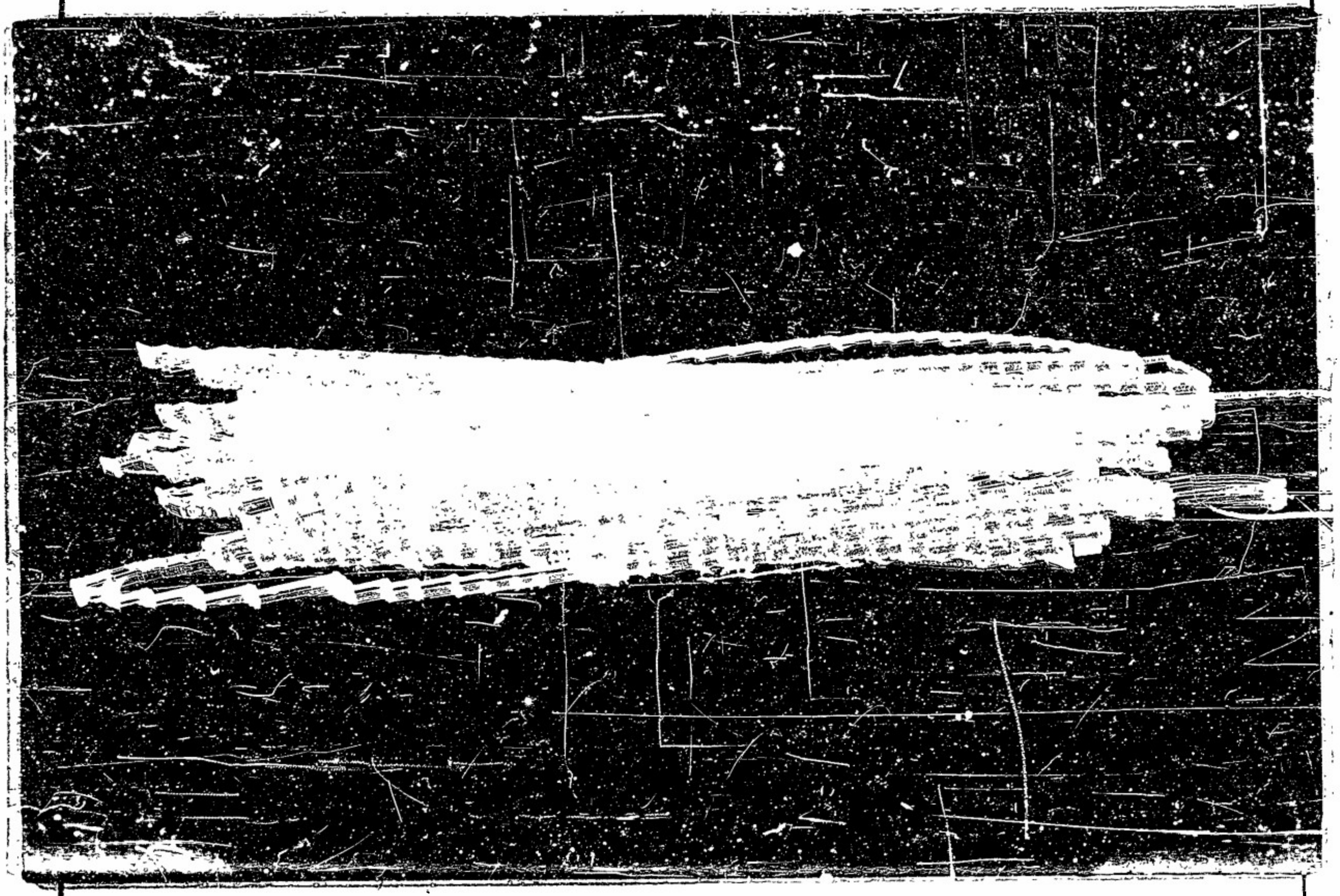
REEL – C

1170

A.T.I.

29237



29237

Final Report - Speech Privacy Problems (None)

Koenig, W.; Fowler, A. D.; Thompson, Z. C., and others (None)
Bell Telephone Labs., Inc., New York, N. Y.
Office of Scientific Research and Development, NDRC, Div. 13 5636

Aug '45 Secr. U.S. Eng. 101 photos, tables, diagrs

Several speech privacy problems of specific interest to the Bureau of Ships were studied and analyzed. In each problem the principal objectives were the evaluation of the security and the transmission performance afforded by the privacy system in question. Material submitted for study comprised working models of two privacy systems, recordings of speech scrambled by three privacy systems and paper proposals for two systems. The British modulator type 2C (manually switched) provided four fixed speech conditions, each involving either one or two simple modulation processes. The British two-dimensional privacy system utilized both frequency and time-division scrambling. The British modulator type 2C (rapidly switched) was the same as the manually switched one, as was the New Zealand switched band privacy system.

Copies of this report obtainable from Air Documents Division; Attn: MCIDXD

Electronics (3)
Communications (1)

Communication, Voice (23994.8); Communication systems, Secret (23992.87)

S-3-1

OSRD 5686
and contains reissue
of OSRD 4692
and OSRD 5232

SECRET

300

NATIONAL DEFENSE RESEARCH COMMITTEE

OFFICE OF SCIENTIFIC RESEARCH AND DEVELOPMENT

DIVISION 13 SECTION ______

OEMsr-1440

FINAL REPORT
ON
PROJECT 13-106

SPEECH PRIVACY PROBLEMS

RELATED SERVICE PROJECT NS-349

APPROVED BY
NDRC DIVISION 13

"THIS DOCUMENT CONTAINS INFORMATION AFFECTING THE NATIONAL DEFENSE OF THE UNITED STATES WITHIN THE MEANING OF THE ESPIONAGE ACT, U.S.C. 50:31 AND 32, ITS TRANSMISSION OR THE REVELATION OF ITS CONTENTS IN ANY MANNER TO AN UNAUTHORIZED PERSON IS PROHIBITED BY LAW."

O.S.R.D. NO.______ SECTION NO.______ COPY NO. 49 DATE August 18, 1945

BELL TELEPHONE LABORATORIES, INCORPORATED
NEW YORK, N. Y.

SECRET

SECRET

NATIONAL DEFENSE RESEARCH COMMITTEE

OFFICE OF SCIENTIFIC RESEARCH AND DEVELOPMENT

DIVISION 13

FINAL REPORT
ON
PROJECT 13-106
SPEECH PRIVACY PROBLEMS

RELATED SERVICE PROJECT NS-349

August 18, 1945

Contract OEMsr-1440

Contractor: Western Electric Company, Inc.
120 Broadway, New York 5, N. Y.

Technical Representative: A. D. FOWLER

Bell Telephone Laboratories, Inc.
463 West St., New York 14, N. Y.

SECRET

PROJECT 13-106

RELATED SERVICE PROJECT NS-349

"SPEECH PRIVACY PROBLEMS"

Foreword

Work on speech privacy problems was formerly carried on under Project C-43, Contract No. OEMsr-435. Reference should be made, therefore, to Parts I and II of the final report on that project for background material on this subject. Part I is a comprehensive report covering the problems involved in the interception, diagnosis, decoding and evaluation of speech privacy systems. Part II is a compilation of reports, such as this, covering specific investigations.

SECRET

FINAL REPORT

ON

PROJECT 13-106

SPEECH PRIVACY PROBLEMS

TABLE OF CONTENTS

SECRET

PROJECT 13-106

RELATED SERVICE PROJECT NS-349

FINAL REPORT

SPEECH PRIVACY PROBLEMS

August 18, 1945

1. Introduction

1.1 History of Project

This project was initiated November 1, 1944, for the study of speech privacy problems of interest to the U. S. Navy Department, Bureau of Ships. Work of a similar nature had previously been carried on under Project C-43, Contract OEMsr-435, the technical aspects of which terminated December 31, 1944. The final report on Project C-43 provides background material for the present project.

Originally, Contract OEMsr-1440 covered the 4-month period ending February 28, 1945. Later supplements extended the terminating date first to June 30, 1945, and then to August 31, 1945.

1.2 Nature and Scope of Work

The work done under this project consisted of studies and analyses, supplemented by laboratory tests, of several speech privacy problems of specific interest to the Bureau of Ships. In each problem the principal objectives were the evaluation of the security and the transmission performance afforded by the privacy system in question.

The material submitted for study and analysis under this project comprised working models of two privacy systems, recordings of speech scrambled by three privacy systems and paper proposals for two systems.

Security evaluations were made under favorable laboratory conditions. It has been assumed that the enemy (1) is thoroughly familiar with the speech privacy system, (2) has the necessary intercept, recording and decoding equipment, (3) has trained personnel, (4) is in a position to receive adequate signals, and (5) is completely organized so that no time is lost in obtaining and making use of intelligence from the decoded message. The security ratings assigned to the several systems which have been evaluated have not taken into consideration any practical difficulties which might be encountered in the field or under combat conditions where the work of intercepting, diagnosing, decoding, and obtaining intelligence from scrambled messages must be carried on under stress. Some of these practical problems are discussed in Chapter VII of the final report on Project C-43.

1.3 Assignments.

The following assignments of work on this project were authorized by letters dated January 18, 1945, and February 16, 1945, from Professor Charles F. Dalziel, Technical Aide, Division 13, N.D.R.C.

1. British Modulator Type 2C (manually switched), working models.

2. British 2-Dimensional Privacy System, recording.

3. British Modulator Type 2C (rapidly switched), recording.

4. New Zealand Switched Band Privacy System, recording.

5. New Zealand Switched Band Privacy System, working models.

6. Proposals of Dr. L. E. Gabrilovitch for privacy systems.

2. Summary of Results

The results of the work done on the several assigned problems are given in detail in Reports No. 1 to 5, inclusive, which form an appendix to this final report. These reports cover the six assignments listed above with the fourth and fifth assignments, relating to the New Zealand switched band system, being combined in one report. All of the systems considered under this project are of the short-term privacy variety. Of these the British 2-dimensional system, discussed in Section 3.2, and in Report No. 2, appears to be the most promising.

3. Brief Résumé of Systems

3.1 British Modulator Type 2C (Manually Switched), Working Models (See Report No. 1, Attached)

This system provides four fixed speech scrambling conditions, each involving either one or two simple modulation processes; the choice of any one of the four scrambling conditions or clear speech is under the control of a manual switch.

When a receiving unit, or its equivalent, is at hand, there is no difficulty whatever in discovering the proper decoding condition in a matter of seconds. The security afforded by the system is, therefore, almost nil.

The fixed code scrambles can be demodulated satisfactorily by a single modulation process without filters, it being necessary only to use the appropriate frequency of the demodulating carrier. For this reason it is possible to obtain intelligence from radio transmissions of the scrambled speech by means of an ordinary type of radio receiver equipped with a beat frequency oscillator. The efficacy of this method will, of course, depend upon having adequate relative stability of the radio carrier and the beat frequency oscillator.

These units appeared to be well constructed and operated satisfactorily from the standpoint of overall speech quality.

3.2 British 2-Dimensional Privacy System, Recording (See Report No. 2, Attached)

This system utilizes both frequency- and time-division scrambling. It employs three frequency bands and ten time elements of 0.065 second duration in a repeated code. The time delay in one direction of transmission (exclusive of delay of the transmission path) is 0.65 second.

The evaluation of this system was based on the study of one recording bearing a single sample of scrambled speech, together with samples of clear speech and speech which had been coded and decoded for comparison. An evaluation based on such limited data is necessarily tentative and should be supplemented by tests on working models.

The speech scrambled by this system appears to be invulnerable to direct listening and to other non-cryptographic attacks. It is, however, vulnerable to cryptographic attacks and a working solution of the code can probably be obtained in a matter of three or four hours. With a model of the receiving equipment at hand, it is conceivable, although it was impossible actually to try it, that a substantial amount of intelligence could be obtained in the order of half an hour. This latter method would involve the use of spectrograms from which suggestions are obtained for setting up partial decodes on the receiving unit.

The most noteworthy weakness in the British 2-dimensional system appears to be the use of a fixed repeated code. The addition of code changing means would increase the cryptographic security very greatly.

The quality of the restored (or decoded) speech presented on the recording compared favorably with the clear (or uncoded) speech on the same recording.

3.3 British Modulator Type 2C (Rapidly Switched) Recording (See Report No. 3, Attached)

This system is the same as that discussed in Section 3.1 except that means are provided for rapidly switching from one scrambling condition to another and that clear speech is used as a fifth "scrambling" condition. The order in which the scrambling conditions are selected is pre-determined according to a code which repeats after a sequence of 20 such selections, each enduring for approximately 0.065 second.

A code switching mechanism for use with the modulator 2C equipments was promised, but was never received. This would have made it possible to make a more positive evaluation of the system than can be made from the recording of scrambled speech. In fact, the results obtained from non-cryptographic attacks on the recorded scramble are considerably at variance not only with what could logically be expected, but also with the results obtained with working models of a very similar system. (See Report No. 4 on the New Zealand Switched Band Privacy System.)

Repeated listenings directly and also through a two-path superposition circuit to the recorded scramble yielded several words and phrases but very little intelligence. Similar tests on the New Zealand system (working models) yielded, on the average, 40-per cent intelligence to direct listening and 80-per cent intelligence with the two-path circuit.

Repeated listenings through an automatic analyzer-decoder circuit yielded approximately 60 per cent of the intelligence from the recorded scramble of the Modulator 2C, rapidly switched, system. This same procedure yielded practically 100-per cent intelligence on the New Zealand system.

A cryptographic solution of the repeated code sequence used in making the recorded scramble can be determined by inspection of two spectrograms in about 15 minutes.

The quality of restored speech on the recording compared favorably with the clear speech on the same recording.

3.4 New Zealand Switched Band Privacy System, Recording and Working Models (See Report No. 4, Attached)

Fundamentally, this system is very similar to the British Modulator Type 2C, rapidly switched, and differs in what appears to be only minor details: The inversion frequencies in the scrambling circuits are somewhat different; the duration of each of the rapidly switched scrambling conditions is 0.043 second (rather than 0.065 second); a sequence of 18 selections of scrambling conditions (rather than 20) comprises the coding cycle. The New Zealand system is equipped with an applique unit for automatically changing the code each cycle for a total of 625 cycles, or for a period of about eight minutes, before repeating.

A recording of two samples of speech scrambled by this system (using repeated codes) was received for analysis and most of the intelligence was obtained by non-cryptographic methods. Somewhat later, the scrambling equipment for two terminal units was received and was set up for tests and demonstration as a two-way privacy system.

The security afforded by this system is very low for military purposes and is inconsistent with its size and weight.

Repeated listenings directly to the scramble yielded on the average about 40 per cent of the intelligence to experienced observers; repeated listenings to the scramble through a two-path superposition circuit yielded about 80 per cent of the intelligence. A repeated code can be determined by an aural method, using the terminal equipment, or its equivalent, in about seven minutes. An automatic analyzer-decoder circuit yielded at least 50 per cent of the intelligence from either a repeated or a non-repeated (eight-minute) code sequence on the first listening and practically all the intelligence with few additional listenings.

By cryptographic methods, a repeated code can be determined in about 20 minutes and a non-repeated code (including the starting point of the automatic code changing unit) can be determined in about one hour.

Mechanically and electrically the units operated satisfactorily; the intelligibility of the restored speech was good but the quality, though fairly good, was somewhat inferior to what might be achieved with improvements in design.

3.5 Proposals of Dr. L. E. Gabrilovitch for Privacy Systems (See Report No. 5, Attached)

Of two proposals by Dr. Gabrilovitch, the first, described as a "Screen Secrecy Set with Narrow Audio Band", appeared to require considerable equipment to obtain only a very limited degree of security with probably poor transmission performance and a sacrifice of operating range.

The second proposal, described as a "Phase Varied Inverter-Distorter (simplified secrecy set)", although similar in basic principle to the RCA-Bedford system developed under Project C-54, offered, theoretically, some possibilities of obtaining a fairly compact and light-weight set having somewhat better restored speech quality than the Bedford system. There were, however, a number of questions regarding the degree of security, coding possibilities, and practicability of some of the electronic processes.

The second proposal was selected by the Navy for further study. In anticipation of a contract for this work, the Halstead Traffic Communications Corporation of New York, New York, undertook a preliminary engineering study of these proposals (only on the second proposal after the Navy's decision) and turned over their papers on this work to N.D.R.C. when the contract did not materialize.

A review of the Halstead papers revealed that work had been discontinued before important progress had been made toward obtaining answers to questions relating to the second proposal. There were indications that serious practical difficulties had been encountered and that a much more complicated system was being considered in order to obtain adequate coding possibilities.

Although the indications contained in the Halstead papers are not conclusive, it appears fairly evident that the development of Dr. Gabrilovitch's second proposal would tend more and more to duplicate that of the Bedford system and would offer few, if any, advantages over the latter when completed. It was, therefore, recommended that further study of this proposal be discontinued.

4. General Conclusions and Remarks

In the course of the work done under this project, a number of conclusions were reached regarding the systems under consideration and their evaluation based on the use of working models as contrasted with phonograph recordings.

4.1 Switched Band Systems

Of the systems considered, vulnerability to repeated listenings directly to the scramble is attributed to the inherent lack of privacy in some of the five speech scrambling conditions. The average intelligence obtained in listening to the five fixed scrambles is 40 per cent, which is approximately the same as obtained (on the average) when the scrambling conditions were rapidly switched. The need for scrambling conditions, each having an adequate degree of privacy, is obviously indicated.

The high yield of intelligence obtained from superposition listening is attributed mainly to the fact that some of the five scrambling conditions are not mutually private and effectively decode one another (Codes A and B in the New Zealand system and Codes 1 and 3 in the British system). This effectively reduces the available number of scrambling conditions. Hence, the five scrambling conditions should be not only inherently private but also mutually private.

The vulnerability of the systems to either direct or superposition listening is independent of whether a repeated or non-repeated code is employed.

The use of a repeated code makes the system very vulnerable to methods of cracking wherein the code is to be determined. It is necessary to decode only one cycle and successive cycles can be used to obtain confirmation.

When the system is not vulnerable to non-cryptographic attack, the use of non-repeated coding increases privacy. If the coding is truly random, it is necessary to decode each individual cycle with no opportunity for confirmation from successive cycles.

4.2 Two-Dimensional System

This type of system involving both frequency and time division scrambling affords more security than can be obtained by using either method of scrambling alone. In the case of the British system considered, the privacy could have been materially increased by using a non-repeating code, more frequency bands and shorter and more time elements.

4.3 Masking Systems

Systems of this type employ a screen of noise overlaying the signal to be masked. This is accomplished in a system suggested by Dr. L. E. Gabrilovitch, by modulating the masking and masked signals on a split-phase subcarrier. The discrimination between these two signals at the receiver requires absolute synchronization and proper phasing of the demodulating carrier. Since this is difficult to achieve in practice, because of the distortions appearing in the transmission channel, the restored speech will be of poor quality, being distorted and noisy.

The relatively large amount of power required for the masking signal reduces the efficiency of the radio transmitter in that smaller transmitting ranges are obtained for a given amount of output power.

4.4 Bedford Type Systems

Systems of this type, of which the Phase Varied Inverter-Distorter system proposed by Dr. L. E. Gabrilovitch is one, depend upon the modulation of speech by a complex coding wave to obtain privacy. Clear speech is obtained at the receiver by demodulation of the scramble with an accurately synchronized decoding wave which effectively is the reciprocal of the coding wave.

In order to avoid the possibility of partially cracking the scramble by demodulating it with a single frequency, it appears to be necessary that the complex coding wave have no predominant frequency components but, instead, should have a fairly uniform spectrum of at least several hundred cycles width within the limits of the speech band. The resulting bandwidth of the scrambled speech exceeds the width of the speech band by an amount equal to the highest frequency in the coding wave. It follows, then, that either the bandwidth of the channel conveying the scrambled speech must be wider than for normal speech bands, or the original speech band must be made narrower than normal if distortion is to be avoided.

Since an accurately synchronized decoding wave of proper phase is required for deriving clear speech at the receiver, this system is sensitive to distortions in the transmission channel. The restored speech should not, however, be as noisy as that of the masking systems. In the Bedford type systems, imperfect demodulation yields unwanted products which are proportional to the speech energy rather than to the relatively large masking energy.

Synchronization by means of a continuous modulated wave (as proposed by Dr. Gabrilovitch) is believed to be superior to synchronization by pulses as proposed in the RCA-Bedford system. In the latter instance, the wave form of the transmitted pulse is both important to the proper operation of the system and sensitive to distortions over a large part of the band of the transmitting channel.

4.5 Evaluation of Security of Systems from Recordings

Phonograph recordings of speech scrambled by a privacy system provide a less desirable means for evaluating the security of a privacy system than do working models of the system. The results of analyses based on phonograph recordings can be used for determining the nature of the privacy system and the code but even though the quality of the recording is good, difficulty may be experienced in direct or superposition listening tests.

Very often it is found that recordings, which are considered moderately good for clear speech are surprisingly inadequate for storing scrambled speech for subsequent analysis and restoration. This appears to be due to (a) harmonic distortion, which, when not too great, passes unnoticed in clear speech, and also to (b) irregular speed variations (in either the recording or reproducing systems) which prevent precise synchronization necessary in some privacy systems. However, the fact that a high quality recording is required in cracking a given privacy system, is, in itself, of considerable practical importance in evaluating the system.

The most effective cracking techniques often involve the use of a receiving unit, or its equivalent. When only recordings are available for analysis, it becomes necessary either to build an equivalent receiver or merely to speculate on what might be done with a working model. Neither of these alternatives is very satisfactory. It is, therefore, highly desirable whenever possible, that evaluations be made by tests on working models.

Att.
Appendix comprising
 Reports No. 1 to 5,
 inclusive

APPENDIX

Report No. 1 - "British Modulator Type 2C Equipment Manually Switched", January 5, 1945

Report No. 2 - "Analysis of Recording of Speech Scrambled by British 2-Dimensional Privacy System", April 28, 1945

Report No. 3 - "Analysis of Recording of Speech Scrambled by British Modulator Type 2C, Rapidly Switched", June 20, 1945

Report No. 4 - "New Zealand Switched Band Privacy System - Working Models and Recording", July 27, 1945

Report No. 5 - "Proposals of Dr. L. E. Gabrilovitch for Speech Privacy Systems", June 30, 1945

Previously issued as OSRD 4192

Report No. 1

PROJECT 13-106

REPORT NO. 1

BRITISH MODULATOR TYPE 2C EQUIPMENT MANUALLY SWITCHED

January 5, 1945

This report describes the results of an investigation of the degree of security afforded by the British Post Office speech privacy equipments designated "Modulator 2C". This work was undertaken at the request of the Navy Department Bureau of Ships in a letter of December 5, 1944.

Experimental Work

The equipments were received at Bell Telephone Laboratories, Inc. on December 7, 1944. They appeared to be in good condition except for some slight mechanical damage to the chassis of the modulator units. When the units were interconnected, however, it was found that one of the oscillators had an intermittent defect. This trouble was cleared by removing the oscillator unit, melting down the sealing compound and removing and replacing the condensers in the oscillator unit.

It had been expected that some sort of commutator switching apparatus would be included with the equipments for rapidly switching from one condition to another in some predetermined sequence as described in British Post Office Radio Report No. 994, dated 26 July 1943. However, no such switching mechanism was furnished. Instead there was only a manual switch for selecting any one of the five conditions, one straight speech and four scrambled or coded conditions.

Listening tests showed that the quality of the restored speech was generally good. The different codes, however, had distinctly different effects on the received quality. The most outstanding difference was in the low frequency transmission. Condition No. 5 (straight speech) provided the best low frequency transmission while conditions Nos. 1 and 3 cut off sharply at about 300 cycles. Conditions Nos. 2 and 4 cut off at about 500 cycles and in addition had a somewhat peculiar quality due to some inverted components appearing in the restored speech as will be seen subsequently.

The scrambled speech appeared to be unintelligible for practical purposes with all the codes. It also appeared, although no extensive tests were made, that the codes were mutually private with the outstanding exception of codes 1 and 3. This combination of codes provides almost complete intelligibility.

The length of time during which a degree of security might be expected from a fixed code system of this type depends on how much equipment the enemy must provide himself with in order to obtain intelligence, and how long it would take him to analyze the scramble and determine how to crack it. Obviously, if the enemy has a captured equipment he can quickly try the four different codes to determine which one is being used at any given moment. If he does not have a captured equipment, he must provide equipment of his own and the following experiments were undertaken to determine what equipment would be required.

The first cracking equipment tried was a simple double balanced varistor modulator* with the carrier supplied by a variable oscillator. No filters were used in either the input or the output. The scrambled speech was fed directly to this modulator, and it was found that for each of the four codes, a suitable choice of carrier frequency would provide almost complete intelligibility. For code 1 of course, which is simple inversion about 3500 cycles, the oscillator should be set at 3500 cycles. Code 3 was made intelligible by this same frequency. For code 2 a carrier of 2500 cycles was used and for code 4 a carrier of 1000 cycles. Naturally, in some of these conditions the resulting quality was rather poor but the intelligibility was judged to be almost complete.

Since the codes could be cracked by a single modulation step with no filtering, it was felt that it should be possible to decode the scrambles with the help of the beat frequency oscillator in an ordinary receiving set. In order to try this out the output of a scrambler was fed to a British Wireless Set No. 48 Mark I which happened to be available through another project. The output of the radio set was received with a National HRO receiver. It was found that for each of the codes the beat frequency oscillator could be set so as to give intelligible speech.

The two decoding methods described above were demonstrated to Lt. Comdr. C. E. Biele, Lt. Comdr. C. F. Clark, Lt. (jg) H. A. Dorschug and Ensign A. Boon of the Bureau of Ships on December 18, 1944. Lt. R. E. Bird and Lt. E. Preston

* Figure 6A page 15 Part I Final Report on Project C-43.

of the British Admiralty Delegation were also present at this demonstration.

Spectrograms

The attached Photographs 133382 and 133383 show spectrograms illustrating the coding and decoding processes described above. The first photograph shows the speech scrambled by the transmitting unit set for each of the four codes. It also shows the speech restored by the receiving unit set for the proper code. The restored speech shows the differences in the low frequency transmission mentioned above. Codes 2 and 4 show, near the middle of the frequency range, some unwanted components which can be identified as inverted because of the slopes of the harmonics. These components appear in the output due to the fact that the 2000 cycle high pass and low pass filters overlap to some extent.

The second photograph shows spectrograms of the speech partially restored by the modulator method described above. In the case of code 1, of course, the restoration is as perfect as it is with the receiving unit. In the case of code 2 a carrier leak of 2500 cycles may be seen. In the region below 2000 cycles clear speech may be seen accompanied by some unwanted modulation products. In the case of code 3 the region below 2000 cycles shows clear speech. Above 2000 cycles may be seen inverted components which however do not appreciably disturb the listener. In the case of code 4 the 1000 cycle carrier leak may be seen together with second and third harmonics. This spectrogram shows more unwanted components than appear with the other codes. It should be noted, however, that in all these spectrograms a rather high degree of level compression is used which tends to make the low level components appear more prominent than they sound.

To the right of the spectrograms in both photographs are shown diagrams of the modulation processes involved, using a convention in which the whole speech band is represented by a wedge, the wide part of the wedge representing the low frequency (high level) components and the narrow portion of the wedge representing the high frequency components. The position of the wedge in the frequency scale shows graphically how the speech band has been divided and its parts shifted in the coding processes. In the case of the partially decoded speech some of the conditions show overlapping portions of the wedges. The diagrams explain the origin of the unwanted components which may be seen in the spectrograms.

