Encl # 1 of item # 3 prepared by Capt Rackem about July, 1944

I. Problem presented

What is the security of enciphered internal references: signatures, addresses, and message numbers?

II. Facts bearing on the case

1. References: signatures and addresses are buried in the message text and enciphered in the same system as the text proper.

2. It is possible to predict the internal references on the basis of external characteristics of the traffic:

   a. Signatures and addresses can be predicted from the stations of origin and destination.

   b. Message numbers can be predicted from the file date/time

3. Methods of isolating references from the text proper tend to become stereotyped.

III. Discussion

See inclosure

IV. Conclusions

Present method of enciphering references is cryptographically insecure.

V. Recommendations

1. The rules of economy should be emphasized to all persons responsible for inserting references in messages.

2. Abbreviations should be used wherever feasible.

3. A special address and signature code directory should be prepared and used in conjunction with the same system used to encipher the text proper.

~~SECRET~~

## SECURITY OF ENCIPHERED INTERNAL REFERENCES IN CRYPTOGRAPHED MESSAGES

The word references is used in this study to include those items which are not an integral part of the informational contents of messages, but which are added for routing and identifying purposes. References may be external to the message text or internal. They may be enciphered or in the clear. Under present U. S. Army procedures, enciphered internal references consist of addresses, signatures, and message numbers.[1]

Unenciphered external references consist of part indication, system indication, call signs, transmission instructions, group count, and file date-time.

---

[1] In the appendix to this study are sample references of actual traffic from the Southwest Pacific Area, the North African Area, European Area, the U. S. Navy, and the British. A consideration of several of them will serve to describe the ramifications involved in the terms addresses, signatures, and message numbers. The following message illustrates a basic type of reference:

PAREN CHARLIE TWO TWO FIVE SEVEN ZERO FROM GHQ SWPA SGD MACARTHUR TO CHIEF OF STAFF WAR DEPARTMENT PAREN

It may be analyzed as follows:

Message number: CHARLIE TWO TWO FIVE SEVEN ZERO (C-22570)
Originating office: GHQ SWPA
Signature of sending authority: SGD MACARTHUR
Address: TO CHIEF OF STAFF WAR DEPARTMENT

The basic type may be amplified in many ways. The address may be augmented to include the chain of command, to include relay instructions, etc. This is illustrated in the following reference:

PAREN CG HQ THIRD SVC COMD ASF BALTIMORE ATT DIR SEC AND INTELL DIV PASS TO CO PHILADELPHIA ORDNANCE DISTRICT PHILADELPHIA PENN FROM TERRY MSG NR FOUR ZERO SIX PAREN

Certain references are essential for routing and identifying purposes. They are enciphered because they reflect the battle order and organization of the U. S. Army. A complete knowledge of references would actually be a picture of the U. S. Army as expressed in its signal communication system. References are also enciphered because a clear version would provide enemy traffic analysts and cryptanalysts with clues for interpreting and solving our traffic.

However, there are certain dangers inherent in the very fact of encipherment. It will be the purpose of this paper to specifically analyze those dangers, and to propose certain changes which will alleviate those dangers.

It is recognized that the problem under consideration is inextricably tied up with the concatenation of security of all communications procedures; and that the security of any specific procedure is dependent in a greater or

---

1 (cont'd)
Analysis of this reference is:

Address:
Immediate recipient: CG HQ THIRD SVC COMD ASF BALTIMORE
Ultimate recipient: ATT DIR SEC AND INTELL DIV
Relay instructions: PASS TO CO PHILADELPHIA ORDNANCE DISTRICT PHILADELPHIA PENN

The signature may also be augmented to include the name of the originating officer and the chain of command as in the following reference:

PAREN FROM DOOLITTLE TO ARNOLD FROM SPAATZ (EASY EIGHT TWO TWO SEVEN EIGHT) SIGNED EISENHOWER REFERENCE WARX THREE ZERO THREE SEVEN FIVE MAY FIRST PAREN

It should be noted that the set of references is contained within PAREN .... PAREN. Functioning as an adjunct to the signature is the symbol for a branch or department. An example:

