

VALUE OF TICOM DOCUMENTS IN WESTERN AREA SECTIONS

AFSA 14  
Via 02, 23, 23B

23B4

21 Feb. 1952

TICOM documents have since 1945 proved to be of invaluable help to a number of cryptanalytic sections working on countries in the Western Area, and a re-survey of the documents available is currently bringing to light additional material which will considerably expand its usefulness.

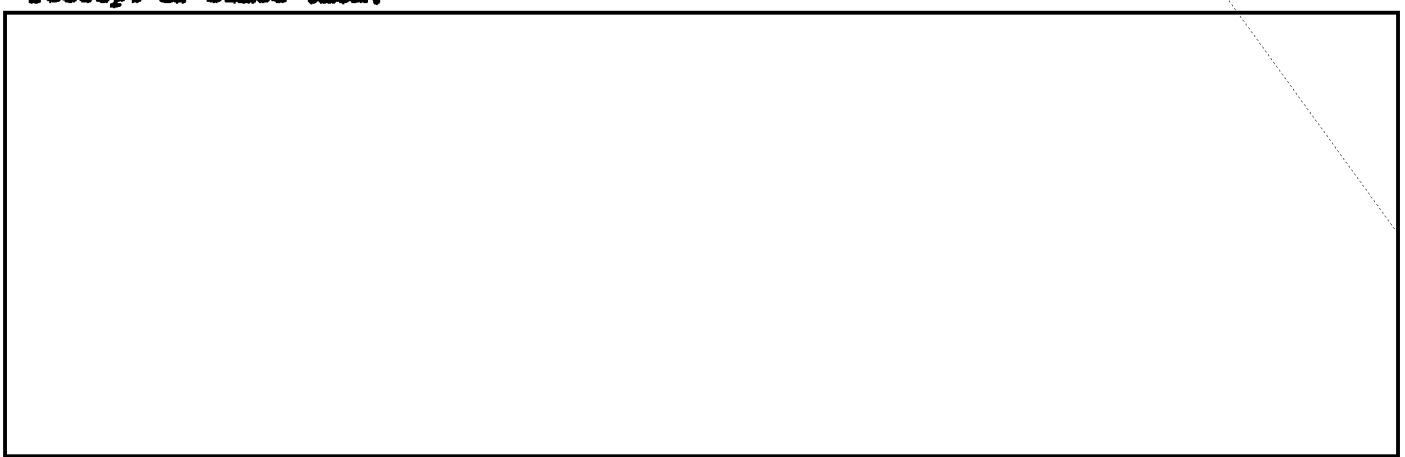
These documents have in general provided two kinds of assistance:

