San Jose Semaphore: The Solution

Ben Rubin
benrubin@earstudio.com
August 7, 2007

She looked down a slope, needing to squint for the sunlight, onto a vast sprawl of houses which had grown up all together, like a well-tended crop, from the dull brown earth; and she thought of the time she'd opened a transistor radio to replace a battery and seen her first printed circuit. The ordered swirl of houses and streets, from this high angle, sprang at her now with the same unexpected, astonishing clarity as the circuit card had. Though she knew even less about radios than about Southern Californians, there were to both outward patterns a hieroglyphic sense of concealed meaning, of an intent to communicate. There'd seemed no limit to what the printed circuit could have told her (if she had tried to find out); so in her first minute of San Narciso, a revelation also trembled just past the threshold of her understanding.

Excerpt from Thomas Pynchon's 1966 novel, *The Crying of Lot 49*

Introduction

San José Semaphore, by artist Ben Rubin, is a public artwork commissioned by Adobe Systems Incorporated in collaboration with the City of San Jose's Office of Cultural Affair's Public Art Program.

Located within the top floors of Adobe's Almaden Tower headquarters in San José, California, San José Semaphore is a multi-sensory kinetic artwork that illuminates the San José skyline with the transmission of a coded message. San José Semaphore's four ten-foot wide illuminated disks rotate every 7.2 seconds, engaging viewers with a steady, glowing, and purposefully moving presence. The artwork's illuminated disks perform a kind of mechanical dance as a method of communication. A low-power radio broadcast provides a soundtrack that is audible within 2-3 blocks of the Almaden Tower on AM 1680. An online simulcast provides a way to see and hear the piece remotely.

Cracking the coded message has been posed as a challenge for the public. This document presents the solution to the code, revealing both the content of the Semaphore's message, and the means by which it was encrypted.

The Message Content Revealed

For the past year, the San Jose semaphore has been broadcasting the full text of Thomas Pynchon's 1966 novel, *The Crying of Lot 49*.

Given the artwork's location (the heart of Silicon Valley) and concept (a semaphore), there was really only one logical choice for the text: Thomas Pynchon's *The Crying of Lot 49*. Although he wrote the book in the mid 1960s, Pynchon's setting is a fictional California city filled with high-tech industrial parks and the kind of engineering sub-culture that we now associate with the Silicon Valley. The book follows the heroine's discovery of latent symbols and codes embedded in this landscape and in the local culture. Is there a message here, she wonders, and what are these symbols trying to tell me? At its heart, *San Jose Semaphore* is an expression of what Pynchon calls "an intent to communicate."

The Code

There were three main principles that went into the design of the code. The first was "crackability." I wanted the code to be hard to crack, but not so hard that a dedicated, knowledgeable person (or team) could not break it within a year or two. The second principle had to do with the visual and audible design of the artwork. I wanted the nature of the code to relate to the form of the artwork (the four turning discs). The third principle was to make the code human-readable. Once its structure is revealed, the cipher can be read with the naked eye, recorded with pencil and paper, and decoded readily (if somewhat laboriously) by hand. This human-scale communication is critical to the artwork's concept.

The 256-letter Alphabet

The nature of the discs themselves dictated the "alphabet" I would use for my ciphertext. Each of the discs can assume four easily distinguishable positions: horizontal, left-leaning diagonal, vertical, and right-leaning diagonal. With these four positions, and four independent discs, the Semaphore as a whole has a total of 256 possible combinations of disc positions, or values (see Fig. 1). These 256 combinations form the alphabet for the code transmission.

