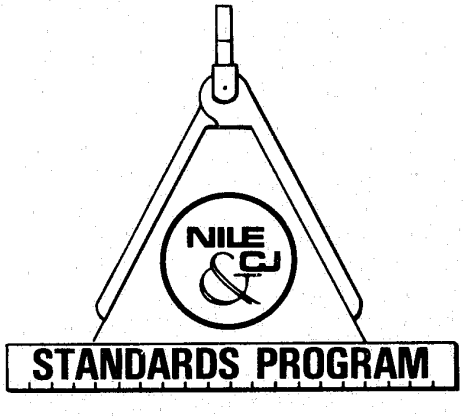
LESP-RPT-0204.00
MAY 1974

LAW ENFORCEMENT STANDARDS PROGRAM

VOICE PRIVACY EQUIPMENT FOR LAW ENFORCEMENT COMMUNICATION SYSTEMS



U.S. DEPARTMENT OF JUSTICE
Law Enforcement Assistance Administration
National Institute of Law Enforcement and Criminal Justice

LAW ENFORCEMENT STANDARDS PROGRAM

VOICE PRIVACY EQUIPMENT FOR LAW ENFORCEMENT COMMUNICATION SYSTEMS

prepared for the
National Institute of Law Enforcement and Criminal Justice
Law Enforcement Assistance Administration
U.S. Department of Justice

by

GEORGE R. SUGAR
ELECTROMAGNETICS DIVISION
NATIONAL BUREAU OF STANDARDS

MAY 1974

U.S. DEPARTMENT OF JUSTICE
Law Enforcement Assistance Administration
National Institute of Law Enforcement and Criminal Justice

For sale by the Superintendent of Documents, U.S. Government Printing Office
Washington, D.C. 20402 - Price 65 cents
Stock Number 2700-00260

LAW ENFORCEMENT ASSISTANCE
ADMINISTRATION

Donald E. Santarelli, *Administrator*
Richard W. Velde, *Deputy Administrator*
Charles R. Work, *Deputy Administrator*

NATIONAL INSTITUTE OF LAW ENFORCEMENT
AND CRIMINAL JUSTICE

Gerald M. Caplan, *Director*

ACKNOWLEDGMENTS

This report 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. NBS Electromagnetics Division staff member John P. Wakefield assisted in the preparation of the report.

FOREWORD

Following a Congressional mandate* to develop new and improved techniques, systems, and equipment to strengthen law enforcement and criminal justice, the National Institute of Law Enforcement and Criminal Justice (NILECJ) has established the Law Enforcement Standards Laboratory (LESL) at the National Bureau of Standards. LESL's function is to conduct research that will assist law enforcement and criminal justice agencies in the selection and procurement of quality equipment.

In response to priorities established by NILECJ, 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, LESP-RPT-0204.00, Voice Privacy Equipment for Law Enforcement Communication Systems, is a law enforcement equipment report prepared by LESL and issued by NILECJ. Additional reports as well as other documents will be 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 Program Manager for Standards, National Institute of Law Enforcement and Criminal Justice, Law Enforcement Assistance Administration, U.S. Department of Justice, Washington, D. C. 20530.

Lester D. Shubin, Manager
Standards Program

*Section 402(b) of the Omnibus Crime Control and Safe Streets Act of 1968, as amended.

VOICE PRIVACY EQUIPMENT FOR LAW ENFORCEMENT COMMUNICATION SYSTEMS

CONTENTS

VOICE PRIVACY EQUIPMENT FOR LAW ENFORCEMENT COMMUNICATION SYSTEMS

ABSTRACT

Law enforcement agencies are finding an increasing need for voice-scrambling equipment to provide privacy on their two-way radio communication systems. Work is underway at the National Bureau of Standards, under the sponsorship of the National Institute of Law Enforcement and Criminal Justice (NILECJ), to develop performance standards for voice scramblers. The four areas being considered are speech intelligibility, voice quality, voice privacy, and general system characteristics. This report first defines a set of special terms, then describes a number of types of scramblers that are now available for law enforcement use. Some inherent problems and weaknesses are discussed. The concepts of intelligibility and privacy are explored in detail. The potential contents of the standard are described, and some problems inherent in preparing and using the standard are discussed. The report concludes with some material intended to be of immediate assistance to the prospective purchaser of scramblers: a survey of units now on the market, some hints on how to proceed in the absence of a standard, and a bibliography of technical publications on voice scrambling.

1. INTRODUCTION

Law enforcement activities throughout the United States are being seriously hampered by a lack of privacy on two-way radio systems. Police radio communications are now continually intercepted, both by casual eavesdroppers and by lawbreakers. Simple police-band receivers cost as little as $20 and for $100-$200 one can purchase a scanning receiver that continually monitors up to 8 different channels. The ready availability of these receivers has virtually eliminated the privacy of communication often essential for effective police work.

One of the ways to increase the privacy of communications is to use electronic devices that encode voice signals for transmission and decode them at the receiver. These devices, loosely referred to as "scramblers", rearrange the voice signals so that, in principle, they are unintelligible to a listener who is not equipped with the proper decoding equipment. Scramblers were used in the 1920's to provide a measure of privacy on commercial radio-telephone circuits and were substantially improved and used during World War II for military and diplomatic [1][1] communications. Since then, the use of voice privacy equipment has spread into many areas of the industrial and commercial world as well as into the various law enforcement and security agencies. At present there are approximately 15 companies in the United States offering voice scramblers at unit prices from $260 to over $6,000.

Many law enforcement agencies have expressed the need to acquire scramblers. A recent survey [2] reports that 9 percent of the 428 departments that responded have scramblers available, and an additional 58 percent need them. However, agencies are confronted with the following when investigating scrambler purchases:

a) It is often difficult to obtain factual informa-

[1] References are listed in Appendix A.

tion on the design characteristics and performance of given units. There are both elements of secrecy and a scarcity of performance data on these scramblers.

b) There are almost no objective ways to compare the performance of different units, thus making it difficult to determine the relative value of each model of scrambler. It is even more difficult to determine the amount of privacy obtained for the money spent.

c) Scramblers often must be tailored to work with specific radio units. In general, the performance of a specific scrambler-transceiver combination cannot be accurately predicted from the listed characteristics of the separate units.

d) Scramblers from different manufacturers are usually not compatible, thus inhibiting their use for communications between different agencies in the same locality.

Under present circumstances it is difficult for a law enforcement agency to make optimum decisions in acquiring scramblers, and it is difficult for scrambler suppliers to compete with each other on the basis of the merits of their products.

One of the long-term goals of the present NILECJ program on voice privacy equipment is to provide a performance standard for evaluating scramblers, thereby hopefully reducing the present confusion regarding scramblers. The general content of the standard will be:

a) a definition of which characteristics of scramblers are important for proper performance;

b) a description of the methods to be used in measuring these characteristics; and

c) acceptable performance levels for the various characteristics.

Four technical areas are now under study. These are intelligibility, speech quality, privacy, and general system characteristics. The present focus is on voice units that will work with existing police radio equipment.

This report has been prepared as an advisory discussion of scramblers. It defines a set of special terms, and then describes a number of types of scramblers that are available for law enforcement use. Some inherent problems and weaknesses are discussed. The concepts of intelligibility and privacy are explored in detail. The potential contents of the proposed standard are described, and some problems inherent in preparing and using it are discussed.

The report concludes with some material intended to be of immediate assistance to the prospective purchaser of scramblers: a survey of units now on the market, some hints on how to proceed in the absence of a standard, and a bibliography of technical publications on voice scrambling.

2. DEFINITIONS

2.1 Attack

An attempt by an unauthorized person to unscramble a scrambled message, or a specific procedure for doing so. Also, a test to determine the relative privacy of a scrambler by subjecting it to various unscrambling procedures.

