PROJECTS–HI-FI–COMPUTERS

$1.00 • DEC. 1977

Radio-Electronics

THE MAGAZINE FOR NEW IDEAS IN ELECTRONICS

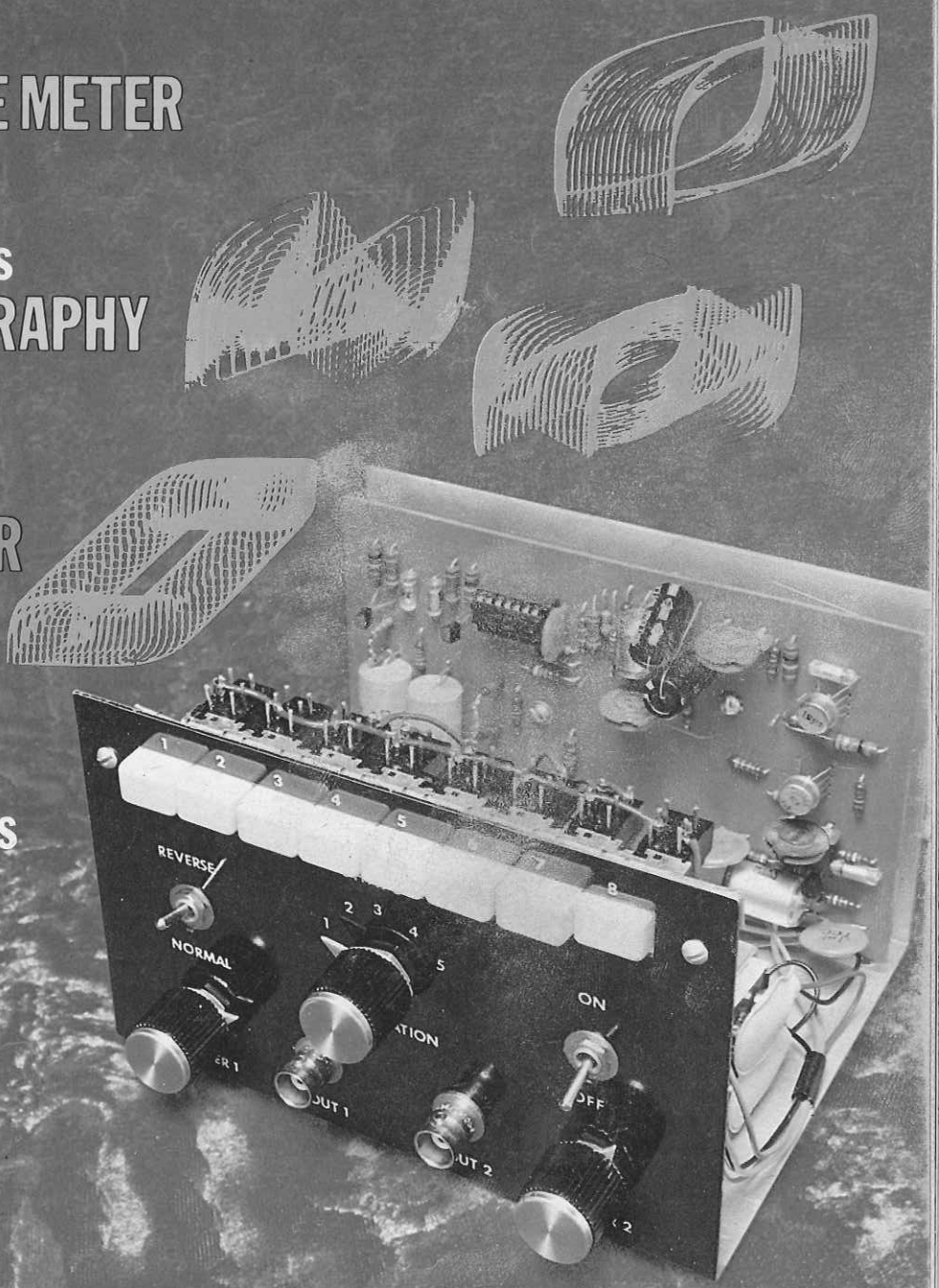
for your workbench build
DIGITAL CAPACITANCE METER
has 4-digit LED readout

