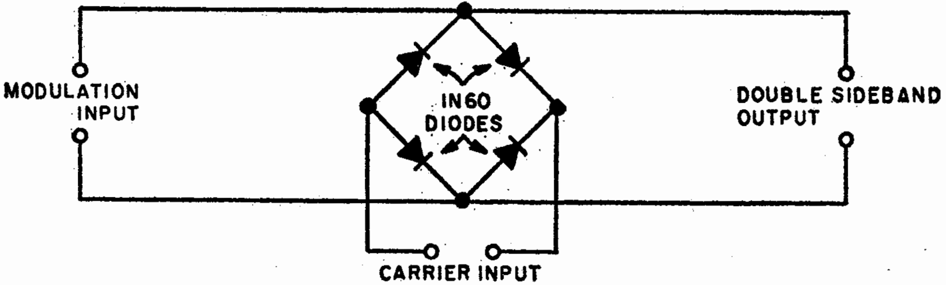
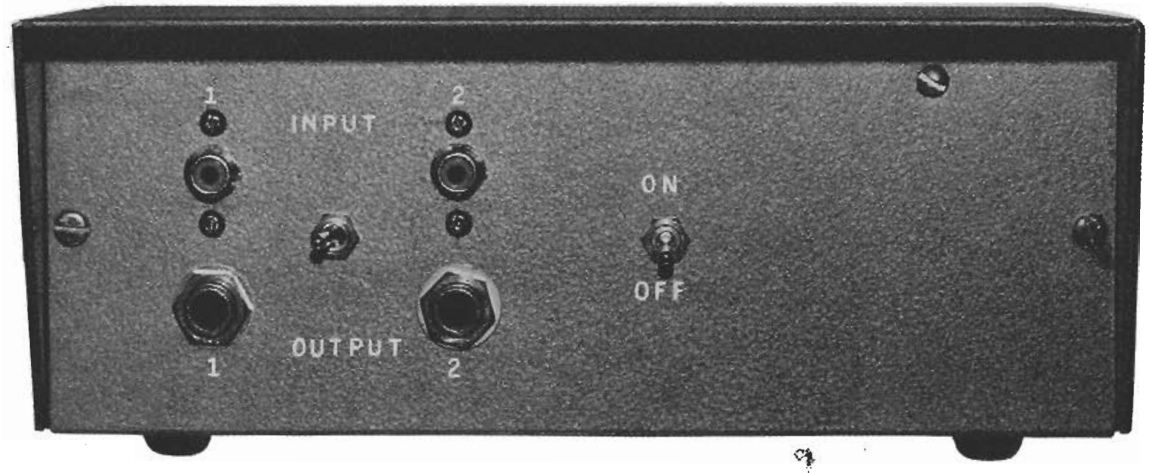
97 Sideband Scrambler



Feed audio modulation to one input, a carrier to another and the output of this sideband generator will be upper and lower sideband with supressed carrier. Where is it used? Try a sideband rig or a telephone speech scrambler. Work the scrambled signal into the modulation input to unscramble your speech scrambler output.



ENJOY PRIVATE MESSAGES WITH A VOICE SCRAMBLER

Low-cost IC circuit makes messages unintelligible without a similar unit

BY JOSEPH B. WICKLUND, JR.

WOULD you like to be able to keep unauthorized people from listening to your private communications? Thanks to recent advances in integrated circuit technology, it is possible to build a low-cost voice scrambler that will make your message unintelligible to anyone who doesn't have a compatible unscrambler. Of course, voice scramblers have been around for many years, but most of them are too expensive or too difficult to use (or both). This circuit is easy to build, is reliable, and can be used as either the scrambler or unscrambler.

How Scrambling Works. The block diagram in Fig. 1 shows how the scrambler works. The incoming audio signal is filtered to remove all frequency components above 3 kHz as shown at (A). The signal is then used to modulate a 3.5-kHz oscillator signal, with a linear four-quadrant multiplier as the balanced modulator. The output (B) of the multiplier includes the sum and difference frequencies between the two inputs. Another filter removes the sum frequencies and any remaining 3.5-kHz carrier, leaving only the difference frequencies as shown at (C).

Secrecy Through Electronics

The art and techniques of security in communications today

BY CLAY TATOM
Motorola Inc.
Semiconductor Products Div.

NOT TOO long ago, "security" meant something very different from what it does today. Now, it is a synonym for "protection" from thefts of anything from real property to communication information. So high is the interest in secure communiations that the U.S. Government plans to make all official communications secure by the mid-1980's. Other governments and many industrial and commercial establishments throughout the world are following suit. So too are a number of private citizens who want to preserve the privacy of their communications.

The growth of electronic communication since 1940 has revolutionized the secret world of cryptology. Wires and radio waves now carry unbelievable quantities of communication information at staggering rates. Electronics provides the means of unauthorized and illegal eavesdropping on this information. Some of this eavesdropping is done by specialists with expensive "bugging" equipment, posing a real threat. Much of it is by amateurs, listening in on business, Public Safety, and other "private" radio broadcasts.

It is interesting to note that, in the output, the voice channel from 300 to 3000 Hz is contained in a single-sideband signal from 3200 to 500 Hz. It can be recorded or transmitted like any other voice signal, but the frequency spectrum of the output is an inversion of the input. (For example, an input frequency of 300 Hz is 3200 Hz in the output and an input of 2500 Hz is 1000 Hz in the output.) The inversion thus makes the voice message unintelligible.

When the scrambled signal is coupled to the input of a similar unit, the signal is re-inverted and the original audio comes out in unscrambled form as shown at (D) and (E) in Fig. 1.

Circuit Operation. The complete schematic of the voice scrambler is shown in Fig. 2. Integrated circuit *IC1* is used as a high-input-impedance buffer amplifier to prevent loading on the signal source. Resistors *R2* and *R3* control the gain of the buffer. An active low-pass filter with a cutoff frequency of 3000 Hz is provided by *IC2* and *IC3*. The shape of the filter is controlled by the feedback components (*R4-R7* and *C2-C7*) and the circuit is designed to provide a four-pole Chebyshev filter characteristic with 1 dB of ripple in the passband and a sharp rolloff. Integrated circuit *IC5* is a stable square-wave oscillator operating at a frequency determined by *R16, R17,* and *C9*. Potentiometer *R17* is used to adjust the oscillator frequency so that two or more units can be matched. The oscillator output is attenuated by resistors *R18* and *R19* and modulated by the output of *IC3*, the filtered input signal. The balanced modulator is *IC4*. Trimpots *R27* and *R28* provide balancing adjustments for the modulator. When they are properly adjusted, only the sum and difference frequencies of the two inputs will appear at the output. Integrated circuits *IC6* and *IC7* form a low-pass filter to pass only the desired output signal.

The output of *IC7* can be used to drive load impe-

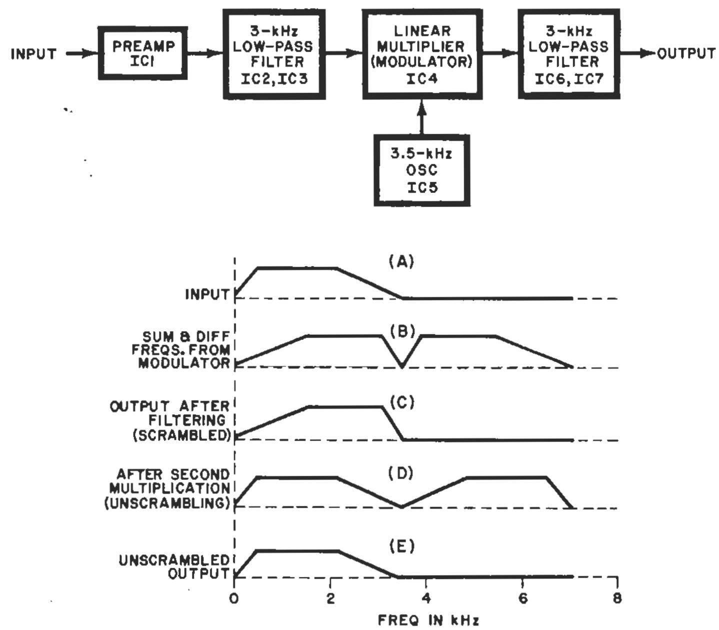


Fig. 1. Block diagram and waveforms show how the scrambler works. (A) is incoming signal; (B) is sum and difference; and (C) is output after filtering. Uncrambling is shown in (D) and (E).

Radio receivers are readily available for monitoring taxicab, aircraft, and police despatches. Some police departments might condone "good-citizen" monitoring of their broadcasts since it increases the number of observers on the lookout for stolen cars, fleeing suspects, etc. More often than not, however, they prefer that private citizens do not listen in. Some communities, in fact, have enacted laws that make it illegal for any but authorized law enforcement personnel to monitor police broadcasts.

Security Goes Public. Industrial and private secure-communication systems generally employ simpler enciphering techniques than those used by the high-level governmental agencies. While these are relatively simple systems today, they would have boggled a cryptanalyst's mind only a few decades ago. Most such systems are electronic, designed to effectively thwart the casual would-be eavesdropper. They are, however, relatively easy to decode if the eavesdropper is willing to spend the money to attack them with sophisticated techniques.