Conclusions

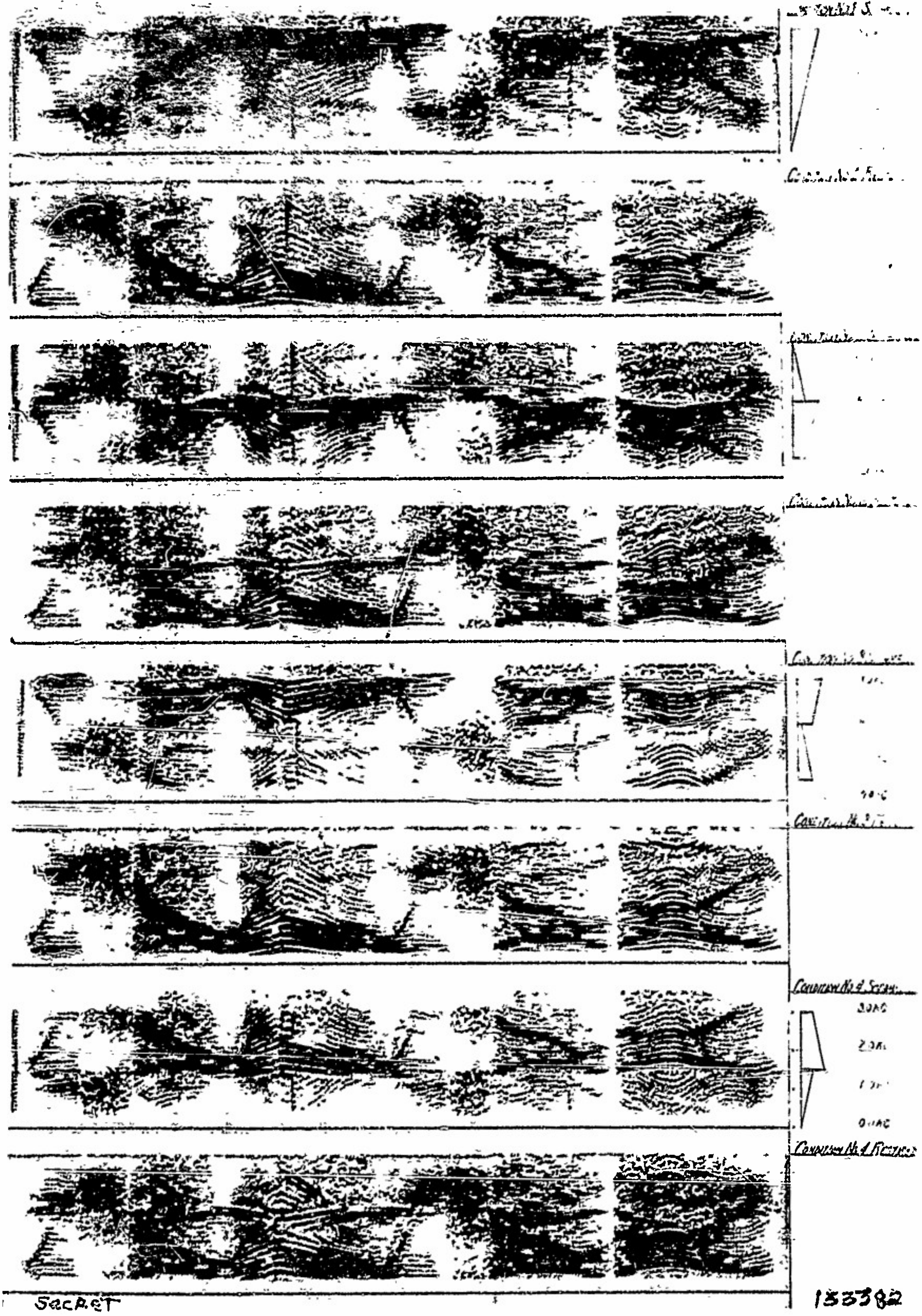
No one, of course, expects a high degree of security from a scrambling system operating on a simple fixed code. If, however, the enemy must analyze the scramble and provide himself with decoding equipment, a certain amount of surprise value can be expected. In the present case, however, the experiments described above show that the analysis can be performed very simply and the receiving equipment can also be very simple. In fact there is a possibility that the enemy, if he has the proper type of radic receiving equipment, will decode the speech by trial in a very short time after he first encounters it. Even the surprise security therefore must be regarded as very doubti l.

The Navy Department letter referred to in the introduction to this report requested a comparison of the security afforded by the Modulator 2C with that provided by the Model PF (TDS) equipment. The Modulator 2C units as furnished provide virtually no security, as discussed above. However, if the codes were rapidly switched the security would be increased. Whether it would then be comparable with the security afforded by the Model PF equipment can only be determined with certainty after the switching mechanisms are made available.

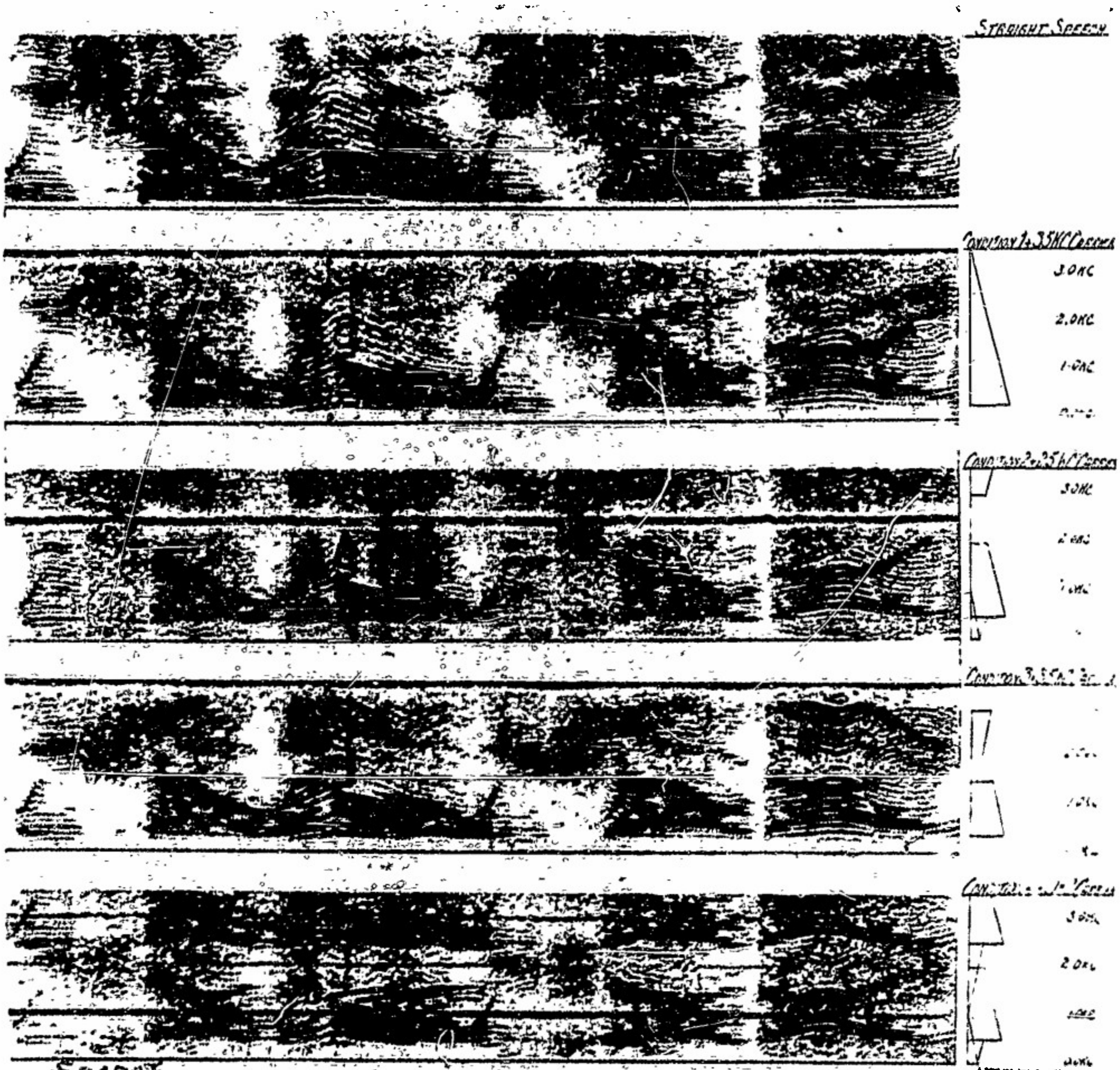
W. KOENIG

Bell Telephone Laboratories, Inc.
463 West Street
New York 14, New York

Attached:
Photographs Nos. 133382
133383


Condition No 4 Sending
3.0 KC
2.0 KC
1.0 KC
0 KC
Condition No 4 Receiving

SECRET



SECRET

133383

Previously issued as OSRD 5232

Report No. 2

PROJECT 13-106

RELATED SERVICE PROJECT NS-349

REPORT NO. 2

Analysis of Recording of Speech Scrambled by British 2-Dimensional Privacy System

Table of Contents

PROJECT 13-106

RELATED SERVICE PROJECT NS-349

REPORT NO. 2

Analysis of Recording of Speech Scrambled by British 2-Dimensional Privacy System

April 28, 1945

1. General

1.1 Introduction

A phonograph recording No. W 44/137 of speech scrambled by a British 2-dimensional privacy system was received for evaluation of this system on December 22, 1944. A recording is usually sufficient to enable the system used for scrambling speech to be diagnosed. However, complete technical information and working models of the system are essential for an accurate evaluation of the security afforded. Consequently results obtained from studies of a recording alone are an approximation. Usually the security will be less than that indicated.

In an attachment to a letter from Lt. R. E. Bird, British Admiralty Delegation, dated December 21, 1944, recording No. W 44/137 is described as follows:

> This record is a copy of an original made on May 17, 1944 when apparatus was at the stage of development outlined in Block Schematic WL 58670.* There are three sections on the record. The first (inside) section is straight speech (ex B.B.C.) passed through 400 c/s H.P. and 3500 L.P. filters only. The second section is coded and decoded speech,

* This drawing has not been available.

and the third (outside) section coded speech. All three sections represent the same speaker. The code used is an arbitrary one selected at random by a disinterested observer. At the time the original record was made, both time division and frequency translation switching were carried out by high speed relays operated from a single commutator with rotating wiper.

The work of analyzing and evaluating this recording under Project 13-106, Contract No. OEMsr-1440, was authorized by letter dated January 18, 1945, from Professor C. F. Dalziel, Technical Aide of Division 13, N.D.R.C.

1.2 Summary of Conclusions

The present appraisal of the degree of security offered by the British 2-dimensional privacy system is based entirely on tests made with this one recorded sample of coded speech in which a single repeated code was employed. Models of the privacy equipment, which normally are assumed to be in the interceptor's hands, were not available. Hence, the important part which these equipments might play in facilitating the decoding work could not be evaluated.

The security afforded by this 2-dimensional privacy system against direct listening to the scrambled speech, on the basis of the sample tested, is good. An occasional word or phrase was thought to have been understood, but upon comparison with the script of the original message these proved to be erroneous.

The code employed in the British 2-dimensional system can be determined by cryptographic methods in which the scrambled segments of a spectrogram are restored to normal order by a matching process.

A solution of the code employed in the sample submitted for analysis has been obtained but no means have been available for checking the accuracy of the solution. It should be noted, however, that it is probably not necessary that the code be entirely correct to enable a substantial amount of intelligence to be obtained. Including the time required to prepare the proper material for matching (30 minutes to one hour), it is estimated that a working solution of the repeated code could be obtained by a trained crew in three to four hours. If models of the privacy equipment were available these might be used to reduce the time required to find the code. While it has been impossible to make any actual tests without models of the equipment, it is conceivable that a substantial amount of intelligence could be obtained in the order of half an hour.

and the third (outside) section coded speech. All three sections represent the same speaker. The code used is an arbitrary one selected at random by a disinterested observer. At the time the original record was made, both time division and frequency translation switching were carried out by high speed relays operated from a single commutator with rotating wiper.

The work of analyzing and evaluating this recording under Project 13-106, Contract No. OEMsr-1440, was authorized by letter dated January 18, 1945, from Professor C. F. Dalziel, Technical Aide of Division 13, N.D.R.C.

1.2 Summary of Conclusions

The present appraisal of the degree of security offered by the British 2-dimensional privacy system is based entirely on tests made with this one recorded sample of coded speech in which a single repeated code was employed. Models of the privacy equipment, which normally are assumed to be in the interceptor's hands, were not available. Hence, the important part which these equipments might play in facilitating the decoding work could not be evaluated.

The security afforded by this 2-dimensional privacy system against direct listening to the scrambled speech, on the basis of the sample tested, is good. An occasional word or phrase was thought to have been understood, but upon comparison with the script of the original message these proved to be erroneous.

The code employed in the British 2-dimensional system can be determined by cryptographic methods in which the scrambled segments of a spectrogram are restored to normal order by a matching process.

A solution of the code employed in the sample submitted for analysis has been obtained but no means have been available for checking the accuracy of the solution. It should be noted, however, that it is probably not necessary that the code be entirely correct to enable a substantial amount of intelligence to be obtained. Including the time required to prepare the proper material for matching (30 minutes to one hour), it is estimated that a working solution of the repeated code could be obtained by a trained crew in three to four hours. If models of the privacy equipment were available these might be used to reduce the time required to find the code. While it has been impossible to make any actual tests without models of the equipment, it is conceivable that a substantial amount of intelligence could be obtained in the order of half an hour.

The most noteworthy weakness in the British 2-dimensional system appears to be the use of a fixed repeated code. The addition of code changing means would increase the cryptographic security very greatly.

The quality of the restored (or decoded) speech presented on the recording compared favorably with the clear (or uncoded) speech on the same recording.

2. Analysis

2.1 Non-Cryptographic Methods

The first step in analyzing recording W 44/137 was to listen directly to the scrambled speech. Listening to selected frequency bands of the speech was also tried. By direct listening to repeated playings of the recording, various words and phrases were thought to have been heard with, however, very little agreement among observers. A comparison of these words and phrases with the script of the original message showed that no intelligence had been obtained in the direct listening tests. At least for the code employed on this recording the security against direct listening is very good.

2.2 Cryptographic Method

The procedure employed in determining the 2-dimensional code was substantially the same as that described in Chapter VI, Section 2 of Part I and in Preliminary Report No. 22, Part II of the Final Report on Project C-43.

Spectrograms of the coded speech on recording W 44/137 clearly revealed the time and frequency boundaries of the 2-dimensional coding. This may be seen by referring to the photographs of two spectrograms of coded speech from the recording (see Figs. 2 and 3, attached) where the boundaries are indicated by grids of pencil lines drawn on the spectrograms. The time elements are 0.065 second and the frequency boundaries appear to be at 175, 1225, 2275 and 3325 cycles/second.

The periodicity of the coding became evident upon inspecting a few spectrograms. It was noticed that in the lowest of the three frequency bands a pair of elements appeared in normal (or unscrambled) order. Such a pair occurred periodically every five time elements. From these observations, it was inferred that the coding was probably the same as that described in Radio Report No. 973, British Post Office Engineering Department, i.e., a matrix of 15 elements (three frequency elements by five time elements) followed by the converse matrix.

After the spectrograms had been photographically enlarged, by a factor of approximately 2:1, the grid on each spectrogram was subdivided into matrices. Since no synchronizing pulse appeared on the spectrograms, matrix boundaries, for reference purposes, had to be selected arbitrarily. The location of these boundaries was first chosen as the beginning of the first element of the pair of elements which appeared in their normal or unscrambled order. The elements within a matrix were then numbered from 1 to 15 as indicated on Fig. 1A. Since a number of spectrograms and matrices was involved, the numbers identifying the elements were followed by a dash and a two-digit number, the first digit identifying the spectrogram in which the elements occurred and the second number identifying the matrix on that spectrogram. These numbers are shown on all of the attached figures.

Having numbered the elements on a spectrogram, the matching boards and the backs of the photographic enlargements were given a coating of rubber cement and the enlargements were cut up along the boundaries of the elements. The proper positions of the elements were then sought by matching the boundaries and obtaining a pattern representing the normal flow of speech.

The matching process was undertaken at first without making use of the properties of converse codes. After several satisfactory matches were completed, conversing was tried and a shift in the matrix boundaries was indicated as illustrated in Fig. 1B. It will be observed from that figure that, although the area between points D and E constitute a complete cycle which is repeated on either side of these boundaries, the elements within the boundaries D and E do not constitute two homogeneous fifteen-element matrices. By shifting the matrix boundary one time element to the right and re-numbering the elements, Fig. 1C was obtained. This figure was derived directly from Fig. 1B by reducing the element numbers of the latter by three, there being three elements within a time boundary. As a result of this change in numbering all of the elements between the boundaries F and G in Fig. 1C are from one matrix and all of the elements between the boundaries G and H are from the succeeding matrix. This latter matrix is the converse of the former. The derived code is shown in Fig. 1D, without the complication of the spectrogram and ~~identifying numbers. Here the numbers in each elemental area~~ represent the settings of the dial or switch to place element No. 1 in the first position, element No. 3 in the second position and element No. 8 in the third position, etc. Using the conversing code for the second group of fifteen elements results in element No. 1' in the first position, element No. 2' in the third position and element No. 3' in the eighth position as shown. In the absence of a synchronizing pulse it is unknown whether the matrix F'G' represents the code or the converse code and similarly with the matrix G'H'. However, with working models of the equipment this should be a simple matter to determine. Spectrograms of the decoded material are shown at the bottom of Figs. 2 and 3. The numbering shown on these elements is that based upon the original arbitrary selection of matrix boundaries and corresponds to Fig. 1B, since it was not convenient to make the actual changes of numbers on the spectrogram elements.

The matching procedure was considerably slowed up by the presence of spurious traces on the spectrograms. These appear to be chargeable to (a) switching transients at the time boundaries, (b) noise and distortion products which probably were introduced during the recording of the scrambled speech, and (c) "spill over" from the narrow analyzing filter in the spectrograph causing the traces from an element of large energy to spill over into the adjacent time element.

Typical instances where the distortion products were pronounced and confusing may be noted at A in Fig. 2, and at B, C, and D in Fig. 3. These were cases where the element in question occupied position 2* in the scrambled sequence and where the element in position 1 contained strong components, the harmonics of which appeared in position 2. Although distortion products were in evidence in other elements, they were most confusing in element 2.

No equipment has been available for checking the correctness of the code determined from the above tests. Since this can be readily done by the originators of this system there seemed to be no justification for setting up equipment for restoring the scrambled speech and correcting any errors that may have been made. This would have required the construction of decoding equipment effectively duplicating the existing system.

3. Evaluation

3.1 General

In arriving at an estimate of the degree of security offered by the British 2-dimensional system several important

* This number refers to the arbitrary numbering system shown on the spectrograms. With the proper number shift, element 2 on the spectrograms becomes element 14 from the preceding matrix, as shown in Fig. 1C.

considerations should be kept in mind: (a) the appraisal given in this report is based on the study of only one sample of the coded speech; (b) the appraisal may indicate a higher degree of privacy than might be found in practice because of the quality of the recording (the recording was a copy, or dub, from another recording and, it appears likely, the clear speech used in making the tests had also been taken from a recording); (c) no models of the privacy system were available for testing the time required to obtain the intelligence by partial decoding; (d) no synchronizing pulse was in evidence - had one been present, it would have facilitated the determination of the code cycle; and (e) lack of familiarity with British diction may have made the scrambled speech less intelligible on direct listening tests.

On the other hand, the signal-to-noise ratios likely to be found in interception work may be fully as adverse to the decoding effort as any of the factors encountered in the present recording.

3.2 Security Against Non-Cryptographic Attack

Since no intelligence was gained from listening to the scrambled speech, the system (as exemplified by this recording) has a high degree of security against direct listening. Experience with this system has been based on only one code; other codes may give more or less security than this particular code.

3.3 Security Against Cryptographic Attack

The repeated code employed in the 2-dimensional system can be discovered by cryptographic methods. The solution, however, requires considerable effort and special equipment, such as a spectrograph, matching boards and, possibly, photographic enlarging facilities. The time required to determine the code may, for convenience in estimating, be divided into two parts: the first covering the time elapsing from the receipt of the scrambled signal to the moment when the spectrographic puzzles are ready for solving; and the second, the time required to solve the puzzles. The first of these periods depends on the amount of material to be prepared and how well equipped and organized the crew is for carrying out the work. To prepare puzzles from photographically enlarged spectrograms would involve an average delay of from 30 minutes to one hour depending on personnel and equipment available.

The second period will depend, to a large degree, on the freedom of the intercepted signal from noise and distortion products and also on the number of men in the crew. When the signal is received with about the same degree of noise and distortion as was present on recording W 44/137, it would appear that about six spectrograms might be required to insure good matching material over the entire 15-element matrix. For efficient use of this material, a crew of six men would be required, and, it is estimated, it would take the crew from two to three hours to obtain a working solution of the code. This assumes that the synchronizing pulse is present and that the crew has complete knowledge of the system.

It is possible that the above estimate may be of only academic interest since (a) it would be useless to determine the code if no receiving terminal were available to unscramble the message, and (b) where the receiving terminal is available it may not be necessary to go to such lengths to obtain the intelligence. In the latter instance, it is conceivable that most of the intelligence could be obtained in less time if a combination cryptographic and non-cryptographic attack were used. In working with the original spectrograms of the 2-dimensional scramble it was fairly easy to spot the elements containing energy which originally had been in the lowest frequency band. Moreover, it was not difficult to place those elements in their proper time sequence, especially where pitch changes were in evidence. Thus by setting up partial decodes on a receiving machine, a substantial amount of intelligence might be obtained. If this procedure should prove to be effective, the security afforded by this system might be reduced to something of the order of half an hour.

4. Discussion of Possible Improvements in Security

The most outstanding weakness of this system (or any privacy system, for that matter) is the use of a repeated code. The introduction of frequent code changes would, of course, very greatly increase the security against cryptographic attack.

A reduction in the length of the time elements from the present value of 65 milliseconds to, say, 35 or 40 milliseconds, would make the cryptographic solution of the code much more difficult, and it ~~probably would~~ not add too much degradation to the decoded speech in an authorized receiver.

Further complications of the system to increase the security might include the use of more and narrower frequency bands, the use of frequency inversion of some of the elements (as proposed in Radio Report No. 973) and the use of a 10 or 20 (time) element matrix rather than two 5-element ones.

A. D. FOWLER

E. C. THOMPSON

Bell Telephone Laboratories, Inc.
463 West Street
New York 14, New York

Attached:
ES-842194, Fig. 1
Photograph No. 134584, Fig. 2
" " 134585, Fig. 3

SECRET

SECRET

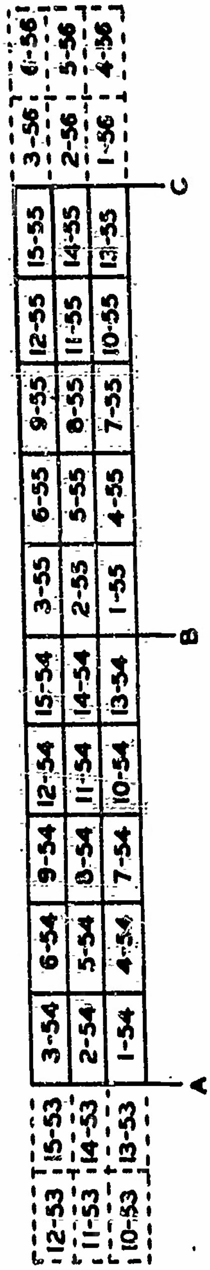


FIG. 1A

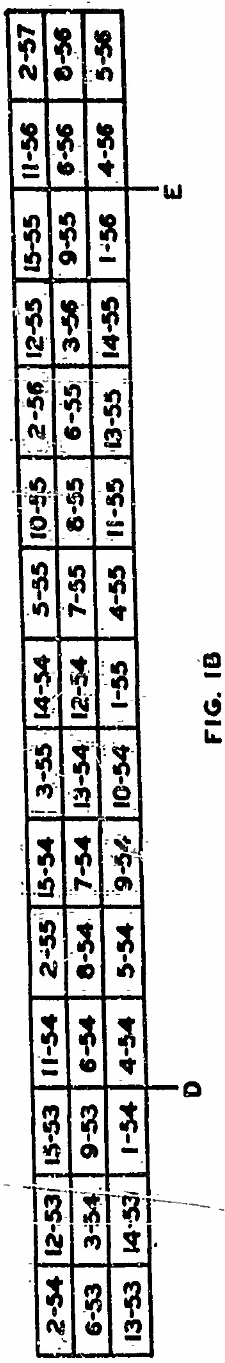


FIG. 1B

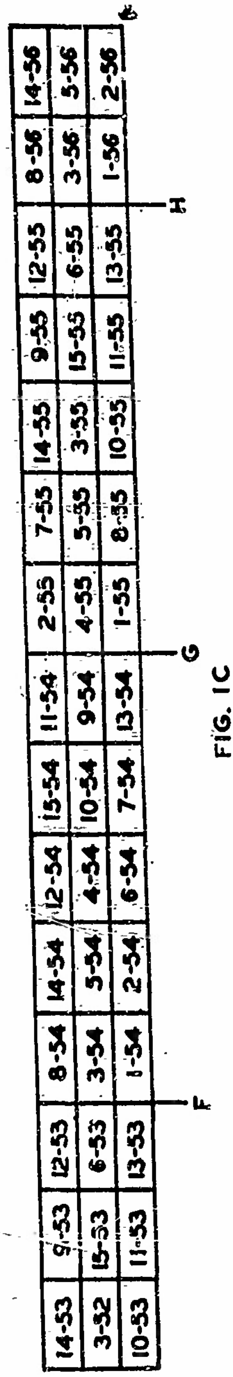


FIG. 1C

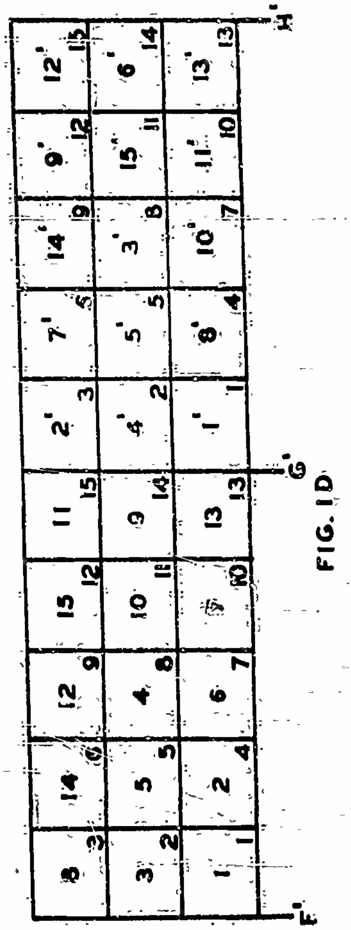


FIG. 1D

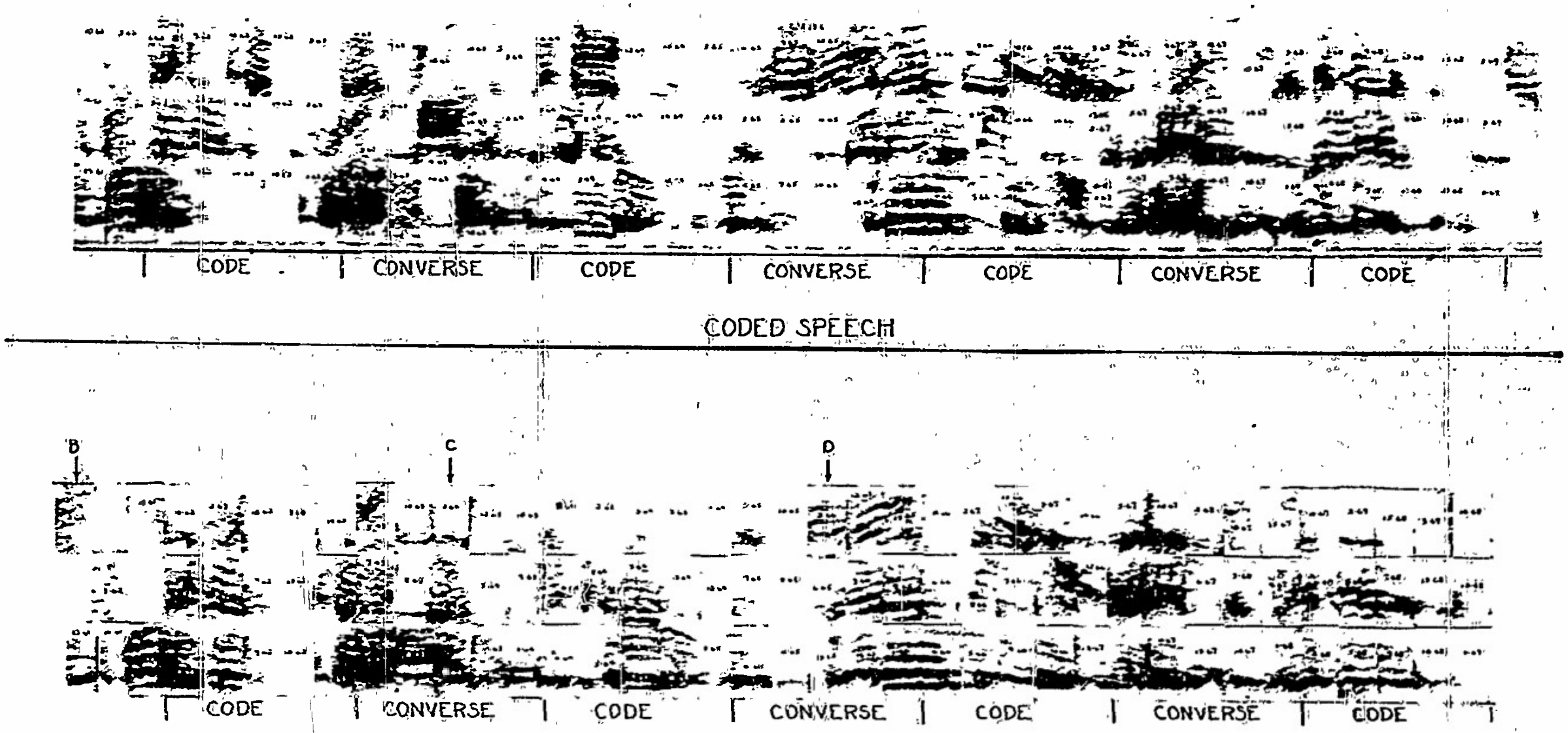
SECRET

SECRET

PRINTED IN U.S.A.

