A CRYPTOGRAPHIC SERIES

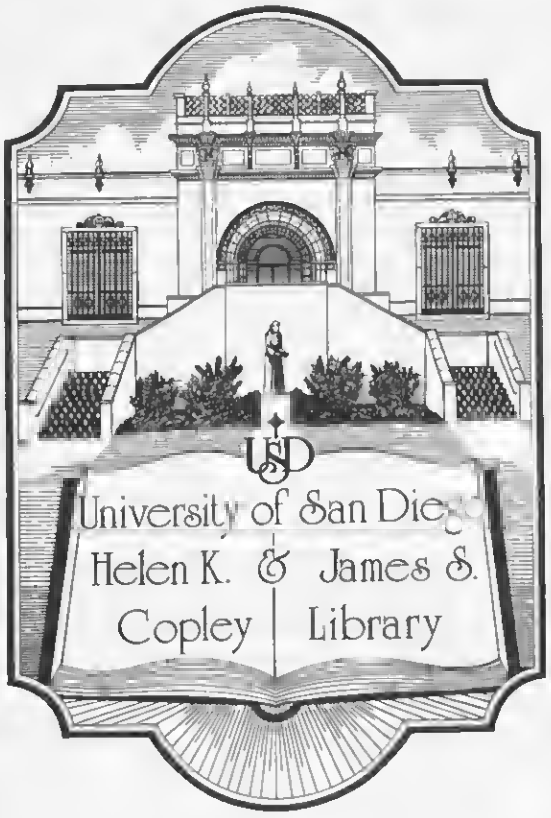
86

VATICAN CODE SYSTEMS

- ✓ General Characteristics of Vatican Systems
- ✓ The Red Code (KIA, KII)
- ✓ The Yellow Code (KIB)
- ✓ The Green Code (KIC)
- ✓ Vatican Commercial Traffic
- ✓ Traffic Identification and Logging
- ✓ Overall Survey of Vatican Codes
- ✓ An Appraisal of Vatican Cryptography

NATIONAL SECURITY AGENCY

From Aegean Park Press



VATICAN CODE SYSTEMS

This text concerns the cryptanalysis or "breaking" of various Vatican code systems used for the transmission of sensitive Vatican communications during World War II. The text, written in 1944, was originally classified. The text now over 50 years later is unclassified; and has been released to the reading public by the National Security Agency (NSA). For easy reading the original text has been typeset by the publisher. Except for the deletion of a few names for the purpose of protecting personal privacy, no changes have been made to the text itself. The original text may be found in the National Archives in Box 1284 where it exists as document *NR 3823 ZEMA100 37012A 19430000 Cryptographic Codes and Ciphers: Vatican Code Systems.*

ISBN: 0-89412-280-0

AEGEAN PARK PRESS
P.O. Box 2837
Laguna Hills, CA 92654
(949) 586-8811
FAX (949) 586-8269

Manufactured in the United States of America

Note

It was a joint effort to "break" the Vatican code systems. The SSA and GC&CS together pooled their resources to accomplish this task. The SSA is an abbreviation for Signal Security Agency, an organization later termed the Army Security Agency, one of the foundation organizations which contributed to the formation of the present National Security Agency. The GC&CS is likewise the abbreviation for Government Code and Cypher School. This was the British code and ciphers organization at Bletchley Park in London during World War II. Today the GC&CS is better known as GCHQ, an abbreviation for Government Communications Headquarters located in Cheltenham, England. Unlike the NSA, which is under the military's Defense Department, GCHQ is today part of the British Foreign Office.

Figures

Foreword

The general plan follows the plan used for Italian Codes and Ciphers 1939-1943, much of which applies equally well to Vatican systems, at least so far as the common language creates similar problems in book recovery and editing of messages. In discussing the various systems the order is from solved to unsolved systems, from systems using trigraphs to those using tetragraphs, and from those using one null to those using two. It is intended to bring the discussion up to date whenever sufficient progress has been made in any period.

18 September 1944

Contents

INTRODUCTION

History of the Solution of Vatican Systems in SSA and GC&CS 1943-1944

1. **Preliminary Exploration.** Work on the solution of the Vatican systems began early in September 1943, with exploratory examination conducted by members of the research group. They had, to begin with, a body of several thousand messages, both code and plain, sorted only by intercept date, mostly originating in the period after 7 December 1941 but with a few earlier messages. GC&CS, moreover, had sent a report of progress on solution of Vatican systems, the result of British analysis begun about June 1942.[1] They had already identified two systems[2] and made considerable progress on the recovery of the book underlying one of them. A photograph of this reconstruction was received, with 2,824 values recovered. Likewise, the two tables for encipherment of the page numbers of KIA had been recovered to about 80 percent each and the two similar tables of KII to about 60 and 29 percent respectively. The digraphic-substitution table for the encipherment of message numbers was also solved but was not sent to SSA.

The American analysts tested the British information, sorted out all KIA traffic, and solved the relative order of the digraphs in the digraphic-substitution table for encipherment of message numbers. They also identified in the traffic a group of messages in tetragraphic system using A and E as nulls, and designated this tentatively as the "AE" system (KIC).

2. **The Gold Section Personnel.** At this point (27 September 1943) a new unit, known as the "Gold Section", was activated, the personnel being drawn from the Italian Diplomatic Section at that time being disbanded, owing to the decline in Italian diplomatic traffic after the fall of Mussolini on 25 July 1943.

---

[1] The British had no information concerning Vatican systems of an earlier date, and no Vatican cryptographic material has ever been captured.

[2] Really three, according to American designations: the "E" system (KIA-KII) and the "YZ" system (KIB).

3. **Progress on KIA.** With a limited staff and the necessity of organizing the routine of the office, work was first begun on indexing of traffic. Since, for reasons of security, traffic was received in the unit in unindexed form, a system of logging had to be set up. This task was hampered by the fact that the digraphic table for the encipherment of message numbers had been solved only relatively so that all messages had of necessity to be logged with tentative message numbers certainly incorrect. As soon as the table was corrected, however, the log sheets were adjusted to the true message-number sequence, and no further trouble was experienced. KIA messages were readable by decoding from photographs of the British reconstruction but these were unhandy, often difficult to read, and the pages were arranged in numerical sequence; i.e., decoding had to begin by looking up the numerical equivalent of the digraphic substitute used in the message and then consulting the photographs for the value. Accordingly, it was necessary to make better decodes than these, and one was made by hand for each key. It was thus possible to make considerable progress in decoding older messages, and these were processed in the reverse of chronological order until by April 1944 all old KIA messages had been decoded.

Routine procedure was now: identification of system, logging, decoding, editing with book recovery, translation, and filing. At first all traffic was translated in full, but gradually certain classes of messages were eliminated until at the present time only such messages as have definite intelligence value are processed beyond decoding.

Very shortly it became clear that the digraphic substitution table for encipherment of message numbers was 11 points off the true position, and this was corrected. One further digraph was later corrected on the basis of British comments, but the table (presented in *Figure 1*) is sound and has stood the test of more the 8,000 messages in the various systems using it.

Active book recovery of KIA continued until May 1944 when the unit was united with the Italian Diplomatic Section. At the present writing (8 September 1944) a total of 5,875 identifications have been entered, 2,824 received from the British, 3,051 recovered in the SSA. Since May 1944, progress in book recovery has been incidental to editing, no other attempt to recover values being carried on at the present time.

4. **Progress on KIB.** As soon as initial pressure lessened, serious work was begun on KIB, but this was hampered by lack of personnel and even more by lack of sufficient traffic. One of the most fruitful sources of help in the early stages of analysis was the discovery of cribs. Search for cribs, however, was greatly hampered by the fact that the natural place to look for cribs was between traffic in KIB in the Washington circuit and traffic in KII in the London circuit,

but the SSA did not[3] regularly receive the second body of traffic, and GC&CS did not regularly receive complete coverage of the first. Only by accident did the British intercept a KIB message to Washington with the same plain-text as a KII message to London on the same date. No such crib was ever found in the SSA with only seven intercepts in KII available. From this crib, however, the British were able to establish the fact that KIB was a book of the same type as KIA but not identical with it, enciphered according to a much more complicated system of digraphic and monoliteral substitution tables. They believed that KIB was somewhat larger and had its personal and geographical names scattered through the general vocabulary rather than segregated in an appendix. As the available traffic continued to be studied, these facts were borne out, but before December 1943, the only significant discovery, made about the same time on both sides of the Atlantic, was that the date appeared to have some relation to the encipherment and that different circuits appeared to use different keys. The British had by that time successfully isolated one family of messages which they called "WAMADU" (Washington, Madrid, Dublin traffic, and also used elsewhere, as was later discovered).

It now became desirable to index the traffic by IBM methods, and most of December was given over to the long task of preparing the traffic so as to remove, for reasons of security, any evidence of its origin. Once indexes and message prints were available in January, analysis began in the SSA, and copies were immediately sent to GC&CS. By examining beginnings and endings of messages and by using statistical methods, more "WAMADU" messages were found, and three other families were isolated, the "OJ", "DR", and "FS" families, so-called from frequent digraphs used, but many messages resisted classification. At the beginning of May active work on KIB was suspended.

5. <u>Progress in Other Systems.</u> While the KIB material was being processed by IBM, all available KIZ plain-text messages were read for their value as examples of Vatican habits of diction and then destroyed. All code messages were examined and logged with the result that external features of KID, KIE, KIF, KIG, and KIH were identified. With the exception of a very small number of special cases, every available message was logged. In the systems mentioned there was too little traffic for any intensive study except in KIF. Here, the system of sixteen keys was recognized, and the traffic was indexed by IBM with the hope that it would be possible to show that the system is an encipherment of the KIA book, but these hopes proved in vain as the index appeared far too flat.

[3] The same situation still obtains. Matters are now somewhat better since the text of 60 messages in KII has been received from GC&CS.

6. **Current Policy.** At present all Vatican traffic is logged, KIA messages are decoded completely and translated or summarized whenever of sufficient intelligence value. All other messages are filed for future study.

I

GENERAL CHARACTERISTICS OF VATICAN SYSTEMS

7. Language. Latin might have been expected as the basic language of Vatican codes, but thus far in the experience of the SSA no Vatican code has been found which is not in Italian. Vatican plain-text (KIZ) appears in Italian, French, Spanish, Portuguese, German, and English, and occasionally in Latin also, but Latin messages are not now permitted by the censorship regulations, and those messages intercepted in Latin have generally been sent by parish priests rather than by diplomatic representatives. Certain of the unsolved systems may later prove to be Latin, but this is unlikely since Latin vocabulary is not well suited for the expression of the facts of everyday life, and the ability to write good Latin, even in the Church, is rarer than one might think. With the single exception of Paschal Robinson, the Nuncio to Eire, every diplomatic representative of the Holy See speaks Italian as a native. Therefore, it is not surprising that Italian is the language of Vatican codes.[4] Experience gained in the solution of Italian diplomatic codes has proved invaluable to analysts working on the Vatican systems, since, in spite of striking differences from the cryptographic point of view, the linguistic problems in both kinds of traffic are fundamentally the same.

[4] It would be interesting to know whether at a date earlier than the experience of the SSA any other language was used. It is known that H26, an Italian diplomatic code of a date earlier than any other so far captured, is in French, the older language of diplomacy.

8. **Types of Systems.** The Vatican systems, so far as is known from the present stage of solution, exhibit certain well-defined tendencies:

a. **Letters.** With one exception (KID) the messages are transmitted in letters.

b. **Code-group.** The code group may be either trigraphic (KIA, KIB, KIF, KIG, KII) or tetragraphic (KIC, KIE, KIH), no information being available concerning KID. This means the trigraphic systems will all be relatively small books, since permutations of the twenty-six letters limit the number of possible code groups to a cube of twenty-six, or 17,576 trigraphs. If, however, as is actually the case, one or two of the letters is used only as a null, then the limitation is correspondingly greater. Trigraphic systems with one null (KIA, KIF, KII) can have no more groups than the cube of twenty-five or 15,625, but KIA is still further limited, since no vowel is used in the page digraphs, i.e. 21 x 21 x 25 = 11,025, which must be close to the actual size of the book. Trigraphic systems with two nulls (KIB, KIG) are limited to 13,824 groups or even less, depending on the possible further limitation of the page digraphs. Therefore, it is certain that KIA, KIB, KIF, KIG, and KII must be approximately the same size, eleven to fifteen thousand. Tetragraphic systems (KIC, KIE, KIH) may, however, be much larger, since they permit a total of 676 x 676 = 456,976 permutations when all letters are used in the code group or, when one is used as a null (KIE) 625 x 625 = 390,625, and when two are used as nulls (KIC, KIH) 576 x 576 = 331,776.[5] That any code is so large is highly improbable[6], and the chances are very good that the tetragraphic codes are eclectic and not much larger than the trigraphic.

c. **One-part.** One part codes seem to be the rule with no two-letter differential, at least so far as is known.

d. **Encipherment.** Encipherment appears to be based on tables of letter-for-number substitution, digraphs being used for the pages in trigraphic codes (KIA, KIB, KIF, and KII), and as remains to be discovered, either digraphs or trigraphs in the tetragraphic codes. The selection of tables seems to be based on the date, either odd and even days of the month, or some other time pattern agreed upon by correspondents in advance since no key indicators appear to be used. Circuits also may affect the choice of keys in some way not always understood. In some instances (KIB and KII) the position symbol may precede that of the page in the transmission, but more usually the page symbol is first. Keys may also change within the message at will.

---

[5] It makes no difference whether the four digits are counted as two pairs or as three digits and a fourth.