Most companies that make secure voice systems use a "scrambler" technique. The scrambler, as its name implies, mixes up (scrambles) the speech portions of the audio-frequency range. Scramblers have the advantage over more secure governmental systems in that they are inexpensive, compact, often require only narrow-bandwidth transmission channels, and offer adequate security for their proposed use. They generally provide several hours of security even against the serious commercial eavesdropper.

A generalized block diagram of a speech scrambler is shown in Fig. 1. The operator speaks into the microphone. Following the mike may be special processing circuits like speech compressors, delta-modulation response-curve generators, etc. The processed speech signal then undergoes some form of encoding, analog or digital, in some combination with an electronic "key" whose methodology appears to be random in nature. If an all-digital scheme is used, an analog-to-digital (A/D) converter becomes part of the encoder, while a digital-to-analog (D/A) converter be-

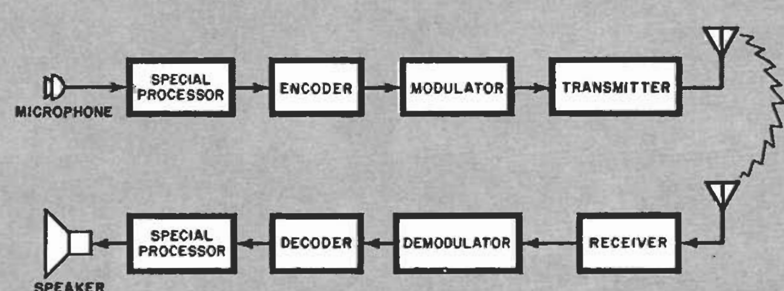
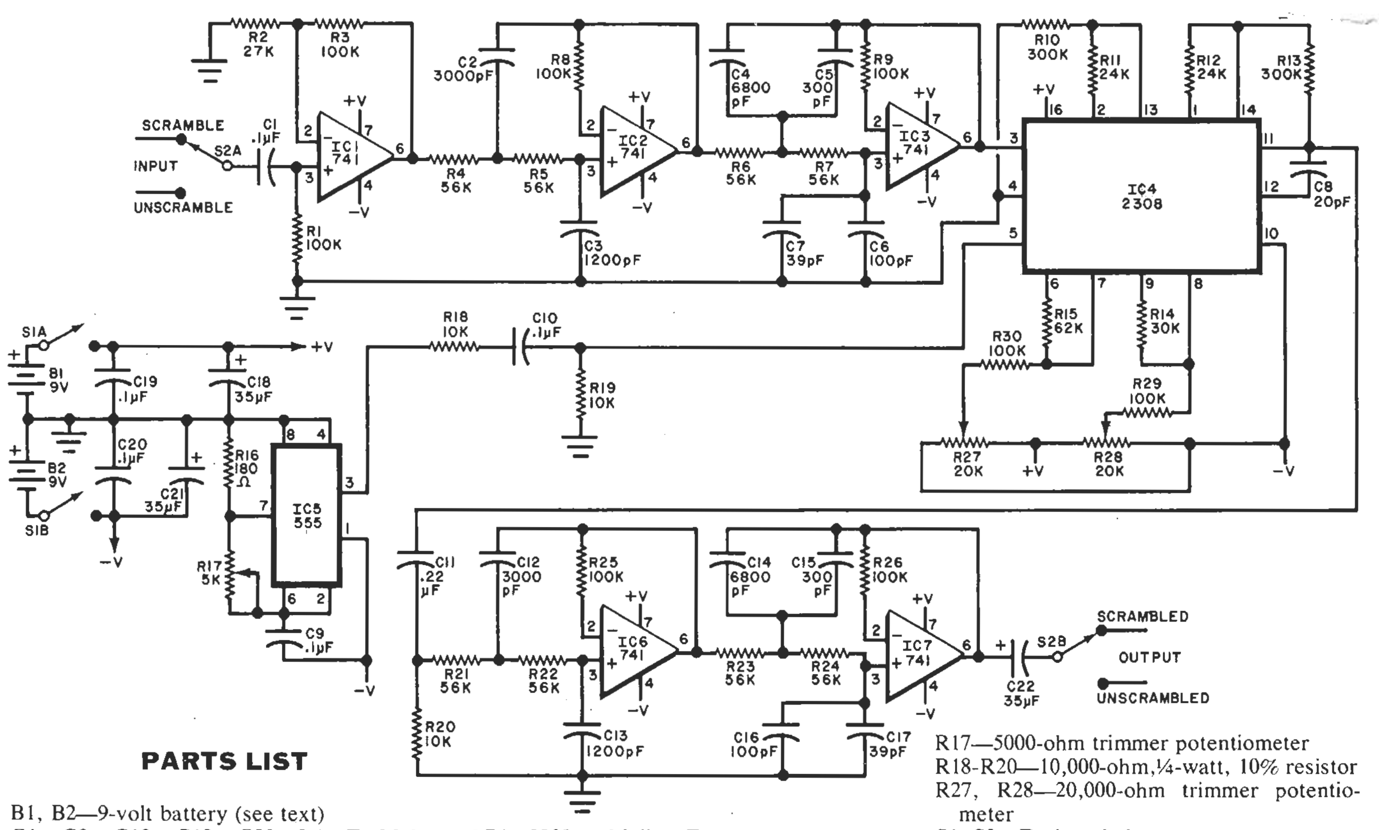


Fig. 1. Simplifed block diagram of scrambler using radio link, but transmitter and receiver can be direct-coupled.



PARTS LIST

B1, B2—9-volt battery (see text)
C1, C9, C10, C19, C20—0.1-µF Mylar capacitor
C2, C12—3000-pF, 5% capacitor
C3, C13—1200-pF, 5% capacitor
C4, C14—6800-pF, 5% capacitor
C5, C15—300-pF, 5% capacitor
C6, C16—100-pF, 5% capacitor
C7, C17—39-pF, 5% capacitor
C8—20-pF, 5% capacitor
C11—0.22-µF, Mylar capacitor
C18, C21, C22—35-µF, 25-volt electrolytic capacitor
IC1, IC2, IC3, IC6, IC7—741 op amp
IC4—2308 multiplier (Exar)
IC5—555 timer
R1, R3, R8, R9, R25, R26, R29, R30—100,000 ohm, ¼-watt, 10% resistor
R2—27,000-ohm, ¼-watt, 10%resistor
R4-R7, R21-R24—56,000-ohm, ¼-watt, 5% resistor
R10, R13—300,000-ohm, ¼-watt, 5% resistor
R11, R12—24,000-ohm, ¼-watt, 5% resistor
R14—30,000-ohm, ¼-watt, 5% resistor
R15—62,000-ohm, ¼-watt, 5% resistor
R16—180-ohm, ¼-watt, 10% resistor
R17—5000-ohm trimmer potentiometer
R18-R20—10,000-ohm,¼-watt, 10% resistor
R27, R28—20,000-ohm trimmer potentiometer
S1, S2—Dpdt switch
Misc.—Suitable chassis (Bud SC2132), battery holders and connectors, mounting hardware, suitable input/output jacks, etc.
Note—The following are available from Northwest Engineering Co., 801 Duchess Rd., Bothell, WA 98011: Pc board (N007-PCB) at $7; IC4 (N007-MULT) at $8.50; case, switches, input/output jacks, batteries (N007-CASE) at $17.50; pc board and components (N007-PK) at $33.50. All postage paid in U.S.via parcel post or UPS.

Fig. 2. Complete schematic of scrambler.

comes part of the decoder. The encoded signal passes on to a modulator where it is impressed on a carrier or other transmission medium. At the receiving end, the reverse of the process occurs.

Encoding Techniques. There are basically two types of techniques used for encoding communication signals to secure them against immediate unauthorized decoding by eavesdroppers. They include a variety of analog and digital approaches.

Simple Speech Inverters: Inverters transpose the high-frequency components of the speech signal to low frequencies. This is done before carrier modulation in radio transmitters or before line transmission in telephone systems. A stable audio oscillator operating at about 3000 Hz can feed a balanced modulator along with the voice signal. The lower sideband generated reflects the mirror image of the speech frequencies. (See Fig. 2.)

Bandsplitters: Bandsplitters divide the audio speech frequencies into several ranges, permitting the narrow frequency bands to be rearranged as shown in Fig. 3. Bandsplitting is usually accomplished with the aid of narrow-bandpass filters. The outputs of the filters are mixed or shifted in frequency, then added together so that some ranges are translated in frequency.

Combined Bandsplitters: Combination techniques offer added security to the basic bandsplitting approach. Not only can the speech frequencies be split and translated, but some can be inverted as well. The order in which the frequency ranges are recombined can also be changed with time as illustrated in Fig. 4. (Some manufacturers term these "rolling-code" bandsplitters and rearrange the frequency band order several times.) Using more bands makes this approach more difficult to decode, and changing the band sequence a greater number of times per second makes the system more secure.

