~~CONFIDENTIAL~~

NSTISSAM TEMPEST/2-91
Date:

COMPROMISING EMANATIONS ANALYSIS HANDBOOK (U)

~~Classified by DIRNSA (National Manager, NSTISS)~~
~~Declassify On: Originating Agency's Determination Required~~

~~CONFIDENTIAL~~

NSTISS
NATIONAL SECURITY
TELECOMMUNICATIONS
AND INFORMATION
SYSTEMS SECURITY

NATIONAL MANAGER

20 December 1991

FOREWORD

1. (U) National Security Telecommunications and Information Systems Security Advisory Memorandum (NSTISSAM) No. 2-91, "Compromising Emanations Analysis Handbook," describes analysis concepts and techniques currently in use. This advisory memorandum supersedes NACSEM No. 5106, "Compromising Emanations Analysis Handbook," dated December 1971.

2. (U) This document contains communications security information. Access by contractor personnel is restricted to U.S. citizens holding final U.S. Government clearances. This document is not releasable to the Defense Technical Information Center per DoD Instruction 5100.38.

3. (U) Representatives of the National Security Telecommunications and Information Systems Security Committee may obtain additional copies of this advisory memorandum from:

Executive Secretariat
National Security Telecommunications and Information
Systems Security Committee
National Security Agency
Ft. George G. Meade, Maryland 20755-6000

4. (U) U.S. Government contractors are to contact their appropriate government agency or Contracting Officer Representative regarding distribution of this document.

(b)(6)

W. O. STUDEMAN
Vice Admiral, U.S. Navy

TABLE OF CONTENTS (U)

CHAPTER 1

INTRODUCTION

Paragraph *Page*

CHAPTER 2

THE FUNDAMENTALS OF TEMPEST ANALYSIS

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

Paragraph *Page*

CHAPTER 3

MATHEMATICS FOR ANALYSIS

CHAPTER 4

PRETEST PLANNING AND ANALYSIS

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

CHAPTER 5

ON SITE ANALYSIS

Paragraph *Page*

CHAPTER 6

IN-DEPTH ANALYSIS

CHAPTER 7

PREPARATION OF ANALYTIC REPORTS

APPENDICES

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

Tables *Page*

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

LIST OF ILLUSTRATIONS (U)(C)

Figure No. *Page*

(b) (1)
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

THIS PAGE IS INTENTIONALLY BLANK

CHAPTER 1

INTRODUCTION

1-1. (U) General.—This document supersedes NACSEM 5106 dated December, 1971. It describes analysis concepts and techniques currently in use.

1-2. (U) Purpose.—This publication brings together the various stratagems, skills, scientific techniques and judgement criteria which constitute the "analysis" of TEMPEST signals. This handbook has two basic purposes:

a. (U) It provides basic guidelines and procedures for performing signal analysis before, during and after TEMPEST tests.

b. (U) It is for use as an aid in conducting TEMPEST analysis training with a view towards increasing the TEMPEST signal analysis capability within the TEMPEST community. This handbook can also be used as a primer for the new analyst-in-training.

1-3. (U) Comments and Recommendations.—Comments and recommendations on this handbook's contents are encouraged. Government organizations should submit their comments to their appropriate department or agency authority. Department or agency authorities may submit their comments to:

Director, National Security Agency
Attention: [redacted]
Fort George G. Meade, Maryland 20755-6000

(b)(3)-P.L. 86-36

Contractors should submit their comments regarding this publication to their cognizant contracting government organization. Industrial firms that have no appropriate government contract may submit their comments directly to the Director, National Security Agency, at the above address. A comment sheet is provided in the back of this document for this purpose. When submitting comments, it is suggested that this form be reproduced or that a similar format be used. Please classify the comment sheet to the appropriate classification after filling it out.

1-4. (U) TEMPEST Analysis.

a. (U) What Is It?—TEMPEST analysis is the art and science of employing mathematical, engineering and other scientific disciplines to determine the information content of signals that are unintentionally radiated, conducted or transmitted, in some manner, from an equipment which processes classified information.

b. (U) What Is Its Objective?—The main objective of TEMPEST analysis is to determine if a detected signal is compromising. Since there are many different types of TEMPEST signals, there is no simple formula for answering this question every time. Each signal must be treated separately. However, guidelines will be provided on how to evaluate many different signal types.

c. (U) When Is It Used?—There are three times during a TEMPEST evaluation when analysis is useful:

(1) before any test to determine the potential vulnerabilities of an equipment,

(2) during and after a test to determine the actual vulnerabilities associated with an equipment and its environment, and

(3) after the test when results can be extrapolated to different environments.

d. (U) What Is The Alternative?—The alternative to analyzing signals for their information content is to consider every signal detected above appropriate TEMPEST limits to be compromising. The result would be the prospect of having to apply "fixes" where no "fixes" are necessary. This is a very expensive alternative — much more expensive than the cost of good analysis. If the TEMPEST test is done properly, careful analysis will identify the cases where a vulnerability really exists and will result in only necessary "fixes".

1-5. (U) The Degrees of TEMPEST Analysis.—There are various degrees of TEMPEST signal analysis. Each degree is based on the skills of the individual performing the test, the instrumentation available at the time of the test and the time constraints in performing the test.

a. (U) Pretest Analysis.—Pretest (predictive) analysis may be applied when test data is nonexistent or minimal. It is used to determine the hypothetical information content of predicted signals. Predictive analysis is characterized by the following description:

Attributes of person performing analysis	Knowledge of the complete operation of the equipment under test (an individual capable of developing a test plan fits this criterion). Ability to properly use 'state-of-the-art' TEMPEST instrumentation. Knowledge of Information and Communication Theory.
Analysis instrumentation required	Access to a computer or data of the type found in Appendix A of this NSTISSAM.
Duration of analysis effort	From a few minutes for systems that have been evaluated in the past to several months for new equipment.
Confidence in results	Can range from low to high depending on the number and validity of the assumptions which must be made.

b. (U) Cursory Analysis.—Cursory analysis is most often used during an on-site TEMPEST test of an equipment which has fairly well known signals. However, it may also be used in a laboratory environment under the same conditions. It will point out the detectable signals that are possibly compromising. Cursory analysis is characterized by the following description:

Attributes of person performing analysis	Skilled in the use of TEMPEST techniques and instrumentation. Knowledge of the complete operation of the equipment under test is useful, but is not required. Knowledge of Mathematics and/or Information Theory is NOT a requirement.
Analysis instrumentation required	Minimal — either an oscilloscope or a raster display and a still camera.
Duration of analysis effort	Limited to visual and/or aural analysis of the signal and is often performed immediately after initial identification of the emanation.
Confidence in results	Can range from low to moderately high. This depends on the type of signal and whether it is a "borderline" case. The confidence should be established qualitatively by the person doing the analysis.

c. (U) In-Depth Analysis.—In-depth analysis may be used when a precise measure of vulnerability associated with a specific signal is desired for defining TEMPEST countermeasures. In-depth analysis is characterized by the following description:

Attributes of person performing analysis	Skilled in the use of TEMPEST analysis techniques. Knowledge of the complete operation of the equipment under test. Knowledge of Probability, Statistics, Information Theory and the ability to implement this using computer programs.
Analysis instrumentation required	Signal acquisition equipment for either on-line or off-line computer analysis. The computer size may vary from a handheld calculator to a mainframe computer.
Duration of analysis effort	Ranges from minutes to weeks.
Confidence in results	High — the results should include a quantitative measure of confidence.

1–6. (U) Contents of This Handbook.—The following is a brief description of each chapter and appendix in this handbook:

a. (U) **Chapter 1** **Introduction.**—This chapter.

b. (U) **Chapter 2** **The Fundamentals of TEMPEST Analysis.**—This chapter describes the entire TEMPEST phenomenon starting with the origin of TEMPEST signal information and the unintentional transmission of this information.

c. (U) **Chapter 3** **Mathematics for Analysis.**—This chapter contains all the fundamental equations necessary for TEMPEST analysis. Examples are presented to clarify the concepts.

d. (U) **Chapter 4** **Pretest Planning and Analysis.**—This chapter describes the planning of TEMPEST analysis. Four steps are discussed that enable testing to be quickly accomplished and more confidence to be attached to the test results.

e. (U) **Chapter 5** **On-Site Analysis.**—This chapter provides guidance for the analysis of TEMPEST signals by individuals performing on-site TEMPEST testing. Recording techniques and data collection procedures for in-depth analysis are also described in this chapter.

f. (U) **Chapter 6** **In-Depth Analysis.**—This chapter describes the procedures used in the statistical analysis of emanations. It contains useful numerical examples of the analysis of specific signals. It also provides guidelines on the recovery of information from TEMPEST signals.

g. (U) **Chapter 7** **Preparation of Analytic Reports.**—This chapter describes the information which should be included in a TEMPEST Analytical Report.

h. (U) **Appendix A** **Tables.**—This appendix contains tables of numerical data and test patterns which are useful for TEMPEST signal analysis.

i. (U) **Appendix B** **Digital Encoding Schemes.**—This appendix describes different encoding schemes used in binary and voice communication channels.

j. (U) **Appendix C** **Supplementary Equipment Requirements.**—This appendix describes various equipments which can be very useful to the TEMPEST signal analyst.

k. (U) **Appendix D** **An Example of an Analysis Report.**—This appendix contains an example of a typical TEMPEST analysis report.

l. (U) **Appendix E** **Glossary.**—This appendix contains TEMPEST analysis terms.

m. (U) **Appendix F** **Sources of TEMPEST Information.**—This appendix contains a bibliography of useful TEMPEST analysis related subjects.

1-7. (U) Uses of the Handbook.—The handbook has three primary uses:
(1) as a learning aid,
(2) as a test and evaluation handbook, and
(3) as a reference.

a. (U) Learning Aid.—Chapters 2 and 3 present the foundations of TEMPEST analysis. They are basically tutorial in nature and can serve to introduce the subject of TEMPEST signal analysis.

b. (U) Test and Evaluation Handbook.—Chapters 4, 5 and 6 are more directly concerned with the application of analysis. They contain useful guidelines for preparing, executing and evaluating tests.

c. (U) Reference.—Appendices A, B, C and, to a certain extent, Chapters 5 and 6, can serve as useful references to be consulted each time an analysis is performed. Chapter 7 and Appendix D should be consulted when analysis reports are written.

1-8. (U) Summary.—The basic information measures presented in this handbook can be applied directly or indirectly to all degrees of analysis. Because of this, several ways of using the measures are developed.

CHAPTER 2

THE FUNDAMENTALS OF TEMPEST ANALYSIS (U)

2-1. (U) **The TEMPEST Model.**—The discussion of the fundamentals of TEMPEST signal analysis will begin with a description of a model of the entire TEMPEST phenomenon. Our model will cover the origin of TEMPEST signal information and the unintentional transmission of this information to the analyst. The TEMPEST channel is somewhat complex but it can be separated into simple parts. Our model will permit this simplification while remaining sufficiently general to cover all the different types of signals that might be encountered.

a. (U) The study of TEMPEST is very similar to the study of communications. In fact, TEMPEST is a communications process. The TEMPEST channel is unintentional. It is not designed to convey information, and as a result, information is usually lost as it moves through a TEMPEST channel. TEMPEST analysis is the art and science of overcoming this loss to recover the information.

b. (U) Figure 2-1 shows an information processing system. The system includes an information source, a message encoder, a channel, and an information consumer. The system could be a secure teletype link, a computer peripheral and CPU, part of a closed circuit television distribution system, etc. This system will be referred to as the primary system.

c. (U) There is also a secondary system shown. This is the TEMPEST system. Information which is intentionally transferred through the primary system can be inadvertently leaked through the secondary system to an unauthorized receiver. This handbook is mainly concerned with the properties of the secondary system. Note that the primary and secondary system share both the information source and the message encoder.

d. (U) Starting at this point, the construction of a model for the secondary system will now be described. Figure 2-2 shows an elaboration of the TEMPEST system model. It includes six parts: (1) the Information Source, (2) the Message Encoder, (3) the TEMPEST Encoder, (4) the Medium, (5) the Detection System, and (6) the Decoder/Analyst. The first two parts are shared with the primary system. The TEMPEST Encoder can change the form of the information considerably. Usually it destroys information. The Decoder/ Analyst is a human, although he may use a sophisticated computer to help him. He tries to use his knowledge of the information source to recover the information that left the source. Each part of the system model will be examined in detail with particular attention to what happens to the message as it passes through the secondary channel.

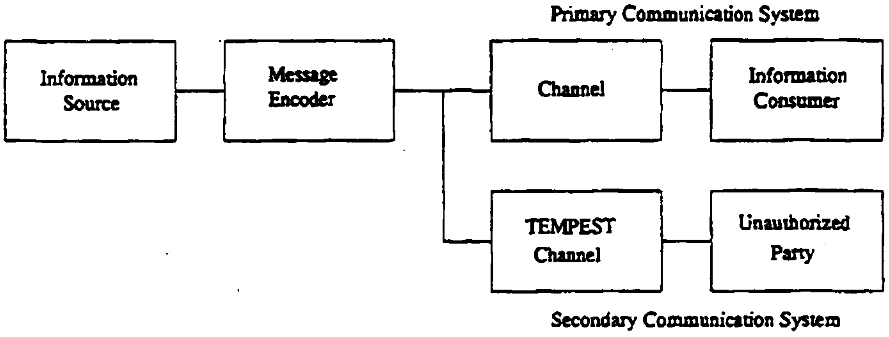


Figure 2-1.—An Information Processing System (U)(U)

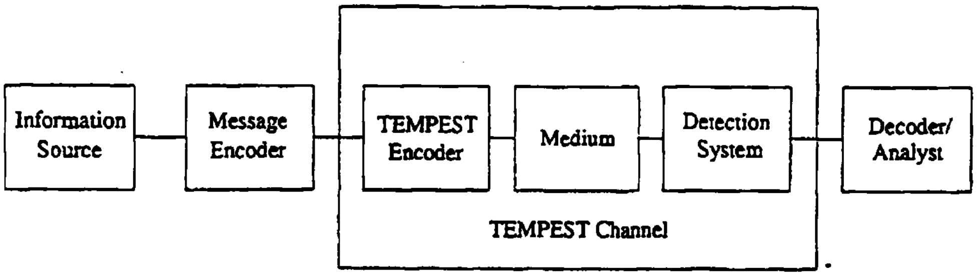


Figure 2-2.—The TEMPEST System Model (U)(U)

2-2. (U) The Information Source.—For purposes of this handbook, the Information Source is a language. From the language, the sender produces a sequence of information units which is called a message. For example, if the primary communication system handles text, then the information units are characters. The primary communication system can be cathode ray tube displays, television, speech, or any other source whose function is to communicate information.

(U) When text is the information source, messages are produced from the language according to spelling rules and the context of the idea which is being represented by the message. These rules result in a situation where each character depends on both previous and subsequent characters. This dependence may exist over several characters.

a. (U) General Properties of Information Sources.—Information sources have important general properties that can now be defined.

(1) *(U) Uncertainty/Entropy.*—The uncertainty or entropy of a text information source is a statistical measure of how uncertain one is (on the average) of each character in messages produced by the source if all previous characters are known (the same concept can be applied to speech). It is normally measured in bits. An information source which can produce many different messages (i.e., has a rich vocabulary) will have a higher uncertainty than a source which can produce fewer messages. A more detailed mathematical discussion of source uncertainty is available in the references listed in Appendix F-3*c*.

(2) *(U) Format.*—An aspect of uncertainty which doesn't depend on the language, but rather on how it is used, is format. This is best explained by an example. Consider the typical business letter heading shown below.

Mr. William A. Jones, Pres.
1151 Wilshire Blvd.
Los Angeles, California

There is no complete sentence in this message and hence there is very little context. However, a knowledge of format alone tells an analyst to look for a name in the first line, an address in the second line, and a city and state in the third line. Military messages are written to follow very strict format rules (e.g., a routing indicator line, a priority line, a classification line, etc.). These rules for message format can simplify analysis considerably when they are exploited.

(3) *(U) Speech.*—Although the acoustic properties of each talker's speech is different, an average characteristic of speech has been determined. When a long time average spectrum of speech is computed over a large number of talkers (including females), the resultant frequency spectrum ranges from approximately 50 Hz to 10 kHz with the greatest energy in the 100 Hz to 600 Hz region (see Figure 2-3). Even if speech is band limited, as in a telephone line where the pass-band is only between 100 Hz and 4 kHz (or in some remote situations 100 Hz to 3 kHz), speech is still intelligible. A study was conducted many years ago where speech was band-pass filtered to have a 1 kHz bandwidth centered about 1.5 kHz and the result was 90% of

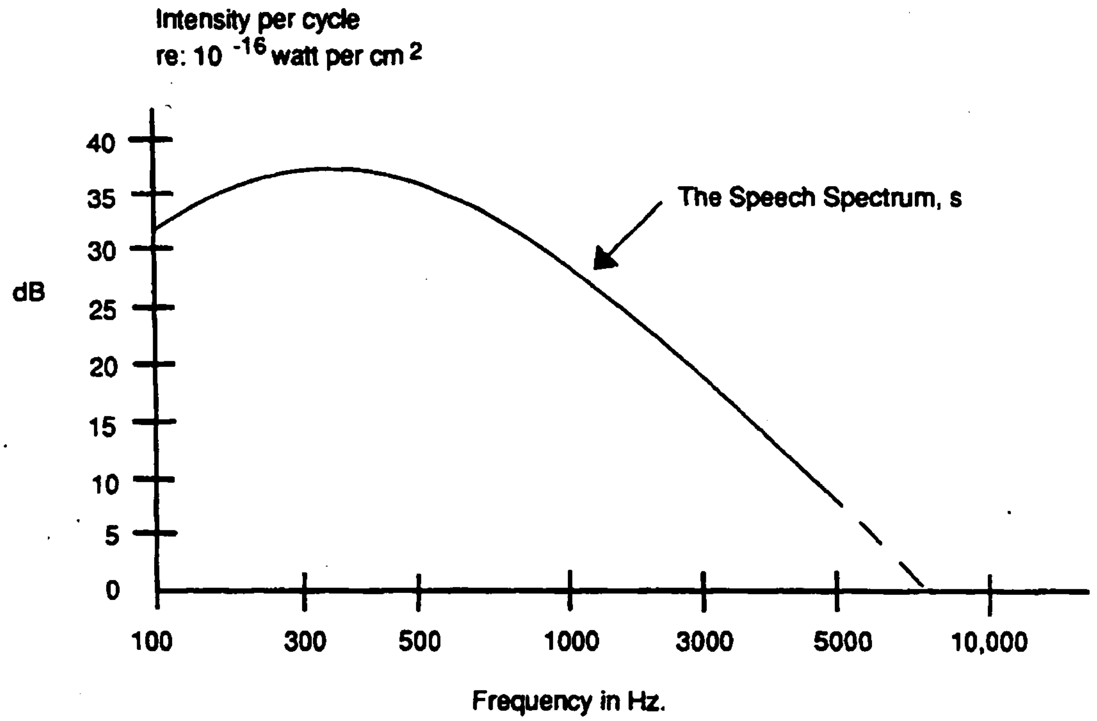


Figure 2-3.—Long Time Average Spectrum of Speech (U)(U)

the sentence was intelligible. From these tests, it is clear that speech is intelligible for very narrow speech bandwidths. However, the speech bandwidth is not the only feature which affects speech intelligibility. Severely clipped speech (or hard-limited speech) is intelligible even though virtually no amplitude information is available provided the zero-crossing information is preserved. Also interrupted speech is intelligible when the interruptions occur greater than 10 per second and the duty cycle of the speech and the interruptions is 100% (i.e., speech half the time and silence the other half). The Journal of the Acoustical Society of America details research performed on this subject.

(U) "Speech intelligibility" is a quantitative measure of how a large number of professional listeners perceive what they hear. Intelligibility is measured using an "articulation test" which is a list of spoken items that can be words, sentences, or individual speech sounds pronounced in meaningless syllables. A test list usually consists of no less than 20 to 25 test items of which several examples of each test item are presented in random order. After hearing the test item, each member of a panel of expert listeners is asked to identify the test item by choosing one of two responses on a test sheet. For our purpose of determining speech intelligibility, sentences are best for testing because context can be derived from the speech without knowing every syllable that was spoken. Any sentences can be used for testing. Appendix A, Table A-9 contains supplementary sentences for testing speech equipment.

b. (U) Types of Information Sources.—If at all possible, the analyst should try to find out what types of information sources will be used with the equipment or system being tested. This has a large impact on how the signals will be analyzed. The following types of language are the ones most commonly encountered in TEMPEST work.

(1) *(U) English Text.*—This includes those messages written in a narrative style, using common text, which follow the rules of spelling and grammar that were learned in school. When an idea has to be

explained in a message, common English is usually the type of language that is used. More is known about the properties of English than any other language since most analysis work has dealt with English text.

(a) (U) The entropy of general English has been found experimentally to be about 1 bit (C. E. Shannon, "Prediction And Entropy Of English Language", Bell System Technical Journal, Jan. 1951, pp 55-62). This subject is explained in more detail when vulnerability measures are discussed (Section 3-4).

(b) (U) Often the use of English becomes very stilted. This happens when clichés come into very common use. Unfortunately, routine government and military messages have this characteristic. The effect is to limit the actual vocabulary of the language. This decreases the entropy considerably. Therefore the information to be protected is more vulnerable if expressed in such a language. The only guideline that can be given to help the analyst select the entropy value to use in cases where a specialized, limited version of the English language is used, is to say: Use the minimum English language entropy value which has been reported by information experiments—1 bit.

(2) *(U) Military Text.*—Often the language seen in military messages doesn't look much like English, even though it is based on the English language. It contains many abbreviations and coined words. However, the military style of writing was designed to be non-ambiguous, provided the reader knows the various terms which are used. (Vast dictionaries of these terms have been compiled.) Actually, military text is just a highly specialized application of English with its own vocabulary. The exact entropy of some particular example of military text is going to vary slightly from location to location and system to system. It is both a difficult and a time consuming task to calculate an exact entropy figure for a particular system. Again the only guideline to help the analyst select the entropy value to use when military text is employed is to say: Use the minimum English language entropy value which has been reported by information experiments—1 bit.

(3) *(U) Alpha-numeric Data.*—Often a system is encountered which processes mixtures of information (i.e., several types of information are contained in the same message). The most common example of this type of message is the kind which consists mostly of tabular data. In these cases, the difficulty of recovery can vary considerably. Often, however, it is possible to determine the format of such a message rather easily. Then the unauthorized analyst can separate the parts with low entropy (i.e., column headings, explanatory footnotes, etc.) and attack only those parts which he thinks will yield the most intelligence. A figure for the entropy of a mixed source cannot be stated because it will vary considerably from case to case. It will almost always be greater than that of common English text. However, to be safe, 1 bit should be used when evaluating signals detected from these sources.

(4) *(U) Pictures.*—Television, either broadcast TV or closed circuit TV (CCTV), is a very popular form of communication. Facsimile has been around for some time but it is a slower means of transmitting pictures. From a TEMPEST standpoint, this is perhaps unfortunate because pictures have undoubtedly the lowest entropy of any information source. Earlier it was stated that uncertainty stems from interdependencies among the symbols of the language (source). In pictures, the symbols are all of those thousands of points of light which constitute a picture. For a picture to mean anything, it must have structure—lines which show shapes. The lines are made up of points so there must be a very high dependence among the intensities of the light points. It is interdependence among the intensities of the light points of a picture which constitute the entropy of the information source for a television/fax system. It is really difficult to put a figure on the entropy of pictures. It must vary considerably among different pictures. It probably is safe to use an entropy of about .70 bits for picture information. (It should be emphasized that this value was decided rather intuitively and should be used with caution.)

(5) *(U) Cathode-ray Tube Displays.*—The type of information displayed on a CRT display can range from simple line drawings through English text to complex pictures. Thus, the entropy can vary considerably. Here again, a safe value of .70 bits should be used for the entropy, unless the information displayed is English text, in which case use 1 bit.

(6) *(U) Speech.*—Speech is another of those extremely complicated information sources of which very little is known. The entropy of speech is lower than that of written English since a person's speaking

(b) (1)
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

vocabulary is much smaller than his written or reading vocabulary which contributes to a lower entropy. Therefore, it is safe to use an entropy of about .70 bits for speech signals.

2-3. ~~(C)~~ The Message Encoder. [redacted]

(U) In this handbook, the definition of a message encoder is somewhat arbitrary. It states that the message encoder converts the most basic information units of the language (e.g., 26 characters and "Space") into mechanical or electrical quantities which a machine can handle.

a. (U) Properties of Message Encoders.—The major property of the message encoder is that it can reduce the overall entropy associated with a message. Consider the twenty-six characters and "Space" which are used to write the English language. If a binary code with four bits per codeword is used, it can encode only sixteen characters. Five bits per codeword would permit the encoding of thirty-two characters. (If it were possible to use a variable length codeword, an average codeword length of 4.23 bits would be sufficient to encode English language characters.) Thus, any more than five bits in the codeword means that more information about a character is transmitted than is absolutely necessary to encode the twenty-seven character English alphabet. This particular phenomenon can be of considerable aid in the recovery of messages from TEMPEST signals which have been corrupted by noise.

b. ~~(C)~~ Examples of Message Encoders.

(1) *(U) Binary Codes.*—The most common message encoders encountered in TEMPEST analysis convert the basic symbols of a written language into binary codewords. Certain binary codes have become a standard and can be applied to many different equipments. Tables A-1 through A-5 of Appendix A list the most commonly used binary communication codes. Appendix B provides examples of common signaling methods used by different equipments. How text information is encoded using the American Standard Code for Information Interchange is discussed below.

(a) (U) The American Standard Code for Information Interchange (ASCII) is a ten bit code (including two synchronization bits) used most frequently in teletypewriter equipments. It is also the standard code for communication between AUTODIN terminals and between CPU's and computer peripherals. When the code is used serially, each character is represented by a sequence of current ("1's", marks) and non-current ("0's", spaces) time intervals. Each sequence includes seven (7) intelligence bits, which are either in a "1" or "0" condition. The eighth bit is a parity control bit which is used to maintain a constant odd (or even) number of "1" bits within each codeword. It is possible that an equipment may be designed to use the code with no parity bit. Preceding the sequence of intelligence bits is a constant "0" referred to as a **START** or **RELEASE** bit. Following the intelligence portion of the codeword is a constant "1" referred to as a **STOP** or **LATCH** bit. The **START** and **STOP** bits are not used to carry information but rather serve to synchronize the transmitting and receiving equipments. Figure 2-4 illustrates the order and function of the ten bits of the ASCII serial codeword.

(b) (U) In Figure 2-4, notice that bits 1, 2, 4 and 7 are in the "1" condition. This is the sequence representing a "K". Also notice that bit 8, the parity bit, is a "0". By counting the number of "1" bits (there are four excluding the **STOP** bit), there are an even number of bits, therefore the parity bit must be

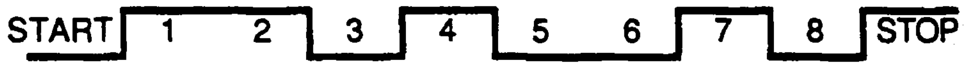


Figure 2-4.—An ASCII Serial Codeword for Character "K" with Even Parity (U)(U)

(b) (1)
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

a "0" to make the sequence contain an even number of "1's". When bit 7 is a "1", it denotes that the sequence represents an alphabetic character, machine function or one of several symbols. When bit 6 is a "1", the sequence represents either a figure, "Space", or one of several symbols.

(c) (U) When ASCII code is used in parallel, the **START** and **STOP** bits are not used and the letter "K" appears as in Figure 2-5.

(2) *(U) Television/Facsimile.*—Television creates a picture by scanning an electron beam horizontally over a phosphor coated surface. As the phosphor is struck by the electron beam, it emits light in an amount proportional to the energy of the beam. After one horizontal scan, the beam is moved downward a fraction of an inch and the whole process is repeated. After an entire picture has been displayed, the beam returns to the top of the picture and traces out the next frame. Such a display is called a raster scan, and it takes place typically 30 to 60 times per second. The electronic component in which this process takes place is called the cathode-ray tube. A reverse process takes place in a vidicon tube in the television camera.

(U) The operation of a facsimile has many similarities with television except that it operates much slower. Also, the electron beam is replaced by a rotating spiral and the picture is created only once.

(3) ~~(C)~~ *Displays.*

(a) ~~(C)~~ [redacted]

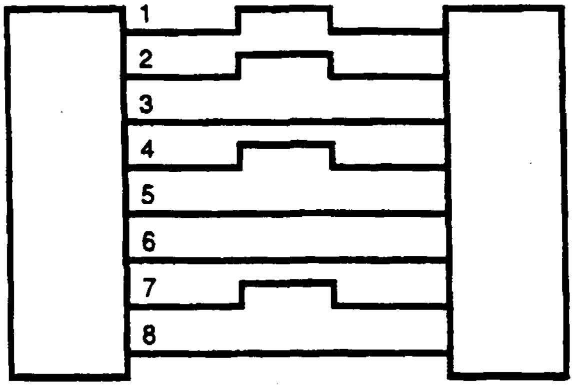


Figure 2-5.—ASCII Parallel Codeword for the Character "K" with Even Parity (U)(U)

(b) (1)
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

(U) Suppose, for example, that a black and white picture (no gray scale) is displayed which has the character "B" located somewhere in the display. The scan is shown in Figure 2-6a. What would actually be seen on the CRT display, if it were examined closely, would be a set of bright dots which are the parts of the scan where the character "B" has a line, as illustrated in Figure 2-6b.

(U) When a CRT display picture is transmitted, the signal can be a binary serial waveform whose amplitude corresponds to the dots on the scan lines. Remember that the electron beam scans all the way across the picture horizontally before returning for another horizontal line. Thus, if the signal for the "B" is studied, the second line would not be seen until all of the first line had been sent. If there is something more in the picture to the right of the "B", parts of it would appear in the serial signal before the rest of the "B". The serial signal might look like Figure 2-6c. If the system uses an interlaced display, the frame consists of two fields. The first field displays all odd-numbered lines followed by a second field which displays the even-numbered lines. The frame is repeated 30 times a second with the field rate being 60 Hz.

(U) Note that the signal decreases in amplitude after each line is displayed. This is done for synchronization purposes and to allow the electron beam to move back to the left side of the picture. After one entire picture has been scanned, the amplitude would stay low longer to allow the beam to move to the top left of the screen before beginning a new picture.

(U) How then does all of this relate to a message encoder? For a black and white picture, the encoding process is just like a serial binary encoding process except that the "bits" which describe vertically adjacent parts of the picture are separated in time. If the bandwidth of the television signal is sufficiently wide, the equivalent serial binary code for the picture of a "B" can be written as depicted in Figure 2-6d. The "..." patterns represent intervals which do not contain any information about the "B".

~~(C)~~ [redacted]

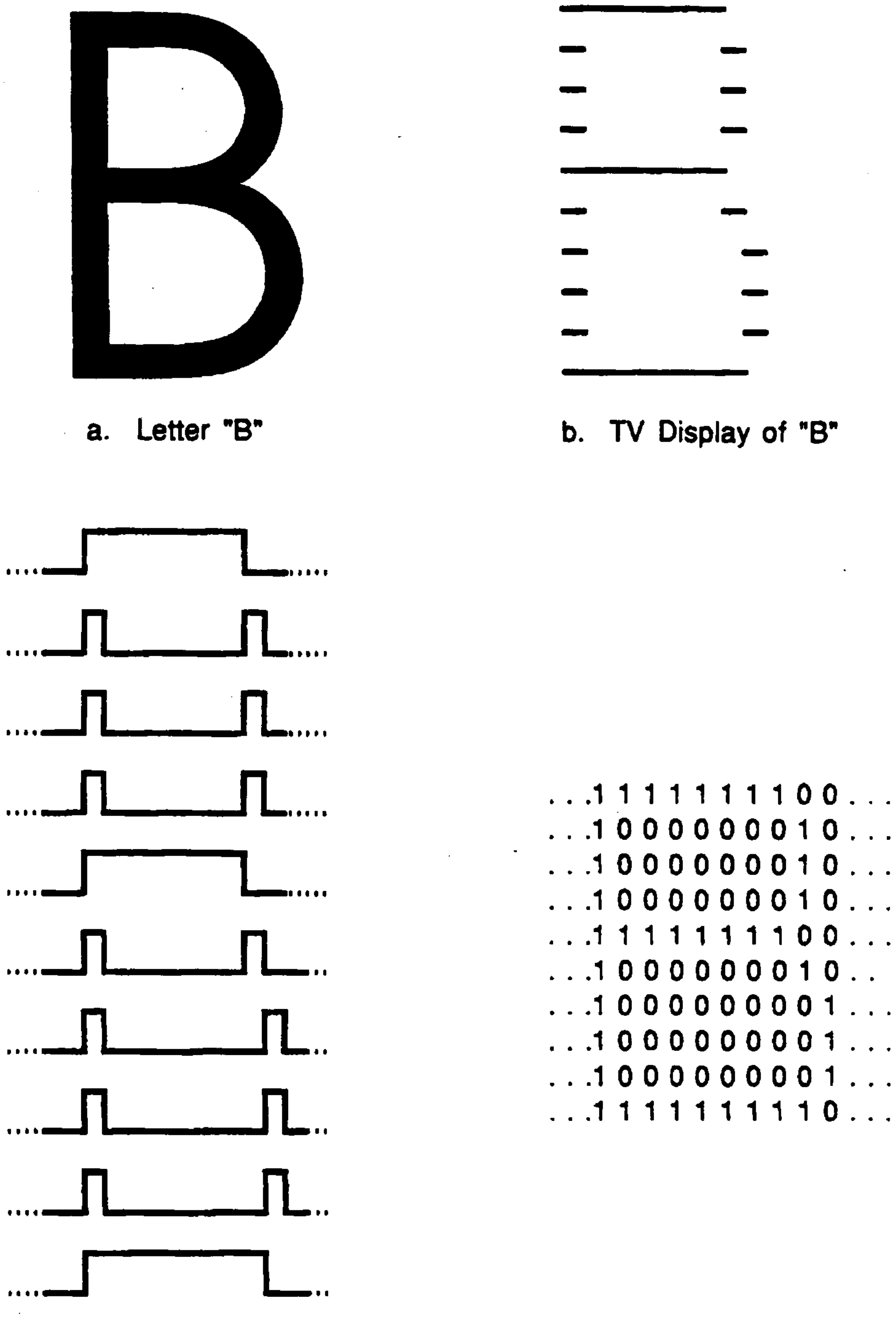
(b) (U) Dot Matrix-Modified Continuous Scan.—This format is also known as a "diddle raster" scan. There are a number of different forms of the "diddle raster" however the following description is common to all.

