27 Aug

EO 3.3(h)(2)
PL 86-36/50 USC 3605

~~TOP SECRET FROTH~~

SURVEY OF WHERE MECHANIZED OPERATION CAN BENEFIT

THE COMINT EFFORT ON LITERAL TEXTS

DRAFT

I COMINT COLLECTION ACTIVITIES

A. Functional Categories of Intercept Problems

1. [redacted] have the highest potential intelligence value. [redacted] are also of value to the COMINT organization in maintaining continuity. [redacted] is on high power, high frequency radio.) High speed morse and radioprinter (both single channel and multiplex) are used on the main links although there is still some manual morse. In general, good [redacted] signals are available at present intercept sites. The problem is largely one of efficient operation and handling of the extremely large quantities of traffic which must be screened for desired messages.

2. National Commercial Radio (NCR)

National Commercial Radio is the name chosen, for the purpose of this paper, for internal networks, such as the Brazilian and Russian Civil. These nets carry internal commercial traffic, of the type generally carried in the U. S. by Western Union.

3. [redacted] might be considered in this category). From the widespread nature of these organizations and the low traffic densities on many links, simpler forms of transmission are to be expected. In [redacted]

30 1259

COPY 11 OF 16 COPIES
PAGE 1 OF 43 PAGES

~~TOP SECRET FROTH~~

EO 3.3(h)(2)
PL 86-36/50 USC 3605

4. Military Tactical

Military Tactical traffic (sometimes referred to as low level) is usually intercepted and, to some extent, processed by Military "Close Support" COMINT organizations, which produce "tactical" intelligence-primarily "Order of Battle" - of direct value to the field commander with results eventually coming to NSA in the form of reports and, later, of the raw intercept itself, are forwarded to NSA. However, the initial user is in the field and control of "Close Support" activities and, to the maximum practicable extent, processing functions are delegated to the cognizant service organization. Military Tactical traffic, since it is generally being sent by or received by subordinate units, is usually low powered and is transmitted by relatively simple communication systems. In the [redacted] Radiotelephone also is used extensively in Military Tactical services.

5. Military Strategic

Military Strategic refers to high level military communications, including those connecting Corps and Army Headquarters with War Ministry (and for corresponding and echelons of the parallel service branches). Normally, high traffic densities and very secure cryptographic systems are used at this level. In the U. S. Armed Forces heavy use is made of radioprinter systems which include the radioprinter multiplexes. In [redacted]

6. Support Communications

Support Communications is the name chosen, for the purposes of this paper, for those communications required, either on a broadcast or a point-to-point basis to support various types of operations. Weather nets and broadcasts, navigational systems and services are examples of support communications. [redacted] support communications (literal) include hand speed Morse and single channel radioprinter.

EO 3.3(h)(2)
PL 86-36/50 USC 3605

B. Major Technical Intercept Problems

1. [redacted] plex on three or four. All three of these have posed serious intercept problems which have required research and development.

[redacted] were inadequately quilified for receiving cryptographic radioprinter, and because technical consideration such as extremely wide and inconsistent frequency keying shifts arose. Magnetic tape recording of the demodulated signal with later central processing to hard (page) copy in NSA preserved vital signal information, and made it possible to carry out the critical processes of printing, under controlled laboratory conditions and prevented the irretrievable loss of information in the field. A tuning aid was devised, and this has enabled operators to make substantially better recordings than was previously possible. Central Processing, in the Special Intercept Techniques Division, Office of Collection, PROD, using synchronized free-running teleprinters provides page copies for the cryptanalysts, showing the time relationship of characters sent by each operator by the coordinates on the page copies. The cryptographic device [redacted]

EO 3.3(h)(2)
PL 86-36/50 USC 3605

EO 3.3(h)(2)
PL 86-36/50 USC 3605

b. [redacted]

Demands for improvement of intercept of this signal have led to considerable efforts on the part of PROD; the signal is now magnetically recorded and centrally processed similarly to the [redacted] described above. Circuit discipline and operator standards are excellent, and relatively [redacted] are believed to be used. The signal is generally transmitted on one side of a Double Frequency Shift transmission. Keying rates and standardization of shifts are such that interception and demodulation may efficiently be accomplished with standard equipment, including the AFSAV D35 Double Frequency Shift Demodulator.

c. <u>Flexible Multiplex</u>

[redacted] consequently, severe tuning and stability requirements are placed on intercept equipment. To date, these special needs have been met by an interim high precision intercept system still undergoing development and improvement, incorporating highly stable receiving and recording equipments and a special tuning indicator. The Flexible Multiplex always appears in a circuit, i.e., with two way transmission and reception between two points, and both links are simultaneously recorded on the same magnetic tape. The recordings are then processed in NSA under conditions designed to give both the best possible transcription and an evaluation of the probable degree of garble. Research and Development on this problem, including the Central Prodessing Aspects, are continuing.

