~~TOP SECRET~~ Draft 16 June 52

~~TOP SECRET~~

Some Circumstances Under Which Automatic Operation Can Benefit the Cryptanalytic Effort

I. Operation with quantities of traffic.

A. Preparation of prints for T/A, and traffic logs for C/A.

Operations involved are transcription of selected parts of traffic from written form to a form which can be read by machine, numerous reorderings according to simple rules, and printing.

B. Selection and printing of plain text material.

Very large quantities of plain text traffic, mostly sent by automatic means and therefore received on perforated tape, are handled. It is required that a selection be made to eliminate obviously uninformative material, the residue being printed, and that a further selection be made to retain only information of interest, and that retained translated.

C. Preparation of prints of multiplex transmissions.

For those multiplex RTP transmissions in which the enciphering process is associated with the multiplexing rather than with the operation of individual channels, it is required that the analyst be presented with a print, on which the text of all channels appears on the same page, and in such form that it is readily seen which characters of different channels were sent in

~~TOP SECRET~~

the same max cycle. In at least one such system, it is desired that certain elementary statistical counts appear with the print of the cipher text.

B. Presentation of quality and timing information.

For certain systems it is desirable that the analyst be presented with a print of cipher text which carries with each letter an indication of the probability of a garble, and in some cases also a time measure.

II. Operations determined by degree of ignorance.

A. Systematic statistical analysis for diagnostic purposes.

Analysis of individual messages or groups of cryptographically related messages may yield useful information, such as "This is a digraph substitution", or "In this system, no letter enciphers as itself", or "Here there is a detectable cryptographic change at noon every day", or "This cipher text is statistically indistinguishable from random".

B. "Blind" search for favorable circumstances.

Systematic search for pairs of messages with unusual similarity may uncover depths, cryptographic error, or other misuse. "Similarity" may include equality of length, pattern equivalence, common textual groups, common indicator groups, similar frequency counts, or some unanticipated unspecified phenomenon. Machine aid here is merely the bringing together one or more of pairs of

~~TOP SECRET~~

messages, the real identification of favorable circumstances cryptanalytically useful being made by an analyst.

XII. Operations becoming appropriate due to the acquisition of specific items of knowledge.

(Operations in this class can rarely be performed until the analyst has made at least one examination of the text being worked on. Frequently there are a number of operations in succession, but which operation is done next is determined by the results of a previous operation.)

A. Depth Search.

If it has been determined that depths ~~regularly~~ exist in normally occur a system, and recognizable manifestations of depth observed— such as indicator similarities, or multiple group coincidences— a search for these manifestations will be made.

B. Pattern repeat search.

Some cipher systems have the property that if in two encipherments of the same plain text nearly but not all of the system variables are the same, the two resulting cipher texts will be simple substitutions of one another. Under these circumstances, a search is made for pairs of stretches of cipher texts bearing this relation.

C. Demon/Sled type operations.

If depths have been found, and the underlying languages are at least partially known, assistance may be given to the

" Depth reading or "Cross-matching"?

~~TOP SECRET~~

analyst, by presenting him with a list of pairs of words along with their meanings, each word having a positive probability of occurrence in one of the messages of the depth, and such that their simultaneous occurrence is consistent with the cipher text under examination. (A literal or digital code is here considered as a "language".)

B. Bombe/Frog type operation.

Machine setting by combinations determining periodic variables

For some machine cipher systems, there are means of attack, combining logical steps with exhaustive trial techniques, which require matched plain and cipher texts and utilize one or several analogues of the cipher machine, which yield some of the periodic variables of the system.

E. Nocate/Wenlock type operations.

Machine setting by statistics determining message variables

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 any 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 variables 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

~~TOP SECRET~~

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.

F. Routine decryption.

At times, the cryptanalytic process yields complete information concerning a cryptographic period. 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.

G. Printing meanings for code groups.

At times, messages are fully decrypted, yielding plain code, by some process not involving meanings of the groups. It is then necessary to print, ordinarily in the original language, the meanings of those groups having known meanings.

H. Partial decipherment.

In the course of attack on a multiple step cryptographic system,

[redacted]

I. Preparation of work sheets.

Analysts often desire cipher text and relevant information printed in accordance with rules which depend on the state of solution of the problem being worked on.

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

3. Exploitation of obscure statistical phenomena.

At times additive key which is used only once,

[redacted]

Here one needs to provide the analyst with pairs of groups, one of which has a probability of occurring as a fragment of plain text, and the other of which has a probability of being produced as

[redacted]

Another favorable case is that which the

[redacted]

K. Procedures involving relatively complex manipulative and logical steps.

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 can be successive columns from the original form, and for each pair make an estimate of the relative probability of their arising casually. 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 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.

~~TOP SECRET~~

IV. Operations not having traffic as basic data.

A. Preparation of special dictionaries, language statistical records, and other linguistic aids.

For use by the analyst at his desk, a variety of dictionary or catalogue type listings with statistical information are required. The information contained in these frequently, but not always, comes from the text of previously decrypted messages. (Here also, a code may be considered as a language.) Characteristically, frequent revision is required as more information becomes available.

B. Preparation of catalogues, tables and listings, where basic data is from specific cipher machines or cryptographic systems.

Hand cryptanalysis is often aided by the ready availability of systematic listings of the results of the performance of substeps of the cryptographic system.

C. Provision of at-the-desk mechanical aids and analogues.

In addition to printed material, analogues of cipher machines, devices which emulate cryptographers, and devices for doing certain types of clerical work may be highly useful, provided that they are at hand, rather than at a remote location.

D. Development of machine techniques in anticipation of problems.

At times in the course of current cryptanalysis, there appear elements not subject to regular periodic change, but such

that a change in them would obviate current methods of attack. Where circumstances suggest a likelihood of such a change, a substantial effort to prepare to solve a problem which will possibly never exist may be justified.

E. Provision of equipment maintainable by relatively unskilled personnel.

This requirement exists by virtue of the unavoidable need to use "short-term" military and other ill-trained men for maintenance.