1. The horizontal sweep is digitally generated, usually from a Digital to Analog Converter (DAC). Digital control is required to allow the trace to pause at each vertical bar while the seven vertical dots are scanned and then jump to the next vertical bar in only one bit period. This allows the dot pattern to be linearly spaced so it can coincide with the video clock signal. The dot pattern is typically 35 dots arranged in a 5 column by 7 row format.

2. The timing diagram is basically the same for each different diddle raster format. Figure 2-7a. presents a diddle raster for a typical 5 by 7 dot matrix. Figures 2-7b. and 2-7c. present the actual timing diagram for an "H" and a "B" respectively.

3. The diddle raster scan is more complex than the conventional vertical raster scan. The diddle raster is not supported by a chip set (i.e., a set of integrated circuits that are designed to perform a specific function). The diddle raster has become almost obsolete except for special function key displays.

4. The diddle raster is difficult to reconstruct from a received TEMPEST signal using available commercial test equipment.



a. Letter "B"

b. TV Display of "B"

```
. . .1 1 1 1 1 1 1 1 0 0 . . .
. . .1 0 0 0 0 0 0 0 1 0 . . .
. . .1 0 0 0 0 0 0 0 1 0 . . .
. . .1 0 0 0 0 0 0 0 1 0 . . .
. . .1 1 1 1 1 1 1 1 0 0 . . .
. . .1 0 0 0 0 0 0 0 1 0 . .
. . .1 0 0 0 0 0 0 0 0 1 . . .
. . .1 0 0 0 0 0 0 0 0 1 . . .
. . .1 0 0 0 0 0 0 0 0 1 . . .
. . .1 1 1 1 1 1 1 1 1 0 . . .
```

c. Serial Unblanking Signal for "B"

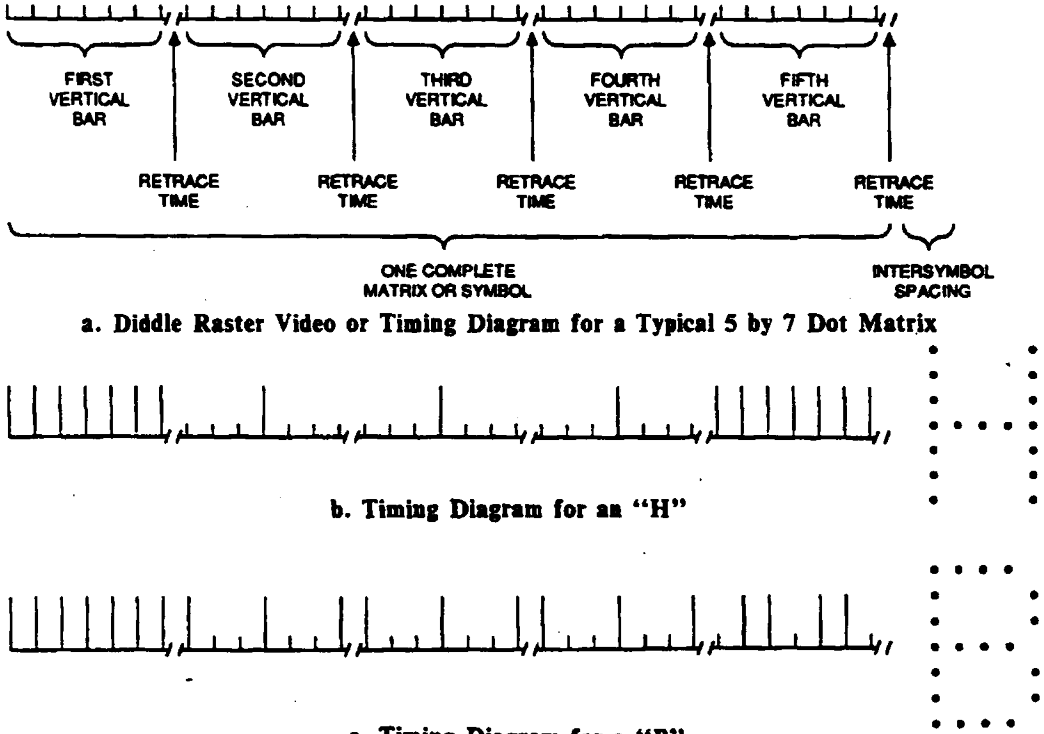
d. Equivalent Binary Code for "B"

Figure 2-6.—Analysis of TV Coding (U)(U)

(b) (1)
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

(c) ~~(C)~~ [redacted]

(4) *(U) Voice Encoding.*—Voice encoding schemes fall into two main classes, entropy encoding schemes and parametric encoding schemes (these are basically analysis/synthesis techniques). Some of the more popular voice encoding schemes include pulse code modulation (PCM), adaptive delta modulation (ADM) (both of these are examples of entropy encoding schemes), linear predictive coding (LPC) and channel



a. Diddle Raster Video or Timing Diagram for a Typical 5 by 7 Dot Matrix

b. Timing Diagram for an "H"

c. Timing Diagram for a "B"

Figure 2-7.—Diddle Raster Format (U)(U)

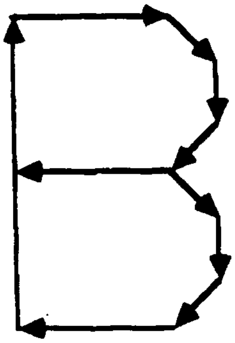


Figure 2-8.—Vector Display of the Character "B" (U)(U)

(b) (1)
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

vocoders (both of these are examples of parametric encoding). A description of these schemes are presented in Appendix B-3.

2-4. ~~(C)~~ [redacted]

~~(C)~~ [redacted]

~~(C)~~ [redacted]

a. ~~(C)~~ [redacted]

Figure 2-9. [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

~~(C)~~

[redacted]

Figure 2-10.

(b) (1)
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

(1) ~~(C)~~ [redacted]

(a) ~~(C)~~ [redacted]

(b) ~~(C)~~ [redacted]

(c) ~~(C)~~ [redacted]

(d) ~~(C)~~ [redacted]

Figure 2-11. [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

(2) ~~(C)~~ [redacted]

(a) ~~(C)~~ [redacted]

Figure 2-12. [redacted]

(b) ~~(C)~~ [redacted]

(c) ~~(C)~~ [redacted]

Figure 2-13. [redacted]

(d) ~~(C)~~ [redacted]

(e) (U) [redacted]

(3) ~~(C)~~ [redacted]

(a) ~~(C)~~ [redacted]

(b) (U) [redacted]

(4) ~~(C)~~ [redacted]

(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

Figure 2-15. [redacted]

b. ~~(C)~~ [redacted]

(1) ~~(C)~~ [redacted]

(a) ~~(C)~~ [redacted]

(b) ~~(C)~~ [redacted]

(2) ~~(C)~~ [redacted]

(a) ~~(C)~~ [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

(b) ~~(C)~~ [redacted]

(c) ~~(C)~~ [redacted]

(d) ~~(C)~~ [redacted]

(3) ~~(C)~~ [redacted]

Figure 2-16. [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

Figure 2-17.

[redacted]

Figure 2-18.

[redacted]

c. ~~(C)~~ [redacted]

d. ~~(C)~~ [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

(1) ~~(C)~~

[redacted]

Figure 2-19

(b) (1)
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

[redacted]

Figure 2-20.-[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

(2) ~~(C)~~ [redacted]

(a) ~~(C)~~ [redacted]

(b) ~~(C)~~ [redacted]

(c) ~~(C)~~ [redacted]

(3) ~~(C)~~ [redacted]

Figure 2-21. [redacted]

Figure 2-22. [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

Figure 2-23.

[redacted]

Figure 2-24.

[redacted]

(4) ~~(C)~~

[redacted]

~~(C)~~

[redacted]

2-5. ~~(C)~~

[redacted]

a. (U) Properties of the Medium.—The medium has four important properties which contribute to the ambiguity: (1) attenuation, (2) noise, (3) bandwidth, and (4) multipath. These properties will now be discussed.

(b) (1)
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

[redacted]

Figure 2-25.

Figure 2-26.

(1) *(U) Attenuation.*—In free space, signal energy travels outward from an emanation source, the signal energy being reduced by a factor of the distance squared. Hence, the signal detectable at any distant point is decreased considerably. This effect is known as attenuation of the signal. However, in conductive materials such as wires or metallic structural material, signal energy is reduced by a factor of the distance. Thus if metallic conductors are present in the vicinity of the emanation, the attenuation of the signal along the conductor may be considerably less than the attenuation in free space.

(2) *(U) Addition of Noise.*—Energy from many non-TEMPEST sources are also present within the medium of a TEMPEST channel. All of this extraneous energy interferes with the TEMPEST signal and must be treated as noise. When either the TEMPEST signal is attenuated or noise is added, the signal-to-noise ratio drops and eventually the information in the TEMPEST signal is completely destroyed. Tables A-1 through A-5 of Appendix A give the signal-to-noise ratios where the information becomes unrecoverable

(b) (1)
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

[redacted]

Figure 2-27.

for some common signal types. Appendix A also contains the statistical definition of the signal-to-noise ratio which is used in the Appendix tables.

(3) *(U) Restriction of Bandwidth.*—The medium can cause ambiguity to be added to the TEMPEST signal by reducing its bandwidth. This is a particular form of attenuation which is not uniform over the frequency spectrum. Fingerprint signals, in particular, can be made very ambiguous by restricting their bandwidth. The signal described in Section 2-4*d*(4) is a typical restricted bandwidth signal.

(4) *(U) Multipath.*—When operating in common free space media, multipaths exist. Multipath occurs when the signal energy arrives at a detection point at different times as a result of traveling different distances by reflection from natural or artificial reflectors. Any reflected signal, when added to the information content of the original signal, reduces the information content. An example of this is a "ghost" on a television set.

b. ~~(C)~~ [redacted]

(1) ~~(C)~~ [redacted]

(2) ~~(C)~~ [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

(3) ~~(C)~~ [redacted]

(4) ~~(C)~~ [redacted]

(5) ~~(C)~~ [redacted]

c. ~~(C)~~ [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

(1) *(U) Serial Binary Signals.*—Attenuation of the signal and addition of noise both have the effect of decreasing the signal-to-noise ratio. At low signal-to-noise ratios (typically less than 8 dB), the medium causes some errors in the detectable signal. This phenomenon is represented in the medium diagram shown in Figure 2-28.

~~(C)~~ [redacted]

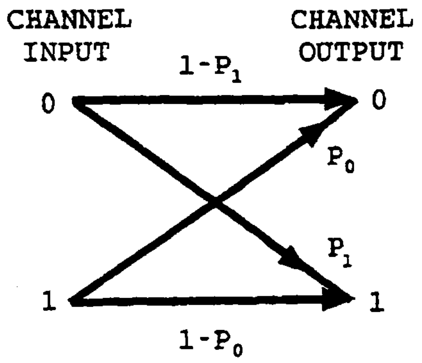


Figure 2-28.—Diagram of a Noisy Binary Channel (U)(U)

~~(C)~~ [redacted]

~~(C)~~ [redacted]

(2) ~~(C)~~ [redacted]

~~(C)~~ [redacted]

(3) ~~(C)~~ [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

Figure 2-29. [redacted]

Figure 2-30. [redacted]

~~(C)~~ [redacted]

2-6. (U) The Detection System.—Any analysis of a TEMPEST channel is not complete without consideration of the detection system. The equipment used to test the EUT actually becomes part of the channel since the detected signals are evaluated at the output of this equipment. Information theory indicates that the detection system cannot increase the amount of information in a signal, but it certainly can decrease it. Care should be taken to minimize the loss in the detection system when collecting signals for analysis.

a. (U) Components of Detection Systems.—The detection system is different for every situation. One possible system is shown in Figure 2-31. Some of the components of a detection system and their effects on information will now be described.

(1) *(U) Signal Detector.*—For the purposes of this handbook, "detector" will be an inclusive term. It includes the transducer and may also include amplifiers, frequency translators, filters, rectifiers, etc. All of these can increase the ambiguity of the signal.

(2) *(U) Signal Recorders and Reproducers.*—Included here are magnetic tape recorders, magnetic disc recorders, transient digital recorders, "smart scopes" and visual display equipment like oscilloscope cameras and oscillograph machines. See Appendix C for more information about signal display equipment.

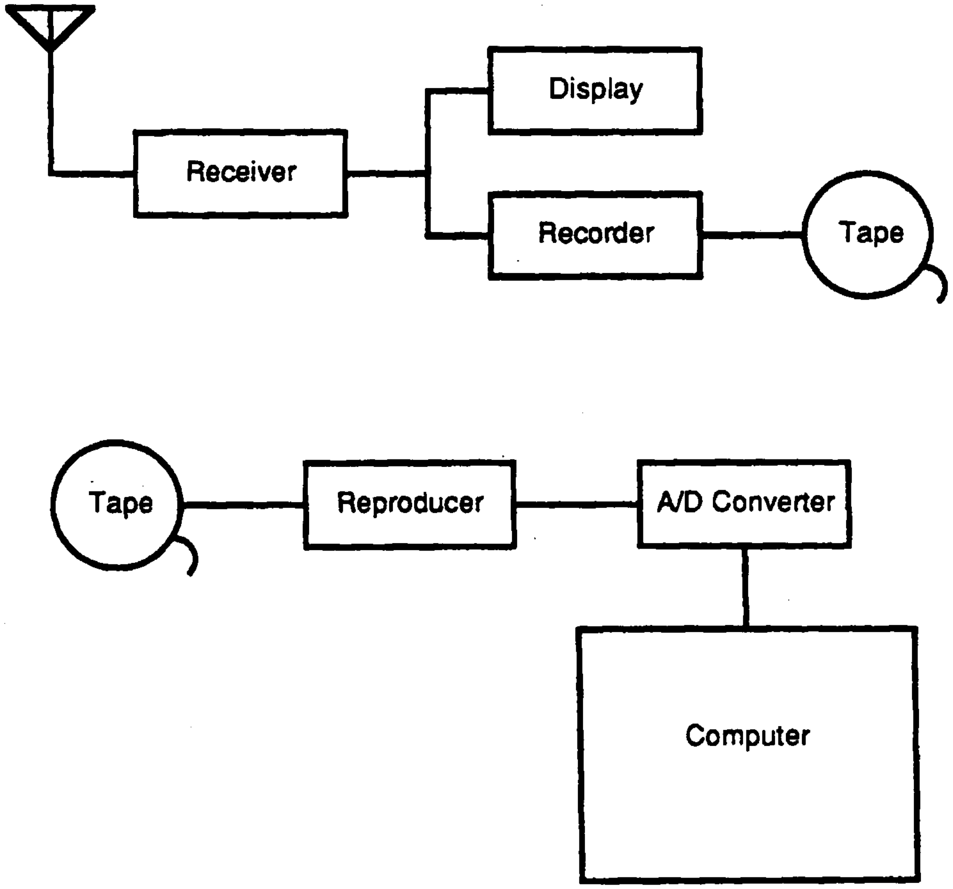


Figure 2-31.—Typical TEMPEST Detection System (U)(U)

(U) Recorders can also add noise, attenuate the signal and restrict bandwidth. Several non-linear operations take place in magnetic recording systems. Each of these destroys phase information. The wow and flutter of any mechanical recording system can severely warp the time base of signals. For some types of signals (bit density), this is not serious, but for others (fingerprint), it can be devastating.

(3) *(U) Signal Displays.*—Most common signal displays cause relatively little information loss. The only ones that cause much problem are the "hard copy" displays such as oscillographs. These have a very limited bandwidth.

(4) *(U) Analog-to-Digital Converters.*—Appendix C-14*a*(2) describes in detail the operation of A/D converters. The quantizing process destroys information by truncating signal values. The amount of information loss caused by this quantization process depends on the amplitude and frequency of the specific signal being converted related to the sampling rate, the number of bits of resolution to quantize the amplitude, and the acquisition time of the converter.

2-7. (U) The TEMPEST Decoder.—Finally, the process of decoding the TEMPEST signal, to produce the original message must be considered. This has been a human operation in the past and will probably continue to be a human operation for some time into the future. Computers and other tools can help in processing and analyzing the TEMPEST signal, but the bottom line is still the capabilities and skill of the human. How human analysts work is difficult to describe using specifications or flow diagrams. They are, moreover, extremely variable. That is, they do not possess uniform skills. One analyst may be able to recover a message rather readily, while another analyst may not succeed. This can lead to widely conflicting results from tests on identical TEMPEST channels.

(U) In order to bypass the subjective effects of the human analyst, measures of the degree of compromise exhibited by common signals have been developed. Three of these measures are the Information Ratio (**IR**), the Generatrix Family Dimension (**GFD**), and the Average Depth of Correct Symbol (**ADCS**). These are described in Chapters 3 and 6 and Section 4-2*b*.

2-8. (U) Summary.—The model of the TEMPEST phenomenon that was described in this chapter fits most test situations. It is intended to serve primarily as a learning aid but is also useful as a point of departure in formulating test plans and extrapolating test results.

THIS PAGE IS INTENTIONALLY BLANK

CHAPTER 3
MATHEMATICS FOR ANALYSIS (U)

3-1. (U) **Introduction.**—TEMPEST analysis can range from a simple evaluation of a trace on an oscilloscope to a more sophisticated evaluation using a large computer. Generally, some intermediate procedure is used. The choice of an analysis procedure depends on three considerations:

a. (U) Confidence in the Results.—The confidence which can be placed on analysis conclusions depends on the degree of in-depth analysis used to arrive at those conclusions. Obviously, if a tester looks at a signal on the scope and says, "I think I could break back the text", one is not as impressed as if he had been handed a recovered message.

b. (U) Cost of Analysis.—Statistically sophisticated analysis, the kind which yields quantitative results, also costs much more than cursory analysis. The cost covers such items as time, equipment and education for the analysts. In many cases, a very expensive analysis can't be afforded.

c. (U) Versatility in the Extrapolation of the Test Results.—The results of a test in one situation may sometimes be used to determine the vulnerability of the same (or similar) equipment in other situations. Any test which receives too little analysis cannot be extrapolated easily to the same (or similar) equipment in other situations without having to make too many assumptions.

~~(C)~~ [redacted]

3-2. (U) **Probability and Statistics.**—Signal analysis is largely a statistical problem and therefore requires some familiarity with probability and statistics on the part of the analyst. This section outlines the minimum background in probability and statistics required.

a. (U) Discretely Distributed Events.—First, two terms need to be defined:

Experiment.—An experiment is a test which has some measurable result. Examples of experiments are tossing a coin, measuring a voltage spike, or observing the time interval between letters printed out by a printer.

Event.—An event is one outcome from a set of all possible outcomes of an experiment. Such an outcome, for example, may be "heads", 2.5 volts, or 26 milliseconds.

(1) *(U) Frequency and Probability.*—Consider an experiment in which a number of events are measured. These events may be a stream of pulses, a set of frequencies, the signal levels of compromising signals, etc. The probability that a given event will occur is the relative frequency that the event occurs out of all possible events. This probability is written as P(A) where A is the event.

$$P(A) = \frac{\text{number of times A occurs}}{\text{total number of events measured}} \tag{3.1}$$

Suppose a set of events are measured, yielding the following samples:

$$\begin{array}{cccccccccc} 18 & 16 & 19 & 17 & 16 & 17 & 17 & 16 & 16 & 16 \\ 16 & 18 & 18 & 17 & 18 & 16 & 16 & 16 & 15 & 16 \end{array} \tag{3.2}$$

The probability of getting a measurement of 16 is estimated as follows:

$$P(16) = \frac{\text{number of times 16 occurred}}{\text{number of samples measured}} = \frac{10}{20} = 0.5 \qquad (3.3)$$

(U) If the probabilities for all detected signals are estimated, one can construct a bar graph called a "histogram". The histogram for the measurements of (3.2) is shown in Figure 3-1.

```
                  x
                  x
                  x
                  x
                  x
                  x
                  x         x         x
                  x         x         x
                  x         x         x
        x         x         x         x         x
14      15        16        17        18        19        20
```

Figure 3-1. — A Histogram (U)(U)

(2) *(U) Probability of Occurrence of a Range of Events.*—Now that the probability that an event occurred has been determined, the probability that a measurement Y is less than or equal to a certain number can be computed. In the case of discrete probabilities, this is known as a *cumulative probability.*

$$P(Y \leq a) = \sum_i P(Y = b_i) \qquad \text{for all } b_i \leq a \qquad (3.4)$$

In the numerical example:

$$\begin{aligned} P(Y \leq 17) &= P(Y = 15) + P(Y = 16) + P(Y = 17) \\ &= 1/20 + 10/20 + 4/20 \\ &= 15/20 = 0.75 \end{aligned} \qquad (3.5)$$

(3) *(U) Joint Probability.*—Now consider two separate experiments. If the outcome of one experiment, X, has no effect on the outcome of the other experiment, Y, then the outcomes of the experiments are said to be *independent*, and the joint probability of X and Y is given by equation (3.6).

$$P(X = a \text{ and } Y = b) = P(X = a) \cdot P(Y = b) \qquad (3.6)$$

(U) For example, if two dice are thrown and a card is picked at random from a deck of cards, the outcomes are independent:

$$\begin{aligned} &P\text{ (dice} = 12 \text{ and} \\ &\quad \text{card} = 10 \text{ of diamonds)} = P\text{ (dice} = 12) \cdot P\text{ (card} = 10 \text{ of diamonds)} \\ &\qquad = P\text{ (dice 1} = 6) \cdot P\text{ (dice 2} = 6) \cdot P\text{ (card} = 10 \text{ of diamonds)} \\ &\qquad = (1/6) \cdot (1/6) \cdot (1/52) \\ &\qquad = 0.00053 \end{aligned} \qquad (3.7)$$

(4) *(U) Conditional Probability.*—The outcome Y of one experiment may depend in some way on the outcome X of another experiment. In such a case, one can speak of a conditional probability $P(Y=a|X=b)$, which is read as "the probability that Y=a, given that X=b". The conditional probability is defined by equation (3.8).

$$P(Y = a|X = b) = \frac{P(Y = a \text{ and } X = b)}{P(X = b)} \qquad (3.8)$$

(U) Given a set of joint outcomes X and Y, the conditional probability $P(Y=a|X=b)$ can be estimated using the relative frequency calculation

$$P(Y = a|X = b) = \frac{\text{number of times that } Y = a \text{ when } X = b}{\text{number of times that } X = b} \tag{3.9}$$

(U) As an example, suppose that the outcomes X,Y from two experiments are observed. Assume that the outcomes X are either 0 or 1 and that the outcomes Y are either 1, 2, or 3. Further assume that the following data is collected:

X: 0 1 1 0 1 0 1 1 0 0 1 0 1 1 1 0 1 1 0 1

Y: 2 3 1 1 2 1 3 1 3 2 2 1 2 3 2 1 1 2 3 3

Given no prior knowledge of the probabilities of the outcomes of either experiment, examples of the probabilities that can be estimated are:

$$P(X = 0) = 8/20 = 0.4$$

$$P(X = 1) = 12/20 = 0.6$$

$$P(Y = 2) = 7/20 = 0.35$$

$$P(Y = 2 \text{ and } X = 0) = 2/20 = 0.1$$

Using (3.8), $P(Y = 2|X = 0) = 0.1/0.4 = 0.25$

or using (3.9), $P(Y = 2|X = 0) = 2/8 = 0.25$

(U) As another example, consider an experiment involving a two character alphabet. Text is composed of two characters "A" and "N". The character X appears in text with the following probabilities:

$$P(X = A) = 0.75 \qquad P(X = N) = 0.25$$

Furthermore, each time the character X is processed, two TEMPEST signals Y_1 and Y_2 are produced.

(U) In the experiment, first the character "A" is processed twenty times. The following values for Y_1 and Y_2 are obtained:

Y_1: 18 16 19 17 16 17 17 16 16 16 16 18 18 17 18 16 16 16 13 16

Y_2: 4 3 4 4 4 4 4 3 2 3 3 4 4 3 4 3 2 3 2 3

(U) For example, $P(Y_1=16|X=A)$ and $P(Y_1=16 \text{ and } X=A)$ can be estimated.

Using (3.9), $P(Y_1 = 16|X = A) = 10/20 = 0.5$

Using (3.8), $P(Y_1 = 16|X = A) = \dfrac{P(Y_1 = 16 \text{ and } X = A)}{P(X = A)}$

Therefore $0.5 = P(Y_1 = 16 \text{ and } X = A) / 0.75$ (3.10)

so that $P(Y_1 = 16 \text{ and } X = A) = (0.5)(0.75) = 0.375$

(U) Note that (3.8) implies that, in general,

$$P(Y = a \text{ and } X = b) = P(Y = a|X = b) \cdot P(X = b) \tag{3.11}$$

(U) Now the character "N" is processed twenty times with the following results:

Y_1: 16 15 15 14 16 15 16 15 14 15 15 15 15 14 15 15 16 15 15 15

Y_2: 12 11 11 10 12 11 12 11 10 11 11 11 11 10 11 11 12 11 11 11

(U) For example, $P(Y_1 = 15 | X = N)$ and $P(Y_1 = 15 \text{ and } X = N)$ can be estimated.

Using (3.9), $P(Y_1 = 15 | X = N) = 13/20 = 0.65$

Using (3.11), $P(Y_1 = 15 \text{ and } X = N) = P(Y_1 = 15 | X = N) \cdot P(X = N)$

$= (0.65)(0.25) = 0.1625$

(U) Conditional probabilities relating channel Y_1 to Y_2 can also be computed. For example,

$$P(Y_1 = 15 | Y_2 = 11 \text{ and } X = N) = \frac{\text{number of times that } Y_1 = 15 \text{ when } Y_2 = 11 \text{ and } X = N}{\text{number of times that } Y_2 = 11 \text{ and } X = N}$$

$$= 13/13 = 1.0 \qquad (3.12)$$

(U) If one would compute $P(Y_1 = y_1 | Y_2 = y_2 \text{ and } X = N)$ for all appropriate values of y_1 and y_2, in each instance the values are either 1.00 or 0.00. Evidently there is a high degree of dependence between Y_1 and Y_2 when $X = N$.

(5) *(U) Bayes' Rule.*—When attempting to recover messages from TEMPEST signals, one is really more interested in a different conditional probability, that being the probabilities of members of the alphabet [X] given the received signals. These can be computed from the conditional probabilities discussed in Section 3-2*a*(4) by the use of Bayes' Rule:

$$P(X = a_i | Y = y_j) = \frac{P(Y = y_j | X = a_i) \cdot P(X = a_i)}{P(Y = y_j)} \qquad (3.13)$$

for all a_i (members of the alphabet) and y_j (signals).

(U) The denominator of (3.13) is a marginal probability and can be computed by:

$$P(Y = y_j) = \sum_{i=1}^{N} P(Y = y_j | X = a_i) \cdot P(X = a_i) \qquad (3.14)$$

(U) The $\sum_{i=1}^{N}$ symbol means that the right side of (3.14) is a sum over all N members of the alphabet. For the sample signals Y_1 in Section 3-2*a*(4),

$$\begin{aligned} P(Y_1 = 16) &= \sum_{i=1}^{2} P(Y_1 = 16 | X = a_i) \cdot P(X = a_i) \\ &= P(Y_1 = 16 | X = A) \cdot P(X = A) + P(Y_1 = 16 | X = N) \cdot P(X = N) \\ &= (0.5)(0.75) + (0.2)(0.25) \\ &= 0.425 \end{aligned} \qquad (3.15)$$

$$P(X = A | Y_1 = 16) = \frac{P(Y_1 = 16 | X = A) \cdot P(X = A)}{P(Y_1 = 16)}$$

$$= \frac{(0.5)(0.75)}{0.425} = 0.882 \qquad (3.16)$$

and similarly $$P(X = N | Y_1 = 16) = \frac{(0.2)(0.25)}{0.425} = 0.118 \qquad (3.17)$$

b. (U) Continuously Distributed Events.

(1) *(U) The Continuous Distribution.*—Many experiments cannot be characterized by discrete events. For example, the instantaneous output of a receiver can be viewed as a continuous random variable. It may assume any value within a particular range. If this range is divided into cells, the output may be quantized into "m" events and treated as in Section 3–2*a*. As both "m" becomes very large and the cell width decreases in size, the histogram becomes a smooth curve as illustrated in Figure 3.2. This curve is called a *probability density function* (pdf).

(2) *(U) The Normal Distribution.*—The type of continuous distribution most often encountered is the *normal (Gaussian) distribution*. The pdf of this distribution is a bell shaped curve which is symmetric about a line drawn from the highest point on the curve to the base line. The center of the distribution is called the *mean* of the distribution and is denoted by the symbol μ. The broadness of the curve is described by the *standard deviation*, σ. The standard deviation of the distribution is defined such that 68.26 percent of the samples are expected to lie within ± one standard deviation of the mean. This is shown in Figure 3–3.

(U) These two parameters, μ and σ, are all that is needed to completely describe a normal distribution. Thus, when measuring signals that are normally distributed, only the μ and σ need to be determined. The equation for the normal pdf is:

$$f(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{\frac{-(x-\mu)^2}{2\sigma^2}} \qquad (3.18)$$

The term σ^2 is called the *variance* of the distribution.

(3) *(U) Probability of Occurrence of a Range of Events.*—When the distribution of signal measurement values is continuous, one can estimate the probability that the measurement lies in the interval $a \leq x \leq b$ by integrating the pdf f(x) over that interval:

$$P(a \leq x \leq b) = \int_a^b f(x)\,dx \qquad (3.19)$$

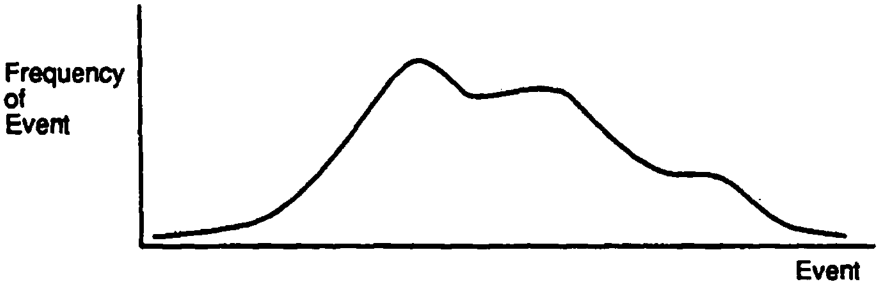


Figure 3-2.—A Probability Density Function (PDF) (U)(U)

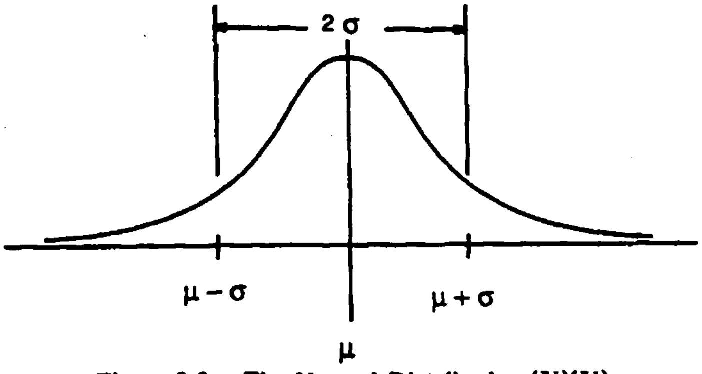


Figure 3-3.—The Normal Distribution (U)(U)

For the normal distribution:

$$P(a \leq x \leq b) = \frac{1}{\sigma\sqrt{2\pi}} \int_a^b e^{\frac{-(x-\mu)^2}{2\sigma^2}} dx \qquad (3.20)$$

This function can be evaluated by the equation

$$P(a \leq x \leq b) = \frac{1}{2} \cdot \text{erf} \left\{ \frac{b-\mu}{\sigma\sqrt{2}} \right\} - \frac{1}{2} \cdot \text{erf} \left\{ \frac{a-\mu}{\sigma\sqrt{2}} \right\} \qquad (3.21)$$

$$\text{where: erf}\,(t) = \frac{2}{\sqrt{\pi}} \int_0^t e^{-x^2} dx \qquad (3.22)$$

Table A-6 in Appendix A contains a table consisting of erf(t), the error function.

(U) Suppose a signal is detected whose mean is 16.7 and whose standard deviation is 1.031. If an A/D converter which truncates signal levels to integer values is used, the probability that a level 16 signal is seen is:

$$P(X = 16) = P(16 \leq x < 17) \overset{*}{=} P(16 \leq x \leq 17)$$

(*true due to the continuous nature of the normal distribution)

$$= \frac{1}{2} \cdot \text{erf} \left[\frac{17-16.7}{1.031\sqrt{2}} \right] - \frac{1}{2} \cdot \text{erf} \left[\frac{16-16.7}{1.031\sqrt{2}} \right] \qquad (3.23)$$

$$= \frac{1}{2} \cdot \text{erf}\,[0.2058] - \frac{1}{2} \cdot \text{erf}\,[-0.4801]$$

$$\text{But, erf}\,(-t) = -\text{erf}\,(t) \qquad (3.24)$$

$$\text{so that,} \quad P(X = 16) = \frac{1}{2} \cdot \text{erf}\,[0.2058] + \frac{1}{2} \cdot \text{erf}\,[0.4801] \qquad (3.25)$$

$$= \frac{1}{2} \cdot [0.2290] + \frac{1}{2} \cdot [0.5028] = 0.3659 \qquad (3.26)$$

(4) *(U) The Central Limit Theorem.*—Now that the normal distribution has been discussed, one might ask: "Why is it so important?". The **Central Limit Theorem** provides the answer to this question. This theorem states that when a large number of samples from distributions that are unrelated to each other are added together, the distribution of the sum will be a normal distribution. The Central Limit Theorem is a powerful mathematical tool because it can be applied to most "real world" signals.

(U) When any signal is emitted, there are many types of noise that get added to the signal before it is received. The noise of the emitter, the noise of the medium through which the signal travels (e.g., the atmosphere, power lines, etc.), and the noise of the receiver are just a few examples. The important thing to remember is that all these types of noise, together with the signal that was originally emitted have distributions that are unrelated to each other. By applying the Central Limit Theorem to the signal and composite noise, the signal actually received will have a normal distribution. Thus, one can assume that any received signal which is made up of an emitted signal and unrelated noises will have a normal distribution. Experience has shown that the assumption is valid.

c. (U) Estimation of Means and Variances.—As stated in Section 3-2*b*(2), the mean and variance completely describe the normal distribution. If the mean and the variance of the TEMPEST emanations can be determined, a complete analysis can be performed. The population mean of a signal set [Y] is the mean which would be computed from all members of [Y]. For example, the signal set [Y] may include all the signals which are emitted when an "A" is processed by an equipment. One would have to test all "A's",perhaps millions of "A's", to determine the population mean. This problem can be avoided by selecting samples of the population and computing its mean. Of course, the result could be in error from the population mean, but if this error is not great, it can be tolerated. Section 3-2c(3)(a) will tell how to estimate what the error might be.