0	–	–	–	–
1	–	–	–	\
2	–	–	–	|
3	–	–	–	/
4	–	–	\	–
5	–	–	\	\
6	–	–	\	|
7	–	–	\	/
8	–	–	|	–
9	–	–	|	\
10	–	–	|	|
11	–	–	|	/
12	–	–	/	–
13	–	–	/	\
14	–	–	/	|
15	–	–	/	/
16	–	\	–	–
17	–	\	–	\
18	–	\	–	|
19	–	\	–	/
20	–	\	\	–
21	–	\	\	\
22	–	\	\	|
23	–	\	\	/
24	–	\	|	–
25	–	\	|	\
26	–	\	|	|
27	–	\	|	/
28	–	\	/	–
29	–	\	/	\
30	–	\	/	|
31	–	\	/	/
32	–	|	–	–
33	–	|	–	\
34	–	|	–	|
35	–	|	–	/
36	–	|	\	–
37	–	|	\	\
38	–	|	\	|
39	–	|	\	/
40	–	|	|	–
41	–	|	|	\
42	–	|	|	|
43	–	|	|	/
44	–	|	/	–
45	–	|	/	\
46	–	|	/	|
47	–	|	/	/
48	–	/	–	–
49	–	/	–	\
50	–	/	–	|
51	–	/	–	/
52	–	/	\	–
53	–	/	\	\
54	–	/	\	|
55	–	/	\	/
56	–	/	|	–
57	–	/	|	\
58	–	/	|	|
59	–	/	|	/
60	–	/	/	–
61	–	/	/	\
62	–	/	/	|
63	–	/	/	/
64	\	–	–	–
65	\	–	–	\
66	\	–	–	|
67	\	–	–	/
68	\	–	\	–
69	\	–	\	\
70	\	–	\	|
71	\	–	\	/
72	\	–	|	–
73	\	–	|	\
74	\	–	|	|
75	\	–	|	/
76	\	–	/	–
77	\	–	/	\
78	\	–	/	|
79	\	–	/	/
80	\	\	–	–
81	\	\	–	\
82	\	\	–	|
83	\	\	–	/
84	\	\	\	–
85	\	\	\	\
86	\	\	\	|
87	\	\	\	/
88	\	\	|	–
89	\	\	|	\
90	\	\	|	|
91	\	\	|	/
92	\	\	/	–
93	\	\	/	\
94	\	\	/	|
95	\	\	/	/
96	\	|	–	–
97	\	|	–	\
98	\	|	–	|
99	\	|	–	/
100	\	|	\	–
101	\	|	\	\
102	\	|	\	|
103	\	|	\	/
104	\	|	|	–
105	\	|	|	\
106	\	|	|	|
107	\	|	|	/
108	\	|	/	–
109	\	|	/	\
110	\	|	/	|
111	\	|	/	/
112	\	/	–	–
113	\	/	–	\
114	\	/	–	|
115	\	/	–	/
116	\	/	\	–
117	\	/	\	\
118	\	/	\	|
119	\	/	\	/
120	\	/	|	–
121	\	/	|	\
122	\	/	|	|
123	\	/	|	/
124	\	/	/	–
125	\	/	/	\
126	\	/	/	|
127	\	/	/	/
128	|	–	–	–
129	|	–	–	\
130	|	–	–	|
131	|	–	–	/
132	|	–	\	–
133	|	–	\	\
134	|	–	\	|
135	|	–	\	/
136	|	–	|	–
137	|	–	|	\
138	|	–	|	|
139	|	–	|	/
140	|	–	/	–
141	|	–	/	\
142	|	–	/	|
143	|	–	/	/
144	|	\	–	–
145	|	\	–	\
146	|	\	–	|
147	|	\	–	/
148	|	\	\	–
149	|	\	\	\
150	|	\	\	|
151	|	\	\	/
152	|	\	|	–
153	|	\	|	\
154	|	\	|	|
155	|	\	|	/
156	|	\	/	–
157	|	\	/	\
158	|	\	/	|
159	|	\	/	/
160	|	|	–	–
161	|	|	–	\
162	|	|	–	|
163	|	|	–	/
164	|	|	\	–
165	|	|	\	\
166	|	|	\	|
167	|	|	\	/
168	|	|	|	–
169	|	|	|	\
170	|	|	|	|
171	|	|	|	/
172	|	|	/	–
173	|	|	/	\
174	|	|	/	|
175	|	|	/	/
176	|	/	–	–
177	|	/	–	\
178	|	/	–	|
179	|	/	–	/
180	|	/	\	–
181	|	/	\	\
182	|	/	\	|
183	|	/	\	/
184	|	/	|	–
185	|	/	|	\
186	|	/	|	|
187	|	/	|	/
188	|	/	/	–
189	|	/	/	\
190	|	/	/	|
191	|	/	/	/
192	/	–	–	–
193	/	–	–	\
194	/	–	–	|
195	/	–	–	/
196	/	–	\	–
197	/	–	\	\
198	/	–	\	|
199	/	–	\	/
200	/	–	|	–
201	/	–	|	\
202	/	–	|	|
203	/	–	|	/
204	/	–	/	–
205	/	–	/	\
206	/	–	/	|
207	/	–	/	/
208	/	\	–	–
209	/	\	–	\
210	/	\	–	|
211	/	\	–	/
212	/	\	\	–
213	/	\	\	\
214	/	\	\	|
215	/	\	\	/
216	/	\	|	–
217	/	\	|	\
218	/	\	|	|
219	/	\	|	/
220	/	\	/	–
221	/	\	/	\
222	/	\	/	|
223	/	\	/	/
224	/	|	–	–
225	/	|	–	\
226	/	|	–	|
227	/	|	–	/
228	/	|	\	–
229	/	|	\	\
230	/	|	\	|
231	/	|	\	/
232	/	|	|	–
233	/	|	|	\
234	/	|	|	|
235	/	|	|	/
236	/	|	/	–
237	/	|	/	\
238	/	|	/	|
239	/	|	/	/
240	/	/	–	–
241	/	/	–	\
242	/	/	–	|
243	/	/	–	/
244	/	/	\	–
245	/	/	\	\
246	/	/	\	|
247	/	/	\	/
248	/	/	|	–
249	/	/	|	\
250	/	/	|	|
251	/	/	|	/
252	/	/	/	–
253	/	/	/	\
254	/	/	/	|
255	/	/	/	/