2.2 Clear

Not scrambled.

2.3 Code

Any one of the set of fixed ways of rearranging voice signals by a specific scrambler. See key.

2.4 Intelligibility

The ability of a voice communication system to convey the content of a transmitted message to the intended listener.

2.5 Key

A specification or setting that controls the sequence in which codes change in a scrambler with continually changing codes. (Key and code are not well-defined in the scrambler industry and are sometimes used interchangeably. This report

distinguishes between them in accordance with these definitions.)

2.6 *Privacy*

The ability of a communication system to conceal the content of a message from unauthorized persons.

2.7 *Scramblers*

A device for providing voice privacy by systematic modification of a voice signal before transmission.

3. VOICE PRIVACY TECHNIQUES

3.1 *General Approaches*

Many different methods of providing voice privacy have been proposed, but relatively few of these are appropriate for current law enforcement use. The available techniques can be categorized as follows:

a) frequency-domain
b) time-domain
c) masking
d) vocoder
e) digital

Frequency-domain systems rearrange the various frequency components of the voice signal so as to produce unintelligible sounds.

Time-domain systems divide the voice signal into brief time elements and transmit the various elements in a rearranged sequence.

Masking systems add extraneous signals and noise to the voice signal, thereby making it more difficult to understand. Masking alone has not proven to be a satisfactory scrambling technique.

Vocoder systems analyze the basic speech elements present in voice signals and transmit a set of signals representing these basic elements.

Digital systems convert the voice signal directly into an equivalent number stream and transmit these numbers in place of the voice signal.

At present, all the systems marketed for law enforcement use are frequency-domain systems or combined frequency-domain and masking systems. Time-domain systems are under study in England [3] and may become available in the near future. Vocoder systems are still too expensive for this application. Present digital systems require more than the nominal 3000-Hz bandwidth now available in VHF police radio systems.

Some of the common approaches to scrambling are discussed below. This section also includes some discussion of scrambler codes—the different device settings that can be used to make two scramblers of the same type incompatible with each other. In addition, limited discussion of the ability of some types of scramblers to provide privacy is included to provide some background for more general considerations of system privacy.

3.2 *Scramblers with Fixed Codes*

3.2.1 *Inversion*

The simplest scrambler now in use is one that interchanges low voice frequencies and high ones. This device is commonly called an inverter. It operates by changing each frequency component present in a voice signal to a new frequency, where the new frequency is the difference between the original frequency and a reference or inversion frequency. For example, for a reference frequency of 3000 Hz, a voice component at 750 Hz would be converted to a component at 3000 minus 750 or 2250 Hz. Figure 1 illustrates how a more complex signal would be changed by an inverter.

Unscrambling the scrambled signal is done by using a second inverter that has the same reference frequency as the first inverter. Using the same example again, a scrambled voice component at 2250 Hz, when subtracted from a reference frequency of 3000 Hz, produces a 750-Hz component, thus restoring the original voice component.

As might be suspected from the simplicity of this scheme, it is easy for an opponent to unscramble inverted speech. All he has to do is use an inverter with an adjustable reference-frequency

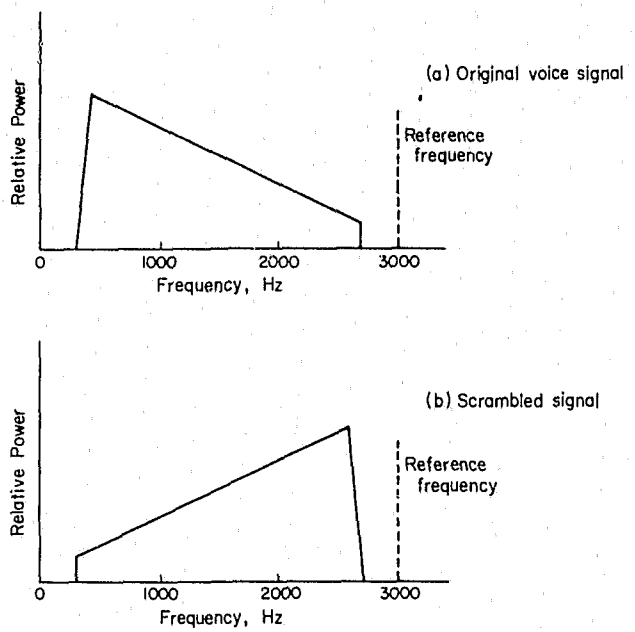


FIGURE 1. Scrambling by inversion.

oscillator and tune this oscillator until the speech is intelligible. Since single-sideband radio receivers have such a capability included as a normal operating feature, simple inversion provides no privacy whatsoever for single-sideband transmission systems.

When first heard by a novice, inverted speech sounds quite unintelligible. However, with careful listening some words can be distinguished. It appears that with concentrated attention one learns to understand inverted speech directly. In some recent experiments [4], people who were able to talk to each other only through inverters learned to communicate with only four hours of practice. Forty years ago, workers at the Bell Telephone Laboratories demonstrated an ability to speak in in inverted form [5, 6]. Their speech was intelligible only when "unscrambled" by an inverter. There is thus little doubt that a trained observer can understand inverted speech directly.

Coding of inverters can be done, at least in principle, by using different reference frequencies in the two inverters that might otherwise form a scrambler/unscrambler pair. If the two frequencies are sufficiently different, the speech is not intelligible. In practice, this coding is quite limited. Although frequency offsets as little as 10 Hz are noticeable, offsets as great as 200 Hz produce only moderate distortion [7]. Thus an offset of substantially more than 200 Hz would be needed for each different code. This requirement conflicts with a need to work with speech input signals that are limited to a nominal 300-Hz to 3000-Hz range and to keep the inverted output nominally within this same range. It therefore appears that only one or two additional codes for inverters can be obtained by the use of different inversion frequencies. Some commercial inverters provide a number of codes by using tone-controlled selective calling to unblock the squelch in the selected units [8].

3.2.2 Band-Splitting

A second form of voice scrambling now in use divides the nominal 300 Hz to 3000 Hz voice band into several subbands, and then interchanges the signals in these subbands, or inverts them, or both. Figure 2 illustrates such a process. This approach is commonly called band-splitting.

Unscrambling this signal is achieved by interchanging the signals in the subbands and reinvert-

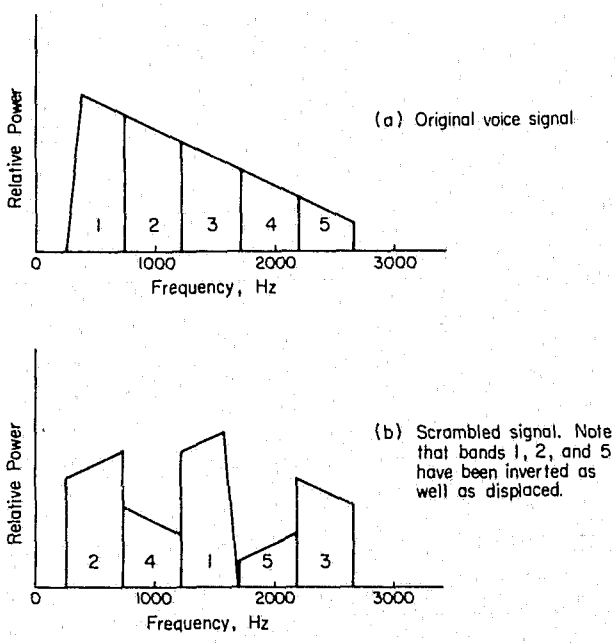


FIGURE 2. Scrambling by band-splitting.

ing them as required. A unit similar to that used for scrambling is required, with only minor internal differences. Many different code settings are possible with band splitters, corresponding to how the different subbands are rearranged in the scrambling process. For example, a system that uses 5 subbands can have 3840 different codes, since there are 3840 distinct ways to shuffle and invert 5 subbands. Not all of these are useful codes, however. One of these 3840 possible code settings produces no scrambling at all. Others produce relatively little scrambling and are thus of little value. In the 5-band band-splitter (called the A-3) installed by the American Telephone and Telegraph Company (A.T.&T.) for radio telephone service in 1937, only 11 of the 3840 possible codes were considered suitable for privacy [1]. Thus availability of a large number of codes in a scrambler should not be interpreted to mean that all of these codes are equally useful.