I. Direct: Specific codebooks and keys still in active use.

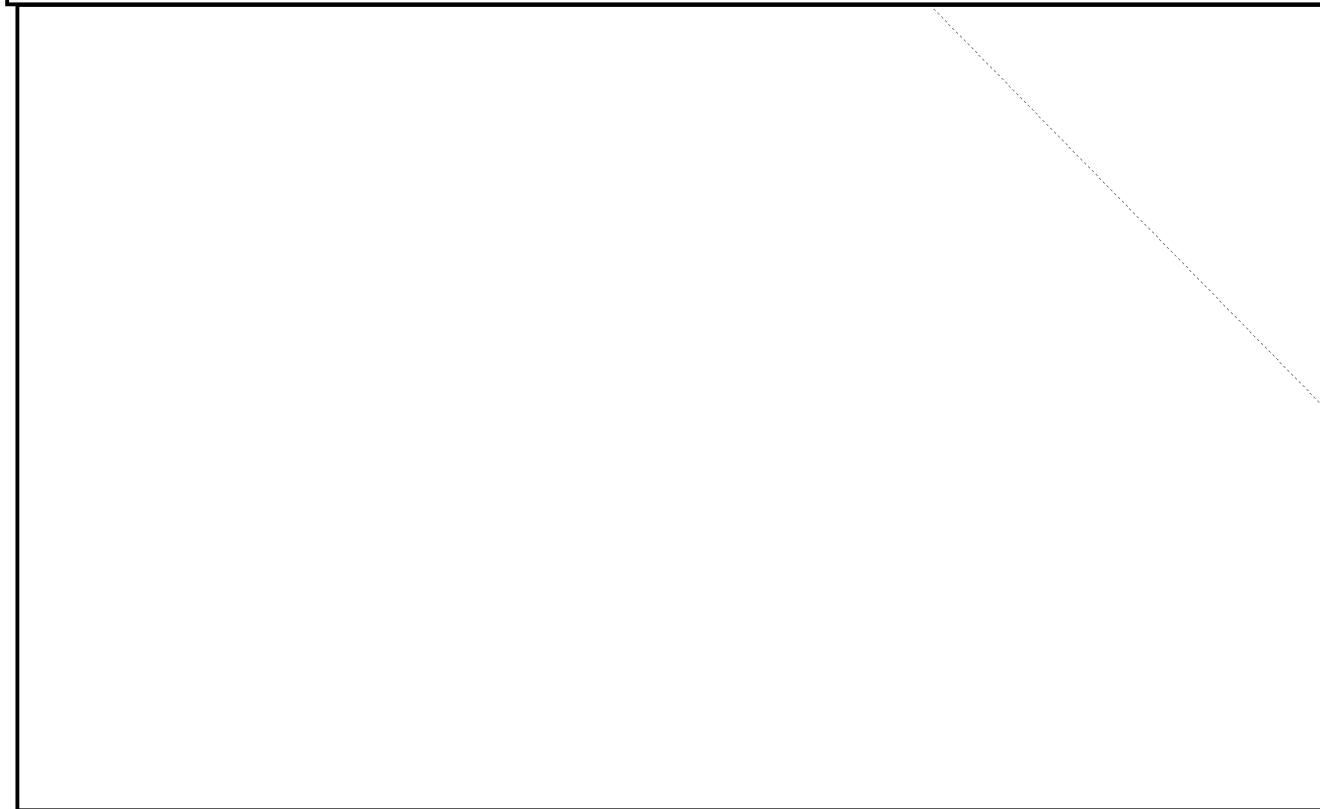
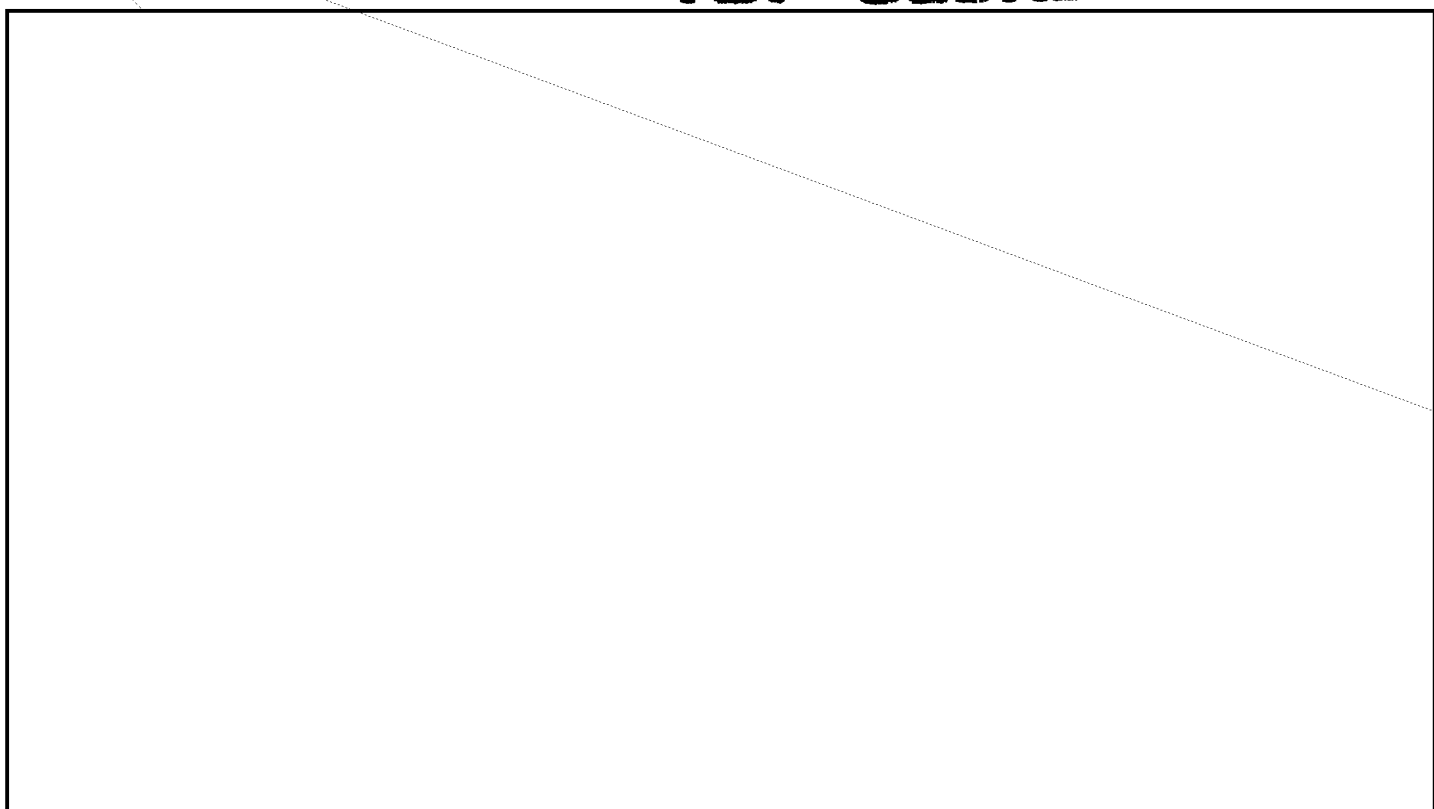
II. Indirect: A background of information on construction of codebooks, general cryptographic practice, code instructions, security consciousness, crypt vocabulary, and the like. Such a historical perspective is of incalculable value in understanding the present.