SECRET

FIG.3

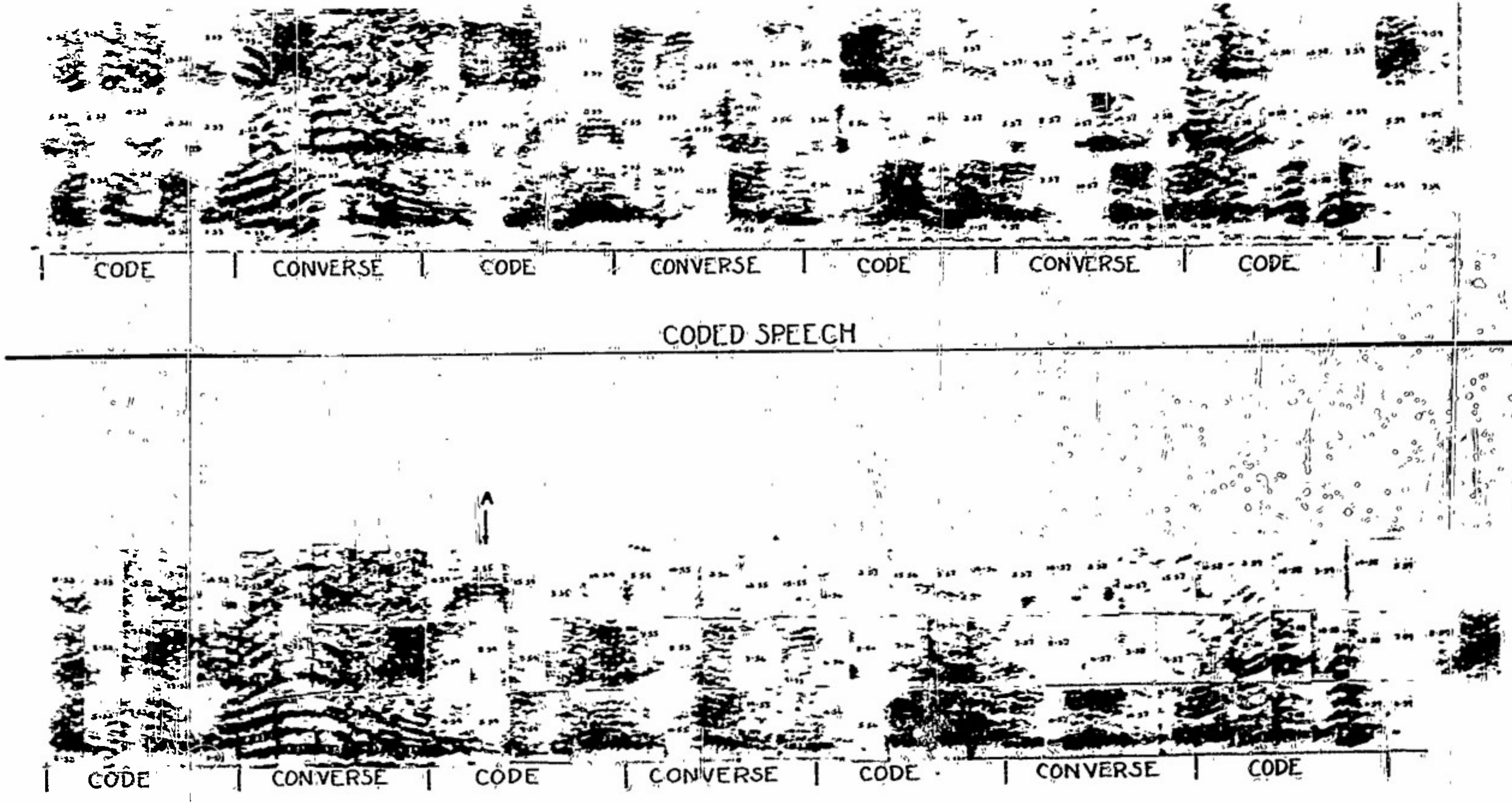


CODED SPEECH

[illegible]

SECRET

FIG. 2



CODED SPEECH

DECODED SPEECH

134584

Report No. 3

PROJECT 13-106

RELATED SERVICE PROJECT NS-349

REPORT NO. 3

Analysis of Recording of Speech Scrambled by British Modulator Type 2C, Rapidly Switched

TABLE OF CONTENTS

Page

PROJECT 13-106

RELATED SERVICE PROJECT NS-349

REPORT NO. 3

Analysis of Recording of Speech Scrambled by British Modulator Type 20, Rapidly Switched

June 20, 1945

1. General

1.1 Introduction

Models of the British modulator Type 20 system were received on December 7, 1944. It had been expected that some sort of commutator switching apparatus would be included with the equipments for rapidly switching from one code condition to another in some pre-determined, but repeated, sequence. However, no such switching mechanism was furnished. An evaluation of the security and speech quality afforded by this system on a manually switched basis has been given in Report No. 1 on this project dated January 5, 1945.

On December 22, 1944, a phonograph record, No. W44/143, of speech scrambled by the British modulator Type 20, rapidly switched, privacy system was received for analysis. Since a recording of speech scrambled by a privacy system does not provide a very satisfactory basis for evaluating the security of the system, work on analyzing the recording was deferred for some time in the hope that tests on working models could eventually be made. However, when it appeared that the commutator mechanism would not be received, an evaluation of the rapidly switched system was made, based partly on an analysis of the recording and partly on the results obtained in evaluating the New Zealand switched band privacy system*. The latter is, in many respects, very similar to the British modulator Type 20, rapidly switched. ~~Although this procedure~~ for evaluating the system is less straightforward than one based on tests with working models, the results obtained are believed to be much more accurate than would have been possible had only the recording been considered.

* See Report No. 4

The work of analyzing and evaluating this recording under Project 13-106, Contract OEMsr-1440, was authorized by letter dated January 18, 1945, from Professor C. F. Dalziel, Technical Aide of Division 13, N.D.R.C.

1.2 Summary of Conclusions

The security afforded by this system is considered very low for military purposes. This conclusion is based mainly on the results obtained from tests made on working models of the New Zealand switched band privacy system. Methods, which proved successful in cracking repeated code cycles in the New Zealand system and which should be equally effective when applied to the British modulator Type 2C system, either could not be tried with the phonograph recording or produced less successful results which, it is believed, are chargeable to the recordin

The method of isolating each commutator segment in turn and detecting by ear the correct decode condition for each segment enabled a repeated code cycle on the New Zealand system to be determined in seven minutes. There is no apparent reason why this method should not prove equally effective when applied to the British modulator Type 2C, rapidly switched.

Repeated listening to the scramble on Recording No. W44/143 directly and also through a simple two-path superposition circuit yielded only a few words and phrases and little intelligence, as contrasted with approximately 40 and 80 per cent, respectively, for the two listening methods applied to the New Zealand switched band system.

When an automatic analyzer-decoder circuit was used, approximately 60 per cent of the words and about the same percentage of intelligence were obtained upon repeated listening to the scramble on the phonograph recording. This contrasts with approximately 100 per cent of the intelligence obtained by this method when listening to the scrambled output of the working models of the New Zealand system.

The repeated code sequence cycle employed on the phonograph recording was determined cryptographically in approximately 15 minutes by careful analysis of the spectrograms of the scrambled speech.

The use of a non-repeated code cycle and an increase in the switching rate should greatly increase the cryptographic security of this system. However, it is doubtful if either of these changes would materially effect the security against any of the repeated listening methods.

The quality of the restored (decoded) speech presented on the recording compared favorably, in general, with the clear speech in the same recording. However, a few unobjectionable switching "chirps" due, presumably, to imperfect synchronization were observed.

2. Analysis

2.1 Cryptographic Method

Two spectrograms of samples of the coded speech on Recording No. W44/143 were sufficient to prove that a repeated 20-element code sequence was used and to permit a complete cryptographic solution of the code. Had the commutator mechanism been available this cryptographic solution would have made possible the direct unscrambling of the recorded speech. These spectrograms, together with wedge diagrams illustrating the energy-frequency distribution produced by the five frequency scramble conditions, are shown on the attached photograph. The time boundaries of each scrambled element are clearly revealed on the spectrograms, and by measuring the distance (average) between adjacent boundaries, the code switching rate was calculated to be approximately 65 milliseconds per element, except for the first element which is slightly longer, due, presumably, to the stop-start synchronizing action of the revolving commutator brush arm. A 3.5-kilocycle pulse also marks the beginning of each code cycle.

By carefully inspecting the intensity distribution and inflection characteristics of each scrambled element on the spectrograms, and, at the same time, bearing in mind the frequency scramble produced by each code condition, it is possible to determine the particular code condition used for each individual time element. Those few elements where the code condition is uncertain or impossible to determine, because of insufficient speech energy, may be checked by inspecting the corresponding elements in another cycle.

It is felt certain that the sequence 5 2 1 4 2 1 4 5 1 4 5 2 4 1 2 5 4 2 5 1, as indicated on the photograph, is entirely correct, although the actual sequence used in making the recording was not available for comparison. As a matter of interest, however, it may be noted that code condition 3 is not used, and that the remaining four code conditions, starting with the first element of the code cycle, appear in five successive groups with a different sequence of the four conditions in each group. Whether or not this code sequence is typical of all the possible sequences that may be set up by the coding system employed is not known.

2.2 Non-Cryptographic Methods

Practically no intelligence was obtained through repeated listenings of the recorded scramble directly, although a few scattered words and phrases were correctly understood. Repeated listenings through a two-path superposition circuit (codes 1 and 5 superposed) and also through an automatic analyzer-decoder circuit,* both similar to the circuits used successfully in cracking the New Zealand system, were also tried. The two-path circuit yielded a few more words making the total word count about 20 per cent, but the intelligence derived was still practically negligible. The automatic analyzer-decoder, however, was relatively successful in that 60 per cent of the words were obtained and roughly the same amount of intelligence. It is not known for certain why these non-cryptographic attacks were less successful in cracking this recording than they were with the New Zealand system but it is felt that the following factors may have been contributing:

1. The lack of familiarity with British diction reduced our ability to recognize partially unscrambled words or phrases.

2. The five frequency scramble conditions, though similar to those of the New Zealand system, may be different enough to have resulted in a somewhat more confusing scramble.

3. The omission of code condition 3 in the code sequence used in the recording reduced the effectiveness of the two-path superposition circuit and the automatic analyzer-decoder because inversion, which will decode condition 1 precisely, will also decode condition 3 effectively.

* See Report No. 4, Section 3.34, for a description of this circuit.

4. The signal-to-noise ratio on the recording was occasionally very poor. In several instances the level of speech, in both the coded and decoded sections of the recording, was low enough to be almost obscured by the background noise.

Since the commutator mechanism was unavailable, it was impossible to try the method of applying each of the five code conditions, one at a time, to each commutator segment in turn and detecting by ear the correct decode condition. This method proved very successful in cracking a repeated code set up by the New Zealand system. It is believed it would have been equally as effective with the British modulator Type 20 equipment or even with the phonograph recording in spite of the adverse factors given above. No attempt is made to recognize words or syllables with this method as the bursts of speech are of very short duration (65 milliseconds.) However, as the five code conditions are applied in turn to a single commutator segment, the ear easily detects which code condition produces speech sounds of correct harmonic relationship regardless of pitch, diction, or language used. Furthermore, since the 65-millisecond switching rate employed by the British modulator Type 20 system is somewhat slower than the 43-millisecond switching rate of the New Zealand system, the correct decode for each scrambled element should be detected with fewer listening samples.

3. Evaluation

3.1 Security Against Cryptographic Attack

Assuming the type of scramble is already known, the repeated code sequence cycle employed in the British modulator Type 20, rapidly switched, can be determined in 15 minutes by analyzing two spectrograms of the scramble.

3.2 Security Against Non-Cryptographic Attack

Inasmuch as the commutator mechanism was not made available, extensive tests to evaluate accurately the security of this system against non-cryptographic attacks could not be undertaken. For this reason the results of the various repeated listening tests made on the single recording, W44/143, may tend to indicate somewhat greater security than that actually afforded by this system. For example, it is quite likely that considerably more intelligence would have been obtained in these tests had the speech not trailed off from time to time into the background noise of the recording. Difficulty with the diction of the speaker was also experienced. On the other hand, there is some evidence that the differences in low frequency cutoff of the various code conditions result in a staccato effect, when rapidly switched, which may interfere with the ability of the ear to recognize partially unscrambled speech.

Experience with the New Zealand system indicates that the aural method of detecting the proper decode for each scrambled element, one at a time, should crack the 20-element repeated code cycle of the British modulator Type 2C in approximately seven minutes.

4. Discussion Of Possible Improvements In Security

By using a non-repeated, or long-cycle, code and increasing the switching rate to say 30 milliseconds per scrambled element, the cryptographic security of this system would be greatly increased without seriously impairing its overall quality. Under these conditions it would be extremely difficult to determine the code sequence by spectrographic analysis of the scramble. Only slight pitch changes would exist in an element and these would tend to be obscured by the closely spaced time boundaries. Furthermore, when the code is not repeated, each element would have to be solved independently - a laborious and time-consuming task in itself. However, it is doubtful if either of these changes would increase the system's security against any of the repeated listening attacks.

D. O. SLATER

E. C. THOMPSON

BELL TELEPHONE LABORATORIES, INC.
463 West Street
New York 14, New York

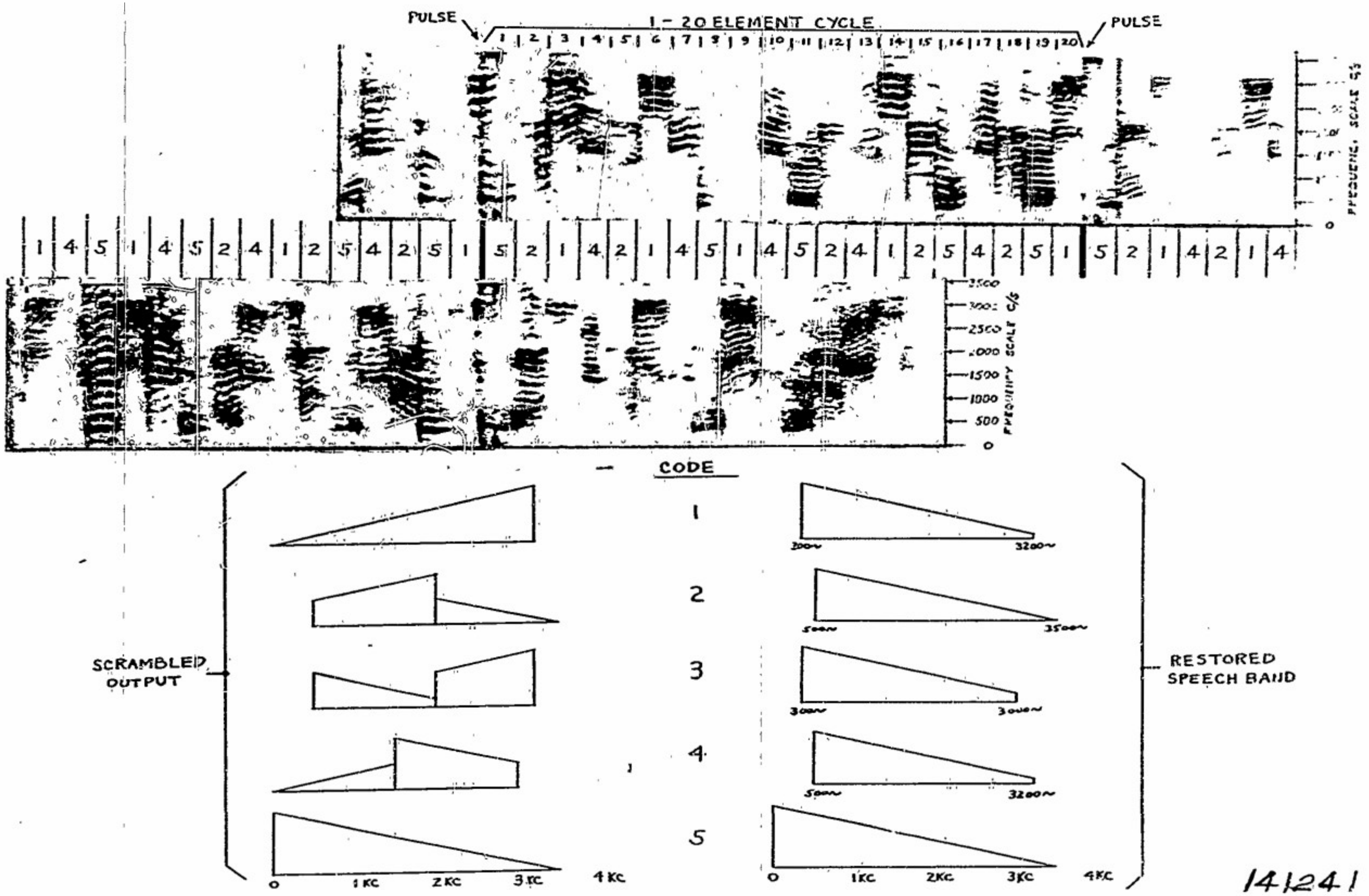
Attached:

Photograph No. 141241

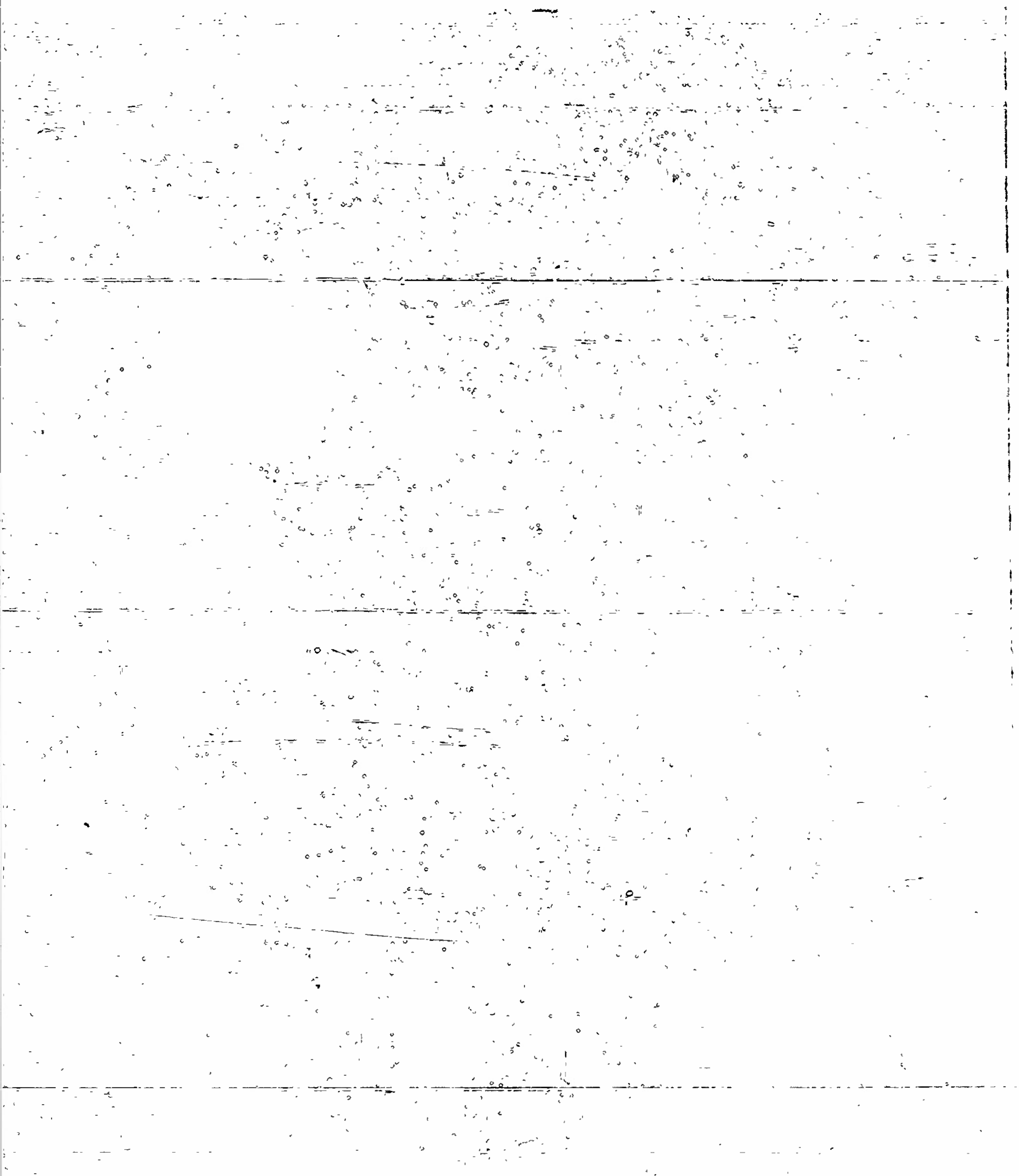
SECRET

BRITISH 2-C MODULATOR (SWITCHED)

CRYPTOGRAPHIC ANALYSIS
FOR REPEATED CODE CYCLE (REC. # W 44/143)



141241



Report No. 4

SECRET

PROJECT 13-106

RELATED SERVICE PROJECT NS-349

REPORT NO. 4

New Zealand Switched Band Privacy System Working Models and Recording

SECRET

PROJECT 13-106

RELATED SERVICE PROJECT NS-349

REPORT NO. 4

New Zealand Switched Band Privacy System Working Models and Recording

TABLE OF CONTENTS

Page

TABLE OF CONTENTS (Cont'd)

PROJECT 13-106

RELATED SERVICE PROJECT NS-349

REPORT NO. 4

New Zealand Switched Band Privacy System Working Models and Recording

July 27, 1945

1. General

1.1 Introduction

On February 13, 1945, a recording of speech scrambled by the New Zealand switched band privacy system was received from the U. S. Navy Department for analysis. This work was undertaken and brought nearly to completion when, on February 23, 1945, the scrambling equipment for two terminal units of the New Zealand system was received for purposes of tests and evaluation under this project. Since an evaluation based on tests with working models is decidedly more reliable than one based on only a recording of the scrambled speech, further work on the latter was postponed until tests on the working models were completed. This report includes the results of the tests made with both the recording and the working models.

A substantial amount of auxiliary equipment, such as power supplies, amplifiers, relay and jack circuits required to use the scrambling units in a two-way privacy system was not furnished. It was necessary, therefore, to provide and construct these items. Two complete terminal units were assembled for two-way operation without benefit of the instruction bulletins or drawings which did not arrive until the work was practically completed.

The work on both the recording and the working models of the New Zealand system was authorized by a letter from Prof. Charles F. Dalziel, Technical Aide, Division 13, N.D.R.C., dated February 16, 1945.

1.2 Summary

The security afforded by this system is very low for military purposes and is inconsistent with its weight, size, and type of design which limits it to permanent installations.

One terminal unit occupies approximately six feet of standard rack space and, with the necessary auxiliary equipment, weighs nearly 300 pounds. The system was designed for use with conventional radio terminals on a permanent installation basis. However, by redesign considerable reduction in size and weight could be achieved.

The frequency bandwidth for satisfactory transmission must accommodate a 50-cycle speed control tone and a 4,000-cycle synchronizing pulse as well as the 200 to 3000-cycle speech band.

Mechanically and electrically the system operates satisfactorily although daily adjustments are usually required. The intelligibility of the restored speech is good but the quality is somewhat inferior to what might be achieved with further improvements in design.

In this system three frequency bands of approximately 1000 cycles each are arranged to provide five code conditions. By means of an 18-segment commutator these five code conditions are switched at intervals of .043 second in a coded sequence. When the same coded sequence, lasting 0.77 second, is set up on each revolution of the commutator brush, the equipment produces a repeated code. An applique unit is furnished with the equipment to extend the time when the code will be repeated. This unit changes the coded sequence each revolution of the commutator brush for 625 revolutions to give a code cycle of eight minutes, referred to in this report as a non-repeated code.

Under favorable conditions for interception, the low security of this system is revealed by various non-cryptographic attacks which gave the following results:

1. An automatic analyzer-decoder circuit will yield at least 50 per cent of the intelligence on the first listening and practically all of the intelligence with a few additional listenings for either repeated or non-repeated codes.

2. With a terminal equipment, or its equivalent, aveilable, repeated codes can be cracked in about seven minutes by detecting aurally the proper decode for each scrambled element.

3. Twenty repeated listenings* to the scramble through a two-path superposition circuit will yield about 80 per cent of the words.

4. Twenty repeated listenings* to the scramble directly will yield about 40 per cent of the words.

Because of the vulnerability of this system to non-cryptographic attack, work on cryptographic decoding methods was directed mainly towards making a fundamental analysis of the coding system to determine its characteristics and weaknesses. However, estimates were made of the security against cryptographic attacks on the assumption that spectrograms would be used for this purpose. Other methods not employing spectrograms might prove to be more rapid but no attempt was made to develop them.

For a repeated code sequence, a correct permutation of the code cords and the settings of the sequence switches can be determined cryptographically by the use of spectrograms in about 20 minutes. In some instances, partial solutions obtained in ten minutes may prove satisfactory. For a non-repeated code sequence, the permutation of the cords, settings of the code sequence switches, and the starting point of the automatic code changer can be cryptographically determined by a trained crew with adequate equipment in approximately one hour.

By redesigning the system to use pre-equalization ahead of the scrambler unit, the effectiveness of the automatic analyzer-decoder circuit can be practically destroyed. Pre-equalization will approximately double the decoding time for all other decoding methods except that for the cryptographic determination of non-repeated codes. In the latter instance the time is increased approximately 50 per cent.

- -

* On an average, 20 minutes of repeated listening were required to extract, from a one minute sample, the percentage of words indicated and additional listenings usually did not increase the percentage materially. These results apply to both the repeated and non-repeated code sequences.

2. Equipment and Operation

2.1 Introduction

The first model of the New Zealand switched band privacy system was developed by the Radio Development Laboratory, Department of Scientific and Industrial Research, Wellington, New Zealand. Its major features were based substantially on the design given in the British Post Office Radio Report No. 994. The present equipment was built by Collier & Beale, Limited, Wellington, New Zealand, and incorporates the basic features of the prototype with the exception of a few minor changes introduced to avoid operational deficiencies and to facilitate the use of the apparatus in a radiotelephone terminal equipment of conventional design. The three units comprising the privacy equipment are not self-functioning. Local power supply sources, amplifiers, to provide the desired volume levels, and equipment to segregate the voice and synchronizing signals are required.

