F COMMERCE
STANDARDS

NBS SPECIAL PUBLICATION 480-8

Law Enforcement
Equipment Technology

A Guide to

VOICE SCRAMBLERS

for Law Enforcement Agencies

A User Guide from the National Bureau of Standards

ACKNOWLEDGEMENTS

This guideline was prepared by the Law Enforcement Standards Laboratory of the National Bureau of Standards under the direction of Marshall J. Treado, Program Manager for Communications Systems and Jacob J. Diamond, Chief of LESL. Technical assistance was provided by George Sugar, Edward Niesen, Edith Corliss and Ed Burnett of the NBS Institute for Basic Standards. This effort was sponsored by the National Institute of Law Enforcement and Criminal Justice of the Law Enforcement Assistance Administration; Lester D. Shubin, Program Manager for Standards.

A Guide to VOICE SCRAMBLERS for Law Enforcement Agencies

Robert E. Nelson

Electromagnetics Division
National Bureau of Standards
Boulder, Colorado 80302

Prepared by the

Law Enforcement Standards Laboratory
Center for Consumer Product Technology
National Bureau of Standards
Washington, D.C. 20234

For the

National Institute of Law Enforcement
and Criminal Justice
Law Enforcement Assistance Administration
Department of Justice
Washington, D.C. 20531

U.S. DEPARTMENT OF COMMERCE, Elliot L. Richardson, Secretary
Edward O. Vetter, Under Secretary
Dr. Betsy Ancker-Johnson, Assistant Secretary for Science and Technology
NATIONAL BUREAU OF STANDARDS, Ernest Ambler, Acting Director

Issued December 1976

Library of Congress Catalog Card Number: 76-600070

National Bureau of Standards Special Publication 480-8
Nat. Bur. Stand. (U.S.), Spec. publ., 44 pages (Dec. 1976)
CODEN: XNBSAV

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 1976

For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402
(Order by SD Catalog No. C13.10:480-8). Stock No. 003-003-01735-3 Price $1.05
(Add 25 percent additional for other than U.S. mailing).

contents

foreword

The Law Enforcement Standards Laboratory (LESL) of the National Bureau of Standards (NBS) furnishes technical support to the National Institute of Law Enforcement and Criminal Justice (NILECJ) program to strengthen law enforcement and criminal justice in the United States. LESL's function is to conduct research that will assist law enforcement and criminal justice agencies in the selection and procurement of quality equipment.

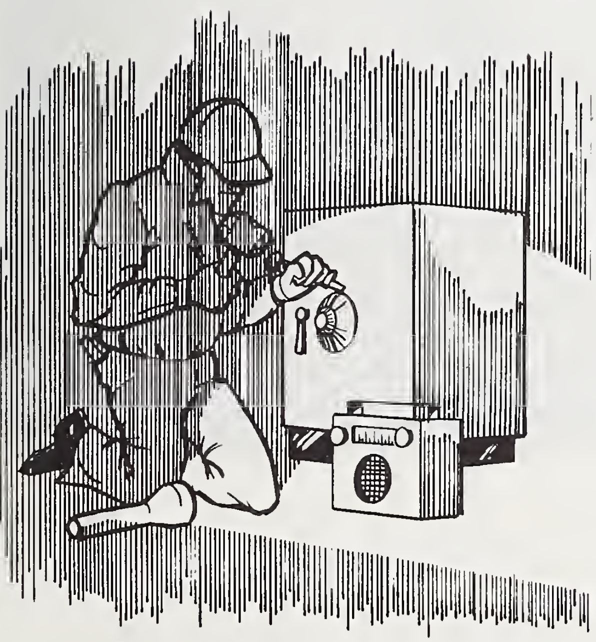
LESL is (1) subjecting existing equipment to laboratory testing and evaluation and (2) conducting research leading to the development of several series of documents, including national voluntary equipment standards, user guidelines, state-of-the-art surveys and other reports.

This document is a law enforcement equipment guideline developed by LESL under the sponsorship of NILECJ. Additional guidelines as well as other documents are being issued under the LESL program in the areas of protective equipment, communications equipment, security systems, weapons, emergency equipment, investigative aids, vehicles and clothing.

Technical comments and suggestions concerning the subject matter of this report are invited from all interested parties. Comments should be addressed to the Law Enforcement Standards Laboratory, National Bureau of Standards, Washington, D.C. 20234.

Jacob J. Diamond
Chief, Law Enforcement
Standards Laboratory

introduction



Radio communications are not private. Not only do criminals monitor law enforcement agency broadcasts to give themselves an edge, but well-meaning citizens and special interest groups also listen in and often rush to the scene of a crime, accident, or civil disturbance where they disrupt police activities. To maintain privacy, many agencies either use or are considering use of voice scramblers. A recent survey of 428 representative agencies [5]* disclosed that 40, approximately 9 percent, used scramblers and 225, approximately 53 percent, felt they needed them.

This guideline is intended to provide law enforcement agencies with guidance in the selection and use of voice scramblers. The information in it comes from scrambler users, scrambler manufacturers, and scrambler tests conducted by the National Bureau of Standards.

Addition of voice privacy to a communications system is not simply a matter of purchasing some voice scramblers. An agency will also have to:

- Identify its requirements.
- Determine what equipment is available that can satisfy these requirements.
- Obtain and evaluate proposals from suitable suppliers.
- Award the contract.
- Evaluate the performance of installed scramblers and rectify any problems encountered.

The first three steps may have to be repeated several times before a contract can be awarded. Initial decisions may have to be modified and compromises made in order to match agency needs and funds with the capabilities and cost of available scramblers

To assist in the solution of problems that may develop after installation, this guideline discusses some that have been encountered by current voice scrambler users and suggests ways to avoid them.

*See Appendix A: References. All numbers in brackets hereafter apply to these references.

identifying needs

Identifying actual needs is the first order of business for an agency contemplating use of voice scramblers. Because equipment capable of satisfying all requirements may not be available, scramblers probably will have to be selected that fulfill only the most important needs. Therefore, the identified requirements should be ranked according to individual relative importance.

An agency will have to identify its needs and preferences in five areas:

- Privacy level.
- Performance requirements.
- Operational or tactical uses.
- Support requirements.
- Special requirements.

privacy levels

In a survey, 2,098 municipal police chiefs identified the eavesdropping groups that created most problems for them [17] as:

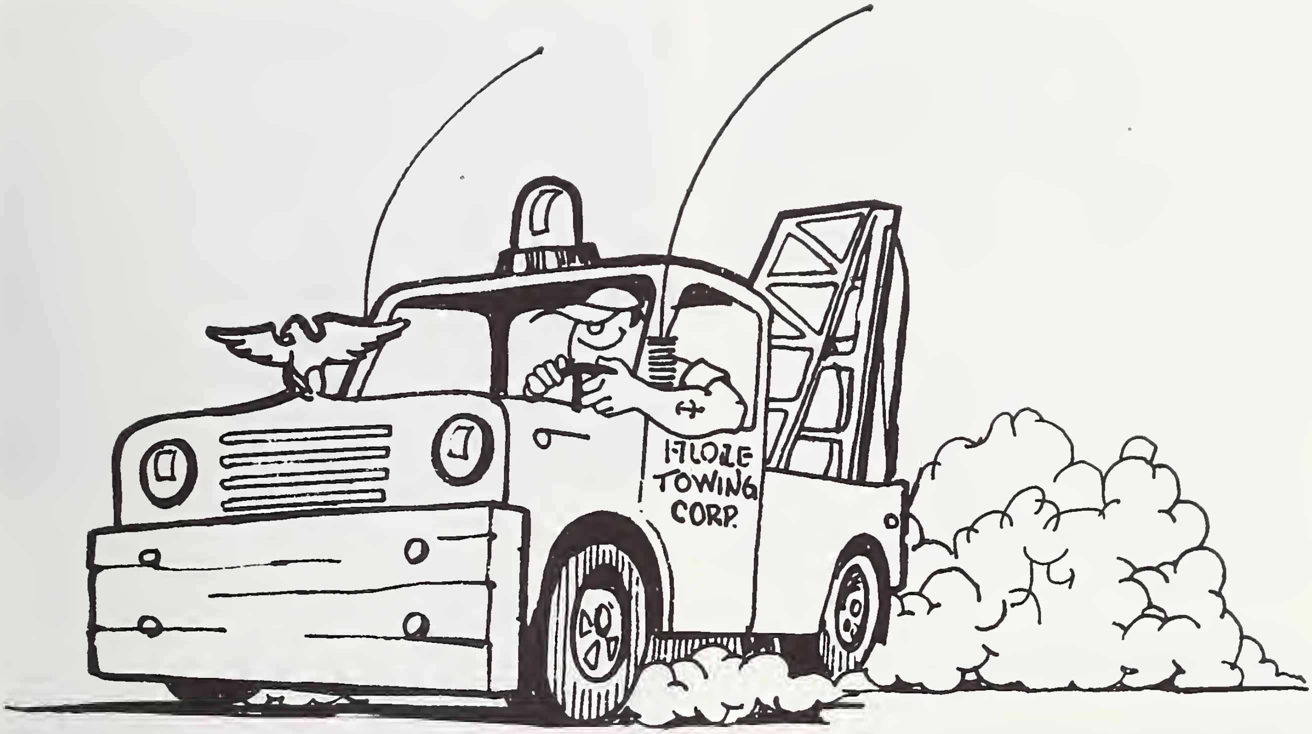
- Juveniles who phone in reports of imaginary crises in order to listen in on resulting frustrated comments of dispatchers and cruisers.

- Burglars who utilize monitors to follow police movements and help them take evasive action before the police arrive. Bookies and narcotics movers are also eager eavesdroppers.

- Special interest groups such as wrecker companies, ambulance services, and news media. Disruption of normal police operations and procedures often results from interference by those with a profit motive.

- The average citizen who just enjoys listening to the police radio is no problem unless enthusiasm carries him to the scene. Small town police, however, often wish to avoid public knowledge of the names and places of police activity because of gossip problems.

- Civil disorder groups were mentioned least often by the chiefs. These eavesdroppers, however, have been among the most numerous and larger cities invariably rated them as first or second in importance. It is safe to assume that any group engaged in a civil disorder will seek detailed knowledge of the course of the disorder and the movements of police dealing with it.



A law enforcement agency must assess for itself the lengths to which an opponent will go to decode a scrambled message. As an example, it has been reported that trained listeners are able to understand scrambled messages from one type of scrambler [2]. Is the opponent aware of this, and is he willing to invest the time and effort required to train himself? Which opponents can be expected to be knowledgeable enough to realize that they may be able to buy or build an unscrambler? Is it worth the investment to them to intercept police messages?