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

I. Listed below are TICOM documents which have been of direct immediate use, giving specific codes or tables in current use at the time of receipt or since then:



~~TOP SECRET SUEDE~~



~~TOP SECRET SUEDE~~

Identification of these compromised codebooks with actively used systems has resulted in the saving of inestimable sums of money in bookbreaking personnel, and of months and even years of valuable time in reading the traffic and getting the intelligence to the interested consumers. Such identification, it should be pointed out, does not take place once and for all, making it possible to discard the residue. The last example given is evidence of the continuing usefulness of keeping TICOM documents readily available as new discoveries and problems disclose a need for material previously thought valueless.

II. No less important - in fact the chief enduring importance of TICOM - is its value in giving a historical perspective on cryptographic practices of a given country, thus casting the light of the past on present problems. This light comes from various sources: obsolete codebooks or enciphering keys, code and encipherment instructions (many of which accompany the codebooks and keys), general cryptographic manuals, German reports of their cryptanalytic progress on systems of various countries, and even sometimes old wartime traffic and intra-governmental correspondence.

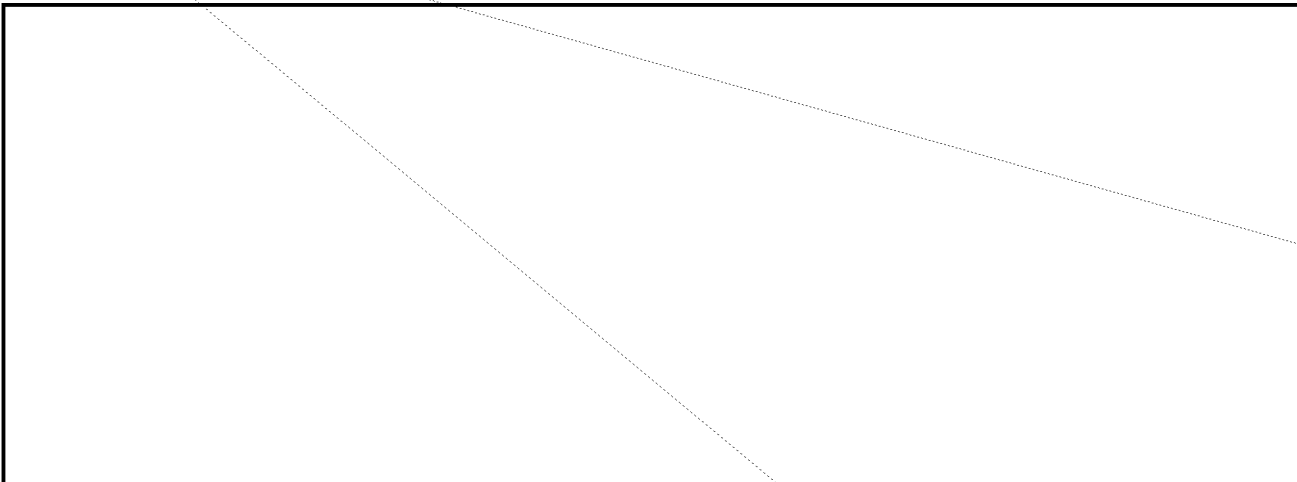
EO 3.3(h)(2)  
PL 86-36/50 USC 3605

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

REF ID: A68702

~~TOP SECRET~~

~~SUEDE~~



Thus TICOM has played a considerable role in turning the art of  
bookbreaking into a science.