(1) *(U) Estimation of the Mean.*—Any computation of statistics begins with the selection of a sample and the first problem is: "How large should the sample be?". Section 5-5*e*. contains a discussion of sample size selection. For the present, consider the example where 20 sample measurements have been taken:

18 16 19 17 16 17 17 16 16 16
16 18 18 17 18 16 16 16 15 16

The sample mean, m, is the average of these samples:

$$m = \frac{1}{20}\sum_{i=1}^{20} y_i \qquad (3.27)$$

$$\begin{aligned} m &= \frac{1}{20}(18 + 16 + 19 + 17 + 16 + 17 + 17 + 16 + 16 + 16 + 16 + 18 + 18 \\ &\qquad + 17 + 18 + 16 + 16 + 16 + 15 + 16) \\ &= 334/20 \\ &= 16.7 \end{aligned} \qquad (3.28)$$

(2) *(U) Estimation of the Variance.*—The variance of a set of samples is defined by the equation:

$$V = \frac{1}{N-1}\sum_{i=1}^{N}(y_i - m)^2 \qquad (3.29)$$

where: N = sample size, and
m = sample mean

The standard deviation, s, is defined as the (positive) square root of V:

$$s = \sqrt{V} \qquad (3.30)$$

It is common to write (3.29) in the following way:

$$s^2 = \frac{1}{N-1}\sum_{i=1}^{N}(y_i - m)^2 \qquad (3.31)$$

This equation can be manipulated into an easier to use form:

$$s^2 = \frac{1}{N-1}\left[\left(\sum_{i=1}^{N} y_i^2\right) - Nm^2\right] \qquad (3.32)$$

Using the sample values presented in Section 3-2*c*(1):

$$\begin{aligned} s^2 = \frac{1}{19}[&18^2 + 16^2 + 19^2 + 17^2 + 16^2 + 17^2 + 17^2 + 16^2 + 16^2 + 16^2 + 16^2 + 18^2 \\ &+ 18^2 + 17^2 + 18^2 + 16^2 + 16^2 + 16^2 + 15^2 + 16^2 - 20 \cdot (16.7)^2] \end{aligned} \qquad (3.33)$$

$$= \frac{1}{19}[5598 - 5577.8]$$

$$s^2 = 1.063$$

$$s = 1.031 \qquad (3.34)$$

(3) *(U) Confidence Intervals.*—One might be interested in knowing just how accurate the estimations of the mean and standard deviation are. A measure of this accuracy is the confidence interval for both the mean and the standard deviation. The confidence interval about m or s is a range of values which contain the true (population) value of the mean or standard deviation with a selected probability (confidence). It is based on the number of samples of the signal that were used for the estimates, m and s. For practical purposes, consider that one would like the confidence interval of the mean and standard deviation to contain the true values with a probability of 0.95.

(a) (U) Confidence Interval for the Mean.—For samples taken from a normal population, the confidence interval of the mean is the range $m-v$ to $m+v$ where v is given by:

$$v = C_N^a \frac{s}{\sqrt{N}} \tag{3.35}$$

where $C_N^a = C_N^{95}$ depends on the number of samples "N" and the desired confidence "a" of the interval. This coefficient is obtained from Appendix A, Table A-7. For example, the confidence interval for the mean computed in Section 3-2*c*(1) may be computed as follows:

$$m = 16.7, N = 20, s = 1.031$$

$$v = \frac{(2.093)(1.031)}{\sqrt{20}} = \frac{2.158}{4.472} \tag{3.36}$$

$$= 0.48$$

And the confidence interval is:

$$\begin{gathered}(16.7 - 0.48) \text{ to } (16.7 + 0.48)\\ \text{or}\\ 16.22 \text{ to } 17.18\end{gathered} \tag{3.37}$$

Thus, with 95 percent confidence the mean of the population lies in the interval between 16.22 and 17.18.

(b) (U) Confidence Interval for the Standard Deviation.—For samples from a normal population, the confidence interval for the standard deviation is the range $B_L s$ to $B_U s$. B_L and B_U are obtained from Appendix A, Table A-8 for the sample size N. For example, using the sample values presented in Section 3-2*c*(1),

$$N = 20, s = 1.031$$

From Table A-8,

$$B_L = 0.7484, B_U = 1.432, \text{ and}$$

$$s_L = B_L s = (0.7484)(1.031) = 0.772$$

$$s_U = B_U s = (1.432)(1.031) = 1.476 \tag{3.38}$$

(U) Hence, with 95 percent confidence the standard deviation of the population lies in the interval between 0.772 and 1.476.

(U) This concludes the statistical background required for TEMPEST analysis. Analytic applications using these tools will now be developed.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

3-3. ~~(C)~~ [redacted]

a. ~~(C)~~ [redacted]

(1) [redacted]

(2) [redacted]

(3) [redacted]

Figure 3-4. [redacted]

(U) If the inputs are arranged as row headers of the channel matrix and the outputs are arranged as column headers (see example in Section 6-3), then the sum of each row must add to one. This is a good check that the computations are correct.

(U) Each row of the channel matrix is the histogram of the output signal representing the input symbol which heads that row. The attractive property of the channel matrix is that it maintains the "relative disjointedness" of the distributions of these signals. It is this "relative disjointedness" that is analyzed.

(U) As shown in Figure 3-4, an additional row and column is added to the channel matrix. The column contains the probabilities of the inputs $P(X_i)$ and the row contains the probabilities of the outputs $P(Y_j)$ computed by the equation:

$$P(Y_j) = \sum_{i=1}^{27} P(Y_j | X_i) \cdot P(X_i) \qquad (3.39)$$

(U) The use of the channel matrix in TEMPEST channel evaluation will be discussed in Section 3-4*b*.

b. ~~(C)~~ [redacted]

~~(C)~~

(U) As with the channel matrix, there is a simple check on the correctness of the reverse channel matrix. Each column must sum to one.

c. ~~(C)~~ [redacted]

Figure 3-5. [redacted]

(b) (1)
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

[redacted]

(U) [redacted]

~~(C)~~ [redacted]

~~(C)~~ [redacted]

(U) [redacted]

~~(C)~~ [redacted]

~~(C)~~ [redacted]

(U) This may sound like a lot of work and it is. Surprisingly enough, the simplest of TEMPEST signals—serial signals—are the most difficult to analyze statistically. If at all possible, a computer should be used to analyze serial signals.

(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

Figure 3-6.

[redacted]

Figure 3-7.

d. ~~(C)~~ [redacted]

~~(C)~~ [redacted]

(U) The number of cells used can make a difference in the TEMPEST vulnerability as measured in Section 3-4. The more cells used, the more accurate will be the measure, though for more cells the cost of analysis will increase. Criteria to define the cell width to ensure minimum error in the vulnerability measures is presented in Section 6-2.

3-4. ~~(C)~~ [redacted]

a. (U) Uncertainty Definitions.—Before introducing the vulnerability measures, a review of some statistics may be helpful. In addition, some measures of uncertainty will be defined.

(1) (U) *Input Uncertainty.*

$$H(X) = -\sum_{i=1}^{K1} P(X_i) \cdot \log P(X_i) \tag{3.46}$$

where: $H(X)$ = the input source symbol uncertainty.

$K1$ = the number of source input symbols. For a monographic English text source, K1 would be equal to 27 (the 26 alphabetic characters plus the "Space" character). For a digraphic English text source, K1 would be equal to 729 (normally the 300 most probable digraphs in the English language are used since this number does include approximately 95% of the total a priori probability of all possible digraphs).

$P(X_i)$ = the probability of symbol X_i in the source language.

(U) The base of the log determines the units of H(X). When the base is 2, the units of H(X) are bits. When natural logs are used, the units of H(X) are nats. When the base is 10, the units of H(X) are hartleys. These units are related by the following equations:

$$\begin{aligned} 1 \text{ bit} &= 0.3010 \text{ hartleys} \\ 1 \text{ bit} &= 0.6931 \text{ nats} \end{aligned} \tag{3.47}$$

(2) *(U) Output Uncertainty.* H(Y) is the uncertainty of the output signal set.

$$H(Y) = -\sum_{j=1}^{M1} P(Y_j) \cdot \log P(Y_j) \tag{3.48}$$

where: $M1$ = the number of different output signals detected, and

$P(Y_j)$ = the probability of the output signal Y_j.

$$P(Y_j) = \sum_{i=1}^{K1} P(Y_j|X_i) \cdot P(X_i)$$

where: $P(Y_j|X_i)$ = the probability of a specific output signal Y_j given a specific input symbol X_i.

(3) ~~(C)~~ [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

~~(C)~~ [redacted]

b. ~~(C)~~ [redacted]

(U) As stated above, the uncertainty is a measure of how much question there is about whether an event will occur before it occurs and can be observed. This can be applied to the detection and analysis of TEMPEST signals.

~~(C)~~ [redacted]

~~(C)~~ [redacted]

~~(C)~~ [redacted]

~~(C)~~ [redacted]

(1) ~~(C)~~ [redacted]

~~(C)~~ [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

~~(C)~~

~~(C)~~

~~(C)~~

~~(C)~~

~~(C)~~

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

(2) *(U) Interpretation.*—How should the IR be interpreted and used?

~~(C)~~ [redacted]

c. ~~(C)~~ [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

(1) ~~(C)~~ [redacted]

~~(C)~~

~~(C)~~

(2) ~~(C)~~ [redacted]

(b) (1)
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

~~(C)~~ [redacted]

~~(C)~~ [redacted]

d. ~~(C)~~ [redacted]

e. ~~(C)~~ [redacted]

3-5. **(U) Signal Averaging.**—If the same message is processed repeatedly, signal averaging can be used to determine the amount of information in the signal. If, for example, the signal is serial binary and is repeated N times with error probabilities P(1|0)=P(0|1)=Q for i = 1,2,. . .N, these errors can be averaged together to get:

if N is odd,

$$P(1|0) = P(0|1) = 1 - \sum_{i=0}^{\frac{N-1}{2}} \binom{N}{i} Q^i(1-Q)^{N-i} \qquad (3.61)$$

if N is even,

$$P(1|0) = P(0|1) = 1 - \sum_{i=0}^{\left\lceil\frac{N-1}{2}\right\rceil} \binom{N}{i} Q^i(1-Q)^{N-i} + \frac{1}{2}\cdot\binom{N}{N/2} Q^{N/2}(1-Q)^{N/2} \qquad (3.62)$$

where: $\left\lceil\frac{N-1}{2}\right\rceil$ is the smallest integer greater than $\frac{N-1}{2}$, and

$$\binom{N}{i} = \frac{N!}{i!\,(N-i)!} \qquad (3.63)$$

(U) As a numerical example, suppose that a particular serial signal is detected 5 times, with Q=.1. The averaged error probabilities are:

$$\begin{aligned} P(1|0) = P(0|1) &= 1 - \sum_{i=0}^{2} \binom{5}{i} (0.1)^i (0.9)^{5-i} \\ &= 1 - (0.1)^0(0.9)^5 - (5)(0.1)^1(0.9)^4 - (10)(0.1)^2(0.9)^3 \qquad (3.64) \\ &= 1 - 0.590 - 0.328 - 0.0729 \\ &= 0.009 \end{aligned}$$

(U) As you can see, signal averaging can make quite a difference. The error probabilities P(1|0) and P(0|1) drop from Q=0.1 to Q=0.009 by averaging the signal 5 times.

(b) (1)
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

[redacted]

Figure 3-9a.

[redacted]

Figure 3-9b.

[redacted]

Figure 3-9c

3-6. (U) Summary.—This chapter has presented the mathematical building blocks from which TEMPEST analysis can be constructed. For more detail on some areas, see the references cited in Appendix F-3.

CHAPTER 4

PRETEST PLANNING AND ANALYSIS (U)

4-1. (U) Introduction.—The material in this chapter provides guidance for predicting the emanations from an equipment so as to incorporate analysis into the TEMPEST test plan and to extrapolate data from one TEMPEST test to other equipment configurations and environments.

4-2. (U) Pretest Planning and Analysis.—The pretest planning and analysis phase of an equipment TEMPEST evaluation consists of four steps. These four steps are:

(1) identify all TEMPEST encoders (RED Sources) in the TEMPEST test plan prepared in accordance with NSTISSAM TEMPEST/1-91*;

(2) analyze all signals identified in the TEMPEST test plan for maximum information content;

(3) develop and incorporate into the TEMPEST test plan, if needed, new test messages for specific signals so that these signals can be easily identified and analyzed during the TEMPEST test; and,

(4) identify specific equipments required to analyze the detected signals.

When these steps are followed, testing can be accomplished more quickly and more importantly, confidence can be attached to the test results.

a. ~~(C)~~ [redacted]

(1) ~~(C)~~ [redacted]

(2) ~~(C)~~ [redacted]

(3) ~~(C)~~ [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

b. ~~(C)~~ [redacted]

(1) ~~(C)~~ [redacted]

(2) ~~(C)~~ [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

~~(C)~~ [redacted]

(U) [redacted]

(3) ~~(C)~~ [redacted]

c. *(U) Test Message Selection.*—The third step of pretest analysis is test message selection. A good choice of test messages during the planning phase makes analysis much easier and less time consuming. Choose the test message so that the predicted TEMPEST signal will give the analyst all the information needed. The analyst shouldn't have to assume signal properties which could have been measured if the test message had been more appropriate. On the other hand, the test message should not be so complicated that the analyst has to search through a signal to find a particular point of interest. The test message should be short, simple sequences which show the compromising potential of the predicted TEMPEST signal. The test message should consist of symbols used in the normal information processing of that equipment.

(1) ~~(C)~~ [redacted]

(a) (U) Type A Test Messages.

1. ~~(C)~~ [redacted]

(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

2. ~~(C)~~ [redacted]

~~(C)~~ [redacted]

(U) [redacted]

~~(C)~~ [redacted]

(U) [redacted]

~~(C)~~ [redacted]

~~(C)~~ [redacted]

~~(C)~~ [redacted]

(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

(b
(b,
(b)

(U) [redacted]

~~(C)~~ [redacted]

(U) [redacted]

~~(C)~~ [redacted]

~~(C)~~

(b) (U) Type B Test Messages.

1. ~~(C)~~ [redacted]

2. ~~(C)~~ [redacted]

~~(C)~~

3. ~~(C)~~

(U) [redacted]

~~(C)~~ [redacted]

(U) [redacted]

~~(C)~~ [redacted]

(c) ~~(C)~~

(b) (3)-18 USC
(b) (3)-

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

~~(C)~~

~~(C)~~

~~(C)~~

~~(C)~~

(d) ~~(C)~~

(2) ~~(C)~~

~~(C)~~

(a) ~~(C)~~

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

Figure 4-1.[redacted]

[redacted]

Figure 4-2.[redacted]

(b) ~~(C)~~ [redacted]

(c) ~~(S)~~ [redacted]

(d) ~~(C)~~ [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

Figure 4-3. [redacted]

(3) ~~(C)~~ [redacted]

d. ~~(C)~~ [redacted]

4-3. ~~(C)~~ [redacted]

4-4. ~~(C)~~ [redacted]

(b) (1)
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

CHAPTER 5

ON-SITE ANALYSIS (U)

5–1. (U) Introduction.—The material in this chapter is intended to provide guidance for the analysis of TEMPEST signals by individuals performing on-site TEMPEST testing. This chapter describes optimal signal display techniques and also describes how to determine if a particular signal can be evaluated on-site or must be recorded for later in-depth analysis. On-site analysis techniques described include using visual techniques and calculating IR's or ADCS's to determine if signals are compromising. Recording techniques and data collection for in-depth analysis, if it is required, are also described in this chapter.

(U) The best way to do a good on-site analysis is by first doing a good pretest planning and analysis. It should be remembered that many factors must be considered in performing a TEMPEST evaluation, and these factors must be controlled in such a manner that the tester is given a high probability of determining where areas of possible compromise exist. Once the characteristics of the EUT are understood, the equipment can be operated in such a manner to enhance the emanations to be tested. Also, it is critically important that the technical limitations of the analysis instrumentation not be a limiting factor in the quality of the analysis.

5–2. (U) Initial Detection System.—The initial setup of the detection system is very important in detecting signals related to data being processed by the EUT. The initial setup is derived from the TEMPEST test plan which provides the different types of data transfers, data rates and the minimum and maximum required bandwidth for optimum detection. Once the signal has been detected, the detection system should be varied to optimize the signal.

(U) During all tests, it is important for the tester to both observe and listen to the signals and noise being detected. An experienced tester can often obtain valuable information from the sound of the signal that cannot be observed by looking at an oscilloscope display. The human ear can detect small changes in the characteristics of the signal which alert the tester to the possible presence of correlated signals which can be verified by optimizing the detection system.

5–3. ~~(C)~~ [redacted]

a. ~~(C)~~

(1) *(U)* [redacted]

(a) ~~(C)~~ [redacted]

(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

Figure 5-1. [redacted]

~~(C)~~ [redacted]

(b) ~~(C)~~ [redacted]

~~(C)~~ [redacted]

(2) ~~(C)~~ [redacted]

(a) ~~(C)~~ [redacted]

~~(C)~~ [redacted]

~~(C)~~ [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

Figure 5-2.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

(b) ~~(C)~~ [redacted]

(3) *(U) Analysis of Serial Signals.*

(a) ~~(C)~~ [redacted]

(U) Depending on the type of emanation, the optimum oscilloscope presentation may be either raster or A-scope. In some cases, however, cursory analysis of serial data can be made easier by using a raster display. Some of the forms in which compromising emanations may exist are shown in Figure 5-5. The following rules of thumb will provide guidance for the cursory analysis of serial signals.

1. (U) Any change in the signal when the test message (monitor) is changed indicates a potentially compromising signal. Further analysis is required to determine the extent of the threat.

2. ~~(C)~~ [redacted]

3. ~~(C)~~ [redacted]

4. ~~(C)~~ [redacted]

5. ~~(C)~~ [redacted]

Figure 5-3. [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

Figure 5-4.

[redacted]

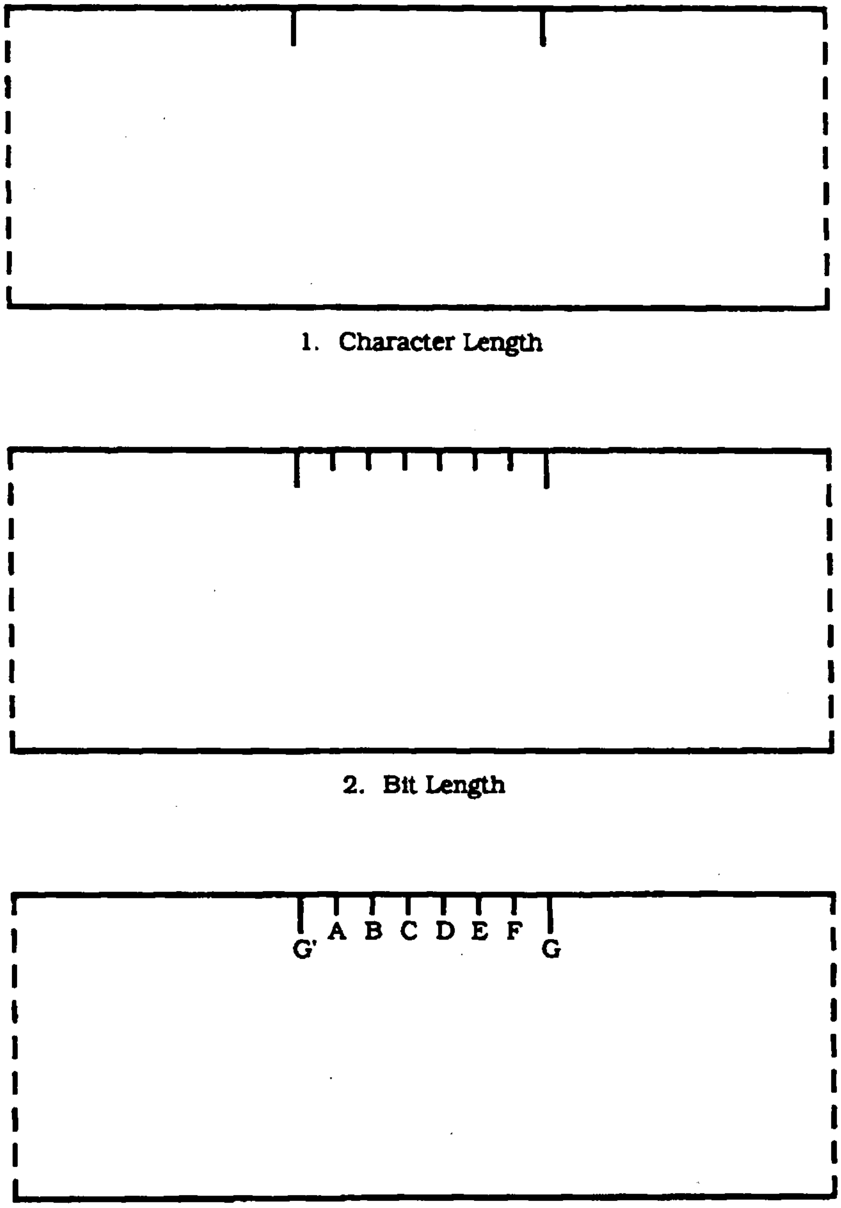
6. ~~(C)~~ [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

Figure 5-5.

(b) (U) Alternate Method of Analysis.—Another way to analyze serial signals is by visual inspection of a hardcopy representation or with an automatic correlator as described in Appendix C-4. When manual analysis is required, first the bit and character lengths must be calculated. Then a baud card may be used to help identify transitions and graphic analysis can be used to obtain character synchronization.



1. Character Length

2. Bit Length

3. Identify Bits and Transitions

Figure 5-6.—Construction of the Baud Card (U)(U)

(b) (1)
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

[redacted]

Figure 5-7.

1. (U) Computation of Bit and Character Length.—To calculate bit and character length, the following data is required:

a) operating speed of the EUT	= O bits/sec,
b) record speed of recorder	= R ips,
c) playback speed of recorder	= P ips,
d) operating speed of oscillograph	= V ips and
e) the code used	= Q bits/character.

Then the bit length is given by

$$B = \frac{(V)(R)}{(O)(P)} \text{ in/bit} \qquad (5.1)$$

and the character length is

$$C = B \cdot Q \text{ in/character} \qquad (5.2)$$

For example, if

O = 75 bits/sec,
R = 15 in/sec,
P = 7.5 in/sec,
V = 10 in/sec and
Q = 7.42 bits/character (i.e., Baudot code with elongated STOP bit),

$$\text{then} \quad B = \frac{(10)(15)}{(75)(7.5)} \qquad (5.3)$$

$$= 0.267 \text{ in/bit}$$

$$\text{and} \quad C = (0.267)(7.42)$$

$$= 2.0 \text{ in/character} \qquad (5.4)$$

2. (U) Baud Card.—The baud card can now be constructed. Simply mark the cycle length C, and the bit length B, on the edge of a 3x5 (or any other suitable) card. Number the bits and letter the transitions as illustrated in Figure 5-6.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

3. ~~(C)~~ [redacted]

a [redacted]

b. [redacted]

c. [redacted]

Figure 5-8. [redacted]

d. [redacted]

e. [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

f. [redacted]

Figure 5-9. [redacted]

g. [redacted]

Figure 5-10. [redacted]

h. [redacted]

[redacted]

Figure 5-11.

[redacted]

~~(C)~~ [redacted]

b. ~~(C)~~ [redacted]

(1) ~~(C)~~ [redacted]

(a) ~~(C)~~ [redacted]

(b) ~~(C)~~ [redacted]

Figure 5-12.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

(2) ~~(C)~~ [redacted]

(a) ~~(C)~~ [redacted]

(b) ~~(C)~~ [redacted]

(c) ~~(C)~~ [redacted]

Figure 5-13. [redacted]

Figure 5-14.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

1. ~~(C)~~ [redacted]

2. ~~(C)~~ [redacted]

3. ~~(C)~~ [redacted]

4. ~~(C)~~ [redacted]

(3) ~~(C)~~ [redacted]

(4) ~~(C)~~ [redacted]

(5) ~~(C)~~ [redacted]

c. (U) Print Actuator and Timing Signals.—This section will cover the analysis of signals that relate to print hammer fire and timing functions from daisy wheel, bar, drum, chain and train printers. Other signals from printers (serial, parallel, etc.) should be analyzed using the techniques described in other sections of this chapter. As in any analysis, the TEMPEST tester or analyst must have a complete and thorough working knowledge of the EUT.

(1) ~~(C)~~ [redacted]

(a) ~~(C)~~ [redacted]

(b) ~~(C)~~ [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

~~(C)~~

(c) ~~(C)~~

[redacted]

Figure 5-15.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

(U) There are several rules of thumb which can be used to determine if a signal correlating to printwheel rotation, ribbon advance, proportional spacing, print hammer fire duration, or daisy wheel location is compromising.

1. ~~(C)~~ [redacted]

2. ~~(C)~~ [redacted]

3. ~~(C)~~ [redacted]

4. ~~(C)~~ [redacted]

(d) ~~(C)~~ [redacted]

(b) (1)
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

[redacted]

Figure 5-16. [redacted]

(2) ~~(C)~~ [redacted]

(a) ~~(C)~~ [redacted]

(b) ~~(C)~~ [redacted]

~~(C)~~ [redacted]

1. ~~(C)~~ [redacted]

(b) (1)
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

[redacted]

2. (U) Determine if the print sequence is every print column or every other print column, etc. for each pass of the type bar. Some printers will print odd print columns when the type bar moves from right to left and even print columns when the type bar moves from left to right or vise versa. Other printers will print all columns on each pass of the type bar. Be exact in determining the print sequence of the EUT.

3. (U) Develop a "paper" replica of the type bar used in the EUT. This can be made to any size as long as the sequence of characters are in the same order as the actual type bar. Also make the paper replica with as many type fonts as there are on the actual type bar. Figure 5-17 shows a typical type bar.

4. (U) Select and process one of the test messages from Appendix A, Table A-11.

5. ~~(C)~~ [redacted]

~~(C)~~ [redacted]

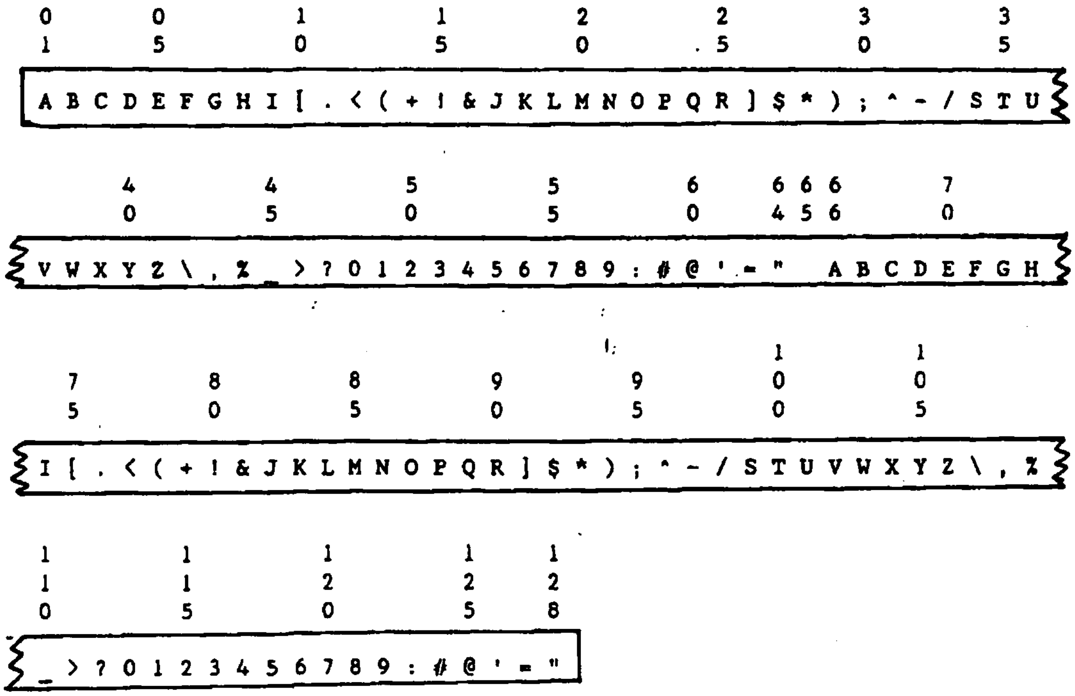

01 05 10 15 20 25 30 35
A B C D E F G H I [. < (+ ! & J K L M N O P Q R] $ *) ; ^ - / S T U
40 45 50 55 60 64 65 66 70
V W X Y Z \ , % _ > ? 0 1 2 3 4 5 6 7 8 9 : # @ ' = " A B C D E F G H
75 80 85 90 95 100 105
I [. < (+ ! & J K L M N O P Q R] $ *) ; ^ - / S T U V W X Y Z \ , %
110 115 120 125 128
_ > ? 0 1 2 3 4 5 6 7 8 9 : # @ ' = "

Figure 5-17.—Typical Type Bar (U)(U)

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

6. ~~(C)~~

7. ~~(C)~~

8. ~~(C)~~

[redacted]

Figure 5-18

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

Figure 5-19

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

Figure 5-20

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

Figure 5-21

(b) (1)
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

[redacted]

Figure 5-22.

9. ~~(C)~~ [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

Figure 5-23. [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

Figure 5-23

10. (U) Repeat this procedure for each line of text until the entire message has been completed.

(3) ~~(C)~~ [redacted]

[redacted]

(a) ~~(C)~~ [redacted]

(b) ~~(C)~~ [redacted]

1. (U) Release the paper feed and pull the paper as fast as possible while processing, for example, a test message consisting of repeated character "A's". From the printed page, determine the print hammer firing order, i.e., do all print hammers fire at the same time, in blocks, or sequentially across the page.

2. (U) With the paper feed released, change the test message to determine if there is a constant starting point for printing.

3. (U) From the detected signal, determine if there is some indication of a line feed pulse or some other pulse that can be called a start signal.

4. (U) Determine the rotation time for the drum to make one complete revolution. Divide this time by the number of rows of characters on the drum. Call this the row time.

5. (U) Make a matrix similar to the one described in Section 5-3c(2)(b) step 7.

6. (U) Process one of the test messages listed in Appendix A, Table A-11.

7. ~~(C)~~ [redacted]

8. (U) Measure the time from the print cycle start signal to the first set of hammer fires. Divide the row time into the measured time and determine which row of characters would have printed at that time.

9. (U) If the EUT prints characters sequentially across the page, determine the print column for the characters and place those characters in the appropriate columns. If all the characters print at approximately the same time, list the characters across that row of the matrix.

10. (U) Continue this process for each line of text until the entire test message has been processed.

11. (U) Compute an ADCS for the completed matrix.

Note that hammer fire emanations should be examined carefully for fingerprint signals correlating the emanation to column position.

(4) ~~(C)~~ [redacted]

d. ~~(C)~~ [redacted]

(1) ~~(C)~~ [redacted]

(2) ~~(C)~~ [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

~~(C)~~ [redacted]

~~(C)~~ [redacted]

(3) ~~(C)~~ [redacted]

1. [redacted]
2. [redacted]

~~(C)~~ [redacted]

1. ~~(C)~~ [redacted]

2. ~~(C)~~ [redacted]

3. ~~(C)~~ [redacted]

4. ~~(C)~~ [redacted]

5. (U) If changes are seen in the signal as different characters are processed but no qualitative assessment can be made on-site, the signals should be recorded and sent back to the laboratory for in-depth analysis.

6. (U) If a signal is detectable every time a character is processed but doesn't change as the characters are changed, the signal is not compromising.

e. ~~(C)~~ [redacted]

(1) ~~(C)~~ [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

Figure 5-24 [redacted]

Figure 5-25. [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

(2) ~~(C)~~

[redacted]

(a) ~~(C)~~

[redacted]

(b) ~~(C)~~

[redacted]

Figure 5-26.

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

(3) ~~(C)~~

[redacted]

~~(C)~~

[redacted]

~~(C)~~

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

Figure 5-28. [redacted]

[redacted] ~~(C)~~

[redacted] ~~(C)~~

[redacted]

(b) (1)
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

[redacted]

Figure 5-29

[redacted]

~~(C)~~ [redacted]

(4) ~~(C)~~ [redacted]

(5) *(U) Storage Display Device.*—The storage oscilloscope is an ideal device for displaying video emanations because, once set up, the scope can store the A-scope or raster display for a posteriori analysis. A storage scope is also useful for the raster display of facsimile signals because of the extremely long time required to scan and reproduce the pattern. An alternative is to use a scope camera with the shutter open for one whole vertical scan and a single vertical sweep.

(6) ~~(C)~~ [redacted]

(a) ~~(C)~~ [redacted]

[redacted]

(b) ~~(C)~~

(c) ~~(C)~~

(d) ~~(C)~~

(e) (U) For both vector display correlated signals and bandlimited dot matrix correlated signals, use the criteria for fingerprint signals discussed in Section 5-3*d*.

(f) (U) For graphic display signals, use the test pattern outlined in Section 4-2*c*(2)(d) and Figure 4-3 and report the resolution that can be detected.

f. ~~(C)~~ [redacted]

~~(C)~~

~~(C)~~

(1)

(2)

(3)

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

Figure 5-30. [redacted]

~~(C)~~ [redacted]

(1) [redacted]

(2) [redacted]

(3) [redacted]

(4) [redacted]

(5) [redacted]

(6) [redacted]

~~(C)~~ [redacted]

(1) [redacted]

(2) [redacted]

(3) [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

(4)

~~(C)~~

(1)

(2)

(a)

(b)

(c)

Figure 5-31.

Figure 5-32.

(b) (1)
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

5-4. (U) Optimizing The Detected Signal.—Once an emanation has been detected that exhibits signs of being related to a monitor signal, two things can be done to optimize the detected signal. They are to:

1. optimize the detection system; and,
2. reduce the noise in the detected signal.

a. (U) Optimizing the Detection System.— Optimizing the detection system is very important in performing good analysis. It is very important for the detection system to have good dynamic range, the proper IF bandwidth, and selective IF and video filtering characteristics.

(1) ~~(C)~~ [redacted]

~~(C)~~ [redacted]

(2) ~~(C)~~ [redacted]

(3) *(U) Filtering.*—For improved detection of TEMPEST emanations, the analyst has several options in regard to filtering.

(a) (U) Tunable Filter Selection.—Although not usually as effective as selecting the optimum IF band-pass characteristics, filtering the receiver's detected video output has some practical advantages. Active filters with continuously variable cutoff frequencies and selectable pulse response characteristics over the DC to 10 MHz range are available for the analyst. As discussed in Appendix C-12, the Gaussian, Butterworth or Bessel filter responses are preferred for TEMPEST emanations to avoid pulse distortion and provide moderately good selectivity.