decipher secret messages
COMPUTER CRYPTOGRAPHY
use your microcomputer

build scope add-on
OPTICAL SYNTHESIZER
for 3D patterns galore

easy to build
CB SWITCHER
for music between CB calls

construction technique
IC BRICKLAYING
for miniature projects



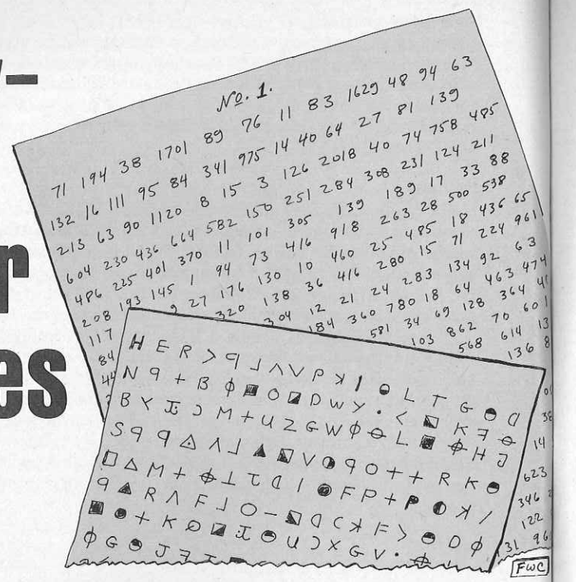
GERNSBACK PUBLICATIONS

PLUS:

☆ Broadcas ☆ Hobby Corner
☆ CB Test E ervice Clinic
☆ Equipment Reports ☆ Hi-Fi Test Reports

Computer Cryptography—

How To Decipher Secret Messages



Looking for a new way to use your computer? Try deciphering secret messages and breaking codes. Its a natural for your computer and plenty of fun.

FREDERICK W. CHESSON

THE BEALE PAPER NO. 1 SUPPOSEDLY describes the exact location of a treasure trove of gold, silver and gems deposited about 1820 somewhere near Bedford, VA. The message is the first part of a famous cryptographic trio. The second describes the treasure and was solved many years ago using the Declaration of Independence as a key. The third paper is said to give the names of the treasure-party members and their next of kin. Ever since the second paper was deciphered, many attempts have been made to find the key to the first and third messages. Neither the Bible, Shakespeare, the United States Constitution or any other federal documents have provided any clues.

In recent years, treasure hunters with metal detectors, "alleged deciphers," and some cryptic clairvoyant revelations have roamed the mountain countryside, much to the annoyance of local property owners.

Meanwhile, back in the computer labs, endless reams of printouts spew forth and video displays scan flickering alphanumerics, as new key-texts and endless variations of old ones are statistically analyzed for meaningful letter patterns. It is, in fact, from the data-processing area of the Beale treasure hunt that the only so far known monetary reward has materialized. In 1970, Dr. Carl Hammer, director of the UNIVAC Division, Washington, DC, was awarded the $500 first prize for his paper: "Signature Simulation and Certain Cryptographic Codes," by the Third Annual Simulation Symposium.

A collection of jumbled alphabetical and geometric figures is shown in Fig. 1. This represents the second in a series of alleged messages from "Zodiac," the slayer of at least 10 persons in the San Francisco Bay area, circa 1969. The text is reported to contain information concerning Zodiac's true identity. If deciphering the cryptogram leads to the killer's arrest and conviction, a reward of at least satisfaction, if not a monetary presentation, may await the lucky code-breaker.

Terminology

Code-making and breaking has its own terminology, as follows: *Cryptology* covers the entire scope of secret communications: Written codes and ciphers, invisible inks, microdots, voice scrambling, infrared and ultraviolet signaling and even electronic jamming and countermeasures.