[redacted]

[redacted]

3. Noise Communications

A communication technique, attractive to communicators both because of certain concealment and anti-jamming features, is known as "noise communications" and is currently undergoing extensive experimentation by U. S. groups. (Noise communications, generally using some form of white, or apparently white, noise as the carrier to be modulated by the intelligence), follow directly from modern information theory studies and the various correlation time domain filtering techniques which are now advancing rapidly. [redacted]

4. Cryptographic Radiation

Various electrical and electromechanical devices, such as teletype machines may radiate signals which can be read on power lines and through the air, as well as on the signal line itself. [redacted] has been developed in studies designed to maintain the security of our own cryptographic devices. These techniques are, however, available for offensive use. Although most operations of this type would be covert, the possibility exists

[redacted]

II TRAFFIC OPERATIONS INDEPENDENT OF SYSTEM

A. Preliminary Processing

1. Logging and Editing

After traffic has been microfilmed and time-stamped it is brought into the analytic sections where it is separated into identifiable systems. A record of all traffic for which a section is responsible is maintained in the form of a log. Messages are hand sorted in an order determined by the format of the log and then recorded in the log by hand. Duplicate messages are noted at this point and messages are given worksheet numbers. Originals and duplicates are filed together. If textual material is to be keypunched into cards or tape the traffic is edited by the logger. This editing includes deletion of uninformative material, reordering of information, discrimination between textual and non-textual groups, correction of group length and run-together groups, etc. often the same messages are logged in two or more different ways by the same or different sections. Properly speaking, logging and editing are not readily separable. One set of logging information could be enough for logs for all needs if a means for ready resorting were available. Currently experiments are being made to determine techniques needed for machine editing. Time in preparing logs must be kept at a minimum for the older the log is the less valuable it becomes. Two prototype editing machines are under construction. When editing is performed logging information can and should be extracted. Logging currently requires about 2% of PROD man hours. As this is often routine and duplicated hand work there is a need for mechanization.

2. Data Conversion

Traffic arrives at NSA in as many as four different forms; hard copy, perforated paper tape, magnetic tape, and occasionally punched cards. In cases in which hard copy does not exist it is usually made. In addition edited versions of this data are required variously in punched cards, perforated paper tape, and magnetic tape as inputs to the various analytic machines. The same data may be required in more than one of these forms. Currently there is considerable duplication of punching in slightly varying forms.

3. Data Storage and Recovery

Currently all hard copy traffic is microfilmed and numbered in order of arrival. This number is needed to refer back to the microfilm. Ordinary photographic techniques must be used to obtain a print which can be used by the analyst. A problem of vast magnitude exists in the storage of collateral information used by the intelligence analysts. These files are of such a nature as to require continual addition both of new subjects and new information under old subjects. Much of the reproduction of this information is done by standard photographic techniques. The recording, reproduction, and cataloging of this material are all in need of mechanized aid. There is currently a study project on this topic.

B. Non-Textual Analysis

Traffic analysis can be thought of as all COMINT obtained from sources other than textual. Of primary importance is the reconstruction of communication nets employed by the enemy. Nets are reconstructed by the analysis of Call signs, frequencies, chatter, numbers, page and pad numbers, addresses, and collateral information. Continuities in one or more of the above mentioned categories may establish nets. Standard IBM sorting and indexing processes aid the traffic analyst, by speeding up and making more accurate his routine operations. These sorts are basically logs arranged according to various characteristics. Since most T/A operates on a reasonably current basis one of the principal problems is to shorten the time to get IBM runs made. This lag is both a function of IBM speeds, keypunch operator shortage, and the slowness of administrative procedures. Machine aids for these listings are needed to permit use of personnel for analytic operations rather than clerical. (Some call sign cryptanalytic problems exist which are suitable for solution by computer programs).