~~TOP SECRET SUEDE~~

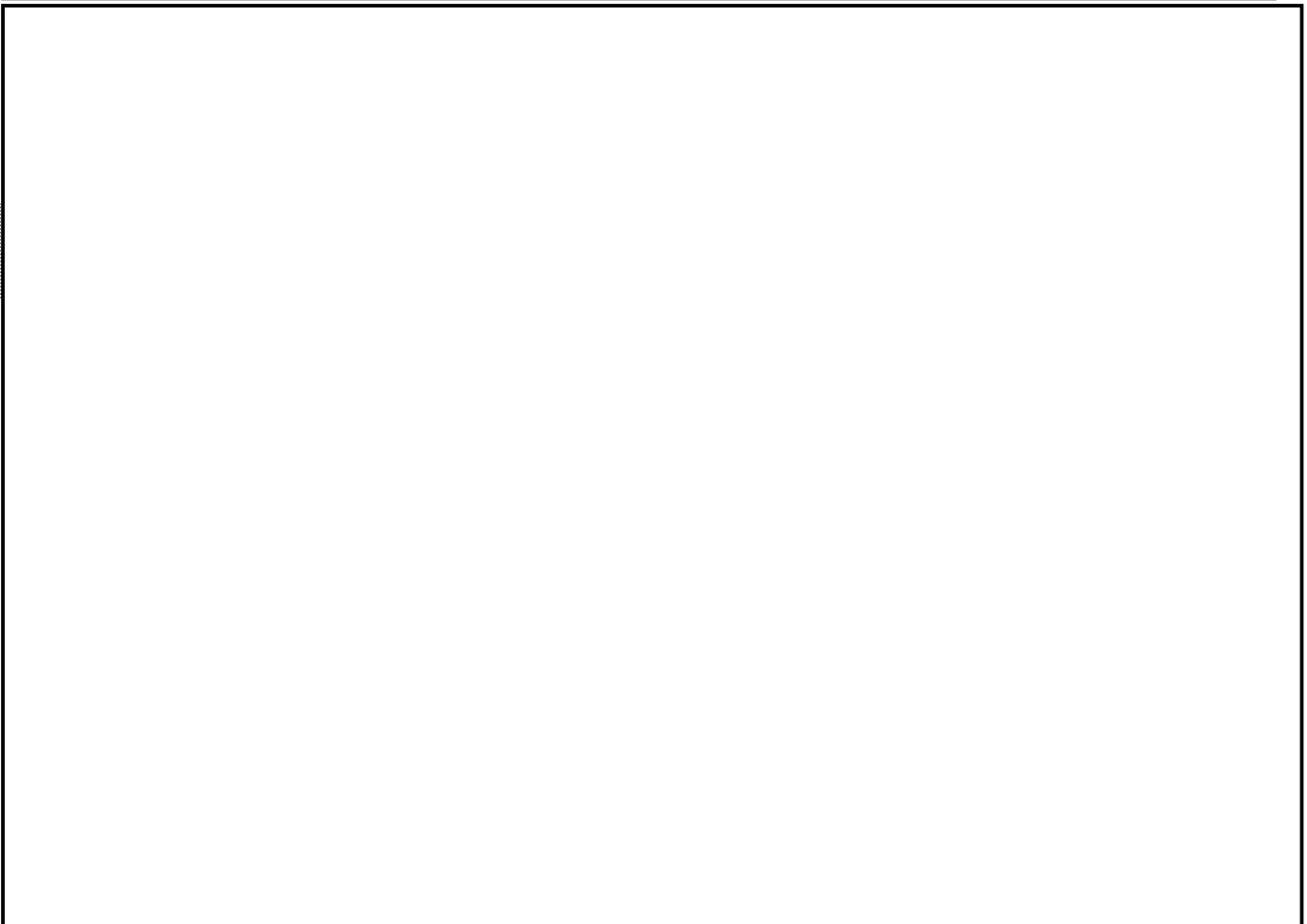
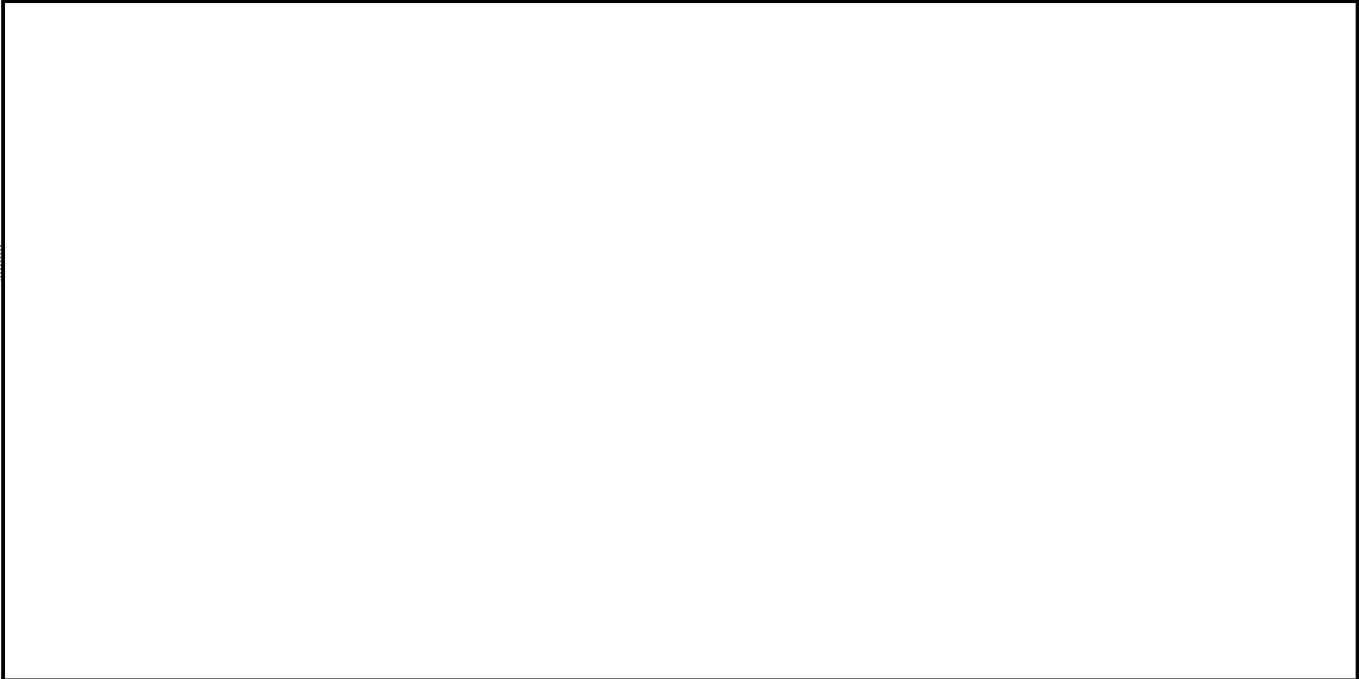
EO 3.3(h)(2)  
PL 86-36/50 USC 3605

