German Agent Systems of World War II

BY FRANK W. LEWIS

~~Secret~~

INTRODUCTION

One of the more intriguing stories of U.S. cryptanalytic success during World War II concerns itself with the German cloak-and-dagger boys in South America. Leafing through the pages of news-weeklies of the period, one would hardly suppose that credit for rounding up the several gangs of conspirators belonged to other than the usual under-cover law enforcement groups; and although the story as told was highly exciting, only by knowledge of the behind-the-scenes activity of our own cryptanalytic group can one appreciate the true picture.

Since few records are available from which to draw examples (or corroborate details) this present account represents the personalized understanding of the author as to what happened, as it happened, within the purview of the Signal Intelligence Section of the Office of the Chief Signal Officer (one of the phases the Army portion of the Agency's predecessors went through).

A certain amount of charity should be shown toward the author if he seems particularly vague in matters of geography or calendar events—the story is basically true, even though examples are illustrative rather than actual.

Long before Pearl Harbor, German agents were active in Spain and South America, carrying on their traditional role in the very thinly veiled disguise of commercial representatives. In particular, a respectable commercial aura was given to their communications, with banking addresses being used on supposedly straightforward encoded, but presumably business-type, financial messages. An address such as SUDAMERIAT WEDEKIND appeared innocent enough but actually covered arrangements for contact, pick-up points, and general activities of a network of German agents. Since we were fortunate enough to break their systems and (because of our 24-hour watch) were reading messages before the recipient had even picked up his copy, the round-up of the entire gang was due in an appreciable measure to our cryptanalytic effort.

Three cryptographic systems come to mind (which have "success story" overtones) that bear setting down on paper, since a cryptanalytic moral can perhaps be drawn from an account of our trials—and errors.

We will briefly discuss the breaking of a grille transposition; a Kryha encipherment (of both plain language and code); and a dictionary code, with one or two mildly embarassing *gaffes* recounted to illustrate the rocky road of the cryptanalyst in his pursuit of plain text. (By tempering success stories with confessions of less-than-brilliant excursions, perhaps one can get away with what otherwise would appear chest-thumping!) It should also be understood that the original analysis of most of the agent systems was very competently performed by agencies other than our own; the dictionary code and Kryha happen to be two examples wherein we independently played a critical role.

Lest the reader react with a "so what's the Big Deal?" to this pronouncement of success on what might now be considered relatively insecure systems, the stage should be set according to the times of this period piece. Of the 40 or 50 "agency personnel," only a handful were available for the entire German problem—diplomatic, military and agent. (The stories of GEC, the double additive system, and GEE, the one-time-pad system have already been recounted in the *Journal*.) Very little machine help (in the form of relatively primitive IBM equipment) could be expected, and neither the level of sophistication of cryptographic techniques nor the accumulated skill of wartime effort on increasingly complex problems had reached maturity. In those days, we learned by doing, with no body of accumulated knowledge to fall back on.

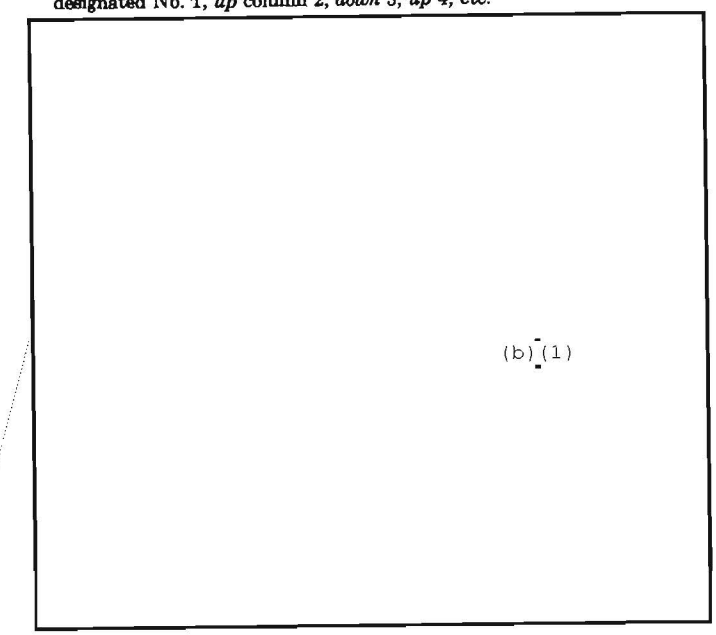
GRILLE TRANSPOSITION

Some hesitancy is felt in giving any detailed account of the Berlin-Rio grille transposition with which the SIS section was most familiar. The reason is that the Coast Guard Unit (with which we maintained excellent liaison) did the original solution of this, along with scores of similar transposition and transposition/substitution systems, and the technical aspects are very well covered in the document "History of Coast Guard Unit No. 387, 1940-1945."

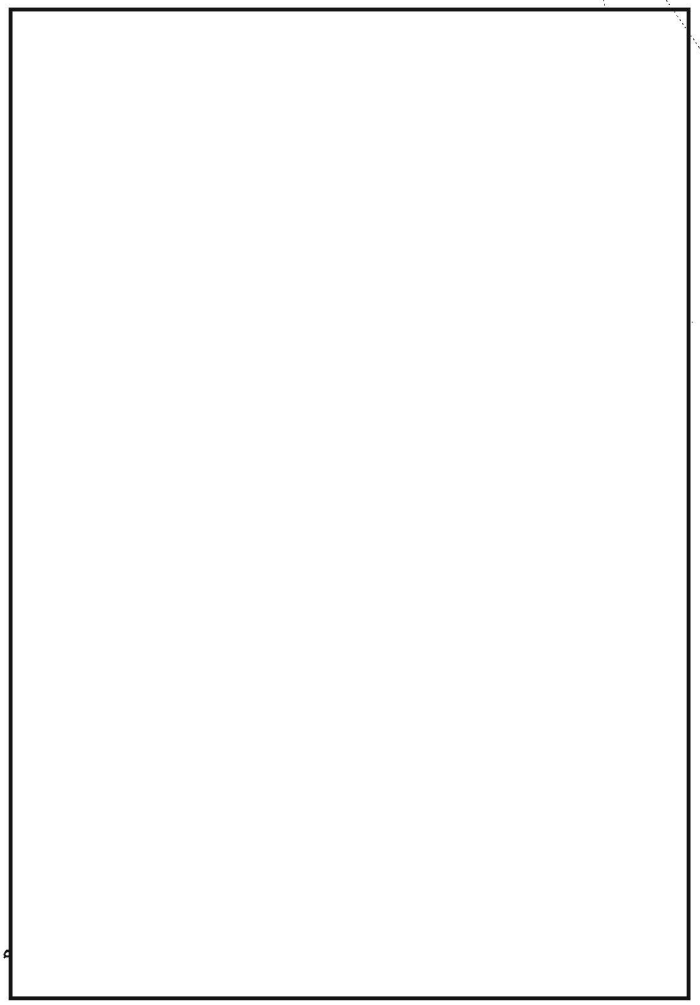
Our role was one of operational solution of current messages. Since we had a couple of people on the "graveyard shift", we were in the position of being able to have copy relayed to us within a short