C. Textual Analysis

1. Plain Text Messages

Large volumes of plain text messages are received by NSA. Much of this is of a commercial nature and is of interest (depending upon the subject matter, firms, or countries involved) as providing valuable collateral information. Since the volume is so great as to preclude detailed examination of all messages, a preliminary scanning is performed upon incoming messages to see if they contain key words, addresses, etc. This is a human operation involving scanning overprinted perforator tape, extracting messages of interest, and printing on tape operated typewriters. When messages are selected for printing they are also categorized as to subject content according to the key words noted. Currently devices are under development both for automatic format controlled printing and for categorization together with format controlled printing. Possibilities for language translation have been considered briefly but no work is going on at the present time in NSA.

2. Commercial Code Messages

This problem is very similar to the plain text problem. Although little work is being done on such systems; it might be desired at some time to place more emphasis on them. Equipment similar to that required for plain text scanning could be used. The problem is simplified by the fact that code groups have a uniform length, and complicated by the fact that many codes might be used over one communications link. Equipment for printing code group meaning currently exists.

III DIAGNOSTIC OPERATIONS

A. Search for and Statistical Evaluation of Phenomena

In many cases traffic appears which is not plain text but has been encrypted by some unknown progess. It is necessary, in the absence of any pertinent information whatsoever, to attempt to make some sort of diagnosis of the crypto-system involved in order that an intelligent attack may be carried out. This diagnosis may be made upon the texts themselves (Identity) or upon some derivative text (Latent).

1. Identity

Among the characteristics which may be searched for are given monographic, digraphic or other polygraphic frequencies or roughness. Sets of messages having the same characteristics may be grouped together and differentiated from other groups of messages. Statistical phenomena occuring with certain periodicities may be sought for. All of these characteristics are searched for and evaluated by means of computers, counters, IBM equipment and in some cases desk aids. In addition to these countable phenomena of individual messages there are between-message phenomena such as high coincidence rates. Machines of the comparator class are used for this problem. Machine aid is usually that of pointing out where phenomena exist and of applying some statistical test of significance to them. Examination of the usefulness of the phenomena requires the work of a cryptanalyst. In performing these operations one of the largest problems is volume of work. For example, if 1000 messages are received per day in a certain system and they are to be compared with each other at all possible juxtapositions a total of about 500×10^6 coincidence searches must be made. This type of operation is being done currently. The problem of doing this for a month's or a year's traffic is overburdenning at present equipment speeds.

2. Latent

Other exploitable phenomena may not be observable from the text of the message itself, but rather from a derivative text such as might be formed by replacing each letter by the difference between itself and the preceding letter, or replacing each letter by the distance to the next repetition of that letter. When these derivative texts have been formed they may be examined as discussed in the preceding paragraph. In general, these latent properties are due to partial, but not complete duplication of variables in the enciphering process. In some cases data conversion and preparation equipment are able to form the derivative text while preparing the data for machine processing. Computers, comparators, counters, and IBM equipment are also used.

B. Tests of Specific Hypotheses

There may be cases in which there is some reason to suspect that a particular encrypting process is used. When this is so more powerful tests may be used to determine the validity of the hypothesis.

1. Machine Systems

Certain machine systems produce noticeable characteristics, for example, the Enigma type machine has the characteristic that a letter cannot encipher into itself. When a frequency count is made of the text letters which occur frequently in plaintext occur with below average frequency in cipher text. A single test of this nature may serve to prove or disprove a given hypothesis. Other machine systems have their individual characteristics which may be used to give more powerful tests. Computers, counters, and IBM equipment may be used to perform these diagnoses.

2. Hand Systems

In some cases it may be believed that a new, unenciphered code is in use. If a variety of traffic is being handled over the link in question, messages must be compared against themselves for within-message group coincidences. If codes become known or partially known messages may be compared with a recognition bank of known code groups and scored statistically. In many cases codes will be enciphered with what are supposed to be one-time-pads. Re-uses of this key may occur on a different link after an extended period. If key has been recovered from one use, other messages may be matched with the key, inspecting the results for either known or unknown codes. Because of the volumes of texts that might be involved all possibilities cannot be tested with present equipment. There must be a reasonable hypothesis that the situation exists before tests can be made. Counters, computers, test and recognition devices, and IBM equipment are all used for these problems.

IV OPERATIONS BASED ON KNOWLEDGE OF THE GENERAL SYSTEM

A. Machine Systems

1. Depth Search and Reading

If it has been determined that depths are likely to exist in a system, an effort is made to search for them. These may be observable from characteristics which appear in a log such as indicators, from high coincidence rates between messages or other observable phenomena. When depths have been found and if the underlying languages are at least partially known, assistance may be given to the cryptanalyst. This may be done by furnishing a list of pairs of words whose simultaneous occurrence is compatable with the texts involved and which have a good probability of occurrence in the language involved. Searching is done with IBM equipment, computers, comparators, and test and recognition devices while depth reading is usually done with test and recognition devices.

