

pre-Independence


Charles Dumas and Franklin

The Dumas Cipher (Partial)

v o u l e z - v o u s s e n t i r
 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17

l a d i f f e r e n c e ? j e t t
 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34

e z l e s y e u x u r l e
 35 36 37 38 39 40 41 42 43 44 45 46 47 48



Dear Sir,
 We have News here that your Fleet has behaved bravely; I congratulate you upon it most cordially.
 I have just received a 14. 5. 3. 10. 28. 2. 76. 202. 66. 11. 12. 272. 100. 14. joining 76. 5. 43. 45. 16. 15.
 484. 238. 29. 200. 90. 580. 11. 120. 27. 56. 35. 104. 502. 28. 075. 85. 79. 38. 63. 44. 22. 209. 17. 66.
 29. 147. 126. 41. but this is not likely to afford 202. 35. 580. 10. 227. 613. 176. 373. 309. 4. 108. 40.
 19. 97. 309. 17. 35. 90. 201. 100. 677.

By our last Advice our Affairs were in a pretty good train. I hope we shall have advice of the
 Expulsion of the English from Virginia.

I am ever,

Dear Sir, Your most obedient &
 most humble Servant
 B. Franklin^r

from *Masked Dispatches*, NSA

Independence

James Lovell and John Adams

1 BRA
 2 CSB
 3 DTC
 4 EUD
 5 FVE
 6 GWF
 7 HXG
 8 IVH
 9 JZI
 10 K&J
 11 LAK
 12 MBL
 13 NCM
 14 OND
 15 PEO
 16 QFF
 17 RGQ
 18 SHR
 19 TIS
 20 UJT
 21 VKU
 22 WLW
 23 YMN
 24 YNX
 25 ZOY
 26 &PZ
 27 AQG

I can only say that we are 27. 11. 12. 21. 16. 4. 14. 3.

21. 19. 18. 18. 26. 23. 19 .3. 7. 24 .13. 19. 2.

26. 1. 11. 8. the latter owing very much to the 2. 15.

10. 11. 23. 25 4. 13. 10. 25. 26. 3. 6. 19. 12.

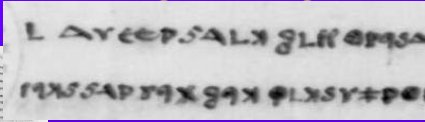
17.*

James Lovell to John Adams, November 1777 from Paris

Keyword: CR; used with nulls

Traitors

Church and George Washington



*To Major Cane in Boston,
 On His Magisty's Service—*

*I hope this will reach you; three attempts have I made
 without success. ...*

*The people of Connecticut are raving in the cause of
 liberty. A number from this colony, from the town of
 Stamford, robbed the King's stores at New York with some
 small assistance the New Yorkers lent them.*

<http://memory.loc.gov/mss/mgw/mgw4/033/0700/0754.jpg>

Washington's Code

+ substitution

One-part code

Source: Papers of George Washington, library of Congress

1	a	37	attone	73	camp
2	an	38	attack	74	came
3	all	39	alarm	75	cost
4	at	40	action	76	corps
5	and	41	accomplish	77	change
6	art	42	apprehend	78	carry
7	arms	43	abatis	79	clergy
8	about	44	accommodate	80	common
9	above	45	alternative	81	consult
10	absent	46	artillery	82	contest
11	absurd	47	ammunition	83	contract
12	adorn	48	be	84	contant

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

from Masked Dispatches, NSA

Patterson's Cipher

pt: Buonaparte has at last given peace to Europe


1 bastpoe
2 uragee
3 ottiau Keywords: nap(213), ben (123)

1 nelvcr
2 ahaeeo
3 pasntp

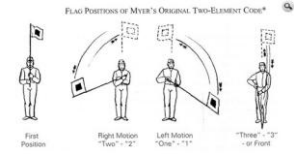
wuragee **rt**bastpoe **hr**hottiau
qAhaeeo **wr**nelvcr **te**gpasntp

ct: wurag eertb astpo ehrho ttiau qahae
eowrn elvcr tegpa sntp

Myer's Wig-Wag System




PLAC POSITION on MYER'S ORIGINAL TWO-ELEMENT CODE*



Letter	1st Motion	2nd Motion	3rd Motion
A	22	R	211
B	2112	S	212
C	121	T	2
D	222	U	112
E	12	V	1222
F	2221	W	1121
G	2211	X	2122
H	122	Y	111
I	1	Z	2222
J	1122		1111
K	2121	flag	2212
L	221	tion	1112
M	1221		
N	11		
O	21	3	end of word
P	1212	33	end of sentence
Q	1211	333	end of message

From http://signal.portal.army.mil/siteDev/signal150/00_wig_wag.html



Route Cipher in the Civil War


“The principle of the cipher consisted in writing a message with an equal number of words in each line, then copying the words up and down the columns by various routes, throwing in an extra word at the end of each column, and substituting other words for important names and verbs.” J.E. O’Brien

Union Cryptography

- I. Combined cipher/code cryptosystem: route or transposition (USHT); simple substitution encipherment in text
- II. Cipher
 - A. disk (Signal Corps, for visual signaling)
 - B. dinomic substitution (Van Lew)
- III. Miscellaneous (Lincoln's reversed phonetics; clothes-line, countersigns, signals)

Confederate Cryptography

- I. Codes
 - A. dictionary
 - B. open code
 - C. signs and signals
- II. Ciphers
 - A. substitution
 - 1. simple, monographic substitution
 - 2. simple, symbols
 - 3. simple, keyed
 - 4. polyalphabetic; Vigenère
 - B. transposition: revolving grille
- III. Concealment
 - A. microdot
 - B. ink
 - C. compact notes



Myer's Cipher Disk

from *Masked Dispatches*, NSA
