Fall 2019
Chris Christensen
MAT/CSC 483
Section 18

Codes

Ciphers substitute for or transpose characters or strings of characters. To encipher or to encrypt means to put a message into cipher. To decipher or to decrypt means to recover the plaintext by a person who possesses the key to the cipher.

Codes substitute for parts of language – words, phrases, sentences, etc. Usually codes are recorded in books. To encode means to put a message into code. To decode means to recover the plaintext by a person who possesses the codebook.

Codebreaking is an informal term for cryptanalysis.

Ciphers are used to hide the meaning of a message, but they do not hide the fact that a message was transmitted.

Codes are used to transmit information correctly and can be designed to detect or to correct transmission errors.

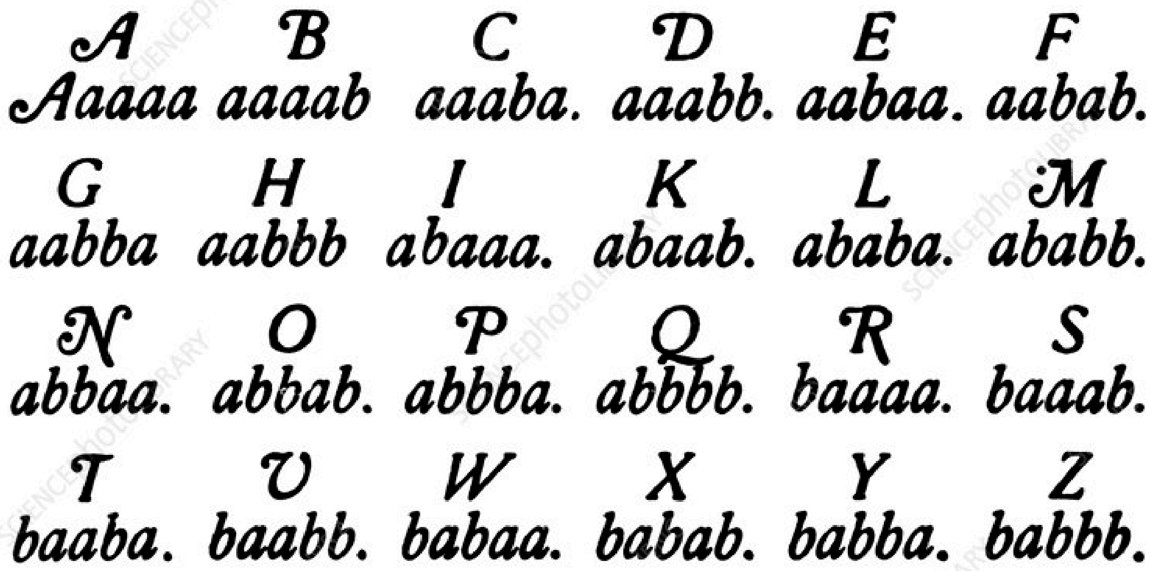
Commercial Telegraph Codes

Commercial codes were developed to shorten the content of a message and, therefore, reduce the cost of its transmission.

