegraph Communications*. Navy Department General Order 2nd Series No. 153. New York Public Library (microform).

Palmer, Michael A. (2005). *Command at Sea: Naval Command and Control since the Sixteenth Century*. Cambridge, Massachusetts: Harvard University Press.

Popham, Hugh (1991). *A Damned Cunning Fellow: The Eventful Life of Rear-Admiral Sir Home Popham KCB, KCH, KM, FRS 1762–1820*. Cornwall, England: Tywardreath.

Postel, J. (Sept. 1981). *Transmission Control Protocol*. RFC 793. IETF. DOI: 10.17487/RFC0793. URL: https://www.rfc-editor.org/info/rfc793.

Ross, Harold (Feb. 17, 1940). “Talk of the town: Explanation”. In: *New Yorker*, p. 13. URL: https://www.newyorker.com/archive/1940/02/17/1940_02_17_013_TNY_CARDS_000179607.

Saltzer, J. H., D. P. Reed, and D. D. Clark (1984). “End-to-end arguments in system design”. In: *ACM Trans. Comput. Syst.* 2.4, pp. 277–288. ISSN: 0734-2071. DOI: https://dl.acm.org/doi/10.1145/357401.357402.

Sechrest, Larry J. (2004). “Public Goods and Private Solutions in Maritime History”. In: *The Quarterly Journal of Austrian Economics* 7.2 (Summer), pp. 3–27. URL: https://mises.org/quarterly-journal-austrian-economics/public-goods-and-private-solutions-maritime-history.

Standage, Tom (1998). *The Victorian Internet: The Remarkable Story of the Telegraph and the Nineteenth Century’s On-line Pioneers*. New York: Walker and Co. ISBN: 0802713424.

Stone, Jonathan and Craig Partridge (2000). “When the CRC and TCP Checksum Disagree”. In: *SIGCOMM Comput. Commun. Rev.* 30.4, pp. 309–319. ISSN: 0146-4833. DOI: https://doi.acm.org/10.1145/347057.347561.

Tunstall, Brian (1990). *Naval Warfare in the Age of Sail: The Evolution of Fighting Tactics 1650–1815*. Edited by Nicholas Tracy. Annapolis, MD: Naval Institute Press.

Weber, Ralph E. (1979). *United States Diplomatic Codes and Ciphers, 1775–1938*. Chicago: Precedent Publishing.

— (2013). *Masked Dispatches: Cryptograms and Cryptology in American History, 1775–1900*. Second edition. Vol. 1. United States Cryptologic History, Series 1: Pre-World War I. Center for Cryptologic History, National Security Agency. URL: https://www.govinfo.gov/content/pkg/GOVPUB-D-PURL-gpo52790/pdf/GOVPUB-D-PURL-gpo52790.pdf.

Williams, Jeanette (2024). *The Invisible Cryptologists: African-Americans, WWII to 1956*. Revised edition. Vol. 5. Series V: The Early Postwar Period 1945-1952. National Security Agency: Center for Cryptologic History. URL: https://media.defense.gov/2021/Jul/13/2002761529/-1/-1/0/INVISIBLE_CRYPTOLOGISTS.PDF.

Zhao, Hang (2009). Private communication.

Codebooks

Bentley, E.L. (1909). *Bentley’s Complete Phrase Code Book*. New edition. London.

Bloomer, J. G. (1874). *Bloomer’s Commercial Cryptograph: A Telegraph Code and Double Index—Holocryptic Cipher*. San Francisco: A. Roman & Co. URL: https://books.google.com/books?id=90UKAAAAIAAJ. Location: Google Books.

Boe, Conrad (1937). *The New Boe Code*. Oslo: Lars Swanström.

Brooke, Gilbert E. (1926). *Code Télégraphique AA (The AA Cable Code)*. Second edition. Singapore: League of Nations Health Organisation, Eastern Bureau. Location: Columbia University.

Charles A. Stoneham & Co (1910). *Code book*. Stoneham & Co.

China Inland Mission (1907). *China Inland Mission Private Telegraph Code*. Shanghai: Methodist Publishing House. Location: Missionary Research Library, Union Theological Seminary.

— (1913). *China Inland Mission Private Telegraph Code*. Second edition. Shanghai: Methodist Publishing House. Location: Missionary Research Library, Union Theological Seminary.

— (1917). *Supplement to the China Inland Mission Private Telegraph Code*. Shanghai: Methodist Publishing House. Location: Missionary Research Library, Union Theological Seminary.

China Republican Code Book (1915). Shanghai: Hsin-Min Telegraphic Code Company.

Cipl, Lubomír (1961). *Unicode: Telegrafický kód s třípísmennou diferencí (Unicode Telegraphic Code with a Three-Letter Difference)*. Czech version. Praha: Foreign Trade Technlogy Library. Location: National Cryptologic Museum Library.

Clausen-Thue, W. (1915). *The A B C Universal Commercial Electric Telegraph Code*. Improved Fifth edition. American Code Company.

Commonwealth of Australia, Postmaster-General's Department (1968). *Telegraph Code*.

Darhan, B. (1912). *Clave Para Asegurar el Mayor Secreto en la Correspondencia Telegráfica (Key to Ensuring the Greatest Secrecy in Telegraphic Correspondence)*. Eighth edition. Madrid. Location: National Cryptologic Museum Library.

Dobal, Carlos (1986). *Habla Liliś: Un Documento Secreto*. Santo Domingo: Biblioteca Nacional.

Droege, William, ed. (1920). *The A B C Universal Commercial Electric Telegraph Code*. Sixth edition. London: Eden Fisher & Co., Limited.