[6] Codes with 100,000 groups (e.g. the Argentine ARB, a captured code) are considered the maximum feasible.

e. **Code-group limitation.** Certain letters are omitted from the composition of the trigraph, either one or two in each system, and these are inserted in the message as nulls, normally between groups rather than within them, and frequently, if not always, they serve as punctuation.[7] The nulls may be the same for all keys in a system (KIA, KIB, KIC, KIE, KIH, KII) or they may vary with the circuit key (KIG), and in one system (KIF) they may vary even within messages since each key is based on a different null. Normally there may be one or two nulls, never more.

f. **Vocabulary.** Code books apparently contain not only the conventional vocabulary inherent in all codes but also many separate appendixes which may be placed either before or after the vocabulary and may contain a wide variety of specialized groups:

(1) Christian and place names
(2) Punctuation
(3) Numbers
(4) Phrases frequent in telegrams
(5) Titles of officials and organizations
(6) Lists of dioceses, etc.
(7) Time adverbs
(8) Inflectional forms of frequent auxiliary verbs
(9) Diseases and health
(10) Miscellaneous

Some of these pages may differ in different copies of the same book, either as the result of official addenda or because even in the printed copy special lists of groups frequent in the traffic have been provided only in the copies assigned to that circuit while the same group in other circuits has different values. Vatican codes do not have surnames as do Italian diplomatic codes.

g. **Encipherment of names.** Cipher systems are unknown among Vatican systems, but cipher is mixed with code in KIA, KIB, KII, and probably in the others as well, to spell long and unfamiliar names. This method is offered as an alternative to spelling out the name with code groups. A doublet of nulls before and after the cipher, e.g. EE . . . . . EE[8], indicates the use of such a spelling cipher; between these doublets, monoalphabetic substitution is applied to the plain text, as in KIA and KII, or polyalphabetic substitution, with random-mixed alphabets, as in KIB. When the name to be spelled is long, considerable economy is the result, because it is necessary to transmit only four more letters than the number in the plain text, but short names may be spelled more economically with code groups, since the two doublets may be then omitted. That at times the code

[7] In KIA the null seems to occur almost always at a break in thought.
[8] When there are two nulls the possibilities for variety are manifold: See p. 31 below.

clerk will use the wrong table, seems to indicate that tables for this encipherment are separate from the page encipherment tables.

9. **General Practices.** Certain features of Vatican communications are of interest:

a. **System indicators.** The first letter of every message is a system indicator[9] and, with one exception, each system has a set of variants which may be used alternately without other significance:

KIA: W, X, Y, Z or B, C, D, E
KIB: B, C, D, E,
KIC: I, J, K, L, M, (N?)
KID: no information available
KIE: no information available
KIF: Q, R, S, T, U, V
KIG: J, K, L, M, (N?)
KIH: A (no variants)
KII: I, J, K, L, M

The possible confusion between KIA and KIB is eliminated by differences in the method of indicating the message number. KIC, KIG, and KII appear to use the same set of system indicators. The first two systems were not used simultaneously, and both are now obsolete. N is a doubtful letter, O appears not to fit the table as given, and P is never found in any traffic.

b. **Message numbers.** These are always enciphered and may appear as trigraphs or digraphs, immediately following the system indicators. If trigraphs, then they may be decoded by using the number pages of the code book (KIA and KII). This method was in use very widely in 1942; in 1943 it was abandoned except for Tokyo and one South American station, and in 1944 it was used for Tokyo alone. In its place a table of digraphic substitutions for the digits 01 to 100 is used in all other traffic (excepting KID, KIE, and some messages in KIG). There is no confusion between KIA and KIB since messages beginning with B, C, D, or E, will be KIA if they have a trigraphic message number, and KIB if they have a digraphic message number. The same digraphic table is used with KIA, KIB, KIC, KIF, KIH, and KII, but never with KID or KIE, and only at times with KIG. Other KIG messages may have a similar but different table. Circular messages bear no message number but have the word "*circolare*" (in code) instead of the message number. Messages between outlying stations are unnumbered. *Figure 1* shows this table in deciphering and enciphering forms. When the digraph for 100 has been used, the sequence repeats but without indication of hundreds. Occasional cross references to messages of which the number is higher

[9] When messages begin with AA, apparently the sign for "urgent", the indicator then follows.

DIGRAPHIC SUBSTITUTION TABLE FOR MESSAGE NUMBERS

DECIPHERING

	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	57	19	84	38	33	42	39	85	80	86	55	16	93	92	78	74	98	06	34	20	14	63	94	03	08
C	25	17	67	09	100	05	69	27	54	75	40	60	28	01	48	51	96	37	52	81	73	22	31	64	35
D	44	12	46	24	56	77	97	10	59	02	13	62	99	32	76	04	72	43	87	71	07	88	58	49	11
E	68	61	65	29	70	95	18	90	21	89	41	30	15	83	66	82	53	23	26	50	45	91	47	36	79

ENCIPHERING

	0	1	2	3	4	5	6	7	8	9
0	CF	CO	DK	BY	DQ	CG	BS	DV	BZ	CE
1	DI	DZ	DC	DL	BV	EN	BM	CC	EH	BC
2	BU	EJ	CW	ES	DE	CB	ET	CI	CN	EE
3	EM	CX	DO	BF	BT	CZ	EY	CS	BE	BH
4	CL	EL	BG	DS	DB	EV	DD	EX	CP	DY
5	EU	CQ	CT	ER	CJ	BL	DF	BB	DX	DJ
6	CM	EC	DM	BW	CY	ED	EP	CD	EB	CH
7	EF	DU	DR	CV	BQ	CK	DP	DG	BP	EZ
8	BJ	CU	EQ	EO	BD	BI	BK	DT	DW	EK
9	EI	EW	BO	BN	BX	EG	CR	DH	BR	DN

FIGURE 1

than 100 show that a record of sequences must be kept in the code bureaus. A new series does not begin at the beginning of a year or at any other period.

c. **Signatures.** These are always sent in clear.

d. **Messages in parts.** Vatican messages are never sent in parts, no matter how long,[10] but several short messages are regularly combined for transmission into a single unit. Each will have its own message number in sequence, the first being indicated by enciphered digraphs, the others by code groups.[11] It was this feature of Vatican traffic that established the true values of the digraphic table.

e. **Date of codes.** KIG was in use roughly from September 1940 to December 1942, after which it was replaced by KIC which was in force until September 1943 when KIH was introduced. September, then, may be the first month of the cryptographic year. The date when KIA was introduced is unknown, but it may have been before 1936 since the code does not have the word for "Axis," afterwards introduced into KIB. Thus KIB was compiled with some probability after 1936. From intercepted messages it is clear that KID is at least eight years old, but there is no evidence as to the dates of the other systems.

f. **Distribution of codes.** KIA is the basic book assigned to all stations. It is missing in traffic from Bangalore and Indo-China, but this situation is probably due merely to difficulties of distribution. These stations use KID which also appears in Tokyo and Vichy traffic but then only in relays to and from Indo-China. KIB is a much more secure code than KIA, and is used by all more important stations and by many of lesser importance, but not by London or Tokyo. It may, in some cases, be supplemented by KIC, KIF, or KIG, or by KIH or KII, held each by a single station, London and Washington, respectively. *Figure 2* shows the distribution of Vatican codes by stations,[12] *Figure 3* that by books and *Figure 4* shows the stations classified according to the number of books each holds.

10. **Code Designations.** The Vatican codes are known to their users by titles taken from colors, perhaps from the color of the covers:

KIA: Cifrario rosso (red)

---

[10] Trigraphic messages are, of course, only a little more than three-fifths as long as pentagraphic messages. Thus, 150 pentagraphic groups could be expressed in 100 trigraphs, assuming the same code and the absence of nulls. Vatican traffic is therefore on the average shorter than Italian diplomatic traffic.

[11] Occasionally the code clerk will use a digraphic number within a message. In this case the message will at once go out of phase. Such a number may be easily identified.

[12] Only stations regularly transmitting traffic are listed. When a nuncio or delegate goes to another place, he may temporarily transmit from that place. A few stations have transmitted only a single message, e.g. Aleppo and Mexico City.

KIB: Cifrario giallo (yellow)
KIC: Cifrario verde (green)
Others: unknown

11. Coverage. Coverage of Vatican traffic is now much higher than was ever possible in the case of Italian diplomatic traffic in the days when the Italians had many representatives and were sending and receiving large volumes in every system. All cable traffic to and from stations in the Western Hemisphere is intercepted 100 percent, but even Tokyo traffic, which must be intercepted exclusively by electrical means, is covered 96 percent, and many of the more important European stations nearly as well.

12. Intelligence. Vatican diplomatic traffic consists of the following types:

Routine Church business,
prisoner-of-war business,
commercial,
diplomatic, and
personal.

VATICAN SYSTEMS-DISTRIBUTION BY STATIONS

Asuncion	KIA, KIB, KIC
Bangalore	KID
Berlin	KIA, KIB, KIF
Berne	KIA, KIB, KIF
Beyoglu	KIA, KIB ?
Beyrouth	KIA
Bogotá	KIA, KIB, KIC, KIG
Bratislava	KIA, KIB
Bucharest	KIA, KIB
Budapest	KIA, KIB
Buenos Aires	KIA, KIB, KIG
Caracas	KIA, KIB
Dublin	KIA, KIB
Guatemala	KID
Hanoi-Hue*	KIA, KIB
Havana	KIA
Honduras	KIA, KIB, KID, KIG
La Paz	KIA
Leopoldville	KIA, KIB, KIG
Lima	KIA, KIB, KIF
Lisbon	KIA, KIB, KIC, KII**
London	KIA, KIB, KIF
Madrid	KIA, KIB
Montevideo	KIA, KIF, KIG
Ottowa	KIE
Peking	KIA, KIB, KIC, KIG
Port-au-Prince-Ciudad Trujillo*	KIA, KIB, KIG
Quito	KIA, KIB, KIC
Rio de Janeiro	KIA, KIG
San José – Panama-Managua*	KIA, KIB
San Salvador	KIA, KIB, KIG
Santiago	KIA, KIB ?
Sofia	KIA, KIC ?
Sydney	KIA, KID ?***
Tokyo	KIA, KIB, KIC, KID***, KIF
Vichy	KIA, KIB, KIC, KIF, KIG, KIH
Washington	

FIGURE 2

* Traffic from either station is signed by the same man and belongs to the same series.

** Full Information concerning the London books is not available.

*** KID messages have been sent and received by these stations, but there is no evidence that the stations themselves can read the messages since in every case the message is a relay to or from the Far East where KID is held.

VATICAN SYSTEMS-DISTRIBUTION BY SYSTEMS

KIA: All diplomatic posts except Bangalore, Hanoi-Hue, Peking

KIB: Asuncion, Berlin, Berne, Beyoglu (?), Bogotá, Bratislava, Bucharest, Budapest, Buenos Aires, Caracas, Dublin, Guatemala, Havana, La Paz, Lima, Lisbon, London, Madrid, Mexico, Montevideo, Port-au-Prince-Cuiadad Trujillo, Quito, Rio de Janeiro, San Salvador, Santiago, Vichy, Washington,

KIC: Asuncion, Bogotá, London, Port-au-Prince-Cuidad Trujillo, Rio de Janeiro, Santiago, Vichy, Washington

KID: Bangalore, La Paz, Hanoi-Hue, Tokyo, Vichy

KIE: Peking

KIF: Berlin, Berne, Lisbon, Madrid, Ottowa, Vichy, Washington

KIG: Bogotá, Buenos, Aires, Guatemala, La Paz, Ottowa, Port-au-Prince-Cuidad Trujillo, Quito, San José – Panama-Managua, Santiago, Washington

KIH: Washington

KII: London

FIGURE 3

VATICAN SYSTEMS-DISTRIBUTION BY NUMBER OF BOOKS HELD

One book:	Beyrouth, Honduras, Leopoldville, Toyko
Two books:	Beyoglu, Bratislava, Bucharest, Budapest, Caracas, Dublin, Havana, Montevideo, San Salvador, San José – Panama-Managua
Three books:	Asuncion, Berlin, Berne, Buenos Aires, Guatemala, Lisbon, Madrid, Ottowa, Quito, Rio de Janeiro
Four books:	Bogotá, La Paz, London, Port-au-Prince-Cuidad Trujillo, Santiago
Five books:	Vichy ?
Six books:	Washington

FIGURE 4

II

SOLVED SYSTEMS, THE RED CODE (KIA, KII)

13. General. The book underlying KIA and KII is known to its users as *"il cifrario rosso"* (the red code) though it is not clear whether this is merely a loose way of referring to the color of the cover or is the exact designation of the title page. As the letter E is used as a null, the code was first designated by the British as the "E" system, a name which continues to be used in GC&CS, though the American designation is now KIA and KII, two short titles indicating different encipherments. The code is used for general purposes, restricted and confidential, though occasionally it will be used for secret communications, e.g., circulars sent to stations not having KIB or another more secret system. It was in use at least as long ago as 1936, but how much earlier is unknown. Nearly every station has a copy (see *Figures 2-4*). KIA messages may be identified by the system indicator which is W, X, Y, or Z, if followed by a digraphic number, or B, C, D, or E, if followed by a trigraphic number. KII messages begin with I, J, K, L, or M, followed in each case by a digraphic message number.

14. The Code. The code is one-part, having twenty-five values to a column, and since code-instruction messages refer to the columns as *"pagine"* (pages), there is probably only one column to the page. The exact number of pages is unknown, but it cannot be greater than 441; the page numbers are enciphered by digraphs forming a square of 21, and it almost certainly must be at least 438, since 401 pages have now been identified, with very good evidence to indicate that groups appear on at least thirty-seven more. The size of the book, then, must fall between a minimum of 10,950 and a maximum of 11,025 groups. Certain of the lines scattered throughout the volume appear to have been blank when the book was printed, and many of them may still be without values though some have now been filled with addenda. Different copies of the book have different values on

certain pages, but there is no way of attempting an estimate of the number of different values in all the copies combined.