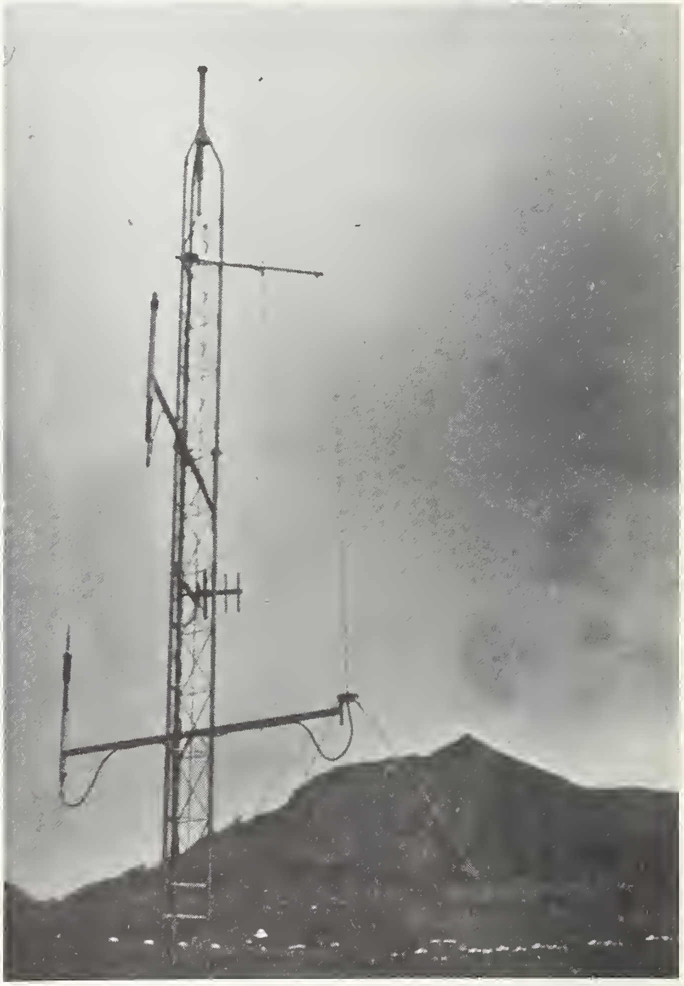
These questions are difficult to answer since they require a judgment as to the benefit to the opponent. For instance, the prankster or someone who eavesdrops, hoping to pick up a few gossip items, may not feel it is worth any extra effort or expense to decode scrambled messages. However, a special interest group may deem it worth a substantial investment to decode messages of interest. The criminal element of most concern to a particular law enforcement agency can vary from the petty thief to the well-organized crime syndicate. If the sophisticated criminal can avoid apprehension by knowing the locations and movements of police as relayed by radio, he may be willing to invest a considerable portion of his "earnings" to protect his "business."

For juveniles and the general public, in most instances, a communication need be kept private for only a few minutes to obtain the desired results. Action against criminal and civil disorder groups may demand that tactical information transmitted by two-way radio be kept confidential for several hours. This is true in situations where long-range plans must be formulated via radio because key personnel are forced to remain in the field to respond to rapidly changing situations.

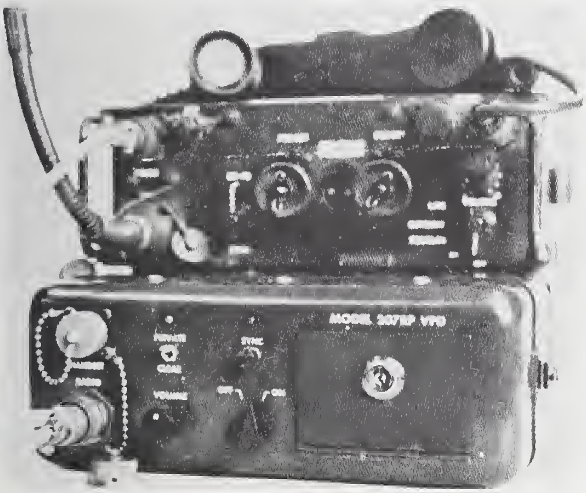
The agency's job, then, is to evaluate the threat as realistically as possible to determine the level of privacy needed. This evaluation may be difficult to make, but it is quite important because, in general, privacy is expensive. High privacy levels require complex scrambling equipment. Law enforcement agencies should be careful not to buy more privacy than they need.

performance requirements

Most law enforcement communications systems are not designed to accommodate scramblers. Consequently, the installation of scramblers is often a problem of retrofit. In addition, some communications systems do not meet minimum performance levels specified in National Institute of Law Enforcement and Criminal Justice (NILECJ) standards [9 through 13], and the addition of scramblers to such marginal systems may cause sufficient degradation to render them useless. Some of the factors that influence scrambler performance are discussed in Appendix B.

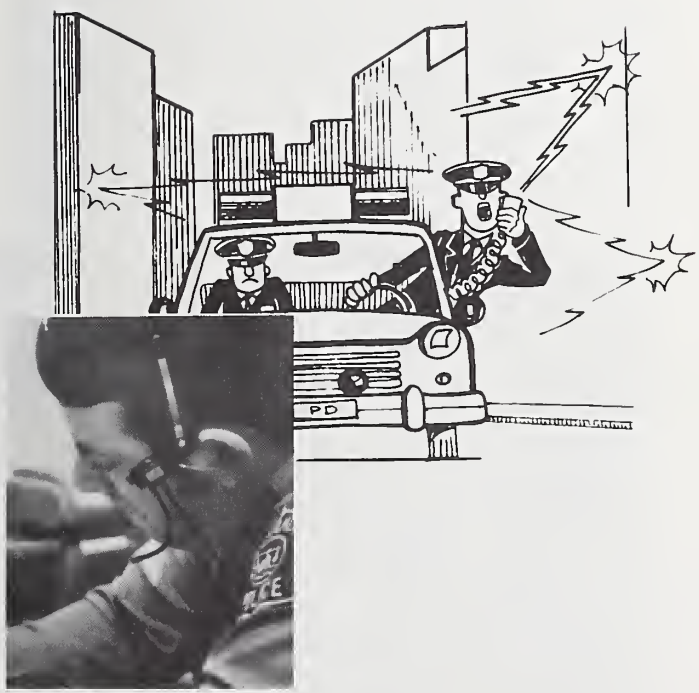


Communications equipment is usually specified and purchased on the basis of the performance of the individual components. There is adequate engineering basis for using this approach if auxiliary equipment such as scramblers are not involved. However, there are no standards available to aid the user in predicting the overall performance of a communications system that includes scramblers. Some of the problems inherent in the development of such standards are discussed in the literature [14,16]. The test program conducted at the National Bureau of Standards revealed that at least one type of scrambler could not be tested using the single frequency audio tones normally used to measure the performance of communications transceivers. Even for those scramblers for which the normal test signals can be used, it is not clear how the results of some tests should be interpreted.



Specifying scrambler performance, then, is a difficult problem. One approach is to specify requirements suggested in the reference literature or by a particular manufacturer. Although this approach has been successful in some instances, there is no guarantee that scramblers will perform satisfactorily in a particular communications system even though they meet specifications. An example of this can be seen in the experience of the Dallas Police Department, discussed later in the "Systems Problems and Cost" section beginning on Page 17.

As an alternative, the law enforcement agency can provide prospective suppliers with the measured performance characteristics and a detailed description of its communications system. The scrambler performance requirement can then be stated as "the scramblers must perform satisfactorily when used in the communications system as described." Suggestions for determining satisfactory performance are discussed in the "Acceptance Tests" section on Page 23.



Communications system parameters that should be measured and techniques for measuring them are given in the NILECJ standards mentioned earlier. The general description of the system should be as detailed as possible. Important items which should be included are:

- Locations of all telephone links and their frequency response characteristics.
- Locations of base stations and repeaters.
- Identification of geographical areas of weak signal or high noise level.
- Identification of signals used for control of repeaters, satellite receivers, or other equipment. (Such signals can adversely affect scrambler operation, especially if the signal frequency falls within the normal voice band of 300-3,000 Hz.)
- Identification of types and models of communications equipment in use.

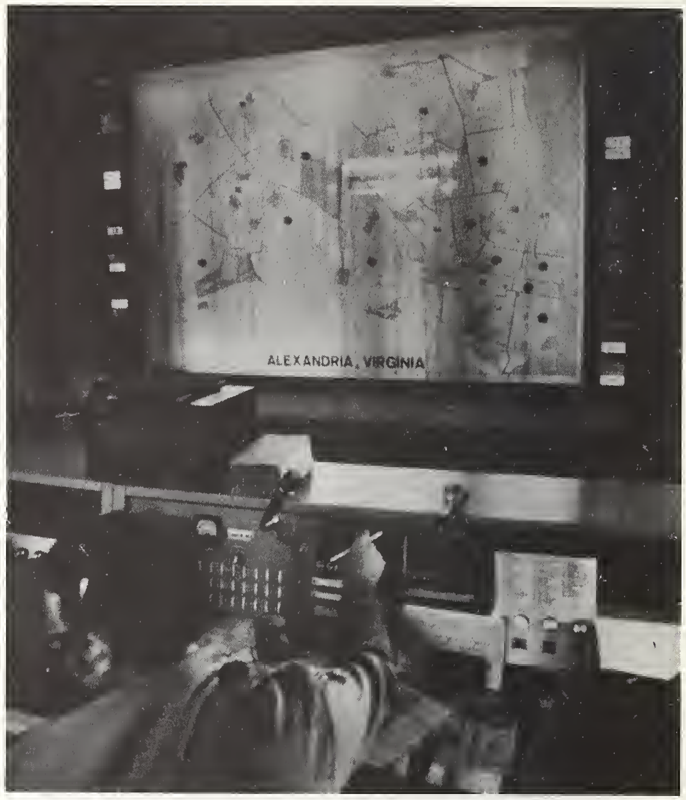
Requirements that apply only to the scrambler and do not affect the communications system can, of course, be specified. These requirements would include such items as the number of key settings, or code settings, required and the method of protecting the scramblers from theft or tampering. Additional special requirements or desirable features are discussed below.

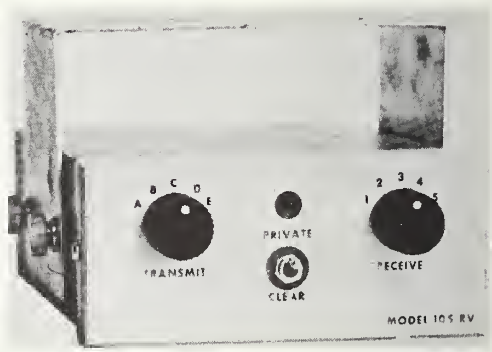
tactical considerations

In addition to performance requirements, prospective scrambler users need to consider a number of other factors that could influence their choice of equipment.

