~~SECURITY INFORMATION~~
~~TOP SECRET SUEDE~~

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

~~TOP SECRET SUEDE - SECURITY INFORMATION~~

COPY

AFSA-23

Necessity of Plain Text in Cryptanalysis
AFSA-23C3 28 February 1952

1. All sections of AFSA 23C are reading some of the cryptographic systems of the countries with which they are concerned. The availability of plain text material has been found invaluable in many cases; on several occasions it has led to solution of new systems. All cryptanalysts and translators will testify to the necessity of bringing together all related data for the optimum exploitation of communications intelligence. Specific examples are cited below.

2. A cryptographic system is not solved in a vacuum nor in an ivory tower of abstract mathematics. Tho basis of operations at AFSA, namely that one operating unit shall process the traffic of a specific country, cipher and plain text, has proved its value. This method has involved the correlation of all available information, historical background, current collateral, plain text and cipher traffic, all of which are essential, not only in cryptanalytic solution but also in scanning, priority assignment and translation of communications intelligence. It is a basic principle in analytic research that all available pertinent materials of a specific, homogeneous type be studied together. The production of communications intelligence is no exception. In an analysis of messages dealing with a specific topic all available messages should be included in the study; the original external form of such messages, whether plain text or cipher, transmitted by teletype, Morse, voice or some other medium, is an incidental feature which has no relevant bearing on the methods of producing COMINT. AFSA's mission is the production of communications intelligence; if AFSA is to carry out its mission, plain text and cipher must not be separated.

3. In addition to the broad requirement for study of plain text in cryptanalysis, the following are specific instances of solution of cipher by use of plain text in AFSA-233:

a. AFSA-[redacted] airfields are referred to by number, and the place name is not mentioned. Thanks to a plain text message addressed to an individual at [redacted]

b. AFSA-[redacted] Message numbers of diplomatic communications include plain text messages in the same series. Present study of these numbers which are suspected of indicating the subject matter, requires the analysis of plain text as well as cipher traffic to test this theory. Once the theory is confirmed, the words, names and phrases of plain text will be used to assume cipher text and thus to verify key. The [redacted] In the recently solved [redacted]

~~TOP SECRET SUEDE~~

App 5

Declassified and approved for release by NSA on 05-30-2014 pursuant to E.O. 13526

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

COPY

Necessity of Plain Text in Cryptanalysis Cont'd

AFSA-23 AFSA-23C3 28 February 1952

c. AFSA-[redacted] Plain text traffic is scanned thoroughly for aid in code recovery of the [redacted] Only recently it was possible to establish the code value for [redacted] because of a plain text message dealing with the same general subject [redacted] referred to the procurement of 2000 and an unrecovered group. From an English and a [redacted] plain text message it was obvious that the group was "mules."

d. AFSA-[redacted] Thanks to a personal plain text message from Phyongyang it was possible to solve the [redacted] By assuming that a cipher message of the same date was signed by the same person, [redacted] his name was cribbed in at the end, and the digraphic substitution square was subsequently recovered.

e. AFSA-[redacted] A circular message was sent out to consulates in both cipher and plain text. When these messages were identified as duplicates, it was possible to [redacted] text was used, by inserting the text from tho plain text transmission.

f. AFSA-[redacted]

[redacted] providing names of people and places, subject matter and phraseology. At present, plain text files are being compiled to aid breaking in the new [redacted]

2) Police plain text has constantly been of great help in roading both regular and security police systems. Warrants for arrest are very often sent in plain text on one link and in one or more police systems (for example: [redacted] on other links. Plain text is particularly important here for providing general phraseology and identification of abbreviations found in the cipher text.

3) Military plain text, [redacted] although comparatively rarely sent, has made possible identification of a few of the more difficult code values in [redacted] for example, the group meaning "Army General Staff."

4) Plain text on the national [redacted] has made possible the identification of 19 of 20 links. Since the cipher material is different for each lane in the [redacted] and probably [redacted] the identification of links is vital.

5) Plain text has been invaluable in training linguists and crypto-linguists. It is used in the [redacted] class given at present by Mr. John Murphy. New linguists in the section are always broken in on plain text.