Fig. 1: The Semaphore alphabet, showing all possible disc combinations and their assigned values

First Layer: Prolog

The code is designed with two layers. The first layer is called the "prolog." The prolog does not contain any actual message content, but it marks the start of each paragraph of the novel and, most important, the prolog contains the *key* to decoding the paragraph that follows.

The prolog is short, and it is always the same length (41 characters). This is in contrast to the paragraphs themselves, which vary considerably in length. The prolog always begins with the words "START MESSAGE TRANSMISSION," followed by a three digit number, a colon, and a seven-letter word. The number is the paragraph number of the text to follow, and the seven-letter word is the key for decoding that paragraph. For example, the plaintext of the prolog for paragraph 226 looks like this:

```
START MESSAGE TRANSMISSION 226:FACTION
```

("226" is the paragraph number, and "FACTION" is the key for deciphering the paragraph)

The prolog is weakly encrypted using a simple substitution cipher (see appendix). My idea was to make the prolog relatively easy to crack (at least two teams got this far), and thereby offer encouragement to anyone trying to break the code. The prolog also gives away a critical piece of information: the key to cracking the text that follows. This key is only of value, however, if the code breaker can figure out how to actually use it to decode the paragraph; revealing the key alone does not reveal this mechanism.

It is easy to identify the prolog when watching and/or listening to the Semaphore. During the transmission of paragraph content (which is most of the time), each of the Semaphore's discs spins either clockwise or counterclockwise, and there is no predictable pattern to the direction of spin. During the prolog, all the discs spin only clockwise.