2. Machine Recovery and Setting

In most cipher machine systems there are two problems; machine recovery and setting. Machine recovery means recovery of the primary variables of the machine system while setting recovery normally refers to the recovery of the message-wise variables which are most often positions in the cipher machine cycle or cycles. Some machine recovery processes are largely statistical in nature. These may be performed on computers or IBM equipment. Others may require methods of attack combining logical steps with exhaustive trial techniques.

These require the assumption of a correct portion of plain text for a given cipher text together with assumption of certain of the periodic variables of the system. Exhaustive trial techniques applied to the remaining variables during the operation of an analogue to the cipher machine together with logical tests at each trial, serve to identify the remaining variables when the correct plain text assumption has been made. Setting and partial machine recovery as well as computers are used for this.

An example is that of a wired-rotor system in which the periodically changing parameters are identity of rotors, a wheel motion controlling element, and the arrangement of a set of manually inserted wires while the message-wise varying parameter is initial rotor settings. (The effect of the wires is to apply a self-inverse simple substitution to the plain text before it enters the rotor maze, and to apply the same simple substitution to the text emerging from the maze to form the final cipher text.)

The wiring of the rotor maze, together with a plain/cipher pair produced with that wiring carries with it a set of restrictions on the substitution, of the form "A is the substitute of B if and only if C is the substitute of D". Given a sequence of plain/cipher pairs and the wiring mazes producing them, the restrictions implied may be sufficient to determine uniquely the substitution. (For example, the two restrictions, "A is the substitution of B if and only if C is the substitution of D" and "A is the substitution of B if and only if C is the substitution of E" together imply that A is not the substitution of B, C is not the substitution of either D or E. A sufficient number of restrictions may yield "A is not the substitution of any letter except F", which is equivalent to "A is the substitute of F".) Moreover, if the logical process of determining the substitution is carried out using a sequence of wirings other than that actually used in the encipherment, if may be that no substitution will satisfy the implied restrictions - that is, the restrictions may be mutually contradictory.

Since, with a limited set of rotors, there is a limited set of mazes possible, and, in this system, rotor motion is strongly limited, it is possible to try for a given matched plain and cipher sequence, all possible maze wiring sequences, eliminating those which yield contradictions, in the effort to determine the substitution wiring.

In some machine systems, the indicators are such that even when all the periodic variables have been determined, the message-wise variables cannot be determined by an easy method. In the absence of any knowledge of the plain text (other than statistical) of a particular message, it may be necessary to do the equivalent of deciphering it for possible values of the message-wise variable and examine the results statistically to determine which actually is plain.

If there is a high probability that a certain word, or one of a list of words, occurs in the plain, it may be more economical to determine those values, if any, of the message-wise variables, which permit the simultaneous occurrence of the cipher text being examined, and one of the words of the list. Setting recovery and computers are used for this.

3. Decryption

At times, the cryptanalytic process yields complete information concerning a cryptographic period. (A period is an homogeneous set of cipher text which has been encrypted with a single cipher machine setup. Any message-wise variations in the machine setup are obtainable from the cipher texts.) It is then necessary to perform the decryption of all available text in accordance with the rules of the system and print the resulting plain. Analogs and decryption devices often using punched card or tape input are used for this.

B. Hand Systems

1. Additive Encipherment

Successful recovery of additively enciphered massages depends on predictability of the key. Key becomes predictable when (a) it is generated in a non-random manner or (b) when it is reused. Exploitable generated key is either produced by a definable process, in which case the problems of additive recovery become almost identical to those of reading machine encipherments, or produced by a unknown process which results in an exploitable characteristic (an example in monographic roughness). Reuse of key permits discovery of the reuse and recovery of the text based on the reconstruction of the key.

There are four facets to the wedges into additive encipherments: (a) System Discrimination, or the minimization of the number of variables that must be considered in reading a new system, is almost always performed by hand or on a computer because of the variability of the steps required; (b) Indicator Recovery, the utilization of the decipherment information supplied to the intended recipient by the sender, has been carried on almost entirely on IBM processes (particularly sorting) but, to a limited extent, has been done on computers and, recognition devices; (c) Depth Search, the discovery of messages having the same key, and isolog search, the discovery of messages having the same under-lying plain text and different (but exploitable) key, is of such importance that it has been attempted on most of the available equipments (comparators, computers, counters, IBM equipment and recognition equipments) as well as by hand; finally (d) Exploitation, the actual code or plain-text recovery on the basis of the information gained in one or more of the preceding steps, is of such a varied nature that virtually every analytic equipment; computers, comparators, counters, IBM and recognition equipment as well as decryption devices and hand method are in use.