(b) (U) Nontunable Filter Selection.—As in the case of tunable detection system filtering, the analyst can improve the display of suspected compromising signals using a selection of cutoff frequencies, improved filter selectivity (multipole filter design) and filters designed to minimize pulse distortion.

(U) The need for careful selection of nontunable pass-bands most often arises when a serial digital signal emanation has energy in the baseband frequency range but is sharply bandlimited above the data rate due to equipment filtering, etc. The analyst should use a continuously variable active filter for this application and vary the high-pass and low-pass cutoff frequencies independently. For data rates which preclude the use of an active filter, a set of fixed cutoff high-pass and low-pass filters may be cascaded (used in pairs) to vary the band-pass.

b. (U) Reducing the Effects of Noise.—Almost always a detected emanation contains noise, be it in the form of an equipment related operation, power line, or ambient environmental noise. These all contribute to obscuring the detected emanation thus making analysis difficult. Various types of active and passive filters are discussed in Appendix C-12 which can be used to minimize these different types of noise. Selection of the proper filters depends upon the characteristic of the noise to be removed.

[redacted]

(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

(U) In addition to using filters, other methods involving the operating procedures of the EUT can be used to reduce different sources of noise. A few of the more common procedures are now presented.

(1) ~~(C)~~ [redacted]

(U) Another technique to reduce or eliminate power supply chopper noise is to use time domain filters under software control. This can be done with a digital computer or a comb filter.

5-5. (U) Signal Collection.—Often the measurement of signal levels and ambient noise is not sufficient to prove that a potentially compromising TEMPEST situation exists. Some data may have to be recorded for subsequent analysis in the laboratory.

(U) The techniques and skills required for signal collection are somewhat different from those required for TEMPEST signal measurement. In this section, the problems of recording signals for later analysis will be discussed.

a. (U) Reasons for Collection.—One may wish to have some documentary proof that the signals measured are actually information bearing. This is sometimes difficult to determine during an on-site test, and it may require that the signals be recorded for later evaluation.

(U) As stated in Chapter 1, there is normally a rather low confidence factor associated with on-site analysis. This is due to the limited time and resources normally allocated to an on-site test. Confidence can be increased by recording some of the signals and making a more detailed analysis in the laboratory.

(U) Alternatively, some time can be taken to measure the statistical properties (mean signal level, ambient noise) of the information bearing parameters of the signals being evaluated. For many types of signals, a "high confidence" analysis as discussed in Chapter 1 can be made from the measurements. In these cases, the actual signal need not be recorded, only the statistics. This can be done with paper and pencil. Section 5-5*b*(2) explains this in more detail.

(U) Finally, one major reason for signal collection is to convince responsible people that a potentially compromising TEMPEST situation exists. This is accomplished by actually showing how intelligence can be recovered from the signal. For this purpose, normal operational traffic may have to be analyzed. This should only be attempted in very limited situations because it can be very time consuming and if not successful, it is inconclusive proof of non-compromise. In all cases, signal collection is the first step in the intelligence recovery process.

[redacted]

Figure 5-33.

b. (U) Types of Collection.

(1) *(U) Sample Collection.*—Signal analysis is largely an evaluation of similarities and differences among the signals related to different information units (characters, bits, etc.). Hence, for any later analysis, some recorded samples of the signals related to all of the information units are needed. In addition, more than one sample of each signal is needed since there is usually some variation among the signals related to the same information unit. This is called sample collection.

(2) ~~(C)~~ [redacted]

c. (U) Unknown Message Recording.—When the tester has access to the EUT, he may be able to prove its TEMPEST vulnerability by processing a message which is unknown to the analyst. The signals must be recorded and later reproduced for the analyst who tries to recover the message.

(U) The type of unknown test message which is used is very important. The test message should not be of such a nature that its text alone causes the message recovery to be more or less difficult than the typical traffic processed on the EUT. A message or data file, if one is kept by the users of the equipment, is a good source of test messages. The message should be complete—not just a series of phrases or disconnected words. For text processors, the test message should have English language statistical properties.

(U) Unless there is a specific reason for using certain text, two more things should be kept in mind:
(1) do not use proper names, and
(2) do not use obscure or archaic words.

It is often possible for these criteria to be met and still keep the messages fairly typical.

(U) As mentioned earlier, unknown message recovery should only be attempted in limited situations where absolutely required. It is generally very time consuming and can lead to false conclusions if unsuccessful.

d. (U) Unknown Signal Collection.—A TEMPEST tester may be faced with the challenge of actually attacking a signal without having access to the EUT to run some test patterns. Normally, this situation is avoided since it can make a test continue for a long time before reaching a conclusion. An unfriendly party presumably would have more time to attack a signal than the few days normally allotted for a TEMPEST test. See Section C-14.

(U) Collection of unknown signals (or known signals from uncontrolled equipment) is characterized by a great amount of feedback between the collection and analysis processes. This is why this type of collection can require a long time to reach a conclusion. However, this feedback can be reduced by the intelligent use of on-site analysis.

(U) There are two approaches to unknown signal collection:

(1) massive wideband recording of all detectable signals in the hope that something compromising will be collected, and

(2) selective recording of one signal which is highly suspected of being compromising.

(U) The first of these is easier for the collector, and can be accomplished without having any on-site analysis, but it requires a fairly expensive (wideband) recorder, long recording time, and extremely long analysis time to increase the probability of recovering compromising intelligence.

(U) The second approach is more difficult in that it requires some on-site analysis. The signal should possess the signs of a compromising signal before it is selected for recording. However, less data has to be recorded. This means either less bandwidth is required or less time is needed to record or both. Subsequent analysis is much easier since the analyst knows exactly what to look for. Consequently, it is recommended that when collecting unknown signals, as much on-site analysis as possible be done before signal collection begins.

e. *(U) How Much to Record.*—One of the first problems involved in planning a signal collection exercise is to determine how much to record. In this section some guidelines will be given on the minimum data required.

(1) *(U) Sample Size Requirements.*—The number of samples required to specify the statistical properties of a signal can vary tremendously depending on the actual distribution of those samples and the errors one is willing to tolerate. If one assumes that the information bearing signal parameters are normally distributed, it can simplify the sample size problem somewhat. The required sample size to establish confident results depends mostly on the standard deviation of the samples. Hence, some data has to be evaluated before the number of samples required can be determined. Often this is not feasible during an on-site test. At this point, experience is the best guide. Numerous signal evaluations have been made with rigorous attention applied to sample size requirements. Usually 25 samples is a good sample size. If more than 100 samples of a signal are required, analysis results are usually negative (i.e., not compromising).

(2) *(U) Length Of Test Messages.*—When recording an "unknown" test message for subsequent breakback, at least 500 characters of text should be used. The text should be typical of the traffic processed on the EUT. After the recording is made (or, if possible, while it is being made), the output of the recorder should be checked to be sure that the signal is being properly recorded.

(U) If the required signals do not have the proper gain (too low in amplitude or clipping the amplitude of the signal of interest), STOP THE RECORDING, make the necessary adjustments to the recorder and START THE TEST OVER. Do not adjust the gain of the system in the middle of a recording session. If the test results are going to be based on the results of a breakback, this recording is the most important data one will take during the on-site test.

(3) *(U) Length of Unknown Signal Recording.*—One great problem in trying to record signals from an uncontrolled EUT is knowing when traffic is being processed. Sometimes it is easy to tell when traffic is being processed but the traffic may be finished before the recorder can be activated. In these cases, run the recorder continuously and hope to record something.

(U) When doing a general coverage collection (i.e., trying to record anything that may be compromising), record as much (bandwidth and time) as possible, remembering that analysis time will probably be at least one hundred times as long as the recording session. When doing a targeted collection (i.e., recording one particular suspect signal), use sufficient bandwidth and record long enough to make sure at least 500 characters of text have been processed and recorded.

5-6. (U) **Data Collection Procedures.**—If on-site analysis of a signal can't be performed, data will need to be collected for in-depth analysis. Therefore, it is important that every effort be made to collect good data. Without good data, the best analyst is at a distinct disadvantage. For certain problems, data just looks good, analytic procedures seem to go smoothly, and a fairly fast decision can be made on whether the emanation is compromising. This may be because the signal is reasonably easy to work with, but it can also be greatly aided by using proper data collection procedures. Detail is the name of the game when it comes to data collection. Good data collection can make a good analyst appear superior. It is imperative that good data collection procedures be implemented and always followed.

(U) Here is a general outline for good data collection procedures.

(1) Draw a diagram of the EUT detection system set-up and label all key parameter settings used on the test equipment.

(2) If the detected emanation is going to be digitized, choose an adequate sampling rate based on the bandwidth used in the detection system.

(3) If the detected emanation is to be recorded, choose a recorder that will accurately capture that signal and determine the proper recording speed (FM recordings are preferred because the FM pass-band records from DC on up).

(4) Remove any DC bias from the detected emanation.

(5) Maximize the detected emanation's voltage level for either recording or digitizing purposes.

(6) Choose the proper test message.

(7) If a synchronization pulse or signal is being used, make sure it is working.

(8) If transient digital recordings are being made, record each monitor signal two times. Then record several occurrences of the detected emanation as a result of processing the test message.

(9) If the signal is either digitized or recorded on an analog recorder, record the monitor signal or signals simultaneously with the detected emanation.

(10) Record background ambient noise when no test message is being processed. This will provide statistical information necessary to design noise reduction filters to improve the signal-to-noise ratio. Note that in most cases the type of filter needed is one which does not alter the signal shape.

(11) Leave some time between different test messages to make them easy to find. For example, if the test message consists of repeated characters of the alphabet, leave a time gap between each character group.

(12) Keep accurate logs specifying the location on tape of each test message processed.

(13) Keep the actual test message typed or processed. If the test message is being typed while the detected emanation is being recorded, ignore all typing errors - don't backspace or overprint. Also, use either all lower case characters or all upper case characters. Do not type punctuation or special characters. Use only one "Space" character between words or at the end of a sentence.

(14) Properly label the tape to identify all key information.

(15) If mean and standard deviation data is collected for IR computations, keep accurate information records.

5-7. (U) **Summary.**—This Chapter has indicated how to make a cursory analysis of TEMPEST signals during an on-site test. It also describes how to record signal data for subsequent analysis. Chapter 6 discusses how to analyze these signals.

THIS PAGE IS INTENTIONALLY BLANK

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

CHAPTER 6

IN-DEPTH ANALYSIS (U)

6-1. (U) **Introduction.**—Signals detected during actual testing often vary from those predicted in pretest planning (Chapter 4). Signal features tend to be hidden by inherent noise in the TEMPEST channel. In-depth analysis is required to overcome the effects of this phenomena. A number of general methods to analyze noisy signals will be described in this chapter. Some of these methods require the use of the Information Ratio or the Average Depth of Correct Symbol. A detailed procedure for computing these measures will be presented.

6-2. ~~(C)~~ [redacted]

~~(C)~~ [redacted]

(1) [redacted]

(2) [redacted]

Figure 6-1 [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

6-3. ~~(C)~~ [redacted]

a. ~~(C)~~ [redacted]

b. (U) [redacted]

STEP 1: [redacted] ~~(C)~~ [redacted]

STEP 2: [redacted] ~~(C)~~ [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

STEP 3: ~~(C)~~

[redacted]

STEP 4: ~~(C)~~

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

STEP 5: ~~(C)~~ [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

STEP 6: ~~(C)~~ [redacted]

STEP 7: ~~(C)~~ [redacted]

STEP 8: ~~(C)~~ [redacted]

STEP 9: ~~(C)~~ [redacted]

STEP 10: ~~(C)~~ [redacted]

STEP 11: ~~(C)~~ [redacted]

(1) ~~(C)~~ [redacted]

(2) ~~(C)~~ [redacted]

(3) ~~(C)~~ [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

Figure 6-3.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

Figure 6-3.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

Figure 6–3.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

6-4. ~~(C)~~ [redacted]

a. ~~(C)~~ [redacted]

(b) (1)
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

[redacted]

Figure 6-4.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

Figure 6-4.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

Figure 6-4.-

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

Figure 6–4.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

STEP 2: ~~(C)~~ [redacted]

STEP 3: ~~(C)~~

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

Figure 6–5.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

Figure 6-6.

STEP 4: (U) Produce the generatrix sequence as illustrated in Figure 6-7 from the generatrix ordering matrix shown in Figure 6-6 and the sequential measurements given in STEP 2 of these procedures.

[redacted]

Figure 6-7.

STEP 5: ~~(C)~~

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

b. ~~(C)~~ [redacted]

c. ~~(C)~~ [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

6-5. ~~(C)~~ [redacted]

a. (U) [redacted]

STEP 1: (U)

STEP 2: (U)

STEP 3: (U)

STEP 4: ~~(C)~~ [redacted]

(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

STEP 5: (U) [redacted]

STEP 6: ~~(C)~~ [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

STEP 7: ~~(C)~~

(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

STEP 8: (U) [redacted]

~~(C)~~ [redacted]

6-6. ~~(C)~~

a. (U) The following procedure may be used to determine confidence limits on the IR:

STEP 1: (U) Compute the IR for several data sets.

STEP 2: (U) Compute the confidence interval on the IR by the method described in Section 3-2*c* (3).

$$IR_L = IR_M - C_N^a \frac{S}{\sqrt{N}} \tag{6.21}$$

and

$$IR_U = IR_M + C_N^a \frac{S}{\sqrt{N}} \tag{6.22}$$

where:

IR_M = the mean IR estimated from the sample data sets;

S = the sample standard deviation of the IR estimated from the sample data sets;

N = the number of sample data sets;

a = the desired confidence for this interval; and,

C_N^a = a constant which depends on N and the desired confidence "a" (values for C are given in Appendix A, Table A-7).

In the following examples, a = 95%.

b. (U) For this example, suppose 12 data sets are processed and the following IR values are calculated for these sets of data:

1.6	1.5	0.9	1.2	1.8	0.5
0.5	1.1	0.9	2.3	1.2	1.0

The computations would then yield

IR_M = 1.21 (see Section 3-2c. for an explanation of how to compute an estimation of the mean and standard deviation)

S = 0.52

N = 12

a = 95 %

C = 2.201 (from Appendix A, Table A-7)

$$IR_L = 1.21 - \frac{2.201 \cdot (0.52)}{\sqrt{12}} = 1.21 - 0.33 = 0.88$$

$$IR_U = 1.21 + \frac{2.201 \cdot (0.52)}{\sqrt{12}} = 1.21 + 0.33 = 1.54$$

Therefore, one can say with 95 percent confidence that

$$0.88 \leq IR \leq 1.54$$

c. (U) N = 12 was chosen in the above example as a matter of convenience. However, because of the Central Limit Theorem mentioned in Section 3-2*b*(4), it would be preferable to have as many as 30 data sets. It is recognized that situations will arise in which very few data sets can be obtained and processed. In these cases the constants for small sample sizes in Appendix A, Table A-7 will yield somewhat wider confidence intervals. To increase the sample size, one can test additional units of the same model, use different personnel or test equipment, or select units of different ages.

d. (U) A similar confidence range can be placed on the ADCS. Suppose 10 messages are processed and the following ADCS values are calculated for these messages:

2.3	3.1	2.4	2.7	2.0
2.6	2.2	2.5	2.5	2.4

The confidence interval determination would proceed as follows:

$$\mathrm{ADCS}_M = 2.47$$
$$S = 0.30$$
$$N = 10$$
$$a = 95\ \%$$
$$C = 2.262$$

Using equations (6.21) and (6.22) as before, except substituting the ADCS values in place of the IR values, one obtains:

$$\mathrm{ADCS}_L = 2.47 - \frac{2.262\cdot(0.30)}{\sqrt{10}} = 2.47 - 0.21 = 2.26$$

$$\mathrm{ADCS}_U = 2.47 + \frac{2.262\cdot(0.30)}{\sqrt{10}} = 2.47 + 0.21 = 2.68$$

Thus one can say with 95 percent confidence that

$$2.26 \leq \mathrm{ADCS} \leq 2.68$$

6-7. (U) Recovery of Text.—The following discussion and examples apply in cases where complete generatrices do not occur, i.e. the generatrix sequence is shorter than 27 long. This situation would arise in noiseless channels (such as bit density signals) or in multiple output signal channels where one might be able to rule out the possibility of some characters occurring in specific character positions within the underlying message.

a. ~~(C)~~ [redacted]

(1)

(2)

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

(1) (U) Case 1: "Space" Unique

STEP 1: Find the longest word in the unknown message. If this word is more than nine or ten characters in length, it will probably be the easiest word to recover and it will convey a lot of information about the rest of the message.

STEP 2: Look for common prefixes and suffixes throughout the generatrix sequence (i.e., "TION", "ED", "PRE", etc.).

STEP 3: Look for common letter combinations throughout the generatrix sequence (i.e., "TH", "QU", etc.).

(2) (U) Case 2: "Space" Not Unique

Look for the longest area in the unknown message where a "Space" is not contained in the generatrix sequence and continue as before.

(3) (U) Example

A specific example is now presented which illustrates the way an analyst went about recovering an unknown message from a generatrix sequence. Consider the generatrix sequence shown in Figure 6-8.

(U) Take note of the fact that in this case there is no long area where a "Space" character is not contained in the generatrices. Therefore, the "Space" character is not unique and word length is not known. The following steps were used by the analyst:

STEP 1: (U) Think of the most common words that begin sentences ("THE", "THIS", "THEY", etc.). These words come to mind since there is a "T" in row 1 and an "H" in row 2. Row 3 does not contain an "E"; therefore the words "THE", "THEY", etc. are eliminated. Since there is an "I" in row 3 and an "S" in row 4, the word "THIS" becomes very probable as the first word of the unknown message.

THIS ____

STEP 2: (U) Once "THIS" has been determined, "IS" falls out as being a definite possible second word. Of course other words could follow "THIS" but "IS" becomes even more probable after the third word of the unknown message is determined.

THIS IS _____________________________________

STEP 3: (U) Rows 12, 13 and 14 are short; therefore the third word of the unknown message easily falls out. The letters that make up these rows are not found in the 4th, 5th, and 6th positions of many 7 letter words. This helps to narrow the possibilities.

THIS IS BECAUSE ______________________________

STEP 4: (U) The fourth word "THE" follows because of the short row 19 and because it fits very easily with what is known so far about the sentence.

THIS IS BECAUSE THE __________________________

STEP 5: (U) From now on things get a little more difficult. The next word is probably either a noun or an adjective. The short rows 23 and 25, of course, are a great help in determining this word.

THIS IS BECAUSE THE SMALL ______________________

(b) (1)
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

[redacted]

Figure 6-8

STEP 6: (U) About the only thing one can tell from context about the next word is that it is either a noun or another adjective. This word is found by using the famous "brute force" method. This method involves listing many words and eliminating the ones that do not fit in the sentence. In this case, because the "Space" character is so prevalent in the generatrices, it might be best to first look at possible long words (10-12 characters) and work down to shorter and shorter words. Once a word is formed that seems to make good sense in the sentence, try to find a word to follow it (seventh word). If a seventh word is not found, it means the sixth word is wrong and to continue searching for another possible sixth word.

THIS IS BECAUSE THE SMALL FISH ______________________

STEP 7: (U) At this point it might be a good idea to look at what is known about the sentence so far. The next words or phrases probably say something about what small fish do. Since row 37 is short, it is best to work around this row and see what can be done. The word "AND" falls out as a very definite possibility.

THIS IS BECAUSE THE SMALL FISH ______ AND ______________

STEP 8: (U) One is now left with two four-character words with the word "AND" connecting them. These words are found by just thinking about what "fish do" and then using the "brute force" method again. It shouldn't take too long to find the two words since there just aren't many things fish do (swim, live, feed, etc.).

THIS IS BECAUSE THE SMALL FISH LIVE AND FEED

b. (U) The Use of a Dictionary in Generatrix Sequence Solving.—A word dictionary can be a very useful tool in generatrix solving. For it to be useful, however, the dictionary should be formatted in the following way:

(1) The words should be grouped by word length, and

(2) The words should be alphabetized by each individual letter in the words; i.e., the first section should have all the words alphabetized by their first letter, the second section should have all the words alphabetized by their second letter, etc.

(U) Once a dictionary has been assembled, it should be required that all unknown text messages be made up of words from this dictionary.

(U) To best describe the use of the word dictionary in text recovery, the sample generatrix sequence of Figure 6-9 will be used. This sequence was generated from a TEMPEST signal:

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

Figure 6-9

STEP 1: (U) Look for the longest word in the unknown message. The example above contains the longest word in a generatrix sequence.

STEP 2: (U) Look for the shortest row in the word. In this example it would be the second character of the word.

STEP 3: (U) Turn to the section in the dictionary with words alphabetized by that character in the word. In this example it ,would be necessary to turn to the section in the dictionary with words alphabetized by their second character.

STEP 4: (U) Within this listing, turn to the subsection listing the word length under scrutiny. In this example it would be necessary to look at the 10-character word section. There are only a few ten character words which have as their second character either "D", "C" or "V". Therefore it will be relatively easy to discover that the unknown word is in fact "EVERYTHING."

From this example it can be seen that with the aid of a word dictionary, it is less difficult to recover unknown text messages even though some of the rows in the generatrix are very long.

6-8. (U) **Summary.**—The techniques presented in this chapter are some basic tools that have been developed from the mathematical foundations of Chapter 3 and years of experience in TEMPEST signal analysis.

THIS PAGE IS INTENTIONALLY BLANK

CHAPTER 7

PREPARATION OF ANALYTIC REPORTS (U)

7-1. (U) Introduction.—A TEMPEST analytic report has two objectives. The first objective is to point out TEMPEST vulnerabilities so that they may be corrected. The analytic report should complement the TEMPEST test report to completely assess the possibility of TEMPEST exploitation. Usually, the personnel responsible for the operation of an equipment or system do not fully understand the consequences of compromising emanations. To ensure their cooperation in implementing any recommended changes, one must convince them that a problem exists. Therefore, the primary purpose of an analytic report must be to show, in a straight forward manner, the extent to which information is recoverable so that corrective action can be taken.

a. (U) The second objective of an analytic report is to serve as a reference for future analysis. One of the main sources of information concerning TEMPEST analysis is analytic reports documenting previous test results. (See Appendix F-2 for information on how to obtain TEMPEST reports from the National TEMPEST Information Center. All TEMPEST reports are filed at this library and may be borrowed by any member of the TEMPEST community.) To be useful as a data base, the analytic report must be detailed. Analytic techniques used and the rationale for using them are as important as the specific results obtained. Often the reader of these reports is looking for an approach to a similar problem. For example, the method of recovering information from a particular CRT display which someone devised may be useful in recovering information from another display.

b. (U) There may appear to be a conflict between the two objectives of the analytic report. How can the same report be simple enough to be understood by personnel with no previous TEMPEST orientation, yet detailed enough to be a useful reference for the discerning analyst? Certain essential elements must be included if the report is to meet these requirements. These elements include:

1) equipment description,
2) detected signal description,
3) analytic techniques, and
4) results.

(U) An example of an analytic report which contains these sections is presented in Appendix D.

7-2. (U) Analytic Report Essential Elements.

a. ~~(C)~~ [redacted]

b. ~~(C)~~ [redacted]

(b) (1)
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

[redacted]

c. *(U) Analytic Techniques.*—The purpose of the analysis section is to describe both the techniques used and the rationale behind them. This section will primarily be of interest to other analysts. However, a clear, logical presentation will justify the results to the general reader and will remove some of the "black magic" from TEMPEST analysis. Explain the analysis technique used and its effect on the signal. Next, explain the actual processing—recording, filtering, analog-to-digital conversion, etc. How was the information content of the signal measured? State the purpose of each analytic procedure. State why that procedure was necessary. Then, summarize the steps of the procedure. The step by step details are best illustrated in a flow chart, not in the body of the report. Finally, discuss the results of each procedure. What did that procedure tell the analyst about the information content of the signal? What new questions did the procedure raise? What procedure was used to answer them? Present the analytic procedures employed in a logical, orderly manner from start to finish. The results of the analysis should be presented in the next section.

d. ~~(C)~~ [redacted]

7-3. (U) **Summary.**—An analytic report has two objectives—to point out TEMPEST vulnerabilities and to serve as a reference. There are sections essential to every report—equipment description, detected signal description, analytic techniques, and results. The analytic techniques section should explain the rationale used. The results section should give the general reader a measure of the information content of the detected signals.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

APPENDIX A

TABLES (U)

A-1. (U) **Introduction.**—This Appendix contains tables of numerical data and test patterns which are useful for TEMPEST signal analysis. Most of the tables are self explanatory, but some facts should be stated about the first five sets of tables.

~~(C)~~ [redacted]

(a)
(b)
(c)
(d)
(e)
(f)
(g)
(h)
(i)

~~(C)~~ [redacted]

(U) From a normal distribution table, it follows immediately that

$$N_v = 2.58\ N_\sigma$$

(U) It is feasible to measure the statistical parameters $\bar{S}$ and N_σ only if some automated technique is used. This is the preferred procedure to obtain signal-to-noise directly. However if visual measurements are made, they can be converted to signal-to-noise ratios as follows:

$$\text{Visual:}\quad \frac{\bar{S}+N_v}{N_v} = 1 + \frac{\bar{S}}{2.58\ N_\sigma}$$

$$\text{Automated:}\quad \frac{\bar{S}}{N_\sigma} = 2.58\left(\frac{\bar{S}+N_v}{N_v} - 1\right)$$

(U) Both sets of values are listed in the tables. The final three columns in the table list these same values after being converted to dB.

THIS PAGE IS INTENTIONALLY LEFT BLANK

ASCII

TABLE A-1(a)

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

TABLE A-1(b)

[redacted]

TABLE A-1(c)

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

TABLE A-1(d)

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

BAUDOT

TABLE A-2(b)

[redacted]

TABLE A-2(c)

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

TABLE A-2(d)

[redacted]

(b) (1)
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

TABLE A-3(b)

[redacted]

TABLE A-3(c)

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

TABLE A-3(d)

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

EBCDIC

TABLE A-4(a)

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

TABLE A-4(b)

TABLE A-4(c)

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

TABLE A-4(d)

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

FIELD DATA

TABLE A-5(a)

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

TABLE A-5(b)

[redacted]

TABLE A-5(c)

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

TABLE A-5(d)

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

THIS PAGE IS INTENTIONALLY LEFT BLANK

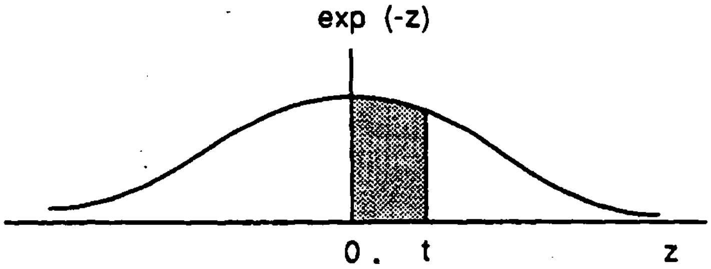
TABLE A-6

TABLE OF VALUES OF erf(t) (U)(U)

For a normal distribution with $\mu = 0.$, $\sigma = 1$

$$\mathrm{erf}(t) = \frac{2}{\sqrt{\pi}} \int_0^t \exp(-z^2)\,dz$$

Graphically that is represented as



The relationship between erf(t) and the cumulative normal distribution function $\Phi(\sqrt{2}\,t)$ is

$$\Phi(\sqrt{2}\,t) = 1/2 + 1/2 \cdot \mathrm{erf}(t) \quad \text{or}$$

$$\mathrm{erf}(t) = 2\Phi(\sqrt{2}\,t) - 1$$

where $$\Phi(\sqrt{2}\,t) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\sqrt{2}t} \exp\left(-\frac{z^2}{2}\right) dz$$

Also note that the erf(t) is an assymmetric function, i.e.,

$$\mathrm{erf}(t) = -\mathrm{erf}(-t)$$

TABLE A-6 (Continued)

TABLE OF VALUES OF erf(t) (U) (U)

t	0	1	2	3	4	5	6	7	8	9
0.0	.00000	.01128	.02256	.03384	.04511	.05637	.06762	.07886	.09008	.10128
0.1	.11246	.12362	.13476	.14587	.15695	.16800	.17901	.18999	.20094	.21184
0.2	.22270	.23352	.24430	.25502	.26570	.27633	.28690	.29742	.30788	.31828
0.3	.32863	.33891	.34913	.35928	.36936	.37938	.38933	.39921	.40901	.41874
0.4	.42839	.43797	.44747	.45689	.46623	.47548	.48466	.49375	.50275	.51167
0.5	.52050	.52924	.53790	.54646	.55494	.56332	.57162	.57982	.58792	.59594
0.6	.60386	.61168	.61941	.62705	.63459	.64203	.64938	.65663	.66378	.67084
0.7	.67780	.68467	.69143	.69810	.70468	.71116	.71754	.72382	.73001	.73610
0.8	.74210	.74800	.75381	.75952	.76514	.77067	.77610	.78144	.78669	.79184
0.9	.79691	.80188	.80677	.81156	.81627	.82089	.82542	.82987	.83423	.83851
1.0	.84270	.84681	.85084	.85478	.85865	.86244	.86614	.86977	.87333	.87680
1.1	.88021	.88353	.88679	.88997	.89308	.89612	.89910	.90200	.90484	.90761
1.2	.91031	.91296	.91553	.91805	.92051	.92290	.92524	.92751	.92973	.93190
1.3	.93401	.93606	.93807	.94002	.94191	.94376	.94556	.94731	.94902	.95067
1.4	.95229	.95385	.95538	.95686	.95830	.95970	.96105	.96237	.96365	.96490
1.5	.96611	.96728	.96841	.96952	.97059	.97162	.97263	.97360	.97455	.97546
1.6	.97635	.97721	.97804	.97884	.97962	.98038	.98110	.98181	.98249	.98315
1.7	.98379	.98441	.98500	.98558	.98613	.98667	.98719	.98769	.98817	.98864
1.8	.98909	.98952	.98994	.99035	.99074	.99111	.99147	.99182	.99216	.99248
1.9	.99279	.99309	.99338	.99366	.99392	.99418	.99443	.99466	.99489	.99511
2.0	.99532	.99552	.99572	.99591	.99609	.99626	.99642	.99658	.99673	.99688
2.1	.99702	.99715	.99728	.99741	.99753	.99764	.99775	.99785	.99795	.99805
2.2	.99814	.99822	.99831	.99839	.99846	.99854	.99861	.99867	.99874	.99880
2.3	.99886	.99891	.99897	.99902	.99906	.99911	.99915	.99920	.99924	.99928
2.4	.99931	.99935	.99938	.99941	.99944	.99947	.99950	.99952	.99955	.99957
2.5	.99959	.99961	.99963	.99965	.99967	.99969	.99971	.99972	.99974	.99975
2.6	.99976	.99978	.99979	.99980	.99981	.99982	.99983	.99984	.99985	.99986
2.7	.99987	.99987	.99988	.99989	.99989	.99990	.99991	.99991	.99992	.99992
2.8	.99992	.99993	.99993	.99994	.99994	.99994	.99995	.99995	.99995	.99996
2.9	.99996	.99996	.99996	.99997	.99997	.99997	.99997	.99997	.99997	.99998

TABLE A-7

CONSTANTS FOR COMPUTING 95 PERCENT CONFIDENCE LIMITS ON THE MEAN (U)(U)

NO. OF SAMPLES	C
2	12.706
3	4.303
4	3.182
5	2.776
6	2.571
7	2.447
8	2.365
9	2.306
10	2.262
11	2.228
12	2.201
13	2.179
14	2.160
15	2.145
16	2.131
17	2.120
18	2.110
19	2.101
20	2.093
21	2.086
22	2.080
23	2.074
24	2.069
25	2.064
26	2.060
27	2.056
28	2.052
29	2.048
30	2.045
40	2.042
60	2.021
120	2.000

Note: Each value for C corresponds to the 97.5th percentile of a "t" distribution with degrees of freedom equal to one less than the number of samples.

TABLE A-8

FACTORS FOR COMPUTING 95 PERCENT CONFIDENCE LIMITS FOR THE STANDARD DEVIATION (U)(U)

NO. OF SAMPLES	B_L	B_U
2	.3576	17.79
3	.4581	4.859
4	.5178	3.183
5	.5590	2.567
6	.5899	2.248
7	.6143	2.052
8	.6344	1.918
9	.6513	1.820
10	.6657	1.746
11	.6784	1.686
12	.6896	1.638
13	.6995	1.598
14	.7084	1.564
15	.7166	1.534
16	.7240	1.509
17	.7308	1.486
18	.7372	1.466
19	.7430	1.446
20	.7484	1.432
21	.7535	1.417
22	.7582	1.404
23	.7627	1.391
24	.7669	1.380
25	.7709	1.370
26	.7747	1.360
27	.7783	1.351
28	.7817	1.343
29	.7849	1.335
30	.7880	1.327
40	.8126	1.272
60	.8431	1.212
100	.8752	1.158

Reference: Lindley, D.V; East, D.A. and Hamilton, P.A. (1960). Tables for making inferences about the variance of a normal distribution. Biometrika, 47,333.

TABLE A-9

SENTENCES FOR TESTING SPEECH EQUIPMENT (U)(U)

1. Mabel stood on the rock.
2. Sue cleaned up the old house.
3. Show the rich lady out.
4. The auto stopped itself.
5. The others liked to play.
6. Don't splash paint on that rug.
7. He caught them at your house.
8. It was too late for lunch.
9. She broke the old red jar.
10. His jackknife looked so sharp.
11. Most gum cost four pennies.
12. That herb garden looks fine.
13. The miners panned for gold.
14. Fred was wrong to be blunt.
15. The plants grew tall and green.
16. Swim to that other rock.
17. The bathroom sink is clogged.
18. You should clean the black pot.
19. No boys can take the course.
20. These mushrooms taste awful.
21. She threw mud on that wall.
22. The lawyers wrote that will.
23. The braid is much too long.
24. She had on elbow gloves.
25. They took a test for school.
26. The stop sign fell over.
27. He lost all those letters.