Penalties of the combined bandsplitting technique are that the recovered speech begins to sound unnatural when frequency slices increase in number and closer synchronization tolerances must

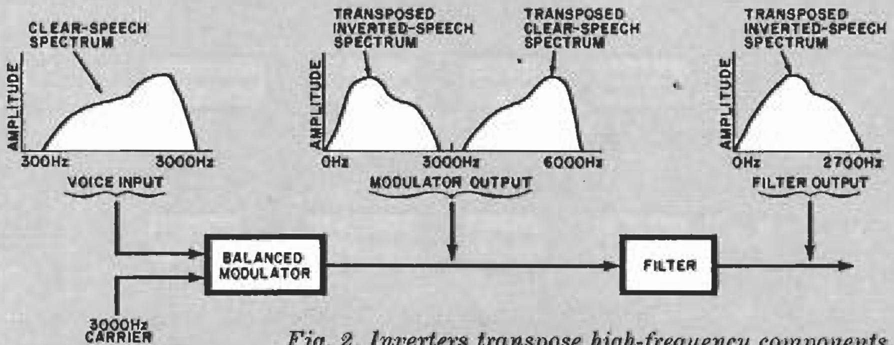
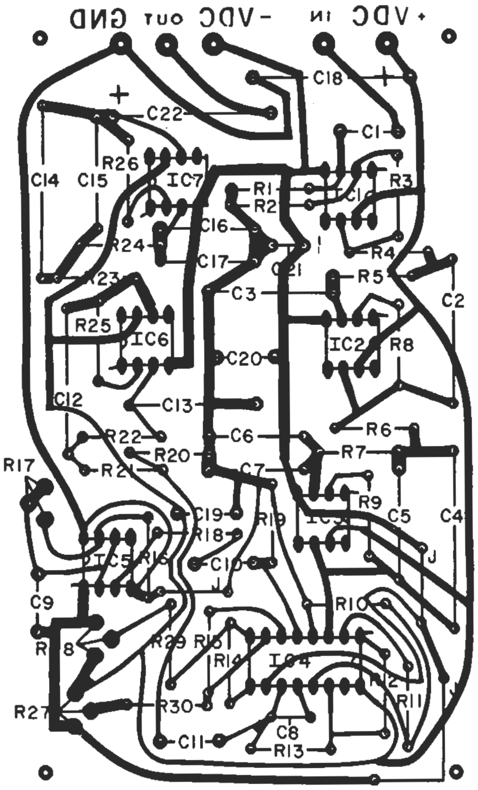


Fig. 2. Inverters transpose high-frequency components.

dances as low as 2000 ohms. It can be used with most amplifiers, for speaker applications, or a set of 2000-ohm headphones.

Construction. To ensure that the active filters are properly tuned, it is recommended that 5% resistors and capacitors be used for the critical components (*R4-R7*,



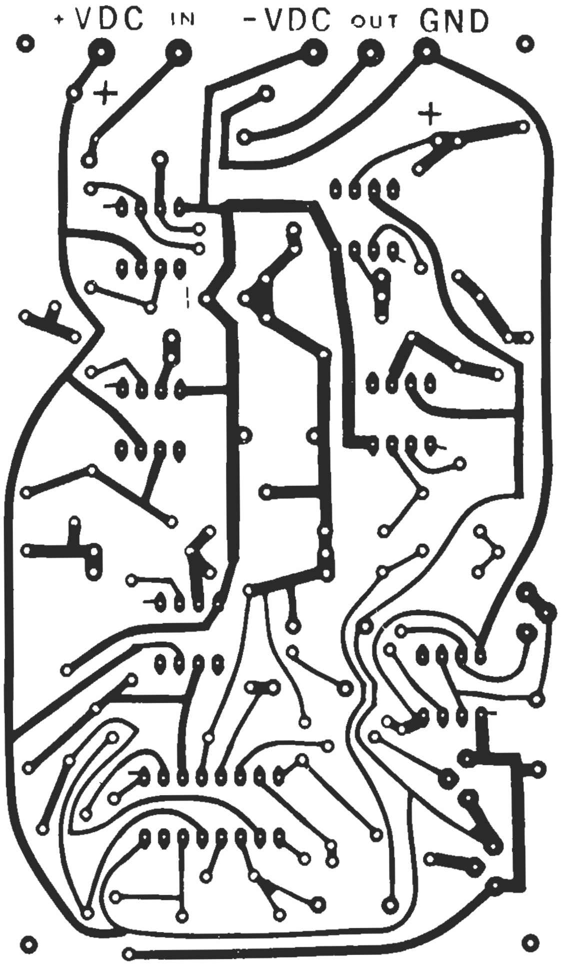


Fig. 3 Actual-size foil pattern for scrambler is shown above at right, component layout at left.

be exercised during band rearrangement.

Masking Techniques: Constant audio tones, or coded sequences of tones, are often used with bandsplitting and inversion. The tones, subtracted from the signal during recovery and decoding, can be higher than or the same level as the intelligence signal (voice). If they are higher in level, they can reduce range since they make up much of the sideband energy and, hence, reduce the system's overall signal-to-noise (S/N) ratio.

Pseudo-random noise generators can also be used in masking techniques. In practice, the human ear and brain provide such selective filtering that in a system supposedly offering about 400 word codes, only 10 or 12 might be all that are really different to a listener. To someone trained in decrypting such systems, often 50 percent of the information can be extracted in just a few attempts. Even inverted speech becomes intelligible after training. Some languages are often less affected than others by these conventional scrambling techniques.

The above mentioned analog encoding techniques have been discussed with

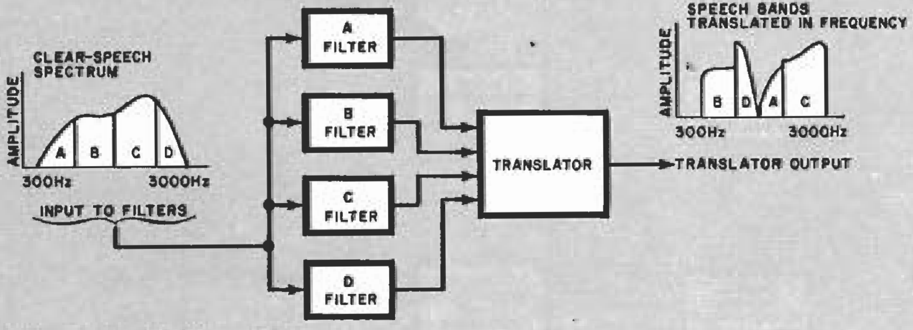


Fig. 3. Bandsplitters divide signal and then recombine.

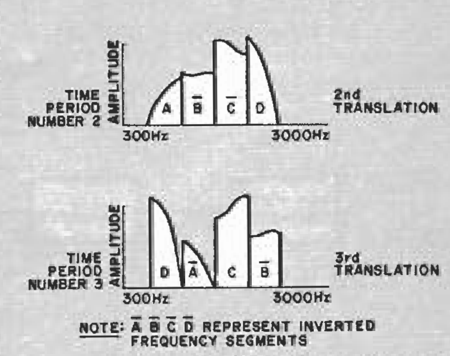


Fig. 4. Combined bandsplitters split and translate speech frequencies to provide more security than simple systems.

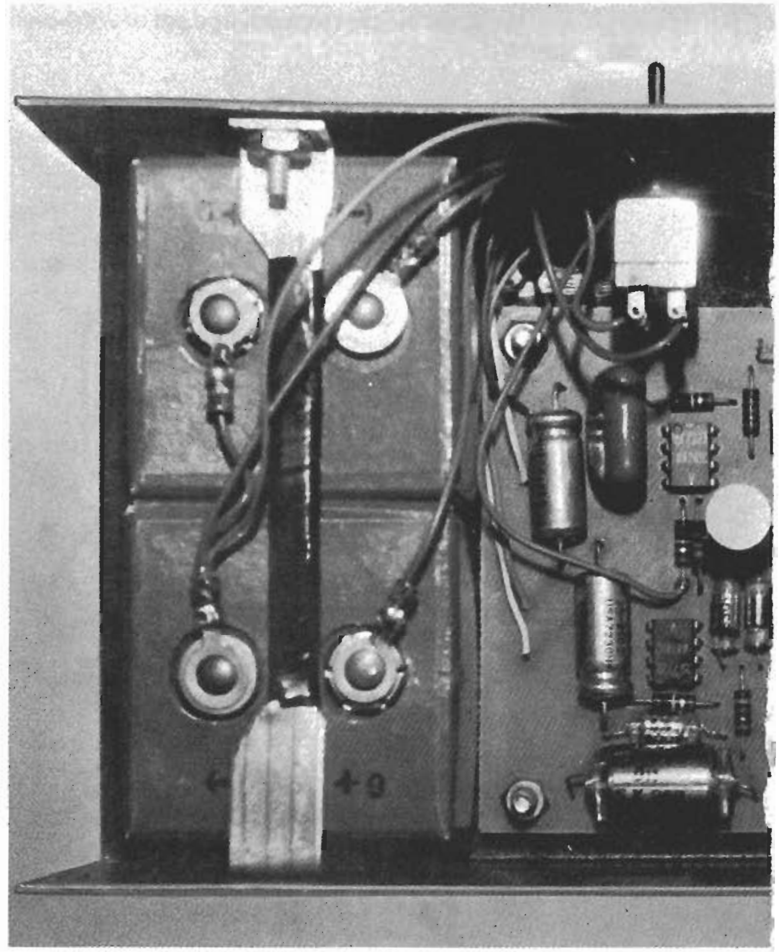
R21-R24, C2-C7, and C12-C17). The gain-controlling resistors for the multiplier (R10-R13) should also have 5% tolerances.