The band-splitter can provide more privacy than an inverter. Unlike the case of the inverter, information has not been found suggesting that one can learn to directly understand the scrambled output of a band-splitter that uses appropriate codes. However, it is reported that an average of 47 percent of the words scrambled by the A-3 were recovered simply by listening to a message several times [1]. In one case intelligibility rose to 76 percent. It is also possible for an opponent to eavesdrop by using equipment that returns just one of the subbands to its proper place [9]. Thus it appears that while band-splitters offer somewhat more privacy than inverters, they are by no means secure against relatively simple attacks.

3.2.3 Masking

The privacy offered by inverters and band-splitters is sometimes increased by adding extraneous tones or noise or both in the scrambler to mask the speech. These need to be added in such a way that they can be filtered out at the unscrambler. In practice, removing this masking at the unscrambler is always less than perfect; and the intended listener is always at least aware that extraneous signals are present. The difficulties of filtering these signals out at the scrambler are aggravated by the presence of harmonic distortion in the radio system, since such distortion will generate noise and tones at new frequencies where they cannot be removed without removing some of the desired voice signals also. Furthermore, the addition of masking signals to the scrambled voice signal will usually require that the voice signal be reduced in amplitude so that the peak value of the composite signal does not exceed the transmission channel specifications. This reduction, of itself, is likely to degrade overall intelligibility of the system. Thus the addition of masking increases the privacy of a system but reduces message intelligibility for the intended listener.

Tones used for masking sometimes also serve to synchronize or control circuits in the unscrambler. They can serve to lock the frequency of the reference oscillator in the unscrambler to that used in the scrambler [10], to operate a selective-calling feature, or to automatically switch the unscrambler in and out of the circuit for an intermixed set of clear and scrambled messages.

3.2.4 Time Division

The scramblers discussed above operate in the frequency domain. That is, they change the frequencies of the voice input to new frequencies. Another approach is to leave voice frequencies unchanged but to change the time sequence of what is said. For example, the time-domain equivalent of an inverter would generate speech backward. In practice this is not done because such a scrambler would need to save the whole message, and to wait until the end occurred before replaying the message in reverse. This would introduce unreasonably long time delays in the communication channel. A more practical approach is to divide the voice signal into small time segments (of about 60 milliseconds or less) and delay these for varying brief intervals before reproducing them. This varying delay mixes the order of the

voice segments and can make the scrambled output unintelligible.

During World War II, much work was done with time-division scrambling techniques, often in combination with frequency-domain scrambling [11]. However, the resulting systems all used magnetic recording devices and were relatively large and expensive. At present there are no time-division scramblers on the U.S. market. However, with the advent of new compact digital and analog [12] semiconductors storage devices that can provide the required time delays, there appears to be renewed interest in this area.

A principal problem of time-division scramblers is similar to that of band-splitters. While there are many ways to rearrange the normal voice sequence, many of these ways do not result in adequate scrambling. The "scrambled" output is often intelligible [3].

3.3 Scramblers with Continually Changing Codes

Thus far, all of the scramblers discussed have used fixed codes. Even though some had a selection of codes, once selected the code was fixed until changed by the user. A number of types of scramblers use continually changing codes to make it more difficult for an opponent to eavesdrop. The code changes typically occur from a few times per second to 100 times per second. Such systems permit the use of different code sequences at different times, thus preventing eavesdropping even by persons who have an unscrambler but who do not know what code sequence "key" is being used at the time. A set of switches is usually employed to adjust the key generator that controls the actual code sequence. A scrambler and unscrambler must be set to the same key to function together. In a properly designed system there will be enough different keys so that it is not practical for an opponent to find the correct one simply by trying all of the different possible switch settings. This is particularly true if the users change the key periodically such as once per day and exercise adequate precautions to prevent dissemination of the key to unauthorized persons.

Special names are commonly given to scramblers with continually changing codes. Two of these are frequency-hopping inverters and rolling-code band-splitters.

The use of continually changing codes adds a cryptographic element that, at least in principle, an eavesdropper must overcome if he is to unscramble messages. For example, digital scramblers can be designed so that the only successful methods of attack require cryptanalysis. On the other hand, the rolling-code band-splitter is reported to be susceptible to non-cryptographic attacks [9, 13]. The fact that it has a large set of different keys may thus be irrelevant in determining its level of privacy.

Some scramblers with continually charging codes also incorporate masking to increase privacy. The mask is sometimes scrambled independently to make the system less susceptible to attacks.

4. INHERENT DIFFICULTIES IN PROVIDING VOICE PRIVACY OVER LAW ENFORCEMENT COMMUNICATION CHANNELS

The designers of scramblers for police (narrowband) radio channels have a substantial set of technical problems to overcome. Therefore it is not surprising that there are so few successful designs. A major part of the problem, the inherent robustness of speech communication, has been succinctly described as follows [11]:

> Beginners in the study of privacy systems never fail to be amazed at the difficulty of scrambling speech sufficiently to destroy the intelligence. The ear can tolerate or even ignore surprising amounts of noise, nonlinearity, frequency distortion, misplaced components, gaps, superpositions, and other forms of interference. Very often partial or even complete intelligence can be obtained from a privacy system by partial or imperfect decoding, and this in turn can often be accomplished by operating on the

scramble in some way which the designer did not contemplate.

The fact that the ear is such a good decoding tool in combination with noncryptographic methods makes the production of privacy systems very difficult. Scrambling systems which look very effective on paper sometimes turn out on trial to degrade the intelligibility very little, although the scrambled speech usually sounds unpleasant. Most methods pushed to the point where they succeed in hiding the intelligibility so distort the speech that it is impossible to restore the speech with good quality. In fact, there are very few speech privacy systems which achieve a high degree of privacy with acceptable quality.

The limited audio bandwidth available in VFH communications channels also provides a substantial obstacle to scrambler designers. The highly secure all-digital scramblers will not fit into the presently available 3000-Hz audio bandwidths of police transceivers. The actual available bandwidth is usually even less than this nominal value. The EIA standard [14] permits the overall frequency response at 300 Hz and 3000 Hz to vary from +3 dB to −11 dB relative to the value at 1000 Hz. This standard is not a mandatory one, and the response of actual units has been reported [15] to be as poor as −20 dB at 3000 Hz. The scrambler designer thus needs to achieve good performance in widely varying bandwidths, with the widest bandwidth being less than optimum.

A further problem faced by designers is the great ingenuity exhibited by eavesdroppers in devising methods to unscramble transmissions. The history of voice scramblers displays a continuing sequence of confident inventors and the subsequent "breaking" of their scrambling systems. In the first U.S. patent on scramblers [16] the inventor states:

> "Thus it will be seen that by my invention absolute secrecy in the transmission of signals is insured—a desideratum long sought, but, so far as I am aware, now for the first time accomplished."

It is not evident whether this invention was ever used. However, it is clear from examining the principle used that the scrambled signal would be at least 40 percent intelligible to an eavesdropper. On the other hand, it is reported [1] that in the 1920's radio amateurs were able to eavesdrop on the inverted signals used then by A.T.&T. for transatlantic radio-telephone service soon after this service was inaugurated.