Also, during paragraph transmission, a variety of pitches are used for instrumental sounds, tones and a signing voice (again, in an unpredictable pattern) to generate an unfolding melody. During the prolog, there is no variation in any of the sounds' pitches, and the melody becomes a kind of monotone chant (more details about the sound are at the end of this paper).

This combination of audible and visible markers was deigned to make the prolog easy to notice, offering a first foothold for would-be code breakers.

The Keys

The keys are seven letter words (the same number of letters as in "PYNCHON") taken in order of appearance from James Joyce's *Ulysses*. I have used text from this novel in previous artworks, and the unique (and sometimes cryptic) language seemed a good fit for this cryptographic purpose. The book is also long and filled with exotic vocabulary, and so it contains a bounty of unique seven-letter words (more than enough to provide a unique key for each paragraph). Potential keys containing the letters H, Q, or X were not used for reasons that are explained below.

Here are examples of seven-letter keys from *Ulysses:*

SINGLED	ABDOMEN	WRONGED	BRUCKEN	ORDINAL
FIGURED	MASTINO	BYGONES	INSULAR	ROMANUS
BRACING	UNSCREW	BASKING	ALIMENT	CRAWLED
ROAMING	LEVYING	DICTUMS	SOLVENT	COGNATE
CARKING	IRATELY	RACKING	DENSITY	FRONTAL
MARKING	INDULGE	LAUREIS	FAILURE	SECULAR
GUNBOAT	UMBRAGE	TOMKINS	FIRSTLY	AGONIES
LASTING	AUDIBLY	NOVELTY	TANDEMS	LOCATED
DURANCE	AROUSED	FOISTED	NEBUKIM	BREVITY
OUTLINE	CUDGELS	OBVIATE	MENDOZA	ORGANIC

I had originally planned to use key words derived directly from *The Crying of Lot 49* itself. I changed my plans, however, after I tried entering an arbitrary selection of four such words into Google, and links to *The Crying of Lot 49* came up immediately. I then realized that I would need to find keys from a different source. I knew *Ulysses* would similarly reveal itself to the code-breakers, but it seemed a worthy red-herring.

Second Layer: The Text

The second layer of the code (in which the 836 paragraphs of *The Crying of Lot 49* are actually encoded), is a variant on the classic Vigenère cipher, which was thought to be unbreakable for nearly 300 years after its publication in 1585. As described on Wikipedia:

> In the Vigenère cipher, the first row of the tableau is filled out with a copy of the plaintext alphabet, and successive rows are simply shifted one place to the left. (Such a simple tableau is called a tabula recta, and mathematically corresponds to adding the plaintext and key letters, modulo 26.) A keyword is then used to choose which ciphertext alphabet to use. Each letter of the keyword is used in turn, and then they are repeated again from the beginning. So if the keyword is 'CAT', the first letter of plaintext is enciphered under alphabet 'C', the second under 'A', the third under 'T', the fourth under 'C' again, and so on. In practice, Vigenère keys were often phrases several words long.

The Semaphore code varies from the classic Vigenère in a two ways: first, the successive rows in the table are not merely shifted, but instead are the product of a simple calculation (described below), and second, where a classic Vigenère cipher always rotates the key forward, the Semaphore code may shift the key in either direction at each step. *They key to the shift direction is hidden in the visible rotation of the discs (and in the corresponding sound).*

The direction for the next rotation of the key is encoded in the rotation of the Semaphore's third disc (the third from the left). Whenever this disc rotates clockwise, the key must be rotated forward, and when the disc rotates counterclockwise, the key must be rotated backwards.[1]

[1] In order to make frequency analysis of the ciphertext a bit more difficult, the rotation directions were generated using an algorithm that maximized the diversity of plaintext / key letter combinations.

The audio contains a parallel indicator: there are two short tones in the sequence that are in quick succession. When the third disc rotates clockwise, these tones always rise (a low tone, followed quickly by a higher one); when the third disc rotates counterclockwise, the tones fall. The tones thus redundantly encode the instruction for the key rotation.

