Decoding Chaocipher Exhibits 2 & 3

Esa Peuha

The National Cryptologic Museum has several documents related to Chaocipher available for download. One of these is [1] which has six pages; the first five pages contain Byrne's encryption of the Exhibit 2 in *Silent Years*, while the last page is a typewritten copy of [3].

On the left edge of the first page, written vertically, is the string

`SIVALESBENEESTW`

with red and blue indicating

`RLRLLRRLLRRLRLR`

and below it

`HWUOAOAFXTJBISV`

If we treated this as a keyphrase in the same way as the keywords of Exhibits 1 and 4, we should be able to start with straight alphabets on the wheels, properly aligned, and then encode

`HIUALOABETJEITV`
`SWVOAESFXNEBSSW`

Unfortunately, encoding the first pair `HS` results in a configuration where the next pair `IW` is not aligned. (Encoding `WI` or `IV` would allow to encode five more pairs, but not `BF`.) However, at the bottom of the first page there are instructions:

Letter S up on right wheel
no 9 " " left "
Then make circular and cascade movements } this also after every group of 52

The 9th letter of the alphabet is not `H` but `I`, and aligning `IS` on straight alphabets lets us encode

`I HIUALOABETJEITV TLXWFWYHBICOJSPURTJMFDKTJBFAEFGBRJOSISVKRGRPKOKXZQBX`
`S SWVOAESFXNEBSSW GALLIAESTOMNISDIVISAINPARTESTRESWWWHORUMOMNIUMFORTIS`

that is, the entire keyphrase and the first 52 ciphertext/plaintext pairs.

From this point forward, the encryption method is no longer true Chaocipher. While Byrne still followed the basic procedure, he ceased to permute the alphabets by taking out letters and inserting them at nadir; he merely rotated the wheels one step relative to each other after encrypting every plaintext letter. The only complication left is that he switched alphabets after every 52 letters, and even that is quite straightforward: with the wheels as they are after the first 52 letters, encode

`DEMSXBWURHTMXV`
`SIVALESBENEEST`

with Chaocipher, record the wheel configuration as #1, encode

`F`
`W`

still with Chaocipher, and record the wheels as #2. (These are from [2] line 1.) Restore the wheels to configuration #1, rotate to match [3] line 1, rotate again to encode

`HSYNZRXDYXZDXBDAGALVCYGCMX ODACULTUATQUEHUMANITATEPRO`
`SIMISUNTBELGAEYPROPTEREAQU EQISZITMNICJQHQXJJUMSAGESX`

with the simple method, restore the wheels to #2, encode

`SIVALESBENEEST`
`CRGWCNJGKHDICG`

with Chaocipher, record the wheels as #3, encode

`W`
`R`

still with Chaocipher, and record the wheels as #4. (These are from [2] line 2.) Restore the wheels to #3, rotate to match [3] line 2, rotate again to encode

```
VINCIAELONGISSIMEABSUNTYMI AECLAKDWJBHBSJDWRQOPHUHPFG
WFJUAKJWUREKMUIXYMFAJCVURV NIMEQUEADEOSMERCATORESSAEP
```

with the simple method, restore the wheels to #4, and so on until near the end; after encoding

```
POWRRNGLFSFJLTBCSCSUOZNZNW PULOSTOTIUSGALLIAESESEPOTI
TENTISSIMOSACFIRMISSIMOSPO TQSBECOEVXFIJWEQSXSFYNSQRF
```

with the simple method, proceed directly to encode

```
SIVALESBENEEST
QNTUYIZMLYGKJA
```

with Chaocipher, rotate to match [3] line 24, rotate again to encode

```
RIPOSSESPERANTW
JPINAPKGFNOJCRK
```

with the simple method, and that is it. Note that the manner in which Byrne rotated the wheels before he recorded them in [3] appears to be completely random; in contrast, the second rotation before using them for encryption is deterministic, as the `S` on the right wheel must coincide with whatever letter happens to be in position 8 on the left wheel in [3]. (It is unclear why this is 8 instead of 9 as might be thought based on his instructions; possibly his intention was to encrypt an extra `S` on the right wheel before the plaintext, like he did at the beginning before the keyphrase, but this is not needed with the simple method.) Note also that on odd numbered lines, the first group of 26 letters of plaintext is on the right wheel while the second is on the left; on even numbered lines these are reversed. These are indicated by an `L` or an `R` on the right margin. Similarly, an `L` or an `R` on the left margin in [2] indicates the wheel for the keyphrase.