CodeNo	Code Word	
00001	*Abacot*	**Abandon.**
00002	*Abactor*	You must abandon
00003	*Abase*	You must not abandon
00004	*Abasement*	Will abandon
00005	*Abatable*	Will not abandon
00006	*Abater*	I (we) will abandon
00007	*Abbacy*	I (we) cannot abandon
00008	*Abbatial*	Not likely to abandon
00009	*Abbess*	Likely to abandon
00010	*Abbey*	Can I (we) abandon
00011	*Abbot*	**Abandoned.**
00012	*Abbreviate*	Was abandoned
00013	*Abdicate*	Was abandoned in a sinking state
00014	*Abdication*	Was not abandoned
00015	*Abdomen*	Why was it abandoned
00016	*Abdominal*	Why was it not abandoned
00017	*Abducent*	Abandoned by the crew
00018	*Abduction*	**Abate.**
00019	*Abed*	Must abate more
00020	*Aberrance*	Cannot abate more
00021	*Aberrant*	Will abate
00022	*Aberration*	Will not abate
00023	*Abet*	I (we) cannot abate
00024	*Abetment*	Not likely to abate
00025	*Abeyance*	Most likely to abate
00026	*Abhor*	**Abide.**
00027	*Abhorent*	You must abide by
00028	*Abider*	Will you abide by
00029	*Abiding*	Cannot abide by
00030	*Abject*	I (we) will abide by
00031	*Abjection*	**Able.**
00032	*Ability*	Are you able
00033	*Abjure*	I am (we are) not able
00034	*Ablactate*	Will you be able
00035	*Ablation*	I (we) shall be able
00036	*Ablegate*	I (we) shall not be able
00037	*Ablepsy*	Will not be able
00038	*Abluent*	Will probably be able
00039	*Ablution*	Have been able
00040	*Abnegate*	Have not been able
00041	*Abode*	Is (are) not able
00042	*Abolition*	**Aboard.**
00043	*Abominate*	All cargo is on board
00044	*Aborigines*	No cargo is on board
00045	*Abortive*	Part cargo is on board
00046	*Abound*	Cannot take cargo on board
00047	*Abrade*	Will not permit cargo to go on board
00048	*Abrasion*	Why is the cargo not on board
00049	*Abridge*	All on board
00050	*Abroach*	Are the crew on board

Baconian Cipher

In 1605, Francis Bacon (1561 – 1626) developed a code to substitute for the letters of the alphabet. The cipher – really a binary code – substituted a five-letter string of a's and b's (the first two letters of his last name) for each letter of the alphabet (i and j use the same substitution, and u and v use the same substitution.).



A	B	C	D	E	F
Aaaaa	aaaab	aaaba.	aaabb.	aabaa.	aabab.
G	H	I	K	L	M
aabba	aabbb	abaaa.	abaab.	ababa.	ababb.
N	O	P	Q	R	S
abbaa.	abbab.	abbba.	abbbb.	baaaa.	baaab.
T	V	W	X	Y	Z
baaba.	baabb.	babaa.	babab.	babba.	babbb.

William and Elizebeth Friedman explored the writings of Shakespeare to determine whether there were coded messages hidden in Shakespeare's writings – writings that would reveal that Bacon wrote Shakespeare. In 1957, they wrote *The Shakespearean Ciphers Examined* which debunking the theory.

The beginning of the paragraph immediately above contains a hidden message encoded with a Baconian cipher by means of different fonts. Hiding the fact that a message is being transmitted is called steganography; it is unlike a cipher which acknowledges that a message is being transmitted.

The Baconian cipher is a multilateral substitution; it is a "five-bit" code.

Morse Code

Morse code was developed in 1844 by Samuel Morse (1791 – 1872) to facilitate transmission of letters of the alphabet by telegraph using short (dot) and long (dash) pulses. The most frequent letters have the shortest substitutions; so, messages has the shortest transmission times.

International Morse Code

1. The length of a dot is one unit.
2. A dash is three units.
3. The space between parts of the same letter is one unit.
4. The space between letters is three units.
5. The space between words is seven units.

A	● ▬
B	▬ ● ● ●
C	▬ ● ▬ ●
D	▬ ● ●
E	●
F	● ● ▬ ●
G	▬ ▬ ●
H	● ● ● ●
I	● ●
J	● ▬ ▬ ▬
K	▬ ● ▬
L	● ▬ ● ●
M	▬ ▬
N	▬ ●
O	▬ ▬ ▬
P	● ▬ ▬ ●
Q	▬ ▬ ● ▬
R	● ▬ ●
S	● ● ●
T	▬
U	● ● ▬
V	● ● ● ▬
W	● ▬ ▬
X	▬ ● ● ▬
Y	▬ ● ▬ ▬
Z	▬ ▬ ● ●
1	● ▬ ▬ ▬ ▬
2	● ● ▬ ▬ ▬
3	● ● ● ▬ ▬
4	● ● ● ● ▬
5	● ● ● ● ●
6	▬ ● ● ● ●
7	▬ ▬ ● ● ●
8	▬ ▬ ▬ ● ●
9	▬ ▬ ▬ ▬ ●
0	▬ ▬ ▬ ▬ ▬

Baudot Code

Emil Baudot (1845 – 1903) in 1870 developed a "five-bit" code for the transmission of the letters of the alphabet by teletype.