Although the circuit can be wired point-to-point on perforated board, it is preferable to use a pc board such as that shown in Fig. 3. Be sure to observe the notch codes on the IC's and the polarities of the electrolytic capacitors so that they are properly installed.

In using a pc board, note that 8-pin DIP 741 op amps are required. If point-to-point wiring is used, other versions of the 741 (round, 14-pin DIP or dual) can be substituted.

Mount the batteries in holders in any convenient location in the chassis. If desired, the power can be obtained from an external supply between ±6 and ±15 volts. The supply voltage is not critical as far as circuit operation is concerned, but the maximum input signal level and the overall gain will vary for different supply voltages. The gain can be adjusted by changing the values of R3 (raising it to increase the gain) and R18 (lowering it to increase oscillator signal level).

The input and output connectors on the front panel must be chosen to suit the application.



Adjustment. For proper operation, the oscillator should be adjusted to 3500 Hz. If an accurate counter or oscilloscope is available, R17 can be adjusted while monitoring the output of IC5 (pin 3). An alternate method of adjustment based on the accuracy of the lowpass filter can be used if necessary. With the input shorted to ground and R17 turned fully counterclockwise, adjust R28 to get an output of 0.15 volt on an ac voltmeter. Now adjust R17 until the output voltage falls to 0.026 volt. The oscillator is now adjusted to approximately 3500 Hz.

To balance the multiplier, it will be necessary to adjust R27 and R28 while monitoring the scrambler output with an ac voltmeter or a set of headphones. With no signal

reference to voice signals. However, the same techniques can also be used to scramble data. They can be applied after the data is fed into a modem and converted to a series of audio tones for analog transmission.

The most sophisticated, expensive, and secure communication systems are digital. In Fig. 5 is shown a typical digital voice-encoding system. At the heart of the security system are the digital encoder/modulator and its counterpart, the decoder/demodulator. These systems combine some digital key with the digitized signal. In many cases, synchonization requirements can be very stringent.

The complexity of the digital encoder varies with the degree of security required. Requirements can range from several years security for high-level governmental communications to a few hours or minutes in the field for military tactical operations. A few hours to several days generally suffice for most industrial and commercial activities.

The main disadvantages of digital encoding systems are their high cost, large size, and often greater bandwidth requirements on the transmission links. On the other hand, such systems provide the highest degree of security available for both voice and data. There is also high flexibility in transmission routing and voice, and data links are often compatible.

Most government systems are classified. Hence, no details of their design or operating principles can be provided here. There is a book, however, *The Codebreakers* by David Kahn, that goes into some detail on the subject, using material from unclassified sources.

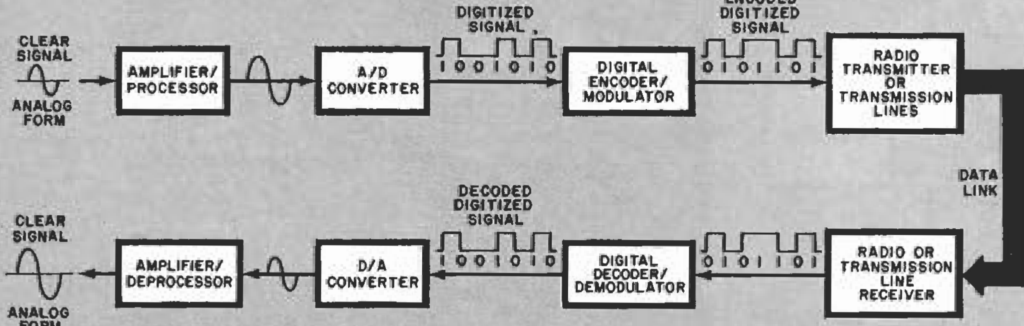


Fig. 5. Diagram of digital voice encoder which provides the best security.

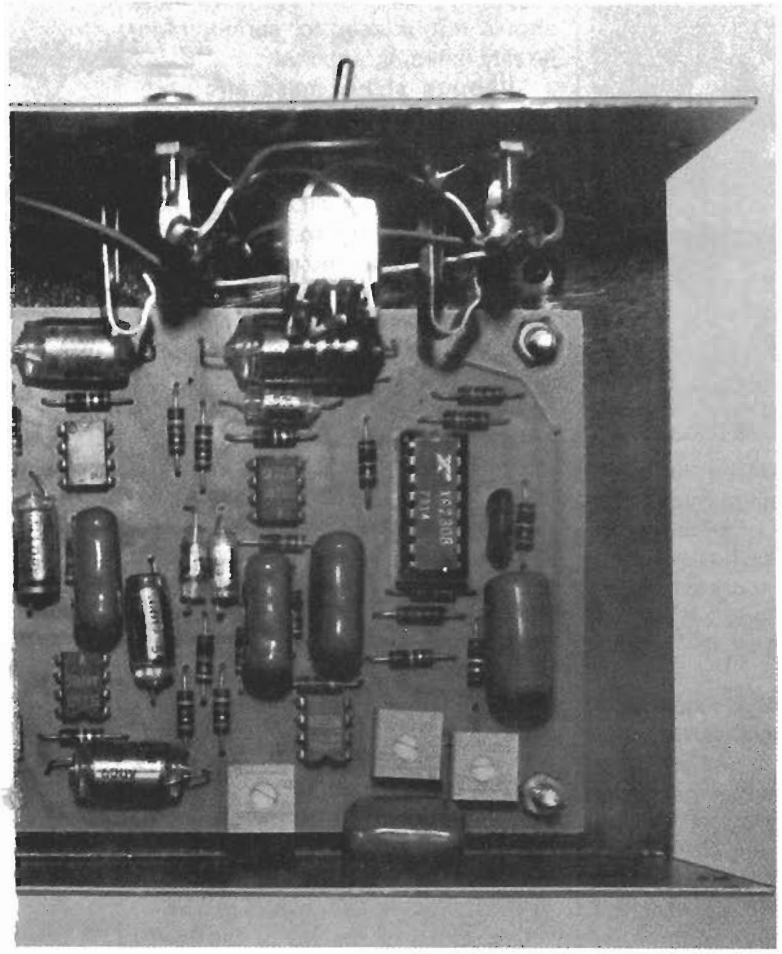


Photo shows how the prototype was assembled. Batteries are at left, but an external supply can be used if desired.

input, adjust *R28* for minimum output (near the middle of its range). To adjust *R27*, it is necessary to disable the oscillator by shorting across capacitor *C9*. With an input signal of about ½ volt (1000 to 3000 Hz), adjust *R27* for minimum output signal. The scrambler is now ready for use.

Use. A crystal microphone can be connected to the input of the scrambler with the output (with unity gain) connected to the MIC input of a tape recorder or transmitter. If headphones are used, the scrambled signal is connected to the unscrambler. Alternatively, the unscrambler can be connected between the recorder preamplifier and speaker amplifier (or receiver detector and audio amplifier).

The multiplier portion of the circuit can be used as a single-sideband modulator. The multiplier can be modified to operate with carrier frequencies as high as 5 MHz. Pins 13 and 14 of *IC4* should be shorted to pin 4, with *R10* through *R13* removed, a 5100-ohm resistor connected betwen pins 4 and 15, and pin 2 connected to pin 16. With *IC5* removed, the desired carrier signal can be coupled into pin 4 (using about 1 volt). The output of *IC4*, from pin 15, can be coupled into a SSB filter to remove the unwanted sideband.

The multiplier can also be used as a variable-gain amplifer, or remote volume control. If the oscillator is removed, the gain of the multiplier can be controlled by varying the dc level on pin 5 of *IC4* from 0 to 5 volts. One way to accomplish this is to include a 100,000-ohm potentiometer in series with a 100,000-ohm resistor across the positive supply. Remove *IC5, R18,* and *R19.* Connect C10 from *IC4* (pin 5) to ground. Connecting the wiper from the potentiometer to *IC4* (pin 5) will provide the desired variable voltage. For wide-band or hi-fi use, remove the two active filters. A control range of 50 dB can be obtained with low distortion. ◈

Cryptanalysis. Most industrial spies record an intercepted message on tape and then apply successive demodulation and/or decrypting techniques. Several switched filter banks and balanced modulators are used to decrypt band splitting, while the eavesdropper uses his ear and brain to tell him when he is getting close to his goal.

Computers are no doubt used in digital cryptanalysis. They make a series of possible solutions of transpositions and substitutions easy to print out. Also, it is easy for the computer to look for patterns in given languages by determining which symbols occur most often. In straight English text, the frequencies of occurrence of alphabet letters are as follows:

e = 1000	d = 392	g = 168
t = 770	l = 360	b = 120
a = 728	u = 296	k = 88
i = 704	c = 280	j = 55
s = 680	m = 272	v = 52
o = 672	f = 236	q = 50
n = 670	w = 190	x = 26
h = 540	y = 184	z = 22
r = 528	p = 168	

(In any average piece of English writing, letters are found in a standard ratio that varies only slightly from message to message. If the message is long enough, it can be decoded by use of letter-frequency tables. Since e is the most common letter, all other letters are given in relation to it. Hence, if e occurs 1000 times, the other letters will be found to have the approximate ratios given above.)