5. POTENTIAL PERFORMANCE MEASURES

As indicated in the Introduction, four technical areas are being considered for inclusion in the scrambler standard: intelligibility, speech quality, privacy, and general system characteristics. In this section each of these areas will be discussed in more detail.

5.1 Intelligibility

One of the first things that a new user observes is that speech transmitted through a scrambler/unscrambler system is usually not as clear nor as easy to understand as it is when the equipment is not used on the radio circuit. The relative ability of a listener to understand what is being said by a talker is called intelligibility. It is quantified as the relative number of correctly heard items, measured in percent. For example, if a talker reads a list of 200 words and a listener identifies 150 of them correctly, the intelligibility for that test was 75 percent. Thus intelligibility testing provides a way of measuring the fidelity of a voice communication system.

Almost all communication systems tend to reduce the intelligibility of speech. The extent of this reduction is dependent on many different factors such as the speaker's voice and diction, the nature of what is being said, the hearing acuity of the listener and his previous experience in listening to a given speaker and a given class of messages and the testing environment. Thus intelligibility is a function of at least the speaker, the listener, the message content, the transmission channel, and the environment. The usual procedure for measuring intelligibility of a communica-

tion channel involves using enough speakers and listeners to average out their individual differences, and controlling the environment, thus arriving at a measure representative of the channel performance and the test material used. The importance of the test material itself can be appreciated by considering some examples of the material used. These include lists of:

A. Single syllable words that sound nearly alike as [17]

hip, hick, hit, hiss
sail, pail, tail, fail
tan, ten, tin, teen

B. Phonetically balanced (PB) word lists, words that contain a representative sample of the sounds that make up speech [18]:

PB-50 List 1

1. cane	14. strife	27. slip	40. rat
2. there	15. dike	28. rub	41. rag
3. dish	16. not	29. feast	42. is
4. hid	17. ford	30. deed	43. wheat
5. heap	18. end	31. cleanse	44. rise
6. pants	19. then	32. folk	45. hive
7. hunt	20. bask	33. nook	46. grove
8. no	21. fraud	34. mange	47. toe
9. bar	22. smile	35. such	48. plush
10. pan	23. death	36. use (yews)	49. clove
11. fuss	24. are	37. crash	50. fern
12. creed	25. bad	38. ride	
13. box	26. pest	39. pile	

PB-50 List 2

1. tang	14. rib	27. nab	40. tan
2. fate	15. pick	28. bait	41. ways
3. suck	16. hock	29. bud	42. bounce
4. else	17. our	30. rap	43. niece
5. pit	18. hit	31. moose	44. awe
6. gill	19. job	32. trash	45. them
7. charge	20. wish	33. gloss	46. need
8. bought	21. nut	34. perk	47. quart
9. cloud	22. dab	35. vamp	48. five
10. mute	23. frog	36. start	49. hire
11. bean	24. log	37. earl	50. shoe
12. scythe	25. snuff	38. corpse	
13. vast	26. blush	39. sludge	

C. Phonetically balanced sentences [19]

1. The birch canoe slid on the smooth planks.
2. Glue the sheet to the dark blue background.
3. It's easy to tell the depth of a well.
4. These days a chicken leg is a rare dish.
5. Rice is often served in round bowls.
6. The juice of lemons makes fine punch.
7. The box was thrown beside the parked truck.
8. The hogs were fed chopped corn and garbage.
9. Four hours of steady work faced us.
10. A large size in stockings is hard to sell.

D. Sentences that request a simple response [7]

1. Name a prominent millionaire of the country.
2. How large is the sun compared with the earth?
3. Why are flagpoles surmounted by lightning rods?
4. Give the abbreviations for January and February.
5. Name the tree on which bananas grow.
6. How often does the century plant bloom?
7. What description can you give of the bottom of the ocean?
8. Explain the difference between a hill and a mountain.
9. What is the chief purpose of industrial strikes?
10. Describe the shoes of the native Hollander.

E. Random five-unit code groups read phonetically [20]

PAPA NINE ROMEO ONE UNIFORM SIX BRAVO DELTA FOUR YANKEE HOTEL MIKE PAPA QUEBEC ZERO

The various types of test material above are arranged approximately in order of decreasing difficulty. Tests based on single-syllable words will tend to be the most difficult ones, i.e., give the

lowest intelligibility scores, while those toward the bottom of the list will tend to be the easiest ones and give the highest scores. While it is possible to derive intercomparisons among the tests, this is a rather lengthy process. In general, comparisons between different communication systems, specifically different scramblers, are valid only when similar test material is used for all systems. For example, a scrambler that provides high intelligibility on 5-unit code groups may be nearly unintelligible for phonetically balanced sentences.

It is easy to conclude from the above discussion that one would like more objective ways of measuring system intelligibility and this in effect has been done for conventional communication systems. For such systems the relations between intelligibility and sound levels, noise levels, frequency response, distortion, and other factors, have been extensively studied. The results of these studies are then applied to permit specifying the performance of conventional communication systems in terms of performance characteristics such as frequency response, harmonic distortion, and noise level, all of which are much more easily measured than intelligibility itself. In the case of scramblers, the relations between intelligibility and these other characteristics have not been established. Indeed, it is not yet clear that it is possible to establish a single set of relationships that will be adequately accurate for all types of scramblers. Different relationships may be required for different types of scramblers. Thus, with the present lack of data on scrambler performance, it is essential that intelligibility be measured directly. For scramblers, there is no proven way to infer intelligibility from more conventional measurements. Various special measuring devices have been developed for measuring articulation index, a quantity closely related to intelligibility [21]. However, the validity of using these devices for testing scramblers has not yet been established.

5.2 *Speech Quality*

While intelligibility refers to the accuracy of message transmission through a system, it excludes many other significant aspects of speech communication. Systems that provide adequate intelligibility may differ in characteristics related to recognition of who is speaking, transmission of the emotional content of speech, conversational effort, etc. Good performance of scramblers in some of these areas is important to some users. In particular, police agencies often depend on good speaker recognition in their voice communication.

This general performance area is referred to as speech quality or listener preference [22]. It tends to include intelligibility as one of its elements. The test methods used [19] are similar to those used for intelligibility testing, but usually are modified to have the observer rate the system quality numerically; or in terms of categories such as excellent, good, fair, poor, and unsatisfactory; or by indicating which of two units he prefers throughout a series of paired comparisons which compare different units in rapid succession.

At present, it appears that the measurement of speech quality of scramblers is substantially more difficult than the measurement of intelligibility and that the results of such measurements will be difficult to interpret in terms of users' needs. The initial scrambler standard will probably not include speech quality performance as a parameter to be measured.

5.3 *Privacy*

In a scrambler system, one desires that the intended listeners receive a perfectly intelligible message. Correspondingly, one desires that other listeners, eavedroppers, etc., receive an unintelligible message. In this report, privacy is the term used to label the ability of a scrambler system to prevent unauthorized interception of messages. It is assumed that it is possible to assign numerical or relative ratings to the privacy provided by different scramblers, and that standard measurement procedures can be devised to determine these ratings. These assumptions seem reasonable, but are yet to be proven. The term security is sometimes used in

addition to or in place of privacy. However, at least in Federal Government usage, a voice security system would be one safe enough to handle classified security information—one that would require perhaps years of expert effort to unscramble. Because of this special usage of the term security, and because few, if any, of the scramblers now available for police use would meet the criteria for a secure system, the term privacy has been used in this report.

5.3.1 The Threat Concept

In examining police needs for scramblers, particularly with a view to determining how much privacy is required, the question arises of what is the "threat"? What level of "attack" must the scrambler system withstand?" If the only protection needed is against casual eavesdroppers who have no criminal intentions, relatively simple scramblers may be adequate. If, on the other hand, protection is needed against highly organized criminal activities, scramblers offering a high degree of privacy may be essential.