Cryptography concerns the written word, whether transmitted by paper or electronically. *Enciphering* is that process by which information is rendered unintelligible to the uninitiated. Normal words, or *plaintext*, are converted into *ciphertext*. When ciphertext is prepared for transmission or just received, the message is called a *cryptogram*. *Deciphering* refers to the reverse process, in which ciphertext is again turned into plaintext for all to read. An unauthorized attempt to break the cryptogram is variously described as *decrypting, cryptanalysis* or simply old-fashioned *code-breaking*.

While the terms *code* and *cipher* are often used interchangeably, cipher is generally considered an overall term for an enciphering process. Code more narrowly describes a process in which a complete word, phrase or entire sentence is replaced by a group of letters or numbers.

Cipher groups

There are two major groups of ciphers, both with a host of subdivisions. A *transposition cipher* scrambles its original letters or words about according to routes or geometrical patterns. The word "cipher" can be transposed into "perchi," for example.

Substitution ciphers are often found in their simplest form in many newspaper cryptogram puzzles. Plaintext letters are replaced by other letters or numbers, according to a general formula and with a particular key, which indicates which letter will become what other letter or number. In the *simple-substitution* cipher, the key remains the same for the entire message; the letter E is always replaced by X, A by Q, T by Z, etc.

More secure systems use multilettered keys, in which E is replaced by J the first time it is used, then by F, then by W or even by itself. Generally speaking, the longer and more random the key, the safer the message.

A modern practical system is *pseudo-random key-generator*. This system, operating on shift-register principles, produces an apparently random series of bits and zeros, which may be further transformed into equally random-appearing key letters or numbers. A 20-stage register could, for example, provide a nonrepetitive stream of over one million bits.

The code-breakers, however, have used computer-assisted cryptanalysis to prove that what is not purely random can be fairly quickly broken. Today, the problems of secure data transmission between computer centers and terminals are the latest chapter in a story as old as recorded history itself.

Microcomputer-based cryptography

Even the most basic microcomputer, combined with an ASCII keyboard input and a video display output, can perform many cryptographic functions, including encoding, decoding and cryptanalysis. Such things as FORTRAN or BASIC compilers and line printer outputs for hard copy, while useful accessories, are not really necessary for the beginner to try cryptography.

FIG. 1—SECOND ZODIAC MESSAGE of 1969 contains the identity of the killer.

As a matter of fact, a slight modification to the TV Typewriter circuit (see **Radio-Electronics,** September 1973 issue) will permit the device to code and decode simple substitution-cipher messages, and to make trial decipherments for a wide variety of other substitution-type ciphers.

TVT modifications

The 512-character memory of the original TV Typewriter is adequate for most cryptograms. Even 256 characters are sufficient for the majority of these puzzles, and 128 will work for most of the "recreational cryptopuzzles."

You need some sort of "store and compare" circuit. This permits a character that will be replaced to be temporarily stored and compared with the other characters in the memory, one step at a time. When a match is made, then the character in question is replaced by another one by depressing a selected key on the keyboard.

For example: Consider "XYZQZ KU CVLXYZQ LVZ . . ." Noting that Z occurs rather frequently, you could substitute E, the most common letter in the English language. First Z is keyed into the temporary memory, then the memory is scanned, with the replacement E keyed in. Every time a Z is encountered in the cipher-text, it is replaced by E. This results in the displayed text now appearing as: "XY*EQE* KU CVLXY*E*Q LV*E* . . ." The location of the two E's in the first word suggests "there." Substituting X = T, Y = H, and Q = R yields "*THERE* KU CVL*THER* LV*E*". Although there isn't much firm statistical information in this brief fragment, you can feel reasonably confident in substituting K = I, U = S, C = A, V = N, and L = O, giving "THERE IS ANOTHER ONE."

The trial decipher process can be considered an "examine and replace" logic routine as follows: "Does memory location 1 = A? If yes, replace location 1 with B and go to the next location. If no, go on to the next location. Continue until the nth location has been examined." The basic flow chart is shown in Fig. 2.

The hardware for this TV Typewriter routine consists of a 74174 hexlatch for storing the character to be replaced, and an 8160 6-bit comparator, for determining whether the particular character in the memory being examined is the same as in the hexlatch. The general circuitry is shown in Fig. 3.