One of these is how often scramblers should be used and by whom. This will depend to a large extent on the opponent and the reasons scramblers were considered necessary in the first place. The user group may vary from a small special group using them a fraction of the time to the entire force using them all of the time. Although limited use is the most common method of operation, the police department of Abilene, Texas, reports effective use of scramblers all of the time by the entire police force [15]

Each method of operation has advantages and disadvantages. If scramblers are used only part of the time and only in critical situations, the opponent has fewer opportunities to penetrate the system. The casual eavesdropper, especially, may feel it is not worth the effort to decode only a few scrambled messages, even though they may be the ones of most interest to him. If this is the case, a relatively low-privacy scrambler can be used quite effectively. Limited use of scramblers also minimizes public relations problems which sometimes occur between the police department and the news media or the general public. Using scramblers all of the time also could result in the loss of cooperation with other agencies on the same channel. In addition, many scrambler manufacturers do not offer a scrambler for personal/portable units, so that 100 percent scrambler operation may not be possible for systems that include such units.





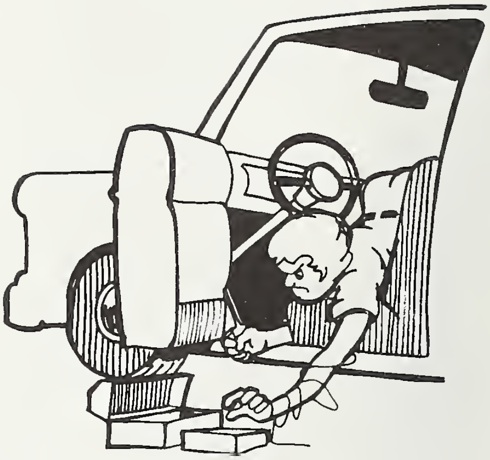
There are also some disadvantages in the restricted use of scramblers. In a tense situation, officers may forget either to use their scramblers or how to use them properly. The opponent also is alerted that something unusual is happening when messages are scrambled, even if he doesn't know exactly what. If scramblers are used infrequently, periodic testing must be performed to insure they will operate satisfactorily when needed.

Some thought also should be given to maintenance and security considerations. This includes the ease with which defective scramblers can be replaced, as well as the effect a defective scrambler has on the transceiver, and vice versa. Points to consider are:

- How complicated is it to connect the scrambler to the transceiver?
- Can a defective transceiver be replaced without adjusting the scrambler or replacement transceiver?
- Can a defective scrambler be replaced without adjusting the transceiver or replacement scrambler?
- If the scrambler fails or is removed temporarily, can the transceiver continue to be used?
- How is the scrambler protected from theft or tampering?
- Which keys or codes, if any, are set by the manufacturer, and which keys or codes, if any, can be set by the law enforcement agency?
- Are the selected keys or codes used by any other law enforcement agency within 100 miles?

support requirements

Support is usually required in the areas of installation, maintenance, documentation, and training. This support may be provided by the law enforcement agency itself, the supplier, an independent organization, or some combination of the three.



If any of the support is to be provided by the supplier, this should be discussed with him and specified in the final contract. If the supplier is not to install or maintain the equipment, provisions must be made to assure that whoever does receives adequate training and documentation such as manuals. Whatever is required from the supplier should be clearly stated to avoid misunderstanding.

special requirements

Some scramblers come equipped with standard or optional special features worthy of consideration.

One of these is "clear voice override." This feature allows the scrambler to receive a clear or unscrambled transmission, even though the receiver is operating in the scrambled mode. However, the operator must have some means of determining when a received message was transmitted in the clear, so that he does not attempt to give a scrambled reply.

Another feature permits an operator to select a limited number of codes from his console. This feature also may include a selective signaling capability to enable different units to use different codes without interfering with one another. However, personnel using different codes on the same channel must be able to determine when the channel is occupied by a transmission in order not to interrupt any transmission in progress.

Some manufacturers also offer scramblers specifically designed for use with telephone systems, such as the equipment shown above and at the left.

scrambler characteristics

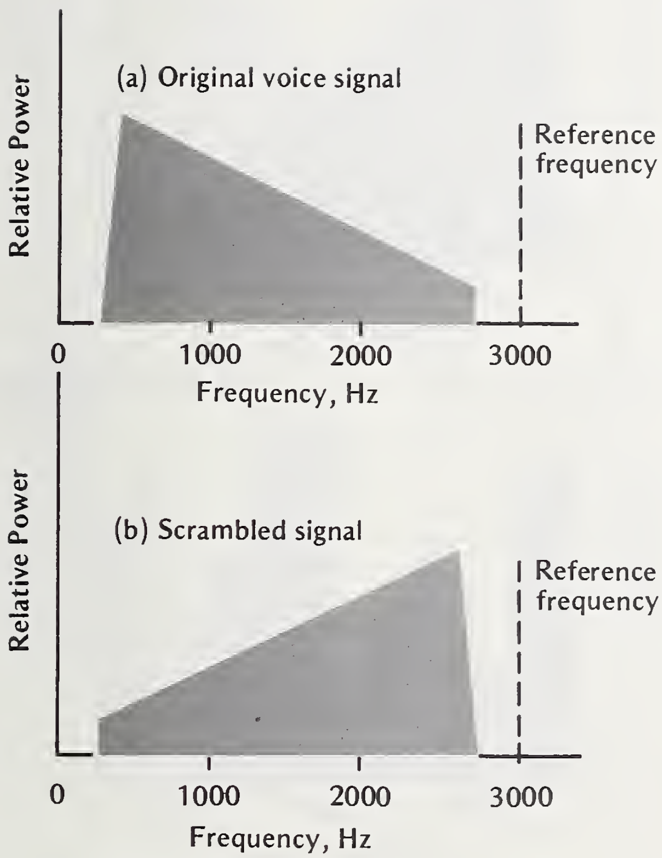
Of the many techniques available today which effectively render speech unintelligible to unauthorized listeners only three are utilized in scramblers currently marketed for law enforcement use. These are inversion, bandsplitting, and masking. Various combinations of the three techniques are also used [7,16].

Scramblers also can be categorized as those having fixed codes and those using continually changing codes.

Fixed-code scramblers generate the scrambled voice signal in the same manner during each transmission. Thus, the opponent need only obtain a similar device to have an unscrambler. For this reason, fixed-code scramblers provide less privacy than scramblers that use continually changing codes.

Scramblers that utilize continually changing codes do so in a manner or sequence determined by the "key". The key's purpose is to force the opponent to use cryptanalysis, that is determine the key, in order to unscramble the message. The mere possession of an unscrambler is of little value to him, providing the number of keys available for changing codes is large enough to prevent him from finding the correct key simply by trial and error. If the key is changed periodically, every day, for example, the odds against the opponent finding the correct key are high, even if only a few thousand keys are available. Also, if the opponent does find the correct key, he must start over again each time the key is changed.

While a discussion of cryptanalysis is beyond the scope of this guide, one point is worth mentioning. In a cryptographic attack, the way the key stream is generated, that is how the key changes the code, may be more important than the total number of keys available.



Scrambling by inversion.

inversion

An inverter is a device that converts each frequency component in a voice signal to a different frequency. The new frequency is the difference between the original frequency and an inversion, or reference, frequency. For example, if the inversion frequency is 3,000 Hz, a frequency component of 500 Hz would be converted to 2,500 Hz (3,000 minus 500). This is illustrated in the figure to the left for frequencies in the nominal 300 Hz to 3,000 Hz speech band.

Inverters using a single inversion frequency are called fixed-code inverters. Masking, which will be discussed later, is sometimes added to the inverted speech.

Some inverters are designed so that the inversion frequency is continually changed according to some predetermined code. These are known as frequency-hopping inverters. Masking also is sometimes used with frequency-hopping inverters.

fixed-code inverters

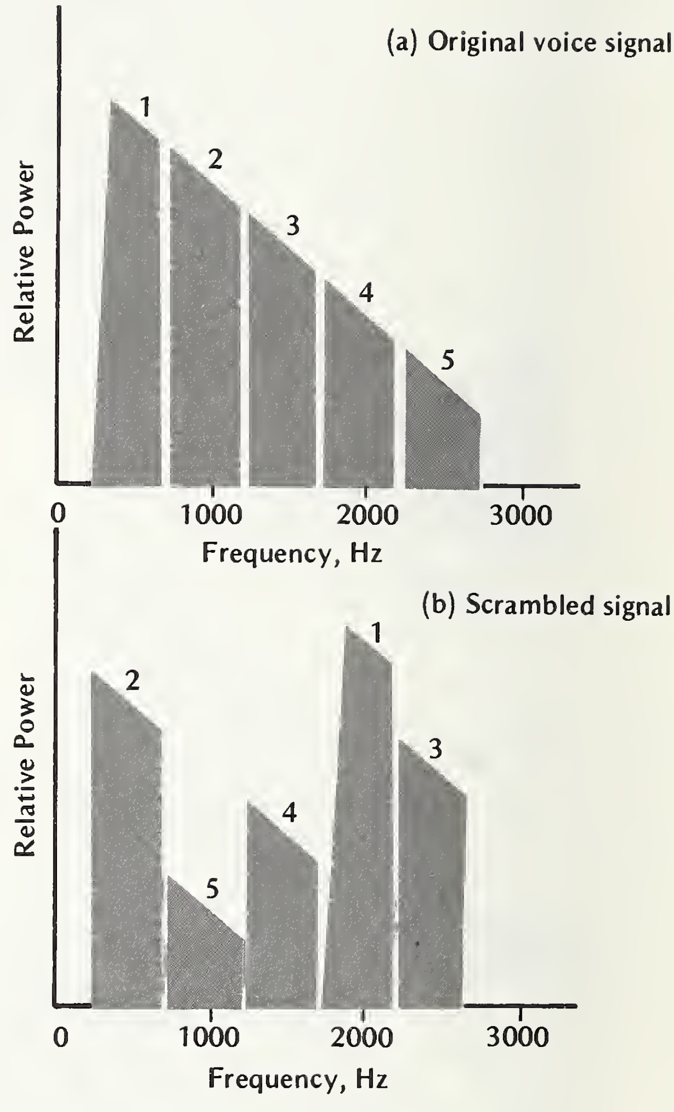
Simple inverters probably offer the least privacy of the voice scramblers being marketed for law enforcement use. It has been reported that some people actually have learned to understand speech in its inverted form [2]. Inverted speech also can be unscrambled by relatively inexpensive equipment. In addition, if used on single-sideband channels, inverted speech can be unscrambled simply by detuning the receiver to receive the other sideband. Simple inverters are available that change their code, or inversion frequency, with a switch or plug-in module. The opponent must then readjust his equipment to unscramble messages.

The fixed-code inverter provides privacy against only the casual eavesdropper. A sufficiently motivated opponent easily can obtain the equipment necessary to unscramble inverted speech. However, fixed-code inverters provide adequate privacy if the opponent is unwilling to go to the trouble and expense of obtaining an unscrambler or does not realize an unscrambler is relatively easy to obtain. Using the scramblers only in critical situations also may help increase privacy. The eavesdropper is still able to monitor most transmissions but is prevented from eavesdropping on only a few occasions.