PAREN CITE SPSIE INGLES CSIGO PAREN

Finally, references may contain the distribution of a message:

PASS TO CO RECEPTION STATION FORT GEORGE MEADE MARYLAND PD ALSO BOOKED TO CHIEF OF TRANSPORTATION WASH D C CMA CG ASF WASH D C CG NRSC EDMONTON ALTA PAREN

lesser degree on the security of every other procedure. Thus, changes in procedures involving call signs, frequencies, encipherment of system indicators, etc., would very greatly affect the analysis of enciphered references. Notwithstanding, there are certain modifications which can be adapted to the enciphered references which will eliminate some of the disadvantages inherent in the present procedure.

## PART I

### Present Procedure

The present practice in regard to internal references is to bury them somewhere in the message text and encipher them in the same system which is used to encipher the message text itself.

The cryptanalytic vulnerability of such practice is well known. The same references - due to the nature of communication - are used again and again, and constitute a stereotype.[2] As such, they provide enemy cryptanalysts with probable words for attacking our systems. However, it is not only necessary for the enemy cryptanalysts to know what probable words to try, but also in what messages to try them; for probable words cannot be tried in every message. The great volume of traffic must be delimited. The vulnerability of enciphered references is not that they exist, not that certain words are probable; but that it is possible to discover which message contains a particular reference or set of references. And this is the crux of the present study. All analysis which follows is based on that thesis.

Specifically, the security disadvantages of enciphered references under the present procedure result from two sources:

(1) Reductions that can be made from a correlation of certain external features of the transmitted form of the message to the enciphered references.

---

[2] What is commonly referred to as stereotype beginnings and endings are infinitesimal in importance when compared to the stereotype of references. Although common beginnings and endings may be composed of a frequent digraph, a word, or at most a short phrase, enciphered references may constitute a paragraph.

(2) Deductions that can be made from the correlation of knowledge of references of a solved system with the references of an unsolved system.[3]

What are the correlations that can be made between external features of the transmitted form of the message and enciphered references?

They are:

I. Correlation between station of origin and internal signatures.

II. Correlation between station of destination and internal addresses.

III. Correlation between file date/time and internal message numbers.

---

[3] Only the security of the first source will be considered in this paper. The second involves the equating of references of one system with references of another system on the basis of external characteristics of the messages in question. The relationship of external characteristics to each other will be dealt with in another study. The second source brings up the idea of differentiation in reference procedures based on the security of systems; that is, if the same procedures are used with SIGABA as with SIGCUM, M209, M138A, and WD Tel Code, an ability to read messages in M138A or in WD Tel Code would provide clues for reading the higher grade systems...if it could be determined which messages used the same references. Consider the following two references. The first was sent in a SIGCUM message of April 12; the second in a SIGABA message of April 23. If the first message was read, and it could be suspected by external characteristics that a similar set of references were in the second message, then the first could be used as a crib for the second.

April 21 (from WD Seattle Wash to CO 3rd SVC Cmd Baltimore) SIGCUM

PAREN RELAY BY ACS SEATTLE FROM TYLER COMMANDING FAIRBANKS ALS REF SEVEN FIVE THREE SEVEN NINETY PD BALTIMORE PASS TO CO RECEPTION STATION FORT GEORGE MEADE MARYLAND PD ALSO BOOKED TO CHIEF OF TRANSPORTATION WASH D C CMA CG ASF WASH D C CMA CG NWSC EDMONTON ALTA PAREN

April 23 (from WD to CG Third SVC Cmd Baltimore Maryland) SIGABA

PD FROM TYLER COMMANDING REF SEVEN FIVE SEVEN SIX NINETY EPT NINETY PD PAREN THIRD SVC COMD PASS TO CO RECEPTION STATION FORT GEORGE MEADE MARYLAND MSG ORIGINATED FAIRBANKS ALS FOR CHIEF OF TRANSPORTATION WASHINGTON D C CMA CG ASF WASH D C CMA CO NwSX EDMONTON CMA COMMANDING OFFICER RECEPTION STATION FORT GEORGE MEADE MARYLAND AND COMMANDING GENERAL THIRD SERVICE COMMAND BALTIMORE MARYLAND PAREN