The Key Table

The Semaphore's version of the Vigenère "tableau" is a key table (see Fig. 2) that assigns 64 possible plain text characters (26 letters, 10 numbers, plus most common punctuation, all in standard ASCII order) to the 256 possible Semaphore values based on 23 key values A through Z (H, P, and X are omitted). The ciphertext (output) values are generated by multiplying the input value by the key value, then taking MOD 256 of the result. Note that H, P, and X are not valid key values, because they end up with duplicate ciphertext entries.

		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
		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		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
2	!	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50	52
3	"	3	6	9	12	15	18	21	24	27	30	33	36	39	42	45	48	51	54	57	60	63	66	69	72	75	78
4	#	4	8	12	16	20	24	28	32	36	40	44	48	52	56	60	64	68	72	76	80	84	88	92	96	100	104
5	$	5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100	105	110	115	120	125	130
6	%	6	12	18	24	30	36	42	48	54	60	66	72	78	84	90	96	102	108	114	120	126	132	138	144	150	156
7	&	7	14	21	28	35	42	49	56	63	70	77	84	91	98	105	112	119	126	133	140	147	154	161	168	175	182
8		8	16	24	32	40	48	56	64	72	80	88	96	104	112	120	128	136	144	152	160	168	176	184	192	200	208
9	(	9	18	27	36	45	54	63	72	81	90	99	108	117	126	135	144	153	162	171	180	189	198	207	216	225	234
10	)	10	20	30	40	50	60	70	80	90	100	110	120	130	140	150	160	170	180	190	200	210	220	230	240	250	4
11	*	11	22	33	44	55	66	77	88	99	110	121	132	143	154	165	176	187	198	209	220	231	242	253	8	19	30
12	+	12	24	36	48	60	72	84	96	108	120	132	144	156	168	180	192	204	216	228	240	252	8	20	32	44	56
13	,	13	26	39	52	65	78	91	104	117	130	143	156	169	182	195	208	221	234	247	4	17	30	43	56	69	82
14	-	14	28	42	56	70	84	98	112	126	140	154	168	182	196	210	224	238	252	10	24	38	52	66	80	94	108
15	.	15	30	45	60	75	90	105	120	135	150	165	180	195	210	225	240	255	14	29	44	59	74	89	104	119	134
16	/	16	32	48	64	80	96	112	128	144	160	176	192	208	224	240	0	16	32	48	64	80	96	112	128	144	160
17	0	17	34	51	68	85	102	119	136	153	170	187	204	221	238	255	16	33	50	67	84	101	118	135	152	169	186
18	1	18	36	54	72	90	108	126	144	162	180	198	216	234	252	14	32	50	68	86	104	122	140	158	176	194	212
19	2	19	38	57	76	95	114	133	152	171	190	209	228	247	10	29	48	67	86	105	124	143	162	181	200	219	238
20	3	20	40	60	80	100	120	140	160	180	200	220	240	4	24	44	64	84	104	124	144	164	184	204	224	244	8
21	4	21	42	63	84	105	126	147	168	189	210	231	252	17	38	59	80	101	122	143	164	185	206	227	248	13	34
22	5	22	44	66	88	110	132	154	176	198	220	242	8	30	52	74	96	118	140	162	184	206	228	250	16	38	60
23	6	23	46	69	92	115	138	161	184	207	230	253	20	43	66	89	112	135	158	181	204	227	250	17	40	63	86
24	7	24	48	72	96	120	144	168	192	216	240	8	32	56	80	104	128	152	176	200	224	248	16	40	64	88	112
25	8	25	50	75	100	125	150	175	200	225	250	19	44	69	94	119	144	169	194	219	244	13	38	63	88	113	138
26	9	26	52	78	104	130	156	182	208	234	4	30	56	82	108	134	160	186	212	238	8	34	60	86	112	138	164
27	:	27	54	81	108	135	162	189	216	243	14	41	68	95	122	149	176	203	230	1	28	55	82	109	136	163	190
28	;	28	56	84	112	140	168	196	224	252	24	52	80	108	136	164	192	220	248	20	48	76	104	132	160	188	216
29	<	29	58	87	116	145	174	203	232	5	34	63	92	121	150	179	208	237	10	39	68	97	126	155	184	213	242