2.2 Physical Description

The weight and size of each of three units comprising one terminal of the scrambling equipment received from New Zealand are given in the table below.

Physical Dimensions

Units	Weight - (Pounds)	Height - (Inches)	Width - (Inches)	Depth - (Inches)
Synchronizing Control	24	8-3/4	19	11-3/4
50-Cycle Power	57	14	19	11-3/4
Scrambler, Including Auto-Coding Unit	136	21	19	22-3/4
Total	217	43-3/4		

The two sets of equipment received were mounted on separate relay racks located in different laboratory rooms so that two identical but independent terminals were available for testing and demonstration purposes. Other necessary auxiliary apparatus which was constructed or provided from laboratory stock was also mounted on each rack. The attached photographs, Figures 1 through 4, show various views of one complete terminal.

2.3 Theory of Operation

2.31 General Description

Five audio frequency code conditions with a means of rapidly changing from one of these conditions to another in a predetermined or coded sequence forms the basis of this privacy system. A synchronizing mechanism is also provided to insure simultaneous operation and optimum quality between two working terminals.

A simplified schematic of the overall system as set up for laboratory testing, including the necessary auxiliary equipment, is shown on Drawing ES-842195. The two terminals are identical, but for purposes of explanation one terminal is shown in the SEND condition and the other in the RECEIVE condition. Speech entering ~~the transmitter (TRANS.)~~ is amplified (AMP #1) to the proper volume level and fed to the second innermost ring of the commutator in the SCRAMBLER UNIT where it is picked up by a revolving brush arm and distributed successively to the 18 commutator segments of the outermost ring. Each of these segments is connected to one of the five code conditions, depending on the permutation of the code cords, setting of the code sequence switches, and position of the selector switches. Likewise, each segment of the inner commutator ring is connected to the output of one of the five code conditions through a duplicate set of contacts. With this arrangement, the incoming speech is distributed in a coded sequence to the inputs of the five code conditions, and is simultaneously picked up, in the same sequence, as scrambled elements of speech on the inner commutator ring and finally fed to AMP #2 through a duplicate set of brush contacts. After amplification, the scramble passes through a 3-kc low-pass filter and 111-C balancing coil where it combines with a continuous 50-cycle wave and a 4-kc pulse which synchronize the SEND and RECEIVE terminals. The combined output passes through the LINE OUT transformer and is transmitted either by radio or wire line to the RECEIVE terminal.

Unscrambling at the RECEIVE terminal follows essentially the reverse process. After passing through the LINE IN transformer, the 50-cycle wave, 4-kc pulse, and scrambled speech are channeled by filters to their proper circuits. The scrambled speech is amplified (AMP #1) and fed to the commutator of the SCRAMBLER UNIT. In order for the scrambled speech elements to be properly restored, the permutation of the code cords and setting of the code sequence switches must be correct. In addition, the selector switches and revolving brush arms of the SEND and RECEIVE terminals must be in identical positions. Under these proper decode conditions, the incoming scrambled speech elements when distributed to the inner ring of segments, will be simultaneously picked up as restored speech on the outermost ring of segments. The speech is then amplified (AMP #2) and fed to the receiver (REC).

Interchanging the SEND or RECEIVE condition of a terminal is performed by relay transfer contacts under control of a push-to-talk button. This method was also used in the prototype equipment. However, when the system was used in conjunction with radiotelephone terminal equipment, as intended, voice operated relays replaced the manually operated push-to-talk button.

2.32 Code Conditions

In the lower left-hand portion of Drawing ES-842195 is shown the circuit used to derive the five code conditions, together with the five wedge diagrams illustrating the frequency translations of the resultant scrambles. Briefly, the five conditions are as follows:

Condition A -	Inversion of 0 to 3000-cycle band.
Condition B -	Inversion of 0 to 3000-cycle band followed by re-inversion of 0 to 2000-cycle portion.
Condition C -	Inversion of 0 to 2000-cycle portion followed by complete inversion of 0 to 3000-cycle band.
Condition D -	Inversion of 0 to 2000-cycle portion only.
Condition E -	Straight transmission (attenuation only).

Each condition has a nominal insertion loss of 37 db and an input and output impedance of 500 ohms. The IN and OUT leads of each condition terminate in double prong plugs so that these cords may be patched conveniently to the jacks of the selector switch box (auto-coding unit), or coding bus jacks associated with the code sequence switches.

2.33 Code Sequence Switches

Six code sequence switches are provided, and each switch has six banks of contacts. These switches are wired to the commutator segments, both inner and outer rings, in such a way that the order and, to some extent, the choice of the five code conditions available to the first group of three successive commutator segments is determined by the position of switch No.1, the second group of three successive segments by the position of switch No. 2, and so on for all 18 segments. As a result, the order in which the five conditions follow one another is coded according to the positions of the six switches. The wiring of the switches also insures against the repetition of any code condition within each group of three segments. Each switch has 11 positions labelled S, 0, 1, 2, 3, 4, 5, 6, 7, 8, and 9. The 0 through 9 positions provide ten different sequences of the five conditions, and the S position opens the circuit to the segments. The six switches, having ten useful positions each, provide 10^6 possible combinations or code sequences, all different.

Further coding is possible in that the five cords from the frequency scrambler unit may be permuted in 120 different combinations to the coding bus jacks of the code sequence switches. However, the total number of different sequence orders obtainable by permutation of the cords and resetting of the code sequence switches is 12 x 10^6 rather than 120 x 10^6, as will be explained later. Thus, for a fixed cord permutation and fixed setting of the switches, a definite coding sequence of the five conditions is set up on the 18 commutator segments and will be repeated each revolution of the brush arm.

2.34 Auto-Coding Selector Switches

By using automatically stepping selector switches, which change the permutation of the five code conditions once each revolution of the brush arm, the above-mentioned repeated code becomes a so-called non-repeated code. The selectors are inserted between the frequency scramble circuit and the coding bus jacks, thus a complete code cycle now depends on the length of the selector cycle. Four, 25-step, 6-bank selectors are used in the New Zealand equipment. Two of the selectors in series permute the inputs of the five code conditions and the other two make the same permutation of the outputs. Since the pairs of selectors operate in series, a total of 25 x 25 or 625 permutations occur before the selector cycle repeats. The brush arm normally rotates at 78 rpm (43 milliseconds per segment). Therefore, with a new permutation occurring each revolution, the time required to complete one major coding cycle is approximately eight minutes.

2.35 Synchronism

To insure proper unscrambling of the incoming elements of scrambled speech, it is apparent that the revolving brush arms of the SEND and RECEIVE terminals should rotate at equal speeds and should maintain the proper phase relationship at all times. In this privacy system a continuous 50-cycle wave, transmitted along with the scrambled speech, is used to synchronize the speeds of the two revolving brush arms, and a short 4-kc pulse is transmitted each revolution to insure the proper phase relationship. These synchronizing signals may originate and remain under the control of either one of the terminals, regardless of whether it is in the SEND or RECEIVE condition. Drawing ES-842195 shows the synchronizing signals originating at the SEND terminal.

To maintain speed control, each terminal is provided with a fairly stable 50-cycle oscillator located in the Synchronizing Control Panel. The output of the oscillator excites the grids of a power amplifier (PWR AMP) which in turn delivers approximately 30 watts of 50-cycle power to a synchronous, 1500 rpm, fractional H.P. motor. The motor drives the brush arm through a worm gear reduction and a friction clutch. At the terminal originating the synchronizing signals, a small portion of the 50-cycle power is tapped off and transmitted to the distant terminal where it is used to synchronize the 50-cycle oscillator. Synchronization is indicated by the Synchroscope meter.

The 4-kc synchronizing pulse is utilized to operate the START-STOP LATCH RELAY at each terminal so that the brush arms will start each revolution simultaneously at identical positions on their respective commutators. Each terminal is provided with a 4-kc oscillator which is used only at the terminal where the pulses originate. Referring to the SEND terminal of Drawing ES-842195, it will be seen that the output of the 4-kc oscillator is fed to a cam operated relay. With each revolution of the cam the relay contacts close momentarily, allowing a portion of the resulting short 4-kc pulse to be transmitted to the distant terminal along with the 50-cycle wave, and the remaining portion of the pulse to be fed to the grid of a self-extinguishing gas tube circuit. The 4-kc pulse fires the gas tube causing the latch of the START-STOP LATCH RELAY to pull up and release the brush arm. At the distant terminal the arrival of the 4-kc pulse performs the same function. This process is repeated for each revolution of the cam, and since the cam is geared to revolve at a slightly slower rate than the brush friction drive (gear ratio 74:75), the brush arm will always rest against the latch for approximately 0.010 second each revolution before it is released. Thus slight discrepancies in the motor speeds, if they exist, are compensated for at the end of each revolution.

A second relay, in series with the START-STOP LATCH RELAY, also operates each time the gas tube fires, and its contacts close the 24-volt supply to the selector switches causing them to step once each time the relay operates.

2.4 Appraisal of Equipment Design and Operation

2.41 Intent of Comments

The original designers of this equipment are well aware of many of its weaknesses and freely admit them in their instruction bulletin. Some of the weaknesses are inherent in this type of privacy system, others undoubtedly arise through unavailability of more desirable parts and materials. Therefore, in judging the design and operation of this equipment we wish to make clear that many of our comments are made with the view of substantiating the opinions of the original designers. In no case is it intended to belittle the engineering design, workmanship, or effort put forth in the building and advancing of this system.

2.42 Construction

Although the prototype model was intended for field use, it is apparent that the present equipment was designed for permanent terminal type installations and is not rugged enough for field use. As received, some of the heavy components, such as a power transformer and two choke coils, had torn loose from their mountings.

2.43 Commutator

During the period in which this equipment was operated for test and demonstration purposes, the chief source of interruption was due to the short circuiting or bridging of adjacent commutator segments by the accumulation of metal particles from the commutator and brush faces and also dirt particles from the air. A thorough cleaning of the commutator at the beginning of each day usually avoided this trouble unless the equipment was operated steadily for more than four hours.

Tests and experience with the Model PF (TDS) equipment indicated that the use of palladium copper brush tips with palladium copper commutators backed on brass practically eliminated the bridging of adjacent segments due to metal particles. Furthermore, a thin film of oil on the face of the commutator reduced the contact resistance between segment and brush as well as reducing brush wear. It was also found that segment bridging due to dust and dirt particles from the air was greatly reduced by fitting tight metal covers over the commutator mechanism.

Alternative methods for rapid code switching, such as relay commutation switching and electronic switching, are possible, of course. The latter, though it may require many vacuum tubes, eliminates all moving parts.

2.44 Start-Stop Latch Relay

In the early stages of testing this equipment it was noticed that the START-STOP LATCH RELAY did not always operate firmly. This caused variations in the starting phase relationship of the brush arms which impaired the overall quality of the restored speech. It was also observed that the selector switches occasionally missed a step. Such failures necessitated the realignment of the auto-coding units so that the scrambled speech would again be properly restored.

Several mechanical adjustments of the START-STOP LATCH RELAY were made in an effort to improve its operation, but with little success. Finally it was discovered that the firmness with which the latch relay operated was determined, to a considerable extent, by the amplitude of the 4-kc pulse. Oscilloscopic observations ~~of the voltage wave shape between the plate~~ of the 884 gas tube and ground showed that the tube did not remain fired throughout the duration of the 4-kc pulse. Instead, the tube fired on the positive portion of the first cycle of the 4-kc pulse applied to its grid and then extinguished on the negative portion. The tube continued to do this on each positive and negative portion of the succeeding cycles. As a result of this oscillatory firing of the tube, the effective current through the relay circuit was not sufficient to permit its firm operation, especially when the amplitude of the 4-kc pulse was low. This phenomenon was due to the fact that the inductance of the relays presented a high impedance to the sudden surge of current when the tube fired. As a result, the potential on the plate of the tube dropped so low that the tube extinguished as soon as the grid went negative. By connecting a 0.25-mf condenser in series with 1500 ohms from the plate of the 884 gas tube to the 220-volt supply, the impedance of the plate circuit was greatly reduced during the sudden surge of current. Having fired on the positive portion of the first cycle, the tube now remained steadily fired until the cathode potential rose sufficiently to extinguish it. The resultant increase in effective current through the relay circuit insured consistently firm relay operation. However, this increase in current flow charged the cathode condenser at a faster rate, thereby extinguishing the tube sooner. As a result, the relay which controls the application of the 24-volt battery supply to the selector switches did not remain operated long enough for the selector magnets to pull up properly. By doubling the capacitance in the cathode circuit of the gas tube, the operate period of this relay was increased sufficiently. However, to maintain the same discharge time constant of the cathode circuit, it was also necessary to halve the value of the bias resistors. The net result of the above circuit changes was the assurance of firm latch operation and consistent stepping of the selector switches for each revolution of the brush arm.

To obtain the proper initial phase relationship of the revolving brush arms at the local and distant terminals, it should be possible to adjust accurately the circumferential position of the START-STOP LATCH RELAY. This adjustment is rather cumbersome to make with the present equipment, especially when in operation. However, by redesigning the relay mounting, it should be possible to make accurate circumferential shifts in either direction by a simple screwdriver adjustment. Furthermore, a scale on the periphery of the commutator would be of considerable aid in making this alignment.

2.45 Transmission Irregularities

Frequency characteristic curves for each code condition, obtained by measuring the insertion loss between the input at the SEND terminal and output at the RECEIVE terminal in 50-cycle steps from 200 to 3000 cycles, indicated the existence of many irregularities. Several of these, such as the trough caused by band splitting in Condition D, were known to have been unavoidable. Others, perhaps, could have been reduced by using isolating pads of greater loss. However, it was noted in Condition D that the average insertion loss for the frequencies between 200 and 1800 cycles was approximately 8 db less than the average for the upper band of frequencies between 2000 and 2900 cycles. This discrepancy was easily corrected by reducing the loss of the pad (4 db per terminal) in the upper frequency by-pass circuit of Condition D. This correction likewise improved the frequency response characteristic of Conditions B and C, and resulted in a small but noticeable improvement in speech quality.

2.46 Synchronizing Circuits

The purpose of the 50-cycle wave, as previously explained, is to synchronize the motor speeds at the two terminals. To prevent the transmitted 50-cycle wave from entering the scrambler circuit, where it would be modulated to higher frequencies and thereby produce annoying clicks and tones, a 100-cycle low-pass filter is normally inserted in the scrambler circuit in tandem with the 3-kc low-pass filter. However, for laboratory testing and demonstration purposes, no 100-cycle low-pass filter was used because the 50-cycle oscillators were found to be stable enough, once adjusted, to provide satisfactory speed control over limited periods (3 or 4 hours) without continuously transmitting the 50-cycle wave. Only occasional frequency checks were necessary, and usually an initial warm-up period of about 30 minutes with power on was sufficient for the oscillators to reach a constant frequency. The stability required for long period independent speed control was undoubtedly not intended when the oscillators were originally designed, and, as such, they probably would not prove satisfactory. However, independent speed control is a desirable feature for this type of system, and several methods of providing it are known.

2.47 Transmission Delay

It was mentioned earlier in this report that the synchronizing signals could originate at either one of the terminals, regardless of whether a terminal is in the SEND or RECEIVE condition, and still provide proper synchronization. This is always true for the 50-cycle wave, but true for the 4-kc pulse only when the transmission delay of the interconnecting link is negligible. If, however, the 4-kc pulses are originating at the RECEIVE terminal, a circuit delay exceeding 5 milliseconds will generally cause sufficient asynchronism of the revolving brush arms to result in a noticeable impairment in the quality of the restored speech, unless the delay is compensated for. The amount of delay which may be tolerated without compensation is, of course, directly related to the code switching rate.

Perhaps the simplest method of compensating for this delay is to have the 4-kc pulse always originate at the terminal that is in the SEND condition. In this way, the 4-kc pulse and the scrambled speech will always be transmitted together, and will encounter essentially the same circuit delay.

2.48 Reduction of Transmission Bandwidth

Elimination of the continuously transmitted 50-cycle synchronizing wave would considerably lessen the rather severe low-frequency transmission requirements its use now imposes. In addition, by employing appropriate and more selective filters, it is quite possible that the frequency of the present 4000-cycle synchronizing pulse could be reduced to say, 3100 cycles, or located within the normal speech band. Thus the bandwidth required for operation of the system could be reduced.

2.5 Appraisal of Restored Speech

The relatively low military security afforded by this system, as indicated by preliminary tests, did not seem to justify the extensive testing required to obtain an accurate transmission rating. However, in the course of other tests and demonstrations, it was observed that the intelligibility of restored speech was good in that seldom was it necessary to repeat words or phrases, and for most listeners it did not require particularly close attention to follow ordinary conversation. As a rule, individual voices were easily recognized, although some sounded less natural than others.

The inherent signal-to-noise ratio of the overall system was better than 40 db.

The most noticeable quality impairment was a slight wavering of the voice, caused by the rapid switching of the five code conditions which have differences in frequency characteristic and insertion loss. These differences could be detected by listening to each code condition separately, although the quality through each was quite satisfactory. While some of these differences are unavoidable, others could be corrected by improved impedance matching and pad design, thereby reducing the wavering effect considerably.

A second, though less noticeable impairment, is the rapid switching clicks which are heard only when speech is present.

The clicks are of short duration and occur each time the brushes slide from one commutator segment to the next. It is impossible to eliminate them entirely as they are a result of filter transients and inherent imperfections in mechanical commutation. They are not, however, particularly loud or annoying.

All the above observations were made under ideal laboratory conditions, and the impairments noted, though not serious, are attributable entirely to the privacy equipment. When the system is used in conjunction with radio transmission it is quite possible that selective fading may produce more serious degradations.

2.6 Field Unit Design Considerations

The usefulness, from a military standpoint, of a small practical field unit incorporating the basic features of this privacy system would depend almost entirely upon its security against unauthorized listeners. From an equipment standpoint, there are a few rather large items in both the present equipment and the prototype model which could be reduced in size and others which could be completely eliminated. Since a 24-volt d-c power supply must be available for operation of the selector switches, it would seem logical to use that source of power also to operate a dynamotor which would drive the brush arm and generate the plate voltage for the audio amplifiers, oscillators, and latch relays. The use of a precision regulating circuit to control the dynamotor speed would obviate the transmission of the 50-cycle wave, and would eliminate the need for a 50-cycle power panel and most of the Synchronizing Control Panel. In addition, a redesign of the commutator mechanism and gear housing would permit further reduction of the weight and size. On the basis of these and other design changes, it is estimated that a complete terminal, including the auto-coding unit, could be mounted in a chassis about the size of the present scrambler unit and weigh in the order of 100 pounds.

3. Analysis of Security

3.1 Discussion of Code Conditions

In order to discuss the various decoding techniques investigated it is advisable to familiarize the reader with the five code conditions which this system makes available for coding purposes. Two fundamental modulation processes are involved: The first, designated "Code A", provides inversion of the full

0 to 3000-cycle band, and the second, designated "Code D", provides inversion of the 0 to 2000-cycle portion with the band from 2000 to 3000 cycles transmitted in its proper position by means of a by-pass circuit. Used in tandem, the first modulation process (Code A) followed by the second (Code D) provides a third condition which is designated "Code B". Likewise, the reverse tandem order provides a fourth condition, "Code C". A path involving only an attenuation pad provides clear speech for the fifth condition which is designated "Code E".

The resultant five codes are illustrated by means of wedge diagrams on attached Drawing ES-842252. Reference to the column headed "Normal Speech" shows the wedge diagram used to indicate uncoded or straight speech. The center column indicates the frequency translations incurred when straight speech is scrambled by each of the code conditions. Subsequent references to the various code conditions will be made in accordance with the designations and conventions set forth on this drawing.

The unscrambling of code conditions involving only a single modulation process (Code A or Code D) is accomplished by the same modulation process at the receiving terminal. The codes involving a tandem use of the modulating processes are properly restored by using the modulation processes in the reverse order. However, it should be pointed out that the reverse order required to restore Codes B and C automatically occurs at the receiving terminal since the incoming scrambled speech passes through the scrambler unit in the reverse direction. Thus Code B, for example, as set up at the transmitting terminal, is properly restored by setting up Code B at the receiving terminal.

3.2 Test Conditions

The two terminals available for test and demonstration purposes were located in different laboratory rooms and were directly connected for convenience on a 4-wire basis. All recordings of the scramble were made on a magnetic tape device, having a high input impedance, which was bridged across the output of the terminal under test. With the exception of a few special tests, the settings of the code sequence switches and permutations of the code cords were chosen at random. This usually resulted in a fairly uniform distribution and occurrence of the five code conditions. In all tests the speech material used was unfamiliar and usually in the form of continuously related thoughts, such as excerpts from magazine and newspaper articles. In some instances, short, terse, command sentences, in which every word is important, were used. The talking rates varied from normal to fairly rapid and several voices were employed.

3.3 Non-Cryptographic Decoding Methods

3.31 Direct Listening

Preliminary tests indicated that only an occasional word or phrase could be understood by listening once to a sample of the scramble. However, it was found that by listening repeatedly to the same sample, considerably more intelligence could be obtained. When the code conditions are rapidly switched the success of this repeated listening method depends, to a considerable extent, upon the amount of intelligence which can be derived from each of the code conditions comprising the coding sequence. The approximate percentage of intelligence (word count) which could be obtained by repeated listening to the individual code conditions was found to be as follows: Code A, 0 per cent; Code B, 10 per cent; Code C, 20 per cent; Code D, 70 per cent, and Code E, 100 per cent. The effect of having partially or completely intelligible elements distributed throughout a cycle provides a sampling of the original speech interspersed with unintelligible material. In addition, since the time relationships of the original speech sounds have not been altered, the cadence of the sounds assists in their recognition.

Tests were performed to determine the vulnerability of this system to direct listening attack by recording one minute samples, using representative coding sequences, both repeated and non-repeated, and then attempting to recognize as many of the words and phrases as possible by repeated listenings to these samples. In these tests, a 3000-cycle low-pass filter was employed in the listening circuit to eliminate the somewhat disturbing effect of the 4000-cycle synchronizing pulse.

Based on listening to samples of speech 20 times (additional repetitions contributed very little), it was concluded that, over a wide range of talking rates, from 30 per cent to 50 per cent of the words could be correctly understood regardless of whether a repeated or non-repeated coding sequence was employed. This degree of word recognition usually revealed the gist of the original speech material. It was also observed that the use of pre-equalization* did not in general appreciably reduce the amount of intelligence that could be extracted, although the number of repeated listenings required was about doubled.

- -

*The pre-equalizing network used in these tests produced a sloping loss characteristic decreasing at the rate of 6 db per octave from 400 cps to 3000 cps.

3.32 Superposition Listening

Next in the family of non-cryptographic cracking methods is that of repeated listening through a superposition circuit. In this method the scrambled speech is transmitted to a multiple-path listening circuit which may include the decodes of two or more of the code conditions employed. With this arrangement, the particular code condition of the scramble appearing at any instant is fed to the various decoding paths of the superposition circuit, and the outputs of these paths are then combined at the receiver. Thus the interceptor will hear, in the case of a circuit involving the superposition of all five decodes, a properly decoded element plus reinforcement or heckle from each of the remaining four incorrect conditions, depending upon how they treat the element in use at that instant. The effect of transmitting, in turn, each of the code conditions through each of the remaining decodes is illustrated on attached Drawing ES- 842435. This scheme is often useful in anticipating the results of various decoding combinations. However, the restoration of each element by complete superposition of all five decode conditions proved unsatisfactory because of the disproportionate amount of interfering heckle present.

As a result of tests involving various combinations of superposed decodes, it was found that a maximum of intelligence could be extracted from the scramble when emphasis was placed on restoring some of the elements as completely and free from unwanted products as possible, while permitting the remaining interspersed elements to remain scrambled. In effect, this method results in a sampling process in which the sampled elements are properly restored and relatively free from interference, whereas in the complete superposition method all the elements are properly restored but heavily masked by unintelligible interference from the other four channels.

The optimum arrangement, as disclosed by these tests, was the use of two superposed paths: One, the decode of Condition A (3000-cycle inversion), and the other, the decode of Condition E (straight transmission), with the straight path arranged so that either the full frequency band or the 0 to 1000-cycle portion could be transmitted. The lower portion of Drawing ES-842252 illustrates this arrangement schematically. The equipment involved includes two 3000-cycle low-pass filters, a double balanced copper oxide modulator unit, a 1000-cycle low-pass filter, an oscillator, and suitable mixing pads. In addition, a variable attenuator is provided in the straight transmission branch to enable the operator to adjust the relative volume levels of the two branches. This adjustment is determined b" the operator for optimum performance. The flexibility of this circuit may be enhanced by providing a switch to permit the use of either path alone.

The extent to which this circuit decodes each of the five scramble conditions is illustrated by the wedge diagram in the third column on Drawing ES-842252. Diagrams designated "Decode A" illustrate the results of passing the scramble of each condition through the inverter path, while those designated "Decode E" show the outputs of the straight transmission branch; the two are combined, of course, at the output of the final mixing pad. These diagrams also indicate the relative amounts of unwanted heckle, as well as showing how the 1000-cycle low-pass filter in the Decode E path materially assists, in certain cases, in the suppression of the unwanted products in that branch.

The choice of this particular superposition circuit proved more satisfactory than any other combination because the 0 to 1000-cycle portion of the true voice spectrum, which usually contains most of the speech energy, is properly restored in three (A, B, and E) out of the five code conditions, with a minimum of interference. Furthermore, any contributions made by the two remaining code conditions (C and D) are retained.

The general procedure in using this method is to record the scramble, preferably on a repeating magnetic tape device, and then play the recording through the superposition circuit until it is felt that all of the intelligence possible has been extracted. All possible conditions of the two-path circuit should be tried since the use of conditions, other than that found to give the optimum results, will generally make xome contribution to the total intelligence.

Extensive repeated listening tests, through the two-path superposition circuit, to scrambles employing either repeated or non-repeated coding sequences indicated that 65 per cent to 85 per cent of the intelligence, based on a word count, could be obtained from a one-minute sample in approximately 20 minutes. To determine the effect which circuit noise might have on these listening tests, thermal noise, confined to a 0 to 3-kc band, was mixed with the scramble. The same results could still be obtained with signal-to-noise ratios as low as 15 db. However, with ratios lower than 10 db, practically no intelligence could be extracted. In all of these tests the optimum arrangement of the two-path circuit utilized both the inverted and straight paths, with the bandwidth of the straight path restricted to 0 to 1000 cycles and somewhat reduced in level relative to the inverter path. As previously indicated, some contribution to the total intelligence obtained was made, in each case, by trying the other conditions of the circuit. However, occasionally a word or phrase could not be recognized regardless of the amount of repeated listening.

It is possible, though unlikely, that a repeated coding sequence might contain a predominance of Conditions C and D. Since the superposition circuit will not restore either of these codes, it would seem, with such an adverse code distribution, that this circuit would be of little assistance in extracting intelligence. However, tests, employing a repeated coding sequence in which Codes C and D constitute 67 per cent of the cycle (maximum possible) indicated that approximately 75 per cent of the intelligence could still be obtained. In this case, the best arrangement was the use of both the inverter and straight path (full band) and with both adjusted to the same volume level. On the other hand, where a predominance of Codes A and B existed, the use of inversion alone often permitted 100 per cent intelligibility.

A final series of tests with pre-equalization at the transmitting terminal were made, and the results obtained were essentially the same as when no pre-equalization was used although a longer listening period was required. Most of the intelligence was extracted using the inverter path only. It was found undesirable to insert complementary equalization at the output of the listening circuit.

3.33 Aural Determination of Repeated Code Sequence

While direct and superposition listening methods enable the partial extraction of intelligence from a scramble composed of frequency translations, these methods are not entirely satisfactory and are rather time consuming. When a terminal of this privacy system, or its equivalent, is available, a better approach is to determine the sequence of scramble conditions, then utilize this information to set up the proper decoding sequence so that the entire message may be restored. Determination of the coding sequence used can be made either cryptographically or non-cryptographically. The latter method will be discussed in this section.