2. [redacted]

EO 3.3(h)(2)
PL 86-36/50 USC 3605

[redacted]

These procedures are normally performed by computers although IBM equipments with many intervening manual steps have been used.

3. Additional Complex Procedures

There are many complicated procedures, more logical than statistical in nature which are used. An example is the solution of a simple columnar transposition, with underlying text ordinary language, but unknown subject matter. Here one will juxtapose each pair of sequences of text from the message which might be successive columns from the original form, and for each pair make an estimate of the relative probability of their arising causally. To the better scoring pairs, trial third columns are added, and new probability estimates and further eliminations are made, until a score is obtained which is unlikely to have been obtained by random in the number of trials attempted.

A second example is the case in which it is known that additive key has been derived by a specific complex manual process (with at least one variable of the system unknown) but such that the detailed nature of the underlying plain is unknown. Here it is necessary to follow the steps of the cipher clerk for each possible value of the missing parameter to generate trial additives, to strip each trial additive from the cipher text, and examine each resulting pseudo plain for language-like properties. Computers are best suited to this work.

V SUPPORT FUNCTIONS

These functions embrace a number of different activities which may employ mechanized aids. These activities are somewhat general to all cryptanalytic work and are not based on any particular traffic or system.

A. Linguistic and Statistical Aids

A number of special dictionaries and statistical studies based upon various languages of interest are required as aids to cryptanalysts. The dictionaries and statistics may be based upon particular traffic decryptions or upon general samples of the language. Dictionaries arranged in special ordering (such as backwards) may be desired. Frequent revision of dictionaries and statistical studies are required. Most studies of this nature have been made using IBM equipment. Some desired studies have not been made because too great a volume of IBM work would have been required. Besides linguistic studies large numbers of special mathematical and statistical tables have been prepared. These include special Poisson, binomial and multinomial tables and others. This work has been done both on IBM equipment and on computers.

B. Generation of Crypto-system data

It is sometimes desired to provide the analyst with listings of data pertaining to a particular cipher machine system. For example, tables which enable computation of cycle distance between specific machine settings and lists of successive settings of a cipher machine. In certain hand systems in which the combining of texts is done in several steps, tables showing the end results of the several steps for various variablew may be desired. These problems are normally done by IBM equipment or computers.

C. Desk Aids

There are a number of small devices which may be provided for the individual cryptanalyst to use directly along with his work. These include commercial adding machines and desk calculators, individual cipher machines, analogs of portions of various cyrpto processes, tallying counters and the like. Such devices may be very useful, providing that they are actually available to the person while working. There is a need for more such equipments to aid in removing clerical burdens from the analyst. Something which is one stage more erudite than a desk calculator would be of use.

D. Cryptanalytic research

There are times, in the course of current cryptanalysis, which during elements appear which are not subject to regular periodic change, but are such that a change in them would obviate current methods of attack. Again there are times when information as to new cipher machines or systems not inuse, but offered for sale, becomes available. In this sort of situation a substantial effort to prepare to solve a problem which may never exist is justified.

DRAFT

APPENDIX I

MACHINE AIDS

INTRODUCTION

In the following pages a brief description of computers and more special purpose devices is made. These descriptions are followed by a listing of the principal machine aids currently available for use, (or shortly to be in use). A short description of the principal functions of each are given. For the listing under computers, an attempt has been made to "define" the categories into which NSA computer programs fall. Some explanation is made as to why certain problems should be assigned to computers and others to special purpose devices in order that the reader may obtain a general notion of the areas in which computers and special purpose devices are best suited.

COMPUTERS

Besides large scale data handling problems, the Agency is faced with analytic problems which may be classified under two general headings: the "work horse" problems which require almost continuous effort to effect almost daily solutions, and problems which require machine effort on a much smaller scale and on a more sporadic time basis. Under the second type, one would include problems requiring only a few machine runs to effect a solution after which no immediate need for machine time is required. These problems are definitely handled by means of a general purpose computer or IBM equipment.

Under the "work horse" machine problems we have the following two classes:

Class 1. Problems which involve many and varied types of computational and logical operations and require a reasonable amount of machine time.