For example, consider the consequences of a criminal acquiring an unscrambler and installing it in his automobile. If the scrambler is one that uses fixed codes, it probably will be relatively easy for him to determine which code is in use at any particular time, thereby possibly rendering the whole scrambler installation relatively useless. Clearly, fixed-code scramblers do not offer adequate privacy under such circumstances. On the other hand, if the scrambler were one that used continually changing codes, it probably would be much more difficult for the criminal to find the correct key. It may be practically impossible to do so just by trying various combinations, especially if the key were changed daily. A possible next step for the criminal would be to gain knowledge of the key from someone in the police agency who had access to it. The protection against such a move would be to strongly limit the number of agency people who had access to the keys. In part this could be done by having the key setting switches in a locked compartment of the scrambler, accessible to only a few highly trusted staff members.

It should be clear from the preceding discussion that the proper choice and use of scramblers is very dependent on the level of the threat. Specifically:

a) From whom must the information be kept?
b) How long must the information be kept private?
c) What skills does the opponent have?
d) What resources does the opponent have?

Once the threat has been evaluated it should be possible to determine the level of privacy required in a scrambler to withstand that threat. Since the costs of scramblers tends to increase rapidly as privacy requirements increase, it is desirable to evaluate the threat as realistically as possible and not purchase more privacy than is necessary

5.3.2 Privacy in Scramblers Having Fixed Codes

Scramblers that employ fixed codes achieve privacy by requiring the intended receiver of the message to have an unscrambler that is similar to the scrambler itself. Anyone possessing the appropriate unscrambler can hear the message. It is helpful but not essential to an eavesdropper to know which specific code is being used in systems that have a number of codes available. For such scramblers it is usually possible for the eavesdropper to tune in to the proper code just as one tunes a radio receiver to the desired station. For example, in units that have multiple code-setting switches, such as fixed-code band-splitters, it will probably be possible to adjust each of the switches in succession until clear reception is obtained [23]. Few of the total number of possible codes need be tried.

For some fixed-code scramblers, it is possible to unscramble messages, probably with some loss of intelligibility, with devices less complex than the normal unscrambler. Thus an opponent may be able to eavesdrop by using equipment that is less expensive than the equipment used by the police agency itself. For example, a radio technician can construct an inverter from readily available parts costing only $20 [24].

In summary, scramblers that use fixed codes offer relatively low privacy because they offer little or no protection against an opponent who possesses a similar unscrambler or equivalent device.

5.3.3 Privacy in Scramblers Using Continually Changing Codes

Scramblers with continually changing codes apply cryptographic techniques to voice scrambling in an attempt to achieve a substantially higher degree of privacy than is possible with fixed codes. The scrambler designer attempts to force opponents to employ cryptanalysis to unscramble the message and to make mere possession of an unscrambler by an opponent be of relatively little value. As was previously discussed, this is done by designing units to have so many different key settings available for use that the opponent cannot find the correct key in any reasonable amount of time just by trying different settings one after the other. If keys are changed daily then a few thousand different settings may be adequate [9]. This is true because in many systems of this type the key setting at the unscrambler must be correct at the start of a transmission to synchronize the two units properly. Only one new key setting can be readily tested on each transmission.

In practice, two factors can reduce the privacy of these scramblers: cryptographically weak systems and non-cryptographic attacks. It is well beyond the scope of this report to include any discussion of cryptographic techniques. These are excellently covered in the literature [25, 26, 27]. However, one important fact is that the number of different key settings available is not necessarily a direct measure of cryptographic security. A system with 1,000,000 key settings may be easier to break than one with 1,000 settings. The most significant consideration is likely to be how the key stream is generated, not the number of key settings. A comment from the literature on cryptanalysis is pertinent in this connection [1].

> Many inventors also invoke the vast number of combinations of keys afforded by their system as proof of its invulnerability. To exhaust the possible solutions would take eons, they contend . . . [erroneously]. For, as Shannon [28] has shown, the cryptanalyst does not go after these possibilities one by one. He eliminates them millions at a time. Moreover, the trials progress from the more probable to the less probable hypotheses, increasing the cryptanalyst's chance of striking the right one early. 'Whereas complete trial and error requires trials to the order of the number of keys,' Shannon wrote, 'this subdividing trial and error requires only trials to the order of the key size in bits,' a very much smaller number.

It is thus clear that the number of key settings is an inadequate measure of privacy.

A scrambling system that is resistant to cryptographic attacks can sometimes be unscrambled by other means. These non-cryptographic methods, which ignore the coding and instead work directly on the scrambled voice signal, may allow an opponent to unscramble a message with relative ease. The rolling-code band splitter is reported to be susceptible to such attacks [9, 13].

In summary, scramblers that use continually changing codes have the potential for offering a high level of privacy. However it is essential that their levels of privacy be evaluated by actual tests and that resistance against both cryptographic and non-cryptographic attacks be determined in these tests.

5.3.4 Measuring Privacy

Consider now the question of how to define and measure the privacy of a scrambler, either in a relative or an absolute sense. In the previous discussion it has been assumed that privacy can be measured. It will be seen from the discussion below that there are substantial problems in defining standard measurement procedures for privacy.

Part of the problem is that the present approach to determining scrambler privacy is not one of measurement, but one of attack. Given a new scrambler, the expert will try a variety of ways to unscramble the messages, starting with simple attacks and proceeding to more complex ones, or perhaps starting with an attack that previously worked with that general type of scrambler. This

approach is both difficult to specify and difficult to measure. Some characteristics that are or may be measurable include:

a) the level of expertise required to break the system;
b) the amount, kind, and cost of the equipment required; and
c) the time required, both for the first time a new system is attacked and subsequent times after the user changes the code or key setting.

It appears that the first of these characteristics, degree of expertise, will be the most difficult to measure. In addition, the required equipment and time can depend strongly on expertise, thus making them less reliable measures. Suppose that one could eliminate the need to measure expertise by writing a set of procedures to be followed in attacking a scrambler. These procedures would describe the various attacks in sufficient detail so that any adequately equipped laboratory could try first one and then another attack to see which were successful and which were not. These results would then be interpreted according to a predetermined rating system to indicate the privacy level of the scrambler. This approach, if it can be made to work, solves the problem of how to specify and measure privacy.

Now to address the second part of the problem. Who is allowed to have copies of the standard for measuring privacy? Normally one would try to get wide distribution of all of the standards so that buyers, sellers, and users all can have a common basis for describing the performance of the equipment. But the privacy standard just described would be very helpful to opponents, too, be they casual eavesdroppers or criminals, since it would tell them exactly how to proceed to decode scrambled messages, what equipment to use, and how long it would take. The standard which was designed to help users get the scrambler performance they need would give their opponents just the information needed to defeat the system. It thus appears that if such a standard for privacy is developed, the standard itself will have to be private and to receive only limited distribution, thereby reducing its usefulness to users. At present it is not clear how to resolve this dilemma.

5.4 General System Characteristics

The fourth area under consideration includes the pertinent performance characteristics that do not fall directly into one of the first three categories. The items tend to be similar to those that are usually contained in standards for more common communications equipment. In many cases they are closely related to intelligibility, quality, and privacy in that they specify conditions that affect these three characteristics. For discussion purposes, the general system characteristics are divided into three parts: electrical, environmental, and installation aspects. The following sections list questions which focus attention on specific performance attributes which must be considered when planning the use of voice privacy equipment. While the focus may appear to be on mobile units, essentially the same considerations do apply to base station and portable units.

