THE MACBETH TEST MESSAGE

David Shulman

Many years ago, my friend Max Katz called my attention to an unsolved cipher in the English translation by J. C. H. Macbeth of André Langie's *Cryptography,* (London, 1922). Katz was a member of the American Cryptogram Association with the nom de plume of DIRIGO, a president of The Society of American Magicians, and the author of a column on ciphers, *The Black Chamber,* for a detective story magazine. He told me that so far as he knew this problem had not been solved, and that he had written for the solution as promised in the book. After receiving it, he informed me that the cipher was a form of Playfair. Errors in it accounted for it not being solved.

Actually, I never saw the solution and I never heard any more about it. In my bibliography, *An Annotated Bibliography of Cryptography* (New York: Garland Publishing Co., 1976), p. 86, I wrote: "See p. 190-92 for message in cipher system proposed by Macbeth. The solution was published separately and disclosed a two-step cipher based upon a Playfair providing a rather cumbersome system which is no harder to solve than a Playfair in actual practice once the system is known."

Recently, I acquired a copy of the Langie-Macbeth book which unlike other copies that I have or have seen has the printed solution tipped in. Evidently, a previous owner of this copy wrote for the solution which the translator had then promised. Since this book is no longer available from Macbeth or the publisher after so many years, it is fortunate that the owner here had the sense and time to provide it with his copy of the book. I acquired the book from the widow of Erwin Newman (Dr. CRYPTOGRAM of the American Cryptogram Association), who in turn had obtained the book from the excellent collection of the late Henry E. Langen (HELCRYPT of the American Cryptogram Association).

Macbeth made some changes in the text of the original French when he translated it and finally embellished the work with his test message. I doubt if André Langie ever knew about it, as Langie seemed to delight in solving unknown ciphers, judging from his own interesting book. Before presenting his test message, Macbeth preceded it with a chapter in which he shows his predilection for the Playfair cipher together with an analysis of its solution by Lt. Cmdr. W. W. Smith of the U. S. Navy. He then proceeds to give his test message. While he did not indicate what kind of system he had employed, his strong devotion to the Playfair should have been a clue that he was using some form of it in his test.

