A polyphonic substitution cipher is one in which several different plaintext letters are enciphered into a single cipher letter or symbol. Perhaps the most simple and well-known example of a polyphonic substitution cipher is the telephone dial, in which the letters ABC are encoded by the number 2, DEF by 3, GHI by 4, JKL by 5, MNO by 6, PRS by 7, TUV by 8, and WXY by 9. This is quite different from the well-known (monophonic) substitution cipher, in which each plaintext letter is associated with a different cipher letter -- if A is encoded by T, then no other letter of the alphabet is also encoded by T. (However, the opposite of the polyphonic substitution cipher is the homophonic substitution cipher in which a single plaintext letter can be enciphered into several different cipher letters or symbols -- for example, E might be represented by the number-pairs 13, 28 or 94.)

Superficially, polyphonic substitution ciphers resemble lipograms. In both cases, the reader is confronted with a message which contains fewer different letters (or symbols) than the normal 26-letter alphabet. However, a lipogram is restricted to those words which contain the allowable letters, whereas a polyphonic cipher allows any word to be encoded. In lipograms, all the words look normal but thoughts must be expressed in a circuitous way; in polyphonic ciphers, the thoughts are normal enough but many words are spelled in weird ways.

Polyphonic substitution ciphers have been known for more than three centuries; David Kahn's The Codebreakers (MacMillan, 1967) states that the Argentis, a family of cryptologists employed by the Pope shortly before 1600, used a polyphonic cipher. However, these ciphers seem to have remained outside the mainstream of cryptologic activity, probably because of their inherent ambiguity. If a cipher letter can represent several different plaintext letters, it is quite likely that two different plaintext words will lead to the same cipher equivalent. In the August 1970 Kicksaws, Dave Silverman pointed out that the telephone dial encodes both PYGMIES and SWINGER in the same way: 7946437. The article "Word-Pairs Differing in a Single Letter" in the May 1969 Word Ways demonstrated that no polyphonic cipher is entirely free of possible single-word ambiguities.

Should then such ciphers be discarded as unworkable? Not necessarily, because single-word ambiguities ought to be resolvable by looking at the context -- other words on either side. It is the purpose of this article to demonstrate that a careful selection of the way in
letters are encoded should hold the ambiguity to a minimum.

How much compression can be allowed in a polyphonic substitution cipher before the output becomes unreadable? Clearly, a cipher allowing 15 or more different symbols ought to cause little trouble; the 11 rarest English letters occur only about ten per cent of the time in normal text. On the other hand, any cipher which jams the entire alphabet into only 5 different symbols is bound to sound like an idiot mumbling Sanskrit in his sleep. Since the ten digits form a natural encoding (as in the telephone dial), it is reasonable to ask whether or not one can construct a polyphonic cipher on this base. Let us make the task a bit harder by insisting that one of the ten digits (say, 0) must be reserved exclusively as an indicator of word spacing, leaving only nine digits to carry the weight of 26 letters.

To make a long story short, we propose that the following polyphonic substitution cipher is about as good as any that can be devised to produce readable text from the cipher output:

1 E 4 I, L, B 7 R, Y, W
2 T, X, Z 5 O, G, J 8 S, F, M 0 Space
3 A, C, Q 6 N, P, K, V 9 H, D, U

Letters have been allocated to digits by a trial-and-error procedure attempting to satisfy various objectives which will become apparent presently.

Suppose that a message is written in this cipher; how does one decode it? Perhaps the simplest technique is to place the alternative letters in a vertical column with the commonest letter at the bottom, and look for patterns of letters that form words. For example:

V V Y
BK MUJ WZ B QM QI KK BKQ U BJ ZU BW MQBZU
LP FDGYX L CF CGPPLPC D LGXD LY FCLXD
IN SHORT I AS AONNIAEH IOTH IR SAITH....

Reading along the bottom, the words IN SHORT I leap out at once. AS does not seem too likely a follow-on to I, but we note that AM is a legal alternative. The next word is obviously a verb, but the bottom line is gibberish, and the next three words are none too clear either. (Before reading on, the reader is encouraged to try and figure out what these words are.) Is it possible that we have been too ambitious in restricting ourself to a nine-symbol code?

What is needed is a way to present to the reader the most plausible possibilities for the hidden words. One way to do this is to ask the following question: given two successive symbols, what is the most plausible bigram of letters corresponding to these symbols? For example, in the fourth word in the message above, AQ is clearly a very unlikely bigram (AORTA and GAOL come to mind), and in fact the bigram CO is overwhelmingly more plausible (AG is a second choice). If the ex-
This, in fact, is the primary basis upon which the alphabet was allocated to digits. Fletcher Pratt's *Secret and Urgent* (Blue Ribbon Books, 1942) gives in Table VIII of the Appendix a list of the 70 commonest bigrams occurring in English text, and in Table V the frequency of occurrence of letters as initials and terminals in English words. Each entry in the table below is the commonest bigram (according to Fletcher Pratt) corresponding to a digit at the left followed by a digit at the top; for example, if the pair 72 is encountered, the table suggests that RT is the most likely plaintext bigram corresponding to this cipher. 57 of the 81 bigrams in the table are included among the 70 commonest bigrams in the English language; in fact, the 30 commonest bigrams are all included in the table (DE is the first one that does not appear).

