...As I trudged up the hall steps of 221 B Baker Street, my attention was drawn to the door of our flat. Someone had written the letters QZHDF LPCIE OAKXC MRVMT in chalk across the upper panels. I had not the least idea what this mysterious message meant, but concluded that it might be some sort of a cipher.

Excitedly I opened the door and rushed into the room. Holmes was sitting at the table, scribbling with a perplexed expression on a sheet of foolscap.

"Holmes," I cried, "What does it mean, and where did it come from?"

"I don't know, Watson," he replied. "Mrs. Hudson called it to my attention when she brought up the afternoon tea. I believe that it may be a substitution cipher with the words run together and then broken up into five-letter groups, but so far I have been able to make little headway with it. It has been carefully constructed to resist the standard methods of solution. For instance, you will note that sixteen letters appear once and two letters appear twice in the message; the normal letter-frequencies have been completely suppressed. I know of no way other than trial and error, and the number of possibilities is astronomical."

"Perhaps," I ventured, "I could help you in the search. If it is really a matter of trial and error, two people working on it can examine twice as many possibilities in a given time."

A flicker of surprise and amusement crossed Holmes' face. "Really, Watson," he said, "I shouldn't think that this would be much up your line. Still, if you wish to try..." He shrugged his shoulders and returned to his labours.

A bit nettled by his condescending manner, I resolved to find the solution to the cipher. It proved, however, to be an arduous task. I worked on it all that evening and most of the following day
with little success, and was nearly ready to admit that Holmes may have been correct in valuing my services so lightly.

I will not bore the reader with an account of my false starts, nor describe the methods which eventually led me to the solution. Suffice it to say that my perseverance was eventually rewarded by the following translation to the message: WHY JUMP A LOT? REGAIN BID. Excitedly I showed my solution to Holmes. "It is obvious," I said, "that this message was written by a devotee of the game of whist. His message points out, reasonably enough, that the careless whist player who follows a bid of two hearts with a bid of four spades foregoes the opportunity to describe the strength of his cards by one or more intermediate bids."

To my chagrin, Holmes appeared singularly unimpressed by my discovery. "Most interesting, my dear Watson. However, I have found that the deciphered message reads PACK MY JUG WITH FUEL, BEN. The unknown writer is requesting a man named Benjamin to fill his jug with kerosene, naphtha or a similar inflammable liquid."

Before I could reply to this unexpected revelation, there was a knock at the door. Holmes strode across the room and jerked the door open sharply, revealing the plump form of our landlady, Mrs. Hudson, with a slip of paper in her hand. "Begging your pardon, Mr. Holmes," she began timidly. "The message in chalk written on your door. I thought that it might be a cipher of some sort and took the liberty of copying it down and attempting to find the hidden message in it. The message says," here she read from her paper, "NYMPHS WALTZ, DO FAIR JIG. Do you have any idea what it means?"

Holmes, who had been listening intently to Mrs. Hudson's narrative, broke into a roar of laughter when she read off the message. "Capital!" he spluttered. "It now appears that our message-writer is a whist-player, a kerosene-purchaser, and the director of a female dancing-school..."

* * *

In his landmark paper "Communication Theory of Secrecy Systems" (published in the Bell System Technical Journal, October 1949), communication theorist Claude Shannon developed a mathematical theory which enabled him to assess the likelihood that a cipher of N letters would have a unique solution. Specifically, the paper defines the unicity distance of a cipher -- the minimum number of letters required in the cipher if it is to have a unique solution with high probability. For substitution ciphers in English, he esti-
Holmes may have had a different opinion. Suf­
ficiently, by the word "GAIN
ous," some of careless
his spades
or by one

I have
FUEL,
min to

I was a
I, Mrs.
written
sort, the hid-
what

narrow-
message.
writer
of a fe-

Readers interested in the solution of cryptograms may
wish to join the American Cryptogram Association which
issues a bimonthly newsletter filled with puzzles of all
degrees of difficulty. For further information, write
the Treasurer, 604 W. Monroe Street, Mexico, Missouri
65265.

mated the unicity distance to be about 27 letters, and commented
"with 30 letters there is nearly always a unique solution to a crypt-
ogram of this type and with 20 it is usually easy to find a number of
solutions". Holmes's cipher, of course, is only 20 letters long.

What is the longest possible substitution cipher for which two
different solutions can be found? If Shannon is correct, there should
be at least a few such ciphers of 30 letters or more. Readers of
Word Ways are invited to try their hand at finding such ciphers. In
order to avoid trivial solutions to this problem, one important re-
striction must be placed on the two solutions to the cipher -- a
cipher letter cannot be replaced by the same plaintext letter in the
two messages. Thus, if cipher V is replaced by plaintext P in the
first message, cipher V must be replaced by some other plaintext
letter in the second one. This avoids a pair of solutions of the form
HE HANDED THE RICH WIDOW A TINY GREEN JUG and HE HAND-
ED THE RICH WIDOW A TINY GREEN BUG.

Readers interested in the solution of cryptograms may
wish to join the American Cryptogram Association which
issues a bimonthly newsletter filled with puzzles of all
degrees of difficulty. For further information, write
the Treasurer, 604 W. Monroe Street, Mexico, Missouri
65265.