In this method the terminal available to the interceptor must be operating in synchronism with the terminal whose repeated coding sequence is to be determined. By applying each of the five decode conditions one at a time to each commutator segment, in turn, the correct decode for each segment can be determined aurally. No attempt is made to recognize syllables as the bursts of speech are only 43 milliseconds in duration. When the various decode conditions are tried, it is possible to determine the condition which causes speech sounds to have the proper harmonic relationships, regardless of pitch, diction or language used. Since each revolution of the brush arm provides a different sample of speech sound, the correct decode is confirmed by successive samples.

Two schemes may be used in the application of this method. The first makes use of an applique circuit comprising 18 switches, one for each commutator segment, and suitable cables and plugs to enable the circuit to be interposed between the coding busses and the commutator segments. Each switch has six positions to enable the operator to cross-connect any one of the five decode conditions to any pair of commutator segments (inner and outer rings) or leave the connection open. The second method employs the six code sequence switches and five permutable cords which are part of the terminal coding equipment.

The procedure followed in using the applique circuit is straightforward. The 18 switches are originally set to the open (S) position, and then, by rotating switch No. 1 through its five decode positions and listening at the output of the terminal, the correct condition for segment No. 1 is determined; this position is recorded before restoring the switch to the open position. In a similar manner the correct decodes for the remaining 17 segments are determined one at a time. Having recorded the decoding condition for each of the 18 commutator segments, the switches of the applique circuit are then set up to give the proper decoding sequence, thus permitting complete restoration of the intercepted scramble. The applique circuit with its connecting cords is shown in Figure 5, attached.

In the second method, the coding controls of the terminal are utilized. First, all but the first code sequence switches are set to the open (S) position. Setting the first switch on the 0 position connects the first three pairs of commutator segments to the first three coding bus jacks, respectively. While listening at the output of the terminal, all five code cords are tried in the first jack position. The cord found to be correct is set aside and the remaining four are tried in the second jack position. Again the cord found to be correct is set aside and the remaining three cords are tried in the third jack position. In this manner the location of three of the five permutable cords is determined. These cords are then inserted in the first three jacks in the order just previously determined and switch No. 1 is turned to the open (S) position. Switch No. 4 is then rotated through its positions until a setting is found where the bursts of speech sound most natural. Since this setting will always involve either one or both of jack positions 4 and 5, it is possible to determine the location of the two remaining cords by first removing the three previously determined cords, and then trying the two cords in jack positions 4 and 5. All five cords are then inserted in their proper jack positions, and the settings of the four remaining code sequence switches are determined aurally, one at a time, as previously described.

If the location of one or more of the permutable cords is incorrectly determined, no satisfactory settings of the code sequence switches will be found. Consequently, the presence of such an error is readily discernible and can be corrected by redetermining the cord locations. However, when the cord positions have been properly chosen, the selection of the switch settings can be made rapidly and accurately since, with three successive segments available to each switch, the bursts of speech will be present in the receiver for a maximum time of 3 x 43 or 129 milliseconds per cycle. This time interval more nearly corresponds to the length of a syllable. For these reasons, more accurate results can usually be obtained with this method than with the applique circuit.

The cord permutation and combination of switch settings obtained with this method will not necessarily agree with that in use at the transmitting terminal, although the coding sequence will be the same. A study of the coding scheme used in this system will show that any of 12×10^6 possible coding sequences may be set up in ten different ways; all dependent upon which of the ten possible variations of the fundamental permutations of the cords is used. This is explained in detail in Section 3.5.

The preceding schemes were first investigated with the transmitting terminal serving as the signal source. This insured exact synchronism between terminals. Further tests were made to determine the feasibility of applying this method to a recorded scramble. The results, using a magnetic tape recording device, were highly satisfactory.

Since either condition A or B could be decoded satisfactorily by the other, it was generally difficult and time consuming to attempt to differentiate between them. The additional time required to determine the correct decode condition was disproportionate to the resulting slight improvement in quality.

For this reason, no great effort was made to determine the precise decode condition when either A or B appeared, and the results given below do not include errors due to such interchanges. Furthermore, it was found that a solution of the decoding sequence in which only two-thirds of the segments were determined correctly, exclusive of A and B interchanges, usually resulted in almost complete intelligibility.

The results of a series of tests employing repeated coding sequences disclosed that on an average the correct decodes for 16 of the 18 segments could be obtained in five to ten minutes using the applique circuit. When the terminal coding controls are employed, essentially the same length of time is required, although the scheme is inherently more accurate. Determination of the coding sequence using a Japanese language recording afforded similar results, thus demonstrating that the operator need not be familiar with the language in use in order to apply the method. The use of pre-equalization at the transmitting terminal increased only the solution time for either scheme by a factor of about two.

In the preceding tests the circumferential position of the START-STOP LATCH RELAY was the same at both terminals. However, there still exists the possibility that the legitimate operators of the system might occasionally shift their latch positions. Under these conditions it would then be necessary for the interceptor to establish the approximately correct position of his latch relay before undertaking the determination of the coding sequence. This position would be found by shifting the latch relay in small circumferential increments until it is possible to determine the proper decode conditions for several segments. The remainder of the decoding sequence would be determined in the usual manner.

The decoding of a non-repeated coding sequence on a cycle-by-cycle basis was also attempted. A single cycle (0.77 second) of the coded signal was recorded on a magnetic tape rotating in synchronism with the sending brush. This recorded signal was then played back through the receiving terminal. In general, the method was found to be unsatisfactory since so few of the elements of the code cycle could be determined with any certainty. The reason for this lack of success lies in the difficulty of making a choice of decodes on the basis of a single speech sample having a maximum possible duration of only 43 milliseconds. However, where considerably longer time elements are used, this method might prove successful.

3.34 Automatic Analyzer-Decoder Circuit

One method of obtaining the intelligence from a coded band-scrambled system would be the use of an automatic analyzing circuit which would provide the appropriate decodes in synchronism with the coding pattern generated by the transmitting terminal. From an inspection of the frequency translations produced by the New Zealand system,it will be seen that the original 3-kc band is divided into three equal bands with frequency boundaries at 0, 1000, 2000, and 3000 cycles, and each code condition employs a different arrangement of these three bands. If the energy level in the 0 to 1000-cycle portion of clear speech is greater than that in the 1000 to 2000-cycle portion, and if the energy level in the 1000 to 2000-cycle portion is greater than that in the 2000 to 3000-cycle portion, the frequency translations of these three bands by the five code conditions would also result in five different energy distributions. When such conditions prevail, it would be possible to identify the frequency translations involved at any instant by comparing the relative energies of the three bands. Furthermore, these comparisons could be utilized to operate differential relay circuits which would automatically insert the proper decode for any instant. It was found, however, that with normal speech sounds the energy in the 1000 to 2000-cycle portion of clear speech was not always greater than the energy in the 2000 to 3000-cycle portion. Consequently, many erroneous decodes were called for, resulting in low intelligibility.

As a result of this experiment, the analyzing circuit was modified to detect, in the scramble, the location of the original 0 to 1000-cycle band which normally contains most of the speech energy. In this scheme, scramble conditions A and E can be recognized and decoded correctly. Condition B is identified as A but can be decoded by the decode of A to give partial restoration with almost 100 per cent intelligibility. Since the location in the scramble of the original 0 to 1000-cycle band does not differentiate between conditions C and D, it was decided that when either occurred, the decode of condition D would be applied. Normally this choice would be correct 50 per cent of the time. Therefore, assuming that the frequency of occurrence of the five scramble conditions is uniform, a proper or partial decode will be supplied 80 per cent of the time in the complete arrangement. The circuit of the automatic analyzer-decoder employed is shown schematically on the attached Drawing ES-842436.

This method was used satisfactorily to decode the

New Zealand type of scramble as long as the transmission medium (microphone, input circuits, etc.) between the talker and the scrambling circuit did not appreciably alter the relative energy levels of the voice spectrum. Tests employing both repeated and non-repeated coding sequences indicated that at least 50 per cent of the intelligence was obtainable on the first listening and that the remainder could be had with a few additional listenings.

The use of pre-equalization at the transmitting terminal greatly decreases the automatic decoding ability of this type of circuit because, as ideal pre-equalization over the voice range is approached, the relative energy differences, which the circuit requires in order to analyze the various scramble conditions, is effectively eliminated. From this standpoint, therefore, it would be desirable to incorporate pre-equalization in the band-scrambled type of privacy system in order to thwart the successful application of an automatic analyzer-decoder circuit by an interceptor. Although the performance of this latter device could be improved through further development, it was intended merely to demonstrate a principle and in this respect represented a satisfactory stage of development.

3.4 Cryptographic Decoding Method

3.41 Repeated Coding Sequence

From analyses of several spectrographic samples of the scramble produced by the New Zealand switched band privacy system, it is possible to determine the frequency translations of the various code conditions employed, as well as determining the duration and sequence of these conditions for a repeated cycle. Recognition of the various frequency translations is based on a study of the pitch changes and energy distribution of each code condition. The time boundaries of each element are clearly revealed by the discontinuities arising from switching the various code conditions, and the beginning of each cycle is indicated by the 4-kc pulse trace.

In most cases, the solution of the sequence of scrambled conditions can be made by careful inspection of the original spectrograms. Often a considerable number of the elements in a sequence can be determined by the analysis of only one cycle. However, as the elements are of rather short duration, the identification of elements not exhibiting pronounced pitch variations may be difficult, and in such cases, corresponding elements in other cycles must be analyzed in order to obtain a complete solution. The determination of questionable elements is also facilitated by recognizing an inherent feature of the coding system, namely, that a particular scramble condition may not be used more than once in any group of three successive elements which are under control of the same code sequence switch. For example, if on the first inspection, a group of three elements is thought to employ the sequence CAC, the two C's should be checked as this sequence cannot be obtained.

Assuming that a terminal or other decoding equipment is available, an alternative method of analysis is to decode the scramble by each of the five conditions separately and make spectrograms to show the elements that are properly restored by each condition. It is obvious that the restored elements must have been scrambled by the same condition that was used in decoding. This method is fundamentally more exact than direct analysis but in practice the difference is almost negligible. It is possible that extremely questionable choices might be resolved by the matching of such restored elements. However, our experience has been that such verifications as are required could usually be obtained through comparison of corresponding elements in other cycles.

In order to utilize the results of a cryptographic solution, the coding sequence may be set up directly either by the special coding applique circuit, or by translation into a combination of code sequence switch settings and a cord permutation which can be applied to the equipment. The method of translation is discussed in Section 3.52.

Complete cryptographic solutions, including the preparation of the spectrographic material, analysis of the spectrograms, and translation of the determined coding sequence to cord permutations and switch settings, can be made in 20 to 25 minutes under favorable conditions. When a minimum of delay is required, partial solutions may prove satisfactory, provided that at least two-thirds of the elements of the cycle are properly restored. Such solutions may be obtained in the order of ten to 15 minutes.

3.42 Non-Repeated Coding Sequence

In general, the cryptographic analysis of non-repeated coding sequences involves essentially the same problems and techniques as in the solution of repeated coding sequences, with the exception that no assistance may be had through comparison of the scramble conditions used for corresponding elements in other cycles. Usually it is impossible to obtain the complete sequence for any 18-element cycle when this type of coding is used.

It would be possible, though very laborious and time consuming, to restore the complete messagesby solving, as completely as possible, each cycle independently. However, a practical appraach, from an interceptor's standpoint, would be to apply the information obtained, from the partial solution of several cycles, to synchronize his auto-coding unit with the authorized terminals, thereby restoring the entire message.

This method, which is discussed in detail in Section 3.5, requires that the cord permutation for each cycle analyzed be determined. In addition, the fixed settings of the code sequence switches and the relative separation of the cycles analyzed must be tabulated. Usually nine cycles scattered throughout the major coding cycle will provide enough data for a satisfactory application of the method. With a trained crew and adequate equipment, this method would require approximately one hour.

It should be emphasized, when dealing with the distinct cycles of a non-repeating code, that only partial solutions of individual cycles can be obtained. However, it is usually possible to determine completely the effective permutation for each of the selected cycles when only two or three of the three-element groups are known. This procedure is discussed in detail in Section 3.55. Since the code sequence switches are fixed during a major coding cycle of the auto-coding unit, the early determination of their settings affords some assistance in determining the permutations for the remaining samples. For this reason it is desirable to begin the analysis with samples that offer as complete and positive solutions as possible.

3.5 Analysis of Coding System

3.51 General

The following analysis of the coding system employed in the New Zealand switched band privacy units is made from the point of view of one who is in possession of a captured terminal unit and wishes to make the most use of it in decoding intercepted scrambled speech transmitted by an identical unit employing an unknown code. One of the problems confronting the interceptor is that of translating the data obtained from analyzing the sequence of speech scrambles into terms of settings of code sequence switches, permutations of the cords from the scrambler unit, and the starting point of the automatic code changing unit so that the scrambled material may be decoded properly. For this purpose a fairly complete knowledge of the coding scheme is necessary.

The proposed method, discussed in Section 3.55, for determining starting points of the automatic code changing unit represents only one, though not necessarily the best, approach to the problem. This method does, however, appear to be practicable and has been used successfully in cracking non-repeated, i.e., eight-minute period, codes.

In the present models of the New Zealand units the design of the coding arrangements is such that fairly simple relationships exist between the settings of the sequence switches and permutations of cords and the resulting sequences of speech scrambles. If the present design were altered to eliminate the systematic changes effected by the sequence switches, the relationships could be made very much more complicated, and possibly, therefore, less useful to the decoding (cracking) technique.

3.52 Translation of Repeated Coding Sequence to Coding System

In the New Zealand scrambler unit the five pairs of coding busses (jacks designated 1, 2, 3, 4 and 5) are connected to the 18 segments of the inner and outer rings of the commutator in a manner determined by the settings of the six code sequence switches, each switch controlling the connections to three adjacent commutator segments. The scheme of connections is indicated below in Table I, which is reproduced for convenient reference from Report R.D. 1/407, Radio Development Laboratory, Department of Scientific and Industrial Research, Wellington, New Zealand, entitled SWITCHED BAND PRIVACY SYSTEM (advance draft copy), dated August 31, 1944.

TABLE I

Position	Switch No. 1	Switch No. 2	Switch No. 3	Switch No. 4	Switch No. 5	Switch No. 6
0	1 2 3	2 3 1	3 1 2	1 3 5	3 5 1	5 1 3
1	2 3 4	3 4 2	4 2 3	3 5 2	5 2 3	2 3 5
2	3 4 5	4 5 3	5 3 4	5 2 4	2 4 5	4 5 2
3	4 5 1	5 1 4	1 4 5	2 4 1	4 1 2	1 2 4
4	5 1 2	1 2 5	2 5 1	4 1 3	1 3 4	3 4 1
5	5 4 3	4 3 5	3 5 4	4 2 5	2 5 4	5 4 2
6	4 3 2	3 2 4	2 4 3	2 5 3	5 3 2	3 2 5
7	3 2 1	2 1 3	1 3 2	5 3 1	3 1 5	1 5 3
8	2 1 5	1 5 2	5 2 1	3 1 4	1 4 3	4 3 1
9	1 5 4	5 4 1	4 1 5	1 4 2	4 2 1	2 1 4
Com. Seg. No.	1 2 3	4 5 6	7 8 9	10 11 12	13 14 15	16 17 18

From an interceptor's viewpoint, the chief use of Table I is in the translation of a repeated coding sequence, which has been determined, to the proper switch settings and code cord permutation. In beginning such a translation, it is permissible to set any one of the six switches on any one of its ten positions because, as will be explained later, there are always ten different translations possible for any sequence and these translations will involve all ten positions of each switch once and only once. The procedure for obtaining one of the ten possible translations may best be explained by an example. Let us assume that the sequence of code conditions for a repeated cycle has been found to be

BDE CBA ADE BAD CDE EDC

and that we have set switch No. 1 on position 0. As indicated in Table I, the setting of switch No. 1 on position 0 connects commutator segments No. 1, 2, and 3 to coding bus jacks 1, 2, and 3, respectively. Since the sequence BDE must appear on these segments, the code cords B, D, and E should be patched to coding bus jacks 1, 2, and 3, respectively. Substituting these jack numbers for the code cords now assigned to them, the sequence will read as follows:

123 -1- -23 1-2 -23 32-

A study of Table I will show that if two out of the three code bus jack connections to any one switch are known, the position of that switch is determined and the remaining jack connection to it is obtained. Thus, in the example, the positions of switches No. 3, 4, 5, and 6 are found to be 1, 9, 1, and 6, respectively, and the sequence will be

123 -1- 423 142 523 325

Comparing this coding bus jack sequence with the original code condition sequence, it will be seen that code cord A must now be patched to coding bus jack 4 and code cord C to coding bus jack 5. This makes the sequence for switch No. 2 read 514 which, from Table I, establishes its setting as position 3. The complete translation is as follows:

Position of Switches	Code Cord Permutation
	(1 2 3 4 5)
0 3 1 9 1 6	B D E A C

The other nine translations for this same sequence may be found in a similar manner by starting with different switch positions. The ten translations of this example are tabulated below:

Position of Switches	Code Cord Permuation
	(1 2 3 4 5)
0 3 1 9 1 6	B D E A C
1 4 2 6 4 8	C B D E A
2 0 3 8 2 5	A C B D E
3 1 4 5 0 7	E A C B D
4 2 0 7 3 9	D E A C B
5 8 6 2 8 4	C A E D B
6 9 7 4 6 1	A E D B C
7 5 8 1 9 3	E D B C A
8 6 9 3 7 0	D B C A E
9 7 5 0 5 2	B C A E D

3.53 Coding System (Without Automatic Code Changing Unit)

The five speech scrambling circuits (cords with plugs designated A, B, C, D, E) may be patched into the coding bus jacks in any order which may be indicated, for example, by the notation

(1 2 3 4 5)
(B E A C D)

It is somewhat more convenient, however, to make the numerical substitution 1 = A, 2 = B, 3 = C, etc., and hence denote the above patching order by

$$\begin{pmatrix}1 & 2 & 3 & 4 & 5\\2 & 5 & 1 & 3 & 4\end{pmatrix}$$

or, more briefly, by the permutation 2 5 1 3 4.

Using this latter notation, Table I may be thought of as portraying the distribution of speech scrambling conditions (rather than of coding busses) when the patching order, or permutation, is 1 2 3 4 5. Similar tables for any other permutation can be derived from Table I by making the changes in the bus numbers as specified by the given permutation.

The scheme of connections portrayed by Table I has the following property: When the orders of patching are denoted by permutations which are members of the same family, the resulting tables derived from Table I will contain the same sequences of three scrambling conditions within the same columns and will differ only in the positions of the switches at which they occur. A family of permutations is defined as that group of ten permutations derived from a given permutation by circular shifts of both the given permutation and the reverse of the given permutation. For example, the family of permutations, of which 1 2 3 4 5 is the dominant* member, is shown in Table II.

TABLE II

Relative Number	Permutation	Operation
1	1 2 3 4 5	Given permutation
2	5 1 2 3 4	One shift to right
3	4 5 1 2 3	Two shifts to right
4	3 4 5 1 2	Three shifts to right
5	2 3 4 5 1	Four shifts to right
6	5 4 3 2 1	Reverse permutation
7	4 3 2 1 5	One shift to left
8	3 2 1 5 4	Two shifts to left
9	2 1 5 4 3	Three shifts to left
10	1 5 4 3 2	Four shifts to left

* The dominant of the family is the permutation having the lowest numerical value when treated as a 5-digit number. It is not necessarily Relative No. 1.

It will be noted that permutations 6 to 10 are the reverse of permutations 1 to 5, respectively.

From the foregoing it follows that any sequence of the scramble conditions, resulting from a given set of switch settings, and a permutation, can be established in a total of ten different ways, i.e., by changing the permutation to others within the same family and making appropriate changes in the positions of the switches. Moreover, the ten different groups of switch settings will involve all ten positions of each switch once and only once.

At this point, a remark on the number of distinct 18-element sequences possible with this equipment may be in order. The six sequence switches, having ten useful positions, give rise to a total of 10^6 distinct coding sequences for a given permutation. The five scrambling circuit cords may be permuted in 120 ways, but only one tenth of these yield distinct sequences. Hence, the total number of distinct sequences is 12 x 10^6 rather than 60 x 10^6 as stated in Report R.D. 1/407.

If the "Relative Numbers" are identified with the "Operations" as indicated in the example of a family of permutations given in Table II, a succinct and complete schedule of the changes in positions of the sequence switches corresponding to changes of permutation within a family of permutations can be given as follows:

TABLE III

Schedule of Positions for Switches No. 1, 2, and 3

Relative Number	1	2	3	4	5	6	7	8	9	10
	0	1	2	3	4	5	6	7	8	9
	1	2	3	4	0	6	7	8	9	5
	2	3	4	0	1	7	8	9	5	6
	3	4	0	1	2	8	9	5	6	7
	4	0	1	2	3	9	5	6	7	8
	5	9	8	7	6	0	4	3	2	1
	6	5	9	8	7	1	0	4	3	2
	7	6	5	9	8	2	1	0	4	3
	8	7	6	5	9	3	2	1	0	4
	9	8	7	6	5	4	3	2	1	0

Schedule of Positions for Switches No. 4, 5 and 6

Relative Number	1	2	3	4	5	6	7	8	9	10
	0	3	1	4	2	7	5	8	6	9
	1	4	2	0	3	8	6	9	7	5
	2	0	3	1	4	9	7	5	8	6
	3	1	4	2	0	5	8	6	9	7
	4	2	0	3	1	6	9	7	5	8
	5	7	9	6	8	3	0	2	4	1
	6	8	5	7	9	4	1	3	0	2
	7	9	6	8	5	0	2	4	1	3
	8	5	7	9	6	1	3	0	2	4
	9	6	8	5	7	2	4	1	3	0

The use of the above schedules can probably be best explained by means of the following example:

Let the settings of the six sequence switches and the permutation be

Settings of Switches	Permutation
5 1 6 2 8 4	3 1 5 4 2 (Relative No. 1)

It is required to determine the new settings of the switches to produce the same coding sequence when the permutation is reversed and shifted two places to the left. It will be seen from Table II that the new permutation (5 1 3 2 4) is Relative No. 8.

Referring to the first schedule in Table III (Switches No. 1, 2, and 3), we find 5 in the column for Relative No. 1 and move horizontally across to the column for Relative No. 8 and find 3. Hence, switch No. 1 must be changed from position 5 to position 3. The other changes in switch positions are determined in the same way, using the appropriate schedule. The final result is

Settings of Switches	Permutation
3 8 4 5 0 7	5 1 3 2 4 (Relative No. 8)

3.54 Families of Permutations

In the previous section a family of permutations was defined and an illustrative example was given. In this section we consider the classification of the 120 (= 5!) possible permutations of five elements into 12 distinct families. These families are designated by their dominant members and the tabulation of the dominant members in numerical ascending order forms the basis of the serial, or family, numbers assigned to them.

TABLE IV

Family Number	Dominant of the Family
1	1 2 3 4 5
2	1 2 3 5 4
3	1 2 4 3 5
4	1 2 4 5 3
5	1 2 5 3 4
6	1 2 5 4 3
7	1 3 2 4 5
8	1 3 2 5 4
9	1 3 4 2 5
10	1 3 5 2 4
11	1 4 2 3 5
12	1 4 3 2 5

3.55 Automatic Code Changing Unit

The automatic code changing unit is a device for automatically changing the permutation of code condition cords once each revolution of the brush arm. The unit has five pairs of input jacks. designated 1, 2, 3, 4, 5 and five output cords with plugs designated A, B, C, D, E. It can therefore be interposed between the five code condition cords (A, B, C, D, E) and the five pairs of coding busses (jacks 1, 2, 3, 4, 5) of the main scrambler panel. Two 25-step selector switches operated in series effect the changes in permutation between the input jack circuits and the output cord circuits of the unit. Since both the "scrambler in" and "scrambler out" circuits are permuted simultaneously, four selector switches, i.e., two pairs, are included in the unit. One of a pair of selectors (the "fast selector") steps each time the latch operates, the other (the "slow selector") steps once each time the fast selector completes 25 steps. Thus, a total of 625 steps, or changes in permutation, is involved before the major cycle of changes is repeated.

Since both sets of cords into and out of the coding unit may be permuted manually, an analysis of the code changes must include not only the changes in permutation effected by the automatic code changing unit itself but also the effect on those changes caused by both the input and output permutations.

For given input and output permutations of the automatic code changing unit, the sequence of permutations presented to the coding bus jacks can be written down for each of the 625 steps of the selector switches. This has been done for the

the case where both permutations are normal, i.e., 1 2 3 4 5, and the resulting series of permutations has been classified according to family numbers given in Table IV. This series of permutations and family numbers is tabulated on attached Drawing ES-842434, pages 1 to 4, inclusive. The series of family numbers has also been arrayed in the form of a 25 x 25 matrix in which the 25 steps of the first cycle of the fast selector are placed in column 1, those of the second cycle in column 2, and so on. This matrix is shown on Drawing ES-842425, attached.

On the average, each of the 12 family numbers appears 52 times in the matrix, and the positions at which a given family number occurs form a definite pattern. There are, obviously, 12 such patterns contained within the matrix. These patterns of like family numbers are basic to the design of the selector switch wiring and are, therefore, unaltered by any changes in the input permutation. It is true that, in general, a change in input permutation changes all the family numbers in the matrix, but the 12 basic patterns remain -- they merely become associated with different family numbers.

It follows, then, that where it is desired to show only the patterns of like family numbers without regard to what the family numbers are, a single matrix, such as the one constructed, will suffice, regardless of the input permutation assumed. The family numbers in the matrix then serve only to identify like family numbers and could appropriately be replaced by 12 letters of the alphabet.

Before considering the effects of changing the permutation of the output cords of the coding unit, it might be in the interests of clarity to see how the matrix is used to find the starting point in the cycle of 625 steps of the selectors when a few 18-element cycles have been solved. In this case it is assumed that the transmitting machine employed a normal, 1 2 3 4 5, permutation of the output cords.

5.56 Problem

Assume the following nine cycles have been partially solved by cryptographic or other means and that the relative step numbers, as determined by counting the 4-kc latch pulses, are known. It is required to determine the settings of the sequence switches, the input permutation to the automatic coding unit, and the step number of the coding unit corresponding to the first 18-element cycle indicated as Relative Step No. 1. It is to be assumed that the permutation of the output cords of the coding unit is 1 2 3 4 5, and that the settings of the sequence switches were unchanged during the entire sample of scrambled speech.

Relative Step No.	Switches 1	2	3	4	5	6
1		AEB	BCD	EDA		
2			AEC	DCB	DAC	
3		CBE	EAD	BDC	BED	
61				EBA	ECB	ACD
62	ACB	BCE	EAD			
63				DEC	DAE	
152					CDA	EDB
153				ECA	EBC	
154	EDB	BDC				

The first step in the solution of the problem is to determine the complete permutation for each of the nine steps and the corresponding switch settings common to all nine cycles. As explained previously, it is admissible to start with any switch on any position. We arbitrarily start with switch No. 3 in position 0, which, from Table I, yields the coding bus sequence 3 1 2. Hence, in Relative Step No. 1, B connects to bus No. 3, C to No. 1, and D to No. 2. Switch No. 2 must be set to give B (or bus No. 3) in the third place and neither busses No. 1 nor No. 2 in the first and second places. Position 2 for switch No. 2 is the only one which satisfies the condition. The bus sequence is 4 5 3. Hence, since the scrambling sequence is AEB, it is required that A be connected to bus No. 4 and E to No. 5. This establishes the permutation as C D B A E or 3 4 2 1 5 and fixes switches No. 2 and No. 3 on positions 2 and 0, respectively. The sequence EDA for switch No. 4 establishes position 2 for that switch.

The switch settings of the remaining eight cycles are assumed to be the same as for the first cycle and the settings of the remaining switches are determined as the work progresses. The permutations for the remaining eight cycles should also be determined in connection with the switch settings common to all nine cycles. The results of this work, together with the classifications of the permutations according to family numbers, are shown below.