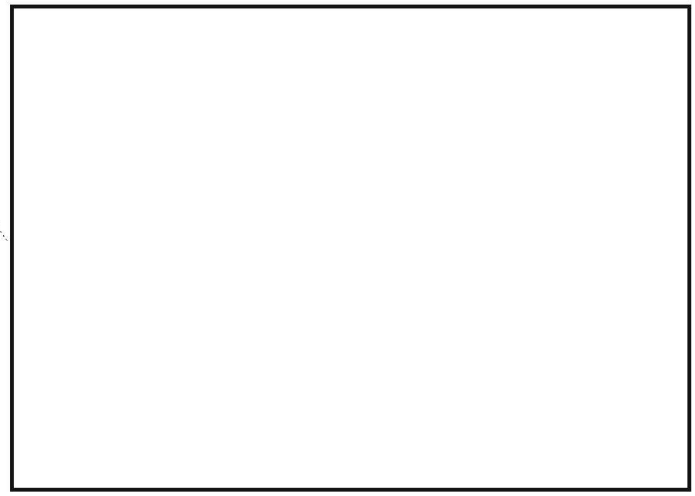
time after transmission, to solve the messages, and to get word of important actions to the proper law enforcement authorities *before* the agent for whom the message was intended could pick up his copy.

The system, which started in September 1941, involved the use of a 13 x 19 grille, with 125 active positions (including 15 nulls). Traffic was sent in blocks of 50 5-letter groups (except for the first block, which contained an indicator, to make the total 51 groups). The indicator (using a 1-0, A-J substitution) showed the page from which a transposition key was obtained, and in which of the 8 possible positions the grille was to be used, designating the corners A-D on one face and E-H on the other. Thus, an indicator group of AGIMF showed page 179 as the key source, with the last letter, F, designating that corner of the grille as the upper left setting. The transposed cipher version was effected by copying the letters *down* the column designated No. 1, *up* column 2, *down* 3, *up* 4, etc.



(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36





USAGE OF THE KRYHA CIPHER MACHINE

I had considered including a much-abbreviated story of the principles and solution of the Kryha (particularly as it applies to German agent usage). However, the absence of a generally usable treatise on this machine prompted my good friend Lambros D. Callimahos to suggest an alternative—extensive cribbing from a rather long and complete treatment written by me 20 years ago. (This is in keeping with advice from my mentor, Dr. Kullback, who feels the reprinting in its entirety of such technical reports as that covering GEE provides an interesting and informative means of tying together the old and the new approaches. In reading such articles as appeared in the *Journal* of July 1959 on the KEYWORD system, more recent arrivals on the cryptanalytic scene may be stimulated by the vicarious experience of such "You Are There" reporting.) Therefore, no further apology may be necessary to those who may recognize the following portion as a 1942 report.

Usage by the German agents involved two models of the Kryha. The earlier model had as the basic mechanism a selector wheel with 17 fixed gear-teeth to control the stops. The later model permitted a variable number of stops by means of the adjustment of any or all of 52 screws which acted as stop controls. As it is more practical to describe the old Kryha in terms of the new model than it would be to

explain the new machine on the basis of the old, this paper will deal with the later, improved model first.

Description

The new type Kryha may be visualized as a machine so devised as to convert a plaintext message into a very long polyalphabet by (viewed in terms of a Vigenère square) selecting one of the 26 possible positions of the cipher component to encipher the first plaintext letter, selecting an entirely different position for the second, etc.

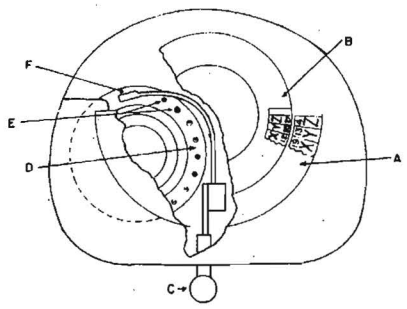
A revolving disc (on which the cipher component is placed) slides against a stationary plain component, the selection of alphabet being controlled by a geared wheel with 52 possible stopping points. The distance between successive stopping points is not necessarily the same, some intervals having three gear teeth, some four, and some five.

A further variable in regard to the shift of alphabets from letter to letter can be created by using only certain stops of the 52 possible. This is done by raising or lowering any combination of the 52 screws which act as stop controls, causing the machine to stop at each point where a screw is turned in, and to pass over those screws set flush with the surface of the wheel. Strictly speaking, the complete cycle of the polyalphabet thus formed may be considered as being composed of 26 subcycles, each subcycle comprising a complete revolution of the selector wheel. At the conclusion of each revolution (or subcycle), the cipher component will have moved exactly three letters to the left, which phenomenon forms the basis of recovery of the cipher component and will be explained in detail in further on.

The complete cycle is dependent on the number of stops employed, being the product of the number of stops selected and 26 (the number of alphabets possible at each stop). The cycle must, therefore, necessarily fall between 26 (when only one screw is depressed) and 1352 (when all 52 openings are used).

The following diagram will illustrate the general action of the various controlling mechanisms, and the terminology used thereon will be adhered to as much as possible in this paper.

The actual mechanics of the enciphering are fairly simple. Those screws (E) which have been selected to control the stopping points are turned down, and the plain and cipher components (A and B) set up. (The individual letters are on metal tabs which can be interchanged at will on the components.) The lever (C) is depressed until the arm (F) engages the predetermined opening to be used as the starting point, and the inner (ciphertext) wheel revolved by hand to set it at the predetermined setting ($X_r = X_p$ for example). The