30	=	30	60	90	120	150	180	210	240	14	44	74	104	134	164	194	224	254	28	58	88	118	148	178	208	238	12
31	>	31	62	93	124	155	186	217	248	23	54	85	116	147	178	209	240	15	46	77	108	139	170	201	232	7	38
32	?	32	64	96	128	160	192	224	0	32	64	96	128	160	192	224	0	32	64	96	128	160	192	224	0	32	64
33	@	33	66	99	132	165	198	231	8	41	74	107	140	173	206	239	16	49	82	115	148	181	214	247	24	57	90
34	A	34	68	102	136	170	204	238	16	50	84	118	152	186	220	254	32	66	100	134	168	202	236	14	48	82	116
35	B	35	70	105	140	175	210	245	24	59	94	129	164	199	234	13	48	83	118	153	188	223	2	37	72	107	142
36	C	36	72	108	144	180	216	252	32	68	104	140	176	212	248	28	64	100	136	172	208	244	24	60	96	132	168
37	D	37	74	111	148	185	222	3	40	77	114	151	188	225	6	43	80	117	154	191	228	9	46	83	120	157	194
38	E	38	76	114	152	190	228	10	48	86	124	162	200	238	20	58	96	134	172	210	248	30	68	106	144	182	220
39	F	39	78	117	156	195	234	17	56	95	134	173	212	251	34	73	112	151	190	229	12	51	90	129	168	207	246
40	G	40	80	120	160	200	240	24	64	104	144	184	224	8	48	88	128	168	208	248	32	72	112	152	192	232	16
41	H	41	82	123	164	205	246	31	72	113	154	195	236	21	62	103	144	185	226	11	52	93	134	175	216	1	42
42	I	42	84	126	168	210	252	38	80	122	164	206	248	34	76	118	160	202	244	30	72	114	156	198	240	26	68
43	J	43	86	129	172	215	2	45	88	131	174	217	4	47	90	133	176	219	6	49	92	135	178	221	8	51	94
44	K	44	88	132	176	220	8	52	96	140	184	228	16	60	104	148	192	236	24	68	112	156	200	244	32	76	120
45	L	45	90	135	180	225	14	59	104	149	194	239	28	73	118	163	208	253	42	87	132	177	222	11	56	101	146
46	M	46	92	138	184	230	20	66	112	158	204	250	40	86	132	178	224	14	60	106	152	198	244	34	80	126	172
47	N	47	94	141	188	235	26	73	120	167	214	5	52	99	146	193	240	31	78	125	172	219	10	57	104	151	198
48	O	48	96	144	192	240	32	80	128	176	224	16	64	112	160	208	0	48	96	144	192	240	32	80	128	176	224
49	P	49	98	147	196	245	38	87	136	185	234	27	76	125	174	223	16	65	114	163	212	5	54	103	152	201	250
50	Q	50	100	150	200	250	44	94	144	194	244	38	88	138	188	238	32	82	132	182	232	26	76	126	176	226	20
51	R	51	102	153	204	255	50	101	152	203	254	49	100	151	202	253	48	99	150	201	252	47	98	149	200	251	46
52	S	52	104	156	208	4	56	108	160	212	8	60	112	164	216	12	64	116	168	220	16	68	120	172	224	20	72
53	T	53	106	159	212	9	62	115	168	221	18	71	124	177	230	27	80	133	186	239	36	89	142	195	248	45	98
54	U	54	108	162	216	14	68	122	176	230	28	82	136	190	244	42	96	150	204	2	56	110	164	218	16	70	124
55	V	55	110	165	220	19	74	129	184	239	38	93	148	203	2	57	112	167	222	21	76	131	186	241	40	95	150
56	W	56	112	168	224	24	80	136	192	248	48	104	160	216	16	72	128	184	240	40	96	152	208	8	64	120	176
57	X	57	114	171	228	29	86	143	200	1	58	115	172	229	30	87	144	201	2	59	116	173	230	31	88	145	202
58	Y	58	116	174	232	34	92	150	208	10	68	126	184	242	44	102	160	218	20	78	136	194	252	54	112	170	228
59	Z	59	118	177	236	39	98	157	216	19	78	137	196	255	58	117	176	235	38	97	156	215	18	77	136	195	254
60	[	60	120	180	240	44	104	164	224	28	88	148	208	12	72	132	192	252	56	116	176	236	40	100	160	220	24
61	\	61	122	183	244	49	110	171	232	37	98	159	220	25	86	147	208	13	74	135	196	1	62	123	184	245	50
62	]	62	124	186	248	54	116	178	240	46	108	170	232	38	100	162	224	30	92	154	216	22	84	146	208	14	76
63	^	63	126	189	252	59	122	185	248	55	118	181	244	51	114	177	240	47	110	173	236	43	106	169	232	39	102
64	_	64	128	192	0	64	128	192	0	64	128	192	0	64	128	192	0	64	128	192	0	64	128	192	0	64	128