5.4.1 Electrical Characteristics

a) Interface to transceiver

1. Does the scrambler plug into the transceiver or must the transceiver be modified to accept it? Are voltage levels and impedance requirements similar?

2. If modifications are necessary, how extensive are they and will they change any transceiver characteristics such as output power and harmonic distortion? At what electrical location does the scrambler connect to the transceiver?

3. Can either a defective transceiver or a defective scrambler be replaced without a significant readjustment or retuning of either the transceiver or scrambler?

b) Transceiver Performance

1. Does the scrambler operating in the clear mode reduce the performance of the transceiver?

2. If the scrambler fails or is removed temporarily, can the transceiver continue to be used?

3. Does the scrambler permit proper operation of squelch circuits and selective-signalling (tone) arrangements?

c) Scrambler Performance

1. What transceiver signal-to-noise ratio is required for proper operation?

2. What audio bandwidth is required for proper operation? (Note that audio bandwidth will depend on the characteristics of transceivers, base stations, repeaters, satellite receivers, and telephone lines.)

3. How is synchronization between scrambler and unscrambler affected by system noise, ignition noise, signal fades, very strong signals, and lengths of transmissions?

4. How long is required to establish synchronization?

5.4.2 Environmental Characteristics

1. What temperature and humidity ranges must be tolerated?

2. What shock and vibration levels must be tolerated?

3. What power supply variations must be tolerated?

4. Does unit operate properly in the radio-frequency fields and conducted rf signals from the transceiver?

5.4.3 Installation Characteristics

1. Is the scrambler secured from theft or tampering?

2. Are the key-setting switches protected from unauthorized access?

6. COMMERCIALLY AVAILABLE SCRAMBLERS

An extensive search has been conducted to identify all of the narrow-band voice scramblers being offered on the open market for police use. Units that were not offered as standard commercial items were excluded, as were devices that clearly required more than 3000-Hz bandwidths. The results of this survey are summarized in tables 1 and 2. Manufacturers' complete names and addresses are given in table 3 as an aid to proper identification of the various units. These data are presented to indicate the range of equipment choice that exists and to illustrate what types of technical data are commonly available. The listed units have not been examined or tested, nor has an attempt been made to evaluate or validate any of the data supplied by the manufacturers. Features and characteristics that are common to all or nearly all units are not given in the tables but are presented below.

TABLE 1.

1	2	3	4	5	6
				CODES OR KEYS	
MANUFACTURER	MODEL	APPLICATION	TYPE	Number	Selection Method
California Security Products	105E	T	Inverter		Set at factory
Com-u-trol	PT 101/102 HS 110/140 RT 120S	T,M,RT	Inverter	10	Plug-in module
Controlonics	CT-200/300/400/500	T,RT	Inverter	10	Plug-in module
	VIP-200	M	Dual inverter	4	Plug-in module
	PD-101	M,P	Inverter	16	Plug-in module
Controlonics	PD-101 Sigma	M	Dual inverter	16	Plug-in module
DTS	AX,DX,HX,RX	T,RT	Inverter		Plug-in module
Johnson	541	PS	Inverter	18	Plug-in module
MIECO	P-10/11/25	M,T	Inverter	5 Transmit, 5 Receive	Switches or set at factory
Motorola	D1021/2/3	M	Inverter	1	None
Pye TMC	S2N	T	Inverter	2	Set at factory
RCA	RS-37	M	Inverter		Set at factory
	RS-38	M	Inverter	5	Switch
Singer	196C	T,RT	Inverter	1 3000 Hz	None
TCC	105	M,P	Inverter	5 Transmit, 5 Receive	Switches
Lynch	E75/E75T	M,T	4 or 5-band band-splitter	4-band: 144 5-band: 1408	Plug-in module
MIECO	P-35A	RT,T	5-band band-splitter		Switches
	P-38	M	4-band band-splitter	8	Switch
	P-41	RT,T	6-band band-splitter		Switches
RCA	RS-39	M	4-band band-splitter	8	
Scientific Radio	SR-800	T,RT	5-band band-splitter	128 or 3840	Plug-in module
Singer	2193B/MA/MB	M,T,RT	5-band band-splitter	449 Transmit 449 Receive	Plug-in module or switches

NOTES:

Column 3: Application

M. Mobile transceiver and base station
P. Personal portable transceiver
PS. Personal portable transceiver with integral scrambler
RT. Radiotelephone or base station
T. Telephone

Column 12: Other Characteristics

1. 8% maximum audio harmonic distortion
2. -40 dB direct signal feedthrough
3. 2500-Hz or 3000-Hz carrier frequency
4. -60 dB direct signal feedthrough

7	8	9	10	11	12	13	14	15
PERFORMANCE CHARACTERISTICS								
Speech input band, Hz	Scrambled signal band, Hz	Audio output, W	Carrier suppression, dB	Temperature range, C	Other	INTERFACE	SPECIAL FEATURES AND OPTIONS	COST, $
						C,		
						C,TH		
300-3000	300-3000		40-60	-30 to +60		TL,TH,C	B,AC,FD	310-445
300-3000	300-3000	3	40-60	-30 to +60		M/S		
300-3000	300-3000	3	40-60	-30 to +60		M/S,HI	a,b	297-485
						M/S	f	158-602
						TL,TH,C		363-493
					1	None	c	950
300-2200		2	50			M/S,C	B	215-330
300-3000			60	-30 to +60	2	S,M/S		260-435
300-2200 or 300-2700					3	300/600:2/4	d	416-462
300-2200		2	50			M/S		
300-2200		2	50					
250-2750	250-2750		60		4	600 ohm: 4-wire	FD	Approx. 700
300-2500	300-2200		50	-20 to +60		M/S	FD,BP	260-569
250-2300 or 250-2900		2		0 to +50				1995
250-3000			40			4 wire		1595
250-2450		5	40			M/S	e	655
300-2850			50			4 wire		1995
			5			M/S		
250-3000			60	-30 to +65		600:2/4		850-985
300-3000		5	55	-30 to +60	4	600:2/4 M/S		1850-3500

Column 13: Interface

C. Acoustic/magnetic coupler to telephone handset
HI. High impedance
M/S. Microphone/speaker
S. Special (Interfaces to manufacturers own mobile transceiver)
TH. Replaces telephone handset
TL. Telephone line (replaces telephone instrument)
300/600:2/4. 300-ohm or 600-ohm 2-wire or 4-wire line
600:2/4. 600-ohm, 2-wire or 4-wire line

Column 14: Special features

a. Unit available for installation in E.F. Johnson FM-540 transceiver
b. Built into telephone handset
c. Compatible with Controlonics PD-101
d. Includes limiters
e. Compatible with MIECO P-10/11
f. Unit modifies Controlonics PD-101 to provide greater privacy

Options

AC. 115-V AC adapter
B. Battery powered (internal)
BP. Battery pack
FD. Full duplex

TABLE 2.