Relative Step No.	Permutation	Family Number	Settings of Switches
			9 2 0 2 6 8
1	3 4 2 1 5	3	
2	5 3 1 2 4	4	
3	1 4 5 3 2	2	
61	4 2 3 1 5	7	
62	1 4 5 2 3	8	
63	2 5 1 3 4	9	
152	2 1 4 5 3	2	
153	4 3 2 1 5	1	
154	5 1 3 2 4	7	

The second step in the solution is to prepare a transparency in accordance with the step and family numbers given above so that the matrix of family numbers may be scanned for the "start" location. This may be done by placing a transparency over the matrix and encircling the nine numbers (marking on the transparency with crayon) corresponding to actual step numbers shown in the "Relative Step No." column. The circles (on the transparency) within which like family numbers should be found are connected together by crayon lines. Those circles having different family numbers will, therefore, have no connecting lines. For the problem at hand, the circles for step numbers 3 and 152 will be connected by a line, as will those for step numbers 61 and 154.

The entire matrix* is then scanned by moving the transparency step by step until the appropriate pattern of family numbers, though not in general the same family numbers, appear in the crayon circles.

Proceeding as above, it is found that when the circle for Relative Step No. 1 is in the tenth column and sixth row of the matrix (equivalent to step 231), the pattern requirements are satisfied. No other position yields a satisfactory pattern. The actual step numbers and the permutations they yield, taken from Drawing ES-842434, for an input permutation of 1 2 3 4 5 are

- -

* For purposes of scanning, it is better to have the matrix extended so that the first column contains the first 50 steps, the second column, steps 26 to 75, and so on. Also, the first half dozen or so columns should be repeated in positions for columns 26 and upward. This will eliminate the confusion occurring at the various boundaries.

tabulated below, together with the permutations required by the problem.

Actual Step No.	Permutations at Output of Unit for 1 2 3 4 5 Input	Permutations Previously Found for Problem	Problem Permutations Shifted 3 to Right
231	5 2 3 4 1	3 4 2 1 5	2 1 5 3 4
232	2 5 1 3 4	5 3 1 2 4	1 2 4 5 3
233	3 4 5 2 1	1 4 5 3 2	5 3 2 1 4
291	4 2 3 1 5	4 2 3 1 5	3 1 5 4 2
292	3 5 4 2 1	1 4 5 2 3	5 2 3 1 4
293	2 4 1 5 3	2 5 1 3 4	1 3 4 2 5
382	1 3 4 5 2	2 1 4 5 3	4 5 3 2 1
383	5 2 3 1 4	4 3 2 1 5	2 1 5 4 3
384	4 5 1 3 2	5 1 3 2 4	3 2 4 5 1

The third step in the problem is to find the permutation at the input of the automatic coding unit. To do this we examine the permutations tabulated above for an input permutation of 1 2 3 4 5 and observe, for example, that 1 appears in the fifth place in the instances of steps 231, 233, and 292. In the second column of permutations above, we look for a repeated number occurring in any position of its permutation (but the same position for all three permutations) for steps 231, 233, and 292. The 4's, as underscored in the above table, are seen to be the ones sought. It is evident that these 4's should appear in the fifth position in order to accord with the 1's, similarly underscored above. To accomplish this we are at liberty to shift all of the permutations in the second column provided they are kept within the same family groups. The appropriate shift* is evidently 3 to the right which corresponds to a change in Relative Number from 1 to 4 (see Table II).

On comparing the shifted permutations, shown in the third column of permutations above, with those in the first

* Shifting the 4's from second place to fifth place can be accomplished in two ways: A shift of 3 to right, or reverse and shift 4 to left. Both may have to be considered before the correct one is determined.

column, a one-to-one correspondence is seen to be established by an input permutation of 4 1 5 3 2.

By reason of the shifts in permutations from Relative No. 1 to Relative No. 4, the switch positions must be changed in accordance with the schedules previously given to 6 0 3 1 7 9. This completes the solution of the problem.

3.57 Effect of Permutation of Output of Automatic Coding Unit

As stated previously, the output permutation of the automatic coding unit refers to the order in which the output cords of that unit are patched into the coding bus jacks. Only 12 orders of patching, corresponding to the 12 families of permutations as discussed in Section 3.53, are significant. It would follow, then, that 12 tables of permutations, similar to that on Drawing ES-842434, but with the elements transposed in accordance with the dominants of the 12 families, would be required to portray all of the significant permutations presented to the coding bus jacks by the automatic coding unit with a normal input permutation. Moreover, the 12 matrices of family numbers based on the 12 tables of permutations would be sufficient to determine the starting points of the selectors by the scanning method described in the preceding section.

Although 12 different matrices can be derived from the permutation tables, only six of these have distinct patterns of like and unlike family numbers. The pairs of matrices having similar patterns are those associated with the following pairs of family numbers of output permutations: 1-10, 2-9, 3-8, 4-12, 5-7, and 6-11. The matrices identified with families 1, 2, 3, 4, 5, and 6 are identical with those for families 10, 9, 8, 12, 7, and 11, respectively, provided each family number appearing in one of the sets of six matrices is replaced by its mate, i.e., 1 by 10, 10 by 1, 2 by 9, 9 by 2, etc. Since, for scanning purposes, cognizance is not taken of the numerical values of the family numbers, but only of patterns of like and unlike numbers, only six matrices will have to be scanned.

Each of the six matrices will be identified with a family number and its mate. Hence, when the starting point is found on a matrix, an ambiguity as to family number arises. This question as to the correct family number of the output permutation cannot be resolved immediately, but it is answered during the course of determining the correct input permutation.

The procedure for determining the input permutation follows the general lines described in Section 3.56, but modified as follows: Each of the permutations (from Drawing ES-842434) corresponding to the Actual Step numbers found for the given problem is transposed by the dominants of the pair of families indicated on the matrix. These two sets of permutations must then be compared with the permutations found by spectrographic analyses to determine, in the manner described in Section 3.56, the input permutation and the shift of the problem permutations. It will be found that only one of the two sets of permutations will yield a solution for the input permutation, and the family number associated with the successful set is the correct family for the output permutation.

As before, the sequence switch settings must be altered in accordance with the shift found necessary for the problem permutations.

3.58 Number and Selection of Samples for Analysis

In selecting 18-element cycles to be analyzed and used in determining the starting point of the automatic coding unit, it is highly desirable, of course, to select no more than is necessary to fix the starting point without ambiguity. Practical experience indicates that patterns comprising nine cycles are usually sufficient for the purpose and are conveniently handled by an operator.

It appears to be somewhat easier to scan the matrices for patterns containing like family numbers than for those in which the family numbers are all unlike. Hence, it may be desirable to use a number of cycles somewhat larger than the minimum in order to insure obtaining some repetitions of family numbers in the pattern. However, if the scanning of the matrices is accomplished by electrical or mechanical means, the use of more than nine cycles would probably be neither necessary nor desirable.

Because of certain periodicities in the present wiring scheme of the selectors, ambiguous solutions of the starting point may occur when the scanning pattern covers less than 100 steps. To avoid this difficulty, it is recommended that some of the sample cycles be separated by at least 100 steps from each other.

With the above exception, the selection of the cycles may be made at random. In using the spectrograph, samples of 2.4 second duration are obtained (in the present models), and this automatically yields two, and sometimes three, consecutive cycles. Six spectrograms should be sufficient to obtain the requisite amount of cryptographic material, assuming that care is exercised to obtain samples containing as few pauses or silent intervals as possible.

3.6 Analysis of Recording

3.61 General

The recording of speech scrambled by the New Zealand system was delivered to the Bell Telephone Laboratories by the U. S. Navy Department, as previously mentioned. It comprised two test samples, each of which was coded by a different repeated sequence. The analysis of this recording, both cryptographic and non-cryptographic, was practically completed when the two terminal equipments of the system were received.

3.62 Non-Cryptographic

Only an occasional word or phrase was understood on the first listening of the recorded samples. With repeated listening, it was possible to extract approximately 20 per cent of the words as compared with 40 per cent when listening directly to the scrambled speech from the models, as discussed in Section 3.31. In these testx a 3000-cycle low-pass filter was inserted in the output of the reproducing system in order to eliminate the disturbing effects of the 4-kc synchronizing pulse.

Repeated superposition listening, using various combinations of decodes, was rather successful. The most satisfactory arrangement was found to be the two-path circuit discussed in Section 3.32 and illustrated on Drawing ES-842252. So much intelligence was obtained from sample TEST 1 that the original Bell System article from which the text had been taken was identified. A comparison of the text with the actual intelligence obtained from the recording disclosed that 77 per cent of the words had been correctly understood. Neglecting errors in insignificant words, such as "the", "and", "a", "of", etc., which may be considered as not affecting the intelligence, this rating is increased to 87 per cent. It is felt that this order of intelligence was also obtained with sample TEST 2, although no original script was available for checking the results. Transcripts of the material obtained are appended to this report.

3.63 Cryptographic

The repeated coding sequence employed in each test sample was determined, by visual analysis of spectrograms of the recorded scramble, and found to be as follows:

TEST 1

CBD CBA DAE DCE DCA DBA

TEST 2

AEB DAC BDC ABD DEB EAC

4. Evaluation of Security

The results of tests employing the various cryptographic and non-cryptographic decoding methods indicate that the security of the New Zealand switched band privacy system is very low for military purposes.

4.1 Comparison of Decoding Methods

Only an occasional word or phrase can be understood by listening directly to the incoming scramble. When the superposition method is applied, considerably more words and phrases can be understood on the first listening, although probably not enough to convey the sense of the message. It is necessary, therefore, to record the scramble and resort to repeated listenings in order to extract the maximum amount of intelligence possible. As discussed under Section 3.2, repeated listenings to the scramble directly yielded from 30 per cent to 50 per cent of the words and superposition listening yielded 65 per cent to 85 per cent. The fact that these percentages of intelligence can be obtained by the repeated listening methods indicates a fundemental weakness of this system, namely, that some of the code conditions, particularly E and D, are not inherently private, and other conditions, such as A and B, are not mutually private. Furthermore, the 20:1 cracking ratio, i.e., 20 minutes of listening to extract the above percentages of intelligence from each minute of the message, does not necessarily denote the real security of the system because the scramble may be divided into convenient portions which may then be cracked concurrently by a proportionately large crew. When the automatic analyzer-decoder circuit is used it is possible to obtain a substantial amount (at least 50 per cent) of the intelligence on the first listening. By recording the scramble and resorting to additional listenings almost complete intelligence can be obtained.

When the speech has been scrambled by a repeated code, and when a terminal unit is available to the interceptor, as is usually assumed, the code can be cracked in five to ten minutes by the aural detection method. A repeated code can also be cracked by cryptographic methods, using spectrograms, in 20 to 25 minutes. There would, however, be no occasion to use the latter method since a terminal unit would be required in order to obtain the intelligence, and, with the terminal unit available, the more efficient aural method could be employed.

When the coding is non-repeated, the interceptor can use the non-cryptographic methods discussed above or a cryptographic method which determines the coding setup. The former methods, which require repeated listening, involve decoding times which are proportional to the length of message and yield, in general, something less than all the intelligence. The latter method involves an initial delay of approximately one hour, but it enables the scrambled message to be decoded in the normal manner with a terminal unit.

4.2 Effects of Pre-Equalization on Security

In general, the use of pre-equalization ahead of the frequency scrambler unit increases the security of this system. Its use inhibits the successful restoration of the scramble by the application of automatic analyzer-decoder circuits.

Simple inversion provides the optimum decoding circuit for repeated listening methods when pre-equalization is used. The time required to obtain the same amount of intelligence is increased. It is approximately doubled for all methods except that for the cryptographic determination of non-repeated codes, in which case the increase is approximately 50 per cent.

A. D. FOWLER

D. O. SLATER

E. C. THOMPSON

Bell Telephone Laboratories, Inc.
463 West Street, New York 14, N.Y.

Att.
Appendix, "Transcript of
Intelligence from Recording"
Photographs
Figure 1 - No. 143302
Figure 2 - No. 143303
Figure 3 - No. 143304
Figure 4 - No. 143305
Figure 5 - No. 143306

Drawings ES-842195
ES-842435
ES-842252
ES-842436
ES-842434
ES-842425

APPENDIX

Transcript of Intelligence
from Recording of
New Zealand Switched Band Privacy System
Decoded by Superposition of Code A and Code E

(Observer - E. C. Thompson)

TEST 1

With the growth of teletypewriter exchange service and the general increase in the use of teletypewriters in private line service of various types, questions frequently asked are:

How the teletypewriter operates
What is the start-stop system
How is it used
What is the .....

This article will attempt to answer some of these questions and explain also the fundamental principles of teletypewriters and their auxiliary arrangements as now employed in the Bell System.

There have been developed to meet the needs .... a facsimile record form of communication and at the same .... systems in operation in connection with the Bell System plant. ... telegraph transmission over long distances, it is fundamental that only a single wire ... transmission path is required to carry a signal.

Furthermore, our long experience with manual telegraphy on long lines has proved that reliable and efficient operation may be had by using not more than two conditions on the line, such as code and no code or positive impulses and negative impulses as contrasted with the use of three or more conditions or current values. The entire telegraph plant in the Bell System as well as practically all other ... telegraph systems have been built on this two-condition basis. The manual Morse code uses a succession of dots and dashes to represent the different characters of the alphabet ..... code conditions. This code is not well adapted to teletypewriter control, however, since the signals or different characters vary widely in the time that is required to print a single dot or letter .... combinations of several dots and dashes for some of the less frequently used letters or numerals.

For efficient operation it thus far appears desirable in order to obtain simple mechanisms and obtain maximum operating speeds with ... signaling frequencies ...... different characters of uniform length, that is, each contains the same number of code units.

This condition is met by a five-unit code where each character is identified by the impulses in five units of time and this is the code normally employed in Bell System practices.

Each of the five units in this code may be either positive or negative, current or no current or either of two values of current and the permutations provided are two to the fifth or 32. The ... for the 26 letters of the alphabet ... spaced ..... different signals involving ... system signals .... to include numerals and punctuation marks.

A chart of this code as used in teletypewriter exchange service (TWX) is shown below.

It will be noted that this keyboard is similar to the ordinary typewriter keyboard except that there are only three rows of keys instead of the four as in the typewriter.

On the typewriter keyboard, the lowest three rows of keys are used ordinarily for small letters with a shift key also operated to type the corresponding capital letters.

The fourth or top row carries the numerals and punctuation marks.

.... has capital letters and no small letters .... shift of ... space.

.... position of the letter key is available for the usual punctuation marks and numerals. Thus only three rows of keys are required on the teletypewriter keyboard. The operation of the signaling key sends a signal .... the receiving machine to switch .... machine so that numerals and punctuation marks are obtained until letters or space ...... restores the machine to lower place.

Start-Stop System

For transmitting a signal in the five unit code over a telegraph line, it is necessary to have some system of starting so that ... five impulses may be properly received, identified and interpreted in each receiving circuit.

TEST 2

After making certain that all the low and high tension fuses are intact, the filament and bias circuits should be energized by turning the remote-local filament control switch to the local position.

At this stage it is desirable to take the reading of the bias supply meter which should approximate 160 volts.

All valves will light and unless they are complete with plate circuit reactances required in place. The first stage is to adjust each final operating frequency carrier unit.

This necessitates the turning of the remote-local high tension switch to the high tension position and the frequency control switch to its appropriate position depending whether the selected frequency for the test is a high frequency or a low frequency. So long as a suitable crystal is in ... (phase) a number of linear .... It is advisable to ..... valve, the 65 stage will oscillate regardless of the setting of the tuning condenser.

With the appropriate high frequency or low frequency ... control as the case may be, advanced to approximately the maximum ...... stage the .... cathode current of the 807 as read on the third cathode milliammeter should approximate 30 milliamperes. The only adjustment necessary is to resonate with the appropriate tuning control which is done by observing the usual plate current dip.

Under these conditions the milliammeter reading should be 10 to 15 milliamperes. This control is set at about ..... to the tuning of the buffer amplifier.

The adjustment of the buffer amplifier, although somewhat unorthodox is by no means difficult. Before applying high tension to the buffer stage it is desirable to turn the control of the entire unit to its minimum position because it can .... .. estimate .... the final radio frequency amplifier stage in the high frequency circuit.

This latter adjustment is performed by an operation in the modulation amplifier isolation switch located on the center of the shelf of the equipment.

With these precautions taken, any remote high tension may be applied by turning the remote-local high tension switch to ... high tension two position.

When the buffer amplifier stage is tuned it will be necessary to temporarily break the tuned circuit by plugging in a hand telegraph key with the .... two contacts closed.

With the two circuits closed a reading should be observed on the buffer stage milliammeter of approximately 3 milliamperes, this being the normal plate current in the valve that is used conducive to any grid ....

The adjustment .... entire section introduces ... first control will produce a rise in cathode current and controls should not vary it from a point where approximately 25 to 30 milliamperes are observed.

With power to the buffer stage established, the tuning of the stage may be undertaken. The tuning of this stage as described in an earlier part of this bulletin is undertaken ... . in acceptance of the circuit. .... susceptance ....

Major variations in .... experience established.

Fine variations may be ... variometer ... with .... circuit.

The appropriate low frequency or high frequency plugs, as the case may be, may be inserted in any one of the panel jacks and the reading of the cathode milliammeter maintained under observation. The process of ... should be continued to test until a reduction in cathode current is observed. As soon as a pronounced reduction is observed the connection should be made from the high tension .... . The appropriate ..... low tension.

The whole ultimate objective of this arrangement is to be able to maintain a flat phase .... in exact resonance ...... with the appropriate variometer set somewhere between maximum and minimum setting. The resonant frequency ...... establishes control .... reading is observed and ..... amplifies this last unit.

The buffer stage resonance which is .... maximum or increased current reading.

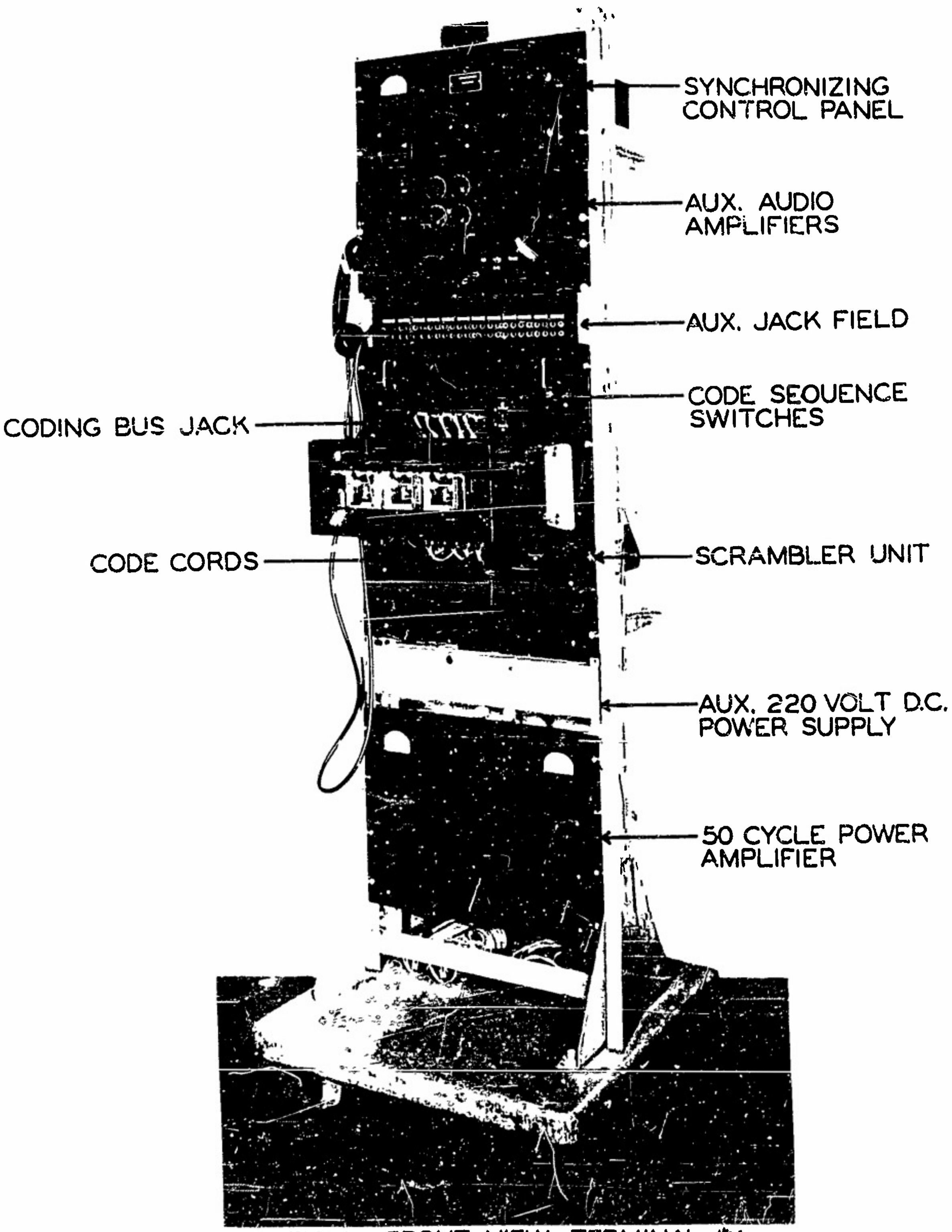


FIG. 1 - FRONT VIEW TERMINAL #1

NEW ZEALAND SWITCH BAND
PRIVACY EQUIPMENT

SECRET

143302

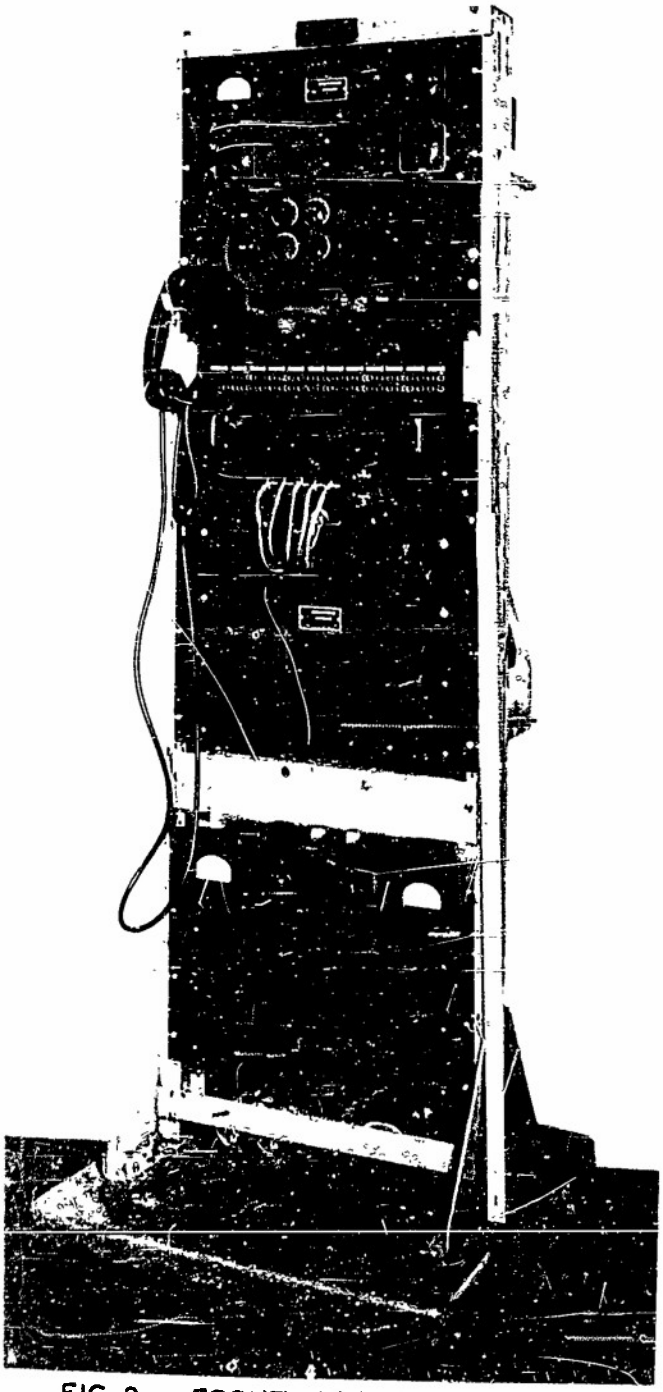


FIG. 2 - FRONT VIEW TERMINAL #1
(AUTO-CODING UNIT REMOVED)