Here is the rather lengthy test message using 1,424 letters as it appeared in the book:

```
KOTDRIQU GHNAZAJG BUPBRGID
DEZXFNOK KWITIBMD ASJYZNFE
NXDWIMCG KOWTFXEN ZYHDRAJX
KLWOCMTU ZECWTGOS JHPUDFND
CLIMJDTO LBVCUSUD QAWMWXEK
LOBLNEKU VJGSITVA HBARDTUZ
SEWQVAVL DUNCDLOX DFBYRGPG
BNEZVCPA VFEBNJCU FGXAPMOQ
AXRNYFLZ EQBUNCSI JKSULVQF
YCFHGUVG RSEWLFAJ AVJBOKYM
CRULMXJO ZTCBATRL UBACRTIM
WFCGGIFXO ZCZLEGLM YZFIGLAS
STUDKVYN PSOJLCDE SFSWOTKM
FXCIBSGE NCDLIWDX OTLDNAJT
SEPFLICH CLATCNDU FRLJYDAJ
EXTASWEL TZUKBPFA RZLJOQUV
VARHITVO SRCWICHB YRTEDOQU
JAXGPBYN CTREZCVJ AKJMBOVQ
ODMBYCXZ DARVKINM CMEZLTVY
LUKRXJEP LUCKMRIG FEZJFMOT
KLAZHZYG VIRVDUXC JFANFESG
RSHNYSPY NCHUVEQR JTOFTSAR
WMYCHKBE ZBUTSUCR LJAFYBLS
YCHLBYVW ONDEJSQF ILMERJVU
PITVHCYZ NEFCTOGK BMURTLIS
CATGLSET CLYRTOCL HDIVSAQM
MDESMACK VYCFLNOL BUVLBNIG
CDSYFLON LCXODIGF HROBETZC
ICERHBYB NHOXDLJU GHVDANCD
NVJAXVWY
```

```
BNHGYKZJ ELKOCWVD ARBGEXDZ
KLVEDEST ABLNYVSG VIWCOCRP
DZRKICXF YTANBECB ZBEWGBHI
GFIDWTCO WCWLADXE RYNQGXYJ
YVPJEGFA BLXUBNQC EXLGAPHI
HICKDROQ UZXHVEFG DQYNZNYW
SBKEQHJK ORLVDICM GIWFYKNJ
EBIZSOBQ SDATWRAL HVISTVAL
CAXSDPED RSBIXFEG YPTAHQPL
OPHYXHEJ ACBNUMOF VRDIRTLZ
SOBLJGET EDRXLAVB ICSZFEDL
FXEZEKLJ UTKYBSEN DNJOCKLA
TJEHSQLO WVFRUGUT REHXZBIT
ABEDZFYT SJUJGADV XFOBGHIZ
SJETVTYD VLHYZBUK BRAVENHL
CRDYFEZF ICJTFOVS ATLFINCK
SFTYZCBE DLTEMRGU KCSJAWEN
DRZLUSIX PEQCFAGF JEFGUDZW
EMNYCHCR IVTBIZBC MEQMYWLF
NTEFTRYD XPMAQBML ONBPANCZ
RJPARXEW DCYVSOSB MLIVCHUB
HLOCKLJE RTCLOCHZ AMUKRXLI
QUDCAKNS CYLABRFO JDSEXVYX
CUMKJOKS LASPBIQZ EVLJMANZ
WLFSONFR GICLMDUG HSAKAVZC
TLXINVHM EPZLFURS QUCKIBNX
UCNZLYDF ALKDENKI SCLURZUL
OTRIWVAV YCANTEDP XDUZVNIL
RABMVUCL FYRLGEXV ROFUGALN
VUKLXUDI FQRBONCD PECORXEL
```

The solution as provided by Macbeth follows:

COPY OF TEST CIPHER PUBLISHED IN ENGLISH TRANSLATION OF
CRYPTOGRAPHY BY LANGIE

Enciphered first by the Playfair system, the key-word being "J. Macbeth" in the first and fifth lines of the square. The resulting cipher was then transposed into the Continental Morse Code, the dots being represented by the first ten consonants (B to M), and the dashes by means of the last ten consonants (N to Z). The six vowels, A E I O U, are used for spacing.

Blank. If you wish to propound a good cryptogram, you should avoid as much as you possibly can duplication of words or portions of words. Stop. This is a thoroughly sound maxim, and adoption of this plan will wondrously add to difficulty of solution, without in any way impairing accuracy or sacrificing clarity. Stop. If you cannot avoid duplication always try to vary translation and find substitutions as shown in this illustration.

I(J)	M	A	C	B
D	F	G	K	L
N	O	P	Q	R
S	U	V	W	X
E	T	H	Y	Z

Bl an ki fy ou wi sh to pr op ou nd ag oz od cr yp to gr am yo us ho ul
LR IP DC KT UT SC VE MU QN PQ UT SN GP RT NF BQ HQ MU LP CA TQ VU TP XF

da vo id as mu ch as yo up os zs ib ly ca nd up li ca ti on of wo rd so
GI UP DN IV FT AY IV TQ VO NU EX MI KZ BC SN VO DB BC EM PO UO UQ NL UN

rp or ti on so fw or ds st op Th is is at ho ro ug hl ys ou nd ma xi ma
NQ PN EM PO UN KU PN NE UE PQ HY DE DE MH TP NP VF ZG EW UT SN AC SB AC

nd ad op ti on of th is pl an wi lz lw on dr ou sl ya dz dt od if fi cu
SN IG PQ EM PO UO HY DE RG IP SC RB KX PO LN UT XD HC LE FE NF MD DM MW