The combination of these correlations form a composite of information that can be used as a cryptanalytic wedge. There is also an additional amount of information provided by the deductions based on I, II, and III. This will be considered as:

IV. Collateral information provided by I, II, and III.

a. the length of the references in a single message

b. the position of references in the message

c. methods of isolating references from the text proper

I. Correlation between station of origin and internal signatures.

Internal signatures may consist of the name of the originating officer or office, the names of the officers in the chain of command and the names of the sending authority.[4]

The station of origin at present can be determined from the use of fixed clear call signs, which are allocated in a definite relationship to the area in which the station is located.[4a]

It is necessary to know whether the call sign of the sending station is the call sign of the originating station; for the message may be intercepted on the second leg of a relay. However, transmitting instructions which occur in clear provide a check on this point.

The signature of the sending authority is the commanding officer of the area. His name is common knowledge and usually appears in every message from a given station. Out of 30 (almost consecutive) messages examined from SWPA 28 carried the signature MACARTHUR; 16 were SGD MACARTHUR, 4 were SIGNED

[4]Straight British procedure does not use officers' names as signatures. They are omitted altogether.

[4a]This is in great contrast to the German use of call signs which change daily irrespective of frequency change. In U. S. Navy, call signs of forces afloat are normally enciphered; call signs of shore activities are usually not enciphered.

MACARTHUR, nad 8 were FROM MACARTHUR. Out of 32 messages examined from the North African Area, 16 were SIGNED WILSON; and 14 were SIGNED DEVERS.[5] Out of 37 messages examined from the European area, all 37 contained EISENHOWER.

It is also possible to make a correlation between the station of origin and the originating officer and chain of command, but not from call signs alone. The correlation must be worked out in conjunction with system used, classification, kind of traffic, length of message, file date/time, etc. However, all these items are available on intercept. The degree of difficulty in making this kind of correlation depends on a knowledge of battle order and traffic analysis.

Few signatures other than MACARTHUR appear in the 30 messages examined from SWPA; however, there were 20 uses of GHQ SWPA as the originating office and 1 instance of CG USAFFE.

The names of various originating officers - SAWBRIDGE...SWITZER...KAUCH ...,MOUNTFORD... - appear in the messages from North Africa in conjunction with the signature WILSON or DEVERS. There were no repetitions. On the other hand, the branch or department symbols in the North African messages can be plotted and correlated with the signature of the sending authority. DEVERS uses symbols that begin NA---; WILSON uses symbols that begin FH---. Thus there are 7 instances of CITE NAAGE, 4 instances of CITE NAGAP, etc. in the DEVERS messages. There are 3 instances of CITE FHMGS, 2 instances of FHENG, etc., in the WILSON messages.[6]

---

[5]Cipher traffic on this series was not available so study could not be made of correlation between external characteristics of the messages in an effort to predict precisely which signature was in a given message.

[6]DEVER'S symbol NA--- undoubtedly comes from North Africa. WILSON'S FH--- may be the FH of AFHQ. The last three letters of the symbol are a trigraph probably representing the branch of the service. Thus FHENG is probably Engineers; FHSIG is probably Signal Corps.

From the European area there is a definite use of originating officers and chain of command. This is shown very clearly in the Appendix. In addition to EISENHOWER, which appears in all 37 messages, we find 15 occurrences of FROM LEE; 6 occurrences of FROM SPAATZ; 4 occurrences of FROM COBB; 2 occurrences of FROM ROSS, as well as several other single occurrences.

II. Correlation between station of destination and internal addresses.

Addresses consist of the name of the ultimate recipient, the chain of command, the immediate recipient, relay instructions, and the distribution of the message. No all of these items are contained in any one message.

As in the previous correlation, the facts are:

(1) Clear call signs and clear transmitting instructions delineate the station of destination.[7]

(2) The location of the station of destination is determined by the geographical assignment of call signs.

(3) A knowledge of battle order furnishes internal addresses and the correlation between the station of destination and internal addresses is made.