Operation

To encode a message, first clear the screen, leave a few blanks and write in the normal alphabet from A to Z. On the next line, directly below, type in the cipher alphabet. Having then written in the message and checked it for accuracy, home the cursor and turn off the WRITE ENABLE.

The choice of an enciphering alphabet is up to the user and his correspondents. In hobby-type cryptography, generally no plain letter is represented by itself in the ciphertext. Two typical cipher alphabets are shown below:

Plain: A B C D E F G H I J K L M N, etc.
Cipher: Q W E R T Y U I O P A S D F, etc.
Plain: A B C D E F G H I J K L M N, etc.
Cipher: Z *K R Y P T I* C A B D E F G, etc.

Notice the key word, *kryptic,* in the second cipher alphabet. Sometimes the plain alphabet is keyed; sometimes *both* alphabets are keyed. It is only necessary that letters not be repeated. Some solvers consider recovering keywords as interesting as solving the message itself.

To encipher "A," depress the A key on the keyboard,while briefly engaging the WRITE key or switch. Now press the Q, Z, or whatever key the cipher equivalent represents, and activate the CLEAR switch. This should cause every A on the video display to be replaced by Q, Z or equivalent. Similarly, proceed down the alphabet to Z (assuming the message has a Z in its text), noting that each plain letter is replaced by its cipher equivalent.

Decoding is similar. For accuracy, again just write in the plaintext and cipher alphabets, one above the other, before entering the message. When you have finished replacement, there should be two normal alphabets above the plain-text message, which will serve as a check that all the cipher letters have been processed.

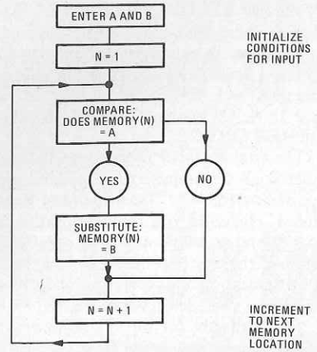


FIG. 2—FLOW CHART for substituting letter B for letter A in a memory of N letters.

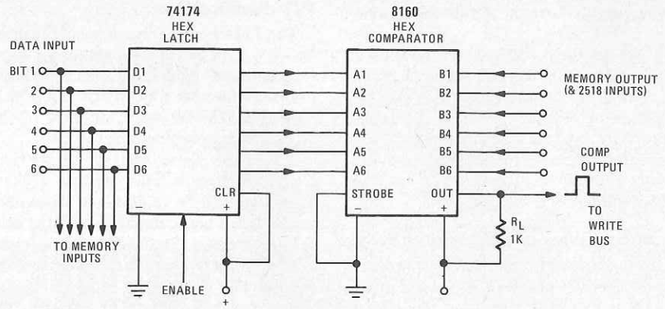


FIG. 3—EXAMINE AND REPLACE circuit for the TV Typewriter.

Cryptanalysis

The following suggestions can help in the solution of simple-substitution cryptograms:

1. Frequency count: The letter "E" is the most common in the English language. The other vowels, except for "U," show a high percentage as well. For standard English, the precedence is: E T A O I N S H R D L U C P F M W Y B G V K Q X J Z.
2. Single letters are almost always A or I.
3. Vowels and consonants tend to alternate, as E-R-E, D-A-N, etc.
4. Certain letters tend to form reversals: ER-RE, ES-SE, ED-DE, etc.
5. Two- and three-letter combinations (called di-grams and tri-grams) have their own frequency-count precedence, such as TH, HE, AN, IN, ER, RE, ED, EN, THE, AND, ION, ING, ENT, ARE, FOR.
6. Letter patterns help: when V-W-X-X-V-Y suggests L-I-T-T-L-E, and Q-K-Y-G-Y, the commonly used T-H-E-R-E.
7. Word patterns are also useful. If XYZ appears frequently, it may well be THE, and WM XYZ or JU XYZ might turn out to be IS THE, or OF THE.