Fixed-code inverters have several advantages over other types of scramblers. They are relatively inexpensive, costing approximately $200 to $700 depending on the type of unit and the options desired. They also generally are less susceptible than other scramblers to channel irregularities and usually perform satisfactorily in a complex communications system. Intelligibility of the unscrambled message normally is quite good, even over a poor channel. In addition, fixed-code inverters usually are fairly simple to install and maintain, require no synchronization, and can be quite reliable.

frequency-hopping inverters

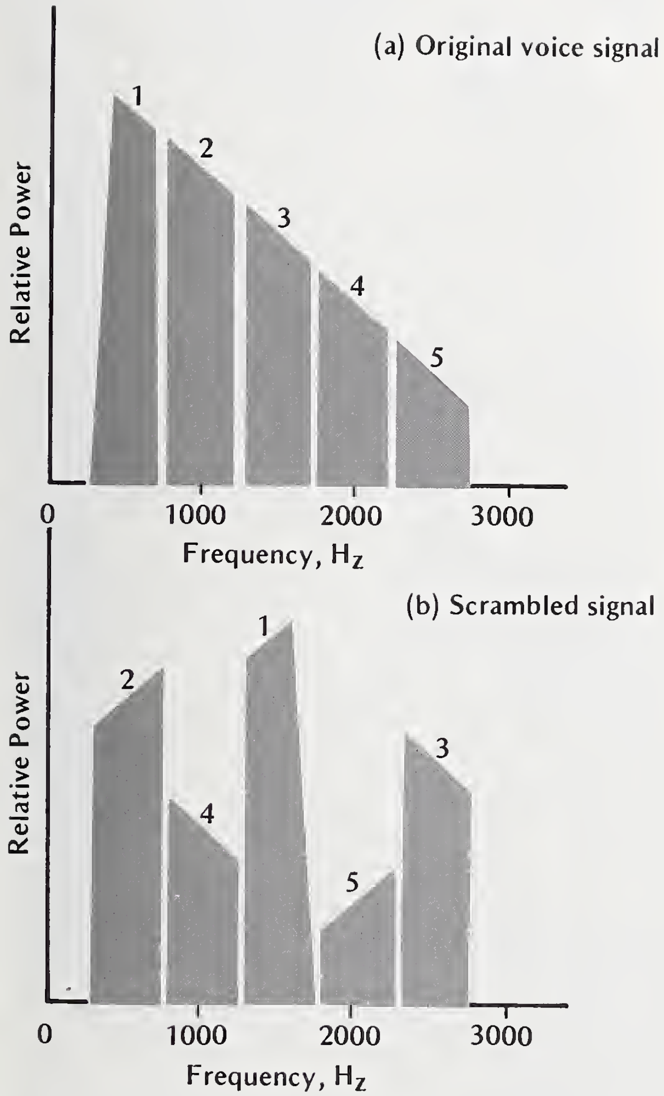
If the key stream for changing the code is properly generated, the frequency-hopping inverter can be highly resistant to cryptographic attack. However, it has been reported that it may not be as resistant to noncryptographic attacks. Techniques similar to



Scrambling by bandsplitting.

those used to unscramble fixed-code inverters and bandsplitters may be effective in unscrambling frequency-hopping inverters [8].

Simple frequency-hopping inverters cost from about $700 to $1,000. They require synchronization to assure that the scrambler and unscrambler are keyed in phase, that is, that the transmitter and receiver use the same code at the same time.



Scrambling by bandsplitting combined with inversion.

bandsplitting

Bandsplitters divide the typical speech frequency band into several sub-bands and then rearrange them relative to each other. This is illustrated on the left. Sometimes the bandsplitting technique is combined with the inversion technique so that sub-bands are not not only rearranged but each sub-band is inverted as well. The other figure on the left shows how speech is scrambled by bandsplitting, with some of the sub-bands inverted.

The fixed-code bandsplitter rearranges the sub-bands in the same order at all times. Bandsplitters that continually change the order in which sub-bands are arranged are calling rolling-code bandsplitters.

fixed-code bandsplitters

Fixed-code bandsplitters offer slightly more privacy than inverters primarily because the opponent needs more equipment to unscramble the signal. The techniques required to adjust the equipment also are more complex. However, it has been reported that a fair amount of intelligence can be recovered by simply listening repeatedly to a recording of the scrambled signal or by arranging only one or two of the bands back into their original positions [6,8].

Bandsplitters currently offered for police communications contain four, five, or six sub-bands. Privacy increases as the number of bands increases because less intelligence is obtained from each sub-band that is returned to its original position. Bandsplitting is sometimes combined with inversion to make the scrambled signals even more complex. Unscrambling this signal requires somewhat more time and equipment but no additional technical skills.

Bandsplitters, then, can apparently provide somewhat higher privacy than inverters. Synchronization is not required, and bandsplitters normally perform satisfactorily over poor channels. Bandsplitters are usually more expensive than inverters, costing from $650 to $3,500. They are somewhat more susceptible to channel irregularities than inverters, and unscrambled voice quality is usually degraded to some extent.

rolling-code bandsplitters

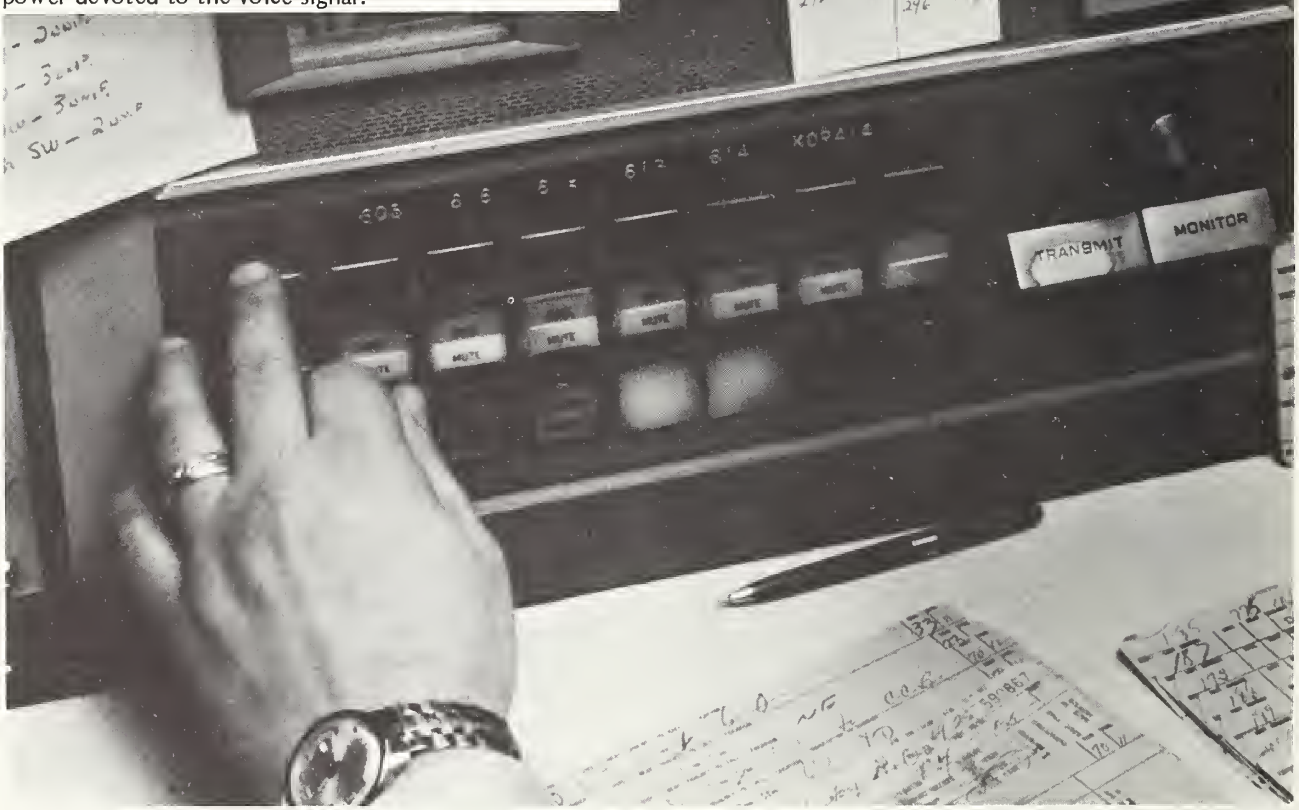
As in the case of frequency-hopping inverters, rolling-code bandsplitters may be susceptible to non-cryptographic attack, even though they apparently offer high resistance to cryptanalysis [4,8].

Rolling-code bandsplitters also require synchronization between the scrambler and unscrambler. Prices for rolling-code bandsplitters generally vary from about $800 to more than $4,000, with one priced at about $6,000.

masking

Masking techniques superimpose extraneous tones or noise, or both, on a speech signal in an attempt to destroy the syllabic content of the speech. Masking by itself, which provides very little privacy, is not used in any of the scramblers marketed for law enforcement use. Combined with other techniques, however, it can provide an added measure of privacy. The technique for removing a tone, a combination of tones, or noise-like masking from a signal is not technically difficult, but it does require additional time and equipment.

The use of masking may decrease effective transmission range because it reduces the transmitter power devoted to the voice signal.



systems problems and costs

In addition to the cost of scramblers themselves, many other factors contribute to the total expense of adding a voice scrambling capability to a communications system. They include maintenance, personnel training, and possible communication system modifications.

Very little data is available concerning maintenance. In general, one would expect a complex scrambler to require more maintenance than a simpler type. However, because scramblers are a relatively recent addition to police communications systems, maintenance histories do not provide enough information on which to base any general conclusions. One point that should be considered, however, is who will perform the maintenance. This should be settled with the manufacturer before the scramblers are purchased.