The book is made up of a general vocabulary and many appendixes, the former occupying 331 pages and 18 lines on another; so the total of the vocabulary is 8,294 groups, assuming that each line is filled with a value. The general vocabulary of this code is thus only about half as large as those appearing in the average Italian diplomatic books. As in them, values appear in the form of root plus ending or endings.[13] While most verbs occur only once, some appear to have several variants for inflectional forms, the second form being frequently, but not always, the present participle. In diction the vocabulary is likely to be archaistic, and there has been no attempt to avoid words regarded as reprehensible by purists. The Vatican code compilers, as members of an international organization, do not suffer from the intense nationalism of the Fascist Party. No personal or place names appear in this list, and there is a high percentage of purely ecclesiastical vocabulary. At the end of the listings under each initial letter a few lines have apparently been left vacant.[14] In general the code is poor in phrases, poorer in variants, still poorer in less frequent words, e.g. *scrupulosamente* must be spelled out in several groups every time it is used, and there are no qualifying groups and no groups giving inflectional endings.[15]

The position of only one of the appendixes can be surely determined. This is the one containing 454 groups for first names and place names. Since it ends with *Zurigo* on line four of the same page as the beginning of the general vocabulary on line seven, this appendix must precede the vocabulary. The others, arbitrarily placed after the vocabulary by the British, come in some instances before and in others after, and include the following:

a. punctuation[16]
b. numbers; units under 100, hundreds, thousands under 10,000, tens of thousands to 200,000 (6 pages)
c. months and days
d. years and anniversaries
e. introductory phrases (6 pages)
f. frequent auxiliary verbs in various forms (6 pages)
g. acts of the Pope

---

[13] For sample pages of the encode and decode forms of this book see *Figures 5-7* below, which show the pages illustrated as they now stand.

[14] Nineteen lines are unidentified at the end of the letter "E" (page 137) and the same number at the end of the letter "G" (page 159). Some of them have addenda which do not fit the alphabetical range.

[15] That is, there are no groups meaning, e.g., "first person plural past." To indicate inflectional endings not provided for by variants the code clerk must spell out the form in two or more groups, e.g. *communic-ate*.

[16] One page to each category is understood unless otherwise stated.

h. names of dioceses, etc. (5 pages)
i. military terms (3 pages)[17]
j. titles of heads of orders
k. adverbs of time
l. titles of officials
m. honorary titles
n. canon law
o. diseases and health
p. names of Catholic organizations
q. miscellaneous

Comment is needed on only one item (h). These pages contain lists of archdioceses, dioceses, vicariates apostolic, prefectures apostolic, etc.,[18] the list in each copy being different from the others and containing those names which belong to the area in which the representative using the copy is stationed. Needless to say, such diversity is troublesome in analysis.

15. **Encipherment.** The three elements which must be enciphered (the page symbols, the position symbols, and the spelling) are enciphered according to one of four different keys. Keys 1 and 2 are called KIA and are used by all stations holding the book, and keys 3 and 4, which are used only in London traffic, are called KII. Each key provides a method for enciphering each element, and the use of one key for page encipherment determines that the corresponding key for position encipherment will be used, and normally, though not always in actual practice,[19] the key for spelling encipherment will be the same also.

a. **Page encipherment.** In the four keys for the encipherment of the page symbols, no relationship has been found. Sometimes a page will by chance have the same identifying digraph in two keys (e.g., WV on page 189 in keys 1 and 3).

(1) **Page key 1 (KIA).** This key consists of digraphs made up of one of the twenty-one consonants (Y is a consonant) in either position, and the 441 digraphs are assigned to the page numbers in a completely random sequence. In normal practice this key is used only on odd days of the month, but at times messages sent on even days will have it, owing to delay in transmitting or to a garbled date, and when once a message has begun in the odd key, it may change at will to key 2 simply by including the group for "change key."[20] For some unknown reason the odd key is

[17] These are useful in carrying on works of mercy among soldiers and prisoners of war.
[18] No titular secs are included.
[19] The result of choosing the wrong key.
[20] There is no group for "change system." When systems are changed, the message says "I now use the ... code."

used oftener than one would expect from the nature of the calendar. The odd table has been recovered for 399 pages, approximately 90 percent, and the unidentified pages are all highly specialized and therefore very infrequent pages. (See *Figure 5)*

(2) **Page key 2 (KIA).** This key, which alternates with no. 1 on even days of the month with the same variations from the norm, is composed of the identical 441 digraphs but in a completely different sequence. In this key 401 pages have been identified, approximately 90 percent, and again the unidentified pages are highly infrequent. (See *Figure 5)*

(3) **Page key 3 (KII).** This key, used on odd days,[21] presumably, and only in traffic to or from London, is composed of digraphs having any letter except the null in either position. Since only 441 of the 625 possibilities are needed, 184 must be omitted, probably chosen in a random manner. Of these digraphs, 323 have been identified, approximately 73 percent. (See *Figure 5)*

(4) **Page key 4 (KII).** This key, used on even days, presumably, of the month and only in traffic to or from London, is composed of digraphs in which any letter except E may appear in second position and any letter but C, E, H, K, P, and V may stand in first position. Thus, the permutations are 19 x 25 = 475 possibilities, 34 more than are needed. Of these digraphs 261 have been identified, or approximately 59 percent. (See *Figure 5)*

b. **Position encipherment.** Here also the encipherment is by four keys but position key no. 3 is identical with position key no. 1 and position key no. 4 with position key no. 2. The two keys are printed in adjacent columns on the page.

(1) **Position keys nos. 1 and 3 (KIA odd days, KII odd days?):** This is a direct standard English alphabet minus E, comprising the sequence of 25 letters identifying the lines of the page.

(2) **Position key nos. 2 and 4 (KIA even days, KII even days?):** This is a reversed standard English alphabet minus E, comprising the sequence of 25 letters identifying the lines of the page.

---

[21] The point is not absolutely certain, since there seems to be some variation in the 65 messages available.

KIA: PAGE ENCIPHERMENT DIGRAPHS FIRST FIFTY PAGES

Page	Key 1	Key 2	Key 3	Key 4	Page	Key 1	Key 2	Key 3	Key 4
1	GT	LL	FK	TI	26	MV	TB		
2	BB	MW			27	SZ	ZZ	ZJ	
3	QL	NB		SA	28	CV	JJ		
4	KX	ZG	CK	DO	29	TR	RZ		LO
5	WW	RB	YD	WD	30	BQ	NL		
6	JF	PF	WS		31	WB	BQ	CP	NT
7	SS	TF	BV	QO	32	ZF	RK	NR	XP (XR?)
8	XD	FP	PB	ZV	33	FF	BL	AW	LR
9	NJ	XC	ZN	IO	34	JV	PC	IV	UA
10	FW	LD	QB	AL	35	XP	HQ		
11	KC	RG	GD	UR	36	TN	LB	NC	ZO
12	RR	HG	CW	IA	37	CZ	FL	AP	MT
13	SG	KK	UC	WG	38	NC	TS		TL
14	LD	WF	GT	DU	39	DQ	PM	XI	DH
15	VW	GX		UY	39a		JW		
16	GM	YK	RQ	NJ	40	RC	KR	ZC	QG
17	DN	PG	HK		41	BD	CR	UT	ZR
18	PP	VK			42	QX	ZN	LP	DC?
19	YJ	NH	CF	JQ	43	YV	QT	DH	SS
20	HQ	NK			44	HZ	DX	QH	OA
21	VD	WT	KR		45	GC	SJ		JQ
22	KK	DG	OM		46	KR	MN	WH	BR (UP?)
23	JB	QC			47	PG	WL	KH	WZ
24	NS	RR	ZW		48	WM	HB	LV	
25	QH	GG	TJ		49	XK	GW	JD	

FIGURE 5

No instance has been found of a message in which position key no. 1 has been used with page key no. 2, or the reverse. It might therefore be thought that the users of these systems have trigraphic tables giving equivalents for both page and position as a unit, but this is unlikely, since in code-instruction messages the positions have been referred to as "lines A and Z," "S and I," etc., showing that the printed book must have a page format similar to that of the reconstructed encode.[22]

c. **Spelling encipherment.** The absence of surnames in the vocabulary and the relative poverty of the code in spelling groups, makes it highly desirable, if not absolutely necessary, to have an auxiliary method of spelling proper names and foreign words. As with the page and position encipherments, there are four different keys, and these are used with the corresponding page and position keys, but at times the code clerk will choose the wrong key. The four keys are merely monoalphabetic substitution based on the following enciphering alphabets:

(1) Spelling key no. 1 (KIA odd days):[23]

plain: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
cipher: Z Y X W V U T S R Q P O N M L K J I H G F E D C B A

(2) Spelling key no. 2 (KIA even days):

plain: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
cipher: B C D F G H J K L M N P Q R S T V W X Y Z A E I O U

(3) Spelling key no. 3 (KII, London traffic only, odd days?):[24]

plain: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
cipher: E N R I W Z A X M Q . U B Y D O . V K C P S F . L G

(4) Spelling key no. 4 (KII, London traffic only, even days?):[25]

plain: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
cipher: G . B M T C S A F . D R . Z E . . O U K P I V . . W

In using these tables, the code clerk will set off the cipher passage from the adjacent code groups by doubling the null, e.g. EE . . . . EE. Occasionally, the

---

[22] See *Figure 8* below for an illustration of this.
[23] Reciprocal alphabets are used here, a standard alphabetic reversed.
[24] The omissions result from too few examples in the available traffic.
[25] The omissions result from too few examples in the available traffic.

clerk will confuse cipher and plain components, which makes no difference in the case of key no. 1 where the alphabets are reciprocal, but elsewhere the result will be gibberish, but the reverse of the process will quickly produce plain text.

d. Transposition. In keys no. 1 and 2, the group is always sent in page-position order, whereas in keys 3 and 4 it may be transmitted in position-page order.

16. Cryptanalysis.

a. Solution in GC&CS. The British began to study the "E" system in June 1942 and by August 1943 had identified 2,824 values, solved 80 percent of the two page-encipherment tables of KIA and about 60 and 29 percent respectively of those of KII, as well as the KIA spelling tables, and the KII spelling tables as far as they are now solved. Though this office lacks any account of how these solutions were reached, the steps must have been very much like the following:[26]

1. Recognition that the encipherment is trigraphic and that E is a null;

2. Recognition of the existence of the two keys;

3. Indexing of available traffic by trigraphs;

4. Assignment of arbitrary numbers to the pages of the general vocabulary, using normal methods of recovery based on frequencies.

5. Recognition of the pattern of position encipherment as soon as sufficient groups had been identified;

6. Gradual assignment of more digraphs to the arbitrary numerical sequence.

7. Normal methods of code recovery thereafter.

8. Solution of the spelling tables as monoalphabetical substitution.

The arbitrary sequence of numbers assigned by the British to the pages proved to be remarkably accurate. The British themselves discovered three pages for which they had not provided a number and inserted them as supernumerary sequences (pages 039a, 070, and 189a). On page 070 no plain value even yet

[26] This list of steps is in part based on the much fuller reports on KIB.

appears in the American copies though the British have recently provided a digraph for this page in key no. 3, on what evidence is not known. The last identified group on page 69 is Y = B *chéque*, and the first on page 71 is A = Z *chi*; so it is difficult to see what values would intervene. Two other pages (386-387), containing a miscellany of frequent words like *che, con, di, per, and si*, have never been used in American traffic with keys nos. 1 and 2, but are used with keys nos. 3 and 4. No explanation is available for this phenomenon, but page 385, which contains the same type of miscellany (*codest, di, in*, etc.), has been used with all four keys, the digraphs being, respectively, ZT, GC, MU, TP.

An additional error seems to have been made at page 304 and 305. In key no. 1 the digraphs are, respectively, NM and VK, and in key no. 2 page 305 has a reconstructed digraph (VW), but no digraph has been found for p. 304. In key nos. 3 and 4, on the other hand, no digraphs have yet been identified for either of the pages. The values on the two pages, however, are identical in three instances, and wherever there is a value on only one page of the two, the sequences fit together nicely except that line N = N has *spiegazione* on 304 and *spingere* on 305; *spiegazione* also appears on line K = Q of page 304 and indeed, the analysts have suspected that the true value of line N = N should be *spoinaggi*. Doubtless, one of the identifications for this line is incorrect, and both sequences are the same, the cause of the error being incorrect assignment of two digraphs in key no. 1 to this page.

b. Solution in the SSA. To continue the same topic here, American analysts recovered two new pages to which they gave the number 389 and 421, containing, respectively, sequences from *apostolic* to *appena* and from *sottasegretario* to *sparire*. The former proved to be page 39a and the latter fitted nicely into a lacuna not previously suspected between pages 302 and 303 and may be numbered, according to the British system, page 302a. The rest of the British page numbers have all been confirmed by American experience.

That some of the appendixes placed after the vocabulary by the British really belong before it was shown when a message was sent to the Vatican by the Apostolic Delegate in Washington on 21 October 1943. He asked that a number of new values, frequent in his reports, be added to the code, and he specified the exact places by giving the numerical values of the pages, i.e., 007, 096, 223, 231, 367, 411, and 467. Obviously, page 007 must be early in the book, and this proved, upon being used in the traffic, to be that numbered by the British as 381, i.e., after the vocabulary. It was not thought advisable, however, to make any adjustment in the book since this information was fragmentary at best.

When work began in the SSA, the British reconstructions were available in photographs, making it possible to decode by the process of converting the page digraph to its numerical equivalent and then to find the value by consulting that

page in the photographs. This process was long and tedious, and by being a double operation provided two chances for error. Moreover, to use it required the preparation of a separate work-sheet for each message, while in addition it was at times very difficult to read the British handwriting. Accordingly, it was necessary to prepare a decode; two were prepared, one for each key (keys nos. 1-2 only). A blank sheet was prepared for each page, illustrated in *Figure 6* for key no 1 and *Figure 7* for key no 2.[27] The values were then copied by hand in pencil.[28] The pages, however, were arranged in alphabetical sequence of the page digraphs, not numerical sequence, and it was thus possible to eliminate from the decoding process the operation of converting the digraph to the number, and since a copy was made for each key, it was possible for two decoders to work simultaneously on different messages. (When "change key" was encountered, the decoder would simply hand the message to the other decoder for completion.) Current traffic was decoded first, but, when time permitted, older traffic was processed until in April 1944, all KIA decoding was up to date.