Class 2. Problems which involve a few operations but may require considerably more machine time.

It is felt that problems in Class 1 are best handled by general purpose digital computers, and that problems in Class 2, in most cases, are best handled by special purpose devices.

Problems in Class 1 might be handled quite well by special purpose devices. However, due to the variety of operations required to effect a solution, the equipment would well approach the design of a general purpose computer. For this reason it is deemed advisable to develop general purpose equipment with the idea that the added cost, if not excessive, is justified in having a device which has general utility even after the problem or problems which motivated the device no longer exists.

Problems in Class 2 are usually given every consideration as computer problems and are handled as such unless by virtue of size, importance, time consumption and monetary savings, it is decided that they warrant special purpose equipment.

COMPARATORS

In searches for causal characteristics (such as reuse of key, encipherment with most variables identical, etc.) it is often desired to make comparisons between texts in an effort to find if and where these circumstances exist. Among the "symptoms" being sought may be such items as high coincidence rates, similar repetition patterns, and characteristic frequency distributions.

Tasks of this nature are often performed on comparator equipments. These equipments have in general the ability to examine texts at many juxtapositions, to generate certain periodic texts, to make various combinations and comparisons using logical circuitry, and to count and compare results against a criterion in order to test for significant results. General purpose comparators, with great flexibility in problem capability, and limited purpose comparators are in use.

SETTING RECOVERERS

In a number of machine cipher systems all periodic variables are often recoverable leaving only a particular message variable, that of the position in the machine cycle, to be recovered. It is desired, therefore, to provide a means for recovering the position or setting of the machine at the start of the encipherment.

Setting recoverers are in general of two varieties: crib placement and statistical placement. In crib placement procedure, a probable plain text word (or crib) is assumed to underlie some position of the message and possible machine settings are tried on an exhaustive trial basis or by a series of logical tests to see if the assumption can be verified or proven false. In statistical placement procedure, a message is decrypted at all possible settings and the resultant possible plain text is examined for statistical plain text characteristics. Since certain languages have a very strong odd letter-even letter unbalance some procedures consider cipher, key and plain text streams solely on a modulo 2 basis for statistical placement.

SETTING AND PARTIAL MACHINE RECOVERERS

In some machine cipher systems not only the message setting but also some of the periodic machine variables are unknown. Procedures have been developed to solve both unknowns.simultaneously. These procedures generally involve exhaustive trial setting runs while applying logical procedures to test assumptions of the other variables. For these tests long cribs may be required, or very long cipher texts and statistical plain text characteristics may be used.

TEST AND RECOGNITION OR CRITERION DEVICES

In situations where key can be predicted or is used more than once, it is desirable to make tests for its occurrence in a particular position and recognize according to plain text (or plain code) characteristics. In the case of codes these may be known or unknown. When the code is unknown or cannot be predicted, recognition of plain code as opposed to random text must be performed by observing group repeats. Otherwise recognition of known code groups, known plain text groups or single letters, and plain text roughness are variously used. Provision must be made for the combining of streams of textual material according to the method of the crypto system involved and selecting the streams in the desired order.

ANALOGS, TEST AND DECRYPTION DEVICES

In the simulation of various cryptosystems a variety of devices is found useful to replace hand operations. A device may simulate all or part of the actions of either a machine system or a hand enciphered system and may have a manual, tape, or card input together with a tape, card, or printed output. Their principal utility is as a labor saving aid. They are aften used in the vicinity of the operating analytic section.

DATA CONVERSION, PREPARATION AND RECORDING

Since data may arrive at the Agency in a variety of forms including hard copy, perforated paper tape, punched cards, and magnetic tape and as it is utilized by both analytic machines and personnel in various of these forms devices are necessary to permit the conversion of data from one such form to another. At this time minor changes may be made in the data such as recoding in a different baud format, deletion of certain characters, insertion of indicative information and spaces, etc. Auxiliary input and output to analytic equipments are required. The variety of such equipments in use is very great.

COUNTERS

In the course of exploratory and cryptanalytic operations a large amount of information is often obtained from making counts of various textual characteristics. A number of specialized counting devices exist for the purpose of making these counts. The devices are often located in the vicinity of the using section.

SELECTION DEVICES

Large quantities of plain text material are received in perforated tape form. These messages require printing in an acceptable message format, and because of the volume involved, deletion of messages of little interest will be needed. By use of a list of key words pertaining to subjects of interest, this deletion function can be performed in a step prior to printing. Format is controlled by identification of heading indications, etc. Similar devices could handle commercial code material but are not currently being planned.