How is this table used to decode a cipher? Note that the terminal letter of one recommended bigram may not coincide with the initial letter of the next recommended bigram; for example, 72 leads to RT but 26 to XP. To get around this problem, the putative plaintext is written on two lines, with a shift from one line to the other whenever there is a disagreement of this sort. Returning to the earlier message, how does it now look?

```
IN SH L AS A D I MAL D AND ETNERI DORT I CONNINCED IOTH LY S ITH XP LENCE
```

How is this table used to decode a cipher? Note that the terminal letter of one recommended bigram may not coincide with the initial letter of the next recommended bigram; for example, 72 leads to RT but 26 to XP. To get around this problem, the putative plaintext is written on two lines, with a shift from one line to the other whenever there is a disagreement of this sort. Returning to the earlier message, how does it now look?

```
IN SH L AS A D I MAL D AND ETNERI DORT I CONNINCED IOTH LY S ITH XP LENCE
```

How is this table used to decode a cipher? Note that the terminal letter of one recommended bigram may not coincide with the initial letter of the next recommended bigram; for example, 72 leads to RT but 26 to XP. To get around this problem, the putative plaintext is written on two lines, with a shift from one line to the other whenever there is a disagreement of this sort. Returning to the earlier message, how does it now look?
of the words from the context; the eighth word (actually, FAITH) was the only one to cause real trouble. The original message, taken from Thoreau's Walden, is:

In short, I am convinced, both by faith and experience, that to maintain one's self on this earth is not a hardship but a pastime if we will live simply and wisely.

Of the 128 letters in this message, the commonest-bigram scheme identified all but 11 to within at most two possible alternatives; even one really rare letter, X, was spotted.

The reader may want to try his hand at decoding another message with the aid of the commonest-bigram table:

\[
\begin{pmatrix}
42048 & 06520 & 61318 & 83770 & 29320 & 30836 & 08959 & 49013 & 76094 \\
80446 & 46504 & 70291 & 08713 & 20580 & 94804 & 75709 & 64188 & 09108 \\
71328 & 01384 & 17029 & 36040 & 95
\end{pmatrix}
\]

The message has been divided into groups of five for ease in reading. The answer can be found in Answers and Solutions at the end of this issue.

So far, we have talked about ways to make a polyphonic substitution cipher as easy as possible to read. Usually the objective of a cipher is just the opposite. Can this cipher be used for secret communications? Suppose that the assignment of letters to digits was rearranged in a way known only to the sender and the recipient; for example, BLI might be encoded as 7, QCA as 2, a space as 5, and so forth. (The shuffling of digits could be easily remembered by means of a ten-letter isogram, such as BACKGROUND or COMPUTABLE.) To improve the security of such a cipher system, a secondary objective in assigning letters to digits was to equalize the frequency with which the different digits would appear in normal English text. Although perfect balance could not be achieved, the range of variation is small: among the digits 1 through 9, the digit 1 will appear most frequently (about 13 per cent of the time), while the digits 5 and 6 will appear least often (about 10 per cent of the time each). Unfortunately, the security of the cipher is seriously compromised by the fact that spaces appear much more often -- perhaps 20 per cent of the time in normal English text. The would-be cryptanalyst can easily identify which digit is being used to represent a space, and it is then an easy matter to recover the digits corresponding to A and I, the only two single-letter words. Anyone contemplating using this cipher, therefore, is strongly encouraged to omit all spaces between words, even though this makes recovery of the plaintext more difficult.

Aside from cryptography, do polyphonic ciphers have any practical uses? Let us return to the telephone dial mentioned at the beginning of this article. The telephone network is already being used to pass data from one computer to another, and in the future one can envisage people interacting with computers on the same network.
If the number of telephone subscribers listed in the computer is large, ambiguities arise; for example, the surnames Aaron, Baro, Baron, Bason, Capon, Caron and Cason (found in the 1973 Morris County, New Jersey directory) are all enciphered by the digits 22766. However, this is somewhat less serious than the ambiguities caused by the fact that many different people have the same surname -- a problem that cannot be solved even with a 26-hole telephone dial! Specifically, if one selects at random one of the 135,000 residential subscribers from the Morris County directory, his surname will on the average be matched exactly by three other subscribers, but his surname will in addition be matched telephonically by only one other subscriber. Some of the worst telephonic garbles are Harrison-Garrison, Morton-Norton, Kane-Lane-Land, Bailey-Bagley, Carey-Casey, Morris-Norris, Barr-Carr-Bass, Butler-Cutler, Carter-Carver, Walker-Waller, Rios-Sims, Ryan-Swan, Gunter-Hunter, Powell-Rowell, Ward-Ware, and Gill-Hill.

Surname garbling can be substantially reduced by modifying the letter-pattern on the telephone dial. If alphabetic order is maintained but any split-points are allowed, the optimum dial is probably AB/CD/EFG/HIJK/LM/NOP/QRS/TUVWXYZ, which reduces telephonic ambiguity by more than one-half. If one rearranges the letters of the alphabet to eliminate as much surname ambiguity as possible, a very good (but probably not optimum) dial is ADPY/BENZ/CMX/FTKW/GS/HU/ILV/JOQR, which reduces telephonic ambiguity to only one-twentieth of its original level. In a list of common United States surnames (those with ten thousand or more representatives in Social Security files), the only ambiguous pairs were Garner-Garber, Kinney-Finney, Beal-Neal, Keller-Weller, Moon-Coon, Mooney-Cooney, Mullen-Cullen, Fay-Kay-Way, Dickens-Pickens, Tilley-Willey, and Finn-Winn. However, a scrambled letter-arrangement on the telephone dial would very likely prove to be unacceptable to the typical user.