TABLE A-10(a)

GENERAL ENGLISH LANGUAGE MONOGRAPHIC LETTER PROBABILITIES (U)(U)

	Alphabetic Order		Probability Order	
1	A	.0657	Sp	.1728
2	B	.0117	E	.1052
3	C	.0275	T	.0815
4	D	.0292	A	.0657
5	E	.1052	O	.0609
6	F	.0195	N	.0607
7	G	.0163	I	.0606
8	H	.0421	S	.0542
9	I	.0606	R	.0519
10	J	.0020	H	.0421
11	K	.0055	L	.0329
12	L	.0329	D	.0292
13	M	.0210	C	.0275
14	N	.0607	U	.0233
15	O	.0609	M	.0210
16	P	.0177	F	.0195
17	Q	.0009	P	.0177
18	R	.0519	G	.0163
19	S	.0542	Y	.0136
20	T	.0815	W	.0133
21	U	.0233	B	.0117
22	V	.0079	V	.0079
23	W	.0133	K	.0055
24	X	.0018	J	.0020
25	Y	.0136	X	.0018
26	Z	.0003	Q	.0009
27	Sp	.1728	Z	.0003

Sp REPRESENTS THE "SPACE" CHARACTER

THIS PAGE IS INTENTIONALLY LEFT BLANK

TABLE A-10(b)

GENERAL ENGLISH LANGUAGE TOP 300 MOST PROBABLE DIGRAPHS AND THEIR PROBABILITIES (U)(U)

	Alphabetic Order		Probability Order			Alphabetic Order		Probability Order	
1	AB	.00146	ESp	.02918	44	DL	.00037	NG	.00649
2	AC	.00292	SpT	.02421	45	DM	.00037	LSp	.00633
3	AD	.00241	SSp	.02367	46	DO	.00129	SpM	.00612
4	AG	.00116	TH	.01966	47	DR	.00065	CO	.00612
5	AI	.00167	HE	.01819	48	DS	.00112	OU	.00602
6	AK	.00068	SpA	.01663	49	DU	.00092	ED	.00595
7	AL	.00768	TSp	.01561	50	DY	.00024	IO	.00578
8	AM	.00122	IN	.01554	51	DSp	.01343	AS	.00568
9	AN	.01139	NSp	.01401	52	EA	.00384	DE	.00558
10	AO	.00037	DSp	.01343	53	EC	.00292	GSp	.00544
11	AP	.00116	ON	.01292	54	ED	.00595	VE	.00530
12	AR	.00731	ER	.01292	55	EE	.00313	RA	.00527
13	AS	.00568	SpO	.01268	56	EF	.00150	SpD	.00520
14	AT	.00976	AN	.01139	57	EG	.00105	SE	.00499
15	AU	.00078	RE	.01132	58	EI	.00105	SpSp	.00496
16	AV	.00153	YSp	.01098	59	EK	.00034	NE	.00479
17	AW	.00031	SpI	.01030	60	EL	.00313	SpE	.00476
18	AY	.00150	SpC	.01027	61	EM	.00269	RO	.00462
19	ASp	.00425	AT	.00976	62	EN	.00969	HI	.00462
20	BA	.00119	EN	.00969	63	EO	.00071	IC	.00462
21	BE	.00391	SpS	.00901	64	EP	.00119	LE	.00456
22	BI	.00092	RSp	.00871	65	ER	.01292	SpN	.00446
23	BL	.00238	TI	.00854	66	ES	.00819	NS	.00442
24	BO	.00105	OSp	.00850	67	ET	.00275	ME	.00442
25	BU	.00112	OR	.00833	68	EV	.00184	SpR	.00425
26	BY	.00065	ES	.00819	69	EW	.00075	ASp	.00425
27	CA	.00395	TO	.00816	70	EX	.00136	LI	.00412
28	CC	.00034	ND	.00809	71	EY	.00099	MA	.00405
29	CE	.00374	ST	.00799	72	ESp	.02918	RI	.00405
30	CH	.00320	SpB	.00792	73	FA	.00078	SI	.00401
31	CI	.00197	IT	.00789	74	FE	.00167	CA	.00395
32	CK	.00139	SpF	.00782	75	FF	.00129	FO	.00391
33	CL	.00044	IS	.00775	76	FI	.00187	BE	.00391
34	CO	.00612	TE	.00768	77	FL	.00034	HSp	.00391
35	CR	.00143	AL	.00768	78	FO	.00391	OM	.00384
36	CT	.00255	SpP	.00768	79	FR	.00204	EA	.00384
37	CU	.00143	SpW	.00758	80	FT	.00041	LL	.00384
38	CY	.00051	AR	.00731	81	FU	.00065	SpL	.00377
39	CSp	.00143	OF	.00717	82	FSp	.00694	CE	.00374
40	DA	.00092	HA	.00717	83	GA	.00061	LA	.00357
41	DD	.00031	SpH	.00711	84	GE	.00302	TA	.00340
42	DE	.00558	FSp	.00694	85	GH	.00184	TR	.00340
43	DI	.00292	NT	.00677	86	GI	.00078	UN	.00337

Sp REPRESENTS THE "SPACE" CHARACTER

TABLE A-10(b) (Continued)

GENERAL ENGLISH LANGUAGE TOP 300 MOST PROBABLE DIGRAPHS AND THEIR PROBABILITIES (U)(U)

	Alphabetic Order		Probability Order			Alphabetic Order		Probability Order	
87	GN	.00027	NA	.00333	130	LO	.00170	KSp	.00204
88	GO	.00119	HO	.00320	131	LS	.00109	FR	.00204
89	GR	.00116	CH	.00320	132	LT	.00075	LD	.00201
90	GS	.00041	LY	.00320	133	LU	.00143	CI	.00197
91	GU	.00041	NO	.00320	134	LY	.00320	WE	.00194
92	GSp	.00544	US	.00316	135	LSp	.00633	OS	.00190
93	HA	.00717	NC	.00316	136	MA	.00405	MI	.00190
94	HE	.01819	PR	.00313	137	MB	.00027	SU	.00187
95	HI	.00462	EE	.00313	138	ME	.00442	FI	.00187
96	HN	.00031	EL	.00313	139	MI	.00190	WI	.00184
97	HO	.00320	OT	.00310	140	MM	.00112	EV	.00184
98	HR	.00048	GE	.00302	141	MO	.00289	GH	.00184
99	HT	.00092	AC	.00292	142	MP	.00092	LO	.00170
100	HU	.00061	DI	.00292	143	MS	.00051	FE	.00167
101	HSp	.00391	EC	.00292	144	MU	.00102	AI	.00167
102	IA	.00133	NI	.00289	145	MY	.00044	RY	.00163
103	IB	.00041	MO	.00289	146	MSp	.00258	IV	.00163
104	IC	.00462	SS	.00289	147	NA	.00333	OP	.00163
105	ID	.00221	TS	.00289	148	NC	.00316	SpU	.00153
106	IE	.00221	UT	.00289	149	ND	.00809	AV	.00153
107	IF	.00122	SpG	.00286	150	NE	.00479	IR	.00150
108	IG	.00116	OL	.00286	151	NF	.00031	AY	.00150
109	IK	.00037	PE	.00275	152	NG	.00649	EF	.00150
110	IL	.00255	ET	.00275	153	NI	.00289	RN	.00146
111	IM	.00136	RT	.00272	154	NK	.00051	AB	.00146
112	IN	.01554	UL	.00269	155	NL	.00044	CU	.00143
113	IO	.00578	EM	.00269	156	NM	.00048	CR	.00143
114	IR	.00150	RS	.00265	157	NN	.00044	CSp	.00143
115	IS	.00775	MSp	.00258	158	NO	.00320	LU	.00143
116	IT	.00789	CT	.00255	159	NS	.00442	VI	.00139
117	IV	.00163	IL	.00255	160	NT	.00677	CK	.00139
118	IZ	.00044	SO	.00252	161	NU	.00027	PL	.00136
119	JO	.00027	PO	.00252	162	NV	.00027	EX	.00136
120	JU	.00031	UR	.00245	163	NY	.00085	IM	.00136
121	KE	.00129	AD	.00241	164	NSp	.01401	UC	.00136
122	KI	.00082	BL	.00238	165	OA	.00048	WO	.00133
123	KS	.00044	TY	.00231	166	OB	.00071	IA	.00133
124	KSp	.00204	OW	.00231	167	OC	.00126	WSp	.00129
125	LA	.00357	WH	.00228	168	OD	.00071	DO	.00129
126	LD	.00201	IE	.00221	169	OF	.00717	FF	.00129
127	LE	.00456	ID	.00221	170	OG	.00065	KE	.00129
128	LI	.00412	PA	.00221	171	OI	.00031	OV	.00126
129	LL	.00384	WA	.00211	172	OL	.00286	OC	.00126

Sp REPRESENTS THE "SPACE" CHARACTER

TABLE A-10(b) (Continued)

GENERAL ENGLISH LANGUAGE TOP 300 MOST PROBABLE DIGRAPHS AND THEIR PROBABILITIES (U)(U)

Alphabetic Order			Probability Order	
173	OM	.00384	SH	.00126
174	ON	.01292	TU	.00126
175	OO	.00109	UG	.00122
176	OP	.00163	AM	.00122
177	OR	.00833	IF	.00122
178	OS	.00190	RD	.00122
179	OT	.00310	SpY	.00119
180	OU	.00602	BA	.00119
181	OV	.00126	EP	.00119
182	OW	.00231	GO	.00119
183	OSp	.00850	IG	.00116
184	PA	.00221	AG	.00116
185	PE	.00275	AP	.00116
186	PI	.00065	GR	.00116
187	PL	.00136	MM	.00112
188	PO	.00252	BU	.00112
189	PP	.00082	DS	.00112
190	PR	.00313	SA	.00109
191	PS	.00048	LS	.00109
192	PT	.00054	OO	.00109
193	PU	.00092	RM	.00105
194	PSp	.00065	BO	.00105
195	QU	.00051	EG	.00105
196	RA	.00527	EI	.00105
197	RB	.00034	MU	.00102
198	RC	.00058	TT	.00102
199	RD	.00122	SpV	.00099
200	RE	.01132	EY	.00099
201	RG	.00065	SP	.00095
202	RI	.00405	HT	.00092
203	RK	.00065	BI	.00092
204	RL	.00058	DA	.00092
205	RM	.00105	DU	.00092
206	RN	.00146	MP	.00092
207	RO	.00462	PU	.00092
208	RP	.00051	RU	.00092
209	RR	.00071	UB	.00092
210	RS	.00265	UE	.00092
211	RT	.00272	YS	.00085
212	RU	.00092	NY	.00085
213	RV	.00031	UM	.00082
214	RY	.00163	KI	.00082
215	RSp	.00871	PP	.00082
216	SA	.00109	UA	.00078
217	SC	.00071	AU	.00078
218	SE	.00499	FA	.00078
219	SH	.00126	GI	.00078
220	SI	.00401	LT	.00075
221	SK	.00024	EW	.00075
222	SL	.00044	OD	.00071
223	SM	.00051	EO	.00071
224	SO	.00252	OB	.00071
225	SP	.00095	RR	.00071
226	SS	.00289	SC	.00071
227	ST	.00799	VA	.00071
228	SU	.00187	YE	.00068
229	SY	.00061	AK	.00068
230	SSp	.02367	BY	.00065
231	TA	.00340	DR	.00065
232	TE	.00768	FU	.00065
233	TH	.01966	OG	.00065
234	TI	.00854	PI	.00065
235	TL	.00054	PSp	.00065
236	TO	.00816	RG	.00065
237	TR	.00340	RK	.00065
238	TS	.00289	UI	.00061
239	TT	.00102	GA	.00061
240	TU	.00126	HU	.00061
241	TW	.00048	SY	.00061
242	TY	.00231	SpK	.00058
243	TSp	.01561	RC	.00058
244	UA	.00078	RL	.00058
245	UB	.00092	XP	.00054
246	UC	.00136	PT	.00054
247	UD	.00051	TL	.00054
248	UE	.00092	VO	.00054
249	UG	.00122	YO	.00051
250	UI	.00061	CY	.00051
251	UL	.00269	MS	.00051
252	UM	.00082	NK	.00051
253	UN	.00337	QU	.00051
254	UP	.00051	RP	.00051
255	UR	.00245	SM	.00051
256	US	.00316	UD	.00051
257	UT	.00289	UP	.00051
258	VA	.00071	HR	.00048

Sp REPRESENTS THE "SPACE" CHARACTER

TABLE A-10(b) (Continued)

GENERAL ENGLISH LANGUAGE TOP 300 MOST PROBABLE DIGRAPHS AND THEIR PROBABILITIES (U)(U)

Alphabetic Order			Probability Order	
259	VE	.00530	NM	.00048
260	VI	.00139	OA	.00048
261	VO	.00054	PS	.00048
262	WA	.00211	TW	.00048
263	WE	.00194	WN	.00048
264	WH	.00228	SpJ	.00048
265	WI	.00184	CL	.00044
266	WN	.00048	IZ	.00044
267	WO	.00133	KS	.00044
268	WSp	.00129	MY	.00044
269	XP	.00054	NL	.00044
270	XT	.00027	NN	.00044
271	YE	.00068	SL	.00044
272	YO	.00051	ZE	.00041
273	YS	.00085	FT	.00041
274	YSp	.01098	GS	.00041
275	ZE	.00041	GU	.00041
276	SpA	.01663	IB	.00041
277	SpB	.00792	SpQ	.00037
278	SpC	.01027	AO	.00037
279	SpD	.00520	DL	.00037
280	SpE	.00476	DM	.00037
281	SpF	.00782	IK	.00037
282	SpG	.00286	RB	.00034
283	SpH	.00711	CC	.00034
284	SpI	.01030	EK	.00034
285	SpJ	.00048	FL	.00034
286	SpK	.00058	NF	.00031
287	SpL	.00377	AW	.00031
288	SpM	.00612	DD	.00031
289	SpN	.00446	HN	.00031
290	SpO	.01268	JU	.00031
291	SpP	.00768	OI	.00031
292	SpQ	.00037	RV	.00031
293	SpR	.00425	XT	.00027
294	SpS	.00901	GN	.00027
295	SpT	.02421	JO	.00027
296	SpU	.00153	MB	.00027
297	SpV	.00099	NU	.00027
298	SpW	.00758	NV	.00027
299	SpY	.00119	SK	.00024
300	SpSp	.00496	DY	.00024

Sp REPRESENTS THE "SPACE" CHARACTER

TABLE A-11

TYPICAL ENGLISH LANGUAGE MESSAGES (U)(U)

IN THE EARLY PART OF THE CENTURY GREAT STRIDES WERE MADE IN ALL BRANCHES OF SCIENCE THE AMERICAN MOTOR CAR BEGAN TO ATTRACT ATTENTION NOT ONLY AT HOME BUT OVERSEAS AS WELL WITH THE ADVENT OF MODERN METHODS OF TRANSPORTATION IT WAS OBVIOUS THAT AN INCREASE IN TRADE WOULD FOLLOW TO SUPPORT THIS INDUSTRIAL PROGRESS MORE FACTORIES AND PLANTS WERE NEEDED ALONG WITH A HIGHLY ACCELERATED RATE OF EMPLOYMENT FOR THIS REASON MORE AND MORE SKILLED WORKERS WERE REQUIRED TO KEEP PACE WITH THE ECONOMY

EQUAL JUSTICE UNDER LAW HAS BEEN A BASIC PREMISE OF THE AMERICAN DREAM SOME PEOPLE DO NOT REALIZE THAT THE HIGH COURT OF THE UNITED STATES IS THE SOUNDING BOARD FOR THE CONSTITUTIONALITY OF ALL LEGISLATION APPROVED BY THE CONGRESS AND SIGNED BY THE PRESIDENT IN THIS WAY THE RIGHTS OF MINORITIES ARE PROTECTED REGARDLESS OF RACE CREED OR PLACE OF ORIGIN THERE ARE NO EXCEPTIONS TO THIS RULE ALTHOUGH THIS SYSTEM MAY NOT BE TO THE LIKING OF SOME IT HAS PROVED TO BE THE BEST THAT SO FAR HAS BEEN DEVISED

FACILITY OF EXPRESSION SHOULD BE EMPHASIZED WHEN JUDGING THE QUALITY OF ANY LITERARY FORM IF THE WORDS USED DO NOT CONVEY A LIFELIKE PICTURE OF THE EVENT OR SITUATION DESCRIBED THEN THE PURPOSE OF THE EFFORT HAS NOT ACHIEVED THE DESIRED RESULT DO NOT GENERALIZE BE BRIEF AND SPECIFIC THE BEST WRITING NOT ONLY HOLDS THE READERS INTEREST BUT SHOULD ALSO TAKE HIM AWAY FROM HIS PRESENT ENVIRONMENT AND BRING HIM TO THE LOCALE DEPICTED IN THE COMPOSITION THE BETTER THE WRITING THE MORE ENJOYABLE THE READING

JUST IN THE LAST FEW YEARS ENVIRONMENTAL POLLUTION HAS RISEN TO A HIGH PLACE ON THE LIST OF PUBLIC CONCERNS THIS IS THE NATURAL RESULT OF THE WORSENING STATE OF THE ENVIRONMENT FOUL AIR IN THE CITIES POLLUTED STREAMS AND LAKES IN THE COUNTRY UNUSABLE BEACHES ON THE SHORE AND EVERYWHERE MOUNTING HEAPS OF GARBAGE AND WASTE PEOPLE ARE INCREASINGLY AWARE OF THE HARMFUL EFFECTS OF POLLUTION ON THEIR BODIES SMOG AND OTHER AIR POLLUTION IRRITATES THE EYES AND AGGRAVATES RESPIRATORY AILMENTS AND DISEASES

THE WEST POINT ACADEMIC PROGRAM PROVIDES THE CADET WITH A BROAD BACKGROUND IN THE ARTS AND SCIENCES AND PREPARES HIM FOR FUTURE GRADUATE STUDY THE GRADUATE RECEIVES A BACHELOR OF SCIENCE DEGREE AND A COMMISSION AS A SECOND LIEUTENANT IN THE REGULAR ARMY A CADET WHO FOLLOWS ONE OF THE PROGRAMS WILL COMPLETE THE EQUIVALENT OF A MINOR AND IN SOME CASES WILL APPROACH THE REQUIREMENTS FOR A MAJOR AS DEFINED AT MANY INSTITUTIONS ADVANCED COURSES ARE AVAILABLE TO THOSE SHOWING EXCEPTIONAL ABILITIES NOW

THIS PAGE IS INTENTIONALLY LEFT BLANK

APPENDIX B

DIGITAL ENCODING SCHEMES (U)

B-1. (U) Introduction.—This Appendix describes selected digital encoding schemes used in various binary and voice equipment.

B-2. (U) Binary Signaling Methods.—Signaling methods are independent of code. Various methods have been devised to increase permissible data rates and provide self-clocked signals. The names of the signaling methods are loosely used in commercial texts. Therefore, it is important to know the exact scheme employed.

(U) Several signaling methods will now be described. For some of these methods, a signaling voltage is maintained for a full bit cell width. Other signaling methods use a pulse where the voltage is maintained for half a bit cell width or less. Both normal and inverted voltage levels are possible.

a. (U) Non-Return-to-Zero (NRZ).—A logic "one" is represented by a positive voltage and a logic "zero" by zero volts. The signal maintains its level between two or more of the same type bits, and transitions occur only when the data changes state. Please note that most of the data listed in Tables A-1 through A-5 of Appendix A assumes a Non-Return-to-Zero signaling method.

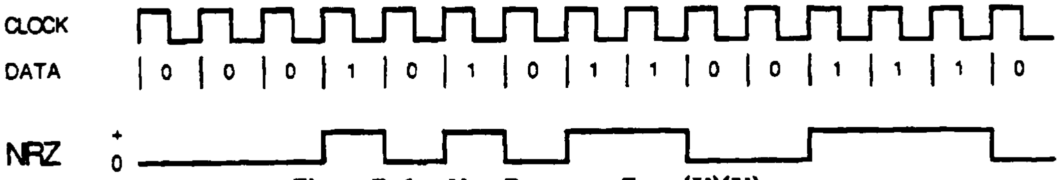


Figure B-1.—Non-Return-to-Zero (U)(U)

b. (U) Bipolar NRZ.—The signal is similar to standard NRZ except that a logic "zero" is represented by a negative voltage.

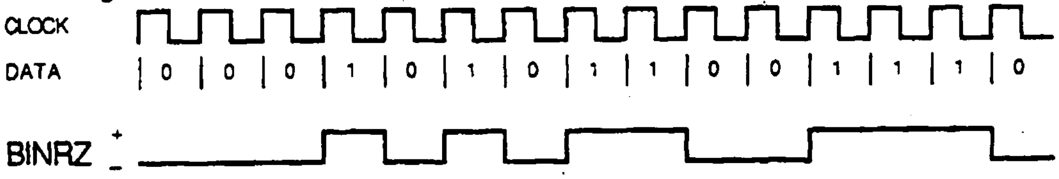


Figure B-2.—Bipolar NRZ (U)(U)

c. (U) Return-to-Zero (RZ) or Return-to-Bias (RB).—A logic "one" is represented by a positive pulse and a logic "zero" by zero volts. The transitions occur during each one bit.

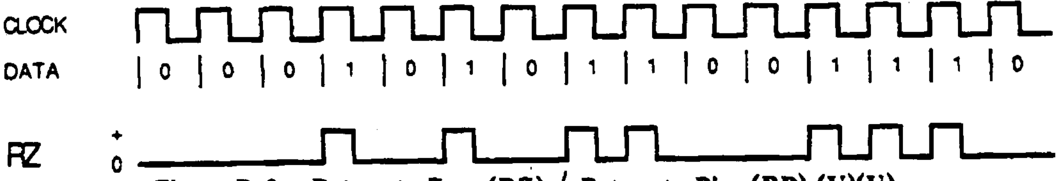


Figure B-3.—Return-to-Zero (RZ) / Return-to-Bias (RB) (U)(U)

d. (U) Bipolar RZ/Polar Keying.—A logic "one" is represented by a positive going pulse and a logic "zero" by a negative going pulse. The signal returns to zero between pulses. This self-clocked scheme requires two transitions per data bit.

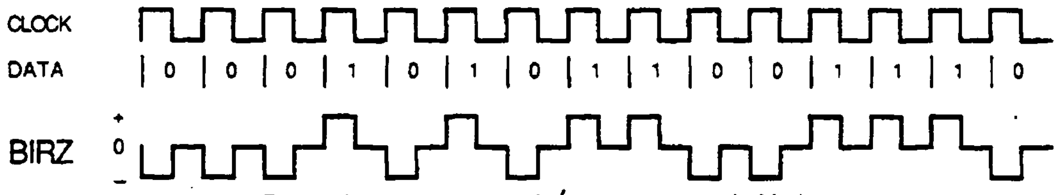


Figure B-4.—Bipolar RZ / Polar Keying (U)(U)

e. (U) Non-Return-to-Zero Inverted (NRZI).—The signal is inverted at each logic "one" at the center of the bit cell. The signal usually initializes at the beginning of a record so that repeating records will produce the same signal.

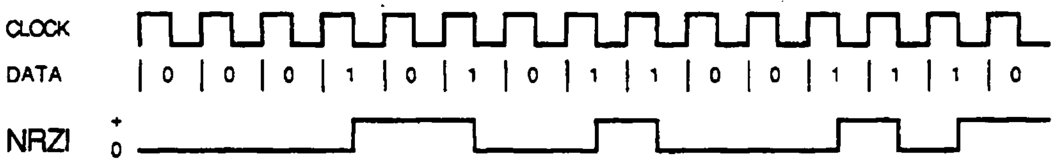


Figure B-5.—Non-Return-to-Zero Inverted (NRZI) (U)(U)

f. (U) Phase Encoding (PE).—Transitions occur at the end of each bit cell. For a logic "one", the transitions are positive going; for a logic "zero", they are negative going. For the transition to occur in consecutive logic "ones", a positive pulse is required in the first half of the bit cell. Consecutive logic "zeros" require the positive pulse in the second half of the bit cell.

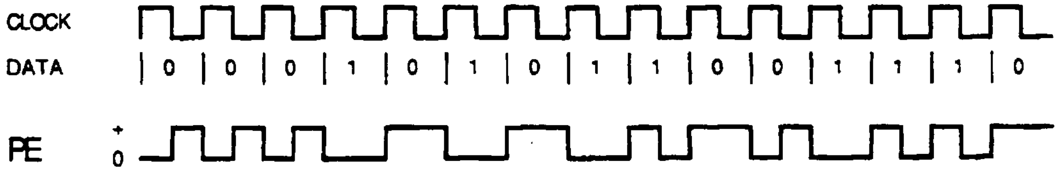


Figure B-6.—Phase Encoding (PE) (U)(U)

g. (U) Manchester Coding (MC).—The signal is identical to Phase Encoding, differing only in Manchester Coding leading by half a bit cell width.

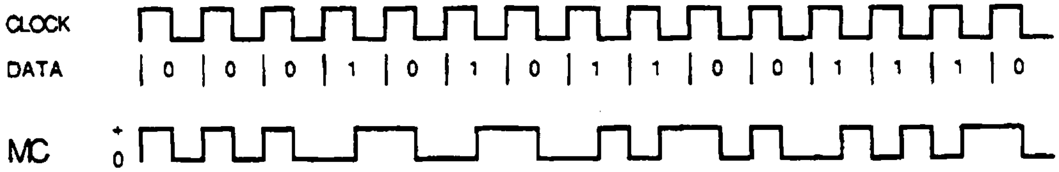


Figure B-7.—Manchester Coding (MC) (U)(U)

h. (U) Frequency Modulation and Run Length Limited.—The following coding schemes are used in magnetic recording on tape and disk. The data is encoded as described, then NRZI'd to reduce the required bandwidth. The reverse process is used when reading the data.

(1) *(U) Frequency Modulation (FM) (Single Density).*—A positive clock pulse is written at the beginning of each bit cell. A logic "one" inserts an additional pulse in the center of the bit cell. It is a self-clocking code with one or two changes per bit cell.

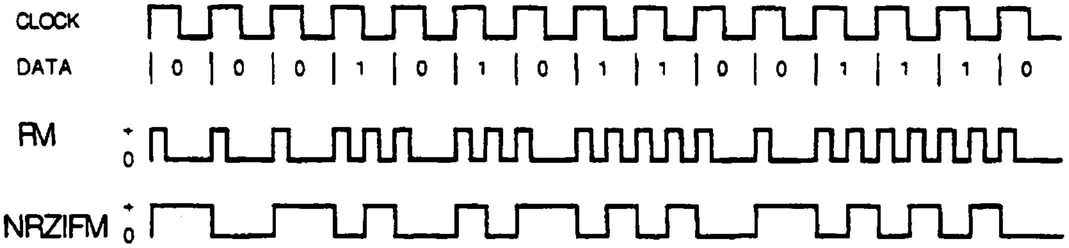


Figure B-8.—Frequency Modulation (FM) (Single Density) (U)(U)

(2) *(U) Modified Frequency Modulation (MFM) (Double Density).*—A logic "one" is represented by a positive pulse in the center of the bit cell. A clock pulse is written at the beginning of the bit cell only when no logic "ones" are present in the preceding or current bit cell. It is a self-clocking code with one change per bit cell.

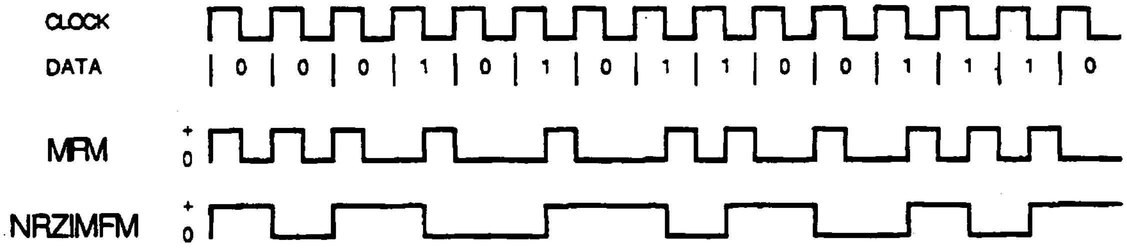


Figure B-9.—Modified Frequency Modulation (MFM) (Double Density) (U)(U)

(3) *(U) Modified Modified Frequency Modulation (MMFM).*—A logic "one" is represented by a positive pulse in the center of the bit cell. A clock pulse is written in the first half of the bit cell only if there are no data or clock bits in the preceding two cells and no logic "one" in the current cell. There is one transition per bit cell.

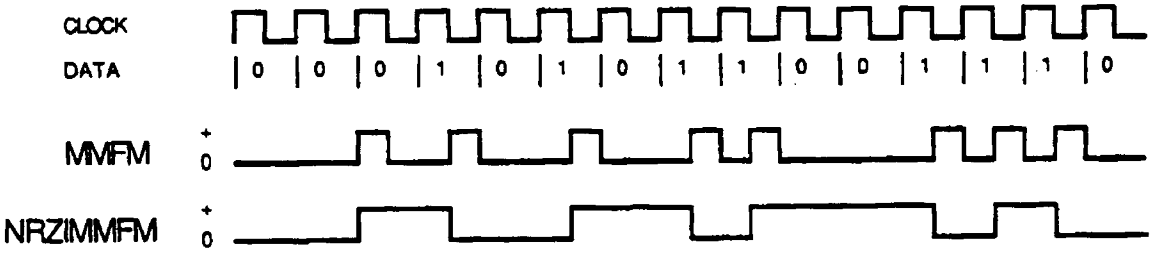


Figure B-10.—Modified Modified Frequency Modulation (MMFM) (U)(U)

(4) *(U) Run Length Limited (2,7) CODE (RLL).*—RLL translates consecutive groups of two to four bits in the incoming binary data into corresponding groups of four to seven bits. The RLL code insures there will be a minimum of two consecutive zeros but no more than six consecutive zeros in the RLL output. Since the number of bits in the RLL output is dependent upon the incoming data, the output is asynchronously clocked.

Binary Data	RLL Code
11	1000
10	0100
000	100100
001	001000
010	000100
0110	0100100
0111	0001000

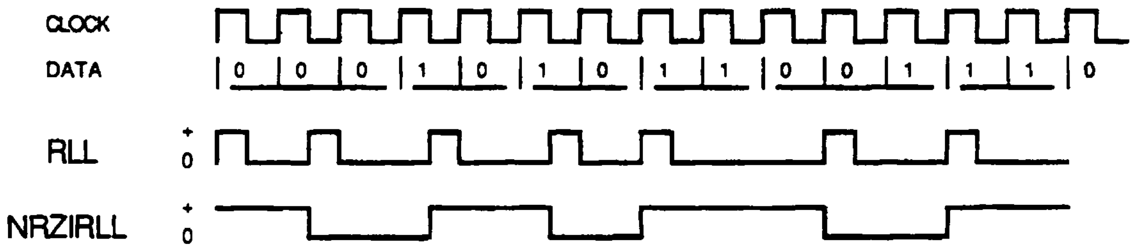


Figure B-11.—Run Length Limited (2, 7) Code (RLL) (U)(U)

(5) *(U) Group Coded Recording (GCR).*—Data translates consecutive groups of four bits in the incoming binary data into five-bit groups of asynchronously clocked output. The output code string contains no more than two consecutive zeros or eight consecutive ones.

Binary Data	GCR Code
0000	11001
0001	11011
0010	10010
0011	10011
0100	11101
0101	10101
0110	10110
0111	10111
1000	11010
1001	01001
1010	01010
1011	01011
1100	11110
1101	01101
1110	01110
1111	01111

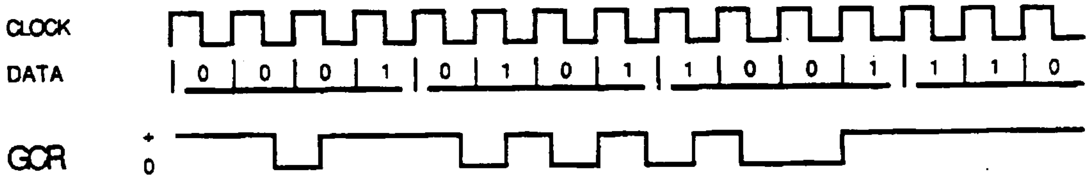


Figure B-12.—Group Coded Recording (GCR) (U)(U)

B-3. (U) Digital Voice Encoding.—Voice encoding schemes fall into two main classes: entropy encoding schemes and parametric encoding schemes (these are basically analysis/synthesis techniques). Examples of entropy encoding are pulse code modulation (PCM) and adaptive delta modulation (ADM). Examples of parametric coding are linear predictive encoding and channel vocoders. Each coding scheme will now be discussed.

a. (U) Entropy Encoding.

(1) *(U) Pulse Code Modulation (PCM).*—In PCM, the voice speech signal is sampled periodically at a rate somewhat in excess of twice the highest frequency component of the speech (Nyquist determined that to uniquely reconstruct a given signal from a set of samples, that signal MUST be sampled no slower than exactly twice the highest frequency component in the signal). These samples are quantized into discrete steps. For speech signals, the step size will either be uniform or follow a logarithmic relationship (as is used in speech companding systems). However in general, the quantizer may follow any rule. In addition, each quantized sample is encoded into a digital PCM word, with each word containing n bits. The more bits used in the PCM word, the smaller the quantization levels and consequently the better the original signal is reproduced. (Note the original signal is a sequence of PCM words.) There is a relationship between the number of bits n, used in a PCM word and the number of quantization levels N, that those n bits can uniquely specify. That relationship is $N=L^n$ where L is the total number of levels each bit can assume. For a binary signal, for example, each bit can assume only one of 2 values (i.e., each bit can assume a "0" or a "1" value), thus L=2. For a binary PCM code 10 bits long, 1024 different quantization levels can be represented (because $N=2^{10}=1024$). Normally these quantization levels are uniformly divided over a fixed voltage range (for example, +1 volt to −1 volt). The peak of the signal is adjusted as close as possible to the maximum value of the voltage range. For speech signals, 8 bit PCM to 16 bit PCM coding is used. PCM is a relatively high data rate transmission system. Rates commonly around 64 Kbits/second are typical (for example, a 4 kHz filtered speech signal sampled at an 8 kHz rate and encoded in an 8 bit PCM code). A block diagram of a typical PCM encoder is illustrated in Figure B-13.

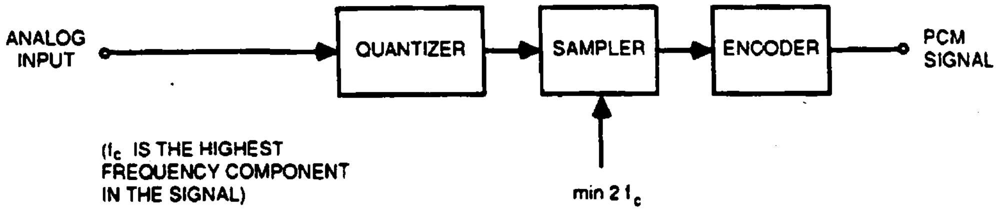


Figure B-13.—Typical PCM Encoder Block Diagram (U)(U)

(2) *(U) Adaptive Delta Modulation (ADM).*—Adaptive delta modulation is a low bit rate digital transmission system (when compared to PCM). However, in order to appreciate the advantages of ADM, a brief description of linear delta modulation is necessary. Linear delta modulation is considered the simplest form of differential pulse code modulation. In this system (see Figure B-14), the quantized error signal $\tilde{e}_f$ is a 1 bit signal (i.e., a two level signal represented by either a "+1" and "−1" or a "1" and "0") that is transmitted to a receiver having the same binary system as the transmitter so that each will use the same algorithm to produce the same approximation to the analog signal. Also, the step size k is fixed and its magnitude is selected to be typically small compared to the dynamic range of the input signal.