For editing and code recovery the photographs were still used as encodes,[29] but in December these were copied once more on blanks similar to those used for the decode, of which *Figure 8* is a sample.[30]

It would have been useful to make an index of the trigraphs in the available traffic, but this would have entailed much IBM work, and it was not thought worth the trouble, particularly since, as one British report put it, in a one-part code of this type, "any identification that is reached is probably right."[31] Accordingly, book recovery was based in the main on single occurrences of which the range was known to within a few variations. As time went on, the analysts began to recall groups which had given trouble and informal notes were made of their occurrences. These were made by inserting into the encode a record of the messages in which groups occurred. At first, no record was made of the occurrence of bad pages (groups of which the digraph had not yet been assigned to any numerical page) for it was not realized that the British tables were incomplete – it was thought that these digraphs were garbles. They became so frequent, however, that they too were indexed in the same informal manner, and, finally, a blank sheet was set up for each digraph not yet identified. Only three of the sheets in key no. 1 have no occurrences listed and only eight in key no. 2, and these may actually be good pages not occurring in the traffic by chance. In any

---

[27] No special decodes have been made for keys 3 and 4 (KII) because of insufficient traffic.

[28] In the illustrations the values are typed for greater legibility. In indicating the various keys, red is reserved for key no. 1, blue for key no. 2, green for key no. 3, and lavender for key no. 4. The pages illustrated contain values identified after the original copying was made.

[29] Strictly speaking, it is not proper to speak of encodes and decodes of a one-part code. The use of more than one key in encipherment, however, and of a mixed table of page encipherment, has the result of giving to the system certain two-part features.

[30] Later this process was repeated, and there are now available two complete encodes and a decode for each key.

[31] The correct page range eliminates all possibilities of garbles in the first two letters and most of them in the third.

SAMPLE PAGE OF DECODE FOR KEY NO. 1 (KIA)

	ZH*(3)	
322	TE*(1)	KZ*(2)
A	TIVE	
B		
C	TIV	
D	TO	
F		
G	TOCC ARE	
H	TOCCAT	
I		
J	TOFLIE	
K	TOI	
L	TOL	
M		
N		
O	TOLLERANZA	
P	TOM	
Q	TOMBA	
R		
S		
T	TON	
U	TONNELLAT	
V	TON O	
W	TONSURAT	
X		
Y	TOR	
Z		

	LI*(3)	XG*(4)
181	TB*(1)	CC*(2)
A	K	
B	KA	
C	KE	
D	KI	
F	KO	
G	KU	
H		
I		
J		
K		
L	L	
M	LL	
N	LA	
O	LAB	
P	LAC	
Q		
R		
S	LACUNA	
T		
U		
V	LAF	
W	LAGN	
X	LAGO	
Y	LAIC	
Z		

FIGURE 6

*In text, these letters are written in color: 1 = red, 2 = blue, 3 = green, 4 = lavender.

SAMPLE OF DECODE FOR KEY NO. 2 (KIA)

	GK*(3)	SF*(4)
339	CC*(1)	NG *(2)

Z	
Y	VERIFIC
X	VERIFICAT
W	
V	VERITA
U	VERO
T	
S	
R	VERS AT
Q	VERSAT
P	VERSAMENT
O	VERSAMENTI
N	VERSION
M	VERSO
L	VERTE
K	
J	VES
I	VESCOV
H	VESCOVAT
G	VESCOVIL
F	
D	
C	
B	VESTIT
A	

	CP*(3)	JG*(4)
019	YJ*(1)	NH*(2)

Z	WASHINGTON
Y	
X	YOKOHAMA
W	ZURIGO
V	
U	
T	A
S	A
R	AA
Q	
P	ALUI
O	AB
N	ABA
M	ABATE
L	ABBADIA
K	ABBADESS A
J	ABBANDON
I	ABBANDONAT
H	
G	
F	ABBASTANZA
D	ABBATT
C	
B	
A	

FIGURE 7

*In text, these letters are written in color: 1 = red, 2 = blue, 3 = green, 4 = lavender

SAMPLE PAGE OF ENCODE OF KIA-KII

		YN*(3)	
	173	PT*(1)	GF*(2)
A	Z	INTANTO	
B	Y	INTATT	
C	X	INTEGR AL MENTE	
D	W	INTEGRITA	
F	V	INTELLETTUAL	
G	U		
H	T		
I	S	INTEND	
J	R	INTENDEVA	
K	Q	INTENDIMENT	
L	P	INTENS	
M	O	INTENTAT	
N	N	INTENZION	
O	M	INTER	
P	L	INTERA	
Q	K	INTERCED ERE	
R	J	INTERCETT	
S	I		
T	H	INTERDETT	
U	G	INTERESS	
V	F	INTERESS	
W	D	INTERESS AT	
X	C	INTERESS	
Y	B		
Z	A		

		JU*(3)	ON*(4)
	174	VZ*(1)	YD*(2)
A	Z	INTERIN ALE	
B	Y	INTERNA MENTO	
C	X		
D	W	INTERN	
F	V	INTERNAZIONAL	
G	U		
H	T	INTERR ARE	
I	S	INTERPRET A	
J	R		
K	Q		
L	P	INTERPUN	
M	O	INTERROG	
N	N	INTERROMP	
O	M		
P	L	INTERVALLO	
Q	K	INTERVENIRE	
R	J		
S	I		
T	H	INTERVENZIONE	
U	G	INTERVISTA	
V	F	INTES A	
W	D	INTEST	
X	C	INTESTA	
Y	B	INFIM	
Z	A		

FIGURE 8

*In text, these letters are written in color: 1 = red, 2 = blue, 3 = green, 4 = lavender

case, they frequently furnish the editor of a message with additional information about the kind of meaning to be found in them, as the work progressed, many of the digraphs have been assigned numerical values and entered in the book.

Progress in book recovery has resulted in a total of 5,875 identifications, of which 2,824 came from the British, and 3,051 were identified in SSA. The page encipherment tables have been recovered for key no. 1: about 90 percent; key no. 2: about 90 percent; key no. 3: about 73 percent; and key no 4: about 59 percent. Recovery of additional digraphs in keys 1 and 2 is now very difficult, since the unidentified pages have highly specialized values or even miscellanies. In keys 3 and 4, the same is true though to a more limited degree.

Throughout the earlier stages of work in the SSA considerable trouble was experienced with the pages on which names of dioceses appeared. A group which the British had identified as Westminster was noticed in contexts which required the name of a diocese in Central America, but no diocese with this name or one like it was known in that region. Another group appeared as the town in Massachusetts in which a certain man lived at a certain number on Boylston Street. Boston seemed to be indicated and consultation of the Boston telephone directory showed that the man did live at this number on Boylston Street, Boston. Accordingly, the group was entered, but the next day a message was received in which the same group stood for the name of a diocese in Venezuela, and on the day following it was the name of a see near Tokyo. Naturally, such phenomenon was highly disturbing, but as time went on, still more evidence of this kind was uncovered, and even when there was no contradiction, alphabeticity was apparently lacking on the pages in question. Three hypotheses were suggested to explain these strange phenomena:

a. The British had wrongly equated digraphs in the different keys;
b. The pages in question did not have alphabetical arrangement;
c. The pages were different in different copies of the same book.

The first hypothesis was never very seriously entertained though, to be sure, there is in the book a page where this has happened.[32] The second hypothesis had to be abandoned because on one page (380 = NT in key 1 = RQ in Key 2) alphabeticity was clear in the sequence:

I S	LOS ANGELES
S I	NEW ORLEANS
T H	NEW YORK
U G	OGDENSBURG
V F	OKLAHOMA

[32] See page 22 for example.

Accordingly, all occurrences of groups on the pages FH, FQ, HR, NT, TH of key no. 1 and their equivalents MV, RS, LC, RQ, BS in key no. 2, were indexed by reading through the 4,000 messages availahle at the time, and these were listed separately by circuits. The point of attack was the Washington list since there were more such occurrences there, and more groups that had been certainly identified. A list of all dioceses and archdioceses in the United States was prepared, and an attempt was made to fit names in the list to lines of the code. By counting back from Winona, the last identified diocese, and the last diocese in the complete list, to the next identified diocese, Scranton, one found exactly the right number of names for the number of lines in the code. Similar counts elsewhere for sequences hetween pairs of identified values proved to be in most cases the right number, though not always so exact. Dioceses of recent creation had to be omitted; dioceses with names possessing a spelling in Italian different from the English form (e.g., *Filadelfia* for Philadelphia) had to be alphabetized in their Italian form. Here and there a name was found to be one off the necessary position, showing that certain possible names were missing in the code. Maryland, for example, identified from the address of Camp Meade, had to be changed to Baltimore and Washington, to fit the range. There was no value for the first line in the sequence, and it has since been determined that Albany, which had been put four lines down, belongs here. One line contained the name of a vicariate apostolic in the neighborhood of the United States but outside its limits. A plain-text message was received giving the name of the see of a newly appointed prelate whose name also appeared with this group in a code message, and it was seen that the group was really Bahama Islands, which fitted the range nicely. It thus became clear that the Washington book has some vicariates apostolic in addition to the dioceses and archdioceses but not all of them.

When the Ottowa lists were examined, it was found that the necessary names fitted the space exactly, but since then some of these have had to be corrected. The same method was applied to all the lists and confirmation of the third hypothesis has been abundant. In general, the Italian name is used (e.g., *Baiona*, not Bayonne, in the Vichy book) and the exact name of the diocese as it appears in the *Annuario Ponteficio* must be used (e.g., *Cuyo, San Giovanni di*, instead of San Juan in the Buenos Aires book). Naturally some lists were more easily recovered on the basis of the patterns than others, but with continued effort nearly all of the lists could be recovered if enough traffic were received. For the most part these names are used, of course, for purely ecclesiastical business of no intelligence value, but occasionally they are used for more interesting messages, e.g., a message from Rio which reported the building of airfields at Pernambuco. The Japanese list has provided the most trouble, except for a sequence of twelve place names in the Far East added by the Delegate to Tokyo in place of those already inserted there.

III

UNSOLVED SYSTEMS, THE YELLOW CODE (KIB)

17. General. The code designated in the SSA by the trigraph KIB and called in GC&CS the "YZ" system is known to its users as "*il cifrario giallo*" (the yellow code), but it is not clear whether this designation is derived from the color of the cover or is really the exact title. Unlike the red code (KIA-KII), KIB is not distributed to all stations, but is sent only to the more important and then not to all of them, e.g., London which uses KII for the same type of communication. KIB is restricted to the more secret type of message and thus is analogous to the enciphered systems of the Italian diplomatic series. Messages begin with the system indicators B, C, D, or E, followed by a digraphic number.

18. The code. Since the system is not yet solved, information about the book is fragmentary. Certain facts, however, are well established. The page contains only twenty-four values, instead of twenty-five, as in KIA-KII, since two of the twenty-six letters are used as nulls. This means, four letters are used, a permutation of twenty-four cubed will give the maximum possible size, i.e., 13,824, but further limitations, as yet unknown, may cut down this maximum still more, though there is good reason to believe that the book is actually larger than KIA-KII. In a crib[33] the plain text was enciphered in KII by 163 trigraphs while only 136 were needed in KIB. Furthermore, the word *asse* (Axis) is sent by one trigraph in KIB but has to be spelled out KII. Because the word *Italia* appears on the same page as *istruzion* and *istitu*, it is clear that the list of personal and place names does not appear at the beginning of the book, as in KIA-KII, but the names are distributed at the proper places throughout the general vocabulary. But there are in all probability other appendixes, including some for numbers and punctuation, unless, as in the Italian diplomatic codes, these signs are spelled out in words and also distributed throughout the vocabulary. The presence of a group

[33] The evidence for most of the statements in this section will be given in detail under cryptanalysis, paragraph 20.

for *asse* may reflect a later date compilation than 1936, the date of the founding of the Rome-Berlin Axis, but since the ending of the third singular past subjunctive active in Italian is *–asse*, this may not be so. It is also probable that in the book the lines are numbered consecutively from 1 to 24, rather than indicated by sequences of letters representing the position encipherment keys as in KIA-KII, since position encipherment appears to be by as many as 31 different keys, and a book printed with position encipherments for that many keys would be very unwieldy.

19. **Encipherment.** The encipherment of KIB is similar to that of KIA-KII in that a digraphic table is used for the page, a single letter for the position, and substitution tables for the encipherment of proper names, and transposition of the group is permissible.

a. **Page encipherment.** Little is as yet certain about the tables of encipherment except that they are digraphic and that any letter except the nulls Y and Z may stand, apparently, in either position of the digraph. This means that there can be no more pages than a square of twenty-four or 576. It is certain that there are many such keys,[34] and probable that there is one for each day of the month in each circuit, though some of these are perhaps identical with some in other circuits. Some stations, e.g., Washington, have different keys for communication with the Vatican from those used for messages to other addresses. At least four families of messages have been isolated, the so called "WAMADU",[35] "QJ", "DR", and "FS" keys, but since many messages do not fit any of these, there are at least two other families and very likely several more.

b. **Position encipherment.** The position is enciphered by a single letter, and there are probably at least thirty-one different keys, perhaps even more. Thus far, there is no indication of any relationship between these keys, akin to that of KIA-KII where key no. 2 is merely the reverse of key no. 1. The keys seem to be completely random mixed alphabets with the nulls Y and Z omitted. There seems to be correspondence between page keys and position keys, i.e., on any day of the month (any month of the year) the traffic in one circuit will have the same page and position key. There have been examples of the same plain text sent in two different messages to different addresses with the same page key but different position keys. Messages apparently bear no indicator of the keys used, or at least none has been noticed so far. As in KIA-KII the variants for system indicators seem to have no significance as key indicators.

---

[34] On 30 August 1944, the nuncio at Bogotá explained to his colleague in Quito that he had enciphered a message, not available, with the "yellow code, table 6 of the little book." This is the only Vatican code-instruction message mentioning one of the encipherment tables.