EDITING DEVICES

The possibilities of mechanised editing are currently beginning to be explored. The problems involve reordering of message information, deletion of superfluous material, adding auxiliary indicative information, collation of several versions of a message to produce a best copy, provision of output for logging, regrouping of information and many others. A first editing device, a limited purpose, character handling computer, is under construction.

IBM EQUIPMENT

This category includes standard IBM equipment plus modifications made to these equipments which enable problems peculiar to the Agency effort to be solved with more facility. The aggregate of ordinary and special IBM equipment is capable of performing tasks of any description (just as is a digital computer) but with certain drawbacks for very large operations including the requirement for manual handling of cards between steps of various operations, and the limitations on speed imposed by mechanical card handling.

DESK AIDS

In addition to all the machine aids previously listed, there is a final category of equipments which are used by the individual cryptanalysts at or on the desk. These include desk calculators, actual cipher machines, and special purpose devices used to simulate portions of a cryptosystem process. These devices are required in general to be small, simply operated and quiet.

DRAFT

1. COMPUTER PROGRAMS

A. Cipher Machine Analog and Simulation:

A program which simulates the operation of a cipher machine in order to study its cryptographic characteristics.

B. Machine Setting:

A program wherein partial knowledge of the machine is known and some subsidiary information (cribs, etc.) is employed to recover the initial setting of the machine.

C. Decrypting:

A program wherein the usually non-machine system is assumed and messages decrypted by means of system analog.

D. Key Study:

A program wherein key is analyzed with view to determine its characteristics and method of generation.

E. Computational:

A program wherein special counts and tables, etc. are made on sets of data.

F. Rough Key Exploitation:

A program wherein key characteristics rather than actual key values are exploited to obtain underlying "plain text".

G. Logical:

A program wherein the basic operation is one of comparing and ordering.

H. Statistical Research:

A program wherein the machine obtains information concerning a population by random sampling.

DRAFT

I. Mathematics Research:

A program wherein mathematical and statistical theory is tested for computational, statistical and cryptanalytic feasibility.

J. Engineering Research:

A program wherein designs or projected designs are analyzed for feasibility and optimal properties.

K. Intercept Studies:

These are programs involving intercept control and direction finding.

D R A F T

2. COMPARATORS

A.	AFSAF D1A	General Purpose High Speed Comparator (Perforated Paper Tape)
B.	Copperhead	Group Repeat Search between messages (Polystyrene tape)
C.	70 MM	Counts 1, 2, 3 and 4 character repeats (70 mm paper tape)
D	DELLA	Limited Purpose High Speed Comparator (1-64 character repeats) (Magnetic Tape)
E.	ROBIN	Coincidence Counter with Threshold (Perforated Paper Tape)
F.	IDA	Coincidence Counter between bands (Perforated Paper Tape)
G.	HYPO (See 3F)	Coincidence Counter with Threshold (35 mm film)

DRAFT

3. SETTING RECOVERY

A.	HECATE	Hagelin Message Setter (Crib)
B.	WARLOCK I	Hagelin Message Setter (Statistical)
C.	WARLOCK II	Wired Wheel Hagelin Message Setter (Statistical)
D.	VIVIAN	Hagelin Message Setter (5 Wheel Parity)
E.	HAGELIN MESSAGE SETTER	Hagelin Message Setter (3 Wheel Parity)
F.	HYPO (See 2G)	Enigma Hagelin Message Setter (3 wheel Hagelin max.)
G.	FIRECRACKER	Purple Machine Message Setter (Crib)
H.	GRENADE	Enigma Setting

DRAFT

4. SETTING AND PARTIAL MACHINE RECOVERY

A.	BOMBE	Enigma Wheel Order and Stecker Recovery
B.	FROG	[redacted] Stecker and Setting Recovery
C.	BRIDE	General Wired Wheel Stecker, Order, Setting Recovery

EO 3.3(h)(2)
PL 86-36/50 USC 3605

DRAFT

5. TEST AND RECOGNITION OR CRITERION

A.	DEMON II	[redacted]
B.	SKATE II	[redacted] Key Finder/Slide Run
C.	DEMON III	Depth of 2 reading/Key Stripping (Base 32: 5 characters; Base 10: up to 15 characters)
D.	SLED I	Wired wheel decipherment/Depth search/ Key finder/Coincidence counts/group I.C. counts/chaining
E.	DUCHESS	Group I.C. counts of differences $\left\{\sum \frac{f(f-1)}{2}\right\}$
F.	MISTRESS	Placode finding (repeat search)
G.	GEEWHIZZER	Digraph weighting of cipher text/Fourier weighting of cipher digraphs