Future Trends. As one might expect, all of the communications security equipment currently being designed relies heavily on solid-state electronics. Most of the industrial and commercial systems still employ discrete components, but the government is forging ahead with more integrated circuits.

The trend is toward more and more sophisticated systems, with the demand for tighter security increasing, as is the technical competence of the would-be eavesdropper. Non-government users are beginning to look at digital techniques. As lower prices and new IC's to perform digital-to-analog and analog-to-digital conversions become widespread, this trend toward digital systems will undoubtedly accelerate.

The Motorola MC1408 D/A converter IC is representative of the new integrated circuits on the market today. A practical encoder would combine an MC1408 with other logic and/or speech-processing circuits to give the particular results desired. Most filtering and speech processing is accomplished with the aid of operational-amplifier IC's.

The encoding and decoding circuits themselves can employ many of the standard shift registers, read-only memories (ROM's), random-access memories (RAM's), and gate arrays already in common use. These types of IC's are available in today's popular logic families.

At one time, governments were the only users of secure communication systems. Later, commercial organizations became security-conscious in their efforts to thwart industrial espionage. Now, the private citizen, concerned over bugging operations and other invasions of privacy, has taken up the security banner. For him, the voice scrambler seems made to order. ◈

AUDIO SCRAMBLING SYSTEM

Here's a high-tech version of the old "Captain Midnight" secret decoder ring. Only this time out you scramble and unscramble sound instead of written messages.

KEVIN LINDELL

PERHAPS THE MOST SERIOUS PROBlem with any kind of radiotelephone transmission is its inherent lack of privacy. Anyone can monitor the signal—using a scanner or a conventional receiver—and eavesdrop on both sides of the conversation.

Although there may be legal considerations either in effect now or under consideration that would limit or prevent the unauthorized reception of some or all radiotelephone signals, the fact remains that there is unauthorized eavesdropping that no amount of laws, rules, or regulations is going to stop.

To thwart both eavesdropping and the unauthorized use of information that might be attained, many communication systems make the signal unintelligible through some kind of scrambling; and only those specially-equipped receivers having matching decoder circuits can unscramble the signal.

One relatively simple but effective technique that's used to scramble voice transmissions is known as "frequency inversion." Briefly, in frequency inversion a fixed-frequency scrambling "carrier" is mixed with the audio signal in such a way that the original audio spectrum is translated into a different spectrum, and the resulting transmitter modulation sounds like duck chatter. As a matter of fact, the scrambled sound is often called "Donald Duck." Even if the scrambled duck chatter is translated back to the vicinity of the original spectrum, *but not necessarily back to the original frequencies*, the audio will still be unintelligible.

Frequency-inversion scrambling is commonly used by the police for radio communications in order to prevent casual listeners from eavesdropping on sensitive messages. Private enterprises also use similar methods to scramble telephonic communications to prevent the interception of proprietary information.

Your own scrambler

If you have a need to scramble and descramble any kind of radio or telephone voice message, even a cassette tape that is sent through the mail, you'll find you can do the job quickly and cheaply with the combination scrambler/descrambler unit described in this article. The scrambled output, whether by radio, telephone, or tape, sounds similar to the duck chatter that is produced when a single-sideband radio transmission is received by an AM receiver.

The scrambler/descrambler uses a device called a *balanced modulator* to produce frequency-inversion scrambling. A balanced modulator is a special kind of mixer that will produce an output containing sidebands when fed both a carrier frequency and modulation. The upper sideband consists of the *sum* of the carrier frequency and the modulating frequencies while the lower sideband consists of the *difference* frequencies. It is the difference frequencies in the lower sideband that are used for scrambling.

The balanced modulator

The balanced modulator inherently tries to null the two original input frequencies in the process of creating new products at its output.

If the carrier and modulation waves are of the form:

$$A_{PEAK}\sin(\omega t) \quad (1)$$

where, A = Amplitude, $\omega = (2\pi f)$, f = frequency, and t = time, then, multiplying two such waves produces:

$$A_{OUT} = (A_c)(A_m)(\sin\omega_c t)(\sin\omega_m t) \quad (2)$$

where, m = modulation frequency, and c = carrier frequency.

Recalling the trigonometric identity:

$$(\sin A)(\sin B) = \tfrac{1}{2}[\cos(A-B) - \cos(A+B)] \quad (3)$$

substituting equation (3) into (2) produces the following equation, which clearly shows the sidebands:

$$A_{OUT} = \frac{A_c A_m}{2}\left[\cos 2\pi(f_c - f_m)t - \cos 2\pi(f_c + f_m)t\right] \quad (4)$$

where

$$\cos 2\pi(f_c - f_m)t$$

is the lower sideband and

$$\cos 2\pi(f_c + f_m)t$$

is the upper sideband

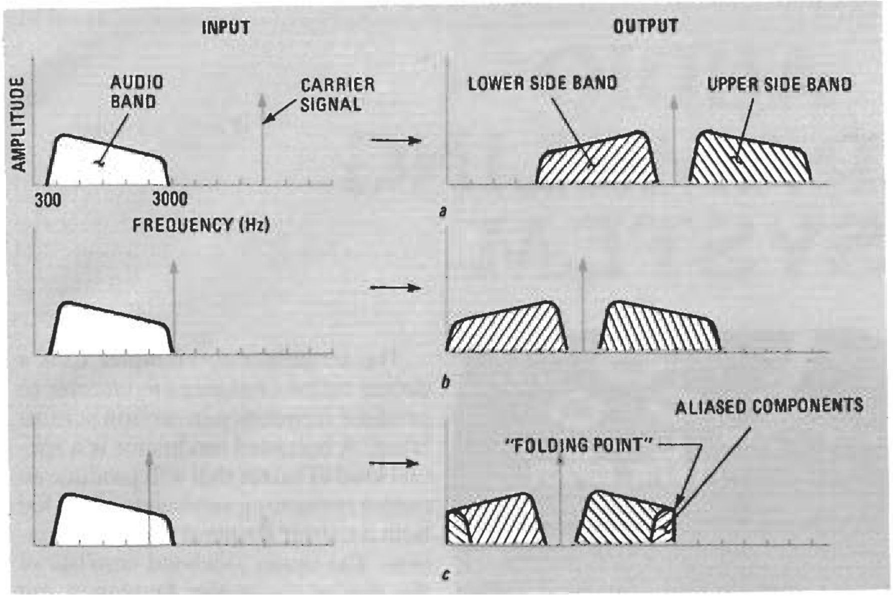


FIG. 1—THE MODULATION WILL FOLD BACK ON ITSELF if the carrier is within the modulation passband. *a* shows how the modulation is inverted and shifted higher in frequency if the carrier signal is displaced from the highest modulating frequency. In *b* the carrier is just above the audio band so the modulation is inverted, but the difference frequencies occupy essentially the original passband. In *c* the carrier is within the audio band, causing some modulating frequencies to fold back within the audio band.

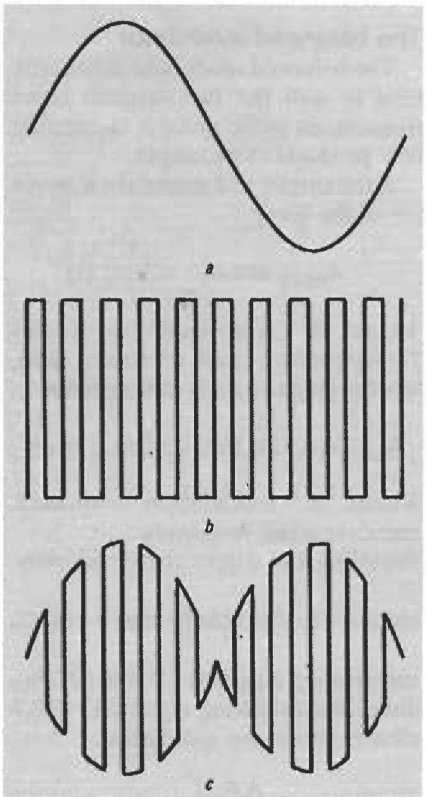


FIG. 2—HOW THE SCRAMBLER'S modulation works. If the audio signal shown in *a* is used to modulate the square-wave carrier in *b*, the resultant output is the signal shown in *c*: the original audio chopped by the carrier.

If the carrier frequency is not higher than the audio range to be inverted, then a distortion that is known as *aliasing* will occur in which the audio frequencies appear to "fold over" on themselves. Figure 1 shows how the aliasing effect might affect a scrambler/descrambler. Figure 1-*a* might be considered normal modulation/carrier positioning. As the carrier frequency moves closer to the audio band (Fig. 1-*b*), the sideband spectrum is shifted lower. When the carrier is within the audio range (Fig. 1-*c*), it causes the output spectrum to produce false, or aliased, products that are "folded" around the carrier frequency.