[35] The derivation of these names will be explained below.

c. **Spelling encipherment.** Like KIA and KII, KIB uses substitution tables for spelling proper names and foreign phrases. These tables, of which there is probably one for each page key, are definitely not monoalphabetic. The only one solved thus far, used in enciphering some, but not all, of the spellings occurring in Bogatá traffic, is polyalphabetic with random-mixed cipher alphabets. Attempts to solve certain of those in Washington traffic by the use of highly probable words were unsuccessful. The use of the two letters as nulls permit greater variety in the doublets, and hence repetitions of the familiar pattern will be much less frequent than in the case of EE . . . . EE in KIA-KII. The following are the possibilities:

YY . . . . YZ	ZZ . . . . YZ	YZ . . . . YZ	ZY . . . . YZ
YY . . . . ZY	ZZ . . . . ZY	YZ . . . . ZY	ZY . . . . ZY
YY . . . . YY	ZZ . . . . YY	YZ . . . . YY	ZY . . . . YY
YY . . . . ZZ	ZZ . . . . ZZ	YZ . . . . ZZ	ZY . . . . ZZ

d. **Transposition.** After the group has been enciphered by a trigraph, it may be transmitted in either the page-position order or the position-page order, but not with the position between the letters of the page digraph, and no indicator has as yet been discovered for this variation, nor any pattern of usage.

20. **Cryptanalysis.**

a. **Solution in GC&CS.** Work began on the solution of KIB in GC&CS only two weeks earlier than in SSA, i.e., "a fortnight before 1 September 1943." Fortunately, very full reports are available for the progress made as far as 17 May 1944, the date of the last report received.

It was soon discovered that KIB messages would not break up into trigraphs if E were taken as a null, nor could they be read with the KIA-KII tables of encipherment. If, however, Y and Z were taken as nulls, the messages would break up into trigraphs with sufficient repetitions of trigraphs within messages to prove that KIB was trigraphic. An index of all available messages was made, but with far from satisfactory results, since repetitions between messages were no more numerous than the random expectation. It was thus at once suspected that the basis of the encipherment was a multiple-key system. The task, then, became an attempt to recognize groups of messages which were in the same key, and, it may be said here incidentally, this task is still far from finished.

Since KIB was not held by London and KII not held by Washington, it was thought likely that the Vatican had on the same day sent the same message to both stations in the two different systems. KII was then fairly readable, and a message sent on 21 June 1943, describing the bombing of Rome, was chosen as the most likely KII message for the search. Another message in KIB sent to

Washington on the same day was examined, and there was soon no doubt that both messages contained the same plain text. Though the lengths were different, the KII message of 163 trigraphs, the KIB of only 136 trigraphs, the pattern of repetition within the two messages fitted nicely together, and was clear that the two messages had the same plain text. From this crib came identifications for fifty KIB trigraphs (at least in the particular key of the message) of which the most significant were:

C CF richied-	R CF richiam-
T BX anche	B BX ancora
E PW militar-	D PW mezz-
K LI protest-	G LI proposit-
A EF sugli	X EF sulle
A DK rigett-	U DK rilev-

Certain facts were immediately apparent. These trigraphs were sent as position-page, rather than page-position. Each of the pairs of two words fell within a sequence of 24 lines in KIA-KII, but *protest-* and *proposit-* are not on the same page of KIA-KII; so the book must be different from the red code, and indeed, it is known now that it is called the yellow code. The position encipherment is more complicated than in KIA-KII, since *anche* and *ancora*, which would come on consecutive lines in that code, are here enciphered by T and B.

At the same time two other messages were found, 20 July 1943, sent on the same date to different addressees in the same page key but with different position keys (Vatican to Dublin and Madrid, and Vatican to Washington) which began as follows:

Dublin-Madrid:	AWR[36]	LT X	RX K	GR H	CN U	VH H	NJ G	NO I	NQ U,	etc.
		LT S	RX M	GR I	CN U	VH I	NJ D	NO H	NQ U,	etc.

In this case, the order is page-position; so it is clear that either order is possible. The Washington-London crib is of odd date, and this later pair is of even, but the scent proved false. Two additional messages were located, sent on different dates to the same addressee with the same page key but different position keys (Vatican to Bratislava, 22 and 27 September 1943) which began as follows:

22 September:	QN P	WT D	BT	B	LI	T	PH N	TN Q	AS R	KP O,	etc.
27 September:	QN L	WT B	(NM)	X[37]	LI	U	PH X	TN R	AS H	KP W,	etc.

The sum of this evidence showed that stations possessed in addition to position keys at least several page keys. This would account for the flatness of the distribution revealed by the general index.

---

[36] This group is unexplained unless it means *circolare*.

[37] A garble.

Though the distribution was flat, it became possible to search for messages which exhibited repetitions, and five messages in the Madrid circuit were found with marked repetitions, all of them dated on the 18th of some month (August, September, October, November 1942, and January 1943). This seemed to indicate that the day of the month was significant, a discovery paralleled by contemporary experience in SSA. Six more messages on the 14th (July, October 1941; July, October, Novemher 1942; September 1943) were found to contain repetitions among them. These were repetitions of the page digraph, and were identical with those repeated in the group of messages sent on the 18th, but apparently the position key was different. It was now possible to build up groups of messages in position key no. 1, position key no. 2, etc. More messages were found which used either the same page digraphs which showed at least six, and possibly as many as thirty-one, position keys, and the page keys appeared to be valid for as long a time as three calendar years.

By Novemher 1943 a group of nineteen messages using the same page key had heen isolated and given the name "WAMADU" (Washington, Madrid, Dublin, though, as since has heen found out, more stations use the key) or "general key no. 1." (The term "general key" is the British equivalent for the American "page key" while their term for "position key" is "margin key.") From the "WAMADU" messages it was possihle to "identity" a certain number of digraphs in that key for pages on which some groups were known to be located.

At this point an attempt to isolate other families of messages using the same page keys were based on repetitions of sequences of two or more groups repeated between messages with the same or different position encipherment, and the result was that at least four distinct page keys were isolated. The crib mentioned above proved to be in one of these groups, and therefore it was possible to say that on fifty of the pages at least one group was known to appear. At the time only fifty were known, but hy the end of 1943 this number had gradually increased to 128. For example, if LI occurred as a page digraph, as it does, it was known that this page had <u>protest</u>- and <u>proposit</u>- on it, and since there are only 24 groups to a page, the alphabetic range of that page was known to a maximum of 47 groups. At this point a new method was introduced. Going through the entire body of traffic, the analysts entered, wherever a digraph appeared of which the page range was known in "WAMADU" (general key no. 1), the tentative range of that page. Each message had to be gone over twice because there is no easy way of telling whether the order is page-position or position-page. As a result of this broad method, a sequence was found in a message which appeared as follows (the parentheses indicate merely the range, not necessarily the actual group itself):

ID J	UI R	UN A	NN I	UI I	KS L
(*non* solo)	(*città Vaticana*)	(*ma*)	Unidentified	(*città Vaticana*)	(*Roma*)

This looks very like "*non sola Città Vaticana ma (?anche?) città di Roma*" (not only Vatican City but also the City of Rome). By use of this method, a number of additional messages were added to the "WAMADU" group.

Simultaneously, progress had been made in reducing the position encipherment to a basic key. This was done in the following manner:[38]

> The letter K is at present the best clue. On page LI the position K means *protest-* but on the same page we also have for certain that G means *proposito*. Measuring by the E code, which will serve roughly, *proposito* is 19 words before *protest-*. We can therefore place K as somewhere below, say, the 17th position on the page (i.e., K = 17 to 24). On page TH the position K means *risparmi-*. We have reason to think that *rispo-* is also on this page. That means that there are at least five words below K = *risparmi-* on this page, i.e. that K must be above position 19 (K = 1 to 18). This narrows K down to 17 or 18 and G to 1 or 2. Compare pages BC and CF where the group on line G is the earliest alphabetically of the groups known on the page. Wherever G or K have been identified and another letter also on the same page we can now make a similar measurement and get a value which will be right in proportion as the vocabulary of YZ code corresponds to E code.

By the end of November this method had resulted in isolating twelve page keys which were recovered in 66 instances out of a possible 264 (eleven of the twelve non-basic position keys with 24 lines each converted to the twelfth).

At this point a method of double-indexing was established. Each trigraph was indexed in pencil whenever the position encipherment had not yet been converted to the basic position encipherment and in ink over it whenever this conversion had taken place. The method was somewhat unorthodox but had the advantage of working. For example the following was noted as repeating twice in one message: VL V BH E FR C. VL is the page with *signific-* on it, and so VL is very provably *signor*. Again, the following was repeated in different messages:

B QT	W HB	D FR	one message
QT D	HB Q	FR J	

[38] The quotation is from an undated British memorandum.

Since QT is the page with *mondo* on it, B QT = QT D suggests *Monsignor-*. A third example was: RX V EO T EO D NM C. RX has *per* on it, EO has *evitare* and NM has *che*. This suggests that EO D is *eventual-ità*; i.e., *per evitare eventualità che* . . . (to avoid the possibility that . . .). As a result of this double-indexing, more groups were recovered on the known pages, and two more cribs with KII were discovered.

The British analysts now attempted to give numerical values to the page digraphs on which known groups appeared. Certain precautions are needed. KIB is longer than KIA-KII, and the appendix of 454 groups at the beginning of KIA-KII is distributed through the book. Thus, a formula was worked out as follows: Page HQ (*istruzion*, *Italia*, *istitu*) is in KIA-KII page 179. From 179 the number of pages in the appendix is subtracted and 160 is the result. To this is added one-fifth, based on the larger book, with the result of 203. Therefore, page HQ was tentatively set down on page 203. On this basis, "WAMADU" was one-fifth solved by the time a report, apparently in preparation over a long period of time but received in SSA on 20 April 1944, was written. In that report lines of further solution were stated as follows: attempts to find more traffic in the partly solved "WAMADU" page key, and attempts to separate all available material into the respective keys.

As no further reports were received from GC&CS until after the British analysts had been sent copies of traffic available in the SSA, in December 1943 it is now necessary to review KIB solution in the SSA.

b. **Solution in the SSA.** At the outset of their work on KIB the American analysts had the advantage of knowing that the system was trigraphic and that the nulls were Y and Z. Progress, however, was slow, owing to lack of adequate personnel and in particular lack of traffic. There were fewer than 600 available messages in all circuits. This would have been sufficient to solve an unenciphered code and probably sufficient to solve even a two-key code like KIA, but with a multiple-key system like KIB, this scarcity of traffic presented a decided handicap.

Messages were studied statistically in an attempt to group them together into keys. It became apparent that messages sent on the same day of the month belonged together, but this observation did not prove to be the rule in every case. Moreover, at first there was no index available, as the necessity for preserving the security of the problem was then thought to preclude the use of IBM procedures; but in December 1943 it was decided that IBM processing really was possible, provided that adequate steps were taken to conceal the identity of the government. This was done by cutting off headings and signatures from the original intercepts and marking each part with a code designation to indicate the circuit, the date, and the worksheet number. The trigraphs, moreover, had to be

separated by lines, and the nulls stricken out, and here the spelling groups presented a real difficulty. It was decided to encircle all such groups with green lines, and to instruct the IBM operators not to punch letters so encircled. This meant, of course, that when a message print was available, the spelling group again had to be inserted at the proper place by hand. As there were fewer than a hundred of these, this did not entail much work. The nulls, however, being stricken out for punching, did not appear in the message print and were actually never copied back in, as doubtless they should have been, since the nulls in KIA-KII frequently seem to have been inserted at points where punctuation is needed or at least helpful. A message print made from such cards will have the disadvantage of not showing the position of the nulls.

When the punching was finished, such a message print was prepared, all messages being separated first into circuits and then into days of the month within that circuit. A general index was made in the page-position order and another in the position-page order. Copies of these three documents were sent to GC&CS as soon as they were available on 20 January 1944.

With this equipment at hand, attempts were made by statistical methods to group messages belonging to the same keys. Tables of random probabilities were worked out for comparison with actual results. By studying the beginnings of messages it was hoped that repetitions would show families. This hope was partially realized, and by the end of April 1944 separate indexes of the traffic in four groups[39] had been prepared: the "WAMADU", the "OJ", the "FS", and the "DR" groups. The first was identical with the British group of the same name, the other three took their names from one of the frequent digraphs appearing near the beginning of messages.

At this point it was planned to begin work on these four families using normal methods of book recovery. Progress in one key would doubtless help in the solution of another, but at the beginning of May 1944 work on KIB was suspended in SSA and the personnel assigned to it transferred elsewhere. Since that time, messages have been continually received and logged, and there are now available over 1150 messages of which only the first 800 have received study.

c. <u>British analysis of SSA IBM studies.</u> When the American IBM indexes and message prints were finally available for the analysts at GC&CS, the Washington traffic was first studied intensively. Certain conclusions were reached by 15 May 1944, the date of the last available report:

a. Traffic in any circuit will on the same day of the month (any month of any year) be in the same page and position keys. Exceptions seem so few as to prove the general rule. Perhaps they are the result of relays.

---

[39] These doubtless coincide roughly with similar groups noticed by GC&CS.

b. Traffic between Washington and stations other than the Vatican does not have the same daily key as the Washington-Vatican circuit.

c. No indication of the order has as yet been discovered, and no proven case of the position symbol placed between the letters of the page digraph.

d. The position keys (presumably 31) are not related in any sort of slide. It is not yet absolutely certain that there are only 31 position keys, but the absence of any indicator seems to show that this is the maximum.

IV

UNSOLVED SYSTEM WITH UNKNOWN NAME (KIF)

21. General. Name and purpose. No information is available as to the name given to this system by its users. Evidence as to such names is usually derived from messages in more than one system since in the red code at least, and probably also in others, there is no group for "change system," and the code clerk must say "I now use the . . . . code." Only one KIF message so far examined begins in another system, and in this case, the other system is KIB and unreadable. Therefore, the groups just before the change cannot be read, and the name of this code is unknown. If, as had been thought probable, KIF is merely a more complicated encipherment of the red code than KIA or KII, there must be a special designation for this encipherment. Even though no message is even partially readable, the occurrence of the system in the traffic suggests that it is used for more secret communications being held by Berlin, Berne, Lisbon, Madrid, Ottowa, Vichy, and Washington.[40] The traffic is probably to be classified as secret. Messages may be recognized by the system indicators Q, R, S, T, U, and V.