14.3305

NEW ZEALAND SWITCH BAND
PRIVACY EQUIPMENT

SECRET

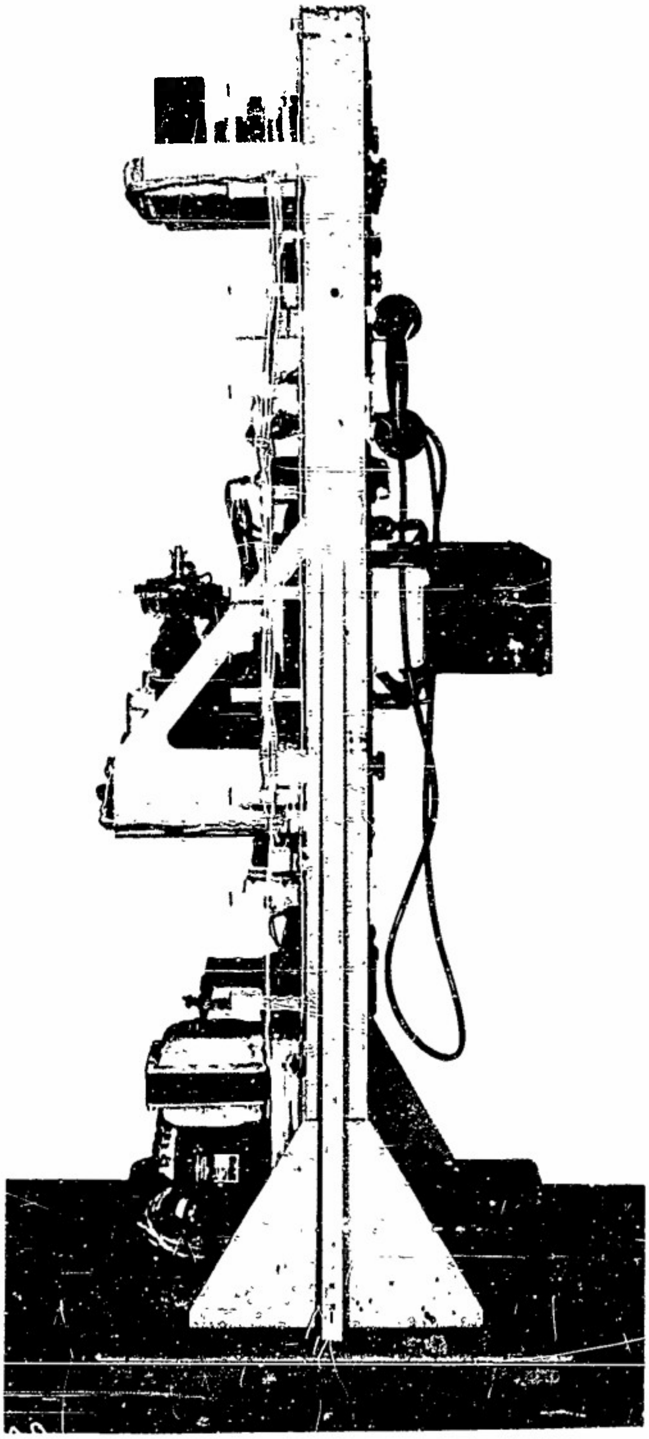


FIG. 3 - SIDE VIEW TERMINAL #1

143304

NEW ZEALAND SWITCH BAND
PRIVACY EQUIPMENT

SECRET

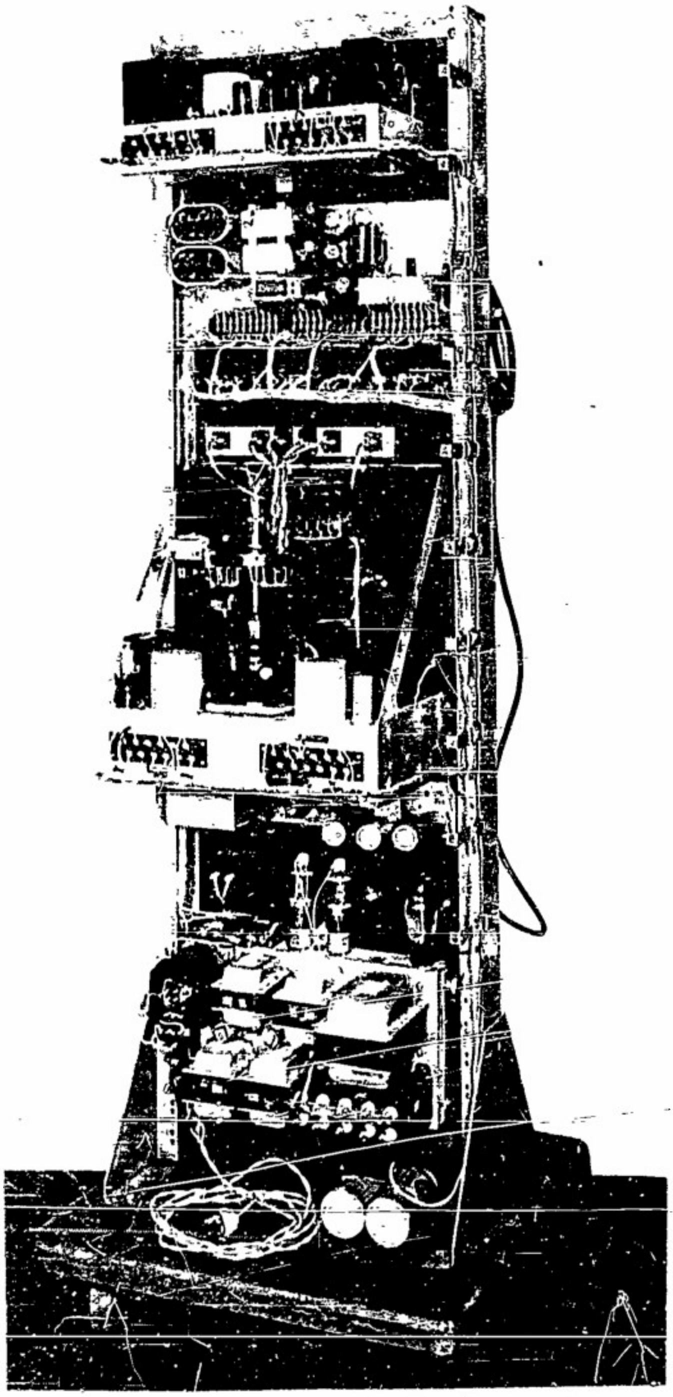


FIG. 4 - REAR VIEW TERMINAL #1

NEW ZEALAND SWITCH BAND
PRIVACY EQUIPMENT

SECRET

143705

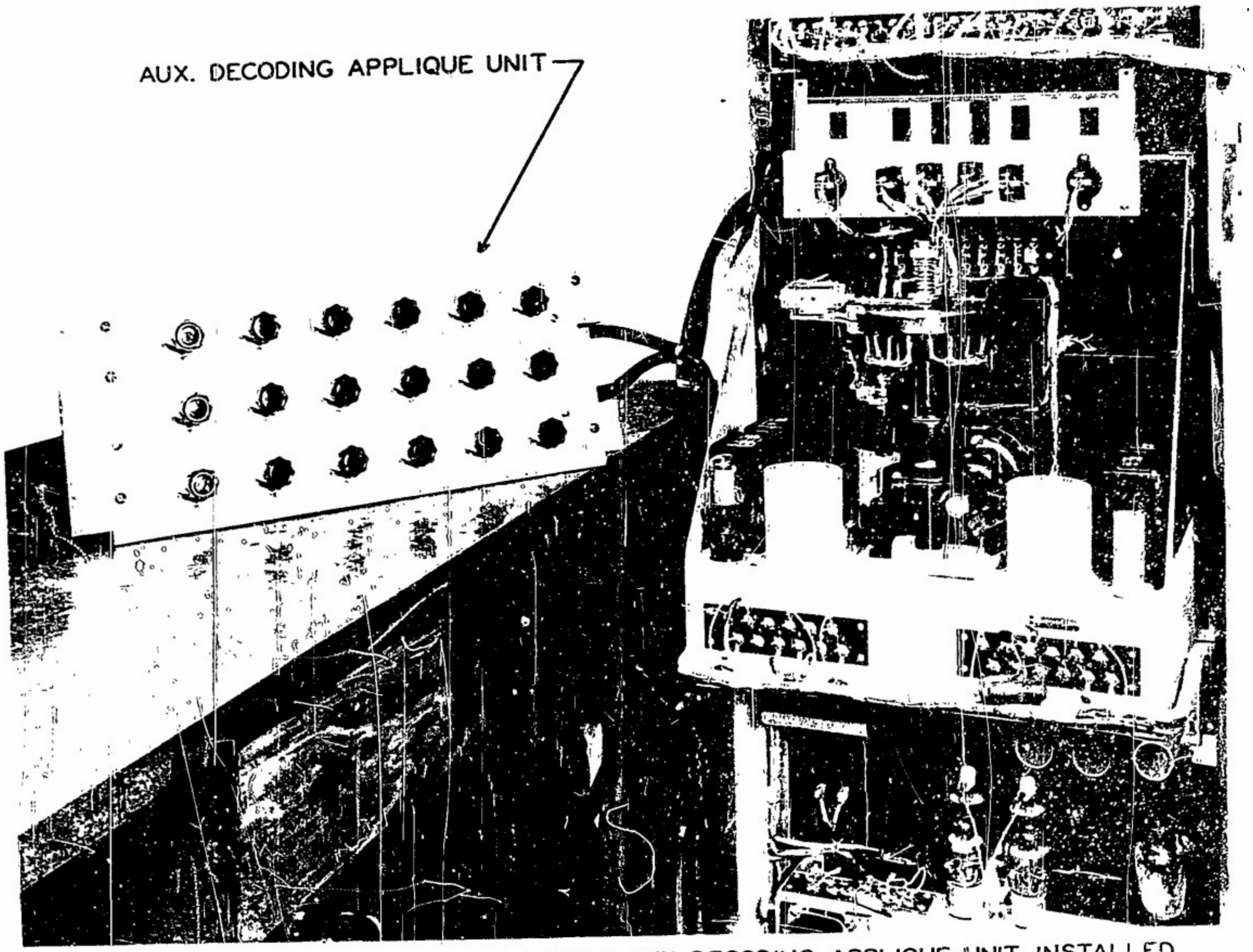
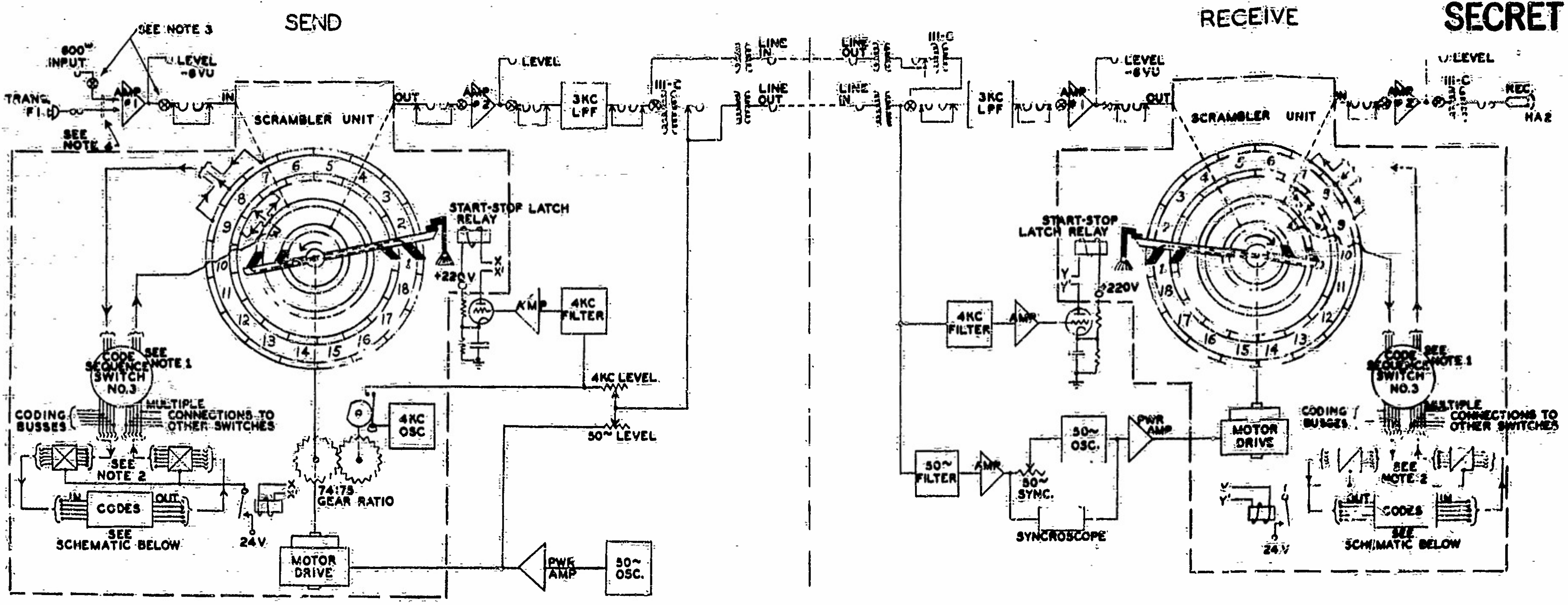


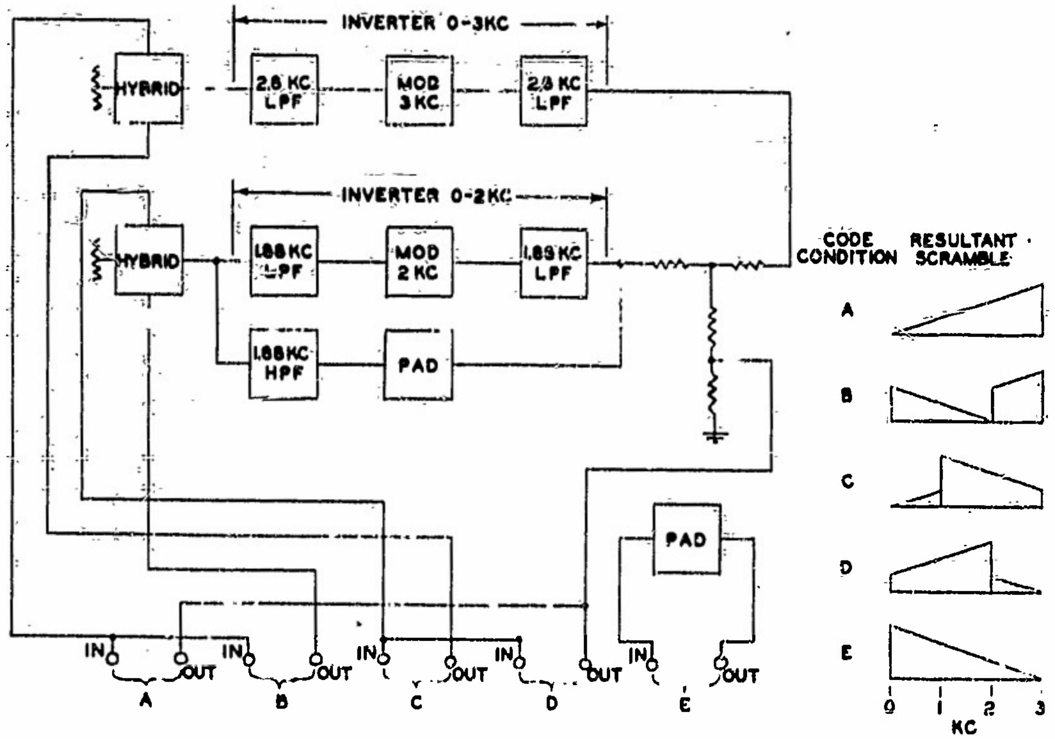
FIG. 5 - REAR VIEW TERMINAL # 1 SHOWING AUX. DECODING APPLIQUE UNIT INSTALLED
NEW ZEALAND SWITCH BAND PRIVACY EQUIPMENT

143306

SECRET

SECRET





NOTE 1
THERE ARE SIX CODE SEQUENCE SWITCHES:
POSITION OF SWITCH NO. 1 CONTROLS SEQUENCE OF CODES TO COMMUTATOR SEGMENTS 1, 2, 3
NO. 2 4, 5, 6
NO. 3 7, 8, 9 SHOWN
NO. 4 10, 11, 12
NO. 5 13, 14, 15
NO. 6 16, 17, 18

NOTE 2
THE SELECTOR SWITCHES ☒ OPERATE ONCE EACH REVOLUTION OF THE COMMUTATOR.

NOTE 3
THE "SEND" AND "RECEIVE" CONDITIONS ARE CONTROLLED BY THE TRANSFER CONTACTS ⊗ OF A PUSH-TO-TALK RELAY.

NOTE 4
CHOICE OF INPUTS UNDER CONTROL OF "MANUAL" SWITCH

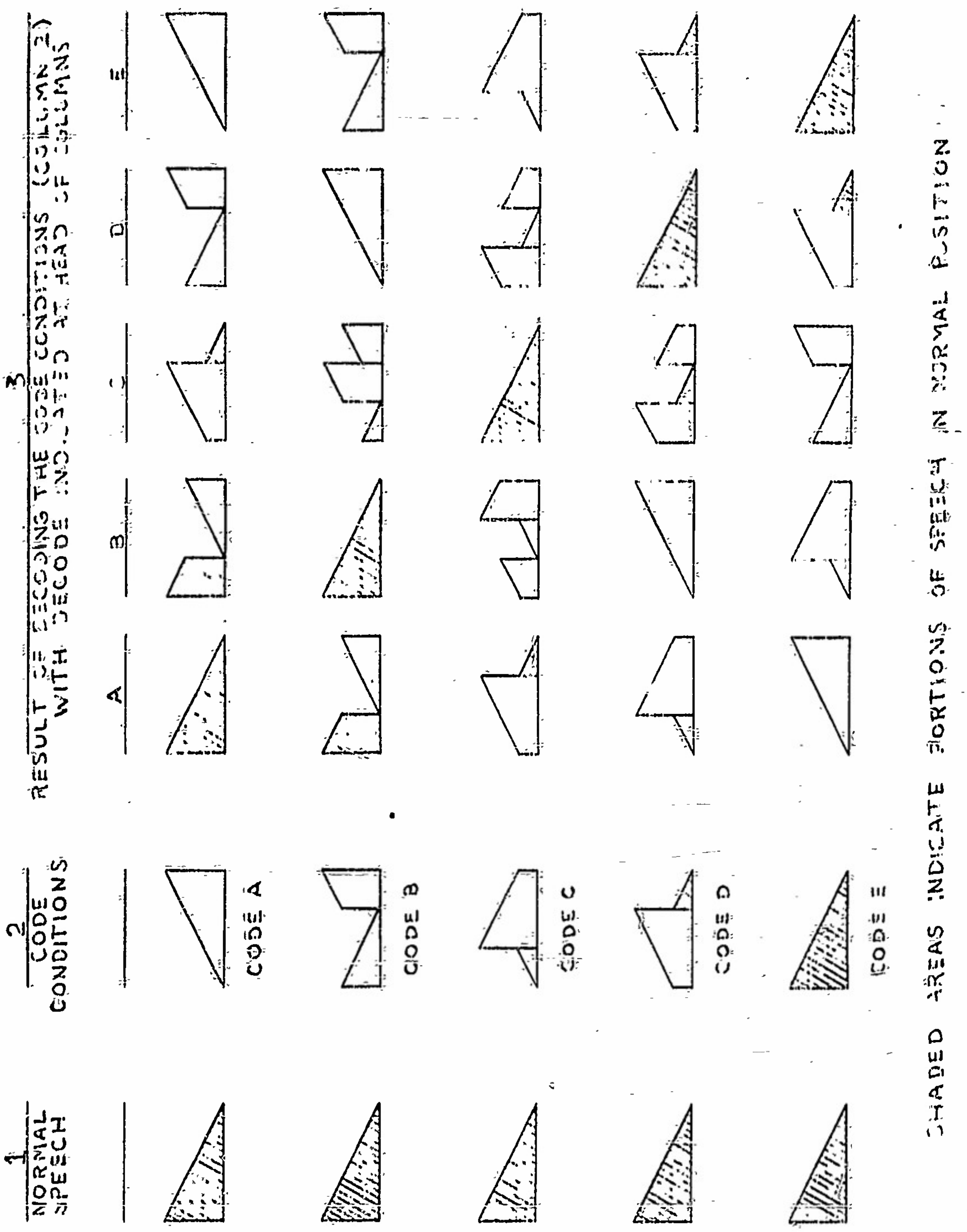
ES-842195
D.O.S. 5-28-45

SECRET

NEW ZEALAND SWITCHED BAND PRIVACY SYSTEM

OVERALL SYSTEM SCHEMATIC

SECRET


1 NORMAL SPEECH
2 CODE CONDITIONS
3 RESULT OF DECODING THE CODE CONDITIONS (COLUMN 2) WITH DECODE INDICATED AT HEAD OF COLUMNS
A
B
C
D
E
CODE A
CODE B
CODE C
CODE D
CODE E

SHADED AREAS INDICATE PORTIONS OF SPEECH IN NORMAL POSITION

SECRET

ISSUE 7-2-45	DR. H.C.W. CH.	TITLE WEDGE DIAGRAMS OF DECODE COMBINATIONS. NEW ZEALAND SWITCHED BAND PRIVACY SYSTEM
	ENG. E.C.T.	SCALE
	APPL.	BELL TELEPHONE LABORATORIES, INC., NEW YORK
		ES-842435

E-318-E (9-42)

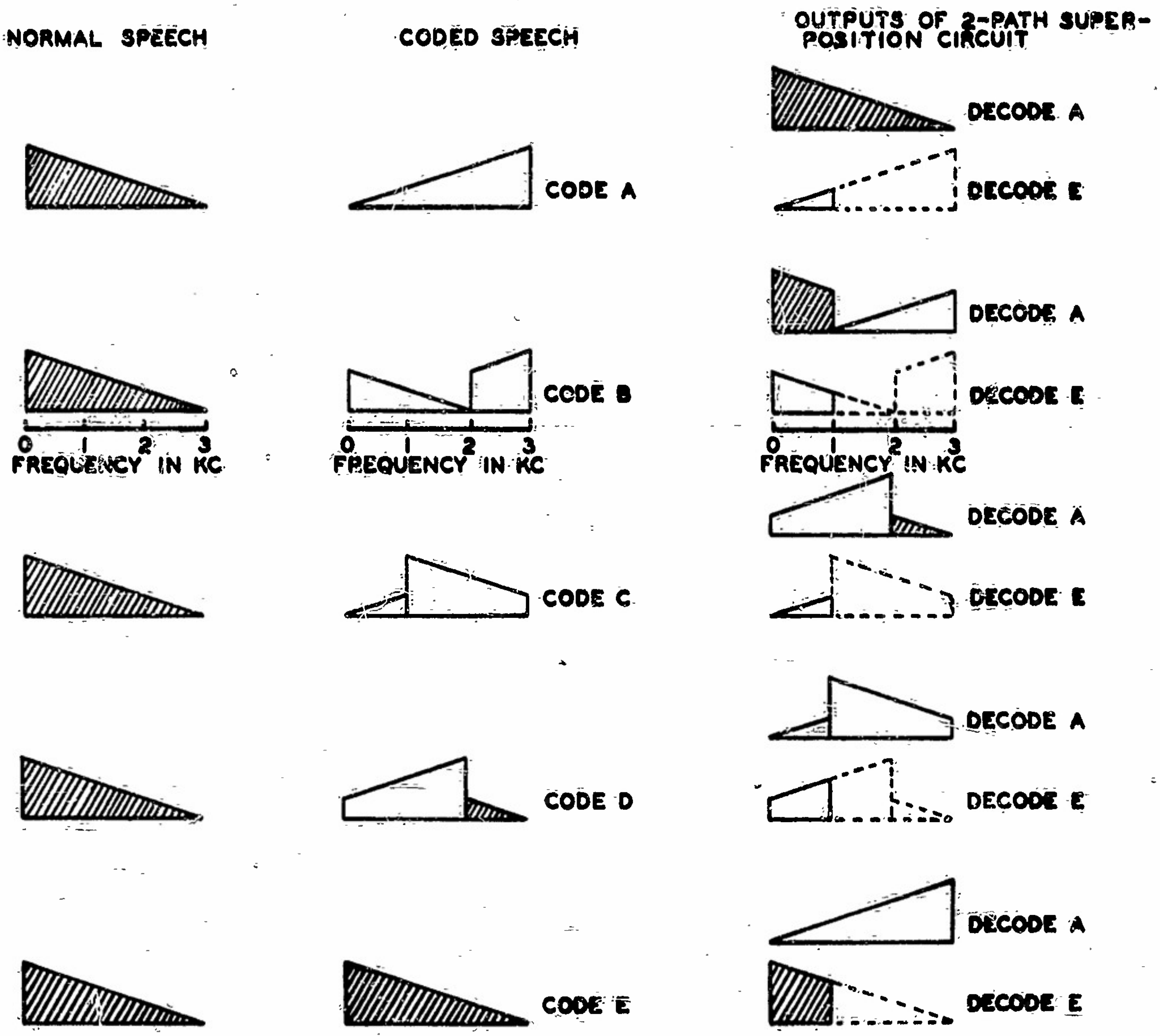
PRINTED IN U.S.A.

BELL TELEPHONE LABORATORIES, INC

ES-842252
E.C.T.3-22-45

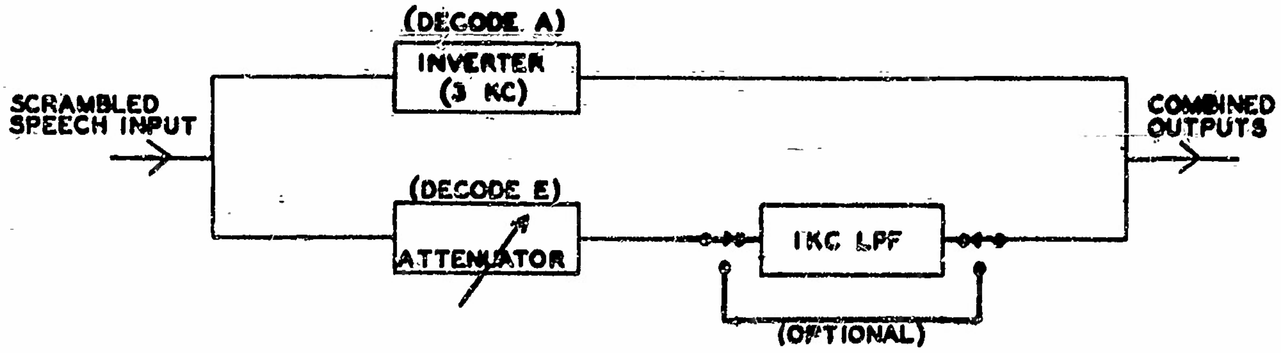
SECRET

FIG. I



1-SHADED AREAS DENOTE PORTIONS OF SPEECH IN NORMAL POSITION.
2-DOTTED OUTLINES DENOTE PORTIONS OF SPEECH SUPPRESSED BY 1KC L.P.F.

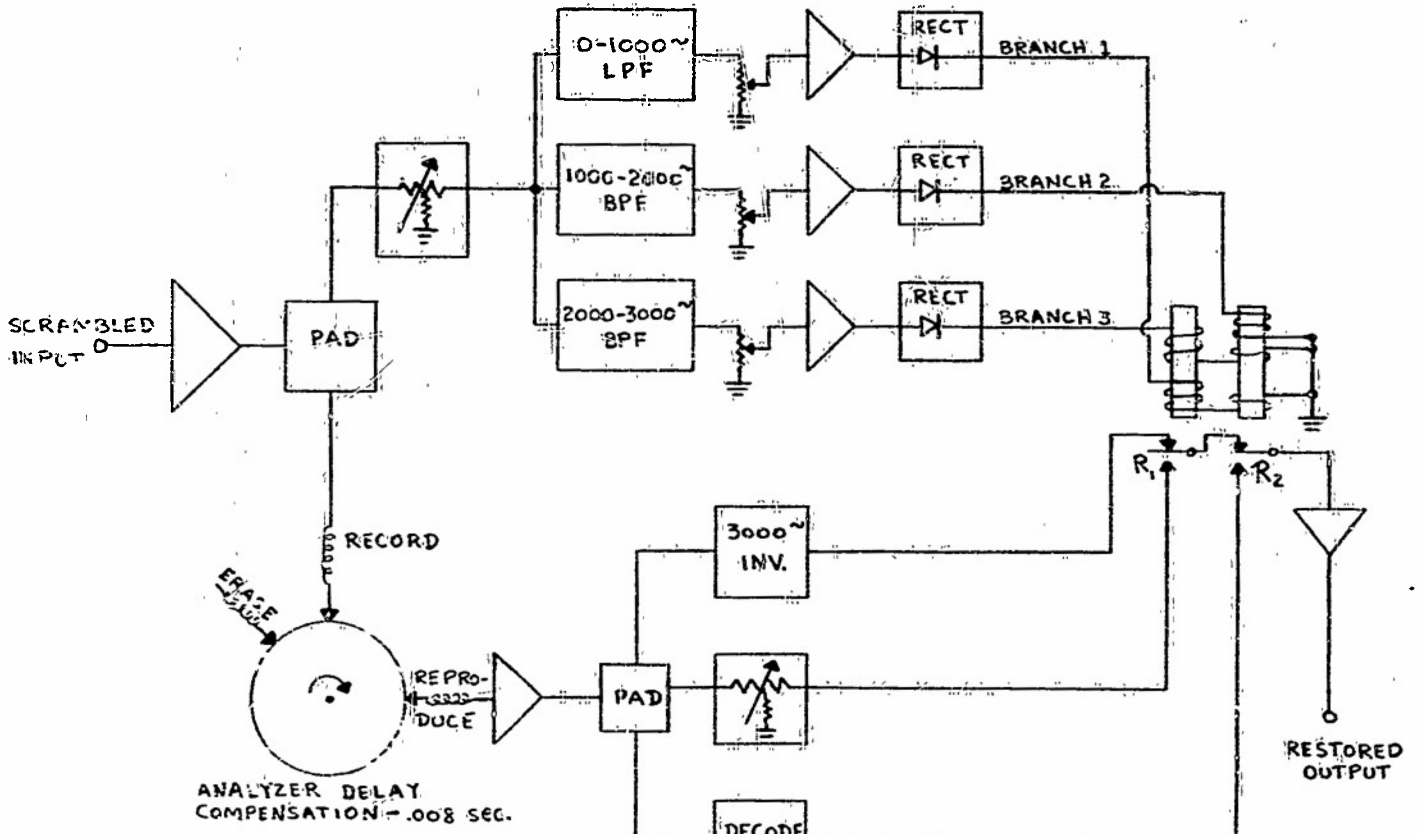
2-PATH SUPERPOSITION CIRCUIT



SECRET

PRINTED IN U.S.A.

SECRET



INCOMING SCRAMBLED CONDITION	MAXIMUM CURRENT IN BRANCH	POSITION OF RELAY R_1	POSITION OF RELAY R_2	CONDITION OF OUTPUT
A	3	UP	UP	RESTORED
B	3	UP	UP	RESTORED (PARTIALLY)
C	2	-	DOWN	UNRESTORED
D	2	-	DOWN	RESTORED
E	1	DOWN	UP	RESTORED

SECRET

ISSUE
7-2-45

APPL.

DR. HCW.

CH.

ENG. D.G.S.

TITLE
AUTOMATIC
ANALYZER-DECODER
CIRCUIT
SCHEMATIC

SCALE

BELL TELEPHONE LABORATORIES, INC., NEW YORK

ES-842436

E-318-E (9-42)

PRINTED IN U.S.A.

Bell Telephone Laboratories, Inc.