Below is a version used by the British Bletchley Park codebreakers during World War II. They called the symbols spark (cross) and no spark (dot).

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

letters	figures	BP notation
A	-	A
B	?	B
C	:	C
D	who are you ?	D
E	3	E
F	%	F
G	&	G
H	Br. Pound sign	H
I	8	I
J	ring bell	J
K	(	K
L	)	L
M	.	M
N	,	N
O	9	O
P	0	P
Q	1	Q
R	4	R
S	'	S
T	5	T
U	7	U
V	=	V
W	2	W
X	/	X
Y	6	Y
Z	+	Z
•••••	not used	/
••X••	space	9 or .
•••X•	carriage return3	
•X•••	line feed	4
XX•XX	shift to figures	5 or +
XXXXX	shift to letters	8 or -

ASCII

With the development of digital computers, Baudot code was succeeded by 7-bit ASCII code (American Standard Code for Information Exchange) in 1963 (which was extended in 1967 and 1986).

ASCII codes for selected characters

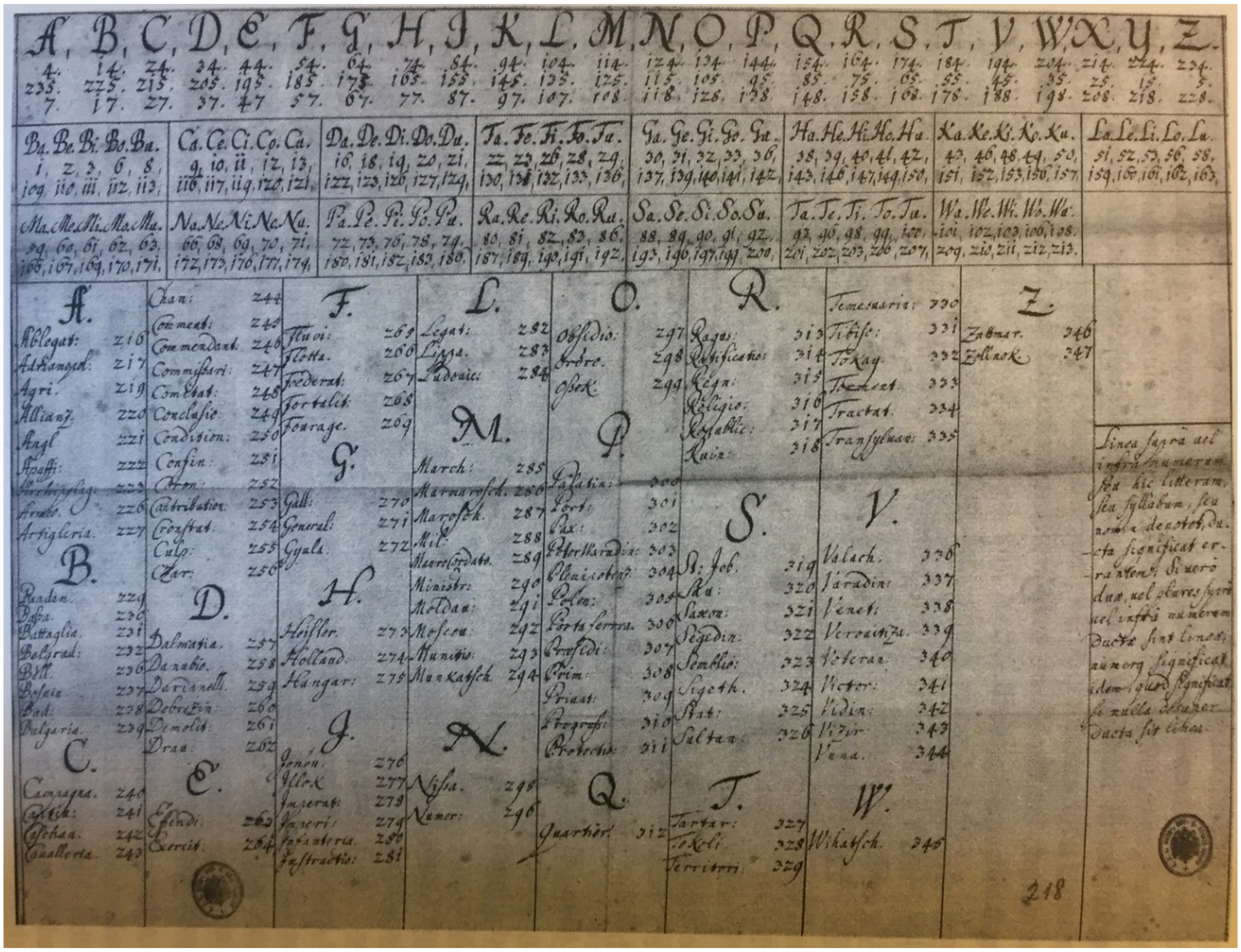
Binary	Character	Binary	Character
0010 0000	Blank	0101 0100	T
0010 0001	!	0101 0101	U
0010 0111	`	0101 0110	V
0010 1100	,	0101 0111	W
0010 1110	.	0101 1000	X
0011 0000	0	0101 1001	Y
0011 0001	1	0101 1010	Z
0011 0010	2	0110 0001	a
0011 0011	3	0110 0010	b
0011 0100	4	0110 0011	c
0011 0101	5	0110 0100	d
0011 0110	6	0110 0101	e
0011 0111	7	0110 0110	f
0011 1000	8	0110 0111	g
0011 1001	9	0110 1000	h
0100 0001	A	0110 1001	i
0100 0010	B	0110 1010	j
0100 0011	C	0110 1011	k
0100 0100	D	0110 1100	l
0100 0101	E	0110 1101	m
0100 0110	F	0110 1110	n
0100 0111	G	0110 1111	o
0100 1000	H	0111 0000	p
0100 1001	I	0111 0001	q
0100 1010	J	0111 0010	r
0100 1011	K	0111 0011	s
0100 1100	L	0111 0100	t
0100 1101	M	0111 0101	u
0100 1110	N	0111 0110	v
0100 1111	O	0111 0111	w
0101 0000	P	0111 1000	x
0101 0001	Q	0111 1001	y
0101 0010	R	0111 1010	z
0101 0011	S	0011 1111	?