When writing in a trial solution, try to avoid confusing cipher letters for plaintext trial letters. If the cryptogram contains E, T, A, I, etc., replace these at the start with numerics, like 1, 2, 3, 4, etc. With the 63-character set available on the original TV Typewriter and most similar sets, transpose the cryptogram's letters into nonalphabetic numeric characters. For example, if you make a frequency count of the cryptogram and find that X, I, V, Z, and O are the highest, then they and the others can be replaced by:

X	I	V	Z	O	T	Y	A	B
1	2	3	4	5	6	7	8	9

The problem can also be eliminated by having an upper- and lower-case character set. It also helps to have the original ciphertext permanently on view. This can be done by writing in the trial decipherment letters *under* the cryptogram letters as follows:

XYZQZ KU CVLXYZQ LVZ
THERE T HER E

The circuitry requires some additional IC's; but in cryptograms of under about 250 letters (and spaces), it eliminates lengthy keyboard rewriting when the cryptanalysis becomes hopelessly garbled. **R-E**

Digital clocks and watches win places in design show

The second annual Design and Engineering Exhibition, held in Chicago this summer, selected among its exhibits two Zenith electronic time-display devices, among the 83 consumer electronics products exhibited for their innovative design.

"BILLBOARD" AM/FM CLOCK RADIO, the Zenith J465W, presents a design innovation, the "billboard" mounting, in clock radios. Placement of the display and the large illuminated numbers make the clock readable even across a room.

"Billboard styling" is introduced in one device, the *Billboard* electronic digital clock radio. Among other features, the clock includes an alarm display that indicates the exact minute to which the alarm is set. A power reserve feature keeps the clock circuits functioning for up to four hours in the event of an accidental disconnection from the line or a power failure.

The other device, the *Port Royal* electronic quartz watch, combines digital and traditional approaches, featuring hands-and-dial display for hours and minutes and an LED digital display for reading out the seconds and date. This new model is manufactured by Zenith Time S.A. in Switzerland, and will be available in the United States this Fall.

The Design and Engineering Show is sponsored by the Consumer Electronics Group of the Electronic Industries Association (EIA).

Teamsters sponsor daily CB newscast

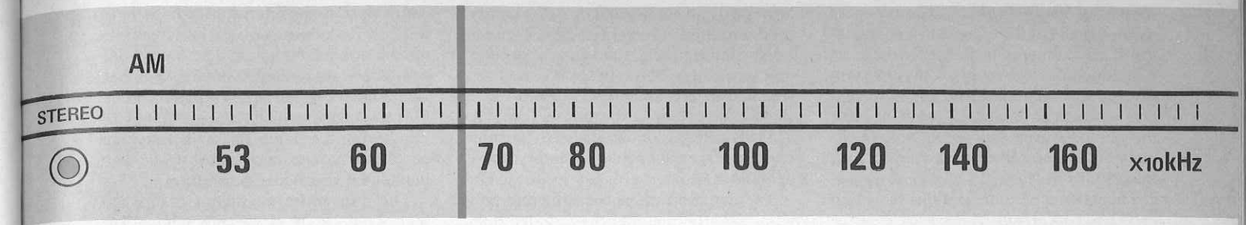
The International Brotherhood of Teamsters who, more than any other group, has been responsible for the tremendous growth and popularity of CB radios, are providing a daily public service newscast to participating radio stations.

The National CB Radio Network broadcasts news of interest to the entire spectrum of CB enthusiasts, from seasoned veterans to laymen. The programs include news stories on the latest equipment and technology, FCC regulation updates, special events, celebrity interviews, as well as human interest stories.

CB industry group backs FCC rulings

The EIA's Citizens Radio Section, a group of CB manufacturers working with the Federal Trade Commission on improving CB radio rules, recently endorsed a ruling barring the sale and use of linear amplifiers. These amplifiers, which raise CB station power to more than the 4 watts allowable, provide considerable amounts of interference to CB's and other electronic equipment.