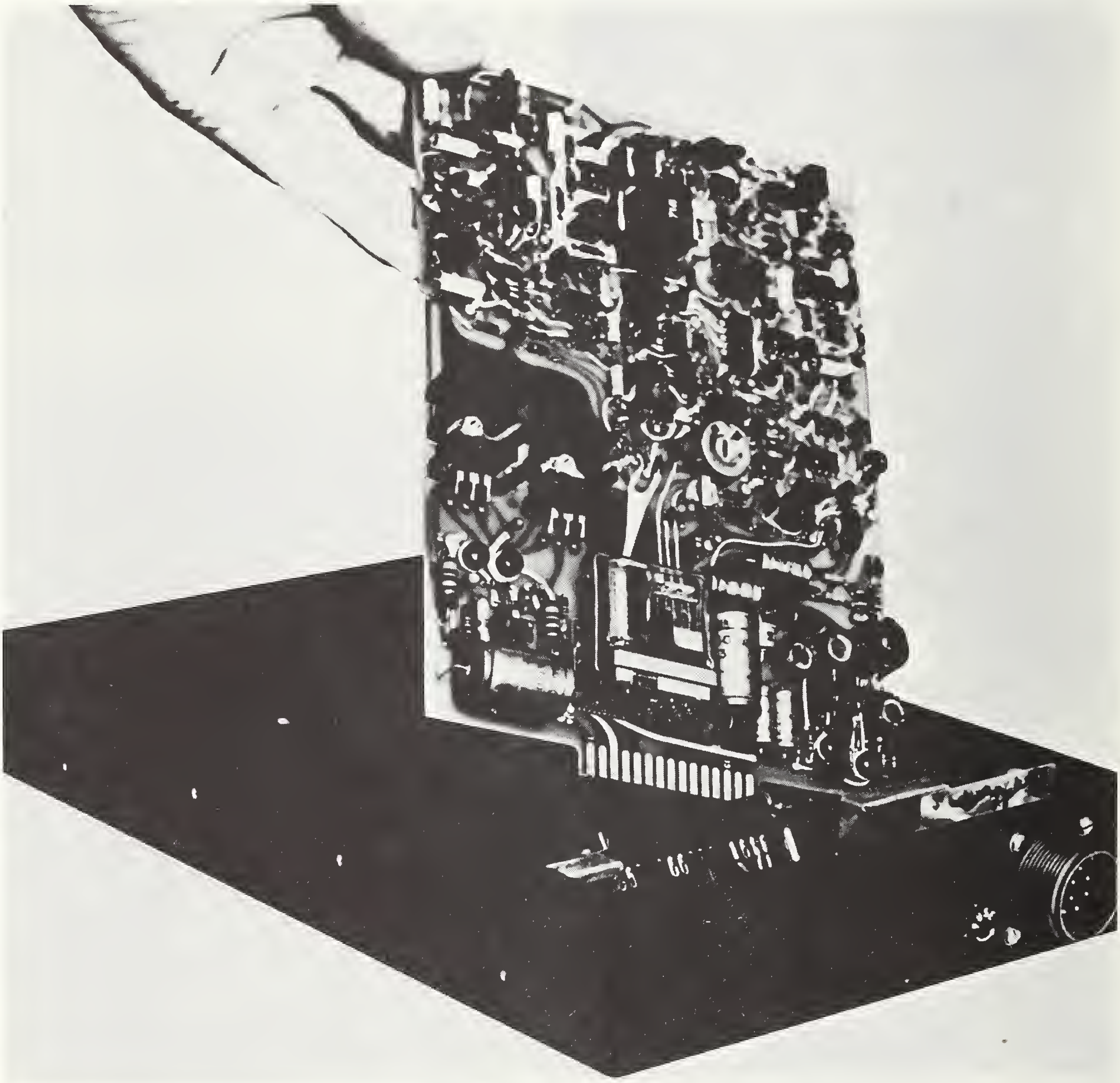
Other cost factors worthy of consideration include the training of maintenance personnel and operators, and possibly a public relations effort directed toward the general public, the news media, and those department personnel who may resist the introduction of new and unfamiliar equipment.

Moreover, it is possible that in some cases significant communications system modifications will be required. An example of this was discussed by City of Dallas, Texas, officials during a conference on speech scramblers held at Texas A&M University in June 1973 [3].

Dallas, feeling inverters did not provide sufficient privacy, purchased more sophisticated scramblers in the fall of 1970. These scramblers did not work, primarily due to the nature of the existing communications system. Quite extensive, it consists of five divisions and uses 12 channels in a mobile-repeater-duplex method of operation. Each component of the system contributed to the problem. Some added harmonic distortion and intermodulation distortion. Others affected frequency response. Telephone lines, used to link various system components, severely attenuated higher audio frequencies and often introduced hum and noise into the system.

City engineers and the scrambler supplier worked for several months to overcome the problems. They made measurements to determine the extent of the system's distortion and narrowed frequency response. This led to drastic improvements through correction of the frequency response characteristics of satellite receivers and design of line equalizers to compensate for degraded response at both high and low frequencies. Insertion of the equalizers not only improved frequency response, it also decreased system distortion. The end result was a substantial improvement in voice clarity and, eventually, the satisfactory operation of the scrambler-equipped system.

It would be fortunate indeed if law enforcement agencies had available a reasonably priced scrambler satisfactory to all their needs and compatible with their communications systems. More likely, they will find a few scramblers which meet most of their more important requirements, require only minor modifications to their communications systems, and are at least within range of their budgets. Those manufacturers whose scramblers appear suitable can then be requested to submit proposals or contacted to begin discussions prior to requesting proposals.



conclusions

Scramblers having fixed codes offer relatively little privacy, because an opponent with a similar device will be able to unscramble the messages. However, fixed-code scramblers are relatively unaffected by communications channel irregularities, have fairly good unscrambled voice quality, can be quite reliable, are relatively inexpensive, and require no synchronization.

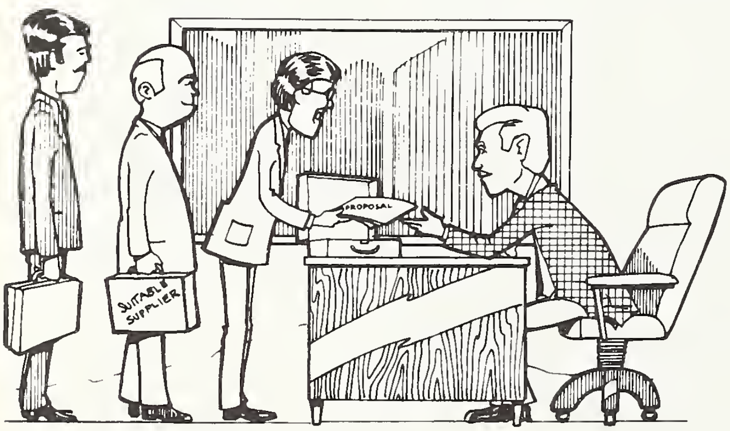
In principle, scramblers using continually changing codes provide more privacy than scramblers having fixed codes. However, they generally are sensitive to channel irregularities, and voice quality and intelligibility usually suffer additional degradation. Although synchronization is established automatically when the transmitter is keyed, synchronization periods can vary from less than one second to as much as four seconds, depending on the scrambler. During the synchronization period, voice transmissions cannot be made because they normally adversely affect synchronization. Synchronization may also be adversely affected by channel irregularities.

Some scramblers offered to police agencies combine two or all three of the basic scrambling techniques. They also may utilize separate key stream generators to control the codes for each technique. Information on the relative privacy of these complex scramblers is practically nonexistent. Judging from the complexity of the signals generated by these scramblers, privacy should be provided from all but the extremely sophisticated opponent. Prices vary, depending on the number and kind of scrambling techniques used, the manner in which the key or keys are generated, the number of key settings available, and the special features included.

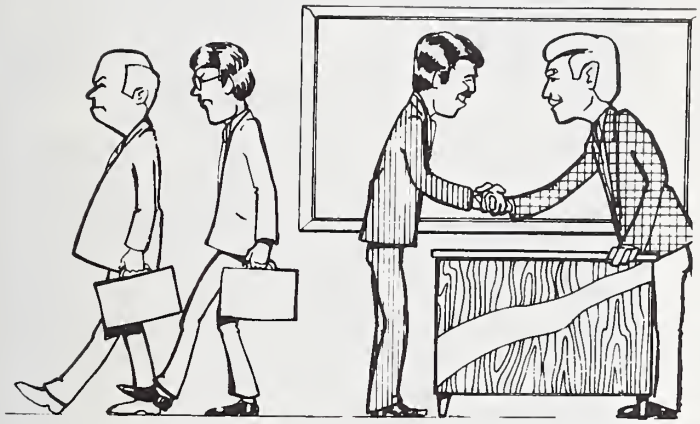
purchasing considerations

IDENTIFY REQUIREMENTS

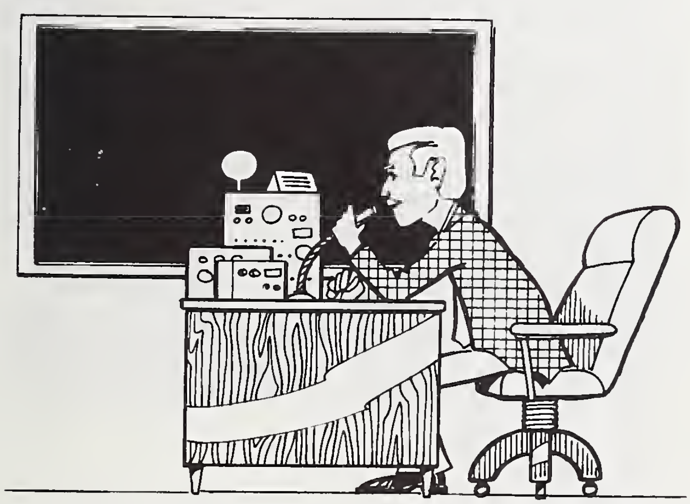
DETERMINE WHAT EQUIPMENT IS AVAILABLE



OBTAIN AND EVALUATE PROPOSALS



AWARD THE CONTRACT



EVALUATE PERFORMANCE

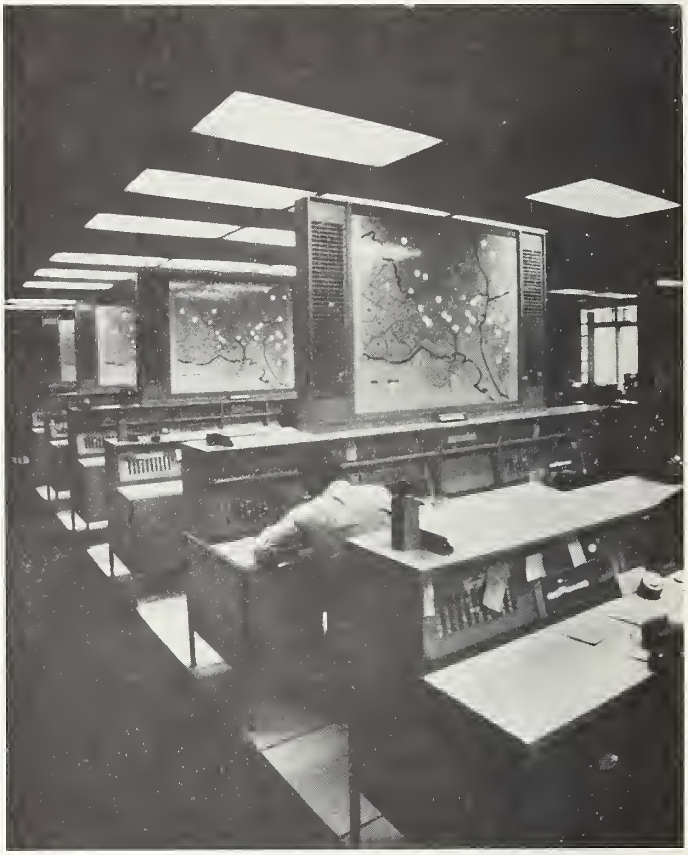
Purchasing scramblers presents different problems than purchasing other communications equipment. Generally accepted standards exist for transmitters, receivers, and antennas. The standards define the parameters to be measured, the techniques for measuring the parameters, and minimum equipment performance requirements. Relationships between such parameters and intelligibility are well established, but no reliable relationships have been established in the case of scramblers. Consequently, actual intelligibility tests must be made with the scramblers installed in a given communications system under normal conditions.