22. The code. On this there is even less information, but it seems clear that the maximum size of the book is a cube of twenty-five, or 15,625 groups, since values are enciphered by trigraphs composed of any twenty-five letters. With this maximum range, the view that the underlying book is the red code (KIA-KII) is entirely consistent; some of the digraphs may be omitted. It is just possible, though very improbable, that the basic book is the yellow code (KIB). The objection is that though KIB and KIF are both trigraphic KIB uses two nulls and has only twenty-four lines to the page, whereas KIF has one null and would therefore seem to have twenty-five lines to the page, as is the case with the red code.

23. Encipherment. The trigraph breaks up into digraphs for the page and single letter for the position, as in the case of KIA-KII and KIB. No evidence has been noticed indicating that the position-page order is ever used, since all trigraphs about which one can be sure, and there are many of them, use the conventional order of page-position.

---

[40] London is conspicuously absent, unless KIF traffic to and from London is available in GC&CS.

Traffic in the Washington circuit is homogeneous and different from that in the other circuits, and it forms the bulk of what is available. The encipherment for this circuit employs sixteen separate and distinct keys, which consist of a digraphic table for each key formed of twenty-five letters for the page symbols and a monoliteral table for the position symbol. The null is different in each key, sixteen letters of the alphabet from A through P being used. Each of these keys is prescribed for use on two days of the month, except for that with E as a null, which is prescribed for only one day:

01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20
C	K	F	I	P	L	M	G	E	O	A	D	B	H	J	C	L	N	K	P

21	22	23	24	25	26	27	28	29	30	31
F	J	G	A	I	D	O	B	M	H	N

A message to or from Washington will thus begin in the key prescribed by this table for the day of transmission, but, as in KIA and KII, and perhaps also in other systems, the key may change at any point to another and as often as wished, one message having been found with eight different keys. To indicate such changes there are provided sixteen switch groups of which there are eight on one page of the book and eight more on another. If the book is really the red code, these were probably added in eight spaces previously blank. The reason for putting the sixteen on two different pages may be in part the difficulty of finding a sequence of sixteen blank lines and in part the desire to cut down the frequencies of the digraphs. In any case, the switch groups which designate the changes from the prevailing key, no matter what that happens to be at any point of change, to a key having either A, B, C, D, E, F, G, or H as null are on one page, and those designating changes to keys having I, J, K, L, M, N, O, or P as null, are on the other. These switch groups then, are nothing more than ordinary trigraphic groups having as their values "change to key of A," "change to key of B," etc. At an early stage in analysis it was thought there were actually 240 of them, i.e., one for a change from each of the sixteen keys to each of the fifteen others, but it was noticed that only about thirty (in a completely solved table there would be thirty-two) digraphs were used in composition of these 240 possible switch groups; i.e., in each prevailing key there were never more than two possibilities: in the key of A the possibilities were IS and BP. Therefore, IS and BP are merely the digraphic equivalents of the numerical designation of the two pages on which the switch groups have been placed. These digraphic equivalents for the switch group pages have been almost completely solved, as follows:

no. of key:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
null used:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
first page:	IS	SC	EK	OG	KG	CC	RP	NR	FP	KI	SW	MO	KX	BH	LS	
second page:	BP	CI	HH	AY	YL	QP	BY		WC	VI	CH	GE	KX	IA	ZU	ZI

Two values have not yet been recovered, and in the case of key no. 13 an error, perhaps the result of a garble, has been made, since KX cannot stand for two pages. An examination of traffic subsequent to 1 May 1944, which has not yet been studied, would doubtless complete the solution and assign KX to the proper page.

The third letter of the trigraph comprising one of these switch groups represents merely the encipherment of the line on which that group is placed. It is therefore possible to construct a table in which the position values of "change to key of A" in each of the sixteen keys are written on a horizontal line, and the same for all of the other indicators, thus:

null	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
number of key	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16
change to A	--	V				O	Y			E				G		
B	Q	--	Q	V				I						P		
C	I	O	--		V		J		U	B	Y	B			Y	
D		P	M	--				R		T				B	P	
E	J	W		F	--		M				F				I	
F	D	L	O	P	M	--			V	S					F	
G	S				R		--		J							
H			F			I		--			C		H		H	
I	P								--							
J	T						V		Z	--						
K		U	X			Q	T		Q	A	--			H	Z	A
L							A		C		X	--	X	Y		
M	U			W		E	O			V	J		--	M		
N			W		C						B			--		I
O	L									Z		P	F	F	--	X
P	X	I	V		Z	P	D		X		L	I	N		T	--

This table has then been recovered in ninety-three of the 240 possibilities, but could probably be pushed much further, were there time to examine all traffic of the last five months. (Presumably, a group really exists for all the possibilities, but it can be identified only through other methods of reconstruction since no instance of, say, "change from key of A to key of A" will occur.)

Actually, these letters are the position encipherment of at least eight and possibly sixteen different lines of the typical page of this book. No letter has so far appeared twice in the same column; so it is possible that the switch groups are

on eight lines of one page and a different eight on the other. This is likely, unless the position encipherment of one page differs from that of another. Such a phenomenon has not previously been noted in any Vatican system and in only one Italian diplomatic code (RA-1). If these really are the encipherment of sixteen separate lines, then the position encipherment of the system has been solved to about 25 percent of the total of 400 letters (25 lines x 16 keys). But what lines are they? By studying traffic one might be able to tell.

Thus far, only Washington traffic has been described. The evidence for other circuits is far from being as complete but shows that, while these circuits use keys with the same general features, the nulls used are not the same set; at least some nulls so far recovered are different and in some instances appear to be taken from later portions of the alphabet. Therefore, it is highly probable that the inventors of this system of encipherment have prepared not sixteen but twenty-five different tables of encipherment, each based on a different letter of the alphabet as a null, and that each station was furnished a set of sixteen of these tables, a different set for each station, with a table prescribing the days on which each table is to be used by that station for the beginning of a message.

Information as to the existence of spelling tables is lacking. The null can apparently be doubled and then repeated after an interval of some letters, and in this way a few spelling groups have been isolated, far to few for even an attempt at solution. Another phenomenon, not yet explained appears. Trigraphs may occur in which the null is doubled as the second and third letter; i.e., assuming that the null in a given sequence is G, then the group HGG may appear. This sort of thing was very disturbing when it was first noticed, but it occurs, if not frequently, at least often enough not to be explained as a garble. It may be an alternative device for indicating a spelling table, but if so, solution is yet to be reached. It was thought possible that a group of the type HGG might possibly mean "from this point on the letters form a spelling cipher until another H is reached," but this idea proved impossible since the very next letter in the instance examined was H.

24. <u>Cryptanalysis.</u> The solution of this system, so far as it has progressed, has been carried on exclusively in SSA, since GC&CS has been concentrating on KIA, KII, and KIB during the past year. The traffic was first recognized as homogeneous from the system indicators. Messages were found which had system indicators not conforming to the pattern of any previously known system; i.e., messages having A, Q, R, S, T, U, and V as their first letters. These were tentatively labeled "unknown system no. 1," "unknown system no. 2," etc., a total of seven unknowns being logged separately. Later experience showed that those messages which began with A were in no way related to those beginning with the other six letters, and, indeed, they are now logged separately

as KIH, but unknown systems nos. 2-7 later proved to be homogeneous and are now called KIF.

The point of attack was to determine if possible whether the system was trigraphic or tetragraphic and what the null or nulls were. It was never necessary to test for tetragraphic, because the system was soon found to be trigraphic. The method was to assume, arbitrarily, that each letter of the alphabet was the null and to see whether, on such an assumption, the message would break nicely into trigraphs.[41] The result was that it appeared that the messages were trigraphic, but that the nulls differed from message to message, i.e., multiple keys of some kind, but this satisfactory result was true only of sequences of various length at the beginnings of messages. At some point or other, sooner or later, the message would run out of phase. The analysts did not allow this fact to discourage them but examined every message carefully, assuming that in some unknown way the null might change within the messages. It was thus soon possible to say that a given message began with a certain null, changed to another on or about a definite point, and at a later point or points, changed to still others. Messages were then grouped according to the first null used and it was discovered that all messages beginning with any null were all sent on one or two days of the month. (Experience with KIB suggested separation of the traffic by circuits.) It was a short step to the conclusion that only sixteen nulls were used, and that each, excepting one only, was used on two days of the month. This produced the table of prescribed nulls for the Washington circuit, and some days for those of other circuits in the other traffic studied.

At the same time the points of change were examined and the trigraphs in the vicinity closely studied. It was found that frequently there were repetitions of digraphs between messages using the same null, and finally that the third letter would be repeated if the new null was the same as that in other messages. Thus, the table of switch groups was partially reconstructed. At last, the pattern of two different digraphs for each of the sixteen keys was noticed and the significance of the third letter also. Analysis was assisted by the fact that frequently, though not quite always, the code clerk after using the switch group would immediately insert the new null as a sort of confirmation of the third letter of the trigraph. This would be particularly useful in case the third letter was garbled in transmission.

At the present time there remain to be recovered only three digraphs (for the two switch group pages). When current traffic is studied, the following is the procedure. The table of prescribed nulls is examined and the message is broken up into trigraphs and the null stricken out, but with a sharp lookout for a digraph indicating change of key. If one of these is found, it is carefully marked and the same procedure followed until another switch group appears. At times, however,

[41] Not all of the 26 possibilities had to be tested in any one message.

messages will go out of phase, and it is hoped that such cases will be found when the prevailing null is H, M, or P, since only then can the table of switch groups be completely solved. When a message in these keys goes out of phase, examination must be extremely careful. The point at which the null is first out of phase is carefully noted, and it is assumed that a switch group not yet identified has been used since the last occurrence of the null. Then, each trigraph is carefully marked off in succession and the next letter examined. If that letter is one of the sixteen prescribed nulls for Washington, then it is assumed that the preceding group means "change key to" that letter, and the following sequence is examined to see whether, if that letter is the null, the message will break up into trigraphs. If so, there is a strong probability that the assumption is correct. The task then is to test each successive trigraph in this way until the right one is identified. If one is identified, it is possible to add both a new digraph and a new position letter to the tables. Additional position letters are, of course, more often recovered than digraphs, since there are many more yet to be recovered. The presence of garbles at any point will, of course, almost certainly prevent solution, but enough good texts will solve the tables entirely.

This system is, in spite of the fact that 395 messages are now available, certainly as secure as KIB,[42] perhaps even more so, since the traffic is homogeneous only in one circuit, and then available messages must be divided, not only whole messages but parts of them as well, into sixteen different keys, before indexing can be satisfactory. This means that there will be relatively little traffic in any one key.

When only 175 messages were available in the Washington circuit, it was thought barely possible that sufficient material was available for an IBM study. It was recognized that 175 messages were far too few to permit the solution of an entirely new book, but it was hoped that it might be possible to remove the encipherment because of the possession of a fairly complete solution of the underlying book, particularly since the position encipherment of the sixteen lines was partially solved. These hopes, however, were in vain; the index showed too flat a distribution, and no point of entry was found. The work was then abandoned until such time as sufficient traffic is available.

[42] KIB has 31 position keys but probably, though not certainly, fewer than sixteen page keys. Moreover, there is much more traffic available.

V

UNSOLVED SYSTEM WITH UNKNOWN NAME (KIG)

25. Cryptography. This system, of which the name and many other important features are completely unknown, was used by nine stations in this hemisphere from September 1940 until December 1942. The period in which it was used is only roughly indicated by these dates, since the fact that many of the messages lack the year of interception (at times even the month also) renders deductions from the traffic very doubtful. A record in the files mentions two messages in 1943, but these are not now to be found, and it is very likely that they were later identified as belonging to some other system. As late as 17 May 1944 a badly garbled message in the Bogotá circuit was tentatively identified as KIG, but the text is so imperfect as to make the identification highly improbable. As the period in question is, roughly, prior to that in which KIC was used, it may be that KIG was replaced by KIC, though two KIC messages, dating from August 1942, antedate the abandonment of KIG. It is probable that KIG was distributed to all stations in the Western Hemisphere, the absence of Asuncion, Caracas, Havana, Montevideo, and Tegucigalpa being merely the result of a failure to intercept the few messages which were sent. (Coverage for this period is scanty.) A few messages have been logged as KIG in the Lisbon and Sydney circuits, but there is a good chance that these are not KIG since they appear not to conform to all the characteristics.

So far as is known, KIG uses the following system indicators: I, J, K, L, M, perhaps N, and perhaps also, but less probably, the letter O. In any case traffic with the letters I to L inclusive is certainly homogeneous. The letter M has the same superficial characteristics as the others, but may have some divergent features not yet understood.

The essential features of the encipherment are trigraphic substitution and two nulls which vary from circuit to circuit but are always the same within the traffic of any circuit. The two nulls have been identified in all the stations using I, J, K, and L as system indicators, but not those using M or N. They are as follows:

Bogotá	K and R
Port-au-Prince-Ciudad Trujillo	U and M
Quito	U and H
San José – Managua-Panama	F and Z

San Salvador	M and Q
Santiago	H and O
Washington	A and B

No information is available as to spelling tables, and nothing can be said about the composition of the page- and position-encipherment keys. The message numbers appear to be enciphered from the digraphic table also used with KIA, KIB, KIC, KIF, KIH, and KII, but only some of the messages will fit their series.[43] It is possible that there was an earlier form of the table now in use, but if so, there is too little traffic for solution. All trigraphs noticed so far are transmitted in the page-position order.

It is definitely possible that KIG is merely another encipherment of the yellow code (KIB) which also uses trigraphs and two nulls.

26. <u>Cryptanalysis.</u> Further attempts at solution of KIG are, of course, quite hopeless with the present available traffic, only 93 messages in all circuits, divided into at least seven different keys.