(U) The integrator in the block diagram of Figure B-14 consists of a linear predictive filter (one type will be discussed in the next section on Parametric Encoding) and a sample-hold network which produces an approximation to the input signal s(t). The receiver has a low pass filter which smooths the approximation $\hat{s}(t)$.

(U) Two types of distortion can occur with a linear delta modulation system. One type is called granular noise distortion and the second is slope overload distortion. Granular noise distortion occurs when the output of the quantizer is an alternating sequence of "+1's" and "−1's" (or "1's" and "0's"). It is caused by the step size k being too large for the instantaneous input signal level. This problem arises during silent portions of the speech signal. Slope overload distortion is caused by the inability of the encoder to follow the input signal when its slope-magnitude exceeds the ratio of step size to sampling period. This is normally detected when $\tilde{e}_i$ is sending a long string of either "+1's" or "−1's" (or either "1's" or "0's").

(U) Adaptive delta modulation has an algorithm which combats these two distortions. It uses the binary output signal $\tilde{e}_i$ to determine the step size. For example, when there are too many "+1's" or "−1's" (or "1's" or "0's") in a row, the step size will be increased in some specified way. When the binary output starts alternating, the step size will be decreased in some specified way. Many different adaptive delta modulation algorithms are possible, but the big advantage of adaptive delta modulation schemes is that only one bit per sample needs to be transmitted for the input signal to be reconstructed. Adaptive delta modulation systems typically operate at either 16 Kbits/sec or 32 Kbits/sec. A block diagram of an Adaptive Delta Modulation system is illustrated in Figure B-15.

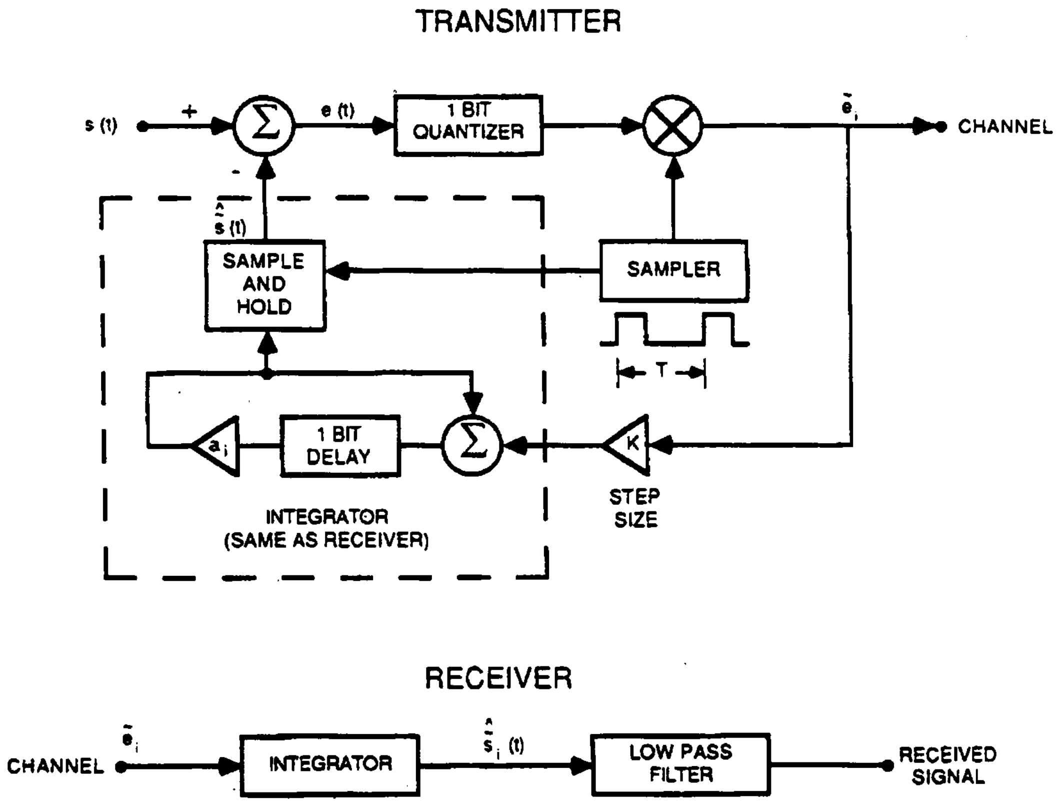


Figure B-14.—Linear Delta Modulation Block Diagram (U)(U)

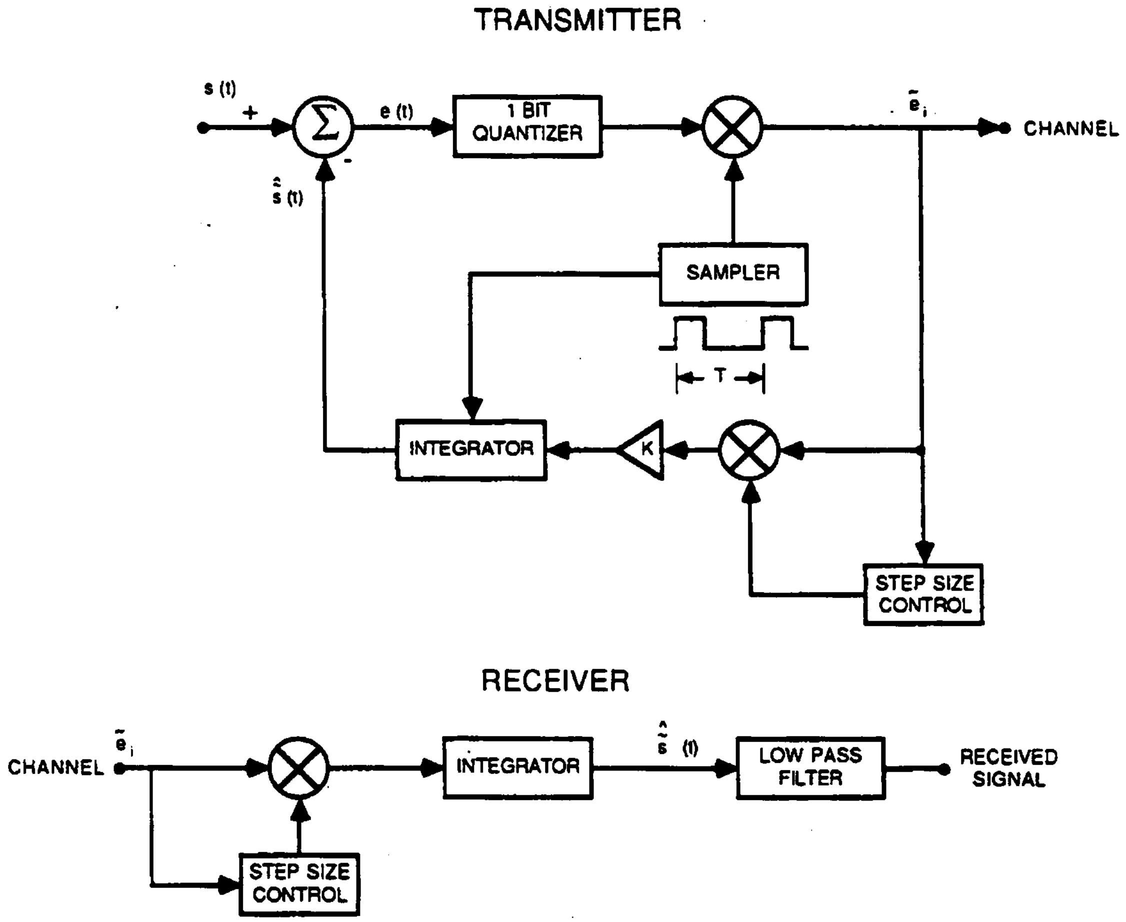


Figure B-15.—Adaptive Delta Modulation System Block Diagram (U)(U)

b. (U) Parametric Encoding.

(1) *(U) Linear Predictive Coding (LPC).*—For many types of information signals, speech included, the value of the signal at a given instant in time is correlated with its values at other instants in time, and hence represents redundant information. One theory of data compression in digital systems is based upon forming an error signal e_i between samples of an input sequence s_i and linear estimates of those samples $\hat{s}_i$, i.e., $e_i=(s_i-\hat{s}_i)$. Generally the estimate $\hat{s}_i$ of sample s_i is formed as a weighted linear combination of samples from some portion of the input sequence s_i. The weighting coefficients used for this estimate are computed from statistics of the sample sequence s_i in a manner which is optimum in some sense. If the input sample sequence is not stationary, the weighting coefficients must be updated periodically. For a linear Nth order linear predictor, estimates are formed by a linear combination of N weighted past samples, i.e.,

$$\hat{s}_i = \sum_{j=1}^{N} a_j s_{i-j}$$

where a_j is the weighting coefficient applied to the past sample s_{i-j}. Normally these weighting coefficients are updated every M input samples, where M is usually much larger than the order of the predictor. For example, with a 10th order linear predictor, the weighting coefficients will be updated approximately every 25ms. Also the error signal is transmitted at the same rate as the input sample sequence. Suppose the error signal is quantized to q bits and the N weighting coefficients are coded to w bits per coefficient. The number of bits needed to specify the M samples to the receiver is (Mq+Nw). The criterion by which the a_j's are determined is a minimization of the square difference between s_i and $\hat{s}_i$. See Figure B-16 for a block diagram of a typical Linear Predictor system.

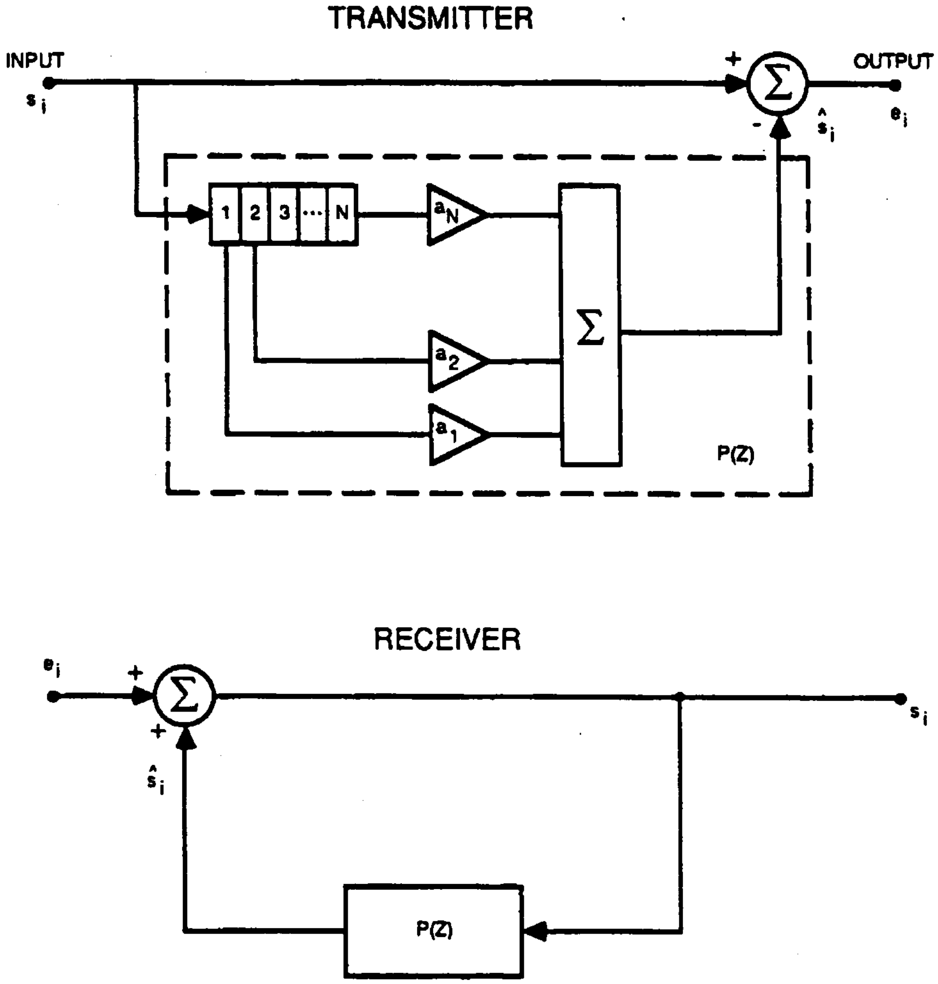


Figure B-16.—Typical Linear Predictor Block Diagram (U)(U)

(U) For practical digital transmission, the error samples and the predictor coefficients are quantized to the fewest possible levels. The receiver of the prediction system uses this data to reconstruct estimates of the sample sequence of the original signal. If care is not exercised, quantizing noise may accumulate in the sample sequence.

(U) Typical parameters for an LPC system are:

Size of the linear predictor: N = 10
Time between coefficient update: 25ms.
Transmission data rate: 2400 bits/sec.
Quantizing level of predictor coefficients

pitch	: 7 bits
energy	: 5 bits
synch.	: 1 bit
coeff. 1–4	: 5 bits/coeff.
coeff. 5–8	: 4 bits/coeff.
coeff. 9	: 3 bits
coeff. 10	: 2 bits
	54 bits/frame

(U) Note that there are many variations of LPC encoders which can be found in references on digital speech processing systems.

(2) *(U) Channel Vocoder.*—The name **VOCODER** (for **VOice CODER**) has become a generic term commonly applied to analysis-synthesis systems in which the excitation and system functions are treated separately. There are a number of different versions and variations of vocoders including channel, formant, linear predictive coding (as discussed in the previous section), correlation, phase, voice excited, and orthogonal function, each having both advantages and disadvantages (see references on speech analysis/synthesis in Section F–3*e* for further details). Since the channel vocoder has been the subject of a number of investigations, a fair degree of sophistication in the implementation has been obtained. A brief description of the channel vocoder follows to give an idea of how vocoders work. The block diagram of a typical Channel Vocoder analyzer is illustrated in Figure B–17.

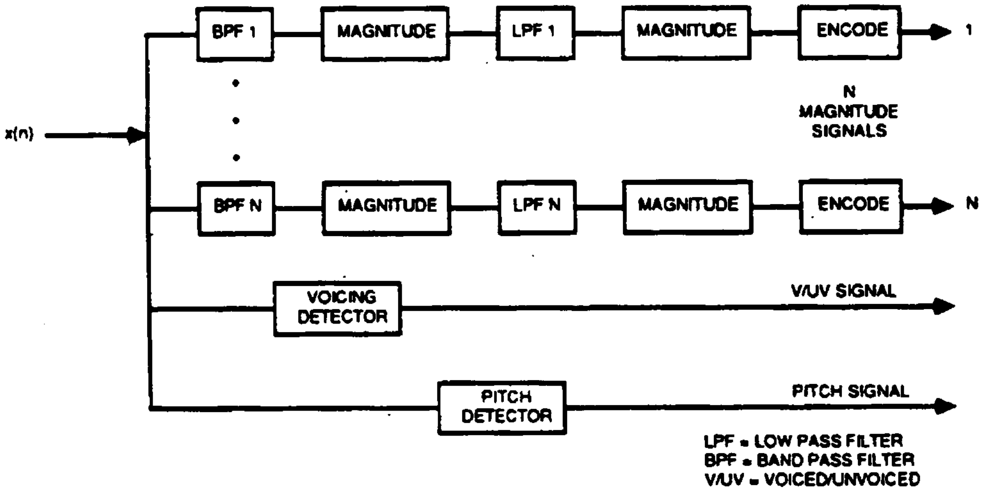


Figure B–17.—Channel Vocoder Analysis Block Diagram (U)(U)

(U) The analyzer consists of a bank of channels with analysis frequencies distributed across the speech band of interest (nominally 300 Hz — 3000 Hz). Each channel detects the amount of energy in its frequency range and encodes it. This technique essentially preserves the short term amplitude spectra of the speech which for speech perception is an important characteristic. To provide proper excitation to the speech signal, the channel vocoder also provides an analysis component for determining whether the speech is voiced or unvoiced, and if it is voiced, the fundamental frequency (or pitch) of the speech signal is determined. This voiced/unvoiced parameter makes the speech signal sound more natural during synthesis.

(U) For synthesis (illustrated in Figure B–18), the encoded filtered levels determined during analysis control the amplitude of the contribution of a particular channel while the voiced/unvoiced signal controls the structure of the synthesized speech. The original channel vocoder developed by Dudley in 1939 had 10 channels; however, vocoders today are typically 15 channels. Typical data rates for 15 channel vocoders range from 1200 bits/sec to 9600 bits/sec with roughly 600 bits/sec devoted to pitch and voicing information and the remaining information devoted to channel signals.

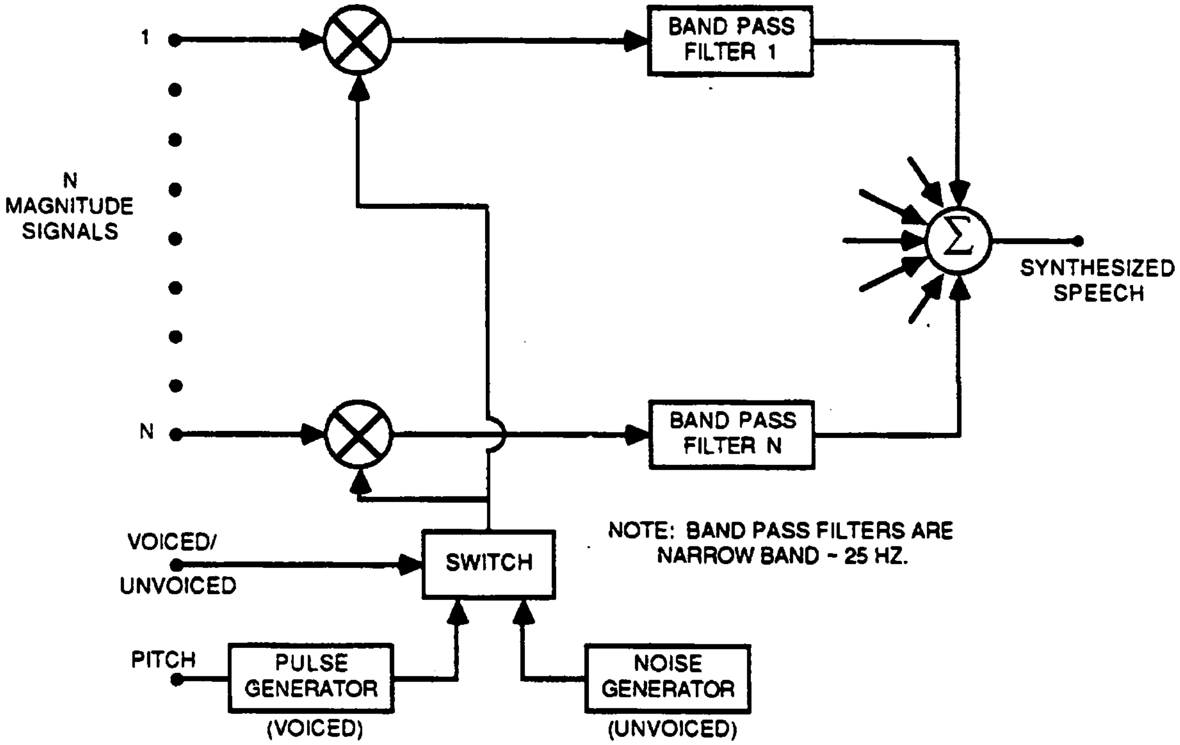


Figure B-18.—Channel Vocoder Synthesis Block Diagram (U)(U)

APPENDIX C

SUPPLEMENTARY EQUIPMENT REQUIREMENTS (U)

C-1. (U) Introduction.—In this appendix various equipment are described that are used to perform TEMPEST analysis. This equipment includes oscilloscopes, raster generators, an Analog Binary Correlator (ABCOR), digital storage/display devices, analog storage scopes, sampling oscilloscopes, signal monitors, spectrum analyzers, sonagraphs, filters and various signal recording equipment.

C-2. (U) Oscilloscope.—This is by far the single most useful device in establishing correlation. Generally, the "A-scope" display which furnishes a time vs. signal amplitude presentation provides the best display. For simple serial signals, a single time base oscilloscope may be adequate. Dual beam oscilloscopes are necessary in many applications especially if photographic recordings are to be made of single trace sweeps of the correlated signal. They are also necessary for signals which have any type of burst characteristic. In general, a dual beam, dual time base oscilloscope configuration provides the versatility necessary to optimize any "A-scope" display.

(U) Besides the configuration, the oscilloscope bandwidth and phosphor decay time are also important. The oscilloscope bandwidth must be greater than the output signal bandwidth of the detector being used. Since dual beam oscilloscopes are available with 400 MHz bandwidth and single beam oscilloscopes are available with 1 GHz bandwidth, this parameter is generally no longer a limiting factor in a detection system. When using either a nontunable detection system for testing data rates above 400 MHz or a tunable detection system for testing data rates above 200 MHz, a 1 GHz bandwidth oscilloscope may be required.

(U) The writing speed and decay time of the CRT are two important parameters for TEMPEST testing. High writing speed provides detectability of low duty cycle correlated signals which may otherwise go undetected. For general applications, a CRT with P31 phosphor would be desired for maximum visual brightness. For low rate CRT sweeping, a P7 phosphor with its slow decay time is often a better choice than a variable persistence storage oscilloscope.

C-3. (U) Raster Generator.—Raster generators have been found to be very useful in TEMPEST testing. By connecting the output of a raster generator to an oscilloscope or a monitor display, the time history of a signal can be viewed. The horizontal sweep rate of the oscilloscope is normally set to display, at a minimum, one character or period of the monitor signal. The vertical sweep rate of the generator is adjusted so that a succession of emanations appear one beneath the other. The intensity of the oscilloscope beam is modulated so that signal peaks appear as bright spots. Alternatively, the signal may be inverted so that a peak may be represented by a dark spot. Examples of rastered signals are presented in Figure C-1.

(U) An oscilloscope containing a P7 long persistence phosphor (or even a variable persistence phosphor) cathode-ray tube will retain the raster image longer. In this manner, many occurrences of an emanation can be "stored on the CRT", thus giving the analyst a large sample of emanations for comparison with the monitor. Often these repetitions enable the analyst to see a trend in the emanations which may not be apparent from viewing them one at a time on an A-scope display.

(U) Commercially available raster generators are capable of other functions. All will serve as a video amplifier with an auxiliary audio output. They have built-in pulse stretchers and a provision for inverting the signal. Some have high-pass and low-pass filters. Of course, all have essentially the same raster generating capability. The bandwidth of these equipment range from 5 MHz to 30 MHz.

C-4. ~~(C)~~ [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

Figure C-1.

~~(C)~~

~~(C)~~

1.
2.
3.
4.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

~~(C)~~ [redacted]

~~(C)~~ [redacted]

~~(C)~~ [redacted]

C-5. (U) **Digital Storage/Display Devices.**—Digital storage/display devices include transient digitizers and digital storage oscilloscopes. A transient digitizer incorporates an analog to digital converter (ADC), digital storage, and optionally a digital to analog converter (DAC) with output for an analog display. A digital storage oscilloscope performs the function of a transient digitizer except that the analog display is included within the instrument. Some of these devices are capable of recording the stored data on magnetic media.

(U) Typically these devices work in the following manner. The input signal is amplified and the resulting waveform is sampled and digitized by an ADC before being stored. A DAC changes this stored signal back to its analog form before it is amplified and applied to the vertical axis input of the cathode ray tube.

(U) The accuracy of a digital storage oscilloscope is usually worse than its resolution since it includes errors due to resolution of the ADC and the non-linearity of the amplifiers. Storage oscilloscopes may typically have resolutions of the order of 0.025% and accuracies of 0.25%. Some oscilloscopes have a dot joining feature which use lines to join the sampled data of the waveforms.

(U) Some digital storage instruments buffer the input signal information prior to final storage. This has the advantage of reproducing the display on either an expanded or reduced time base, and further offers the capability of utilizing pretrigger viewing. With pretrigger viewing, the waveform can be viewed both before and after the triggering event.

(U) Other digital storage instrument advantages include signal processing features like averaging a number of snapshots of the input signal to reduce the effects of noise, performing calculations on the waveform parameters, or outputing the waveform data over RS-232 or IEEE-488 standard interfaces.

(U) Within digital instruments, there are two main techniques of quantizing signals and the technique implemented has a direct effect on the application of the instrument. Only "real-time·sampling" digital storage oscilloscopes can capture single-shot signals. There are two alternative "equivalent sampling" methods, but both require many repetitions of the input signal. In exchange for that requirement, the "equivalent sampling" methods have the ability to measure signals more than ten times faster than can be done with "real-time sampling."

(U) For "real-time sampling" digital storage oscilloscopes, there is a "useful storage bandwidth" specification. It expresses the highest frequency sine wave that can be captured in a single sweep and displayed so that waveform measurements can be taken. Both the digitizing rate (how often the oscilloscope takes samples) and the display reconstruction technique (how the oscilloscope displays what is in its memory) must be taken into account in the "useful storage bandwidth." The ADC is usually the limiting component of a digital storage oscilloscope, and its speed determines the frequency response of the instrument.

(U) The digitizing rate required to capture high frequency single events is approximated by:

$$\text{Digitizing Rate} \geq \frac{f}{180} \cos^{-1}\left(\frac{x}{100}\right)$$

where:

f = highest frequency component in the signal, usually the video bandwidth of the detection system, and

x = percent accuracy of the maximum amplitude of a sine wave.

To achieve a 3 dB accuracy, a minimum sampling rate of four times the signal bandwidth is required.

(U) For digital storage oscilloscopes using "equivalent time sampling", the bandwidth specification is "equivalent time bandwidth". This represents the highest frequency signal that can be stored and displayed with less than a 3 dB signal amplitude loss.

(U) As the digitizing rate must be at least 2f but normally higher, memory capacity is an important concern. The digitizer must have sufficient memory to record the full signal of interest at whatever digitizing rate is required. Meeting measurement accuracy requires not only a high digitizing rate but also high resolution in the digitizer. The number of bits of resolution is defined by:

$$\text{Bits} \geq \log_2\left(\frac{100}{100 - x}\right)$$

where: x = percent accuracy of the amplitude measurement (full scale).

(U) For example, theoretically to achieve 95% accuracy for "full scale measurements", at least a 5 bit digitizer is required. However, for TEMPEST applications, where signals use the full range of the A/D converter, a minimum of 8 bits is necessary to accurately capture the emanation. For lower amplitude signals, more bits are required to accurately capture the signal. As a general rule, the lower the signal amplitude, the more bits are necessary for high resolution.

C-6. ~~(C)~~ [redacted]

~~(C)~~ [redacted]

a. ~~(C)~~ [redacted]

b. ~~(C)~~ [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

c. ~~(C)~~ [redacted]

C-7. (U) Analog Storage Oscilloscopes.—A non-storage oscilloscope needs a relatively high frequency periodic signal in order to display a steady trace. The persistence of the screen can vary from a few milliseconds to a few seconds depending on the type of phosphor. Storage oscilloscopes are used primarily to display transient events but they are also used for signals with very low repetition rates in which, on a conventional oscilloscope, the first bit of the trace will begin to fade before the sweep is finished.

(U) Analog storage oscilloscopes employ a method of integrating the signal intensity. This, in effect, is a method of increasing the persistence of the phosphor to many seconds. The basic mechanism used in this type of storage oscilloscope is "charge storage" on some form of insulating surface such as magnesium oxide. A sheet of this material is placed in the path of the electron beam in the CRT. The electrons strike the surface and leave charged areas in the shape of the waveform. After this image is stored, a source of low velocity electrons is placed in such a way that it floods the storage surface. The electrons are drawn through the charged areas, but are deflected everywhere else. Circuitry incorporated in the oscilloscope generates the various control pulses necessary to erase the target voltages to store the signals.

C-8. (U) Sampling Oscilloscope.—The sampling oscilloscope has potential for use in TEMPEST signal analysis. It permits sampling successive portions of a periodic waveform once per selected number of occurrences of the waveform (see Figure C-3). The waveform will be reproduced at a much slower than real-time rate. This has several advantages and applications. Modulated high frequency carriers may be sampled and the entire envelope displayed. Frequencies may range up to several GHz. Repetitive signals which occur too rapidly for available recording capability may be sampled and "read out" at a slower rate. Plug-in units are available to allow a storage oscilloscope to become a sampling storage oscilloscope.

(U) The disadvantages of the sampling oscilloscope are more complex operating procedures and the requirement for a repetitive signal.

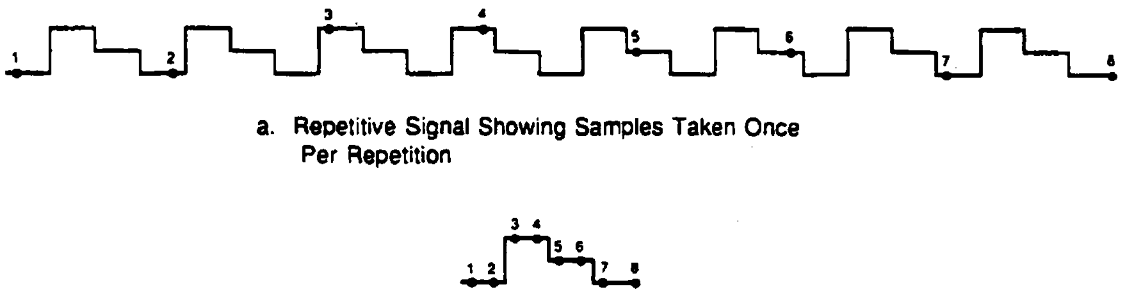
C-9. (U) Signal Monitor.—This device is similar to the spectrum analyzer described in Section C-10. It is exceptionally useful for viewing the intermediate frequency (IF) output of a receiver. The monitor display is similar to an oscilloscope display. The demodulated IF signal amplitude is connected to the vertical axis of the monitor and a linear ramp function calibrated in frequency is connected to the horizontal axis. The frequency display can be varied so that all signals within the IF pass-band may be displayed or it may be expanded and repositioned to allow more detailed viewing of a particular signal. The rate at which the IF pass-band is swept is usually fixed at a low frequency of some tens of Hz. Because of this limitation, the signal monitor is best suited for indicating the presence of a sine wave carrier or a wideband noise-like signal, neither of which may be observed easily at the demodulator output. The monitor is not useful for indicating the presence of impulsive signals or variations in the envelope (modulation). The only exception is when the signal's repetition rate is very close to the horizontal sweep rate, then the signal will appear stationary or slowly sliding. A typical sideband envelope is presented in Figure C-4.

(U) Specifications on these signal monitors include the sweep width (which should include the widest bandwidth of the receiver to be used), the sensitivity (which indicates the minimum detectable signal according to some usually unspecified criterion), and the resolution (which specifies the frequency separation between two carriers required to determine that two carriers are actually present and not just one). Of course, the center frequency of the monitor must be the same as the receiver's IF.

(b) (1)
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

[redacted]

Figure C-2



a. Repetitive Signal Showing Samples Taken Once Per Repetition

b. Reconstructed Signal as Seen on CRT

Figure C-3.—Sampling Oscilloscope Operation (U)(U)

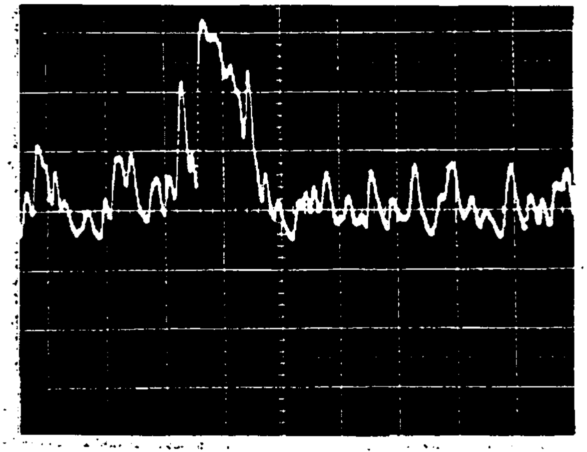


Figure C-4.—Signal Monitor Display (U)(U)

C-10. (U) Spectrum Analyzers.—Spectrum analyzers have long been a useful tool in the evaluation of electromagnetic interference (EMI). They are also valuable for preliminary design troubleshooting and TEMPEST testing. In TEMPEST, the spectrum analyzer's ability to display wide frequency spans provides easy and convenient capability for locating RED signal related spectral "hot spots." For example, using properly matched high-pass filters in conjunction with the spectrum analyzer, the conducted spectrum of an EUT output line can be examined. If the output of that line is a digital serial signal, the waveform will be trapezoidal. By measuring the period and transition times of the bits, a projection can be made of the anticipated envelope of the spectrum resulting solely from that signal and its associated line driver. This can then be compared with the displayed spectrum of the analyzer in order to examine contributions to the overall spectral components of the signal line.

(U) To be useful in making measurements in the frequency domain, the analyzer must be capable of making quantitative measurements. Specifically, an analyzer must do the following:

1. make absolute frequency measurements;
2. make absolute amplitude measurements;
3. operate over a large amplitude dynamic range;
4. have high resolution of both frequency and amplitude;
5. have high sensitivity; and,
6. provide a means of observing, preserving and recording its output in a convenient and rapid manner by using either a variable persistence display or a digital storage oscilloscope.

(U) Frequency readout accuracy depends upon the tuning and readout techniques employed, as well as the stability of the frequency reference within the spectrum analyzer. Dial indicators nominally provide 1% of full scale of frequency accuracy. Synthesized local oscillators allow accuracies to ±4 Hz at 1500 MHz in narrow frequency spans. When the spectrum analyzer is used in conjunction with a tracking generator, accuracy much better than 1% can be achieved by counting the generator output.

(U) The spectrum analyzer should be calibrated for amplitude measurement. This means the spectrum analyzer indicates to the user what the log/reference level or linear sensitivity is regardless of control settings. Either a warning light or a CRT message indicates an uncalibrated condition, making operation of the analyzer easy and foolproof.

(U) Microprocessor controlled analyzers feature built-in calibration routines which account for changes in analyzer controls such as the resolution bandwidth and the RF attenuator.

(U) The dynamic range of a spectrum analyzer is defined as the difference between the input signal level and the average noise level or distortion products, whichever is greater. Hence, dynamic range can be either distortion limited, noise limited or display limited. Microprocessor controlled analyzers can be set to ensure that distortion products of on-screen signals will be below a certain level.