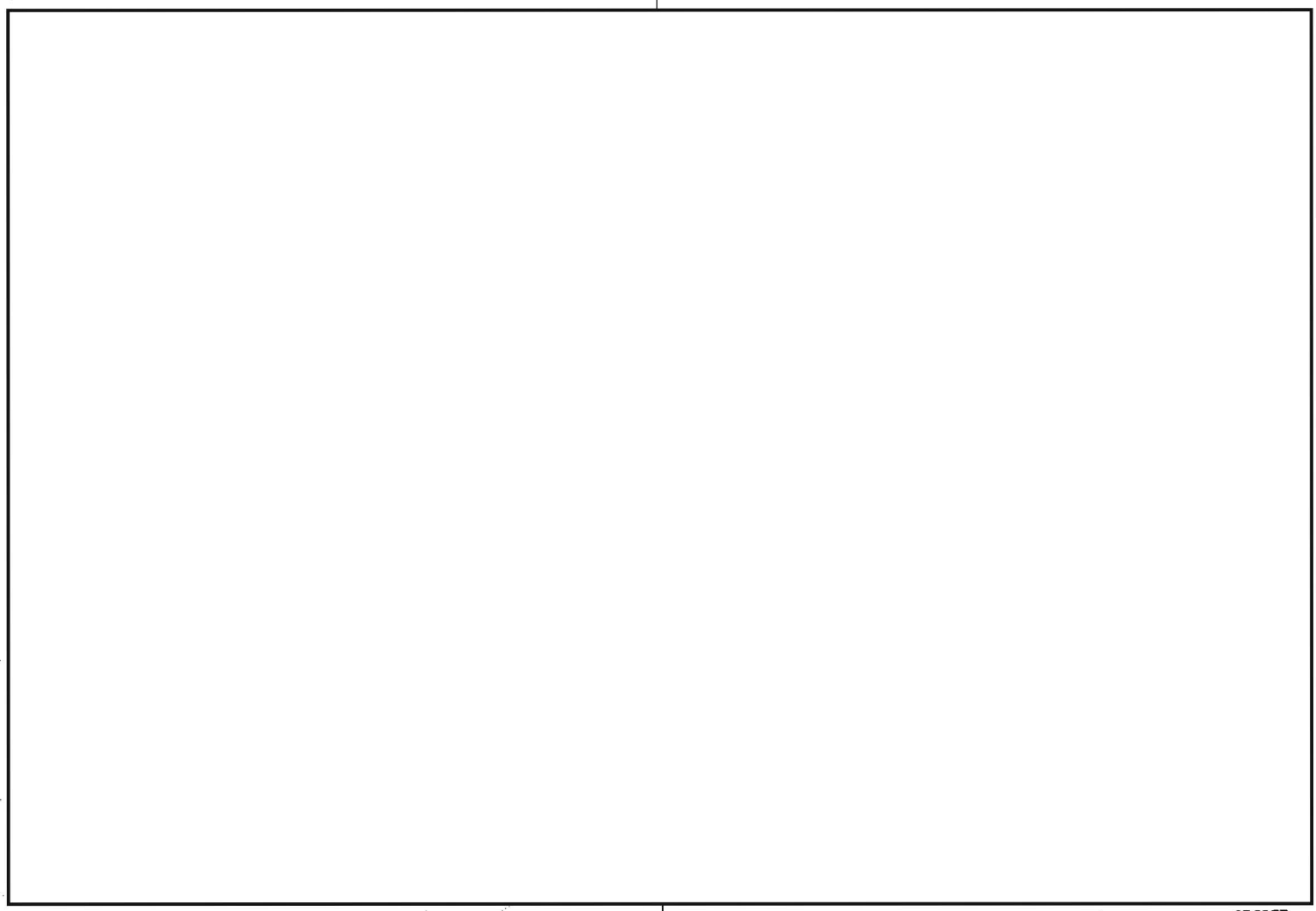


NEW TYPE "KRYHA" CIPHER MACHINE

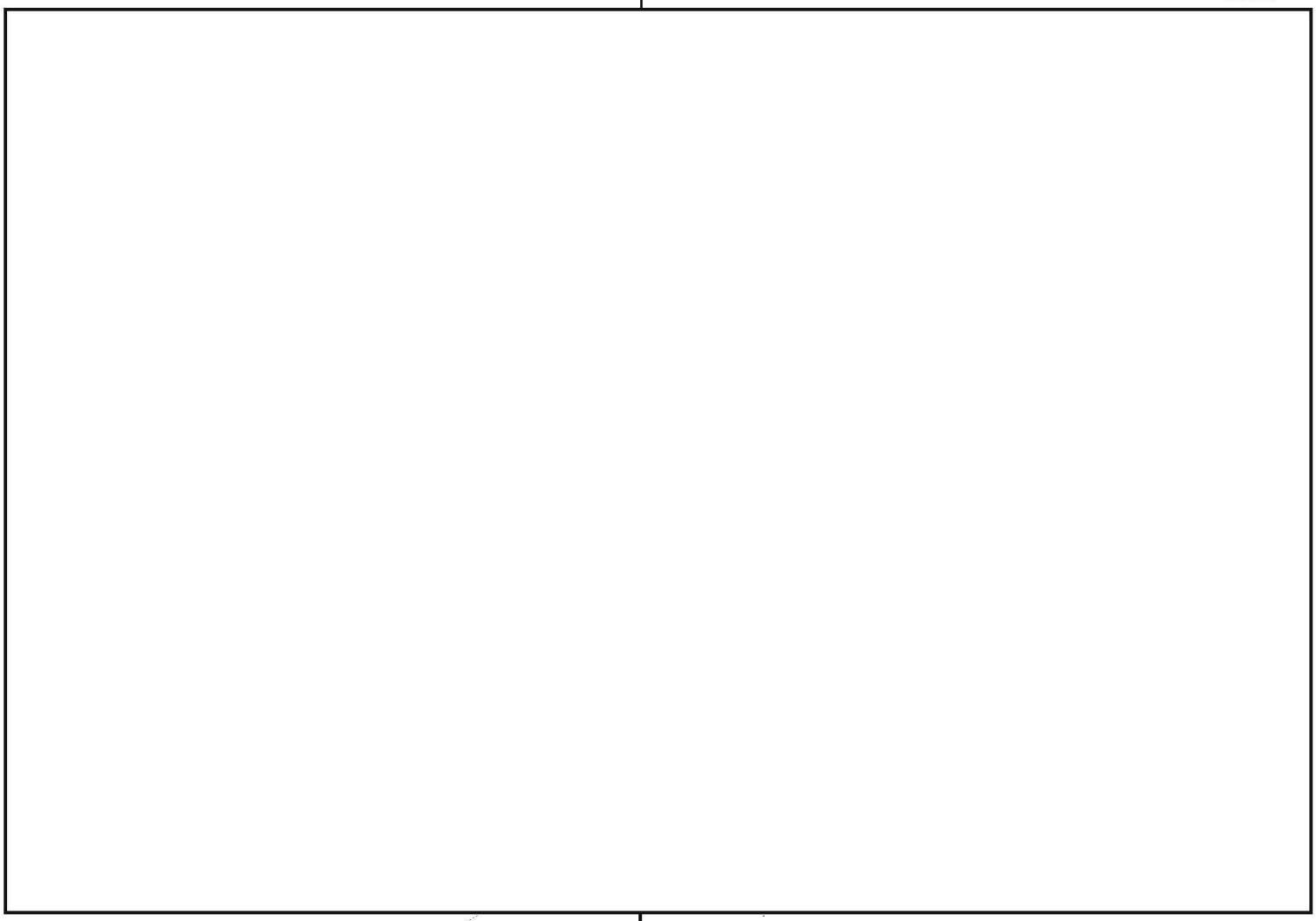
A – Plain-text Component
B – Cipher-text Component
C – Hand Lever which disengages F
D – Selector Wheel
E – Stops
F – Selector Arm which engages the stops