1	2	3	4	5	6
				CODES OR KEYS	
MANUFACTURER	MODEL	APPLICATION	TYPE	Number	Selection Method
Boeing	BE1007	M,RT	Frequency-hopping inverter with tone masking	Greater than 200,000	Switches
Controlonics	PD101X	M	Frequency-hopping inverter	16/family, 20 families	Plug-in module and internal module
	PD101XL	M	Rolling-code 5-band band-splitter	16 per family 20 families	Plug-in module and internal module
Datotek	DV-505	T,RT	Rolling-code 5-band band-splitter	2,000,000/family 16,000,000 families	Switches and plug-in-module
Ground Data	203	M,T,RT	Frequency-hopping inverter	10,000/family 300,000 families	Switches and internal module
Ground Data	204	M,T,RT	Frequency-hopping inverter with independent frequency-hopping tone masking	4,000,000	Plug-in module with switches
MIECO	P-37	RT,T	Rolling-code 5-band band-splitter	Greater than 10,000	Switches
TCC	107	M,P,T	Inverter with tone and sideband masking	25/family, 4 families	Plug-in module and set at factory
	207	M,T	Band-splitting, frequency-hopping inversion, and tone and noise masking	122,800	Switches

NOTES:

Column 3: Applications

M. Mobile transceiver
P. Personal portable transceiver
PS. Personal portable transceiver with integral scrambler
RT. Radiotelephone or base station
T. Telephone

Column 12: Other Characteristics

4. -60 dB direct signal feedthrough
5. Code changes 4/second
6. Maintains synchronism for at least 20 minutes
7. Code changes 50/second
8. Code changes 2/second
9. Sync time is 1 second
10. Also available for 300-Hz to 2800-Hz, 3100-Hz, or 3400-Hz channel response. (-10 dB points relative to 1 kHz)
11. Maintains synchronism for at least 3 minutes

7	8	9	10	11	12	13	14	15
PERFORMANCE CHARACTERISTICS								
Speech input band, Hz	Scrambled signal band, Hz	Audio output, W	Carrier suppression, dB	Temperature range, C	Other	INTERFACE	SPECIAL FEATURES AND OPTIONS	COST, $
300-3000		5		-20 to +60	11	M/S	h,i	800-1200
300-3000	300-3000	5	60	-30 to +60		M/S	f,i	730
							f	810
377-2457	377-2457	4	60	0 to +50	4,5,6	600:2/4, TL,C,TH	g	6000
350-2700				-30 to +70	7	M/S,TL, 600:2/4, C,T	h,i, VOX	less than 1000
300-2400	300-2750			0 to +60	7	M/S,TL, 600:2/4,T	VOX	2250
			40		8,9		FD	3695-4295
	300-2500	4		-30 to +60	10	M/S, HI, 600:2/4, C,TH	i	595-1500
	300-2400	5		-30 to +60		M/S 600:2/4	h,i	1870-2585

Column 13: Interface

C. Acoustic/magnetic coupler to telephone handset
HI. High impedance
M/S. Microphone/speaker
T. Telephone instrument
TL. Telephone line (replaces telephone instrument)
TH. Replaces telephone handset
600:2/4. 600-ohm, 2-wire or 4-wire line

Column 14: Special features

f. Unit modifies Controlonics PD-101 to provide greater privacy.
g. Can also operate as fixed 5-band band-splitter
h. Selective calling
i. Clear override

Options

FD. Full duplex
VOX. Voice-actuated switch for telephone use

TABLE 3. Manufacturers

Boeing Electronics Products
P.O. Box 24666
Seattle, Washington 98124

California Security Products, Inc.
21748 Devonshire Street
Chatsworth, California 91311

Com-U-Trol Division of DASA Corp.
4825 Scott Street
Schiller Park, Illinois 60176

Controlonics Corp.
One Adams Street
Littleton Common, Massachusetts 01460

Data Transmission Sciences, Inc.
P.O. Box 1308
Danbury, Connecticut 06810

Datotek, Inc.
P.O. Box 12388
Dallas, Texas 75225

E. F. Johnson Co.
Waseca, Minnesota 56093

Ground/Data Corp.
4014 N.E. 5th Terrace
Fort Lauderdale, Florida 33308

Lynch Systems Inc.
204 Edison Way
Reno, Nevada 89502

MIECO, Inc.
1928 Green Springs Drive
Timonium, Maryland 21093

Motorola Communications and Electronics, Inc.
1301 E. Algonquin Road
Schaumburg, Illinois 60172

Pye TMC
15 Sheffield Street
Toronto, 385 Ontario
CANADA

RCA Mobile Communications Systems
Meadow Lands, Pennsylvania 15347

Scientific Radio Systems, Inc.
367 Orchard Street
Rochester, New York 14606

Singer Tele-Signal
250 Crossways Park Drive
Woodbury, Long Island, New York 11797

Technical Communications Corp.
442 Marrett Road
Lexington, Massachusetts 02173

6.1 Common Characteristics and Features

The following list describes the characteristics and features shared by most or all units in the tables. Exceptions are noted in the tables under the "Other" and "Special Features and Options" headings.

Half-duplex—The unit is capable of scrambling and unscrambling (transmission and reception) but only one of these at any time. A minimum system contains two units, one at each end of the radio or telephone link.

Compatibility—In general, units from different manufacturers are not compatible with each other. Most mobile units are available to operate with any mobile transceivers, but the specific model must be identified.

Power supply—Units for mobile operation operate from the normal 12 volt automobile battery. Units for fixed operation operate from the nominal 115 v AC line.

Mounting arrangements—Mobile scramblers usually come as single units for under-dash mounting or as two units, an under-the-dash control head and a trunk-mounted electronic unit. Base-station scramblers usually come as single units for tabletop or relay rack mounting.

6.2 Description of Tables

In preparing the tables, scramblers were divided into three categories: fixed-code inverters, fixed-code band-splitters; and all other types. Data on the inverters and band-splitters are presented in table 1, arranged alphabetically by manufacturer for each of the two types. Data on all other types are given in table 2, alphabetically by manufacturer. The listing of a unit in table 2 does not imply that it is superior to units in table 1. Blanks in the tables indicate that the manufacturer has not supplied the corresponding data.

Columns 1 and 2 give manufacturer and model number. Different models are grouped together as a single entry when they represent merely different mechanical or electrical versions of the same unit.

Column 3 lists the intended application. The symbol, "M," designates units designed for use with mobile transceivers and their associated base stations. "T" designates units for use with telephone systems. "P" designates units for use with personal/portable transceivers. "PS" designates a personal portable transceiver with a self-contained scrambler. "RT" (radio-telephone) designates units that appear to be designed for base station use only, where no version is offered for mobile installation.

Column 4 lists the scrambling principle used. The terms used here are chosen to be self-consistent and may differ slightly from the manufacturers' terminology.

Columns 5 and 6 indicate how many different codes or keys are available and how they are selected. The term plug-in module is used in a general sense to indicate all plug-in elements, including elements that do not contain any electronic components but simply act as a mechanical key or switch.

Column 7 lists the speech bandwidth that is accepted at the input to the scrambler. It is assumed that voice frequencies outside of this band are rejected by the scrambler and not utilized.

Column 8 lists the bandwidth of the scrambled speech signal. Note that while this is a crucial characteristic in determining the compatibility between given scramblers and transceivers, most manufacturers do not supply this information.

Column 9 lists the audio power output of those units designed to drive a loudspeaker directly. This is a less significant factor for units that interface in other ways, and data for the other units have been omitted.

Column 10 lists carrier suppression; that is, the amount that internal reference signals are reduced relative to the normal scrambled output. It is not clear that all manufacturers measure this in the same way, and the values therefore may not be comparable.

Column 11 lists the ambient temperature range specified for proper operation.

Column 12 indicates some other performance characteristics given by the manufacturer that may be important to scrambler performance but did not fit elsewhere in the tables.

Column 13 describes the intended methods of interfacing the scrambler with the transceivers and base stations. Note that most suppliers will probably furnish units to meet any interface requirements. Those listed here are the most readily available ones.

Column 14 indicates special features that are supplied as standard items with specific units and optional items available at extra cost.

Column 15 indicates the advertised price per unit, in unit quantity, or the corresponding range of prices for various versions of the same unit.