There are two basic ways to make a balanced modulator. One method uses devices that have non-linear characteristics, such as a diode's voltage/current relationship. That method requires a critical matching of the components to achieve good performance. The second method, which is used in the scrambler/descrambler, uses time-variant devices having two states, either *on* or *off*. The two-state characteristic can be used to pass or not pass a signal through a circuit or a circuit path. If the signal can be toggled through a symmetrical pair of switches whose outputs are summed in a balanced manner (i.e., with equal magnitude and opposite sign), the result will be the signal multiplied in time by the switching rate.

The balanced modulator in our scrambler/descrambler uses a quad FET IC having four closely-matched switches in a single package (which reduces the component-matching problem). The circuit also uses an op-amp to provide the balanced summing operation. The switches are controlled by the clock circuit. Toggling the switches rapidly creates a constant amplitude and frequency square-wave carrier for the balanced modulator.

How it works

Figure 2 shows how the scrambler works in the time-domain. Fig. 2-*a* shows a typical sinewave audio-input signal. Figure 2-*b* shows the square-wave carrier. If the input signal is chopped by the carrier into several smaller pieces at the carrier rate and the phase is reversed at each chopped

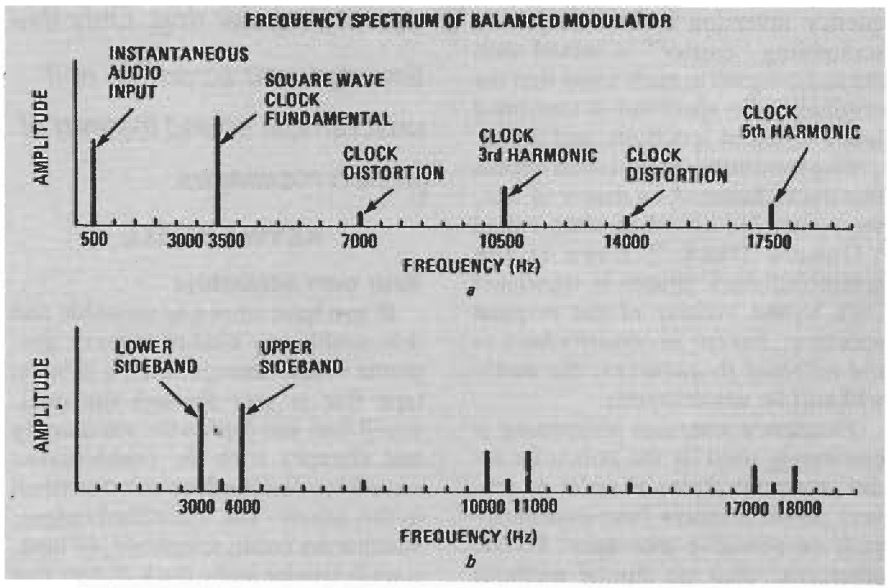


FIG. 3—THE SQUARE-WAVE CARRIER produces unwanted audio products in the form of harmonics and sidebands, shown in *a*. Those products must be filtered out. The resulting frequency spectrum, shown in *b*, has components located at the modulation frequencies both above and below each carrier harmonic.

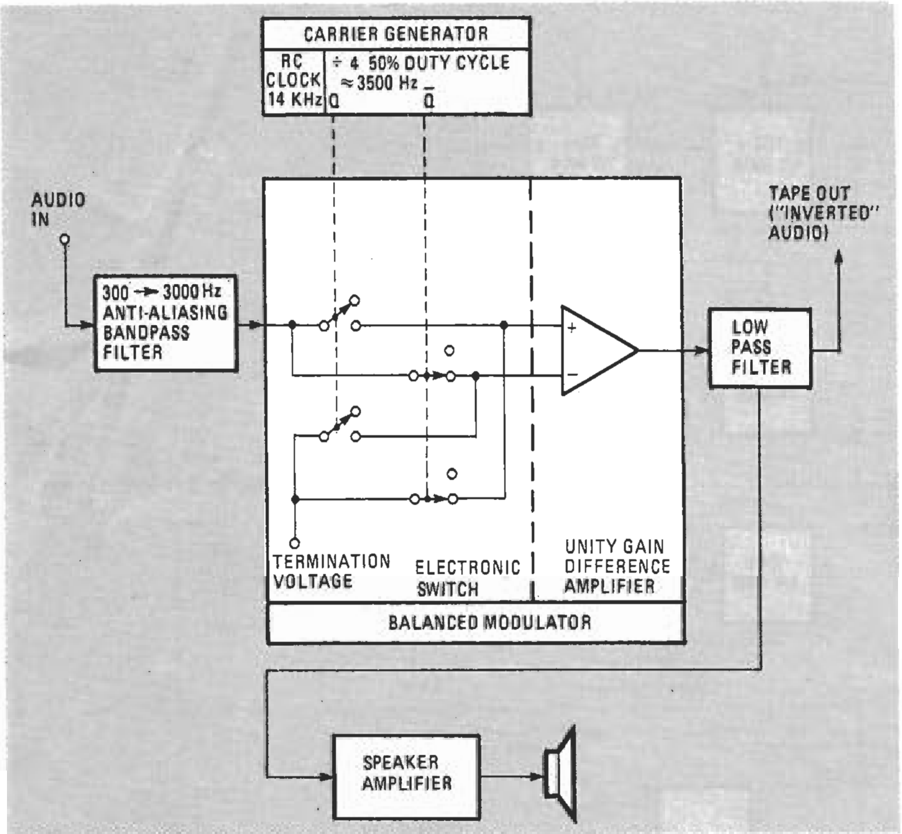


FIG. 4—FUNCTIONAL DIAGRAM OF THE SCRAMBLER. The switching is actually done by a balanced modulator that is driven from the carrier generator.

interval, the resulting output will appear as shown in Figure 3-*c* when viewed on an oscilloscope.

As shown in Fig. 3-*a*, the square-wave carrier also produces unwanted audio products in the form of harmonics and sidebands. Those products add to the distortion and must be filtered out in order to return the audio signal to its original form.

Mixing the squarewave with the audio-input signal results in an output that has sideband components centered around each harmonic of the square wave. As shown in Fig. 3-*b*, the resulting frequency spectrum has components located at the modulation frequencies both above and below each carrier harmonic, but there are no components at the carrier frequency or its harmonics. Filtering out the lower sideband, which is below the fundamental frequency of the squarewave, produces the scrambled audio output.

As long as the carrier switching-rate is maintained slightly above the normal audio range, the scrambled audio will still be audible, but low input tones will produce high output tones, and vice-versa, making the final output sound highly distorted and unintelligible. If an identical method is used to demodulate the distorted speech, the signal will be restored to its original form.

A graphic representation of how the scrambler/descrambler affects the normal audio input is shown in Figure 3-*b*. The carrier, or switch-toggle rate, is set at 3500 Hz. The audio input at the instant shown in this example equals 500 Hz. Note the sidebands that are produced. The upper sideband, also called the sum frequency, is equal to the carrier frequency plus the audio frequency, which, for this example, is 4000 Hz. (3500 Hz plus 500 Hz.) The lower sideband, or difference frequency, is 3000 Hz. (3500 Hz minus 500 Hz). Having selected the lower sideband as the scrambled audio, the 500 Hz tone, which was put into the scrambler, is changed into a 3000 Hz tone. Similarly, a 3000 Hz audio input tone produces a 500 Hz output tone. Carrying that process on for the entire spectrum of input audio frequencies produces the scrambled result. Reversing the process effectively descrambles the audio. The original carrier tone may still be heard when there is no audio modulation present—although at a volume much below that of the scrambled audio level. Carrier leak-through is due to the fact that the carrier frequency is in the audible range and that the balanced modulator is not perfectly balanced.

The major components

Figure 4 is a block diagram of the scrambler's five major sections. The CARRIER GENERATOR is an RC clock and divide-by-four counter that produces the switching signals for the balanced modulator.

The ANTI-ALIASING BANDPASS FILTER conditions the audio-input signal by limiting the frequencies fed into the balanced modulator to the nominal range of 300–to 3000 Hz, thereby reducing the high-frequency components that would cause aliasing distortion. Without the filter the balanced modulator would include erroneous information that would appear in the output signal as distortion.

The BALANCED MODULATOR is the heart of the scrambler/descrambler. Its purpose is to feed the conditioned audio input alternately, at the timing-generator rate, to the inverting input and then the non-inverting input of a differential amplifier. That process mixes the conditioned audio with the timing generator's square-wave signal, thereby creating a composite output signal that contains several sideband and harmonic frequencies.

The LOWPASS FILTER removes all but the first lower-sideband frequencies from the balanced modulator's output. The filter's output is "inverted audio," the scrambled signal.

The SPEAKER AMPLIFIER drives an internal speaker. When the device is used as a scrambler the speaker reproduces the scrambled output from the lowpass filter. When the device is used as a descrambler the speaker reproduces the descrambled sound. Alternately, the sound can be fed through the TAPE OUTPUT connection to an external amplifier, speaker, tape recorder, or whatever.

Circuit description

Figure 5 shows the schematic of the scrambler/descrambler. Integrated circuit IC1 is an astable 7555-timer circuit running at approximately 14 kHz. The timer's frequency is determined by R1, R2, and C2. Small changes to the frequency can be made by adjusting R1, which is an externally-accessible multi-turn trimmer.