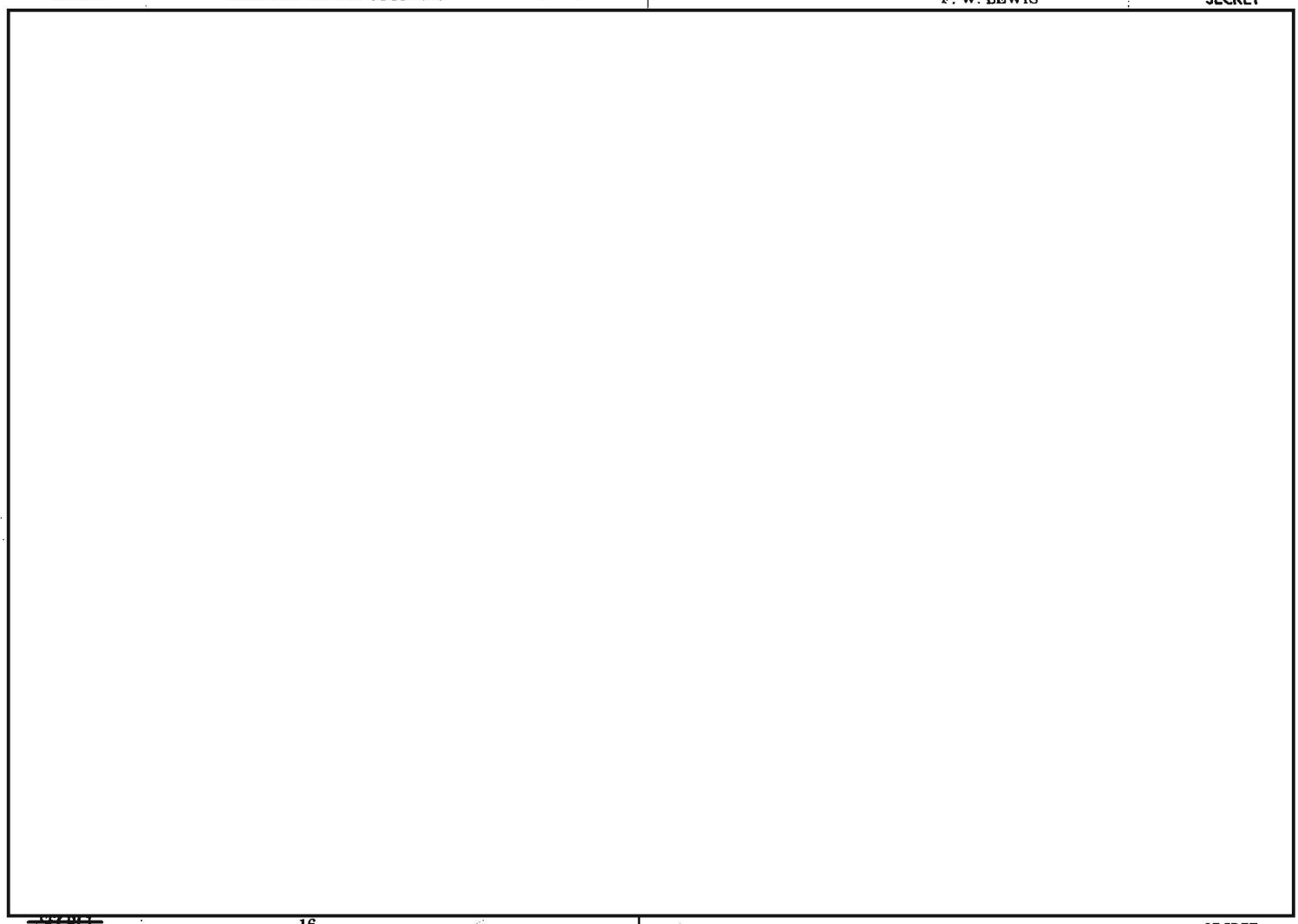
Fig. 1.

first plaintext letter is now located on the plain component, and written down in terms of the cipher equivalent. The controlling lever is then depressed, moving the ciphertext wheel to its new position ready for enciphering the second plaintext letter.