The CB group has also backed a proposed FCC rule change on the type acceptance of commercially produced amateur radio equipment. It is recognized that there are two groups of such equipment: one designed for legitimate amateur use, the other purporting to be such but actually intended for improper use. Although the latter equipment is rarely sold to legitimate amateurs, the Citizens Group believes that a ruling on type acceptance would be in the public interest. **R-E**



Broadcast Systems For AM Stereo

A number of different systems have been conceived in the years since AM stereo was first proposed. The FCC may soon select one as the standard

LEN FELDMAN
CONTRIBUTING HI-FI EDITOR

BY THE TIME YOU READ THIS, THE NATIONAL AM Stereophonic Radio Committee (an audio industry group formed under the auspices of the Electronic Industries Association) will have completed its lab and field tests in Bethesda, MD. These tests are the culmination of a long series of events dating back to the 1950's, when the Federal Communications Commission was asked to make rules for stereophonic FM broadcasting. At that time, it was proposed that rules also be made for stereophonic AM broadcasting as well as for the stereophonic broadcasting of the audio portion of TV.

Rule making was initiated only for stereo FM broadcasts at that time, and in 1961, compatible stereo FM broadcasting began. It was felt that there was no real need for stereo sound on TV and that, in the case of stereo AM, owners of AM broadcast stations were doing quite well financially, whereas FM station owners were facing extreme economic hardships. To bolster the FM situation, action was first taken with regard to stereo FM to give those stations a clear advantage over their AM competition.

At present, FM broadcasting is an extremely healthy industry (some say it has surpassed the older AM in its economic success), and it is the AM broadcasters who have been crying for help! Apparently, if timetables hold, help is on the way. Before long, the FCC will be examining the massive amount of data submitted to it by the NAMSRC (*N*ational *AM S*tereophonic *R*adio *C*ommittee) with an eye towards setting up new rules for stereo AM broadcasting.

When this committee began, at least five proponents offered stereo AM broadcast techniques for consideration. These were Leonard Kahn (whose stereo AM system has been successfully used in transmissions from Mexico for many years), RCA, Magnavox, Motorola and Sansui. In recent months (and in the field tests themselves), the number of systems has narrowed down to three: Magnavox, Motorola and the Belar Company (whose system is essentially that proposed originally by RCA). While the mathematics of each of the remaining systems is rather complex, we will review briefly how each system works and what changes must be made in transmitting and receiving equipment in order to handle each of the three remaining systems.

Magnavox system

The proposed Magnavox stereo AM broadcasting system is an AM/PM (*P*hase *M*odulation) system that places left-plus-right (L + R) information on a phase-modulated channel with a proposed phase deviation of one radian. In addition, a 5-Hz subaudible tone is frequency-modulated into the carrier with a deviation of approximately 100 Hz. This tone is for stereo identification (similar to the way a 19-kHz pilot carrier in stereo FM lights an indicator on the receiver) and is an attractive selling point.

A block diagram of the complete transmitter system is shown in Fig. 1. The transmitter uses nearly all of an existing monophonic AM transmitter with no modification. The channel oscillator is replaced with a phase-modulated signal generator and signal tone source. This signal generation method provides for on-frequency operation, eliminating the need for multiplying or mixing stages. The station carrier is generated on-frequency and modulated with a 5-Hz tone. This signal is then used as a reference for a wideband phase-locked-loop to generate a true phase-modulated (PM) signal on-frequency. The latter signal is then amplified and modulated by the L + R audio signal in the existing transmitter. The processing blocks shown at

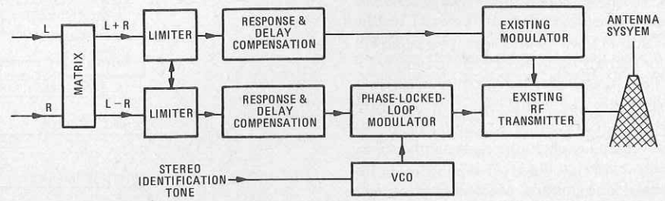


FIG. 1—TRANSMITTER FOR MAGNAVOX SYSTEM uses a phase-locked-loop to produce a phase modulated carrier. The audio signals are limited and compressed after matrixing.