The output from IC1 is fed to the clock input of IC2, a dual D-type flip-flop that is used to divide the 14-kHz clock output by a factor of 4 (÷2 +

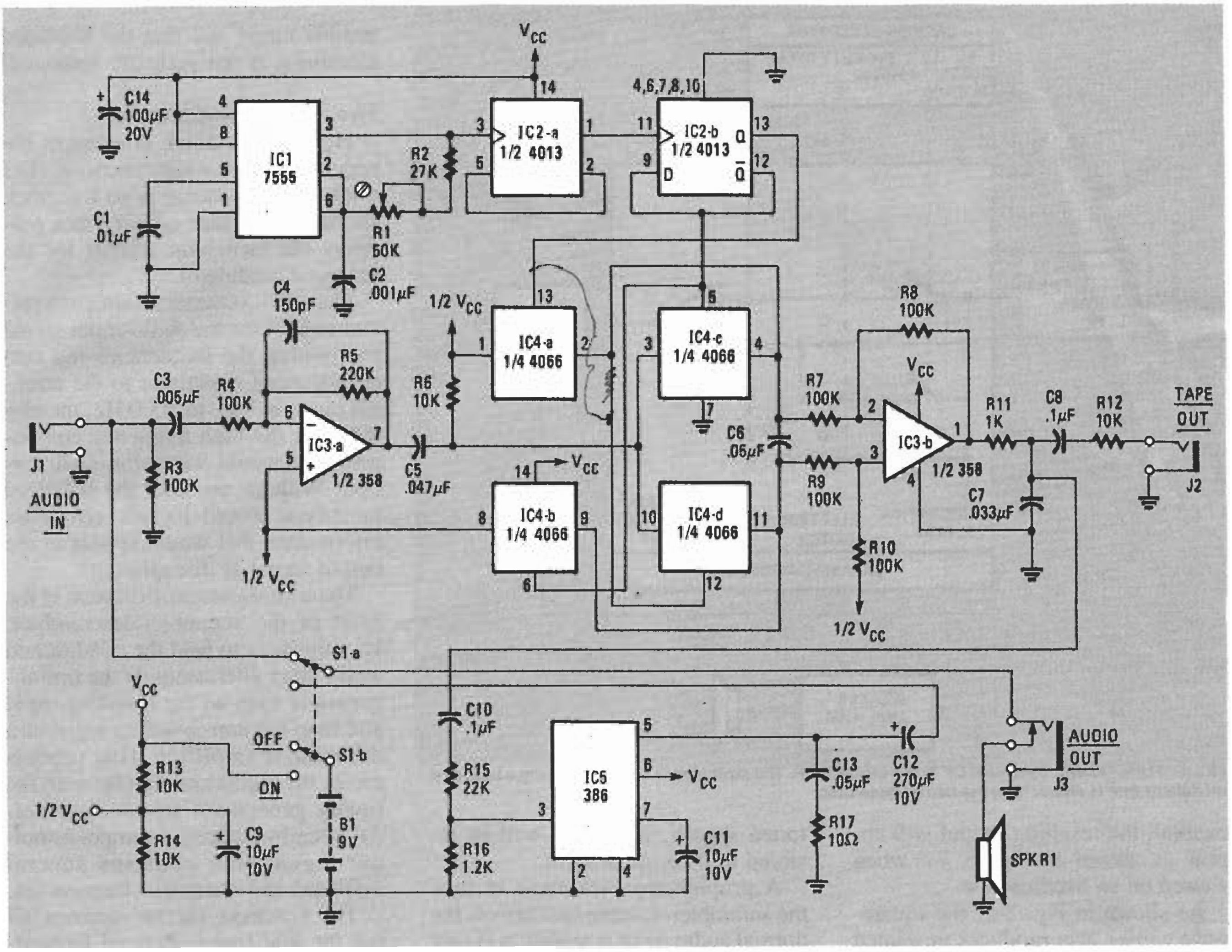


FIG. 5—THE COMBINATION SCRAMBLER/DESCRAMBLER. Switch S1 controls the power through one section and bypasses the scrambler through its other section.

÷2). The division creates a 3.5-kHz 50% duty-cycle square wave at IC2 pin 13, and an identical but inverted waveform at pin 12. The two squarewave signals are used as carriers to control IC4, a quad analog switch that functions as the balanced-modulator's switching network.

The other input to the balanced modulator is the audio signal from J1 that is to be scrambled. The input signal should be derived from a low-impedance source such as a tape-player's headphone or speaker-output jack. Using a line-level or AUX signal source is not recommended because the scrambler's speaker is connected directly to the audio input when the scrambler unit is off, and the low impedance of the speaker would load down a high impedance line or AUX signal source. The input signal's frequency range is limited to nominally 300–3000 Hz by bandpass filter IC3-a.

At any given time the squarewave carrier will turn on either switches IC4-a and IC4-d, or IC4-b and IC4-c at the 3.5-kHz rate. When switches IC4-a and IC4-d are on, IC4-d passes the audio input signal to the non-inverting input of differential amplifier IC3-b, and IC4-a terminates the inverting input. Switches IC4-c and IC4-d work similarly on the other half of the squarewave carrier cycle.

Unity-gain differential-amplifier IC3-b multiplies the audio input by a factor of plus or minus one, depending on the state of the IC4 switches. Resistors R7 and R8 set the gain on the inverting input while resistors R9 and R10 set the gain on the non-inverting input.

The balanced-modulator output, IC3 pin 1, is fed through the R11/C7 low-pass filter, which passes only the scrambled audio to TAPE OUT jack J2. The output level from J2 will depend on the input level to the scrambler. A sample of the signal fed to J2 is also fed to audio power amplifier IC5. The output of that device drives SPKR1.

Switch S1 turns the scrambler circuit *on* and *off*. When switch S1 is *off*, section S1-a connects the audio input directly to the speaker, thereby bypassing the audio scrambler circuit so that normal, unscrambled audio, can be monitored.

Construction

A template for the printed-circuit board is shown in PC Service. A pre-drilled board is available from the source given in the Parts List. Figure 6 shows how the components are installed on the PC board.

Although there is nothing unusual about the assembly, standard CMOS component-handling precautions should be used avoid damage from static discharges. Whether you choose to use a large or a small cabinet, installation of the switch and the jacks is easier if they are pre-wired to the PC board before being mounted on the case.

If you intend to unscramble mes-

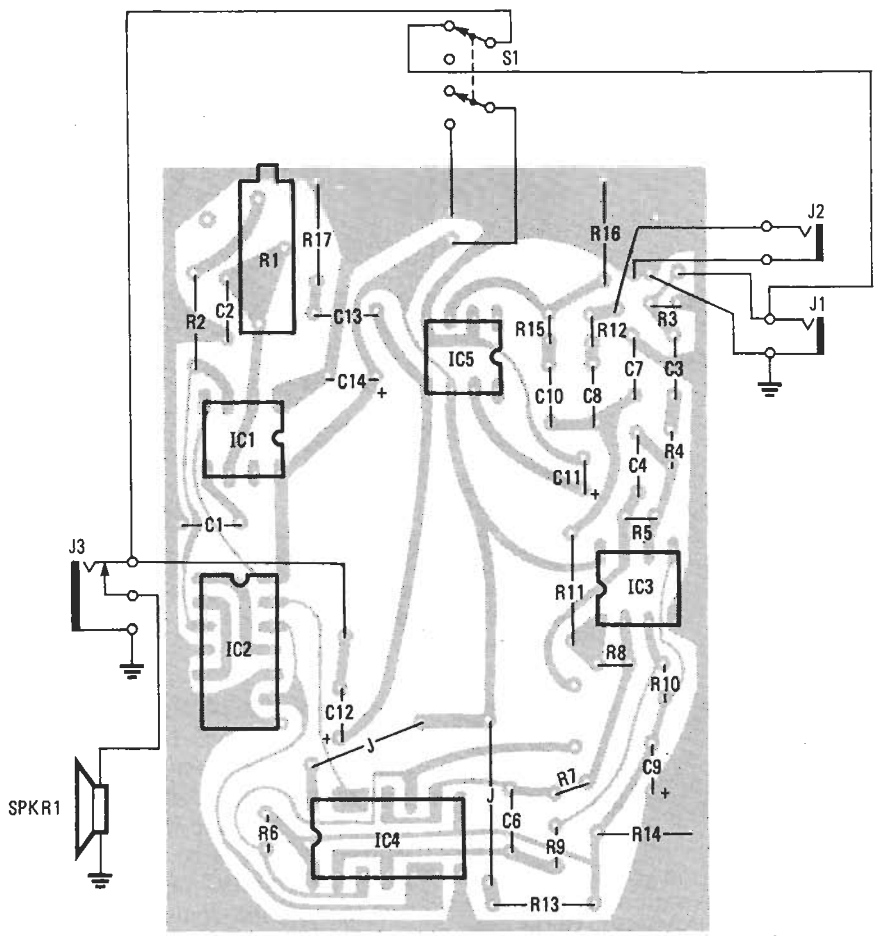


FIG. 6—THE PARTS LAYOUT. Keep the center of the board free so it can fit over the speaker.