[43] Coverage for the period is so scanty that it is, of course, out of the question to correct garbled message-numbers, as is frequently possible in later periods.

VI

UNSOLVED SYSTEM, THE GREEN CODE (KIC)

27. **Cryptography.** This system, called KIC by American analysts and the "AE" system by GC&CS, is known to its users as "*il cifrario verde*" (the green code). This makes it certain that it is a different book from the red code (KIA, KII) and the yellow code (KIB).

It was used by six American stations (Asuncion, Bogotá, Port-au-Prince, Rio de Janeiro, Santiago, and Washington) and also by Vichy (in a single message 13 September 1943). The earliest dated message is 18 August 1942 and the last 15 September 1943, after which no KIC messages have been intercepted.[44] Two KIC messages antedate the abandonment of KIG (August 1942), and one message (15 September 1943) was sent a few days after the first KIH message (10 September 1943), but, roughly speaking, KIC replaced KIG and was in turn replaced (only at Washington) by KIH. Nothing is known about the encipherment beyond the bare fact that the group is tetragraphic, that the nulls are A and E, and that spelling groups are used in the same way as in the other systems.

28. **Cryptanalysis.** KIC was the first Vatican system identified in the SSA, this being one of the results of the exploratory examination conducted early in September 1943. As only 46 messages had been received when the system became obsolete, there is no question of further solution, unless the system should be revived.

[44] In September 1944, after this was written, a Berlin message was received in what appears to be KIC. This was still later confirmed by the appearance of KIC in Vichy and Washington traffic.

VII

UNSOLVED SYSTEM WITH UNKNOWN NAME (KIH)

29. Cryptography. Nothing is known of the name or basic book of this system which is used only by Washington circuit, the first message being sent on 10 September 1943. Only forty-seven messages have been received to date (September 1944).

Messages can be distinguished by the use of the letter A, without variation, for the system indicator. The encipherment is tetragraphic with J and X as nulls. Nothing more is known, but it is possible that KIH is a different encipherment of the green code (KIC) which also uses tetragraphic groups and two nulls. Moreover, KIC was apparently abandoned about the time KIH was introduced, the two systems overlapping by only five days (10-15 September 1943). KIH is, however, not based on the same book as KIG, the predecessor of KIC, since that is trigraphic, but it seems clear that the three systems, KIG, KIC, and KIH were used in successive periods for the same general purpose, undoubtedly for the most secret communications.

30. Cryptanalysis. KIH was first logged as "unknown no. 1" but was soon discovered not to be related to unknowns nos. 2-7 (KIF). Traffic is too light (47 messages) for any further analysis.

VIII

UNSOLVED SYSTEM WITH UNKNOWN NAME (KIE)

31. Cryptography. KIE is the designation for all traffic between Vatican City and Peking, and no traffic goes in the opposite direction, since the Apostolic Delegate in Peking is permitted to communicate in code only through his colleague in Tokyo. Only twenty-one messages are available, one from 1937, two from 1939, one from 1940, three from 1941, three from 1942, ten from 1943, and one from 1944. This is an average of only three messages a year, certainly very light traffic, but is probably a high percentage of coverage at that. On 20 February 1944 Tokyo reported to the Vatican Secretary of State that the Apostolic Delegate in Peking had received only six messages from the Vatican since 1 May 1943. The Assistant Secretary of State replied to Tokyo on 24 February 1944 that in the same period ten messages had been sent, nos. 37-46 inclusive. Which four were not delivered is not known, but all six actually received in Peking are available in SSA.

The system employs tetragrapbs and a single null which is G, but the traffic is too light for further analysis. Nothing is known of the message-numbers, but they seem to be taken from the code number pages.

IX

UNSOLVED DIGIT SYSTEM

32. KID. This is the designation for all Vatican digit messages. These are sent in groups of five digits, and nothing whatever is known about the nature of the system. Its use is confined to traffic to and from two stations, Bangalore in India and Hanoi-Hue in Indo-China, except for a single message to La Paz (31 May 1942) which commences in KIB and then changes to digits. This may be a relay to some representative of the Vatican, temporarily in La Paz, to whom the digit code had been given for special purposes.[45] The appearance of KID in Tokyo or Vichy traffic is always in connection with relays of messages to or from Hanoi-Hue (a single station, the representative merely sending messages from either city), and it is not believed that Tokyo or Vichy can read KID. The earliest available message is dated 22 December 1936, and the system is still in current use after nearly eight years, perhaps only because of the difficulty of transmitting new books to the stations using it.

[45] Or actually a relay in some non-Vatican system.

X

VATICAN COMMERCIAL TRAFFIC

33. **Commercial Traffic.** The Vatican Cryptographic Bureau has published no specifically commercial systems, but the Special Administration of the Holy See, the business branch of Vatican City which directs the investments of the Papacy and functions also as a purchasing agency for Vatican City, from time to time has made use of well known commercial systems, such as Peterson's, in communication with banking institutions in the United States. Under present Censorship regulations, such code communications may not be filed at either end except when special licenses have been issued and a decodement of the message is furnished at the same time. A number of such messages have been received in the SSA from time to time, and occasionally attempts have been made to identify the commercial systems used, but no study has been made of the traffic.

On rare occasions the Vatican has sent messages in an unknown system with a heading in KIA asking that the Apostolic Delegate to Washington relay the text of the rest of the message to some unknown addressee. An agreement was reached that such messages would in the future be headed with ZZZ, but no more have been seen in the intercepted traffic. Attempts to identify the unknown system through files at the Office of Censorship resulted in failure.

XI

TRAFFIC IDENTIFICATION AND LOGGING

34. Traffic Identification and Logging. When traffic is received in unindexed form it must be separated as to system and logged. The following points will prove helpful in carrying out the process.

a. If the message begins with AA, these letters should be disregarded. They are not system indicators but probably mean "urgent".

b. The first letter of the message, or the third if the message begins with AA, is the system indicator. If this letter is one of the following letters, or if the other features listed are present, the system can at once be identified without further trouble:

W, X, Y, Z,	KIA
F, G, H	KIB
Digit-groups	KID
Peking as addressee	KIE
Q, R, S, T, U, V	KIF
A (not AA)	KIH

If however, the message begins with B, C, D, or E, it may be KIA or KIB. It will be KIA if after the initial letter a trigraph occurs which will give a number in the KIA decode, and the text thereafter will break up into trigraphs with E as null. It will be KIB, however, if the next two letters give a number from the digraphic table for message numbers, and the text thereafter will break up into trigraphs with Y and Z as nulls. A little observation will quickly settle the point, since there is really no confusion, except that the logger must be careful not to confuse the digraph CP = 48 with CP, the digraph for a number page in both keys 1 and 2.

If the first letter is I, J, K, L, M, or N, it is more difficult to identify the system, but the message will more probably be in KII than in KIC or KIG, since these systems are now probably obsolete. If the system is KII, a further test can be made by noticing if the addressee is London and whether the text will break up into trigraphs with E as null. If so, the message is certainly KII, but if these tests are negative, then the message may be KIC or KIG. The way to test then is to see whether the text is tetragraphic with A and E as nulls. If so, then it is KIC. The remainder may be presumed to be KIG, but there is no positive test for KIG since

it is trigraphic with two nulls varying with the circuit, the nulls of some circuits being as yet unknown.

c. The presence of garbles, however, will continue to present difficulties in system identification. There are no good rules to apply except to use a little ingenuity. A watch must be kept for obvious garbles, e.g., if the message number turns out to be IB, it may be that I is a garble for E. Then test the resultant number against the series on the proper page. Furthermore, be sure that the system indicator is consistent with the position of the nulls in the message; i.e., if H is the indicator, do not expect the null to be E. If it is, decide whether the indicator is wrong or the null is really something else. Care must be taken with relays from Berne which frequently begin in one system and change to another. A little manipulation of the trigraphs will show when this has happened, and if not, decoding surely will.

d. Messages in which the preamble is missing will present problems which can be solved by remembering salient characteristics of Vatican traffic. If the residence of the addressee is missing, then the words Nunzio Apostolico in . . . . must not be identified as a station having instead a Delegato Apostolico. The signatures on messages to the Vatican will invariably identify the sending station, and rarely are both preamble and signature missing. The call signs will occasionally indicate the circuit, though not always.

e. When the system has been identified beyond doubt, then logging may be begun; and the following items should be entered:

(1) Date of transmission
(2) Source of intercept
(3) System
(4) Work-sheet number
(5) Indication of tenth group (optional)
(6) Time of intercept (optional)
(7) Signature (optional)

It will generally be found convenient to go through the entire body of new traffic deciphering all message numbers at once, after which traffic should be sorted first into messages from the Vatican and messages to the Vatican, and then into individual circuits. This will save time in turning the pages of the log. If the number does not coincide with that required by the date, consider the possibility that the number is garbled. It often is, but there will be occasions when the fault is that of the code clerk and nothing can be done except to indicate that the message is off the proper number.

f. After the message has been decoded, some short indication of the subject should be indicated, and if translated or summarized, the proper numbers should be entered, translation numbers in any case and bulletin numbers if there are any. XBT should be clearly entered if the message is translated by the British.

XII

OVERALL SURVEY OF VATICAN CODES
(Based on information available on 25 September 1944)

35. KIA, *il cifrario rosso*, British "E" code with keys 1 and 2

a. One-part trigraphic, with E as null; enciphered: 11,950-12,025 groups

b. Distribution: all stations except a few in Asia

c. Classification: restricted and confidential, occasionally secret

d. Encipherment:
- page symbol: digraphic tables without vowels
- position symbol: direct standard English alphabet without E and the reverse of this
- spelling: monoalphabetic substitution
- message number: digraphic table without A and with B, C, D, or E in first position
- system indicators: W, X, Y, Z, or B, C, D, E

e. Solution:
- page encipherment: better than 90 percent
- position encipherment: 100 percent
- spelling tables: 100 percent
- vocabulary: approximately 57 percent

f. Readability: approximately 99 percent

g. Traffic: earliest 1936, current since then. Over 6,700 messages available

36. KIB, *il cifrario giallo*, British "YZ"

a. One-part trigraphic, with Y and Z as nulls; enciphered by multiple keys; probably about 15,625 groups

b. Distribution: most important stations

c. Classification: secret

d. Encipherment:

page symbol:	digraphic tables without Y and Z
position symbol:	random mixed alphabets without Y and Z
spelling:	polyalphabetic based on random mixed alphabets
message number:	same as KIA
system indicators:	B, C, D, E

e. Solution:

page encipherment:	unsolved, analysis suspended since 1 May 1944
position encipherment:	
spelling tables:	
vocabulary:	

f. Readability: none

g. Traffic: earliest 1942, current since then. Available to date 1188 messages.

37. KIC, *il cifrario verde*, British "AE"

a. One-part tetragraphic with A and E as nulls; enciphered; no information as to number of keys or size of book

b. Distribution: Most American stations, Berlin and Vichy

c. Classification: secret (?)

d. Encipherment: no information except system indicators I, J, K, L, M, (N?)

e. Solution: unsolved

f. Readability: none

g. Traffic: 1942-1943, a few messages in September 1944. Only 47 messages to date.

38. KID:

a. Uses digits; no other information available

b. Distribution: Hanoi-Hue and Bangalore

c. Solution: not studied

d. Traffic: a few since 1936, only 46 messages available

39. KIE:

a. Tetragraphic with G as null; no other information available

b. Distribution: Peking only

c. Traffic: since 1937, only 22 messages available

40. KIF:

a. One-part, trigraphic with 16 keys each using a different null, size probably between 12,025 and 15,625 groups. May be same book as KIB.

b. Distribution: Berlin, Berne, Lisbon, Madrid, Washington, Vichy

c. Classification: probably secret

d. Encipherment:

page symbol:	digraphic with 16 tables
position symbol:	random mixed alphabet
spelling:	uncertain
system indicators:	Q, R, S, T, U, V

e. Solution: switch groups solved about 25 percent, otherwise unsolved

f. Readability: none

g. Traffic: 1942 to date, only 420 messages available

41. **KIG:**

a. Trigraphic with two nulls which vary with circuit. No information as to encipherment or size , except system indicators are same as KIC: I, J, K, L, M, (N?)

b. Distribution: most stations in Western Hemisphere

c. Solution: not studied

d. Readability: none

e. Traffic: 1941-1942, only 93 messages available

42. **KIH:**

a. No information available, except that distribution is confined to Washington and system indicator is A, without variants

b. Traffic: since September 1943, only 46 messages available

43. **KII, *il cifrario rosso*, British "E" system, keys 3 and 4:**

a. Same code as KIA

b. Distribution: London only

c. Classification: secret

d. Encipherment:

page symbol:	digraphic in two keys
position symbol:	same as KIA
spelling:	monoalphabetic substitution
system indicators:	I, J, K, L, M

e. Solution:

page symbols:	80 and 60 percent
position symbols:	100 percent
spelling:	about 80 percent

f. Readability: about 90 percent

g. Traffic: 7 intercepts, 60 messages received from GC&CS

XIII
AN APPRAISAL OF VATICAN CRYPTOGRAPHY

Four decades ago studies in the early history of cryptography made by the German scholar, Aloys Meister,[46] showed that as early as the fourteenth century the Holy See was using cryptographic communications with the papal legates, and that by the end of the fifteenth century the Roman curia employed the services of highly skilled cryptographers. Though Meister prints in his list of the secretaries for cipher one who took office as recently as 1796, the bulk of his attention is confined, of course, to the earlier period. Following Meister's work, there is no available information concerning Vatican cryptography until we come to the *cifrario rosso*[47] (KIA-KII), introduced probably about a decade ago. The British, who so frequently in the case of other governments have been able to furnish historical material from a period antedating the experience of this office, did not begin to study the *cifrario rosso* until the summer of 1942, and the present staff working on the problem in GC&CS has no information concerning earlier attempts as solution of Vatican traffic in modern times.