— ed. (1936). *The A B C Universal Commercial Electric Telegraph Code*. Seventh edition. London: Eden Fisher & Co., Limited.

Eckelman, Gerold (1936). *Cosmos Trading*. New York: Mackay Radio & Telegraph Co., Inc.

Gilburt, E.B. (1900). *Tourists' Telegraphic Code*. New York: Brown Brothers & Co.

Government Telegraph Code (1908). London: Secretary's Department, War Office.

Great Britain Admiralty (1816). *Telegraphic Signals for the Use of His Majesty's Fleet*. London: C. Roworth. URL: `https://www.columbia.edu/cgi-bin/cul/resolve?clio6396307`. Location: EBOOK via Columbia University Library.

Greely, Adolphus W. (1899). *Preliminary War Department Telegraphic Code, Supplemental to and to be Inserted as an Appendix to Western Union Telegraphic Code*. War Department Document Number 93. Washington, DC: Government Printing Office. Location: New York Public Library (microform).

Hartfield, Thomas W. (1896). *The Atlas Universal Traveller's and Business Telegraphic Cipher Code*. Second edition. C. Amory Stevens.

International Police Telegraph Code (1930).

Japanese Ministry of Telecommunications (1943). *Gembun Honsho*. C. Itoh & Co., Ltd. Location: National Cryptologic Museum Library.

Japanese Special Code Book (1943). First edition. Mitsui Steamship Co. Location: National Cryptologic Museum Library.

Korean Telegraphic Code Book (1950?).

McCutcheon, Frederic George (1885). *The Telegram Formula and Code Combiner*. London: Marchant SInger and Co. Location: Columbia University.

McDougal, J.B. et al. (1921). *Federal Reserve Telegraph Code*. Copy number 10. Leased Wire Committee.

McNeill, Bedford (1908). *McNeill's Code*. 1908 edition. facsimile reduction. London: Whitehead, Morris & Co.

Meisenbach, A.C. (1923). *Acme Commodity and Phrase Book*. San Francisco: Acme Code Company.

Miller, Frank (1882). *Telegraphic code to Insure Privacy and Secrecy in the Transmission of Telegrams*. Google graciously scanned this book at my request. New York: Charles M. Cornwell. URL: https://books.google.com/books?id=tT9WAAAAYAAJ&pg=PA1#v=onepage&q&f=false. Location: Library of Congress.

Mitsui Bussan Japanese Code Book (1941). Seventh edition. Location: National Cryptologic Museum Library.

National City Bank of New York (1938). *Confidential Authenticating Code of the National City Bank of New York*. Location: National Cryptologic Museum Library.

New York Central Lines VAN Code (1923).

Pantelegraphy Simplex Translating & Check Card (1907). London & New York: The Pantelegraphy Publishing Co., Ltd.

Peterson, Ernest E. (1923). *Peterson International Code*. Second edition.

Private Telegraphic Code of Swift & Company (1931). Peterson Cipher Code Corporation.

Rlung 'phrin gtong deb shes bya kun khyab: Manual for Use in Sending Tibetan Telegraphic Wireless Messages (1985). Reproduced from a rare print of the 1949 Lhasa blocks. Sambhota Publications. Location: East Asian Library, Columbia University.

Satoshi, Tomokiyo (2019). *Japanese Telegraph Codes*. URL: https://cryptiana.web.fc2.com/code/jtelegraph_e.htm.

Sheahan, W.A. (1892). *Cipher Code for Telegraphic Correspondence*.

Slater, Robert (1870). *Telegraphic Code, to Ensure Secresy in the Transmission of Telegrams*. First edition. London: W.R. Gray. URL: https://books.google.com/books?id=MJYBAAAAQAAJ.

— (1876). *Banking Telegraphy: Combining Authenticity, Economy, and Secrecy, a Code for the Use of Bankers and Merchants*. London: W.R. Gray. URL: https://books.google.com/books?id=6A4EAAAAQAAJ.

— (1938). *Telegraphic Code, to Ensure Secrecy in the Transmission of Telegrams*. Ninth edition. London: Simpkin Marshall, Ltd.

Smith, Francis O.J. (1845). *The Secret Corresponding Vocabulary, Adapted for use to Morse's Electro-Magnetic Telegraph: and Also in Conducting Written Correspondence, Transmitted by the Mails, or Otherwise*. Portland, ME: Thurston, Ilsley & Co. URL: https://books.google.com/books?id=Z45clCxsF7EC. Location: Rare Book & Manuscript Library, Columbia University.

Tariff Book No. 77 (1953). Western Union Telegraph Company.

Telling, H.G. (1929). *New Standard Code*. London: Amalgamated Code Compilers, Ltd.

Theatrical Code Publishing Co. (1905). *The Theatrical Cipher Code; Adapted Especially to the Use of Everyone Connected in any Way with the Theatrical Business*. Los Angeles. Location: New York Public Library for the Performing Arts.

Unicode (1886). Second edition. Cassell & Company.

Victorian Railways (1972). *Telegraph Code Book*.

War Department Telegraphic Code (1899–1904). Washington: United States Government Printing Office. Location: New York Public Library (microform).

Western Union Telegraphic Code (1900). Universal edition. International Cable Directory Company.

Wynne, Richard B. (1828). *A New Code of Telegraphic Signals for Yachts and Pleasure Boats*. Edinburgh: Printed for the author. URL: `https://books.google.com/books?id=PC8IGV7fUGMC`. Location: Oxford University.

Where a location is noted without a URL, it is the physical copy I actually consulted. If no location or URL is given, the book is in a private collection, often my own before the donation.