7. HINTS FOR THE PROSPECTIVE PURCHASER

As has already been indicated, this report has been prepared as one of the preliminary steps toward developing a guideline and a standard for scramblers. It is hoped that the present report will be useful both in understanding and applying the standard when it is available, and in assisting agencies in purchasing scramblers in the interim. In this latter regard the following suggestions are offered:

a) Evaluate the threat situation as realistically as possible and do not buy a more complex scrambler system than you need.

b) Get a factual explanation of the scrambler operating principle used, in terms that will allow you to compare various scramblers. Assume that your opponents will have at least as much information about the units as you do.

c) Ask suppliers the questions listed above in section 5.4 and compare their answers with your needs wherever possible.

d) Determine which installation and performance aspects the supplier will take responsibility for and which you must be responsible for.

e) Get a demonstration, using your entire com-

munications system, under a variety of normal and unusual operating conditions. (A one-week trial by users under normal operating conditions can be very informative.) Such a demonstration is essential before purchasing scramblers. During this demonstration, carefully observe the installation procedures to see how much modification and adjustment of scramblers and transceivers are required to achieve satisfactory operation.

f) Do not test scramblers with only your best transceivers if they must work with average and poor transceivers. Adding scramblers will usually reduce the intelligibility achieved in a system and this reduction may not be tolerable in situations that were marginally accepted without scramblers.

g) Be prepared to encounter significant installation and maintenance difficulties. Until otherwise proven, plan to do more routine maintenance on transceivers that use scramblers than on those that do not.

APPENDIX A. REFERENCES

1. Kahn, D., *"The Codebreakers,"* (Macmillan Company, New York, 1967) pp. 551–560, 776.
2. *"LEAA Police Equipment Survey of 1972, Volume II: Communications Equipment and Supplies,"* NILECJ-RPT-0002.00, U. S. Department of Justice, Washington, D. C. 20530.
3. Phillips, V. J., Lee, M. H., and Thomas, J. E., *"Speech Scrambling by the Re-Ordering of Amplitude Samples,"* The Radio and Electronic Engineer, Vol. 41, No. 3 (March 1971) pp. 99–112.
4. Blesser, B. A., *"Inadequacy of a Spectral Description in Relationship to Speech Perception,"* Acoustical Soc. America, 78th Meeting Abstracts, J. Speech and Hearing Research, Vol. 15, (Acoustical Society of America, New York, 1972) p. 19.
5. Richey, J. L., as cited in Blesser, B. A., *"Speech Perception Under Conditions of Spectral Transformation: I. Phonetic Characteristics,"* J. Speech and Hearing Research, Vol. 15, (Acoustical Society of America, New York, 1972) p. 25.
6. Beers, Y. O., personal communication (1973).
7. Fletcher, H., *"Speech and Hearing in Communication,"* (D. Van Nostrand Company, Inc., New York, 1953) p. 300 and 352.
8. McCalmont, A. M., private communication (1972).
9. McCalmont, A. M., *"Communications Security for Voice—Techniques, Systems, and Operations,"* Telecommunications (April 1973) pp. 35–42.
10. Alexander, D. M., *"Speech Privacy Circuit,"* Signetics Linear Phase Locked Loops Application Book, (Signetics Corp., Sunnyvale, California, 1972) pp. 66–68.
11. U.S. Office of Scientific Research and Development, *"Speech and Facsimile Scrambling and Decoding,"* Summary Technical Report of Division 13, NDRC, Vol. 3 (Washington, D.C., 1946).
12. Motorola Solid State Technology, Vol. 3, No. 1 (1973) p. 53.
13. French, R. C., *"Speech Scrambling,"* Electronics & Power (July 1972) pp. 263–264.
14. EIA Standard, RS-237, *"Minimum Standard for Land-Mobile Communication Systems Using FM or PM in the 25–470 MC Frequency Spectrum"* (Electronic Industries Association, Washington, D.C., August 1960).
15. Miller, C. K., *"Voice Scramblers in Two-Way Systems,"* Communications News (August 1972) pp. 32–33.
16. U.S. Patent No. 251, 292 (December 20, 1881).
17. Schubert, E. D., and Owens, E., *"CVC Words as Test Items,"* private communication.
18. American National Standards Institute, *"USA Standard Method for Measurement of Monosyllabic Word Intelligibility,"* USAS S3.2–1960 (American National Standards Institute, New York).
19. 1965 Revised List of Phonetically Balanced Sentences (Harvard Sentences) as given in IEEE Standard No. 297, IEEE Recommended Practice for Speech Quality Measurements, (Institute of Electrical and Electronics Engineers, Inc., New York, 1969) p. 15.
20. Smith, R., personal communication (1973).
21. Hecker, M. H. L., von Bismarck, G., and Williams, C. E., *"Automatic Evaluation of Time-Varying Communication Systems,"* IEEE Transactions on Audio & Electroacoustics, Vol. AU-16, No. 1 (March 1968) pp. 100–106.
22. Rothauser, E. H., *"A Comparison of Preference Measurement Methods,"* The Journal of the Acoustical Society of America, Vol. 49, No. 4 (Part 2) (1971).
23. Maitland, P., *"Communications Security,"* 1972 Carnahan Conference on Electronic Crime Countermeasures, private communication (University of Kentucky, 1972).
24. Rakes, C. D., *"Builds e/e's Scramble Phone,"* Electronic Hobbyist, (Spring-Summer 1973) pp. 27–30, 119–120.
25. Twigg, T., *"Need to Keep Digital Data Secure?"*, Electronic Design, Vol. 23 (Nov. 9, 1972) pp. 68–69.
26. Meyer, C. H., and Tuchman, W. L., *"Pseudorandom Codes Can Be Cracked,"* Electronic Design, Vol. 23, (Nov. 9, 1972) pp. 74–76.

27. Geffe, Philip R., *"How to Protect Data with Ciphers That are Really Hard to Break,"* Electronics (Jan. 4, 1973) pp. 99–101.

28. Shannon, C. E., *"Communication Theory of Secrecy Systems,"* Bell System Technical Journal, Vol. 28, also Bell Monograph #1727, pp. 656–715.

APPENDIX B. GENERAL BIBLIOGRAPHY

Arizona Public-Safety Communications Officers Association, *"1969 Report on Public Safety—Voice Privacy Equipment,"* Engineering and Research Committee. Arizona APCO (October 1969).

Baker, H. C., *"Voice Privacy Transmission Techniques,"* Communication News (June 1972) pp. 38–41.

Guanella, G., *"Methods for the Automatic Scrambling of Speech,"* Brown Boveri Review (December 1941) pp. 397–408.

Carlson, R. L., Tellez, J. M. Schreiber, W. L., *"Privacy of Voice Communication,"* Security World (May 1972) pp. 49–53.

Detwiler, W., *"Scrambler Design Parameters,"* Communications (June 1970).

French, R. C., *"Computer Simulation of a Speech Scrambler,"* Conference on Digital Processing of Signals in Communications, Loughborough, Leies., England, 11–13 April 1972, (London, England, IERE, 1972) pp. 339–345.

Gill, A. J., *"Privacy Systems for Radio Telephony,"* The Post Office Electrical Engineers' Journal (October 1933) pp. 224–230.

McCalmont, A. M., and Eramo, W. J., Jr., *"Communications Privacy,"* Telecommunications (October 1970).

Rompel, J. D., *"A Discussion of the Use of Speech Scramblers with Police Radio Communications Systems,"* Electronics Research Laboratory, Montana State University (Bozeman, Montana, March 1973).

Teacher, C. F., *"Problems Encountered in the Design of Speech Privacy Systems,"* Proceedings of the 1970 Carnahan Conference on Electronic Crime Countermeasures (University of Kentucky, 1970) pp. 44–58.

Timothy, L. K., and Boll, S. F., *"A Secure Voice Communication System with Low Bit Rate and High Voice Quality,"* Proceedings 1973 Carnahan Conference on Electronic Crime Countermeasures (University of Kentucky, 1973) pp. 5–8.

☆U.S. GOVERNMENT PRINTING OFFICE: 1974 O—549–857