Fig. 2: The Semaphore's Vigenère "square" (key table). Plain text (input) values are shown at left in yellow, and key values are shown across the top, also in yellow.

I chose this scheme as a way to expand my 64-character plaintext alphabet (26 letters, 10 numbers, and assorted punctuation) to use the entire 256-member Semaphore alphabet, ensuring that there would be as much visual variety as possible in the movement of the discs.

The Soundtrack

In addition to its aesthetic value, the soundtrack adds a redundant means of receiving the code transmission. The Semaphore is designed so that the code can be fully transmitted (and cracked) based solely on the visible movements, or solely on the sound — all the critical information is fully represented in each modality.

The voices communicate the positions of the discs when they come to rest. The first voice, a distant spoken voice, speaks a letter of the NATO phonetic alphabet (Alfa, Bravo, Charlie up through the alphabet to Papa), and the second voice sings a number between one and sixteen. The first voice indicates the positions of the leftmost pair of discs, and the second voice indicates the positions for the rightmost pair. Each letter or number corresponds to a unique combination of positions as shown in the table below (Fig. 3).

SPOKEN	SUNG		
ALFA	ONE	–	–
BRAVO	TWO	–	\
CHARLIE	THREE	–	|
DELTA	FOUR	–	/
ECHO	FIVE	\	–
FOXTROT	SIX	\	\
GOLF	SEVEN	\	|
HOTEL	EIGHT	\	/
INDIA	NINE	|	–
JULIET	TEN	|	\
KILO	ELEVEN	|	|
LIMA	TWELVE	|	/
MIKE	THIRTEEN	/	–
NOVEMBER	FOURTEEN	/	\
OSCAR	FIFTEEN	/	|
PAPA	SIXTEEN	/	/

Fig. 3: The key to decoding the voices

As discussed above, two of the tonal sounds in the soundtrack provide a redundant indication of the spin direction for the third disc (and hence, provide parallel instructions for rotating the substitution key). The other sounds, like the spin directions of the other three discs, are purely ornamental.

The aesthetic of the soundtrack is based on my childhood memories of listening to the shortwave radio; for me, they evoke the mysterious cold-war "numbers stations" broadcasts, as well as the regular pulsing rhythm of National Bureau of Standards' Atomic Clock.