EO 3.3(h)(2)
PL 86-36/50 USC 3605

~~TOP SECRET~~ ~~FROTH~~

EO 3.3(h)(2)
PL 86-36/50 USC 3605

DRAFT

6. ANALOGS, TEST AND DECRYPTION DEVICES

A.	B-211	[redacted] B-211 Analog
B.	C-38 (NAG)	Hagelin C-38 Analog
C.	SATYR	Hagelin C-38 Analog
D.	STURGEON Analog	Model C, D and E in one package
E.	EMBRYO OPHIS	G.P. wired wheel
F.	BABY OPHIS	G.P. wired wheel
G.	ROE	Deciphers Sturgeon traffic using externally prepared key tapes
H.	HELLCAT	Polyalphabetic (26) decipherer
I.	AFSAF D6Ø	[redacted] "N" square decipherer
J.	MAISIE	Code lookup and printer
K.	PEELER	Additive Stripper and Tester
L.	MATTHEW	Strips key from cipher using externally prepared key tapes
M.	Chinese Typewriter	Draws a stylized (straight line) characters from special coding in that card
N.	CALL 35	Call sign decipherment
O.	HOYLE	Playfair decipherment
P.	M-8	Enigma Analog and/or "Key" generation
Q.	PADDLE	Decipherment of two letter enciphered code

EO 3.3(h)(2)
PL 86-36/50 USC 3605

~~TOP SECRET~~ ~~FROTH~~

DRAFT

7. DATA CONVERSION, PREPARATION AND RECORDING

A.	MILLIE	Perforated Paper Tape to magnetic tape ("regen" or patternized)
B.	MATTHEW	2-to-1 conversion of perforated paper tape
C.	JOHN	Mononome Dinome Decipherment
D.	ASAF 25	High speed perforated paper tape reader (Potter) used in tape checking
E.	BUNNY	High speed perforated paper tape pluggable regen and patternizer
F.	CENSOR	Checker for coded paper tapes (Atlas, Demon)
G.	AYE AYE	Perforated paper tape patternizer
H.	PRIMATE	Computer Program Tape Punch
I.	MAYBE	Computer Magnetic Tape Preparation Device
J.	CXCO	Perforated Tape Readers, Typewriters and Punches
K.	CAPPY	Card to Tape Converter
L.	TIZZY	Tape to Card Converter
M.	AFSAF 44	High speed digital and/or literal recorder
N.	Hi Speed TT Reader	High speed mechanical perforated tape reader
O.	Hi Speed TT Punch	High speed perforated tape punch
P.	Ferranti Reader	High speed photoelectric perforated tape reader

DRAFT

9. COUNTERS

A.	CADILLAC	Monographic Counter/I. C. computation/ baud level totals
B.	BABY ALCATRAZ	36 category monographic frequency counter (differencing optional)
C.	DELTA COUNTER	Counts baud-no baud changes in 5 levels plus character totals
D.	DELTA-DOT COUNTER	Counts runs of bauds and no bauds in 5 levels of tape
E.	DIFFERENCE COUNTER	Counts differences between two tapes (digital)
F.	DINOME COUNTER	Counts dinomes supplied as one digit from each of two tapes

DRAFT

10. SELECTION DEVICES

A.	PATRICIA	Message Categorization Unit
B.	BUDDY	Message ending recognition - Format Controlled Printing
C.	PADDY	Message Categorization - ending Recognition - Format Control Printing

DRAFT

11. EDITING DEVICES

A.	BOGART	Limited purpose character handling computer

DRAFT

12. IBM EQUIPMENT

A.	Standard IBM	Punches, Verifiers, Sorters, Collators, Reproducers, Tabulators
B.	Special IBM	Coordinating Reproducer, Brute Force Device, Card-to-Tape, Tape-to-Card
C.	Auxiliary Devices	Relay Gates
D.	604	Small General Purpose Calculator

DRAFT

13. DESK AIDS

A.	Calculators	Computational Work
B.	NCR	Additive testing
C.	B-211 Handtester	B-211 testing
D.	Electric Hagelin	Keyboard C-38
E.	WW Handtester	General Wired Wheel testing
F.	PICCOLO	[redacted] Crib Tester and Decipherer
G.	ROSE	Sturgeon Crib Tester and Decipherer