Writing a set of specifications and putting them out for bid is, therefore, not yet appropriate for scramblers. One alternative is to negotiate with suitable suppliers before writing a firm contract. This approach has been used successfully for other types of equipment, such as computer systems, where definite specifications could not easily be identified. Instead of listing specific requirements to be met, general objectives are outlined, special requirements are identified, and any other relevant facts are given. This general outline of requirements is then sent to prospective suppliers who are requested to submit proposals identifying the requirements they can satisfy, the requirements they can partially satisfy and how well they can satisfy them, and the requirements they cannot satisfy. The proposals are then evaluated in terms of those needs that can be satisfied and how important they are. The suppliers that most nearly meet the requirements are then contacted, and negotiations begin. The process of negotiation and evaluation of proposals continues until a suitable scrambler can be selected or a decision made that no scrambler is suitable.

request for proposals

Any request for proposal should describe the agency's requirements and the communications system within which the scramblers must operate.

The system should be described as outlined earlier in "Performance Requirements" under "Identifying Needs." In addition, the system's parameters should be measured as described in the NILECJ standards for communications equipment [9 through 13]. Certain parameters have been identified by users and manufacturers as being especially critical to scrambler performance. These are system audiofrequency response, SINAD ratio, and phase distortion. A discussion of how each of these critical parameters affects scrambler operation and performance is given in Appendix B.



proposal evaluation

When their initial proposals are submitted by prospective suppliers, it is unlikely that any one of them will satisfy all the listed requirements. The proposals must be carefully evaluated and a judgment made as to which suppliers seem most likely to be able to satisfy the more important needs.

Negotiations should be started with those suppliers. Representatives of the law enforcement agency should meet with each supplier, explain what needs were not adequately satisfied by his proposal, and ask him to submit a revised proposal. Some compromises will probably have to be made. Less important requirements or desirable features may have to be sacrificed in order to satisfy more important needs and still remain within the budget. This process should eventually result in the elimination of all suppliers except one.

In assessing the ability of a supplier to satisfy scrambler requirements, the company itself should be evaluated as carefully as its proposals. It is important that the company be willing and able to stand behind its product. Important factors to be considered are:

- Reputation as a scrambler supplier.
- Attitude of representatives and their willingness to cooperate.
- Financial and technical resources.
- History and financial growth.
- Background of top management and key technical personnel.

acceptance tests

The final contract should contain a detailed description of how acceptance tests will be conducted and what level of performance is required.

Objective intelligibility tests should be included, preferably conducted in the actual environment in which the scramblers will be used. The tests should be conducted by speakers and listeners who routinely use the communications system, utilizing text material familiar to them. This should provide a fairly realistic measure of intelligibility. Descriptions of other types of tests and comparisons between them are in the literature [1,16,18]. However, intelligibility test scores can vary widely according to their individual text material and procedures, and it is difficult to compare results when the same procedures and text material are not used. Moreover, if two types of scramblers are being compared, tests utilizing phonetically balanced word lists [1] probably provide a better comparison than other tests because they are sensitive to small differences in intelligibility.

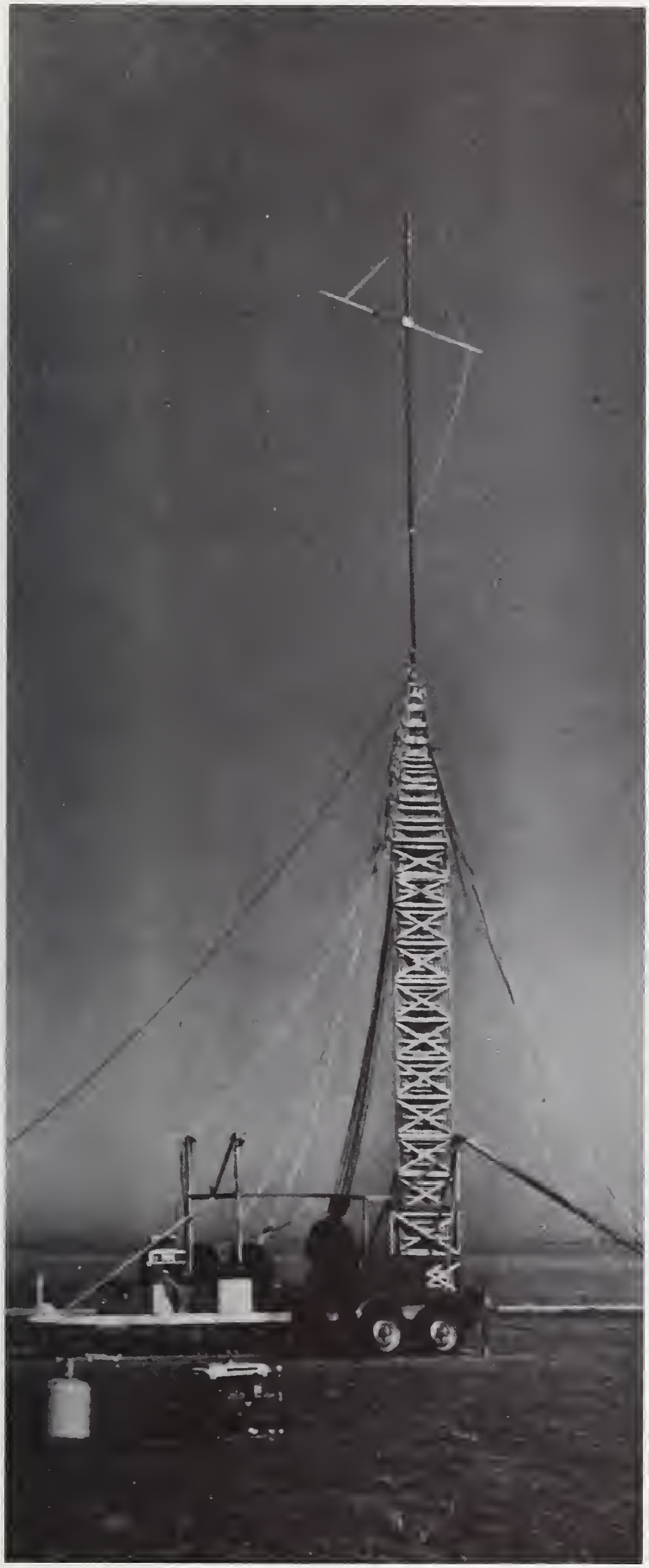
Test scores using the scramblers should be compared with test scores obtained when the communications system is used without the scramblers. A sufficient number of listeners and speakers must take part so that individual differences will be averaged out. At least four speakers and four listeners, used in all 16 possible combinations, are required to achieve reasonably repeatable results. For tests with familiar text material, the average of the test scores using scramblers should not be more than 10 percent lower than the average of the test scores using the communications system without scramblers.

If different types of communications equipment are used in the system, test the scramblers with each type. Interfacing problems may differ for equipment manufactured by different companies and even for different models manufactured by the same company.

Don't test the scramblers with the best equipment in service if they must work with poorer transceivers.

Conduct the tests in locations where communication is marginal, such as areas where fading occurs, signals are weak, or noise is high. Also, try to use all components of the system, such as repeaters, telephone links, and satellite receivers.

other considerations



Some thought must be given to personnel problems that may arise. If these problems are considered early in the planning stage, steps can be taken to minimize them and to smooth the transition to scrambler use.

Operator training may be necessary even for simple scramblers. If the scrambler is fairly complex, or has several operational features, more extensive training probably will be required. Some operators may resist the use of scramblers simply because they are unfamiliar. Voice quality is usually degraded to some degree. In fact, as a general rule, the more sophisticated the scrambler, the more the voice quality is degraded. This can be irritating to a user, especially if he is not prepared for it. Better microphone procedures and more careful diction are necessary for optimum intelligibility. An operator who becomes excited or begins to shout may not be understood. Also, for those scramblers that require synchronization, a time lapse is required to permit the scramblers to synchronize properly after keying the transmitter. If this is not done, part of the transmission could be lost or the units may not synchronize at all. Synchronization time varies from less than one second to as much as four seconds [8], depending on the type of scrambler used.

Procedures for protecting both scramblers and codes should be well defined. Opponents may decide it is easier to try to obtain a scrambler and its code rather than to crack scrambled messages. As few persons as possible should have access to scramblers or codes, and security responsibilities should be clearly defined and understood.

In order to maintain good relations with the general public and members of the news media who monitor police communications, a public relations effort may be desirable well in advance of the operational use of scramblers. This can be an important factor in avoiding public relations problems.

The scrambler control unit should be convenient and easy to use, and the power consumed by the scrambler should not be excessive.

Police departments which record messages on tape should preferably record descrambled messages. Primarily because of variations in tape playing speeds, messages taped in scrambled form may not be easily unscrambled later.

Since scramblers must operate in the same environment as radio transceivers, they must meet the same temperature, humidity, shock, and vibration requirements [9 through 13]. Protection against dust also is important, especially for those scramblers that have switches for changing codes.

summary

In general, the procurement and installation of scramblers poses different problems that the procurement and installation of other types of communications equipment. Due to absence of adequate performance standards for scramblers, procurement procedures and acceptance testing do not follow normal procedures. The suggestions given in this guideline provide law enforcement agencies with one possible approach in the absence of standards. Summarizing:

- Identify agency needs and assign relative importance values to each need.
- Identify possible suppliers of scramblers that can satisfy at least most of the important requirements.
- Generate a "request for proposal" to be sent to possible suppliers. The request for proposal should include agency needs and a description of the communications system.
- Evaluate proposals received from suppliers by assessing how well each can satisfy agency requirements.
- Renegotiate proposals with suppliers who are judged capable of meeting important needs.
- Repeat the above steps, making appropriate adjustments and compromises until one supplier has been selected to provide the scramblers.
- Write a contract which specifically identifies areas of responsibility for the vendor and the agency and includes details of the acceptance testing.
- Arrange for any necessary training and desired public relations efforts.
- Have the scramblers installed and operating satisfactorily before final acceptance.

Many of the important decisions must be based on incomplete information. The assessment of the threat and the evaluation of proposals usually are best guesses. It is hoped that this guideline will be of value to law enforcement agencies until suitable standards can be developed and promulgated.

appendix A
references

1. American National Standards Institute, "USA Standard Method for Measurement of Monosyllabic Word Intelligibility," USAS 53.2-1960 (American National Standards Institute, New York).

2. Blesser, B.A., "Inadequacy of a Spectral Description in Relationship to Speech Perception," Acoustical Society of America, 78th Meeting Abstracts, J. Speech and Hearing Research, V. 15, p. 19 (Acoustical Society of America, New York, 1972).