APPENDIX: The simple substitution cipher used for the prolog

<table>
<tr><th>SEMAPHORE</th><th>PLAINTEXT</th></tr>
<tr><td>- - - -</td><td></td></tr>
<tr><td>/ - \ -</td><td>!</td></tr>
<tr><td>| - | -</td><td>"</td></tr>
<tr><td>\ - / -</td><td>#</td></tr>
<tr><td>- \ - -</td><td>$</td></tr>
<tr><td>/ \ \ -</td><td>%</td></tr>
<tr><td>| \ | -</td><td>&</td></tr>
<tr><td>\ \ / -</td><td></td></tr>
<tr><td>- | - -</td><td>(</td></tr>
<tr><td>/ | \ -</td><td>)</td></tr>
<tr><td>| | | -</td><td>*</td></tr>
<tr><td>\ | / -</td><td>+</td></tr>
<tr><td>- / - -</td><td>,</td></tr>
<tr><td>/ / \ -</td><td>-</td></tr>
<tr><td>| / | -</td><td>.</td></tr>
<tr><td>\ / / -</td><td>/</td></tr>
<tr><td>\ - - -</td><td>0</td></tr>
<tr><td>- - \ -</td><td>1</td></tr>
<tr><td>/ - | -</td><td>2</td></tr>
<tr><td>| - / -</td><td>3</td></tr>
<tr><td>\ \ - -</td><td>4</td></tr>
<tr><td>- \ \ -</td><td>5</td></tr>
<tr><td>/ \ | -</td><td>6</td></tr>
<tr><td>| \ / -</td><td>7</td></tr>
<tr><td>\ | - -</td><td>8</td></tr>
<tr><td>- | \ -</td><td>9</td></tr>
<tr><td>/ | | -</td><td>:</td></tr>
<tr><td>| | / -</td><td>;</td></tr>
<tr><td>\ / - -</td><td><</td></tr>
<tr><td>- / \ -</td><td>=</td></tr>
<tr><td>/ / | -</td><td>></td></tr>
<tr><td>| / / -</td><td>?</td></tr>
</table>

<table>
<tr><th>SEMAPHORE</th><th>PLAINTEXT</th></tr>
<tr><td>| - - -</td><td>@</td></tr>
<tr><td>\ - \ -</td><td>A</td></tr>
<tr><td>- - | -</td><td>B</td></tr>
<tr><td>/ - / -</td><td>C</td></tr>
<tr><td>| \ - -</td><td>D</td></tr>
<tr><td>\ \ \ -</td><td>E</td></tr>
<tr><td>- \ | -</td><td>F</td></tr>
<tr><td>/ \ / -</td><td>G</td></tr>
<tr><td>| | - -</td><td>H</td></tr>
<tr><td>\ | \ -</td><td>I</td></tr>
<tr><td>- | | -</td><td>J</td></tr>
<tr><td>/ | / -</td><td>K</td></tr>
<tr><td>| / - -</td><td>L</td></tr>
<tr><td>\ / \ -</td><td>M</td></tr>
<tr><td>- / | -</td><td>N</td></tr>
<tr><td>/ / / -</td><td>O</td></tr>
<tr><td>/ - - -</td><td>P</td></tr>
<tr><td>| - \ -</td><td>Q</td></tr>
<tr><td>\ - | -</td><td>R</td></tr>
<tr><td>- - / -</td><td>S</td></tr>
<tr><td>/ \ - -</td><td>T</td></tr>
<tr><td>| \ \ -</td><td>U</td></tr>
<tr><td>\ \ | -</td><td>V</td></tr>
<tr><td>- \ / -</td><td>W</td></tr>
<tr><td>/ | - -</td><td>X</td></tr>
<tr><td>| | \ -</td><td>Y</td></tr>
<tr><td>\ | | -</td><td>Z</td></tr>
<tr><td>- | / -</td><td>[</td></tr>
<tr><td>/ / - -</td><td>\</td></tr>
<tr><td>| / \ -</td><td>]</td></tr>
<tr><td>\ / | -</td><td>^</td></tr>
<tr><td>- / / -</td><td>_</td></tr>
</table>