Messages in the Appendix have been examined for stereotyped addressees. In the case of each message, the ultimate destination is WAR. In the 30 messages examined coming into WAR from SWPA, the following are some of the internal addresses noted:

---

[7]In the following typical relay message, the call signs of the first leg show:

A2D V BF6 T-KFR

A2D is the station called, and in this case is the relay station with instructions to transmit the message to KFR. BF6 is the station of origin. When A2D transmits the message to KFR, the call signs show:

KFR V A2D A-BF6

indicating that it is a relay message and that the originator is BF6

~~SECRET~~

TO AGWAR - 12

TO AGWAR WASHINGTON - 4

TO AGWAR INFO ATC WASHINGTON - 3

TO CHIEF OF STAFF WAR DEPARTMENT - 7

TO CHIEF OF STAFF WASHINGTON D C - 1

TO CHIEF SIGNAL OFFICER WASHINGTON D C FOR GENERAL INGLES - 1

FOR MARSHALL -2

It can be seen that TO AGWAR occurs 19 times, (or in more than 50% of the messages) sometimes by itself and sometimes enhanced. Out of the 32 messages coming into WAR from North African Area, AGWAR occurs 25 times as an address or as part of an address. Messages from the European Area do not exhibit any general stereotype in address. Perhaps if the cipher traffic were available it would be possible to make some specific correlation. For example: TO ARNOLD occurs 4 times. If it were possible to distinguish air traffic, a definite correlation might be found between type of traffic and the address, TO ARNOLD.

The cryptanalytic vulnerability of the correlation between station of destination and addresses is vitally shown in the Japanese Army systems which use an externally enciphered address (ATE) and a separate code book to disguise the destination (TIYA). The clear destination must first be determined. Battle order and knowledge of past traffic provides probable addresses. Solution is based on a correlation between the Ate and the Tiya.

In some Jap traffic also, the distribution of the message is enciphered internally, using the same system as the text itself. This constitutes one of the most important cryptanalytic wedges.

The relay message presents certain differences of its own. A relay occurs when there is no direct communication channel between the station of origin and station of destination. The message must then be routed through an intermediary station that has a direct channel with both. The relay message permits not only the correlation of station of destination with internal addressee, but also permits a correlation between the relay station and relay instructions enciphered internally in the message. It is on relay traffic, moreover, that cross-system duplicates may be used; for the ultimate recipient may not have the same system as the originating office. This may impose the responsibility of paraphrasing on the relay station.

III. Correlation between file date/time and internal message numbers.

The file date/time group is placed in the clear in the preamble of the message.[6] The originating center must file messages logically in order to find them again; the recipient must have a simple and convenient manner of referring to any particular message. Hence, message numbers are assigned in serial order. It is because of this seriality that a direct correlation is possible between the file date/time and internal message numbers; it is not a disadvantage due to the file date/time in the clear, for the transmittal date/time or the cryptographic date would be practically as valid in making the same correlation.

---

[6] See Appendix II.

It is possible to assign message numbers in some manner other than serial order, but not too feasible. Serial numbers as such are not used by the U. S. Navy. Instead, the date/time group of a message functions as its message number.[9]

The very fact that there is a definite order to internal message numbers provides a cryptanalytic attack. The daily average amount of traffic from a given center can be ascertained, and the approximate message number can be predicted. If any message from the originating center has been read, its number can be used as a point of departure for calculation. If no message has been read, it is assumed that numbering begins over again on or about January 1 of each year.

Let us consider the references of 4 actual messages selected at random, and attempt to correlate the file date with internal number. We shall leave the file time out of our consideration.

April 18
PAREN MARX TWO FOUR FOUR NINE NINE SPTOR SEVEN SIX NAUGHT FROM SOMERVELL THIRD SVC COMD PASS BALTIMORE SUB POE FOR ACTION FWHERE PAREN 24499

April 21
PAREN MARX TWO FIVE NINE FOUR THREE FROM DUNLOP ACTING THE ADJUTANT GENERAL SPSTP RPT SPSTP PAREN 25943

April 22
PAREN MARX TWO SIX FOUR TWO TWO SPTOR RPT SPTOR EIGHT FIVE SIX FROM SOMERVELL THIRD SERVICE COMMAND PASS TO BALTIMORE POE RPT POE PAREN 26422

April 23
PAREN MARX TWO SIX NINE SEVEN ZERO PAREN 26970

Suppose we had at our disposal only the two messages of April 18 and April 21. To get the daily average, we take the difference between 25943 and

[9] Communications Instructions, U. S. Navy, 1944, CNC Par. 2038. This procedure necessitates false time on 2nd, 3rd, 4th ——— parts of a message; for part indication is enciphered.