Nomenclators

A nomenclator is a combination of a code and a cipher. Typically a nomenclator consists of a substitution cipher for the letters of the alphabet and codewords for commonly used names, locations, phrases, etc. Sometimes nomenclators use homophones – have more than one substitution for high frequency letters or words or phrases.

Nomenclators were popular from the 14th century until the 18th century.

Here is a nomenclator (in French) from the 17th century.



A,	B,	C,	D,	E,	F,	G,	H,	I,	K,	L,	M,	N,	O,	P,	Q.	R.	S.	T,	V,	W,	X,	Y,	Z.
4.	14.	24.	34.	44.	54.	64.	74.	84.	94.	104.	114.	124.	134.	144.	154.	164.	174.	184.	194.	204.	214.	224.	234.
235.	225.	215.	205.	195.	185.	175.	165.	155.	145.	135.	125.	115.	105.	95.	85.	75.	65.	55.	45.	35.	25.	15.	5.
7.	17.	27.	37.	47	57.	67.	77.	87.	97.	107.	108.	118.	128.	138.	148.	158.	168.	178.	188.	198.	208.	218.	228.

Ba. Be. Bi. Bo. Bu.	Ca. Ce. Ci. Co. Cu.	Da. De. Di. Do. Du.	Fa. Fe. Fi. Fo. Fu.	Ga. Ge. Gi. Go. Gu.	Ha. He. Hi. Ho. Hu.	Ka. Ke. Ki. Ko. Ku.	La. Le. Li. Lo. Lu.
1, 2, 3, 6, 8,	9, 10, 11, 12, 13,	16, 18, 19, 20, 21,	22, 23, 26, 28, 29,	30, 31, 32, 33, 36,	38, 39, 40, 41, 42,	43, 46, 48, 49, 50,	51, 52, 53, 56, 58,
109, 110, 111, 112, 113,	116, 117, 119, 120, 121,	122, 123, 126, 127, 129,	130, 131, 132, 133, 136,	137, 139, 140, 141, 142,	143, 146, 147, 149, 150,	151, 152, 153, 156, 157,	159, 160, 161, 162, 163,