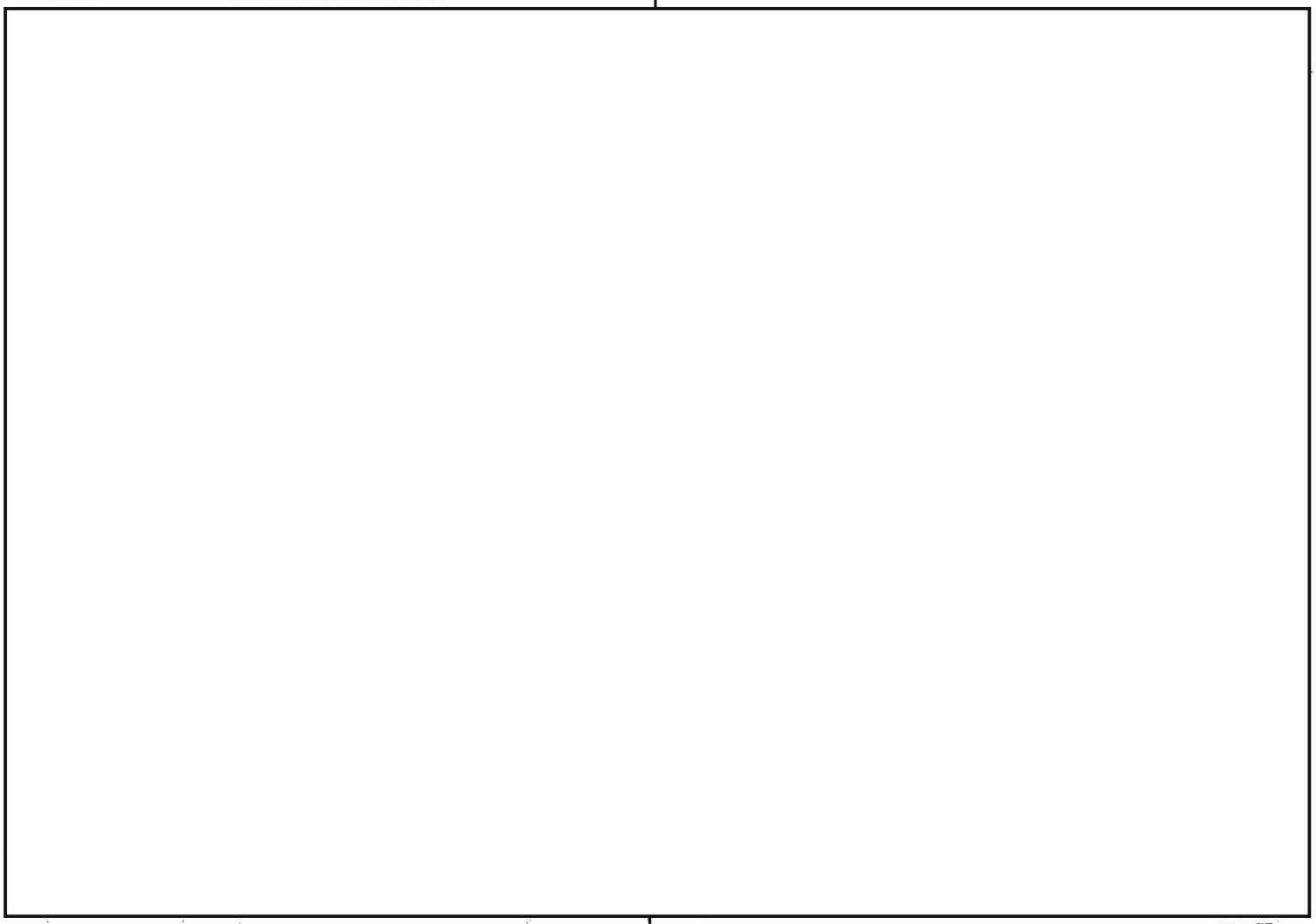


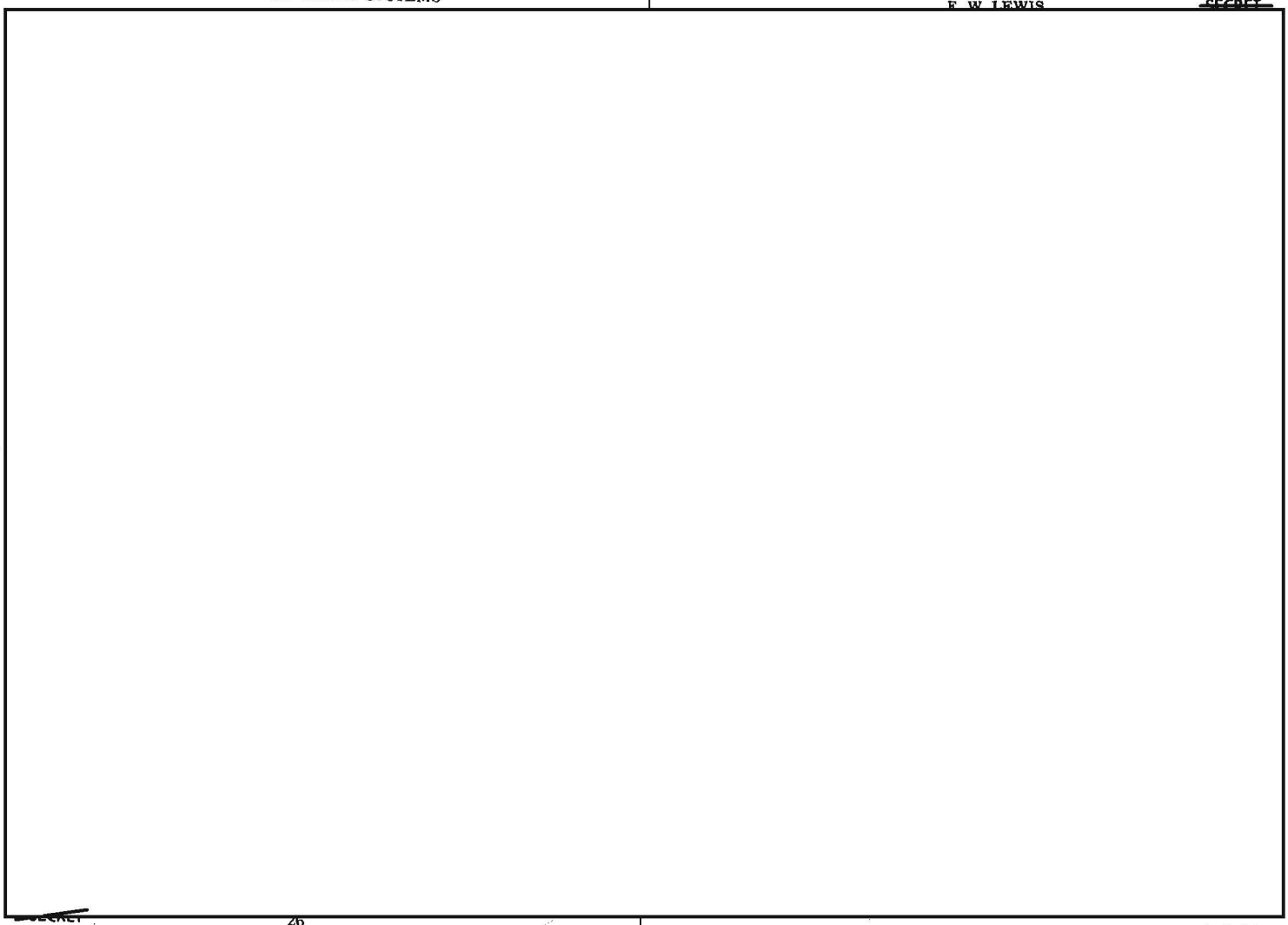
(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