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

~~TOP SECRET SUEDE - SECURITY INFORMATION~~

COPY

Necessity of Plain Text in Cryptanalysis Cont'd

AFSA-23 AFSA-23C3 28 February 1952

6) Plain text provides not only training material, but constant working material. Thus when an important system becomes readable, translators can be pulled temporarily off plain text, and conversely if an important priority is given out for a subject found in plain text, or if a large cipher system becomes unreadable, translators can be shifted temporarily to plain text. All this increases the flexibility and efficiency of the section as a whole.

g. AFSA-[redacted] section has developed new mathematical techniques for attacking the major [redacted] By using the phraseology from several plain text messages of the same date period, it was possible to predict text and to verify both text and key on a [redacted] thus gaining entry into hitherto unreadable traffic, and thus confirming the effectiveness of the new techniques.

h. AFSA[redacted] The break into code recovery on the two readable and one partially readable [redacted] systems was accomplished by the fact that most [redacted] plain text refers to cipher messages and vice versa. A start in solving the construction of the presently unreadable [redacted] system which contains five code books super-enciphered with additive has been greatly aided by plain text references to tables, codes, additive, etc. When solution of the system reaches book-breaking stage, the [redacted] plain text messages of the same period will be the springboard from which the leap into first recoveries will be made. One of the previous [redacted] was solved with the aid of [redacted] in the plain text. This has been the history of all plain text and cipher traffic. It is so intermingled that the separation of one from the other would present to the cryptanalyst and book-breaker an almost unsurmountable difficulty.

[redacted] has been facilitated by the collation of plain text and cipher. References in plain text to cipher messages provide information of the content of the cipher message, names, addresses, format, etc. At present there is on file in the section a large group (100 to 200 plain text messages) which refer to the presently unreadable [redacted] These, when the super encipherment is solved (and they may well help to solve it) will provide for the book-breader suggestions as to the contents of encoded messages.

[redacted] The subjects of traffic in the diplomatic system [redacted] are predominantly foreign trade and commercial in nature. When working on book text recovery or on recovery of substitution squares it has been and will continue to be important to know as much as possible about all details of the trade transactions as given by plain text. This includes the commodities involved, ships and shipping arrangements, established practices, format and usual phraseology of these messages, signatures, etc. That knowledge of this

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

~~TOP SECRET SUEDE~~

~~TOP SECRET SUEDE - SECURITY INFORMATION~~

COPY

Necessity of Plain Text in Cryptanalysis Cont'd

AFSA-23 AFSA-23C3 28 February 1952

sort is indispensable for the training of new personnel who are to be initiated into this work is beyond question. As for the strictly diplomatic portion of this material, plain text traffic has in the past yielded important collateral information without which the breaking of cipher would have been far more difficult if not impossible. It has yielded details to confirm the accuracy of questionable or partially unreadable cipher materials, as in the case of lists of films which were sent from [redacted] to China. Names of personalities such as [redacted] first occurring in plain text soon appeared in cipher also. Previous recognition of the name [redacted] facilitated breaking into the [redacted] substitution squares, since as soon as a portion of the word appeared, the analyst was able to recognize this otherwise unusual form as a possible portion of the text.

That there is a certain amount of intermingling of plain and cipher is shown by the fact that tables of contents of training films first requested from [redacted] in a cipher message were furnished in a plain text reply from [redacted]

4. Brilliant cryptanalytic work has been done by crypto-linguists who used their language first in the translation of [redacted] plain text traffic. When they were assigned to [redacted] much of whose traffic deals with foreign trade, they were able to predict text not only because of their knowledge of the language, but because of their background in [redacted] communications of the country concerned.

5. The inter-relation of plain text is further illustrated by the fact that certain countries encipher communications which other countries may send in the clear. All the voluminous communications on trade between [redacted] and [redacted] are in cipher, but relays of shipments of goods from [redacted] to [redacted] may come in plain language messages between [redacted] Trade between [redacted] and [redacted] is discussed in plain text; the same type of transactions are dealt with in the high-grade [redacted] cipher system. It is impossible to divorce one type of communication from another, either by subject matter or manner of transmission.

ELIZABETH R. BROWNELL
AFSA-23C3

~~TOP SECRET SUEDE~~