24499 and divide by 3. The result is 481. This daily average now becomes a yardstick with which to predict other message numbers. To approximate the numbers on April 22, add about 500 to 26422. Had we added 481 - the daily average as determined between the messages of April 18 and 21, we would have been only 2 off, for the difference between 26422 and 25943 is 479!!! This is phenomenal. So precise a prediction is generally impossible from large centers. In large centers, a prediction will be satisfied with a variance of 100, forgetting about the units and tens position entirely.

If we take the daily average between April 18 and April 23, the figure will be slightly higher, but still within the locus of 100 variation.

Now, suppose we have no solved messages at all at our disposal. In that case we must assume messages start numbering over again on or about January 1. We would then take traffic of that period to work on. If we are successful, we can then use the resulting message numbers as a control in later predictions.

If we have no traffic or if we are unable to work on traffic of the January 1 period, we must get traffic analysts to give us traffic volumes from January 1 to the period under consideration. This will give an idea of the approximate message number.

Let us consider another kind of correlation. Suppose we have a single solved message at our disposal, what can be done? Using the message of April 23 with the internal number 26970, we divide 26970 by the number of days between January 1 and April 23 — 114. This result — 236 — is now a daily average based on January 1. Traffic volume and flow, however, fluctuates a great deal, and so this figure must be adjusted by traffic analysts. It then can be used for cryptanalytic purposes.

By taking file time as well as file date into consideration, a rather precise prediction can be made. The number interval between messages bearing short file time differences will be very small. This means no change in the hundreds or tens position of the message number; only a change in the units position.

The daily average traffic volume must be analyzed for each center. This has been done for all Jap Army traffic, where about 2500 series have now been established. Below is a specimen chart showing how Jap message numbers are plotted.[10] After the plotting reaches a certain level, daily averages are estimated.

IV. Collateral information provided by I, II, and III

The length of enciphered references sometimes becomes quite sizable. Under ordinary conditions, it averages over 60 letters; and in not too unusual conditions may exceed 300.[11] Needless to say, the longer the set of references, the great security disadvantage, for there is more stereotype material available. In some messages, the references may constitute as much as 1/3 of the text.

This longevity is not peculiar to U. S. traffic. In Jap Army over 10% is taken up by internal enciphered references in addition to the external enciphered routing, addresses and signature.

It is possible also to localize the position of the references in a message. Practice has determined that enciphered references should not be

[10] See Appendix III

[11] See message of April 23, from MVD to CG Third Svc Cmd., page 5, this report.

buried in the beginning or at the end of messages. The result has been to use the second fourth. Conventionally the Japs bury references in the last third of a message, while Germans prefer the opening. Using type X machine, it has estimated that British references nearly always have started about the 90th character. This has been partly due to form used in writing messages.

One of the cancerous additions to the references has been the method used to separate the references from the text proper, so as to eliminate confusion as to what is message text and what is reference material. This has been done by enclosing references in PAREN. The use of PAREN for this purpose has become such common practice that it is not exaggerating to say that it is used in over 90% of all messages. The use of PAREN in pairs to segregate references provides a 10 letter crib, the isolation of which in any text will determine the position and length of the set of references. [12]

The use of PAREN is similar to the Jap use of TEXT ENDS and TEXT BEGINS. Once isolated, TE and TB determine the position and length of the references in the Jap message. The first attack and the most successful is to discover the location of these two parenthetical devices. The second step is to go after the references themselves. In some conditions, the isolation of TE and TB is so destructive that solution follows in a matter of minutes. That the Japs realize the vulnerability of such practice is fairly certain, for gradually the use of TE and TB has dimished almost to the point of disappearance from certain centers. Nothing has replaced it, proving that it was unnecessary.