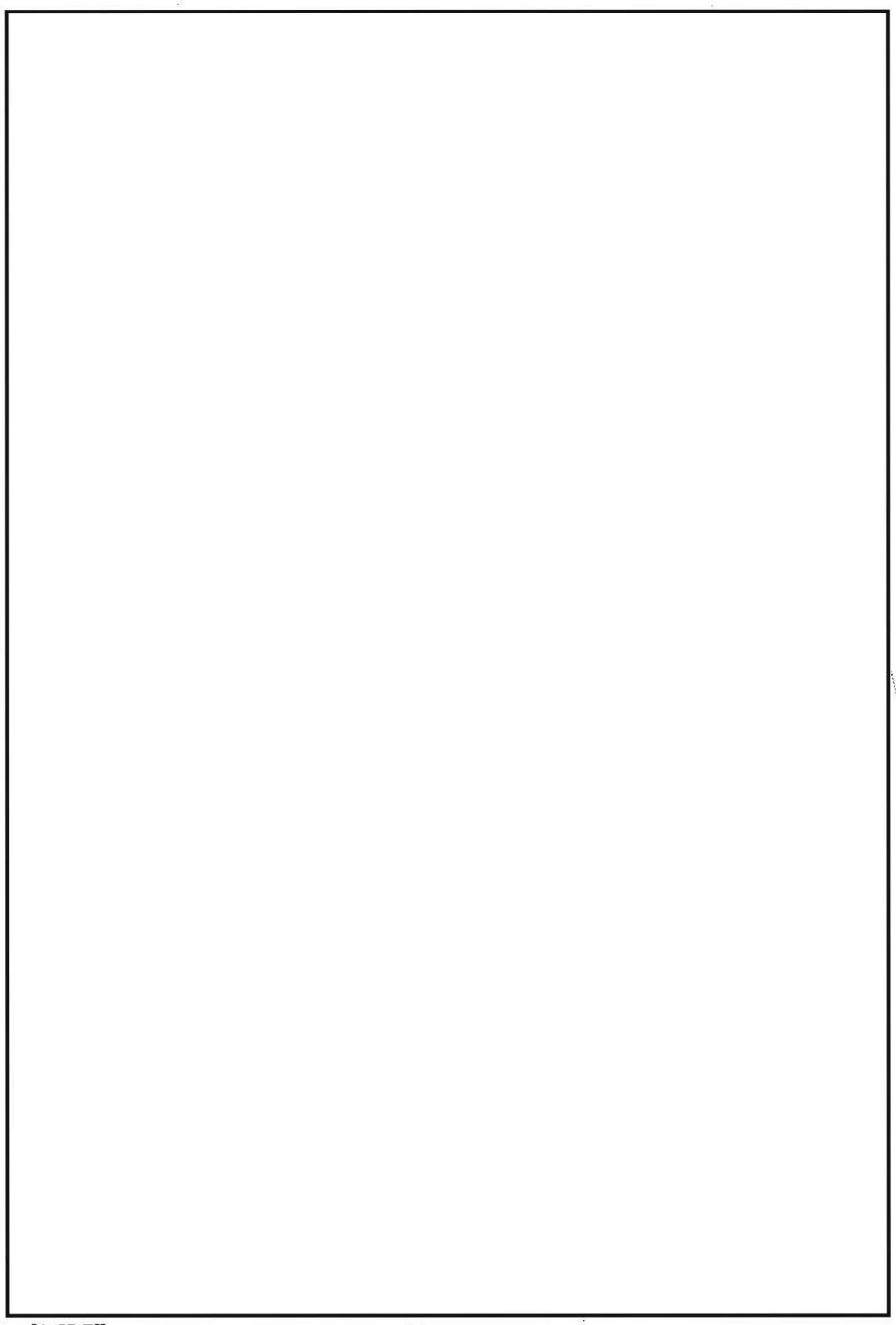




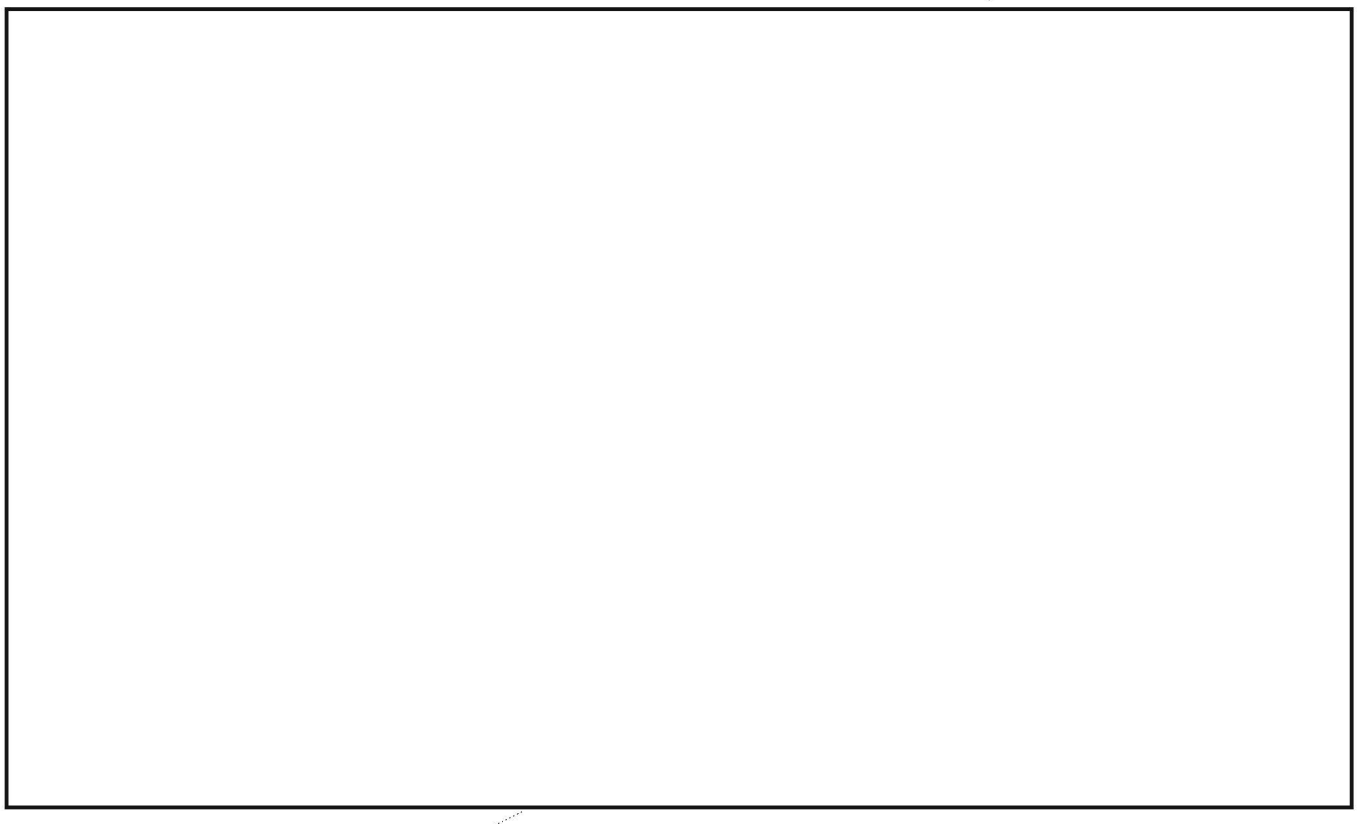
(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36