(U) Frequency resolution is the ability of the analyzer to separate signals closely spaced in frequency. The frequency resolution of an analyzer is a function of three factors:

1. minimum IF bandwidth—can range down as low as 1 Hz for some spectrum analyzers;
2. IF filter shape factor—specifies the selectivity of the IF filter (can be defined as the ratio of the 60 dB bandwidth to the 3 dB bandwidth); and,
3. spectrum analyzer stability—the residual FM (short term stability) should be less than the narrowest IF bandwidth. If not, the signal will drift in and out of the IF pass-band.

(U) Amplitude resolution is a function of the vertical scale calibration. Typically, both log calibration (for observing large amplitude variations) and linear calibration (for observing small amplitude variations) are available display options of spectrum analyzers.

(U) Sensitivity is a measure of an analyzer's ability to detect small signals and is often defined as the point where the signal level is equal to the noise level or $(S+N)/N=3dB$. Since noise level decreases as the bandwidth is decreased, sensitivity is a function of bandwidth. The maximum attainable sensitivity ranges from −150 dBm to −120 dBm.

(U) Both high resolution and sensitivity require narrow bandwidths and consequently slow sweep rates. Because of these slow sweeps, both digital display and variable persistence oscilloscopes are virtually indispensable in providing a bright, steady, flicker free trace.

(U) The only way to simultaneously avoid spurious, multiple, harmonic and image responses is to filter the RF signal through a tracking preselector. This is an electronically tuned band-pass filter that automatically tracks the analyzer's tuning. A preselector improves the spurious free range of the analyzer from 70 dB to 100 dB.

(U) On low frequency analyzers, adaptive sweep effectively speeds the measurement times. For very low sweep times (required when using the 1 Hz bandwidth), adaptive sweep allows the scan to sweep rapidly when no signals occur and slow down when a signal is above a preset level. The measurement time savings can be greater than 20:1.

(U) In modern spectrum analyzers with FFT processors, many conventional analog circuits (intermediate frequency, detection, and display) have been replaced by their digital signal processing counterparts. Freedom from analog drift or calibration and the ease of building a programmable instrument with convenient digitally stored spectrum displays are two advantages of the digital approach. By making it possible to process an entire part of a spectrum in parallel simultaneously, the FFT makes a unique contribution to spectrum analysis.

(U) The local oscillators within conventional spectrum analyzers must be swept slowly, so signals at each input frequency have enough time to pass through the IF filter and be detected before the next analysis frequency is chosen. So when narrow analysis bandwidths are desired, the sweep rates must be reduced and overall measurement times must increase. Spectrum analyzers with FFT IF structures can usually make comparable narrow bandwidth measurements approximately two orders of magnitude faster than comparable analog instruments.

(U) Typical spectrum analyzers might make use of complex 1024 point FFTs which allow sweep rates that are about 200 times faster than those possible with the analog approach. The FFT promotes an additional feature, that being real-time operation (the ability to monitor a part of the spectrum continuously) with no gaps in analysis intervals because the processor can calculate the entire transform in less time than it takes to gather the next set of input data samples for analysis.

(U) The measurement capability of a spectrum analyzer can be greatly enhanced by programming a desktop computer to control instrument functions and record frequency and amplitude information. Data can be gathered and processed into a variety of formats very rapidly.

C-11. (U) **Sonagraph.**—The Sonagraph is a proprietary device (Kay Electric Co.) which is essentially a spectrum analyzer for application in the audio frequency range. It records a sample of the signal to be analyzed, and as this sample is repetitively played back, a narrow bandwidth filter is swept through the frequency range. The amplitude of the signal energy in the pass-band of this filter is detected and plotted on a three-dimensional plot of time (x) vs. frequency (y) vs. energy (z). See Figure C-5 for an example of a Sonagraph of a speech signal.

C-12. (U) **Filters.**—The purpose of using filters in TEMPEST analysis is to improve the signal-to-noise ratio of detected signals. The two primary classifications of filters are passive and active. Several different types of filters exist within each of these categories. In addition, there are a number of other special signal shaping and enhancing devices which will be discussed in the digital filter section.

a. (U) Passive Filters.—Passive, linear filters are the filters most frequently used in TEMPEST signal processing. Their networks consist of discrete and/or distributed resistance, capacitance and inductance. They produce very low noise, require no power supply and have wide dynamic range. The types of filters are band-pass, band-reject, high-pass and low-pass. They are used in TEMPEST receivers to produce the required sensitivity and overall detection system bandwidth of the TEMPEST specifications. Some receivers with wide

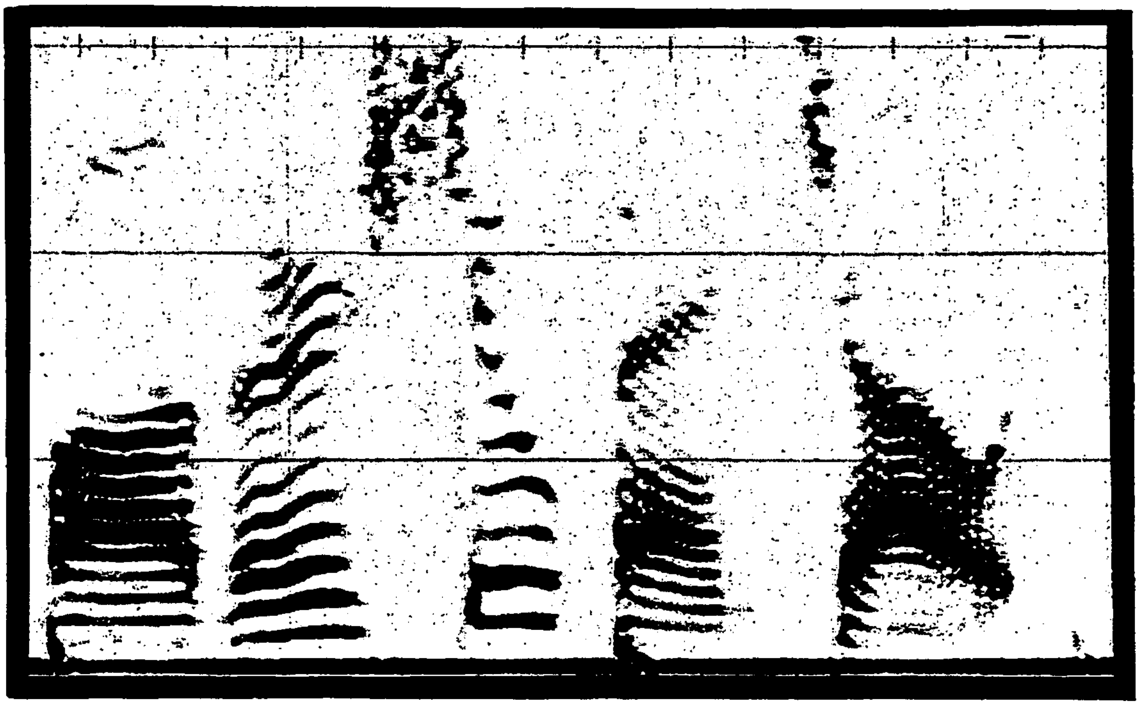


Figure C-5.—Sonagraph of a Speech Signal (U)(U)

bandwidth RF circuits may require additional filtering between the transducer and RF input to eliminate strong in-band signals from overloading the RF amplifier. High-pass filters are frequently used to prevent this problem during tests of AC power lines and active digital signal lines. Since passive filters are difficult to make adjustable over a wide frequency range, a set of selectable fixed frequency high-pass filters are usually employed to minimize overload problems.

(U) Passive filters are also used with low noise wide bandwidth amplifiers to produce required nontunable detection system bandwidths. A large selection of RF filters are commercially available because they have been developed to meet the requirements of HF, VHF and UHF radio and other RF systems in the 5 MHz to 100 MHz range. Band-pass filters are typically available with standard pass-bands of 1, 4.5 and 6 MHz in the 30 to 300 MHz and 500 to 900 MHz ranges. Wide bandwidth, high selectivity band-pass filters are available in the same frequency ranges. Their wide pass-bands and sharp rolloff characteristics are obtained by cascading appropriate low-pass and high-pass filters. Tunable preselect type band-pass characteristics conform to specified communication bands, i.e. FM and TV. These RF filters are generally adaptable for TEMPEST applications but the user should determine their complete stop-band performance in the frequency range of interest if attenuation is required more than two octaves above the cutoff frequency. Do not assume that the minimum specified rejection extends to 1 GHz.

b. (U) Active Filters.—Continuously tunable electronic filters are available with operating frequency ranges from DC to 3 MHz. These filters provide the same performance characteristics as passive linear filters with the added capability of a wide adjustment range, including digital programming. Their primary TEMPEST application is post detection filtering since their noise contribution would degrade detection system sensitivity elsewhere. They have excellent dynamic range and linearity, and at lower frequencies provide significantly better performance than passive filters. Their filtering characteristics can be made essentially independent of either source or load impedance (whereas passive filters are very much dependent upon their termination impedance). They can be configured by simple switching from low-pass to high-pass and can be cascaded without significant interactions for band-pass or band-reject operation. Typically, active filters are designed to have a high input impedance, 50-ohm output impedance and 0 dB voltage gain. As in the case of RF filters, the user is cautioned to evaluate the active filter stop-band performance above the operating frequency signals that may leak around the active circuit.

(U) Linear active and/or passive filters are employed in TEMPEST analysis for the primary purpose of enhancing the correlated portions of the A-scope waveform or raster display. This is most often accomplished by bandlimiting the ambient noise to the point of optimizing the signal-to-noise ratio. Filter transfer functions must be selected based upon both amplitude flatness, rolloff and linear phase response. A good filter transfer function for distortion free filtering of impulsive signals is the Bessel (or maximally flat phase) filter. The Bessel filter, however, has relatively poor rolloff and pass-band flatness characteristics. For TEMPEST applications, the Butterworth transfer function provides a good compromise between selectivity and signal distortion. Butterworth filters exhibit maximally flat pass-bands, have moderately sharp rolloff and a slightly non-linear phase response that causes less overshoot and ringing of impulse signals than the Chebyshev or Elliptic filters. Chebyshev or Elliptic filters feature very fast rolloff near cutoff, but exhibit a non-linear phase characteristic that can cause significant overshoot and ringing of impulsive signals. Gaussian response filters will also provide excellent pulse response. Poor rolloff characteristics can be improved by increasing the number of poles in the filter.

c. (U) Digital Filters.—Digital filters are far more versatile than hardware filters. Finite Impulse Response (FIR) and Infinite Impulse Response (IIR) filters can be designed to perform the same functions as hardware low-pass, high-pass, band-pass and stop-band filters. Additionally, digital filters can be designed for special applications like adaptive filters (filters that change their parameters as the shape of the signal or noise changes), matched filters (filters like Kalman filters that are designed to find a specific shaped signal buried in other signals or noise), comb notch filters (designed to filter out a primary frequency and all its harmonics such as a power line signal) and other applications. Digital filter responses can be easily changed by changing the parameters of the equations generating them. The main disadvantages of these filters are that they are not real-time filters and most often are programmed on a digital computer. This may not be a problem if the detected emanation is going to be analyzed in the laboratory but can limit their use for on-site analysis.

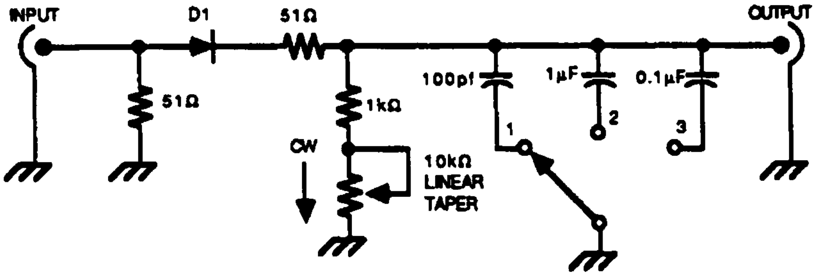
(U) One digital filter application that is often needed in TEMPEST is the comb notch filter which is used to eliminate power line noise. Sharp notch filtering is provided at the harmonic frequencies of a repetitive interfering (noise) signal, while TEMPEST emanation signal components are passed without attenuation. The comb notch filter is realized by digitizing the signal plus noise waveform under the control of a reference (sampling) clock which is harmonically related to the repetitive interfering signal. The "signature" of the interfering signal is maintained and updated in a recirculating memory. These signal components are basically subtracted from the total TEMPEST emanation, providing significant noise reductions. Available hardware is limited to a bandwidth of 10 kHz with capability of tracking interference signals between 40 and 80 Hz. Notch attenuation is approximately 70 dB at the fundamental (reference) frequency with a rolloff of about 6 dB/octave to 10 kHz. Notch bandwidth is selectable from 0.3 to 30 Hz. The device's primary application is the elimination of power line related interference in audio systems.

C-13. (U) Pulse Stretcher.—A pulse stretcher capability is often included in a video amplifier or raster generator. There are times when the signal to be analyzed is of very short duration and the time between pulses is much longer than the duration of one pulse (implying a very short cycle). In these cases, the pulse may be stretched by means of a diode-resistor-capacitor circuit as shown in Figure C-6.

(U) The circuit works in the following way. The diode permits the capacitor to be charged from the low impedance source during the rise-time of the pulse. The diode is reverse biased when the input signal is finished, thus presenting a very high resistance to the capacitor. The capacitor discharges slowly through the variable resistor and high impedance load. The rise-time of the pulse stretcher is fairly faithful because of the low diode resistance and capacitor time constant. The fall-time, however, is characteristic of an RC low-pass filter. The high impedance load may be either an oscilloscope or a high impedance amplifier input. The output will be substantially lower in amplitude than the input. Care must be taken that the stretching time does not cause successive signals to overlap. The charge and discharge time constants should be selected in accordance with NSTISSAM TEMPEST/1-91*.

(U) A pulse stretcher can also take the form of a one-shot, or monostable multivibrator. The pulse width is easily adjustable but some control over the triggering threshold is required.

C-14. (U) Signal Recording Equipment.—There are two main reasons for recording emanations. One is to make a permanent record of the emanation so it can be documented in a report. However, the most important reason is to be able to study the signal to determine if it is compromising.



SWITCH POSITION	RANGE OF STRETCHING (USE POTENTIOMETER)
1	100ns – 1.1μs
2	1μs – 11μs
3	10μs – 110μs

DO NOT LOAD OUTPUT WITH LESS THAN 100 KILOHMS
D1: HP 2305 OR EQUIVALENT

Figure C-6.—Pulse Stretcher Circuit (U)(U)

* This section references information contained in the current version of NSTISSAM TEMPEST/1-91. For specific details see that document.

(U) No matter what the reason for recording the signal, the most important criterion to be met is to accurately capture the signal. Accuracy must have first priority or all effort expended on the recorded signal, even the recording effort itself, will be wasted. The hardest statement to make in TEMPEST analysis is "The signal isn't compromising." If an emanation's correlating properties are lost due to the recording process, the above statement based on analysis of the recordings is false and misleading.

(U) The parameter that most influences the choice of signal recording equipment is the bandwidth of the signal. The signal bandwidth is generally determined by the detection system bandwidth. Another influencing factor in selecting the signal recording equipment is the purpose for making the recordings. If, for example, the only purpose is to document the detected signal shape, then a visual display (i.e. hardcopy) or a photograph is all that is required. If however, detailed analysis is the main purpose for recording the signal, then appropriate magnetic media equipment should be used. If no magnetic media equipment is capable of recording the signal (i.e., has sufficient bandwidth), then the only alternative is to obtain a visual presentation of the signal and analyze the signal as best as can be accomplished through visual inspection.

(U) This section will describe a number of different types of equipment which can be used to record a detected signal. First, magnetic media recording equipment (both analog and digital) will be described. Equipment discussed include direct mode and FM mode of operation analog tape recorders, analog disc recorders, transient digital recorders and "smart-scopes". Then equipment which provide only a visual display of the signal will be described. Included in this category are cameras (photographs), the galvanometer oscillograph and the transverse oscillograph.

a. (U) Magnetic Media Recording.—Magnetic recordings are typically used because of their large storage capacity. They may be thought of as long term (including infinite) storage. Magnetic recording is permanent in that, if the medium is protected as specified by the manufacturer, the information recorded will not deteriorate or be altered. The medium may be "erased" and new data recorded. This record, erase, re-record process may be repeated until the medium physically wears out or the distortion becomes intolerable. The recording process involves a "modulation" of the magnetic state of ferromagnetic material in a predictable way. In the reproduce process, the magnetic state is sensed and translated to a replica of the input signal. The medium may be magnetic tape, ferrous discs or drums.

(1) ~~(C)~~ [redacted]

(U) It is very important to understand the operation and capabilities of recording equipment well in advance of using it in a field environment. Manufacturer's literature should be read closely to determine recorder characteristics which will affect the fidelity of the recording. Bandwidth, tape speed, number of tracks, dynamic range of record/playback amplifiers and any other pertinent data should be known before any recordings are made. It is recommended that simulated signals be recorded and played back to check recorder operation and to gain familiarity with the entire system, including receivers, cables, recorders, etc. The signals to be examined should simulate the types of signals which are anticipated in the operational environment. This will enable the analyst to trouble-shoot the system, determine if any distortions or idiosyncrasies are present, learn the adjustments and interrelationships between system gain controls, and to gain both confidence and experience to make high quality recordings.

(U) Recordings are usually made to produce an exact replica of a signal which can be played back at a later date for further analysis. Since it is important that the information bearing portions of the recorded waveform are present on the recording media, the recordings must be constantly monitored to verify proper operation. Analog recording may be done either on tape or disc. A discussion of each follows.

(a) (U) Tape.—Magnetic tapes are a very useful and flexible recording medium. They can be used to record vast amounts of information. Several signals may be recorded and then reproduced simultaneously. Usually the reproduce head will allow almost simultaneous reproduction of the recorded signal during the record process to act as a monitor or check that the signal has been correctly recorded. Tape speeds can be changed to permit changes in the time base of recorded signals. The tapes can be removed from the recorder for storage or transmittal. Care must be taken to ensure that tapes recorded on one machine can be reproduced on another. The relative speed accuracies of each are particularly important as is the wiring of the heads on multi-track machines. The tapes may have to be bulk erased (degaussed) because many recorders do not possess erase heads and the bias is not sufficient to do an adequate erase job. Some tape recorders use a tape loop on which a portion of the signal of interest is recorded. It can be played back repetitively to allow unlimited study of the signal.

(U) Recording time depends on both the reel size and the recording speed. The reel size is usually fixed for a particular machine, but using thinner tape allows a longer length of tape to be placed on the same reel size. However, the main factor in recording time is tape speed. At 120 inches per second, even a 4500 foot roll of tape will last only 7.5 minutes. Changing the signal time base by either doubling or halving the tape speed halves or doubles the signal's apparent duration. Thus, for a signal recorded at 120 inches per second, playing back at 15 inches per second will result in a signal duration eight times longer than "real-time." Signal frequency components will also be reduced by a factor of eight.

(U) Some tape recorders use rotary or helical heads and can provide temporary "stop action" with a synchronization pulse at the beginning of the window. Tape wear limits the playback in "stop action" to a few minutes.

1. (U) Modes of Operation.—There are two modes of operation for recording analog signals on tape. They are the direct mode and the FM mode. A discussion of each mode will be presented. Included is a list of the advantages and disadvantages of each mode.

a. (U) Direct Mode.—In the direct mode, the signal to be recorded and a sinusoidal bias signal are linearly added and recorded on the same tape track. The main purpose of the bias signal is to place the signal to be recorded on a linear portion of the magnetizing curve of the tape so that the resulting magnetization of the tape is linearly proportional to the amplitude of the signal. The frequency of the recorded signal is directly proportional to the tape speed and inversely proportional to the wavelength of the signal.

(U) In playback, as the tape passes over the reproduce head, the magnetic field recorded on the tape induces a voltage into the reproduce head. The induced voltage is determined by the rate of change of the magnetic flux on the tape. The playback voltage is thus somewhat dependent on frequency, and some equalization is necessary to produce a playback frequency response which is the inverse of the reproduce head characteristic. The reproduce head output gain is very low and at very low frequencies it falls below the inherent noise level of the system. This portion of the characteristic cannot be equalized so it becomes impossible to reproduce signals below a certain cutoff frequency. This has the effect of a high-pass filter acting on the signal.

(U) There is also an upper cutoff frequency. When the wavelength of the input signal is approximately the width of the reproduce head gap, the head sees an average value of the recorded signal. Hence no changing flux is detected and essentially all wavelengths shorter than the gap-width (or frequencies higher than the reciprocal of the gap-width) will not be reproduced. The frequency response can be improved by narrowing the head gap at the cost of a lower output and lower signal-to-noise ratio. Trade-offs may be seen in the manufacturer's specifications.

(U) Another technique for increasing high frequency response is increasing the tape speed. Doubling the tape speed doubles the high frequency cutoff. Recording time is reduced and head wear is increased as the tape speed is increased.

(U) A factor which degrades the quality of the recorded signal is the presence of surface irregularities, such as bumps, dirt or scratches on the tape. These will cause a drop-out of the reproduced signal. This effect is most serious at the higher frequencies. Irregularities associated with the speed of the tape across the head cause a distortion in the apparent frequency or period of the recorded signal. A high rate of speed fluctuation causes "flutter" in the signal frequency. A slow rate causes "wow."

(U) The most important advantages of the direct mode are:
(1) a wide frequency response (up to a few MHz);
(2) a wide dynamic range; and,
(3) the associated electronics are simple.

Disadvantages include:
(1) drop outs; and,
(2) the inability to record very low frequencies.

b. (U) FM Mode.—Using the FM mode overcomes the two basic limitations of the direct mode — the inability to record low frequencies and the distortion due to dropouts. In the FM mode, a carrier frequency is frequency modulated by the signal to be recorded. The modulated carrier is recorded at a constant level and is detected (reproduced) via limiter discriminator circuits. Thus, amplitude variations, even those caused by dropouts, have little or no effect on the recording. The carrier center frequency corresponds to zero voltage input. Deviation from the center frequency is proportional to the amplitude of the input signal. Signal polarity determines the direction of deviation. In playback, the amount of deviation and direction is reproduced as voltage level and polarity.

(U) Since changes in tape speed change the wavelength of the recorded signal, any variation in speed results in noise accompanying the reproduced signal. "Wow" and "flutter" are usually minimized when using the FM mode.

(U) The high frequency response of the FM mode is limited by the center frequency. A low-pass filter following the discriminator removes carrier components. By necessity, it must cut off at some fraction of the center frequency. Since the tape and head response are the same for either direct or FM mode, the center frequency, at full positive deviation, can be no higher than the highest frequency which can be recorded using the direct mode. The head gap is still the limiting factor. Thus, the overall bandwidth of the signal to be recorded (or reproduced) will be some fraction of the maximum direct recording bandwidth.

(U) Just as the direct mode frequency response is a function of tape speed, the FM carrier must also be scaled down in direct proportion as the tape speed is reduced. The low-pass filter in the reproduce amplifier must also be changed to keep its cutoff frequency a fixed fraction of the center frequency.

(U) The advantages of the FM mode include:
(1) the ability to record low frequencies down to DC,
(2) relative freedom from dropouts, and
(3) excellent phase shift vs frequency characteristics which permit accurate preservation of the signal waveform. It provides a somewhat higher signal-to-noise ratio than direct recording.

Its disadvantages include:
(1) lower high frequency response or, conversely, a higher tape speed to achieve the same frequency response as direct recording, and
(2) more complex electronics.

(b) (U) Disc.—Disc recorders are small in size and have a wide frequency response, usually from DC to several MHz.

(U) Disc recording is in many ways easier to set up and use than tape recording. It offers the great advantage of repetitive playback of a selected portion of recorded signals. The intended application of disc recording should be to make a temporary recording of a signal having a bandwidth which exceeds the bandwidth of other recording equipment or to use the repetitive feature for presenting a synchronized display. The recording time is limited to 10 or 20 seconds. Thus, the maximum signal duration must not be any greater. If one is planning to continuously repeat the signal, the maximum playback time is in the order of 20 ms. Thus, the individual signal or components thereof should not be any longer.

(U) Dual channel models are also available for simultaneously recording a monitor, a timing reference, or one signal from two transducers or detection systems. The ideal applications are for viewing hard-to-synchronize signals generated by electromechanical devices or to study in detail portions of fingerprint signals. The stop-action feature will permit hard copy recording by photography of the stable display on an oscilloscope or by making a transverse visicording.

(U) With these goals in mind, setting up the recorder is quite easy. Since the recorder cannot simultaneously record and play back (as a check on the recording process), the set-up procedure performed before recording involves an automatically made connection between the FM modulator and demodulators within the equipment. The input and output levels are adjusted for a specific peak-to-peak output level or an unclipped replica of the input. Since disc recorders are extensively used in television recording, the specified levels are usually peak-to-peak thus facilitating set-up for TEMPEST signals.

(U) Making a short recording will involve some coordination between the recorder operator and the EUT operator to ensure that the test message or pattern is recorded. The recorder will reset at the end of the recording time. The operator can choose a continuous playback or the manually selected, repetitive track playback. The repetitive playback mode is accompanied by a synchronization signal once per disc revolution. The time base used to view this signal should be the same as would be used in real time. The operator must know the signal period or duration in order to recognize the reproduced signal. From this point on, the display may be magnified using the scope's display magnifier or by using delayed sweep and shortening the display time base.

(U) One particular difficulty seems to be recognizing the window or time for the disc to rotate once. A time/division setting of 1/10 the stated length of the window will do. Some recorders have a disc rotational speed of 30 revolutions per second. Thus one rotation will require about 33 msec. The horizontal sweep of the scope should then be about 3.3 msec/cm. Five msec/cm will show all of one track plus part of the next track. The division between repetitions is usually a short burst of noise. Should this noise obscure a desired part of the signal, the manual positioning control can be adjusted slightly to position the noise burst at some other portion of the signal. Since the recorder is a wide bandwidth device, it is important that connections to the recorder are terminated in the input or output impedance to obtain the best signal-to-noise ratio.

(c) (U) Methods of Recording Analog Signals.—Recordings of receiver output can be made at either the predetection (IF) output or the post detection (video or audio) output. The following is a discussion of each.

1. (U) Post-Detection Tape Recording.—The operator should observe the signal for the presence of low frequency components, noise above the level of the signal and the repetition rate of the signal. The upper frequency components should generally be about one-half the IF bandwidth of the receiver. Band-limiting using filters can be accomplished during playback as long as none of the signals being recorded cause saturation or other problems.

(U) The noise above the signal level should be clipped to prevent overloading the recorder and to permit the desired signal to cover the recorder's dynamic range. Using a diode clipper is preferable to letting the record amplifier saturate on the noise peaks. This saturation will cause unwanted distortion of the desired signal.

(U) Both high and low frequency characteristics must be considered when the signal time base is changed by changing the tape recorder speed. When playing back a tape at a slower speed, the frequency components of the signal are reduced by a factor of one-half, one-fourth, etc., accordingly as the recorder speed is halved, quartered, etc. This means that a signal whose lowest frequency component was originally above the recorder's low-pass cutoff may eventually be translated below the low-pass cutoff as the recorder speed is lowered. Thus information or fidelity would be lost. If this occurs, the FM mode should be used. Since the response of FM always extends to DC, any amount of speed reduction and hence frequency reduction will not result in loss of low frequency signal energy.

(U) Following the choice of recording mode, the next step is to connect the signals to the recorder and adjust levels. The level range of the record amplifier dictates the level of signal supplied by the receiver or video amplifier. Since many TEMPEST signals are impulsive in nature, their peak or peak-to-peak level must be considered. Most recorders are specified as to their rms input level. The peak level of impulsive signals exceeds by far their rms levels, thus great distortion of the peak amplitude will result if an rms measurement or built-in record level meter is used to set levels. The safest and most reliable means of setting levels is to supply about a one volt peak-to-peak video signal to the recorder with the record level control set at a minimum. With the tape running, observe the output of the tape recorder for undistorted output as the gain control is advanced. Next (or first, if the record amplifier output is not provided) make a trial recording while viewing the output of the reproduce amplifier (if provided) simultaneously with the input signal. Advance the reproduce amplifier level control (if provided) to a usable level, again to about 1 volt. If peak distortion is evident, first lower the reproduce amplifier gain. If that has no effect, then reduce the record amplifier gain until the distortion is eliminated. Note these levels and gain settings for future use. Next, observe the baseline. If there is noise present on the output of the reproduce amplifier but not on the input to the record amplifier, reduce the record amplifier gain while simultaneously increasing the video level from the detection system. This should indicate if the noise is produced in the record amplifier. If not, it may be caused by too high reproduce amplifier gain or the fact that the reproduce amplifier has not been properly terminated. This condition may also indicate dirty or worn heads or worn or scratched tape. Again compare the baseline of the input and output signals. If the overshoot in the reproduced signal is greater than desired and one is using the direct mode, change to the FM mode. If sharpness in detail seems to be missing from the signal, a higher tape speed is needed.

(U) In addition to checking the signal, check the monitor also. Be sure to check for interaction between the monitor and the emanation and between direct and FM channels. The interaction may show up as a modulation of the emanation by the monitor or a coupling of the monitor or the derivative of the monitor on the emanation channel.

(U) The above discussion appears to be slanted toward using FM mode recording. This is indeed true because of the advantages of FM in all cases except for either predetection recording or the requirement of very wide bandwidth. If any doubts exist, both direct and FM mode recordings should be made simultaneously to cover the cases where one may need both modes of recording but the opportunity to return for a retest does not exist.

(U) The same discussion applies to recording monitor signals. A digital Non-Return-to-Zero monitor whose data rate is within the pass-band of the FM capabilities of the recorder is best recorded using the FM mode because the ON and OFF levels will be accurately recorded. Using the direct mode will tend to differentiate the signal thus distorting the ON and OFF times by giving them an exponential fall-off rather than the sharp transition from one state to the other.

2. (U) Predetection Tape Recording.—If predetection recording will achieve the end results desired, one must determine if the parameters of the system will permit recording the signal of interest. First, the IF bandwidth of the receiver must be wide enough to prevent frequency distortion of the signal. Next, the IF-to-tape converter must have a comparable bandwidth. The output of the converter must be within the bandwidth of the recorder. Lastly, the tape speed must be chosen to provide the required bandwidth.

(U) Setting up the levels is essentially the same as for post-detection recording. Ensure that the receiver IF level is at least the level required by the IF-to-tape converter. Ensure that the signal is not overdriving the receiver so as to cause peak distortion. Connect the IF signal to the converter with the converter level control initially set at a minimum. As in the case of post-detection recording, display the down-converted signal (the output of the IF-to-tape converter) and the original IF signal on a dual-beam scope. Adjust the video output level control for the same record amplifier input level previously found to be satisfactory (in post-detection recording) without clipping the peaks in the converter. Now view the output of the record amplifier as its gain control is advanced to provide the highest unclipped output level and an exact replica of the input. Next, with the recorder running, compare the output of the reproduce amplifier with the IF output. Advance the reproduce level control to produce a one volt peak signal level. Proceed as in post-detection recording to adjust levels for maximum dynamic range and minimum noise.

(U) While making the trial recording, the next step is to up-convert the reproduced signal using the tape-to-IF converter. Again, view the converted signal for comparison with the original IF signal. Advance the output level controls for true reproduction of the original signal. Connect the output of the up-converter to a suitable IF demodulator or receiver tuned to the IF. Adjust the IF bandwidth to match the up-converted signal bandwidth (this is determined by the original receiver bandwidth, the bandwidth of the tape recorder, and the bandwidth at the up- and down-converters). Adjust the RF, IF and video level controls for a clean replica of the original signal. If the up-converter has a tuning control to permit centering the reproduced signal in the IF pass-band of the detector, it should be adjusted for maximum output to the detector.

(U) Using a narrower final IF bandwidth and the tuning control will permit selection of narrow bandwidth signal components in the up-converted signal. The use of the tunable receiver which can cover the up-converted signal frequency range will achieve the same effect.

(2) *(U) Digital Recording Systems.*—The purpose of digitally recording TEMPEST emanations is to perform computer aided analysis to determine its information content. (*Note*: Signals recorded using analog recording systems can be digitized using an A/D converter to perform computer-aided analysis.) The advantages of computer-aided analysis are that it is faster, more accurate, and more repeatable than manual analysis techniques. In addition, the processing speed of computers enables the analyst to perform sophisticated signal analysis that would be overwhelming if performed manually.

(a) (U) Parameters of Digital Recording Systems.—The important parameters of a digital recording system are:

1. sampling rate,
2. capacity,
3. amplitude resolution, and
4. recorder-to-computer data transfer rate.

These parameters represent constraints that limit the capability of the digital recording system.

1. (U) Sampling Rate.—The sampling rate must be variable. The maximum sampling rate determines the maximum signal bandwidth that can be acquired without suffering distortion as a result of under-sampling the signal. Generally, a sampling rate of five times the detection system bandwidth is adequate for analysis. This assumes that the detection system bandwidths have been optimized for maximum information recovery (this is usually the same as adjusting the bandwidths for maximum signal-to-noise ratio).

2. (U) Capacity.—The capacity is the total number of amplitude samples that can be stored from one continuous emanation. A large capacity is preferred, as wide bandwidth, long duration signals are frequently encountered.

3. (U) Amplitude Resolution.—Amplitude resolution is governed by the number of bits used to quantize the signal. The more bits the better, however eight bits is an absolute minimum.

4. (U) Recorder-to-Computer Data Transfer Rate.—The recorder-to-computer data transfer rate can affect acquisition time to a large degree. To minimize the time, a high-speed parallel bus is recommended on which binary data (as opposed to ASCII data) is transferred. One of the worst case methods is to transfer ASCII data over an IEEE-488 bus. As an example, the number -2.125 requires six bytes to transfer in ASCII while a binary transfer would only require one byte.

(b) (U) Signal Acquisition.—What signals are acquired, and the way they are acquired, depends on these major factors:

1. the synchronization signal quality;
2. limitations of the recording system; and,
3. characteristics of the signal.

These factors will now be discussed in terms of the synchronization and samples per emanation.

1. (U) Synchronization Signal.—The quality of the synchronization signal affects the time required to perform analysis and the quality of the analysis results. The synchronization signal is used to initiate the signal recording. If the synchronization signal exhibits time jitter, then the emanations will not be time aligned. Additional processing, which can be extremely time consuming, must be performed to eliminate the jitter. The alternative to dejittering the signal is to use position independent features or transformations of the signal. Here the risk is that some of the information bearing properties of the signal may be lost, resulting in a reduction in the amount of information that can be extracted from the signal.

(U) A good quality synchronization signal is one that:
(1) occurs once and only once per symbol or group of symbols;
(2) exhibits a constant time delay between the synchronization signal and the symbol transfer; and,
(3) has a sharp leading or trailing edge.