---

[12] In Navy messages, X represents every mark of punctuation. For clarity, however, punctuation marks can be spelled out. Communications Instructions, U. S. Navy, 1944. DNC 5, Par. 2034.

The security disadvantages of enciphered references have now been enumerated. The attempt has been made to show how the disadvantages could be used from a cryptanalytic point of view. Several comparisons with enemy systems were made in order to demonstrate practically how we (at the present time) are taking advantage of deficiencies in enemy systems; deficiencies which also occur in our own systems. We must assume that if we can do it to them, they can do it to us.

Specifically, it has been pointed out that references enciphered by the same system as the text itself are dangerous and jeopardize the text because there is a direct correlation between external characteristics of the message and the internal enciphered references, which constitute a stereotype that can be localized in the traffic and used as a crib.

The next step is to consider what can be done.

## PART II

### What Can Be Done

In considering what can be done, we must rephrase the question in the light of preceding examination to read: What can be done to block the correlation between external characteristics and enciphered references? This question could be attacked from either or both of two perspectives. We could make a conscious effort to disguise the external characteristics (AS THE GERMANS DO); or we can propose means of disguising the references. There is no reason why both can't be done simultaneously. In this paper, however, the problem will be approached solely from the viewpoint of the references.

Whenever an analysis is true, there is a certain universality about it which makes it valid irrespective of the modification of conditions which originally gave rise to it. The security - or lack of security - of enciphered references has long been recognized. Various solutions have also been proposed as a remedy.

Following is a quotation by Mr. W. F. Friedman. It was written in connection with material used for educational purposes, and some of the phrases in it refer to a particular situation; nevertheless, it is given in its entirety.

> "The danger to cryptographic security resulting from the inclusion of cryptographed addresses and signatures in cryptographic messages becomes quite obvious in the light of solution by the probable-word method. To illustrate, reference is made to the message employed in Pars. 19-22. It will be noted in Par. 22b that the message carried a signature (Treer, Col.) and that the latter was enciphered. Suppose that this were an authorized practice, and that every message could be assumed to conclude with a cryptographed signature. The signature

"TRLER COL" would at once afford a very good basis for the quick solution of subsequent messages emanating from the same headquarters as did the first message, because presumably this same signature would appear in other messages. It is for this reason that addresses and signatures must not be cryptographed; if they must be included they should be cryptographed in a totally different system or by a wholly different method, perhaps by means of a special address and signature code. It would be best, however, to omit all addresses and signatures, and to let the call signs of the headquarters concerned also convey these parts of the message, leaving the delivery to the addressee a matter for local action."

W. F. Friedman
1938 Page 43 Par 25a
Military Cryptanalysis
Part II

It will be noted that Mr. Friedman has considered 3 possibilities:

(1) "addresses and signatures must not be cryptographed"

(2) "if they must be included they should be cryptographed in a totally different system or by a wholly different method"

(3) "perhaps by means of a special address and signature code"

Here is a universal analysis perfectly applicable to the problem of enciphered references. There is however, one more question which must be added to those raised by Mr. Friedman, and that is the practicability of putting into effect either one or more of the 3 possibilities.

Let us digress for a moment at this point to examine some of the methods that are now being used by the enemy and by us in an attempt to solve the problem of enciphering references.

The Japanese go to one extreme in the use of external encoded and enciphered routings, addresses, and signatures, by providing a separate code book for each of these, and a separate additive for enciphering the last two. This is in addition to another code book and additive used on the

text. However, even with these precautions, there is a certain portion of the references that must be buried in the text itself. The buried portion consists of the originating office, the message number and part, and the distribution of the message; and these are encoded and enciphered by the same system as the text itself. It is this latter material which provides entry into the Jap traffic.

Practically every Jap message contains some kind of routing instructions and external enciphered address. On the contrary, very few Jap messages have external enciphered signatures.

With frequent change of code and additive books in the present Jap methods, it is far from easy to solve the external enciphered addresses and signatures.

Solution of internal references in Jap messages are comparatively easier.