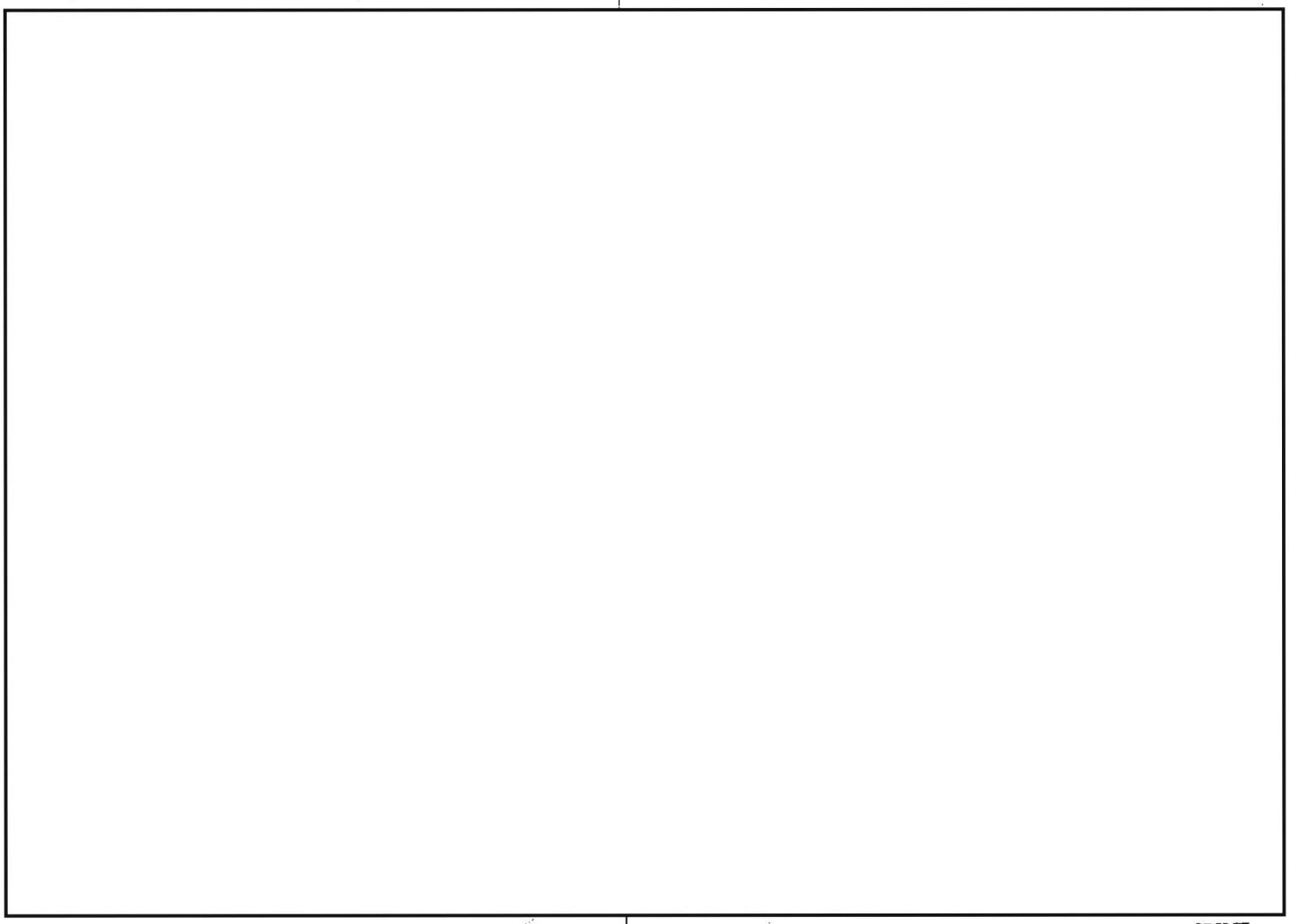


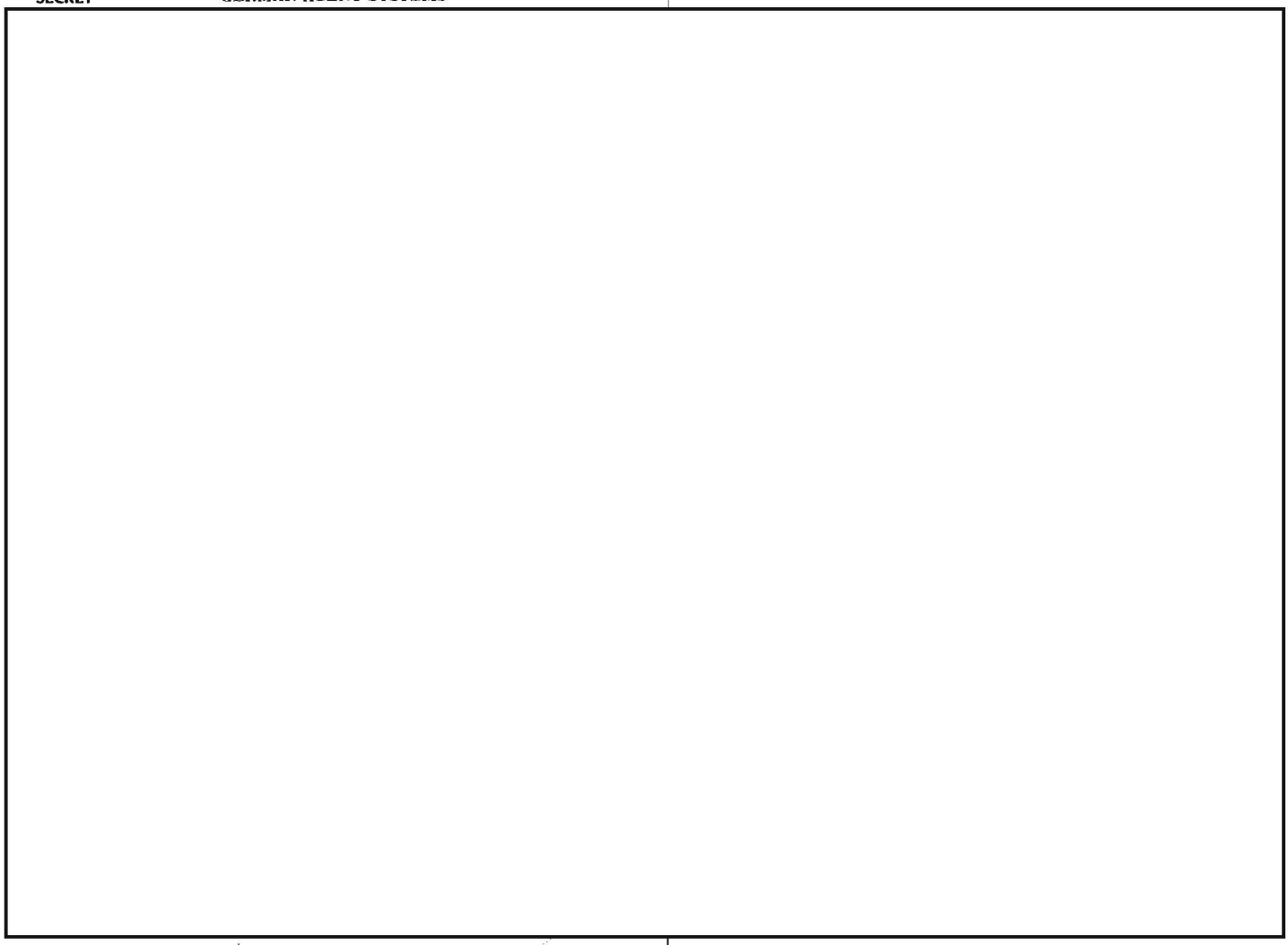


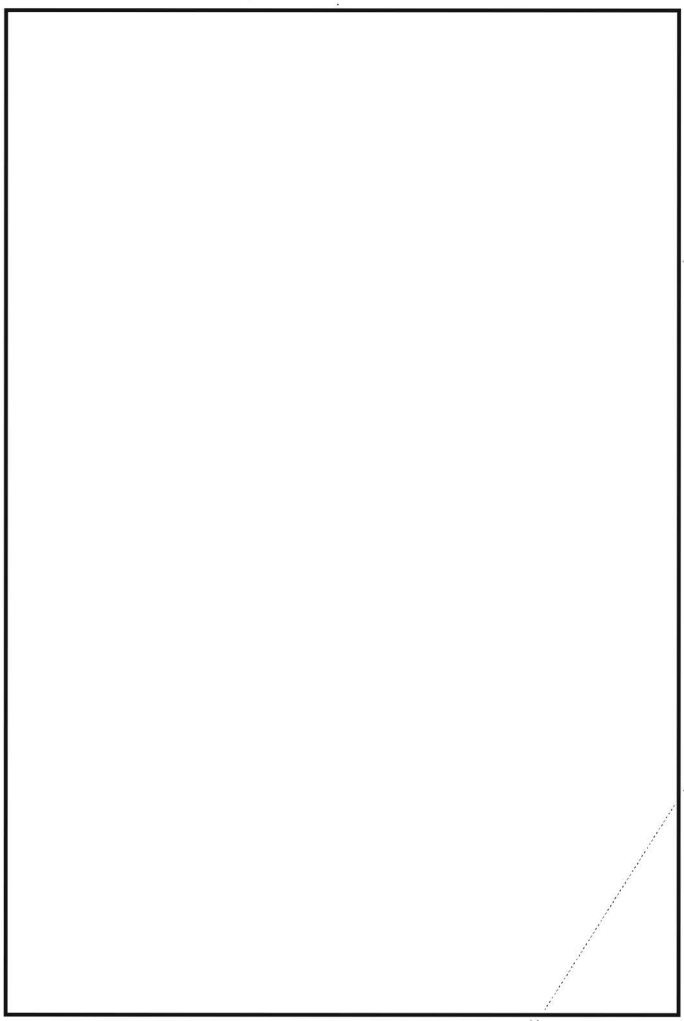
(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36



