SIGHT-READING SUBSTITUTION CIPHERS

JEAN C. SABINE
Belmont, California

The usual procedure when trying one's hand at a new craft is to undergo some kind of indoctrination before taking any action. The purpose of this article is to invite the reader, if he has little or no acquaintance with cryptography, to explore the potential of knowledge already in his possession. Instant linguistic recreation will result.

Of the many types of ciphers, simple substitution is the most amenable to a linguistic attack. The others are primarily in the field of recreational geometrics. Simple substitution is by definition a method of encipherment whereby each letter of the alphabet is replaced by one and only one other letter, and is never represented by itself. No punctuation is preserved. Proper names are indicated by an asterisk preceding the enciphered form of the name.

With this definition in mind, the reader is urged to examine Example 1 quite thoroughly before reading the account of its solution which follows.

All examples are from The Cryptogram, the official publication of the American Cryptogram Association, and are reproduced here with the kind permission of the editors and publishers. (For subscription details, write Eugene Rogot, 9504 Forest Road, Bethesda, Maryland 20014.)

Example 1 August/September 1954 (A-1), by W. Charles Bell III

YDI LPM EDQ TWFIX YDPY YDI EDQKI EQWKH FX APH MINIW DPH P KFYYKI TDFKH YDWQE FYX PWLX PWQZMH DFX MITJ.

For present purposes, sight-reading may be defined as decipherment without analysis and, ideally, without recourse to an eraser. There are many clues in Example 1, and possible decipherments can be tested mentally against other parts of the message until it is clear that a start free of conflicts has been made. The following account was copied from notes made during the actual solution, amplified to explain the sequence of steps. Note-taking is not properly a part of sight-reading, and was done to ensure accurate reporting of the examples chosen as illustrations.

1. Considering P KFYYKI: P = a or I (with no punctuation to set it

off, the vocative o is ruled out). If P = a, then YDPY YDI could be that the. Testing this against P KFYYKI: this becomes a KFttKe (K representing a repeated letter). Between tt and e the most likely letter is l, and a little is almost certainly correct.

2. Six identifications have now been made: Y = t, D = h, I = e, P = a, K = l, and F = i. To test further: DPH = haH. Preceding a little, has or had is satisfactory. Two words end in KH, for which ls and ld are both acceptable. Noting FX, FYX, and DFX: these are deciphered iX, itX, and hiX. The repeated letter is s, so X = s and H = d.

3. Noting EDQ and EDQKI EQWKH: these are deciphered EhQ and EhQle EQWld. EDQ cannot be the or she (these letters have already been used) but it could be who or why. E = w and Q = o gives whole woWld, so W = either r or u.

4. Considering YDWQE: this is deciphered thWow, so W = r. This is ample to ensure the solution: the man who cries that the whole world is bad never had a little child throw its arms around his neck.

The second example is somewhat more difficult, as indicated by the fact that the editor of The Cryptogram placed it tenth in the customary series of 25 problems in simple substitution. Nevertheless, it was sight-read with little difficulty.

Example 2 August/September 1952 (A-10), author unknown

*XHPFVTPAP: WCMT *POFVR *'XHPYFVTPAZ', CMFFVE FCHEU, JMCS HDVS QN FYV *TVKZRPE *ZESZPED JYM PRRMTLPEZVS *LVSCM SV *PAIPCPSM ZE YZD VKLAMCPFZME MW *RVEFCPA *PTVCZRP, WCMT YPIZEX VERMHEFVCVS P SVPS JMCT-VPFVE FCVV EVPC FYV LPAPRV MW FYV UZEXD.

Proper names are of dubious value as entries, since they have so many linguistic origins. Example 2 was solved by the following steps:

1. Considering P SVPS: it is easier to test P = a than P = i because a requires that S be a consonant. SVPS is a noun or an adjective, and rear, roar and dead are the only eligible words which come to mind.

2. Between two proper names, and uncapitalized, SV could be de, and if V = e, FYV may be the and FCVV may be tree.

3. Between a dead and tree is a hyphenated word JMCT-VPFVE which is deciphered JMrT-eateE. E = n, giving EVPC as near.

4. If JMCT is worm, WCMT and MW may be from and of, JYM is who, and CMFFVE is rotten, in keeping with the dead tree theme.

The solution can now be filled in: Guatemala: from Aztec 'Guahte-

mali', rotten trunk, word used by the Mexican Indians who accompanied Pedro de Alvarado in his exploration of Central America, from having encountered a dead worm-eaten tree near the palace of the kings.

In Example 3, punctuation gives the starting clue:

Example 3 August/September 1952 (A-8), by Madeline Wilson
FRANCE SC NCPIAAIECRK YG PZI TIENLTSPRAI SC NKDAIECSJTI LSNF: "HI ZSMI WYCEAIESPIF SP PZNL PNKI, JIWSRLI HI SAI WYCLNFIANCE S CIH DAYFRWPNYC, NC HZNWZ HI LZYRTF TNBI *EAIEYAV *DIWB PY DTSV *IFHSAF *EANIE".

1. LSNF must be said. It could be this or thus, but these are ruled out by a one-letter word s in the third line. The rest of the solution is left to the reader to work out.

Additional problems follow for the reader's immediate entertainment, with solutions given in Answers and Solutions at the end of this issue. For an unlimited supply of such problems, the reader is referred to The Cryptogram.

Example 4 August/September 1952 (A-3), by Isabel M. Murdock
OEO XKT GJKV SCLS ED LHH SCR VLSRP EJ SCR *YPRLS *HLGRQ VRPR MTIMRO KTS, SCRPR VKTHO AR RJKTYC SK BKURP SCR BKTJSPX DPKI BKLQS SK BKLQS LJO DPKI *BLJLOL SK *IRWEBK SK L ORMSC KD DEDSRRJ DRRS?

Example 5 August/September 1952 (A-1), Richard A. Hammell
S NXRRBEB BQJNSZUXW NSW AB S AUE DBRH UW RSZBI RUTB, BYHBNUSRRL KDBW UZ NXGBY ZX EBZZUWE TXXZASRR ZUNFBZY. *ABWWBZZ.

Example 6 February/March 1951 (3), by Oliver Aberth
ZYXW VYX UTSVTA BAXCSADEXC FDPYV XNXASDCX, YX UTXCW'V OXGW MLOBDWP GV STWSFLCDTWC, GWU ALWWDWP LB EDFFC.

Example 7 August/September 1954 (A-10), author unknown
YC YB TSPSBBMEJ MOGMJB CA MYL MC NSYTW YTCSESBCYTW EMCXSE CXMT SHMPC UAE CXS BISPCMCAE UAEWYFSB SFSEJCXYTW SHPSIC QESMEYTSBB. *FAOCMYES.

Example 8 November/December 1968 (A-9), by Lea Neece
CHBQWF BUMU IHLSK XHNF CHLFQUEF KBHIWK, NEIEFV RLQ NGHBW MEBBUVWK, KWUBEFV WKRUIW SHLQWK.