The Germans use internal enciphered references, in a rather modified fashion. They leave out whatever is not absolutely necessary, depending on call signs which change daily to furnish addresses. They also at times use internal cover name or code names to disguise addresses and signatures. This is not a frequent practice. The most important wedge into German diplomatic traffic is the enciphered internal references which usually occur in the opening of the message.

The U. S. Navy has attempted to limit the length of the stereotype provided by enciphered internal references by issuing a book of address and signature abbreviations.[13]

At CBI, a kind of code directory has been put into effect for lateral use (BICPAC-2). The directory uses 5 letter groups called "internal

[13] What do British, Finns, Russians, Swedes, French do?

address indicators" or "designators" to replace addresses and signatures. It is unfortunately not constructed from a 2 letter differential permutation chart, so that there is a possibility of difficulty with garbles. The assignment of values in the directory is based on the official designation of a unit, since - as stated in BICPARS - geographical locations and personnel change, but the official designation of a unit seldom changes. BICPARS contends that the internal address indicators are accurate, offer cryptographic security, and reduce the time of message preparation and transmission. Following are 2 examples:

(1) PAREN CRFLA CAB (msg serial no.) FROM CABAH PAREN

(Signal Officer Army Air Forces No. _____ from Commanding General AAF, CBI)

(2) ACTION CRAGG CFB_____ INFO CTAAC AND CASAE FROM CFBDS

(Action C.G. Hqs USAF-CBI Branch Hqs, USAF-CBI #_____
info C.G. ICWATC, Station No. 1, Calcutta and
commanding general ASC from C.G. Branch Hqs, USAF-CBI)

BICPARS contains a systematic assignment of values in which the first 3 elements of the code group constitute a trigraph designating the main headquarters or unit and the last two elements are a digraph designation of a sub unit. This may be desirable within the local theater. It is questionable whether this would be desirable for world wide communication.

In the light of the analysis of Part I and the methods now being used, what suggestions can be proposed to modify the present procedure in U. S. Army? .... keeping in mind that whatever is suggested must involve techniques that are not alien to U. S. cryptographic procedure and so will not entail too much training of personnel. It must cut down

the length of references as much as possible. It must be a system which will differ in some way from that used on the text proper. It must not hinder the preparation and transmission of messages.

That the general rules of economy make for cryptographic security is axiomatic. Thus, it is imperative to omit entirely what is not absolutely necessary. If the name EISENHOWER occurs in every single message coming into WAR from the European Area, it is superfluous, for it can be taken for granted. Likewise with GHQ SWPA and TO AGWAR from the Southwest Pacific. If chain ofcommand routings are the normal ones, they also can be taken for granted. The intent of enciphered relay instructions may be implicit in the external transmitting instructions.

Abbreviations should be used wherever possible. They are not only economical but also very disconcerting to a cryptanalyst as anyone who has worked on the German police cipher can testify.

However, in addition to rules for economy, it is felt essential that some additional steps be taken to disguise the internal references.

It is hereby proposed that a special address and signature code directory be prepared and used in conjunction with the same system used to encipher the text proper.

(1) Directory should contain 5 element groups based on a 21 letter differential chart.

(2) Consist of individual groups for high echelon units.

(3) Contain groups for 1000 numbers which can be used in various combinations with each other for encoding internal message numbers.

(4) Contain individual groups for most frequent routings.

(5) Would be distributed by cryptonet holder. Each holder would get a section of the master code directory - that portion pertaining

to his usual channels of communication. Certain centers would hold several sections.

(6) Directory would be changed at irregular intervals.

(7) Use of special address and signature code directory is not mandatory. If no code group exists for a particular unit or routing, or if the code directory is not available, the practice now in use can be followed. Partial coding, also, is permissible.

It will be seen that these suggestions are but expansions on Mr. Friedman's idea that a special address and signature code be used.

The practicability of a special address and signature code directory is evidenced by MICARS which is now in use for lateral communication within CBI. Reports indicate that it is feasible. If a directory can be used in lower echelons, it can be used in higher echelons. A directory of abbreviations now in use by the U. S. Navy demonstrates practicability of an extra book. A special telephone directory has long been conventional in the U. S. Army. So the idea of an address and signature book is quite in line with U. S. procedure.