Knowing the method of encryption makes it clear that Byrne made four errors, present both on the worksheets and in *Silent Years*; these are harmless, because with his simplified method (unlike full Chaocipher) they do not affect the encryption of any other letters. Nevertheless, here is a list of them:

line	group	printed	correct
5	11	DOIIU	DEIIU
10	1	WODHB	WOTHB
12	10	NASLV	NASLM
23	2	UOZJZ	UOZNZ

What about Exhibit 3? It turns out that none of it is proper Chaocipher; all of it is encrypted with the simplified method that Byrne used in most of Exhibit 2. The keyphrase for deriving the alphabets is

```
COMPREHENSIBLE
```

with disk pattern

```
LRRLLRRLRRRLLR
```

which are referred to in [4], page 332, footnote 8. Starting with straight alphabets on the wheels, encode

```
CNKPRDBEGHZBLH
COMRVEHLNSINIE
```

with actual Chaocipher, rotate the wheels relative to each other so that `T` on the left wheel matches `O` on the right wheel, and encode

```
THEHISTORYOFWARTEEMSWITHOC DQWOCPRIWFLQXQPBGRNSJKZYRH
ODHSTOCOCPBHRSLTANURICIAVZ CASIONSWHERETHEINTERCEPTIO
```

with the simple method. Not knowing the other alphabets, the rest of the lines cannot be verified directly, but it is still possible to proceed. First there are a few errors:

line	column	printed	correct
21	11	RZTIS	RZRIS
22	23	ABJZV	ABBZV
30	22	GQYPW	GQBPW

All of these errors are present both in *Silent Years* and in [5]. After these corrections, it is a simple matter to find alphabets that match the remaining text, assuming that it was encrypted with the same method; this makes it almost certain that it is the method actually used to encrypt the text, instead of real Chaocipher or some other method Byrne might have known. However, these alphabets are necessarily incomplete, because not all letters are present; not unique, because (in addition to missing letters) some

letters can be placed in more than one position; and possibly slightly wrong, because there could be errors that only affect the placement of one or two letters. For these reasons, the alphabets should be regarded with some caution, but here they are anyway:

```
XBPSUC.QVRFLHWO.EDGIT.NA..
BAFDVCWEK.LIQ.NPTSX.GZHOR.

HXDEBN.T.VRFL.SJ.P.IMAK...
JW..NLIBTY.MV.SEXUGHORADF.

.HLYVJOS.MPGC.RWF.X.EBINAT
EULORM...JSWZNGATH...YX.KC

ENAPKWT.XH.BS.OGUICR.ZLDVJ
DTIB..K.CG.ELRQXFPV.SWONHA

ENV.AI.F.H.L.SOGMUTPCRXYZD
.GMDNBLHA.YFPKVSWEORTIXJZU

DLGNSMI.X.ZHEU.OJAT.CFWRQV
EAHY.MC.KN.W.OR.QTUI...SGB

ERQNVLGSY.D..OJAMI.PT.HCWF
.W.OTHERQF.KZLVSBXUAIM.YC.

AGM..PY.HF.ETLSD.UWR..N.IO
N.DSX.TH.ERP.ZBGWILVA.Q...

HN.OTILA.G.PYKFESC.UWRJZBV
TDI.O.ERB..LV.AUQMP..FSN.C

U.RMBVH.KSXTC.AWJ.GYZPN.OE
TMXOP.RJW.CY.AUQEHLBKFNSZI

SXTRECADY...PNOULWIM..GQHF
EP..FZIWATM.OLHRG.SCNVYD.Q

CIDJ..Z.GQX.U.POLWE.HSNTRA
ATD.XLH.CMN.YOURE.WS.JBIKF

EMFS.TRKCD.LHWBYN.GQVUA.PO
VOSRZXWJF.B.IUATPE...HGCKN

OWIPFBYNKQV.AH.EMS.ZGTRCJ.
EF.CHDQGIAK.SRJZWL...NMOTP

HF.TJRCPS.Y..NKGQ.OLEWUIBA
SRLY.KUCOTJPQ.ZFXBHDNGIA.E

DTRSW.PU.I..BG.FJVXO.CEAN.
FXBHGIA.M.UCOVT.JSEYNQRWZ.

.GKRQXJ..YP.......SL.V.E.N
E.B.A...M.O.....NH..C.T...
```

References:

[1] http://www.nsa.gov/about/_files/cryptologic_heritage/museum/library/chaocipher_2_and_si_vales.pdf
[2] "Exhibit 2 Working Draft A" by email from Moshe Rubin
[3] "Exhibit 2 Working Draft B" by email from Moshe Rubin
[4] Moshe Rubin (2011) "John F. Byrne's Chaocipher Revealed: An Historical and Technical Appraisal", Cryptologia, 35:4, 328-379, DOI: 10.1080/01611194.2011.606751
downloadable from http://www.tandfonline.com/doi/abs/10.1080/01611194.2011.606751
[5] "Exhibit 3 Encipherment Grids" by email from Moshe Rubin