lt yo fs ol ut io nw it ho ut in an yw ay im pa ir in ga cz cu ra cy or
FZ TQ DU RF TM NM QS ME TP TM DS IP CY CH MA VA BN DS PG BY MW PB KC PN

sa cr if ic in gc la ri ty st op if yo uc an zn ot av oi dz du pl ic at
VI BQ MD MB DS KA GB NB HZ UE PQ MD TQ WM IP ER UM GH NM LE FS RG MB MH

io na lw ay st ry to va ry tr an sl at io na nd fi nd su bs ti tu ti on
MN OI KX CH UE QZ MU HG QZ ZO IP XD MH MN PI SN DM SN UV IX EM MT EM PO

sa sz sh ow ni nt hi si lz lu st ra ti on
VI XE VE QU SD OE EA ED RB FX UE PB EM PO

After using the Playfair cipher for encipherment, Macbeth then used the Continental Morse Code to obtain the final cipher text. In order to clarify his procedure, let us consider each actual step with enough of the beginning of the message to illustrate without the tedious entire text.

Here is the alphabet of the Morse Code:

A	. -	N	- .
B	- . . .	O	- - -
C	- . - .	P	. - - .
D	- . .	Q	- - . -
E	.	R	. - .
F	. . - .	S	. . .
G	- - .	T	-
H	. . . .	U	. . -
I	. .	V	. . . -
J	. - - -	W	. - -
K	- . -	X	- . . -
L	. - . .	Y	- . - -
M	- -	Z	- - . .

The encipherment of the plaintext using the given Macbeth Playfair square starts as follows :

```
BL AN KI FY ..... plain
LR IP DC KT ..... cipher.
```

The conversion to the Morse code and the final cipher text is the next step:

```
L          R          cipher 1
. - . .    . - . .    code
B N H G Y  K Z J E    cipher 2
```

Decipherment, of course, is a reverse process. The first two groups of the cipher message are deciphered:

```
B N H G Y K Z J E L K O C W V D    cipher 2
. - . .   . - .   . .   . - - .    code
L         R       I     P          cipher 1
```

This explanation should now make the modus operandi of the Macbeth cipher clearer. As stated previously, one should have suspected that the challenge was a Playfair and even suspected the use of the Morse code, because Macbeth indicated in his mailing address that he was associated with the Marconi International Code Corporation.

The system was original with Macbeth. In the section on fractionated ciphers in *Elementary Cryptanalysis,* at page 209, Helen Gaines does not include this type. Nor does the latest index to *The Cryptogram,* July-August 1978, under Morse code. The method of concealing the Playfair cipher text in the second step of this two-step cipher is clever. The choice of any letter from one group of ten to represent a dot and any one from another group of ten to stand for a dash and the use of a choice of A, E, I, O, U, or Y for the spaces between letters destroys the characteristics by which a Playfair cipher can be recognized.

In my opinion this system provides a good example of an unbreakable cipher unless one suspects Playfair and Morse code and fortuitously tries for such a solution.

Its disadvantage is that it is a two-step cipher requiring extra time in encipherment and decipherment which makes it cumbersome and that errors with dots and dashes and the choice of letters automatically lead to further errors in the text if not detected at their initial points. As problems in the

exercise of one's skill, messages in the Macbeth system should be intriguing, but for practical purposes, the system is unsuitable, unless mechanised or programmed on a computer.

Macbeth himself states in his translation of Langie, p. 192: "I should hesitate to say that a cryptogram can be invented that will defy solution, provided it is of reasonable length and is not so involved and intricate as to make its use inexpedient. For practical purposes a cipher should be based upon some system which can be easily committed to memory, and it should not involve any great expenditure of time in coding messages."

Macbeth hoped that his system would qualify. If it has not succeeded, it turns out to be a good attempt. However, he is not alone in attempts to frustrate the cryptanalyst with unsolvable cipher systems.