SECRET
ES-842434
4 pages, page 1
A.D.F. 6-29-45

OUTPUT PERMUTATIONS AND FAMILY NUMBERS OF AUTOMATIC CODE CHANGING UNIT FOR 625 STEPS OF SELECTORS

Input and Output Cords in Normal (12345) Positions

Step No.	Permutation	Fam. No.	Step No.	Permutation	Fam. No.	Step No.	Permutation	Fam. No.	Step No.	Permutation	Fam. No.
1	12345	1	51	51324	7	101	35124	3	151	21354	4
2	53124	4	52	43512	3	102	41352	10	152	43215	1
3	24351	3	53	12345	1	103	52143	5	153	15342	3
4	43512	3	54	23451	1	104	21435	5	154	53421	3
5	34152	12	55	32541	8	105	12345	1	155	35241	10
6	12543	6	56	51423	11	106	35421	4	156	21453	2
7	21354	4	57	15342	3	107	53142	10	157	12545	1
8	54123	2	58	42513	9	108	42351	11	158	45213	6
9	35214	5	59	34152	12	109	14532	2	159	34125	5
10	32541	8	60	31425	10	110	15423	7	160	31452	8
11	41352	10	61	25341	5	111	23145	8	161	52341	12
12	34125	5	62	32514	12	112	12354	2	162	35214	5
13	45213	6	63	24153	11	113	24531	4	163	54123	2
14	42531	10	64	21435	5	114	25413	8	164	51432	12
15	51342	9	65	45321	2	115	43125	6	165	42351	11
16	24135	10	66	12534	5	116	52314	8	166	15234	12
17	15243	9	67	54123	2	117	34521	6	167	24153	11
18	42351	11	68	21345	6	118	25143	12	168	51342	9
19	51432	12	69	45231	8	119	43215	1	169	42531	10
20	24315	9	70	12354	2	120	52134	6	170	15324	11
21	15423	7	71	54213	4	121	34251	9	171	24513	7
22	43251	12	72	23145	8	122	21543	1	172	53142	10
23	54132	8	73	42531	10	123	42315	7	173	45231	8
24	23415	12	74	13254	8	124	51234	1	174	13524	10
25	14523	5	75	52413	10	125	32451	7	175	25413	8
26	34251	9	76	45213	6	126	12543	6	176	34521	6
27	12345	1	77	32451	7	127	35124	3	177	15342	3
28	45213	6	78	51234	1	128	24531	4	178	42513	9
29	52134	6	79	12345	1	129	45312	4	179	25134	9
30	25314	10	80	21435	5	130	54132	8	180	52314	8
31	34152	12	81	45312	4	131	12345	1	181	34125	5
32	43215	1	82	54231	7	132	21534	3	182	43512	3
33	15342	3	83	31452	8	133	34125	5	183	12345	1
34	21435	5	84	23541	2	134	53214	2	184	51432	12
35	24153	11	85	25314	10	135	52341	12	185	54123	2
36	53214	2	86	14235	11	136	41532	11	186	23514	11
37	25341	5	87	21453	2	137	54123	2	187	52341	12
38	51432	12	88	13542	4	138	43215	1	188	21435	5
39	54123	2	89	15324	11	139	42351	11	189	24153	11
40	13254	8	90	34215	3	140	31542	7	190	13524	10
41	45321	2	91	51423	11	141	24153	11	191	42351	11
42	31452	8	92	43512	3	142	13245	7	192	31425	10
43	54213	4	93	15234	12	143	42531	10	193	24513	7
44	13524	10	94	34125	5	144	31452	8	194	13254	8
45	45231	8	95	51243	3	145	24513	7	195	42531	10
46	31542	7	96	43152	9	146	13425	9	196	31245	4
47	52413	10	97	12534	5	147	45231	8	197	25413	8
48	15324	11	98	31425	10	148	34152	12	198	12354	2
49	42531	10	99	52143	5	149	25413	8	199	45231	8
50	35142	11	100	41352	10	150	14325	12	200	32145	2

SECRET

Bell Telephone Laboratories, Inc.

SECRET
ES-842434
4 pages, page 2
A.D.F. 6-29-45

OUTPUT PERMUTATIONS AND FAMILY NUMBERS OF AUTOMATIC CODE CHANGING UNIT FOR 625 STEPS OF SELECTORS
Input and Output Cords in Normal (12345) Positions

Step No.	Permutation	Fam. No.	Step No.	Permutation	Fam. No.	Step No.	Permutation	Fam. No.	Step No.	Permutation	Fam. No.
201	43152	9	251	25314	10	301	43512	3	351	25341	5
202	21435	5	252	43251	12	302	25431	6	352	13254	8
203	35124	3	253	51342	9	303	31524	9	353	54312	6
204	51243	3	254	13425	9	304	15243	9	354	43125	6
205	15423	7	255	31245	4	305	51423	11	355	34215	3
206	43251	12	256	25413	8	306	43215	1	356	25143	12
207	34125	5	257	52341	12	307	34521	6	357	52314	8
208	25431	6	258	41253	5	308	21435	5	358	14253	10
209	12345	1	259	34521	6	309	52341	12	359	31524	9
210	13254	8	260	35412	2	310	53214	2	360	35142	11
211	34123	2	261	12345	1	311	14523	8	361	42315	7
212	15432	1	262	31254	6	312	51432	12	362	34251	9
213	52341	12	263	14523	8	313	12345	1	363	41523	12
214	53214	2	264	15432	1	314	13254	8	364	45132	7
215	24153	11	265	42315	7	315	24513	7	365	12345	1
216	35412	2	266	31234	1	316	31452	8	366	54231	7
217	42351	11	267	24513	7	317	42315	7	367	21543	1
218	53124	4	268	15342	3	318	13524	10	368	45312	4
219	24513	7	269	42135	4	319	24153	11	369	12435	3
220	35142	11	270	51324	7	320	31542	7	370	54321	1
221	42531	10	271	24153	11	321	42135	4	371	21453	2
222	51324	7	272	13542	4	322	15324	11	372	43512	3
223	25413	8	273	41235	2	323	21453	2	373	14235	11
224	31542	7	274	53124	4	324	35142	11	374	53421	3
225	45231	8	275	21453	2	325	41235	2	375	24153	11
226	52143	5	276	34125	5	326	52413	10	376	31425	10
227	31524	9	277	51342	9	327	34521	6	377	54312	6
228	24135	10	278	42153	5	328	21435	5	378	12453	4
229	41352	10	279	21534	3	329	14352	5	379	24531	4
230	14532	2	280	12354	2	330	41532	11	380	42351	11
231	52341	12	281	34521	6	331	52314	8	381	31524	9
232	25134	9	282	43152	9	332	25431	6	382	13452	6
233	34521	6	283	52341	12	333	31524	9	383	52314	8
234	13254	8	284	15432	1	334	43251	12	384	45132	7
235	12345	1	285	14523	8	335	42315	7	385	41523	12
236	45132	7	286	23154	7	336	15432	1	386	23451	1
237	14523	8	287	12345	1	337	41523	12	387	42315	7
238	43251	12	288	25431	6	338	13254	8	388	25134	9
239	42315	7	289	24513	7	339	12345	1	389	21543	1
240	35142	11	290	53124	4	340	35412	2	390	53421	3
241	24513	7	291	42315	7	341	21543	1	391	12345	1
242	53241	11	292	35421	4	342	53214	2	392	35124	3
243	42135	4	293	24153	11	343	12435	3	393	21453	2
244	35412	2	294	53214	2	344	35142	11	394	53241	11
245	24153	11	295	42135	4	345	21453	2	395	12435	3
246	53421	3	296	35241	10	346	53124	4	396	35214	5
247	41235	2	297	21453	2	347	14235	11	397	24153	11
248	34512	1	298	52314	8	348	31542	7	398	52341	12
249	21453	2	299	41235	2	349	24153	11	399	14235	11
250	54321	1	300	32541	8	350	51324	7	400	32514	12

SECRET

Bell Telephone Laboratories, Inc.

SECRET
ES-842434
4 pages, page 3
A.D.F. 6-29-45

OUTPUT PERMUTATIONS AND FAMILY NUMBERS OF AUTOMATIC CODE CHANGING UNIT FOR 625 STEPS OF SELECTORS
Input and Output Cords in Normal (12345) Positions

Step No.	Permu-tation	Fam. No.	Step No.	Permi-tation	Fam. No.	Step No.	Permu-tation	Fam. No.	Step No.	Permu-tation	Fam. No.
401	13542	4	451	25431	6	501	14532	2	551	35421	4
402	25134	9	452	14253	10	502	25143	12	552	14352	5
403	34521	6	453	53412	5	503	43521	5	553	52413	10
404	45213	6	454	34125	5	504	35214	5	554	24135	10
405	54123	2	455	43215	1	505	53124	4	555	42315	7
406	13245	7	456	25134	9	506	14235	11	556	35124	3
407	31524	9	457	52413	10	507	41523	12	557	53412	5
408	24135	10	458	13254	8	508	23145	8	558	12354	2
409	52314	8	459	41523	12	509	52413	10	559	41532	11
410	53241	11	460	45132	7	510	54231	7	560	45123	1
411	41523	12	461	32415	11	511	31524	9	561	23415	12
412	54132	8	462	43251	12	512	53142	10	562	42351	11
413	42315	7	463	31524	9	513	32415	11	563	21534	3
414	43251	12	464	35142	11	514	34251	9	564	25143	12
415	21543	1	465	12435	3	515	21534	3	565	13425	9
416	34152	12	466	53241	11	516	43152	9	566	52341	12
417	12345	1	467	21534	3	517	12435	3	567	31524	9
418	43521	5	468	35412	2	518	34521	6	568	25413	8
419	21453	2	469	12345	1	519	21354	4	569	13245	7
420	34512	1	470	53421	3	520	43512	3	570	52431	9
421	12435	3	471	21354	4	521	12345	1	571	31254	6
422	45321	2	472	34512	1	522	35421	4	572	24513	7
423	24153	11	473	13245	7	523	23154	7	573	12345	1
424	35412	2	474	54321	1	524	45312	4	574	54231	7
425	14235	11	475	23154	7	525	13245	7	575	32154	1
426	52314	8	476	41325	8	526	53214	2	576	41235	2
427	43521	5	477	53412	5	527	42531	10	577	52413	10
428	21345	6	478	12354	2	528	31245	4	578	13254	8
429	13452	6	479	23541	2	529	12453	4	579	32541	8
430	31542	7	480	32451	7	530	21543	1	580	23451	1
431	52413	10	481	41523	12	531	53412	5	581	41532	11
432	25341	5	482	14352	5	532	35241	10	582	14253	10
433	41523	12	483	52413	10	533	41532	11	583	53412	5
434	34251	9	484	35142	11	534	24351	3	584	25143	12
435	32415	11	485	31524	9	535	23415	12	585	21534	3
436	15342	3	486	24351	3	536	15243	9	586	34251	9
437	31524	9	487	32415	11	537	21534	3	587	23415	12
438	14253	10	488	25143	12	538	14352	5	588	35142	11
439	12435	3	489	21534	3	539	13425	9	589	31524	9
440	45312	4	490	54321	1	540	45213	6	590	54231	7
441	21534	3	491	12435	3	541	31524	9	591	13425	9
442	54213	4	492	45123	1	542	54312	6	592	45132	7
443	12345	1	493	21354	4	543	13245	7	593	31254	6
444	45132	7	494	54231	7	544	45123	1	594	54321	1
445	21354	4	495	12345	1	545	31254	6	595	13245	7
446	54123	2	496	45213	6	546	54132	8	596	45312	4
447	13245	7	497	23154	7	547	12345	1	597	32154	1
448	41532	11	498	52431	9	548	41523	12	598	53421	3
449	23154	7	499	13245	7	549	32154	1	599	12345	1
450	51425	11	500	42513	9	550	51432	12	600	43512	3

SECRET

Bell Telephone Laboratories, Inc.

SECRET
ES-842434
4 pages, page 4
A.D.F. 6-29-45

OUTPUT PERMUTATIONS AND FAMILY NUMBERS OF AUTOMATIC
CODE CHANGING UNIT FOR 625 STEPS OF SELECTORS
Input and Output Cords in Normal (12345) Positions

Step No.	Permutation	Fam. No.
601	14523	8
602	35142	11
603	42531	10
604	25314	10
605	52134	6
606	14325	12
607	41532	11
608	32145	2
609	53412	5
610	54321	1
611	21534	3
612	52143	5
613	23415	12
614	24351	3
615	31524	9
616	42153	3
617	13425	9
618	24531	4
619	31254	6
620	42513	9
621	13245	7
622	25431	6
623	32154	1
624	45213	6
625	12345	1

SECRET

ES-842425
A.D.F. 6-15-45

MATRIX OF FAMILY NOS.

SELECTOR INPUT PERMUTATION: 1 2 3 4 5, FAMILY NO. 1
SELECTOR OUTPUT PERMUTATION: 1 2 3 4 5, FAMILY NO. 1

SLOW SELECTOR STEPS

FAST SELECTOR STEPS

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
1	1	9	7	6	3	6	4	6	9	5	10	5	3	10	5	10	4	8	8	8	2	2	4	2	8
2	4	1	3	7	10	3	1	3	5	9	12	9	6	6	8	6	9	5	10	5	12	10	5	10	11
3	3	6	1	1	5	4	3	9	3	10	9	3	9	5	6	4	6	6	5	2	5	4	10	8	10
4	3	6	1	1	5	4	3	9	3	10	9	3	9	5	6	4	6	6	5	2	5	4	10	8	10
5	12	10	8	5	1	8	10	8	7	2	4	2	11	11	3	11	2	7	1	7	4	1	7	1	6
6	6	12	11	4	4	1	2	5	12	12	8	6	1	8	12	9	7	10	9	12	11	5	3	11	12
7	4	1	3	7	10	3	1	3	5	9	12	9	6	6	8	6	9	5	10	5	12	10	5	10	11
8	2	3	9	8	11	5	6	1	6	6	5	12	5	9	10	8	10	12	8	10	8	11	2	5	2
9	5	5	12	2	2	2	5	12	1	8	8	1	12	12	9	7	8	9	12	11	10	3	11	12	5
10	8	11	10	10	7	12	8	2	8	1	2	8	2	7	11	12	11	11	7	9	7	12	1	3	1
11	10	2	5	11	8	11	12	11	2	7	1	7	8	1	7	1	12	3	11	3	9	9	12	9	3
12	5	5	12	2	2	2	5	12	1	8	6	1	12	12	9	7	8	9	12	11	10	3	11	12	5
13	6	12	11	4	4	1	2	5	12	12	6	6	1	8	12	9	7	10	9	12	11	5	3	11	12
14	10	2	5	11	8	11	12	11	2	7	1	7	8	1	7	1	12	3	11	3	9	9	12	9	3
15	9	8	2	3	6	7	11	10	11	11	7	4	7	2	1	3	1	4	3	1	3	6	9	7	9
16	10	2	5	11	8	11	12	11	2	7	1	7	8	1	7	1	12	3	11	3	9	9	12	9	3
17	9	8	2	3	6	7	11	10	11	11	7	4	7	2	1	3	1	4	3	1	3	6	9	7	9
18	11	4	6	12	12	10	9	7	4	4	3	11	10	3	4	2	5	1	2	4	6	7	8	6	4
19	12	10	8	5	1	8	10	8	7	2	4	2	11	11	3	11	2	7	1	7	4	1	7	1	6
20	9	8	2	3	6	7	11	10	11	11	7	4	7	2	1	3	1	4	3	1	3	6	9	7	9
21	7	7	4	9	9	9	7	4	10	3	11	10	4	4	2	5	3	2	4	6	1	3	6	4	7
22	12	10	8	5	1	8	10	8	7	2	4	2	11	11	3	11	2	7	1	7	4	1	7	1	6
23	8	11	10	10	7	12	8	2	8	1	2	8	2	7	11	12	11	11	7	9	7	12	1	3	1
24	12	10	8	5	1	8	10	8	7	2	4	2	11	11	3	11	2	7	1	7	4	1	7	1	6
25	8	11	10	10	7	12	8	2	8	1	2	8	2	7	11	2	11	11	7	9	7	2	1	3	1

SECRET

CH.		TITLE MATRIX OF FAMILY NUMBERS
DR. H.C.W.	ENG. A.D.F.	SCALE
APPL.		BELL TELEPHONE LABORATORIES, INC., NEW YORK
		NO. OF SHEETS PER SET SEE SHEET 1
		ES-842425 SHEET

ISSUE

Report No. 5

PROJECT 13-106

RELATED SERVICE PROJECT NS-349

REPORT NO. 5

Proposals of Dr. L. E. Gabrilovitch for Speech Privacy Systems

Table cf Contents

PROJECT 13-106

RELATED SERVICE PROJECT NS-349

REPORT NO. 5

Proposals of Dr. L. E. Gabrilovitch for Speech Privacy Systems

June 30, 1945

1. General

1.1 Introduction

Two proposals for speech privacy systems, submitted to the U. S. Navy Department by Dr. L. E. Gabrilovitch, were referred to Bell Telephone Laboratories, Inc., for review under Project 13-106. This work was authorized by a letter, dated January 18, 1945, from Professor C. F. Dalziel, Technical Aide, Division 13, N.D.R.C.

These proposals were the outgrowth of earlier ones made by Dr. Gabrilovitch and discussed informally with Navy and Bell Telephone Laboratories personnel in connection with Project C-43. For convenience in referring to these two proposals, they will be designated as Proposals No. 1 and No. 2. The former is described as a "Screen Secrecy Set with Narrow Audio Band" and the latter as a "Phase Varied Inverter-Distorter (Simplified Secrecy Set)".

1.2 Summary

Both proposals offered, at most, no more than a speculative hope of providing a basis for a satisfactory privacy system. Proposal No. 1, for the reasons given in Section 2.1, was not recommended. Proposal No. 2 was selected for further study on a breadboard basis. Some preliminary engineering work done by Halstead Traffic Communications Corporation, New York, New York, indicated that serious practical difficulties were encountered. Subsequently, further work on these proposals was abandoned.

2. Analysis

2.1 Analysis of Proposal No. 1

This proposal, described as a "Screen Secrecy Set with Narrow Audio Band", employs a well-known principle in the theory of modulation. This principle may be briefly described as follows:

Two distinct signal waves, when modulated on carriers having identical frequencies but different phases (sometimes called a split-phase carrier), can be detected separately by demodulating carriers having exactly the same frequency as the original carriers but phased so as to be in quadrature with the carriers of the undesired modulations. For example, if the two signal waves are $S_1(t)$ and $S_2(t)$, the sum of the modulation products resulting from modulating $S_1(t)$ on a carrier wave*, $\cos \omega t$, and $S_2(t)$ on the same carrier frequency shifted in phase by 90 degrees is

$$S_1(t) \cos \omega t + S_2(t) \sin \omega t. \tag{1}$$

In the wave represented by (1), the component frequencies of $S_1(t)$ and $S_2(t)$ appear as double sidebands about the suppressed carrier frequency. If $S_1(t)$ and $S_2(t)$ contain components within the same frequency range, the sidebands from the two modulated signals will overlap, and any attempt to detect the wave (1) by the usual methods of rectification will result in distortion and severe crosstalk of the two signals. On the other hand, demodulation of (1) by $\cos \omega t$ yields $S_1(t)$, and demodulation by $\sin \omega t$ yields $S_2(t)$.

The use of the above principle was proposed by Dr. Gabrilovitch to obtain screening, or masking, of the speech band in two successive steps:

a. Of the original speech band, extending from 300 to 2700 cycles per second, the lower third is selected and translated to the 0 to 800-cycle region of the spectrum. This comprises a signal such as $S_1(t)$.

- -

[*] Assumed to have a frequency greater than any component in $S_1(t)$ or $S_2(t)$.

A second signal, $S_2(t)$, is masking noise derived from $S_1(t)$ by modulating it with a plurality of low-frequency carriers (fundamental of 50 cycles per second) and confining the resulting modulation products to the 0 to 800-cycle band. The two signals, $S_1(t)$ and $S_2(t)$, are then modulated on 800-cycle carriers in phase quadrature to produce overlapping sidebands in the 0 to 1600-cycle band. The resulting signal, $S_3(t)$, consists of part of the original speech band modulated on an 800-cycle carrier and masked by a noise generated from itself.

b. The upper two-thirds of the speech band, not used in Item (a), is translated to the 0 to 1600-cycle position in the spectrum and comprises signal $S_4(t)$. The two signals, $S_3(t)$ and $S_4(t)$, are then modulated on 1600-cycle carriers in phase quadrature to produce overlapping sidebands in the 0 to 3200-cycle band.

In the last modulation process, arrangements are made for periodically interchanging the 1600-cycle carriers on which $S_3(t)$ and $S_4(t)$ are modulated. This interchange is under the control of an electronic switch, the rate of change of which is integrally related to the 50-cycle fundamental.

This proposal, although theoretically sound, does not appear practicable for the following reasons:

1. It requires a rather large amount of equipment (seven or eight modulators, as many low-pass or band-pass filters, an electronic switch, and other auxiliary electronic devices).

2. The coding possibilities appear to be limited. Hence, with a duplicate receiver it would not be difficult to crack (decode) the scrambled, or masked, speech.

3. For adequate masking, the masking energy must be greater than the signal to be obscured. Hence, for a given amount of output power the range for satisfactory operation is less for systems employing the masking principle thanfor other systems.

4. The overall speech quality of this system would probably be considerably impaired by background noise resulting from imperfect detection when phase distortion in the transmission medium is encountered. Small errors in balancing out the rather large noise components would leave a relatively large residuum of noise.

2.2 Analysis of Proposal No. 2

This proposal, described as a "Phase Varied Inverter-Distorter (Simplified Secrecy Set)", employs as its basic principle the production of an unintelligible scramble of speech by modulating the original speech signal with a fairly complicated coding wave, the spectrum of which lies within the speech band. This basic principle was employed in the RCA-Bedford privacy system* developed to the stage of laboratory models several years ago under Project C-54.

Dr. Gabrilovitch, in his proposal, uses a coding (or modulating) wave comprising two different waves used alternately under the control of an electronic switch, the rate of change of which is predetermined as part of the coding arrangement. Each of the two waves comprises a 50-cycle fundamental and its first seven odd harmonics (a cosine series), all of equal amplitudes. The two waves differ only in the phases of the fundamentals from which the harmonics are derived. The phase difference is 90 degrees.

If we take S(t) as the original speech wave, then the scramble resulting from modulating, i.e., multiplying, the speech wave by the coding wave is

$$S(t)\,\frac{\sin 16\,\omega t}{\sin\,(\omega t + \varphi)}$$

where $\omega/2\pi$ is the fundamental frequency (50 cycles per second) and φ is the phase of the fundamental having the values of 0 degrees and 90 degrees periodically.

- -

* See FINAL REPORT ON PROJECT C-43, Part I, Chapter III, Section 8, page 22, and Chapter VI, page 53; also Part II, Preliminary Report No. 18.

4. The overall speech quality of this system would probably be considerably impaired by background noise resulting from imperfect detection when phase distortion in the transmission medium is encountered. Small errors in balancing out the rather large noise components would leave a relatively large residuum of noise.

2.2 Analysis of Proposal No. 2

This proposal, described as a "Phase Varied Inverter-Distorter (Simplified Secrecy Set)", employs as its basic principle the production of an unintelligible scramble of speech by modulating the original speech signal with a fairly complicated coding wave, the spectrum of which lies within the speech band. This basic principle was employed in the RCA-Bedford privacy system* developed to the stage of laboratory models several years ago under Project C-54.

Dr. Gabrilovitch, in his proposal, uses a coding (or modulating) wave comprising two different waves used alternately under the control of an electronic switch, the rate of change of which is predetermined as part of the coding arrangement. Each of the two waves comprises a 50-cycle fundamental and its first seven odd harmonics (a cosine series), all of equal amplitudes. The two waves differ only in the phases of the fundamentals from which the harmonics are derived. The phase difference is 90 degrees.

If we take S(t) as the original speech wave, then the scramble resulting from modulating, i.e., multiplying, the speech wave by the coding wave is

$$S(t)\ \frac{\sin 16\ \omega t}{\sin\ (\omega t + \varphi)}$$

where $\omega/2\pi$ is the fundamental frequency (50 cycles per second) and φ is the phase of the fundamental having the values of 0 degrees and 90 degrees periodically.

---

* See FINAL REPORT ON PROJECT C-43, Part I, Chapter III, Section 8, page 22, and Chapter VI, page 53; also Part II, Preliminary Report No. 18.

The recovery of the original speech in the receiving unit takes place in two steps: First, modulating (multiplying) the scramble by sin $(\omega t + \varphi)$, which yields the original speech modulated by a single frequency (800 cycles per second); and, second, by modulating the result just obtained with a wave comprising an 800-cycle fundamental and its first three odd harmonics (a sine series), all of equal amplitudes. This second modulating wave has the form

$$\frac{1 - \cos 128\,\omega t}{\sin 16\,\omega t}$$

and, when it is multiplied into S(t) sin 16 ωt, there results

$$S(t) - S(t) \cos 128\,\omega t.$$

The second term on the right, being the original signal modulated on a 6400-cycle carrier, can be removed by filtering, leaving the desired original speech signal.

As an extra precaution against direct listening to the scramble, Dr. Gabrilovitch proposes to invert the speech band before the modulation processes take place. This requires the re-inversion of the signal recovered in the receiver.

The synchronization between the transmitter and receiver is accomplished by means of a carrier falling just outside the band required to transmit the scramble. The carrier is amplitude modulated with a low frequency integrally related to the 50-cycle fundamental.

On comparing the above proposal with the RCA-Bedford system, two rather important differences will be noted:

1. The coding wave and the complementary decoding wave are much simpler in form than those of the Bedford system and, theoretically, can be generated with much less equipment.

2. The synchronization is accomplished by a continuous modulated wave rather than by recurring pulses which, in the Bedford system, imposed rather stringent phase requirements on the transmission path.

Because of the above differences it appeared possible that the Gabrilovitch proposal might lead to a smaller and less weighty unit than the Bedford unit and, at the same time, have a somewhat better overall speech quality.

There were, on the other hand, some questions as to the vulnerability of the scramble to non-cryptographic attacks, to the number of parameters which could be varied for coding purposes, and to the practicability of some of the electronic processes which, theoretically, appeared sound.

The first, and probably the most important, of these questions could not be answered positively without making tests on working models, but it appeared probable that the scramble would be unintelligible. The other questions could not be answered without further engineering study and the building of breadboard models.

5. Role of Halstead Traffic Communications Corporation

At the instance of Comdr. A. B. Jones, of the Bureau of Ships, a conference was held at Bell Telephone Laboratories, Inc., on January 16, 1945, to discuss the feasibility of having breadboard models of one of Dr. Gabrilovitch's proposals developed by the Halstead Traffic Communications Corporation of New York. Present at this conference were Dr. Gabrilovitch and representatives of the Navy, N.D.R.C., Halstead Traffic Communications Corporation and Bell Telephone Laboratories. After an analysis of the two proposals was presented, the Navy representatives agreed that Proposal No. 2 had some attractive features and offered more promise of a satisfactory privacy system than Proposal No. 1 with the expenditure of less development effort. Accordingly, Proposal No. 2 was selected for further study and for the development of breadboard models.

In a letter, dated February 8, 1945, to Professor C. F. Dalziel, in reply to his letter of February 5, 1945, there was outlined a suggested program of laboratory work, on a breadboard basis, which should answer several important questions relating to the feasibility of Proposal No. 2.

In anticipation of a contract with N.D.R.C., the Halstead people began a preliminary engineering investigation of the Gabrilovitch proposals, considering only Proposal No. 2 after the conference of January 16, 1945. This work continued for about a month and a half and was then dropped when an agreement in regard to a contract could not be reached. The papers relating to this work (referred to as Halstead's Job No. 51) were turned over to N.D.R.C.

The Halstead papers were submitted by N.D.R.C. for examination under Project 13-106. From these papers it appeared that work had been discontinued before important progress had been made in obtaining the solution of questions raised in the conference of January 16, 1945. There were indications that some fairly serious difficulties had been encountered in attempting to reduce Proposal No. 2 to practice, both from the standpoint of making the system work properly and from that of providing adequate coding parameters.

Although the evidence obtained from the Halstead papers was not conclusive, there were strong indications that much more complicated coding and decoding waves were being found necessary in order to obtain an acceptable degree of freedom in coding. This would be a definite trend toward making the development of Proposal No. 2 duplicate that of the [illegible] system. For this reason, and because the development effort appeared to be much more formidable than was first anticipated, it appeared that there was little to be gained by continuing with the development of the proposal. Accordingly, it was recommended that further work on these proposals be discontinued.

A. E. FOWLER

Bell Telephone Laboratories
463 West Street
New York 14, N. Y.