REF ID: A66702

~~TOP SECRET~~

~~SUEDE~~

SECRET



~~TOP SECRET~~ ~~SUEDE~~

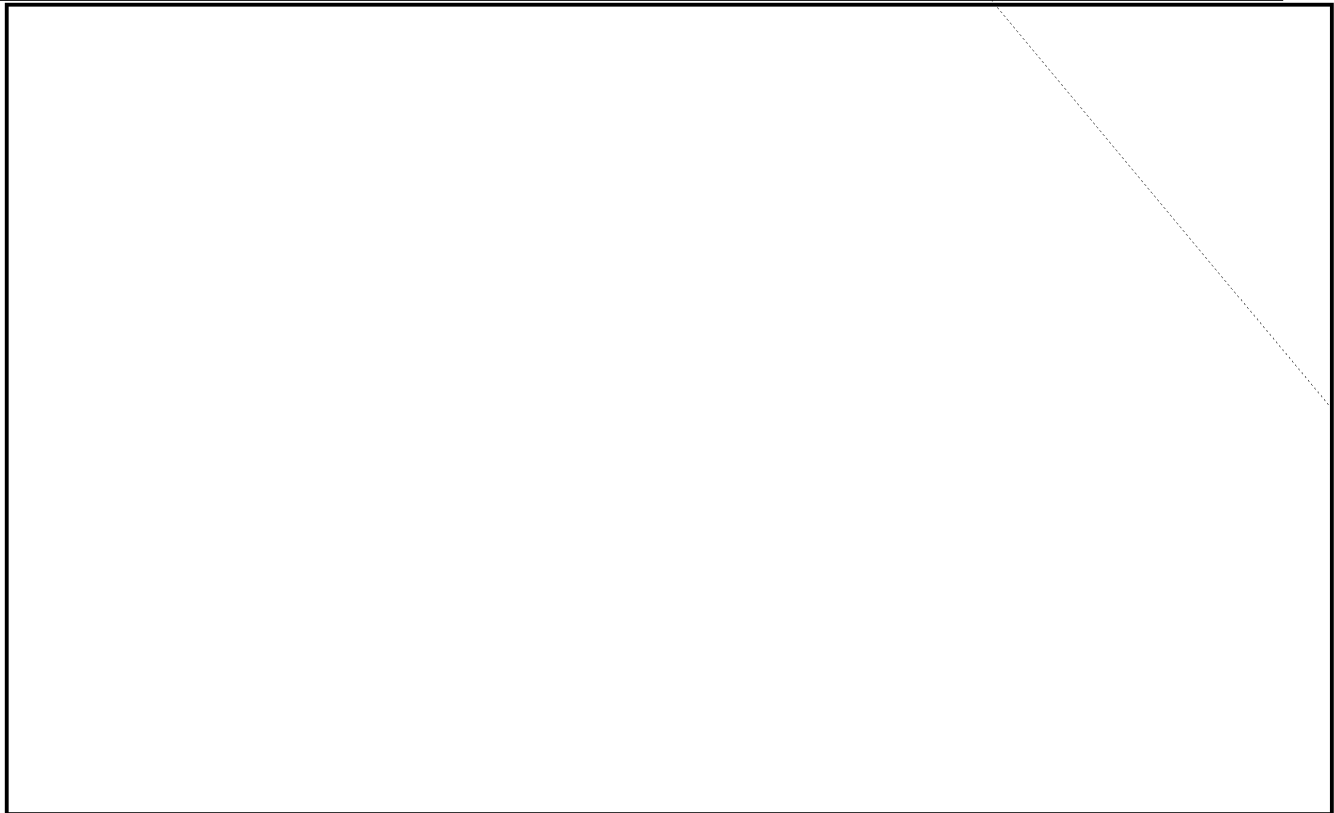
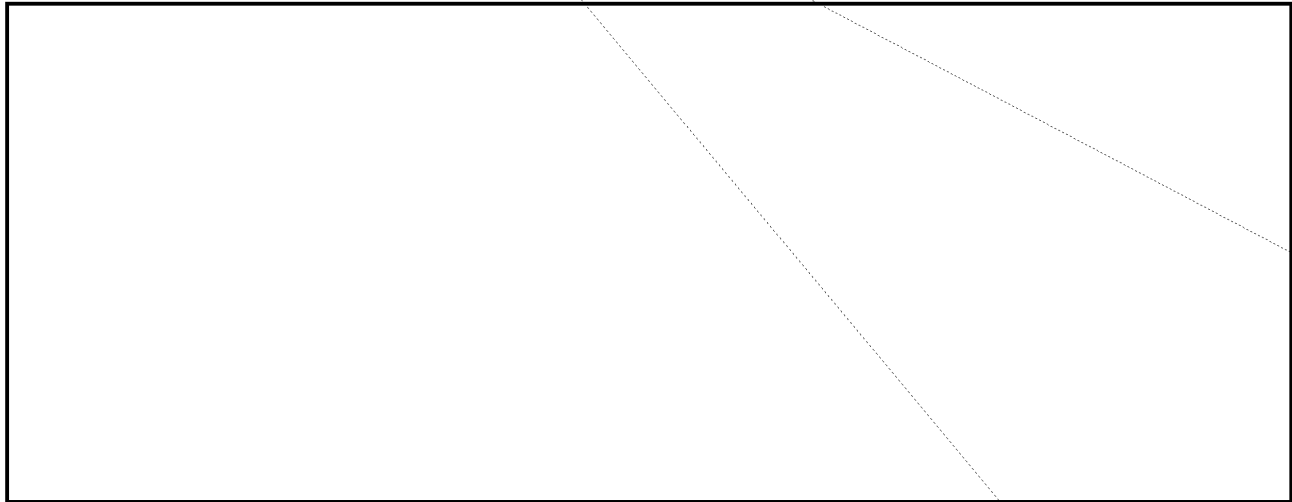
~~TOP SECRET SUEDE~~

EO 3.3(h)(2)

PL 86-36/50 USC 3605

D. German reports.

German wartime cryptanalytic progress reports on systems of various countries have as a rule contributed little that was not already known here.



The value of all this general background material is none the less real for being beyond the limits of precise measurement.

*Katherine L. Swift*

~~TOP SECRET SUEDE~~