The Annuario Ponteficio for 1943 lists Monsignor Giovanni Battista Montini as the third in rank of the officials of the Vatican Secretariat of the State, preceded only by the Cardinal Secretary, a post now vacant, and by the *Segretario per gli affari estraordinari*, at present Monsignor Domenico Tardini. While the late Secretary, Cardinal Luigi Maglione, was still living, Monsignor Montini signed about a third of the messages sent from Vatican City, but these rarely ever proved to be more than routine business; since the cardinal's death, Monsignor Montini has been signing a larger proportion, the remainder being signed by Monsignor Tardini who previously never signed any. Monsignor Montini's title "*Sostituto per gli affari ordinari e Segretario della Cifra*" (Substitute for ordinary business and code secretary). Messages to the Vatican intended for Monsignor Montini will at times be marked, in code, as for *Monsignor il Sostituto*. This term has in Italian doubtless less unpleasant connotations than the literal translation would have in English. A visitor to Rome in the years immediately before the outbreak of the present war was informed that Monsignor Montini was the Vatican's expert in cryptography; so apparently this prelate is not an ecclesiastic nominally at the head of the cryptographic bureau but actually one of its experts. If so, he is a cryptographer of no mean ability. The Vatican probably lacks adequate facilities for radio interception and doubtless depends more on the

---

[46] Aloys Meister, *Die Geheimschrift im Dienste der päpstlichen Kurie von ihren Anfängen bis zum Ende des XVI.* Jahrhunderts ("Quellen und Forschungen aus dem Gebiete der Geschichte," vol. XI; Paderborn, 1906). Meister's earlier work: *Die Anfänge der modernen diplomatischen Geheimschrift* (Paderborn, 1902), is devoted chiefly to the cryptography practiced by the northern Italian cities.

[47] See paragraphs 13-16.

acumen of its observers in all the capitals of the world, possessed, as they are, of an unparalleled position in the diplomatic corps, for the intelligence reports which help to make the papal secretaries so well informed on world affairs. We may be reasonably certain that there is no cryptanalytic section at Vatican City.

At the outset of work on the solution of Vatican systems in the SSA, the analysts who were assigned to the task had rather little respect for the security of these systems. This reflected the fact that they approached the problem *in medias res*, at a point when the British had already solved KIA and made considerable progress on KII.[48] Moreover, the code underlying these two encipherments was not such as to inspire much respect for the ability of its compilers.[49] It was a very small one-part code with only two keys for the position symbol, one a direct standard alphabet minus the null, the other merely a reversed sequence of the same letters. The code being small was very poor in vocabulary, a defect greatly heightened by employing many highly needed groups for the specialized phraseology of the Church. For example, all surnames had to be excluded,[50] variants were few, and phrases, of course, still fewer. The size of the code was doubtless dictated by the used of a trigraphic code group which permits a maximum of only 17,576 groups, if all letters are used, but here there are further limitations. One letter was used only as a null and no vowel was admitted to the page digraphs. Consequently, the code cannot be larger than 12,025 groups. The encipherment employed, though based on random mixed substitution, had only two keys in one encipherment (KIA) and two in the other (KII), and these two keys were used on alternate days. The encipherment of proper names, likewise quite elementary, being monoalphabetic substitution, and while two of the four keys used random mixed alphabets for the cipher components, the other two used, respectively, a reversed standard alphabet and an alphabet in which the vowels were placed after the consonants, both in alphabetical order. All of these facts caused the analysts to believe that the solution of other Vatican systems would not prove difficult.

Subsequent experience with KIB[51] and KIF[52], the only other systems on which attempts at solution have been made, proved the contrary to be true. The difficulties encountered showed that considerable intelligence was matched against the analysts. These difficulties are as follows:

---

[48] See paragraphs 3 and 16.

[49] See paragraphs 13-15.

[50] The surname of the present pope is naturally omitted, since at the time the code was compiled Pius XII was only Cardinal Pacelli, and the surnames of even the cardinals are omitted. Moreover, it is not possible to encode the Latin name of the present pope, even though two popes reigning in this century before him had the same name. "Pio" of course appears among the common first names, but "Pius" must be spelled out. On the other hand, messages normally do not need to use the name, since the pope is regularly referred to as His Holiness or the Holy Father. Whether the code includes the surname of the preceding pope, Achille Ratti, we have no way of knowing, for only a very few messages are available from his reign (1922-1939).

[51] See paragraphs 17-20.

[52] See paragraphs 21-24.

a. **Lack of traffic.** Sufficient traffic in a homogeneous system or key is, of course, the *sine qua non* of all successful cryptanalysis, but, though coverage of the radio traffic extremely high, the number of messages sent in any system other than KIA (used for less secret communications) is relatively low. A number of factors make this so. Pouch communication within the Vatican diplomatic service is still possible and is widely used, not only by means of the Vatican's own couriers but those of friendly nations; codes used are sufficiently numerous for the traffic; and both the secretariat and the dependent legates have kept the traffic to an absolute minimum. For example, KIB is the most widely used of the more secret codes. It has been regularly intercepted in the thirty-five months since Pearl Harbor, but the total number of messages from all stations is a few more than 1200, an average of only slightly more than one message a day. KIF has been in use for a shorter period, but the average per day is even less, only a few more than 400 messages being available from all stations. Only one of the other less used systems has produced more than fifty messages: KIG in which there are only 93, and this system is to all intents and purposes obsolete. In this respect then, Vatican policy is far different from that of the Italians who failed to provide enough systems for the heavy traffic sent and sent so many messages that adequate traffic was inevitable in almost all systems and keys.

b. **Accuracy of operations.** The Vatican code clerks show much more care in the preparation of messages than do those in the employ of the Italian government. Where errors appear in the messages they are usually those of transmission rather than of cryptography. Moreover, the central office never commits such a blunder as the establishment of a new system through a message in an older system. Code instructions are apparently sent from Vatican City only in pouches, since they have never appeared in the traffic. (The few code-instruction messages intercepted all originate with the envoys and are limited to the establishment of addenda to the vocabulary.) Cribs between plain text and code messages are almost nonexistent, only one such message have been intercepted. This was a plain-text message to the Archbishop of Mexico City, prescribing ecclesiastical regulations for Easter week in 1944. The text was exactly the same as that of a KIA circular which had been sent previously to various South American stations. Unfortunately, the code text was completely readable, and the plain text was of no help. Cribs between different systems are only slightly more frequent. If more of these are hidden in unsolved systems, at least their existence has not yet been suspected. This high standard of accuracy is probably to be explained by the use of ordained priests, men of high education, as code clerks.

c. **Multiple keys.** This is probably the greatest obstacle in the way of the cryptanalysis of the unsolved Vatican systems. With the *cifrario rosso* only four keys are used, but in KIF there are sixteen for each station and each station

gets a different set. In KIB the number of position keys is probably thirty-one; the number of page keys is unknown but certainly large. If, as is the case, there are no unenciphered key indicators, and the traffic externally looks homogeneous,[53] as it does, the multiple key is a very strong feature.

d. External characteristics. Certain other features tend to preserve security. One of these is the use of variants for system indicators,[54] and the use of nearly all, if not all, of the letters of the alphabet in these discriminants. The message number, moreover, is always enciphered,[55] and except for trigraphic code numbers used only by one station,[56] the cipher equivalents for these numbers use every letter but A. The running together of the trigraphic code groups into telegraphic pentagraphs also tends to conceal the trigraphic pattern, and in general, there seems to have been a definite attempt to prepare different systems so that the external characteristics of several will be the same. The universal transmission of the signature in clear prevents its use as an entering wedge.

In conclusion, it may be said that the general policy was to use a relatively simple system for communications of a routine nature, reserving the better systems for the more secret messages. This policy must, of course, be followed by most governments, but in this case there seems to be a greater divergence between the simple and the complex systems, both as to form and volume of traffic.

---

[53] The use of letters for all but one system (KID) tends to heighten the effect of similarity.
[54] See pp. 15, 29, 39, 42, 45, 57.
[55] See p. 8.
[56] See pp. 8, 15.

C-1 Manual for the Solution of Military Ciphers, *Hitt*
C-2 Cryptanalysis of the Simple Substitution Cipher with Word Divisions, *Barker*
C-3 Elements of Cryptanalysis, *Friedman*
C-4 Statistical Methods in Cryptanalysis, *Kullback*
C-5 Cryptography and Cryptanalysis Articles, Vol. 1, *Friedman*
C-6 Cryptography and Cryptanalysis Articles, Vol. 2, *Friedman*
C-7 Elementary Military Cryptography, *Friedman*
C-8 Advanced Military Cryptography, *Friedman*
C-11 Solving German Codes In WWI, *Friedman*
C-12 History of the Use of Codes, *Friedman*
C-13 The Zimmermann Telegram of Jan. 16, 1917 and its Cryptographic Background
C-14 Manual of Cryptography, *Sacco*
C-16 The Origin and Development of the Army Security Agency, 1917-1947
C-17 Cryptanalysis of the Hagelin Cryptograph, *Barker*
C-18 The Contribution of the Cryptograph Bureaus in the WW, *Gylden*
C-19 Course in Cryptography, *Givierge*
C-20 History of Codes and Ciphers in the U.S. Prior to WWI, *ed. Barker*
C-21 History of Codes and Ciphers in the U.S. During WWI, *ed. Barker*
C-22 History of Codes and Ciphers in the U.S. Between the World Wars, Part 1, 1919-1929, *ed. Barker*
C-23 Riverside Puhlications, Volume 1, *Friedman*
C-24 Riverside Publications, Volume 2, *Friedman*
C-25 Riverside Publications, Vulume 3, *Friedman*
C-26 Cryptanalysis of an Enciphered Code Problem, *Barker*
C-27 The Voynich Manuscript-An Elegant Enigma, *D'Imperio*
C-28 Manual of Cryptography, *British War Office*
C-30 Military Cryptanalysis, Part I, *Friedman*
C-33 Course in Cryptanalysis, Volume 1, *British War Office*
C-34 Course in Cryptanalysis, Volume 2, *British War Office*
C-35 The Origin and Development of the National Security Agency, *Brownell*
C-36 Treatise on Cryptography, *Lange and Soudart*
C-37 Solving Cipher Secrets, *Ohaver*
C-38 Cryptography, A Study on Secret Writings, *Langie*
C-39 Cryptanalysis of Shift-Register Generated Stream Cipher Systems, *Barker*
C-40 Military Cryptanalysis, Part II, *Friedman*
C-41 Elementary Course in Probability for the Cryptanalyst, *Gleason*
C-42 Military Cryptanalytics, Part I, Volume 1, *Friedman & Callamahos*
C-43 Military Cryptanalytics, Part I, Volume 2, *Friedman & Callimahos*
C-44 Military Cryptanalytics, Part II, Volume 1, *Callimahos & Friedman*
C-45 Military Cryptanalytics, Part II, Volume 2, *Callimahos & Friedman*
C-46 Pattern Words- Three Letters to Eight Letters in Length, *Carlisle*
C-48 Pattern Words-Nine Letters in Length, *Carlisle*
C-49 The Index of Coincidence and Its Applications in Cryptanalysis, *Friedman*
C-50 Cryptographic Significance of the Knapsack Problem, *O'Connor & Seberry*
C-52 The American Black Chamber, *Yardley*
C-53 Traffic Analysis and the Zendian Problem, *Callimahos*
C-54 History of Codes and Ciphers in the US Between the World Wars, Part II. 1930-1939, *ed. Barker*
C-55 Introduction to the Analysis of the Data Encryption Standard (DES), *Barker*
C-56 Elementary Cryptography and Cryptanalysis, *Millikin*
C-57 Secret Ciphers of the 1876 Presidential Election, *Glover*
C-58 Solving Cipher Problems, *Lewis*
C-59 Cryptanalysis of the Singular Columnar Transposition Cipher, *Barker*
C-60 Military Cryptanalysis, Part III, *Friedman*
C-61 Military Cryptanalysis, Part IV, *Friedman*
C-62 Pattern Words-Ten Letters and Eleven Letters in Length, *Wallace*
C-63 Pattern Words-Twelve Letters in Length, *Wallace*
C-64 US Naval Cryptographic Activities in the Philippines Prior to WWII, *Carlisle*
C-65 US Naval Communications Intelligence Activities, *Safford & Wenger*
C-66 Fundamentals of Traffic Analysis (Radio-Telegraph) *Dept. of the Army*
C-67 Six Lectures Concerning Cryptography and Cryptanalysis, *Friedman*
C-68 The DES-An Extensive Documentation and Evaluation, *Simovits*
C-69 Cryptanalysis of the Double Transposition Cipher, *Barker*
C-70 Achievements of the Signal Security Agency in World War II, *Dept. of the Army*
C-71 An Historical Bibliography of Cryptology to 1945, *Galland*
C-72 Secret and Urgent, The Story of Codes and Ciphers, *Pratt*
C-73 Cryptanalysis of the Single Rotor Cipher Machine, *Dawson*
C-74 Classical Cryptography Course, Volume 1, *Nichols*
C-75 Venona, Soviet Espionage and the American Response, *Benson & Warner*
C-76 Classical Cryptography Course, Volume 2, *Nichols*
C-77 Descriptive Dictionary of Cryptologic Terms
C-78 Cryptology, System Identification and Key-Clustering, *Kumar*
C-79 Basic Cryptanalysis, Field Manual 34-40-2, *Dept. of the Army*
C-80 US Army Signals Intelligence in WWII, *Gilbert & Finnegan*
C-81 The Story of Magic, Memoirs of an American Cryptologic Pioneer, *Rowlett*
C-82 Briefing Notes Concerning Analysis of German Air-Force Low-Level Communications During WWII
C-83 NSA Cryptologic Documents, *National Archives*
C-84 General Solution for the Double Transposition Cipher, *Kullback*
C-85 Russian Cryptology During World War II, *Dettmann, Fenner, Flicke, Friederichsohn, Paschke*

ISBN:0-89412-280-0
90000
9 780894 122804
KATER-BOUND
KATER-CRAFTS INCORPORATED
PICO RIVERA, CA 90660-2199