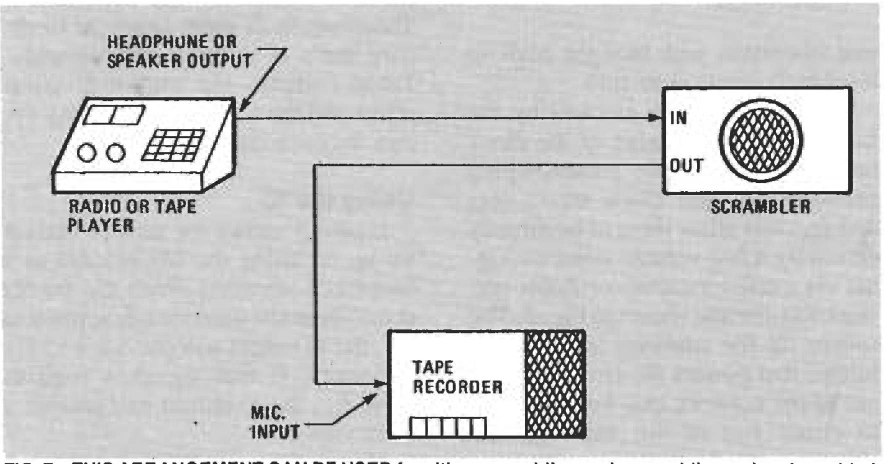


FIG. 7—THIS ARRANGEMENT CAN BE USED for either scrambling or descrambling a signal provided by a radio or tape player.

PARTS LIST

All resistors are ¼-watt, 10%, unless otherwise noted.

R1—50,000 ohm, 10-turn trimmer potentiometer
R2—27,000 ohms
R3, R4, R7–R10—100,000 ohms
R5—220,000 ohms
R6, R12–R14—10,000 ohms
R11—1000 ohms
R15—22,000 ohms
R16—1200 ohms
R17—10 ohms

Capacitors

C1—.01 µF, 100 volts, ceramic disc
C2—.001 µF, 100 volts, mica
C3—.005 µF, 100 volts, ceramic disc
C4—150 pF, 100 volts, ceramic disc
C5, C6, C13—.05 µF, 100 volts, ceramic disc
C7—.033 µF, 100 volts, ceramic disc
C8, C10—0.1 µF, 100 volts, ceramic disc
C9, C11—10 µF, 10 volts, electrolytic
C12—220 µF, 10 volts, electrolytic
C14—100 µF, 20 volts, electrolytic

Semiconductors

IC1—7555, CMOS timer
IC2—4013, dual D-type flip-flop
IC3—LM358, dual op-amp
IC4—4066, quad analog switch
IC5—LM386, audio power amplifier

Other components

B1—9-volt battery
J1, J2—Miniature phone jack
J3—Two-circuit miniature phone jack
S1—DPDT toggle switch
SPKR1—2⅛" speaker

Miscellaneous: battery terminals, battery holder, printed-circuit board materials, enclosure, wire, solder, etc.

sages from several sources using different scramblers, it's possible that trimmer potentiometer R1 might have to be re-adjusted for each scrambling source; hence, to minimize headaches later on, R1 should be installed so that it is conveniently accessible from outside the cabinet.

Tuning and adjustment

Trimmer potentiometer R1, which is used to tune the square-wave scrambling/descrambling carrier signal, should initially be set to approximately its center position. If the scrambling device that was used to scramble the audio is also used for descrambling, no further adjustment will probably be required. If different scrambler units are used, as is sure to be the case in a typical two-way communication setup, the receiving unit's R1 will have to be tuned manually until the scrambled audio is successfully descrambled and can be clearly understood.

Applications

The device can be used in many applications, although its use may be restricted by local and/or Federal laws. It should only be connected to the telephone line through an FCC-approved interface, and in conformance with local regulations or procedures of the local telephone company. Be sure to comply with any restrictions before using the device.

Figure 7 shows the scrambler/descrambler connected to a radio, or a tape player. In this application, the device will either scramble the audio coming from the source or descramble an incoming scrambled transmission. The output can be monitored via the built-in speaker and/or passed on to a tape recorder.

The scrambler/descrambler also can be connected between a tape recorder and its source in order to create

continued on page 77

AUDIO SCRAMBLER

continued from page 55

scrambled tapes, or between a tape recorder and its output to decode them.

The device can also be used to scramble and descramble two-way telephone conversations. For instance, a single scrambler/descrambler unit can be used in a half-duplex mode, which means only one person can speak at a time because the unit must be switched between connections. A mechanical TX/RX switch can be used to do the switching. A much better approach is a full-duplex set-up. Figure 9 shows how two scrambler/descrambler units are connected for full-duplex, meaning that no switching is necessary. (The conventional telephone is full-duplex.) Other than merely eliminating the RX/TX PUSH-TO-TALK switch needed in the half-duplex configuration, the full-duplex application offers a more secure environment. A would-be eavesdropper would have to descramble both sides of the conversation, a difficult task because each transmitting scrambler unit would, of course, be tuned to a slightly different frequency by the users.

The device can also be used to provide computer data transmission security. For that you can connect the full-duplex configuration to a 300-baud computer modem. **R-E**

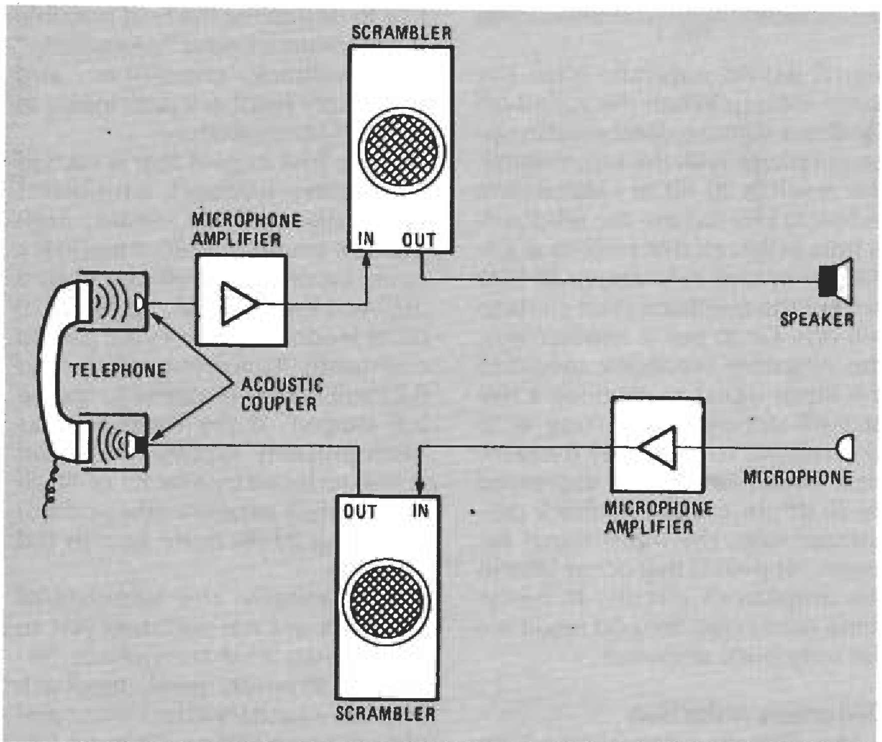
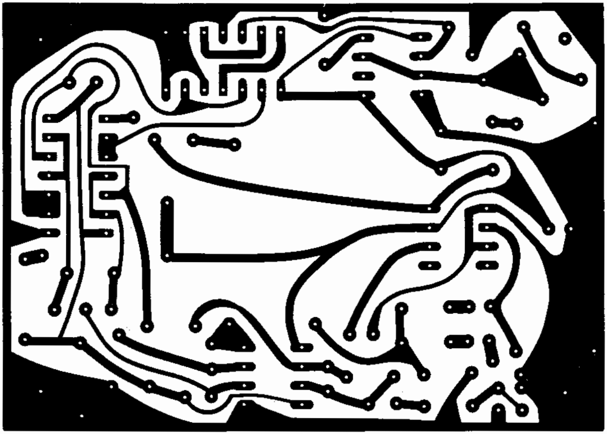


FIG. 8—TWO SEPARATE UNITS are needed in order to provide full-duplex telephone scrambling/descrambling.



3⅛ INCHES

THE AUDIO SCRAMBLER lets you communicate in privacy. The circuit is built on this PC board. The story begins on page 51.

LETTERS

AUDIO SCRAMBLING SYSTEM

I've needed a secure communications system for years, and your "Audio Scrambling System" (January 1988 **Radio-Electronics**) is the only device I've found that didn't cost megabucks. But I've had some trouble getting it going. Were there any circuit changes?

I need several units, so I want to purchase pre-made PC boards. Where can I buy them? The article stated that there was a source for PC boards in the parts list, but it wasn't there.

TIM CATLIN
Chicago, IL

If your project used a PC board made from our template there is no circuit change. If you built the circuit using Fig. 5 in January as a reference, however, make the following corrections: Delete the connection between IC4-a, pin 2 and IC4-d, pin 12. Add a connection between IC4-a, pin 13 and IC4-d pin 12. The schematic should then be correct.

An etched and drilled PC board is available postpaid for $8.00 from Wavelink Laboratories, P.O. Box 199, Trumbull, CT 06611. Connecticut residents must add appropriate sales tax.—Editor