3. Center for Urban Programs, "Proceedings of a Conference on Speech Scramblers," Report No. TEES 1007-73-1, Texas A&M University, College Station, Texas, June 1973.

4. French, R.C., "Speech Scrambling, Electronics & Power," pp. 263-264, July 1972.

5. LEAA Police Equipment Survey of 1972, Volume II: "Communications Equipment and Supplies," NBSIR 73-211 (National Bureau of Standards, Washington, D.C., 1973).

6. Maitland, P., "Communication Security," 1972 Carnahan Conference on Electronic Crime Countermeasures. Private Communication (University of Kentucky, 1972).

7. McCalmont, A.M., "Communications Security for Voice-Techniques, Systems, and Operations," *Telecommunications*, pp. 35-42, April 1973.

8. McCalmont, A.M., "How to Select and Apply Various Voice Scrambling Techniques," *Communications News*, pp. 34-37, January 1974.

9. NILECJ-STD-0201.00, "Standard for Fixed and Base Station FM Transmitters," (National Institute of Law Enforcement and Criminal Justice, Department of Justice, Washington, D.C., GPO Stock Number 2700-00283, September 1974).

10. NILECJ-STD-0202.00, "Standard for Mobile FM Transmitters," (National Institute of Law Enforcement and Criminal Justice, Department of Justice, Washington, D.C. GPO Stock Number 2700-00287, October 1974).

11. NILECJ-STD-0205.00, "Standard for Mobile FM Antennas," (National Institute of Law Enforcement and Criminal Justice, Department of Justice, Washington, D.C., GPO Stock Number 2700-00250, May 1974).

12. NILECJ-STD-0206.00, "Standard for Fixed and Base Station FM Receivers," (National Institute of Law Enforcement and Criminal Justice, Department of Justice, Washington, D.C., GPO Stock Number 027-000-00358-3, September 1975).

13. NILECJ-STD-0207.00, "Standard for Mobile FM Receivers," (National Institute of Law Enforcement and Criminal Justice, Department of Justice, Washington, D.C., GPO Stock Number 027-000-00344-3, September 1975).

14. Sugar, G.R., "Developing Standards for Speech Scramblers," Center for Urban Programs, Proceedings of a Conference on Speech Scramblers, Report No. TEES 1007-73-1, Texas A&M University, College Station, Texas, June 1973.

15. Panel Discussion, ibid.

16. Sugar, G.R., "Voice Privacy Equipment for Law Enforcement Communication Systems, LESP-RPT-0204.00," (National Institute of Law Enforcement and Criminal Justice, Department of Justice, Washington, D.C., GPO Stock Number 2700-00260, May 1974).

17. "The Need for Voice Privacy," *Communications Magazine*, pp. 43-45, June 1970.

18. Webster, J.C., "Compendium of Speech Testing Material and Typical Noise Spectra for Use in Evaluating Communications Equipment," Technical Document 191, (Human Factors Technology Division, Naval Electronics Laboratory Center, San Diego, California, 13 September 1972).

appendix B
factors which may affect scrambler performance

Some degradation of system performance nearly always occurs when scramblers are installed. Intelligibility and voice quality are affected to some degree and some loss of range can be expected. This appendix discusses some of the technical problems that may be encountered in integrating scramblers into a communications system.

Because speech is so redundant and the human ear is such an excellent decoder, most voice communications systems can transfer a considerable amount of information under very poor conditions. With the addition of scramblers to a system, however, this no longer holds true. Any scrambler will degrade the system to some extent. Generally speaking, the more complex the scrambling technique, the more the system will be degraded. This is especially true in communications systems which are in themselves complex. The addition of repeaters, satellite receivers, telephone lines, and other links in the communications chain all tend to interfere with the optimum operation of voice scramblers. Present-day transceivers utilize many schemes to make voice transmission more efficient and increase intelligibility and quality. Unfortunately, however, schemes such as pre-emphasis, de-emphasis, and limiting introduce a certain amount of distortion, which may be acceptable for normal operation but may seriously degrade scrambler performance. Scramblers that utilize masking techniques seem to be especially affected by nonlinear distortion.

System audio bandwidth is another significant factor in scrambler operation. If the bandwidth is too narrow, some of the scrambled signal may be lost, and, since voice frequencies are usually rearranged in the scrambled signal, those frequencies lost may be the ones which provide the most intelligence.

A poor SINAD ratio in the system may result in poor intelligibility, a decrease in the effective range, and a tendency towards desynchronization.

The synchronization required for scramblers using continuously changing codes can be adversely affected by several conditions, including fading and multipath, as well as poor system SINAD ratio. An abrupt change in the length of the transmission path can also cause loss of synchronization. This loss could occur, for example, when a patrol car moves from the capture area of one voting receiver to that of another.

A communications system may incorporate several links, which usually introduce distortion, phase delays, and noise. For example, in addition to the normal propagation of the signal through the atmosphere, the signal may pass through a satellite receiver, a repeater, a telephone link, or several combinations of these. The poor frequency response of telephone lines may adversely affect a scrambled signal, and the lines may need to be equalized. Voting receivers may introduce abrupt phase changes because of variations in the signal path length via telephone lines. Many repeaters are controlled by signals in the audiofrequency range. These control signals may seriously affect the scrambled signal, and conversely, the scrambler may affect the control signal.

Electromagnetic interference (EMI) may also cause problems in scramblers. Interference, either radiated or conducted, may be generated externally or within the system. If EMI is a problem, shielding of the scrambler may be necessary to avoid radiated interference; or filters may be required in power supply cables and other cables to prevent conducted interference.

Any high-level ambient audio noise (such as a teletype unit in operation) will be scrambled along with the voice transmission and may produce an unintelligble signal at the receiver.

Other sources of noise or distortion which may become more noticeable when scramblers are used include dirty switches and fuses, poor grounding contacts, power supply ripple, ignition noise, and alternator whine.

appendix C
scrambler test program

cautions on the use of test results

The results of the tests described in this appendix must be interpreted with care. Relationships between laboratory results and actual performance of scramblers in the field have not been established. In addition, since limited tests were conducted on only three scramblers, the results do not necessarily apply to scramblers in general. Because the tests were preliminary and the test methods have not been validated as standard methods, the validity of some of the test results is open to question. In fact, some of the results raised more questions than they answered. This was especially true for the tests to establish intelligibility as a function of SINAD ratio, tests for susceptibility to poor audiofrequency response between receiver and unscrambler, and tests of scrambler susceptibility to ambient audio noise. Much work remains to be done to establish valid and meaningful measurement techniques for evaluating scramblers. The test results can be used, however, to indicate possible sources of trouble when attempts are made to incorporate scramblers into a communications system.

test objectives and description

The initial objective of the test program at NBS was to determine whether the parameters usually measured and the techniques normally used to evaluate communications transceivers were applicable to scramblers. Three different types of scramblers were selected for test. Scrambler A combined frequency-hopping inversion with tone masking while Scrambler B combined bandsplitting with frequency-hopping inversion. Scrambler C used a fixed-code inversion technique.

Most measurements performed on communications transceivers require the use of a single-frequency tone (usually 1,000 Hz) as a test signal. Single-frequency tones were found to be unsuitable for use as standard test signals for scramblers.

Since standard transceiver tests could not be performed on all scramblers, the test scramblers were, instead, subjected to various influences, and the effects on intelligibility and synchronization (if appropriate) were observed.

Intelligibility tests were performed using phonetically balanced word lists recorded on magnetic tape. Each reported value was obtained by averaging the scores of a group of eight listeners, each of whom was given two 50-word lists. In all, 16 listeners participated, and 10 different 50-word lists were used.

The laboratory test system included a base station transceiver and a mobile transceiver. The base station transceiver was shielded to prevent its radiation from affecting the rest of the test system. In addition, the transmitting signal from the base station transceiver had to be attenuated to a level that could be accepted by the mobile transceiver. The transmission path between them consisted of approximately two meters of coaxial line with step attenuators in the line to control the SINAD ratio. A simplified block diagram of the test system is shown in Figure C-1.

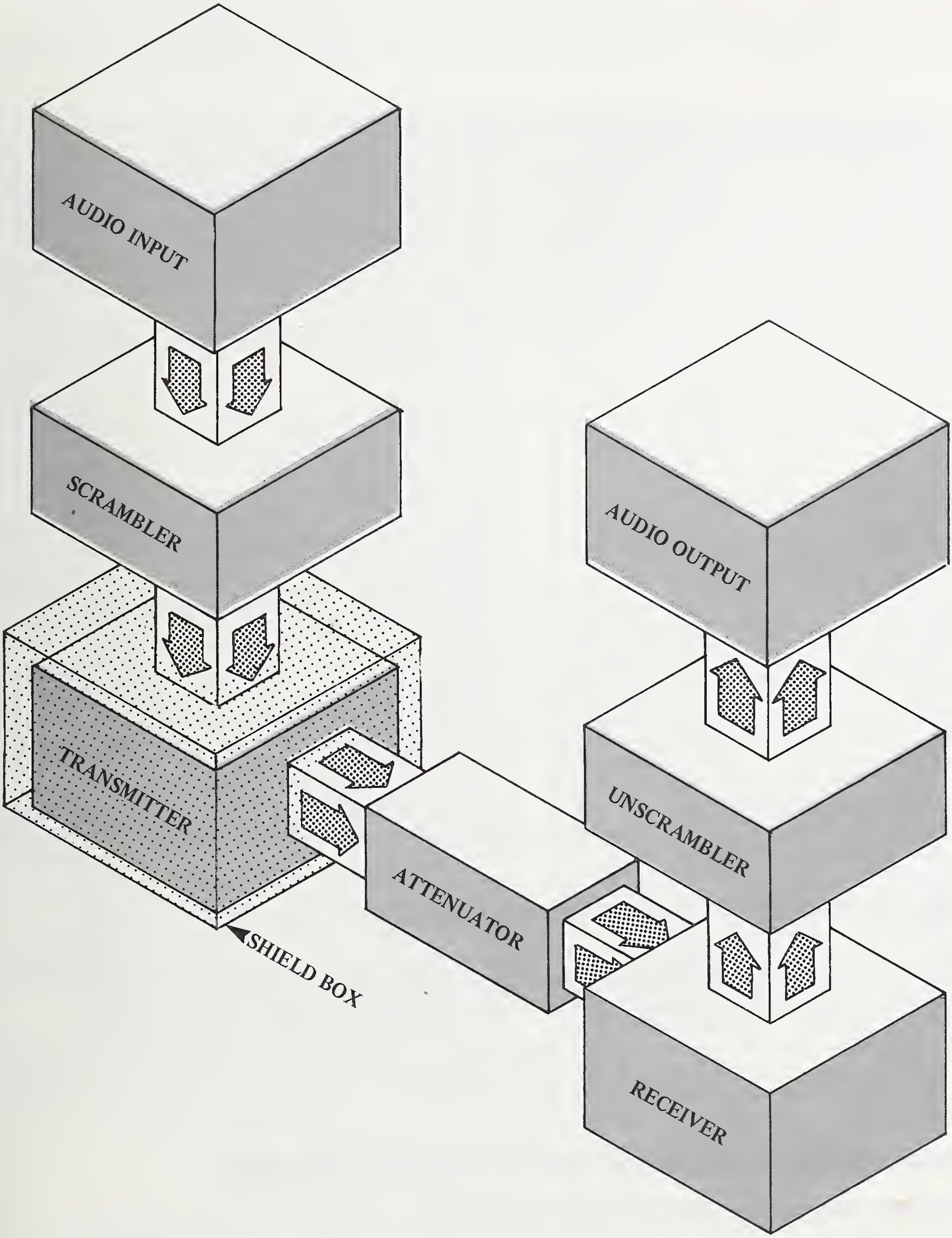


Figure C-1. Simplified diagram of test arrangement.