(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

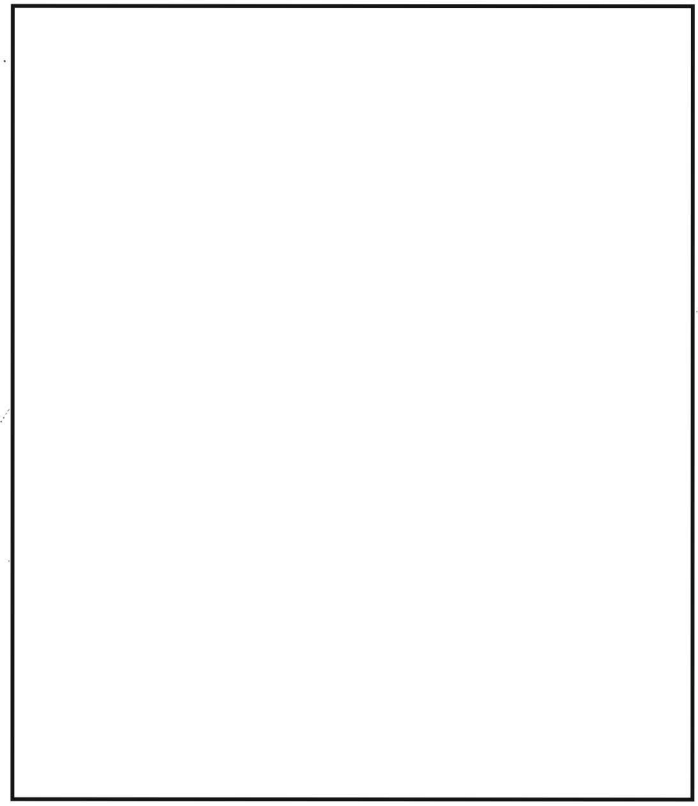


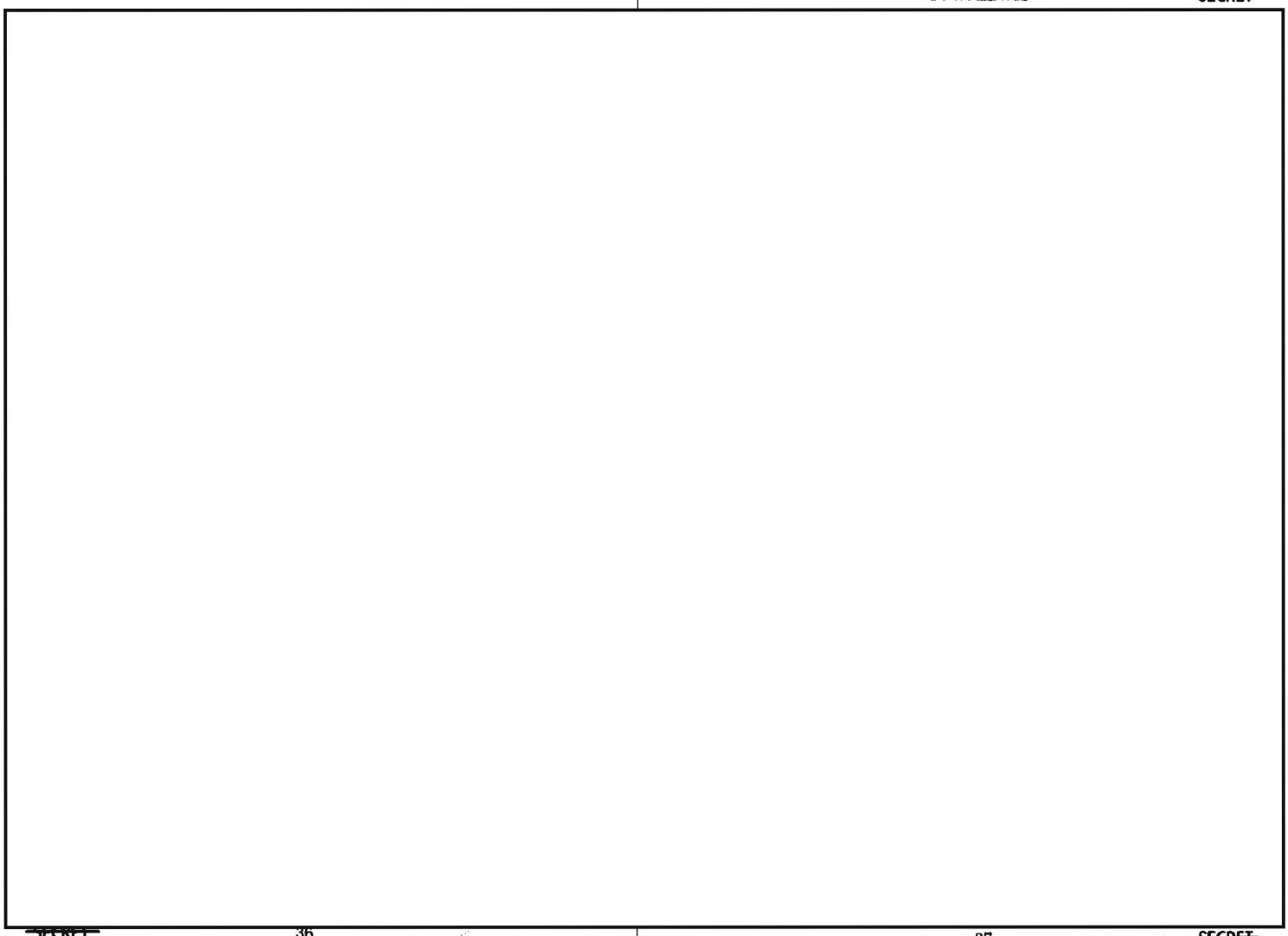


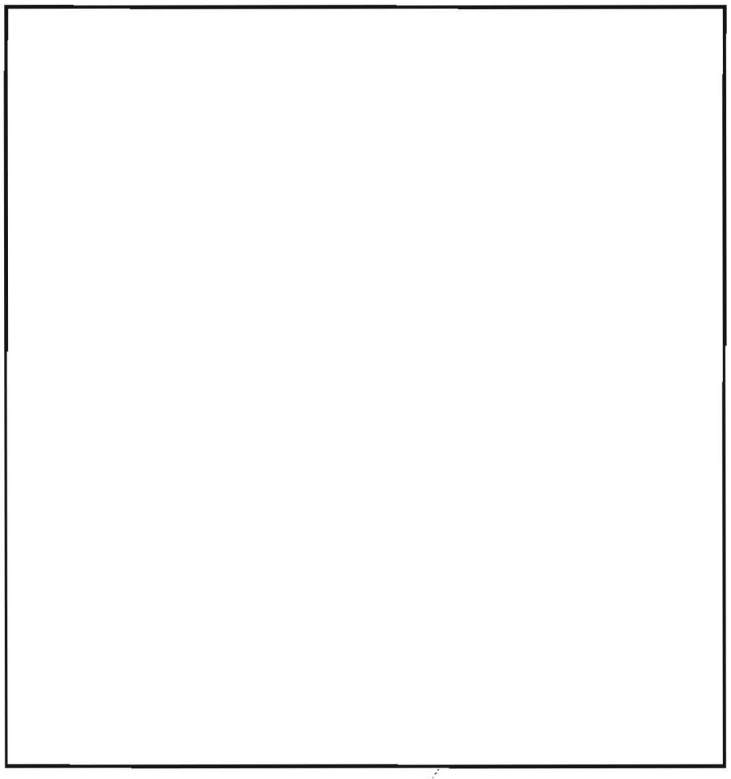


DICTIONARY CODE

The third type of agent system under present discussion involved the use of a German-Spanish dictionary as a code book, designating the page and the ordered position on the page, for each word, with encipherment of the resultant digits to a final literal cipher. This presents no formidable problem, given a reasonable amount of traffic, but the early diagnosis, preliminary code reconstruction, and eventual acquisition of the actual dictionary being used, all contribute to a somewhat Black-Chamber-like story.







(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36