Ma. Me. Mi. Mo. Mu.	Na. Ne. Ni. No. Nu.	Pa. Pe. Pi. Po. Pu.	Ra. Re. Ri. Ro. Ru.	Sa. Se. Si. So. Su.	Ta. Te. Ti. To. Tu.	Wa. We. Wi. Wo. Wu.
59, 60, 61, 62, 63,	66, 68, 69, 70, 71,	72, 73, 76, 78, 79,	80, 81, 82, 83, 86,	88, 89, 90, 91, 92,	93, 96, 98, 99, 100,	101, 102, 103, 106, 108.
166, 167, 169, 170, 171,	172, 173, 176, 177, 179,	180, 181, 182, 183, 186,	187, 189, 190, 191, 192,	193, 196, 197, 199, 200,	201, 202, 203, 206, 207,	209, 210, 211, 212, 213.

A.	
Ablegat:	216
Adrianopol:	217
Agri.	219
Allianz.	220
Angl	221
Apaffi:	222
Archipelag.	223
Arnaut.	226
Artigleria.	227
B.	
Baaden.	229
Bassa.	230
Battaglia.	231
Belgrad:	232
Bell.	236
Bosnia.	237
Bud:	238
Bulgaria.	239
C.	
Campagna.	240
Castell:	241
Caschau.	242
Caualleria.	243
Chan:	244
Commeat:	245
Commendant.	246
Commissari:	247
Comitat:	248
Conclusio.	249
Condition:	250
Confin:	251
Coron:	252
Contribution.	253
Cronstat.	254
Culp:	255
Czar:	256
D.	
Dalmatia.	257
Danubio.	258
Dardanelli.	259
Debrezin:	260
Demolit:	261
Drau:	262
E.	
Effendi.	263
Exercit:	264
F.	
Fluvi:	265
Flotta.	266
Foederat:	267
Fortalit:	268
Fourage.	269
G.	
Gall:	270
General:	271
Gyula.	272
H.	
Heissler.	273
Holland.	274
Hungar:	275
I.	
Jenou.	276
Illock	277
Imperat:	278
Imperi:	279
Infanteria.	280
Instructio:	281
L.	
Legat:	282
Lippa.	283
Ludovic:	284
M.	
March:	285
Marmarosch.	286
Marosch.	287
Mil:	288
Maurocordato.	289
Ministr:	290
Moldau:	291
Moscou:	292
Munitio:	293
Munkatsch.	294
N.	
Nissa.	295
Numer:	296
O.	
Obsidio:	297
Ordre.	298
Ossek.	299
P.	
Palatin:	300
Port:	301
Pax:	302
PeterWaradin:	303
Plenipotent:	304
Polon:	305
Porta ferrea.	306
Praesidi:	307
Prim:	308
Priuat:	309
Progress:	310
Protectio:	311
Q.	
Quartier.	312
R.	
Ragus:	313
Ratificatio:	314
Regn:	315
Religio:	316
Respublic:	317
Ruin:	318
S.	
St: Job.	319
Sau:	320
Saxon:	321
Segedin:	322
Semblio:	323
Sigeth.	324
Stat:	325
Saltan:	326
T.	
Tartar:	327
Tekeli	328
Territori:	329
Temesuarin:	330
Tibisc:	331
Tokay.	332
Toement.	333
Tractat.	334
Transsyluan:	335
V.	
Valach:	336
Varadin:	337
Venet:	338
Verovitiza.	339
Veteran.	340
Victor:	341
Vidin:	342
Vizir	343
Vena.	344
W.	
Wihatsch.	345
Z.	
Zathmar.	346
Zolnok	347

Linea supra vel
infra numerum,
seu hic litteram,
seu syllabam, seu
nomen denotet, du-
cta significat er-
rantem. Si vero
duæ, vel plures supra
vel infra numerum
ductæ sint lineæ,
numerus significat
idem, quod significat
si nulla desuper
ducta sit linea.

218