The tests were made with SINAD ratios of 27 dB (a good channel) and 12 dB (a poor channel). A 12 dB SINAD ratio is the minimum level of performance required by NILECJ standards. The SINAD ratios were measured before the scramblers were added to the circuit.

intelligibility as a function of SINAD ratio

The intelligibility of the system without scramblers was measured at each SINAD ratio to establish reference levels. The results are given in the table below, together with the results obtained after each scrambler in turn was introduced into the system. Differences in individual scores varied as much as 46 percent for a given test condition. However, the averages of two groups, consisting of eight individuals each, differed by only a few percent for each test condition.

Average Intelligibility Versus SINAD Ratio

SINAD Ratio (dB)	System Without Scramblers	Scrambler A	Scrambler B	Scrambler C
27	98%	88%	90%	97%
12	68%	82%	63%	88%

The addition of Scramblers A and C to the system operated at 12 dB SINAD ratio resulted in higher intelligibility scores. These results are surprising and may have been caused by so-called voice enhancing circuits incorporated in the scramblers. However, this has not been definitely established.

susceptibility to interfering tones

Scramblers B and C were not appreciably affected by the introduction of audiofrequency tones until the power levels of the tones equaled that of the voice power. As the tone power level was increased above that of the average voice power, intelligibility seemed to be reduced somewhat, but quantitative measurements were not made.

Synchronization of Scramblers B and C was not affected by the tones, but synchronization of Scrambler A was affected, as shown in Figure C-2. The plotted squares indicate the power of the test tone (relative to the average voice power) that caused the scramblers to lose synchronization.

susceptibility to fading or signal loss

Fading was simulated by increasing the attenuation between the transmitter and the receiver, thus reducing the signal level at the receiver. This also reduced the SINAD ratio. The intelligibility results were those reported above as the test for intelligibility as a function of SINAD ratio.

Synchronization was not lost until the signal was attenuated to a level too low to unsquelch the receiver (approximately 3 dB SINAD ratio). As the signal level was increased, synchronization was recovered. The ability of the scramblers to establish initial synchronization was not affected by the SINAD ratio for ratios of 12 dB or more. The results were the same for all three scramblers.

susceptibility to poor audiofrequency response between receiver and unscrambler

The poor frequency response of some transmission links (such as telephone lines) was simulated by inserting a bandpass filter between the receiver and the unscrambler. The roll-off characteristic of the filter was 12 dB per octave, and the filter

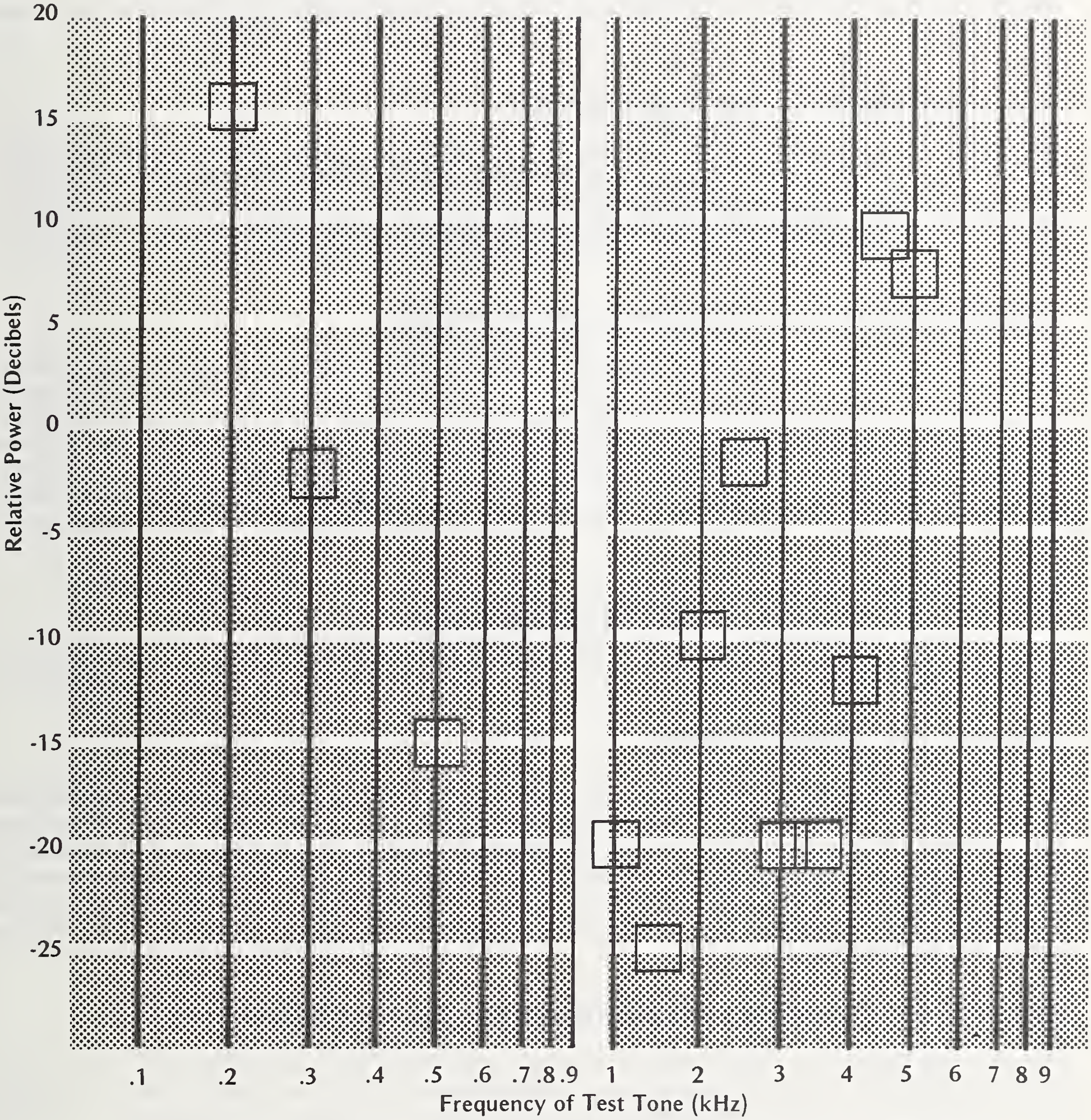


Figure C-2. Effects of test tone on synchronization of Scrambler A. The ordinate represents the relative power of the test tone required to cause synchronization loss. The zero decibel level is the average voice power required to produce maximum deviation of the transmitted signal.

was adjusted so that the signal levels at 300 and 3,000 Hz were 12 dB below the signal level at 1,000 Hz. No effect on intelligibility or synchronization was observed for any of the scramblers. The results were somewhat unexpected because several users and manufacturers had suggested that poor frequency response could be a problem. However, the test simulated the effect of only one such transmission link, whereas two, three, or more links in series are not uncommon in complex systems.

susceptibility to ignition noise

Ignition noise was introduced into the system to simulate noise radiated (as opposed to noise conducted) from a vehicle. The noise level corresponded to that produced by a field strength of 30 μ V/m/kHz being received by an antenna with a relative gain of one. This is the maximum field strength that can be expected to be radiated by an unsuppressed vehicle at a distance of 15 meters (approximately 50 feet). No effect on intelligibility or synchronization was observed in any of the scramblers.

susceptibility to ambient audio noise

As an elementary test of the effects of audio noise, broadband audio noise (so-called "white" noise) was introduced at the input to the transmitter scrambler. With an initial 27 dB SINAD ratio, Scrambler A exhibited some decrease in intelligibility when the average noise power in the 300-3,000 Hz band reached a level 10 dB below the average voice power. With an initial 12 dB SINAD ratio, Scrambler A lost synchronization at a level 10 dB below the voice power. Scrambler B exhibited the same intelligibility characteristics but at an average noise power of 5 dB below average voice power for both a 27 dB SINAD ratio and a 12 dB SINAD ratio. The synchronization of Scrambler B was not affected. Scrambler C exhibited some degradation of intelligibility when the average noise power was equal to the average voice power.

effects of supply voltage variations

Power supply voltages were varied 20 percent above and below those specified as nominal by the scrambler manufacturer. No effect was observed on any of the scramblers.

effects of phase delay

This test was designed to simulate a phase shift due to a sudden path length change, as when a continuous transmission is captured by a different voting receiver than the one that had captured it initially. A worst case condition (180 degree phase shift) was simulated for this test. This was accomplished by inserting a phase-reversing transformer between the scrambler and transceiver. The polarity of the transformer was then reversed by actuating a switch during a continuous transmission. With a SINAD ratio of 27 dB, Scrambler A lost synchronization for one or two seconds. With a 12 dB SINAD ratio, Scrambler A lost synchronization and did not recover. Scramblers B and C were not affected by phase reversals for either SINAD ratio.

effects of duration of continuous transmission

Scrambler A exhibited quite variable responses to continuous transmission. With a 27 dB SINAD ratio, the periods of continuous transmission for which synchronization was maintained varied from 1-1/2 to 22 minutes. With a 12 dB SINAD ratio, the periods varied from 27 seconds to 9-1/2 minutes. Scrambler B maintained synchronization for continuous periods of 22 minutes irrespective of the SINAD ratio. Scrambler C did not require synchronization.

effects of length of time between transmissions

No effects on any of the scramblers were observed as a result of time delays between transmission, for delays up to 15 hours. All scramblers established synchronization every time the transmitter was keyed on. Results were the same for the 27 dB SINAD ratio and the 12 dB SINAD ratio.

ANNOUNCEMENT OF NEW PUBLICATIONS ON NATIONAL CRIME AND RELATED SUBJECTS

Superintendent of Documents,
Government Printing Office,
Washington, D. C. 20402

Dear Sir:

Please add my name to the announcement list of new publications to be issued on the above subjects (including this NBS series):

Name ______________________________

Company ______________________________

Address ______________________________

City ______________ State ____________ Zip Code __________

(Notification key N-351)