(U) The signal to be analyzed may be used as the synchronization signal if that signal meets the quality requirements. An example where the signal CANNOT be used as its own synchronization is serial data because there are multiple transitions within each emanation. The digital recording system would indiscriminately trigger on different transitions from symbol to symbol.

(U) If the recording will contain emanations from more than one transmitted symbol, then record the synchronization signal on a second channel. The recorded synchronization signal will be used later to partition the recording into separate emanations which is required for TEMPEST analysis.

2. (U) Samples per Emanation.—The limitations of the recording system and the characteristics of the signal determine the number of amplitude samples per emanation that can be recorded. The number of samples N is found from

$$N = T \cdot SR$$

where: T is the duration of the emanation to be recorded; and,
SR is the sampling rate.

(U) If the digital recording system has a storage capacity less than N, then either the sampling rate or N must be reduced. Both alternatives give rise to the possibility that information will be lost. Decreasing the sampling rate will produce under-sampled recordings. Reducing N means that a portion of the emanation will be lost. The analyst must decide which alternative will do less damage. Also recognize that the computed degree of compromise may be less than its true value due to the loss of information.

(3) (U) Event Capturing Equipment.—Two equipments that can capture event type emanations are the transient digital recorder and the "smart scope". These equipment rely on having a high quality synchronization signal and a short time duration emanation to allow accurate capture.

(a) (U) Transient Digital Recorder.—This term generally refers to an equipment containing a relatively fast A/D unit, some memory capacity to store a limited number of A/D samples, and a way of off-line storing each recording of the emanation.

(b) (U) "Smart Scopes".—This term generally refers to an oscilloscope which has a limited digital computer capacity. This device may be useful in evaluating the emanation both on-site and in the laboratory. These scopes can be programmed to compute averages and perform correlations for pattern matching. Much can be learned about the emanation by doing these simple procedures. If one doesn't have a computer, one of these scopes can prove quite useful.

b. (U) Visual Recording.—If only a visual presentation is required to document the emanation, then photographs, chart recordings, and oscillograph traces can be used. Equipment which produce these permanent records will now be discussed.

(1) *(U) Still Scope Camera.*—The most common and inexpensive visual record is a photograph of the A-scope display. The camera uses packs of instant developing film. The most desirable camera is one which fills the entire picture with the scope display. The camera should swing away to allow an undistorted full view of the scope face when the camera is not in use. Some experimentation is needed to adjust trace and graticule intensity along with f-stop and shutter speed to obtain a well exposed photograph. The shutter may be opened manually and the scope trace swept once to record a transitory or single event waveform. The graticule may be recorded using a second exposure.

(U) Camera sophistication can range from completely manual settings to completely automatic settings. Some cameras feature automatic film advance after photographing a single sweep. Other cameras can have interchangeable film packs permitting alternate use of different size film.

(U) Oscilloscopes have a maximum writing speed beyond which no record of the signal can be made with a camera. Sampling or storage scopes are necessary to display these signals or else very fast film and large apertures (small f-stops) must be used. Care must be taken to ensure that the camera can be attached to the scopes being used. Adapters can be obtained from either the scope or camera manufacturer. Most signal monitors are not provided with camera attachments but do have X and Y outputs so that these signals may be displayed on a conventional scope having an attached camera.

(2) *(U) Chart Recorder.*—Chart recorders are used to produce longitudinal recordings. The digitized data is fed to pen servos as the paper is fed from the recorder. The equivalent time base on the chart recording is a function of the original sampling rate and the selected paper speed. Usually these instruments have multiple channels which allow for simultaneous printing of more than one time segment of the record.

(3) *(U) Transverse Oscillograph.*—The transverse oscillograph is similar to a laboratory oscilloscope with the addition of a Fiber Optic (FO) face plate on a Cathode-Ray Tube (CRT). The FO transfers the light trace on the inner phosphor coating to the recording media. As the light trace moves in accordance with the signal, a photographic record is made on paper. The paper is then "developed" by exposure to light, but if exposed for a long period of time, the entire paper will darken and the image will be lost. The paper is best handled under incandescent light. The paper may also be developed by ordinary photographic techniques producing a permanent record.

(U) For longitudinal recording, the data signal is applied to the horizontal amplifiers of the FO-CRT and the monitor CRT. This records the signal in the direction of paper travel with the record speed providing the time base as in a conventional oscillograph. Paper speed up to about 100 in/sec is possible. An intensity modulation input (Z-axis) is provided to modulate the intensity of the electron beam.

(U) For transverse recording, the data signal is applied to the vertical amplifier of the FO-CRT. This records the signal across the paper. It is sometimes useful in recording certain keyboard emanations. When a variable delay synchronization signal is available from a key punching device, this may be used as a horizontal trigger. The variable delay in conjunction with the horizontal sweep speed can be used to center the desired portion of the emanation near the center of the paper. The synchronization provides a means of feeding the paper only when an emanation under investigation is present, resulting in conserving recording paper.

(U) The transverse oscillograph is capable of recording successive sweeps of an oscilloscope trace across the width of the recording paper. The sweep can be either triggered or left free running depending on the repetition rate of the displayed signal. Equivalent paper speeds of 390,000 inches per second can be achieved. Vertical input bandwidths to 100 kHz with intensity modulation input bandwidths to 10 MHz can be obtained. A monitor oscilloscope may be included so that the operator will know exactly what is being recorded. This device can record anything that can be displayed on an oscilloscope. If the trigger accompanying the signal occurs at the beginning of the signal, the early portions of the signal may be expanded. If the trigger to the oscillograph is used in conjunction with an oscilloscope time base that generates a delayable trigger, positioning the delay trigger during the time epoch of the signal will allow any portion of the signal to be expanded and recorded. The application of this feature is useful in studying fingerprint waveforms.

(U) The transverse oscillograph can have time and amplitude calibration features similar to an ordinary oscilloscope with time calibration marks printed on the recording paper.

THIS PAGE IS INTENTIONALLY BLANK

APPENDIX D

AN EXAMPLE OF AN ANALYSIS REPORT* (U)

D-1. (U) Introduction.

a. (U) This report contains the results of the TEMPEST signal analysis performed on the QED Automatic Typewriter/Contról Unit. This report complements the TEMPEST test report to provide a complete assessment of the vulnerability of this equipment to TEMPEST exploitation.

b. (U) TEMPEST exploitation is the recovery of classified information by unauthorized personnel through detection and analysis of compromising emanations emitted from a data processing device. The type of emanations detected are a result of the TEMPEST encoders in the equipment. A TEMPEST encoder is an unintentional and undesirable phenomenon which converts information intentionally processed into a different format, and transmits it through a TEMPEST channel. Usually this conversion is not unique—ambiguity is added and information is lost within the TEMPEST encoder. TEMPEST signal analysis is the process of using statistical attacks to reduce the ambiguity added and thereby recover the information processed. The first step of TEMPEST signal analysis is to study the equipment under test to determine the possible TEMPEST encoders.

D-2. (U) Equipment Description.

a. (U) General.

(1) (U) The QED Automatic Typewriter/Control Unit (AT/CU) features punched tape input and output in addition to the normal keyboard input and page printer output. The Automatic Typewriter (AT) utilizes the eight level "selectric" code (see Figure D-1). The Control Unit (CU) provides code conversion so that any punched tape code may be used for input and output. The punched tape code may contain up to seven information bits plus one parity check bit. Both the units process information in parallel (i.e., all information bits of each character are processed simultaneously).

**Note:* This is a fabricated example to illustrate an analysis report.

	1	2	3	4	5	6	7	8	DENSITY
A			X	X	X		X		4
B						X	X		2
C			X	X		X	X		4
D	X		X	X		X	X		5
E	X		X			X	X		4
F		X	X	X			X		4
G	X	X	X	X			X		5
H	X					X	X		3
I	X			X	X		X		4
J	X	X	X				X		4
K			X			X	X		3
L	X			X		X	X		4
M	X	X	X	X	X		X		6
N		X	X			X	X		4
O		X	X	X		X	X		5
P	X		X				X		3
Q			X				X		2
R	X		X	X	X		X		5
S	X				X		X		3
T	X	X	X			X	X		5
U			X		X		X		3
V		X	X	X	X		X		5
W					X		X		2
X	X	X	X	X		X	X		6
Y	X						X		2
Z	X	X	X		X	X	X		6
Sp			X						1

(Note: Sp indicates the "Space" character)

Figure D-1.—The "Selectric" Code (No Parity) (U)(U)

(2) (U) To perform effective analysis, one should correlate the detected emanations to possible TEMPEST encoders. Therefore, it is necessary to understand parts of the system timing and the signal path circuitry. Figure D-2 illustrates the pertinent portions of the timing and circuitry.

b. (U) Automatic Typewriter.

(1) (U) CLOCK B activates the eight optical sensors in the tape reader. During CLOCK B time (approximately 4 msec), the coding detected by these sensors is read in parallel into the control unit. At the end of CLOCK B, this information has been converted into "selectric" code and transferred in parallel into the AT data bus register. During CLOCK B time, this information is then encoded by the CU into the desired output code.

(2) (U) At CLOCK D time, both the punch magnets and the printer magnets are activated. There are eight punch magnets. The combination of punch magnets energized depends on the code furnished by the CU. The printer utilizes 14 magnets, 7 of which are used in various combinations to print the alphanumeric characters. The other seven perform carriage movement functions. The "Space" character is treated as a carriage movement function, rather than as an alphanumeric character.

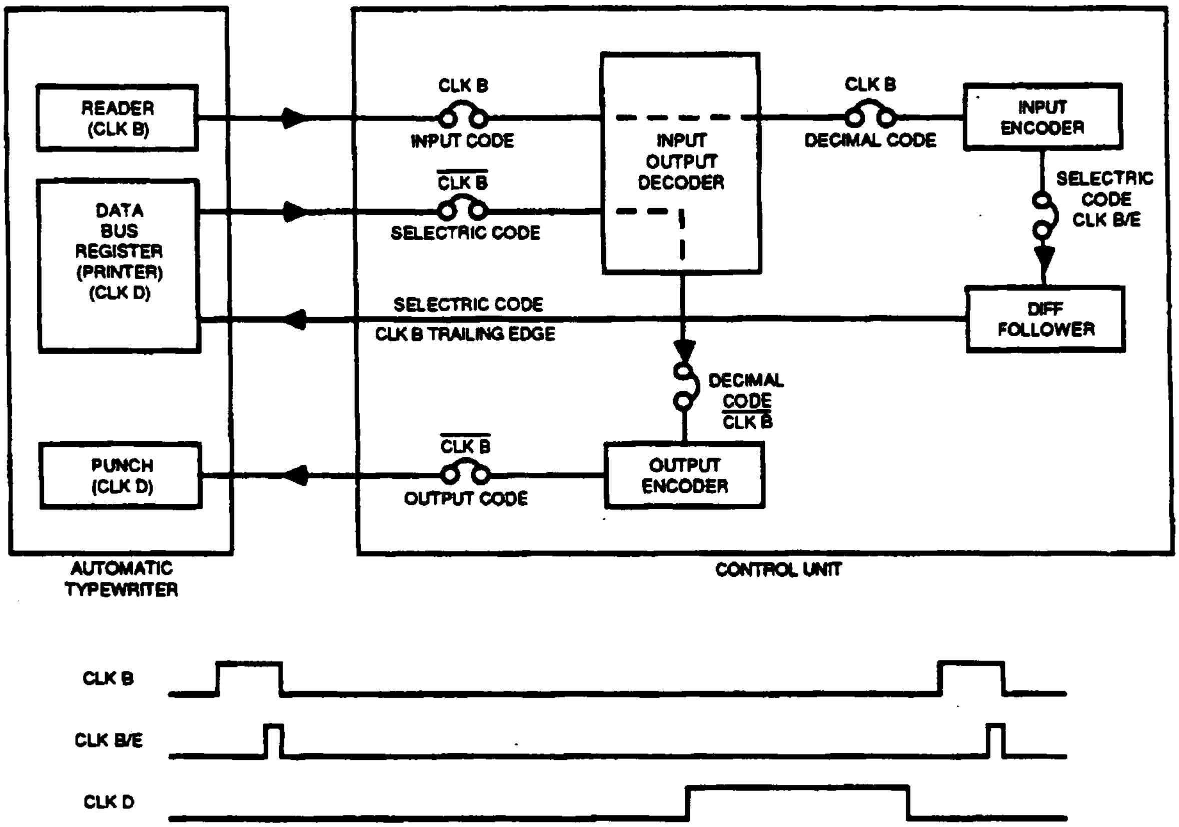


Figure D-2.—Block Diagram and Timing Chart of the QED Automatic Typewriter/Control Unit (U)(U)

(3) (U) At the initiation of the next CLOCK B pulse, the previous character is cleared from the data bus register. The cycle is then repeated. Should information be entered on the keyboard rather than on the tape reader, input code conversion is not required. Depression of a typewriter key selects a combination of six bail switches. In the "selectric" code, the seventh bit indicates only that an alphanumeric character has been selected. Therefore, only six bits determine each character uniquely. The corresponding data bus registers are then set so that the required coded information is present at the end of CLOCK B.

c. *(U) Control Unit.*

(1) (U) At the beginning of CLOCK B, information from the AT tape reader is transferred in parallel to the CU input/output decoder. Only seven of the input lines are decoded; the eighth bit, if used, is a parity check bit. Each unique combination of input coding represents a binary number. The input/output decoder provides the decimal representation of this number, and activates the corresponding exit hub on the patch panel. This hub is patched to a selected input encoder hub. During CLOCK B/E time, the input encoder provides the "selectric" code equivalent of the character.

(2) (U) The "selectric" code representation is transferred in parallel to the AT at the trailing edge of CLOCK B. This transfer is executed by a set of seven differentiator followers. Each differentiator follower is triggered by the trailing edge of CLOCK B if and only if it has been previously set by its corresponding input encoder line.

(3) (U) Output code conversion is accomplished in a similar manner. It occurs, however, at CLOCK D rather than at CLOCK B.

(b) (1)
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

D-3. (U) Possible TEMPEST Encoders.

a. ~~(C)~~ [redacted]

Figure D-3.

~~(C)~~ [redacted]

b. ~~(C)~~ [redacted]

c. ~~(C)~~ [redacted]

D-4. (U) Detected Signal Description.

a. ~~(C)~~ [redacted]

b. ~~(C)~~ [redacted]

D-5. (U) Analytic Techniques.

a. ~~(C)~~ [redacted]

b. ~~(C)~~ [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

Figure D-4.

[redacted]

Figure D-5.

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

Figure D-6

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

Figure D-7. [redacted]

D-6. (U) Results.

a. ~~(C)~~ [redacted]

~~(C)~~ [redacted]

b. ~~(C)~~ [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

c. ~~(C)~~ [redacted]

APPENDIX E

GLOSSARY (U)

(U) This is not an all-inclusive glossary. It includes primarily terms pertinent to TEMPEST signals analysis but also includes some general TEMPEST terms which may help clarify the subjects discussed in this handbook. Terms defined in NSTISSAM TEMPEST/1-91 or its replacement document are not repeated herein.

A

A-Scope Display (U)—An oscilloscope display with the input signal as the vertical (y-axis) component and a time base as the horizontal (x-axis) component.

Adaptive Delta Modulation (ADM) (U)—A type of digital encoding system used for speech transmission.

Adaptive Filter (U)—A type of digital filter whose filter characteristic adapts to or tracks a predictable changing signal characteristic in order to filter it out.

Aliasing (U)—When a signal is sampled at a rate less than twice its highest frequency component, the high frequency part of the signal folds back and is added to the lower frequency components, creating a distortion and making impossible the reconstruction of the analog signal by linear filtering.

Ambiguity (U)—A condition which precludes positive identification of specific characters and functions utilizing the parameters of the detected signal. This condition exists when the intelligence-related signal emanation can be equated to more than one character or function or groups of characters or functions.

Analog Signal (U)—A signal whose amplitude, phase, or frequency content is continuously proportional to the stimulus.

A Posteriori Probability (U)—The probability that a character or group of characters was processed, given that a particular signal was received.

A Priori Probability (U)—The probability of a character or a group of characters in the source language.

Asynchronous (U)—This word is used in two different ways:

a. A serial system which requires an additional bit or bits for speed adjustment (i.e., latch and release bits);

b. A method of operating the EUT or the display equipment so as to optimize the probability of signal detection.

Average Depth of Correct Symbol (ADCS) ~~(C)~~ [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

(b) (1)
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

B

Backward Channel Probability (U)—See *A Posteriori Probability*.

Bandwidth (U)—Several definitions of bandwidth are encountered.

a. Half power—The frequency interval between the upper and lower frequencies where the output signal is attenuated to one-half the power of the input signal (down 3 dB). This is the bandwidth usually specified for receivers, tape recorders, filters, etc.

b. Message—The frequency interval between the upper and lower frequencies beyond which the energy content of the signal is negligible or unnecessary for conveying information.

c. Sampling—One-half the sampling rate. When a signal is sampled (for A/D conversion), frequencies below 1/2 the sampling rate are retained. All higher frequencies are folded back (aliased) and distort the lower frequencies.

Baud (U)—The unit of serial signal rate.

Baud Card (U)—A 3 x 5 index card (or larger if needed) used to mark off bit and character lengths of a serial processed TEMPEST signal.

Bayes' Rule (U)—An equation for relating conditional probabilities. See Section 3–2*a*(5).

Bit (U)—Three definitions are used:

a. A unit interval of time;

b. A binary digit; or,

c. The basic unit of information, I(X). If the probability of occurrence of event X is P(X), the knowledge that X has, in fact, occurred is I(X)= −log P(X) bits of information (base 2 logarithms). If P(X)=1/2, I(X)=1 bit of information.

Bit Density Information ~~(C)~~ [redacted]

Byte (U)—A set of binary digits forming a single information word.

C

Central Limit Theorem (U)—The distribution of the sum of a large number of independent random variables is approximately normal. This means that the distribution of a received signal may be approximated by a normal distribution.

Channel Matrix (U)—A two-dimensional array of conditional probabilities P(Y|X) where [Y] is the set of received signals and [X] is the set of transmitted signals. (This is also called the forward channel matrix.) The array of P(X|Y) is called the reverse channel matrix.

Channel Uncertainty (U)—See *Uncertainty.*

Channel Vocoder (U)—A type of digital encoding system used for speech transmission.

Code (U)—A scheme of representing one set of symbols by another set of symbols.

Comb Filter (U)—An analog filter used to filter AC noise, i.e., it filters 60 Hz and all harmonics of 60 Hz.

Communications Security (COMSEC) (U)—The protective measures taken to deny unauthorized persons information derived from telecommunications of the United States Government related to the national security and to ensure the authenticity of any such communications. Such protection results from the application of security measures (including cryptosecurity, transmission security, and emissions security) to electrical systems generating, handling, processing, or using national security information. It also includes the application of physical security measures to communications security information or materials.

Conditional Probability (U)—The probability of an event occurring given that another event has already occurred.

Conducted Signals (U)—Electromagnetic or acoustic emissions of undesired signal data which become induced and propagated along wire lines or other conductors.

Confidence Interval (U)—A range of values which contain the true value with a selected probability called the confidence level.

Cycle (U)—The total number of bits (synchronizing, intelligence, error checking, or control bits) required to transmit any given character in a serial communication system.

D

Detection (U)—The act of determining the presence of TEMPEST emanations by technical surveillance techniques.

Detection System Bandwidth (U)—Refer to the current version of NSTISSAM TEMPEST/1-91.

Deterministic Channel (U)—A channel in which each input is converted to one and only one output. Such a channel can be characterized by a channel matrix with one and only one non-zero element in each row. *Note:* The inverse (each output represents only one input) is not necessarily true.

Digital Signal (U)—A nominally discontinuous electrical signal that changes from one state to another in discrete steps.

Disjoint Generatrices (U)—See *Mutually Exclusive.*

Digraphic Information ~~(C)~~ [redacted]

Digraphic Processing (U)—Processing where the data (bits) are parallel processed, and the characters are processed two at a time.

E

Electric Space Radiation (ESR) (U)—That portion of an electromagnetic field which is caused by a difference in potential.

Electromagnetic Field (U)—Energy which exists in the vicinity of a conductor of electricity. It consists of Electric Space Radiation and Magnetic Space Radiation components.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

Entropy (U)—See *Uncertainty.*

Entropy Encoding (U)—A class of digital speech encoding techniques where the digital representation of the speech will exactly reproduce the input speech waveform.

erf (U)—The function erf (X) is the probability that a sample from a standard normal population has a value of less than or equal to X.

Estimation (U)—The process of obtaining an approximation of a population parameter (mean, standard deviation, etc.) from a statistical sample.

F

Fingerprint Signal (U)—A unique emanation caused by the processing or transfer of an information unit (e.g., character, byte, etc.) by the EUT. (Also called signature.)

Format (U)—An aspect of entropy which doesn't depend on language but rather on how messages are structured.

Forward Channel Probability P(Y|X) (U)—The probability of detecting signal Y given that the character X was processed.

Full Bit Emanation (U)—An emanation which correlates on a one-to-one basis with the bits of the message code signal.

G

Gaussian Distribution (U)—See *Normal Distribution.*

Generatrix (U)—The set of characters which are considered to be the cause of a particular received TEMPEST signal, arranged in order of probability.

Generatrix Family (U)—The groups (sets of generatrices) into which the characters of the alphabet are assigned by the TEMPEST encoder. Also, the groups into which the characters are assigned at the output of the detector for analysis purposes.

Generatrix Family Dimension (GFD) ~~(C)~~ [redacted]

Generatrix Sequence (U)—The sequence of generatrices resulting from a test where a representative test message for the EUT is processed. One generatrix is generated for each received signal.

H

Histogram (U)—A bar graph which represents relative frequencies of discrete events. The height of each bar is proportional to the number of times the corresponding event has occurred. It is often used to approximate the probability density function by assigning a range of values to each event.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

I

Independent Events (U)—Two events are independent if their joint probability equals the product of their individual probabilities.

Information Ratio (IR) (U)—A measure of the amount of information which can be derived from a detected signal. It is the ratio of the amount of information contained in a signal to the amount of information necessary for 100 percent recovery of plaintext information.

Information Source (U)—Two definitions are used:
a. A language which a sender uses to produce a sequence of information units to form a message;
b. A mathematical description of an information-generating mechanism. The source emits a sequence of symbols from a fixed finite source alphabet. Successive symbols are selected according to some fixed probability law.

Information Theory (U)—The study of measures of information and the investigation of the properties of these measures.

L

Latch or Stop Bit (U)—A bit which serves to bring the receiving mechanism of a serial processing equipment to rest in preparation for the reception of the next character.

Linear Delta Modulation (U)—A type of digital encoding system used for speech transmission.

Linear Predictive Coding (LPC) (U)—A type of digital encoding system used for speech transmission.

M

Magnetic Space Radiation (MSR) (U)—The component of the electromagnetic field which is caused by current flow.

Marginal Probability (U)—The weighted sum of the conditional probabilities.

$$P(A) = \sum_{B} P(A|B) \cdot P(B)$$

Mark (U)—This is the serial signal condition when the equipment under test is in an energized (current-flow) condition or when there is a change in the polarity of the signal.

Markov Information Source (U)—A general type of information source where the occurrence of a source symbol may depend upon a finite number of preceding symbols.

Mean (U)—The average value of a random variable.

Message Encoder (U)—The system which converts the most basic information units of a language (characters and "Space") into mechanical quantities which a machine can handle.

Monographic Information ~~(C)~~ [redacted]

Monographic Processing (U)—Processing where each character is sequentially processed in a bit parallel format.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

Mutually Exclusive (U)—If each individual alphabetic character and/or special function is found in one and only one generatrix after classification, the generatrices are said to be mutually exclusive.

N

Narrowband Signal (U)—A TEMPEST signal which is correlated to the baseband representation of the information processed.

Noisy Channel (U)—A channel in which signals are corrupted by noise. Also, a channel described by a matrix with at least one row containing two or more non-zero elements.

Normal Distribution (U)—A continuous distribution characterized by a "bell-shaped" probability density function curve centered on the mean whose width is proportional to the standard deviation.

P

Parametric Encoding (U)—A class of digital speech encoding systems where the digital representation of the speech approximates the input speech waveform.

Parity (U)—The use of extra bits to check for errors in codewords.

Phoneme (U)—The smallest information bearing unit of speech.

Polygraphic Information (U)—Information which results when the TEMPEST emanation corresponding to one function and/or character is affected by the processing of one or more other functions and/or characters.

Polygraphic Processing (U)—Processing where the data (bits) are parallel processed more than one at a time.

Population (U)—Any finite or infinite collection of individual things, objects, or events.

Probability (U)—The relative frequency of occurrence of a given event out of all possible events.

Probability Density Function (pdf) (U)—This function describes the probability that a random variable will assume a value within some defined range at any instant of time.

Probability Distribution Function (U)—A function which gives the probability that a random variable is less than or equal to the argument.

Pulse Code Modulation (PCM) (U)—A type of digital encoding system used for speech transmission.

R

Radiated Signal (U)—Electromagnetic or acoustic emissions of undesired signal data which are propagated through space.

Radiation (U)—Signals emanating from an equipment which appear as electromagnetic fields or as spatial longitudinal waves. These include induction field, magnetic field, electric field gradient and acoustic waves.

Raster Scope Display (U)—An oscilloscope display in which the input signal intensity modulates the screen while the vertical and horizontal sweeps are controlled by two different synchronized time base generators.

Release or Start Bit (U)—A bit which serves to prepare the receiving mechanism of an equipment for the reception and the registration of a character.

S

Sample (U)—A portion of a population.

Sampling (U)—There are two definitions used:
a. To select a small number of samples from a large population for inspection or analysis;
b. A technique or process of quantizing a signal, usually performed at regular intervals.

Serial Signal (U)—A signal in which information is conveyed by the time relationship of bits, i.e., bits are transferred one at a time in a specified manner.

Signal Bandwidth (U)—That portion of the frequency spectrum which must be passed by signal processing equipment in order to minimize signal distortion.

Signal-To-Noise Ratio (S/N, SNR) (U)—A ratio of signal voltage, current, or power to noise voltage, current or power.

Space (U)—This is the serial signal condition when the equipment under test is in an unenergized (no current) condition (as opposed to Mark). Note: This is NOT the definition of the "Space" character.

Space Radiation (U)—The phenomena in which electromagnetic or acoustic signals emanate from the equipment under test into free space.

Spectragram (U)—A display technique. Time is represented along the x-axis, frequency is represented along the y-axis, and intensity of the signal is represented (by lightness-darkness) along the z-axis.

Standard Deviation (U)—A measure of the spread of a probability density function.

Synchronous (U)—A system that does not require an additional bit or bits for speed adjustment, i.e., latch and release bits.

T

Time Correlated Pulse (U)—A pulse which occurs at exactly the same time in the character cycle each time a particular character is processed by the equipment under test.

Transition (U)—The change from one signaling condition to another, for example the change from "mark-to-space" or from "space-to-mark."

Transitional Signal (U)—In the TEMPEST channel, the impulse that occurs at the time of a change from one signaling condition to another such as the change from "mark-to-space" or from "space-to-mark."

Transition Density Information ~~(C)~~ [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

U

Uncertainty (Entropy) (U)—Two definitions are used:

a. The average amount of information gained per received signal;

b. The average amount of information required before one is certain that an event has occurred. The types of Uncertainty are:

(1) *Input Uncertainty $(H(X))$*—This is the average amount of information provided by the source language.

(2) *Output Uncertainty $(H(Y))$*—This is the average amount of information provided by the received signal.

(3) *Forward Channel Uncertainty $(H(Y|X))$*—This is the average amount of information required to be certain what signal will be received if the transmitted symbol is known.

(4) *Reverse Channel Uncertainty $(H(X|Y))$*—This is the average amount of information required to be certain what symbol was sent if a certain channel output is observed.

(5) *Transinformation or Information Gain $(I(X|Y))$*—This is the average information that is obtained about which symbol was transmitted if the channel output is observed and the source language statistics are known.

V

Variance (U)—A measure of the spread or dispersion in a population. The population variance is usually approximated by the sample variance, s^2.

APPENDIX F

SOURCES OF TEMPEST INFORMATION (U)

F-1. (U) Introduction.—This appendix contains some suggested references which may be found useful in TEMPEST analysis activities. All too often analysts waste time "rediscovering the wheel" because they do not realize that the work has already been done. Specific information on TEMPEST signal analysis is available from reports filed in the National TEMPEST Information Center as discussed in Section F-2. Related information is available in standard textbooks on probability, statistics, communication theory, information theory, and speech and signal processing such as those listed in Section F-3.

F-2. (U) National TEMPEST Information Center.—The National TEMPEST Information Center (NTIC) is maintained at the National Security Agency for the collection, control, and interchange of reports on Government conducted or sponsored tests for compromising emanations including results obtained and corrective action taken or contemplated.

(U) Reports in the NTIC may be obtained on a loan basis by government organizations concerned with TEMPEST and their authorized contractors on a need-to-know basis. Requests for these reports should be addressed through appropriate department or agency channels to:

Director, National Security Agency
ATTN:[redacted]NTIG. . . . . (b) (3)-P.L. 86-36
Fort George G. Meade, Maryland 20755-6000

F-3. (U) Textbooks.

(U) There are many texts which deal with subjects related to TEMPEST analysis. Some of the suggested texts are:

a. Probability and Statistics.

Elementary Texts (no calculus required)

1. Theory and Problems of Statistics, by Murray R. Spiegal, Schaum's Outline Series, McGraw-Hill, New York, 1961.
2. Introduction to Probability and Statistics, by B. W. Lingren and G. W. McElrath, MacMillan Co., New York, 1966.
3. Experimental Statistics, National Bureau of Standards Handbook 91, 1963.

Intermediate Texts (calculus required)

1. Introduction to the Theory of Statistics, by A. M. Mood and F. A. Graybill, McGraw-Hill, New York, 1963.
2. Probability, Random Variables and Stochastic Processes, by A. Papoulis, McGraw-Hill, New York, 1965.
3. Tables for Making Inferences about the Variance of a Normal Distribution, by D. V. Lindley, D. A. East and P. A. Hamilton, Biometrika, Vol. 47, p. 333, 1960.

b. Communication Theory.

1. An Introduction to Random Signals and Communication Theory, by B. P. Lathi, International Textbook, Scranton, 1968.
2. Communication Systems: An Introduction to Signals and Noise in Electrical Communications, by A. Carlson, McGraw-Hill, New York, 1968.
3. An Introduction to the Theory of Random Signals and Noise, by W. B. Davenport Jr. and W. L. Root, McGraw-Hill, New York, 1958.
4. Linear Systems, by R. J. Schwarz and B. Friedland, McGraw-Hill, New York, 1965.
5. Signal Detection Theory, by J. C. Hancock and P. A. Wintz, McGraw-Hill, New York, 1966.
6. Detection, Estimation, and Modulation Theory, by H. L. Van Trees, John Wiley and Sons, New York, 1968.
7. Principles of Communication Engineering, by J. M. Wozencraft and I. M. Jacobs, John Wiley and Sons, New York, 1965.
8. Introduction to Statistical Communication Theory, by David Middleton, McGraw-Hill, New York, 1960.
9. Reference Data for Radio Engineers 5th Edition, Howard Sams and Company, New York, 1968.

c. Information Theory.

1. Information Theory and Coding, by N. Abramson, McGraw-Hill, New York, 1963.
2. An Introduction to Information Theory, by F. Reza, McGraw-Hill, New York, 1961.
3. Information Theory, by R. Ash, Interscience Publishers, New York, 1965.
4. Transmission of Information, by R. Fano, John Wiley, New York 1961.
5. Elementary Information Theory, by D. S. Jones, Oxford University Press, Oxford, 1979.
6. Mathematical Foundations of Information Theory, by A. I. Khinchin, Dover Publications Inc., New York, 1957.
7. An Introduction to Information Theory, by John R. Pierce, Dover Publications Inc., New York, 1980.
8. Ergodic Theory and Information, by Patrick Billingsley, Robert E. Krieger Publishing Company, Huntington, New York, 1978.
9. Information Theory and Reliable Communication, by Robert G. Gallager, John Wiley and Sons, New York, 1968.
10. An Introduction to Information Theory and Communication Theory, by Fred Haber, Addison-Wesley Publishing Company, Reading, Massachusetts, 1974.
11. The Mathematical Theory of Communication, by Claude E. Shannon and Warren Weaver, The University of Illinois Press, Urbana Illinois, 1964.
12. Coding and Information Theory, by Richard W. Hamming, Prentice-Hall Inc., Englewood Cliffs New Jersey, 1980.
13. The Theory of Information and Coding, by Robert J. McEliece, Addison-Wesley Publishing Company, Reading Massachusetts, 1982.

d. *Computer Programming.*

1. A Fortran IV Primer, by E. Organik, Addison-Wesley Publishing Company, Reading Massachusetts.

e. *Speech and Signal Processing.*

1. Modulation Theory, by Harold S. Black, D. Van Nostrand Co., 1953.
2. Delta Modulation Systems, by Raymond Steele, Pentech Press, London, 1975.
3. Digital Processing of Speech Signals, by Lawrence Rabiner and Ronald W. Schafer, Prentice-Hall, New York, 1978.
4. Speech Analysis, Synthesis, and Perception, by James L. Flanagan, Springer-Verlag, New York, 1965.
5. Speech Analysis, Synthesis, and Perception 2nd edition, by James L. Flanagan, Springer-Verlag, New York, 1972.
6. The Speech Chain, by Peter B. Denes and Elliot N. Pinson, Bell Telephone Labs., 1964.
7. Factors Governing the Intelligibility of Speech Sounds, by N. R. French and J. C. Steinberg, The Journal of the Acoustical Society of America, Vol. 19 No. 1, Jan. 1947.
8. The Design of Speech Communication Systems, by Leo L. Beranek, The Proceedings of the I. R. E., Vol. 35 No. 9, Sept. 1947.

THIS PAGE IS INTENTIONALLY BLANK

Unclassified Until Filled

COMMENT FORM
FOR
COMPROMISING EMANATIONS ANALYSIS HANDBOOK

Use one form per comment. Return completed form to: Director, National Security Agency
Attn: [redacted]
Fort George G. Meade, Maryland 20755-6000

(b)(3)-P.L. 86-36

1. Date:

2. Name of Contributor:

3. Address of Organization:

4. Reference paragraph, page number, and line number if required. If general comment, describe subject to be discussed:

5. Comment (What should be changed?):

Unclassified Until Filled

6. Alternative (What should it be changed to?):

7. Rationale (Why should change be made?):

If more space is required for any of the above items, use extra sheet(s) and attach to this form.

COMPROMISING EMANATIONS ANALYSIS HANDBOOK (U)