Would the use of a special signature and address directory hinder the preparation and transmission of messages?

On the contrary although extra time would be involved in the encoding and decoding process, the time of enciphering and transmitting messages would be cut down since entire routings would frequently be condensed into a single 5 letter group.

Is the use of a special address and signature directory cryptographically more secure than the present practice?

This question will be considered in the light of ability to make deductions from a correlation of external features of the transmitted form of the message to the enciphered code references.

(1) Plain text word assumptions would be utterly invalid.

(2) It is very likely that stereotype internal signatures and addresses in the form of code groups will continue to exist; but it would be impossible to make correlations between external characteristics and the code groups unless many messages are solved and the directory reconstructed or the directory captured and compromised. The former is not easy despite the fact that directory groups will be built on a two letter differential basis; the latter is not too probable for high echelon centers. Also, succeeding editions of the directory are contemplated.

The use of a single code group for an entire routing will make references shorter and provide less cipher text on which to work, besides offering the handicap of a code.

As for internal numbers: — They will be represented by code groups. However, an additional change in procedure is advocated; that number series start over again at irregular periods and not run consecutively for an entire year. This will obstruct the ability to use any number groups that may have been solved by enemy cryptanalysts.

It may or may not be necessary to use some method of isolating the code references from the text proper. If necessary it is suggested that the use of PAREN be discontinued. The use of X as a universal punctuation sign used by the Navy is an alternative; or perhaps it may be advisable to use 2 letter separators in which case XX, YY or ZZ could be used in any combination; as: XQZ —— YI, XY —— QZZ, YQZ —— ZX, etc.

## SAMPLES OF REFERENCES TO SERIAL NUMBER, ADDRESSEES, AND SIGNATURES, CRYPTOGRAMMED WITHIN MESSAGES.

These samples are taken from actual traffic. Only the specific numbering series have been changed so as not to give numbers of actual messages; the order and form is authentic. Positions of these insertions are fairly well varied, though there is a tendency to place them toward the beginning of the message.

~~SECRET~~ FROM SOUTHWEST PACIFIC AREA

PAREN CHARLIE TWO TWO FIVE SEVEN ZERO FROM GHQ SWPA SGD MACARTHUR TO CHIEF OF STAFF WAR DEPARTMENT PAREN

PAREN TO CHIEF OF STAFF WAR DEPARTMENT FROM MACARTHUR CHARLIE TWO TWO FIVE SEVEN ONE /beginning of msg/ FROM GHQ SWPA SGD MACARTHUR CHARLIE XRAY TWO TWO FIVE SEVEN TWO TO AGWAR INFO ATC WASHINGTON

PAREN CHARLIE TWO TWO FIVE SEVEN SIX FROM GHQ SWPA SGD MACARTHUR TO AGWAR PAREN

QQQQQ FROM GHQ SWPA SGD MACARTHUR TO AGWAR INFO TO ATC WASHINGTON CHARLIE XRAY TWO TWO FIVE SEVEN EIGHT PD

PAREN CHARLIE TWO TWO FIVE SEVEN NINE FOR INGLIS FROM AKIN PAREN PAREN REURAD WILLIAM FOUR SIX ONE FOUR ONE THREE SEVENTH MAY CITE OPSOT PAREN

PAREN FOR OBOE PETER DOG PAREN PAREN TO AGWAR FROM MACARTHUR CHARLIE TWO TWO FIVE EIGHT ZERO PAREN

PAREN FOR OBOE PETER DOG PAREN CHARLIE TWO TWO FIVE EIGHT ONE FROM GHQ SWPA SGD MACARTHUR TO AGWAR PD

PAREN FROM GHQ SWPA SIGNED MACARTHUR TO AGWAR CHARLIE TWO TWO FIVE EIGHT THREE PAREN

PAREN FROM MACARTHUR GHQ SWPA CHARLIE XRAY TWO TWO FIVE NINE ZERO TO AGWAR INFO ATC WASHINGTON YOUR WILLIAM FOUR FOUR FIVE SEVEN ONE PAREN

PAREN CHARLIE TWO TWO FIVE NINE ONE FROM MACARTHUR GHQ SWPA TO CHIEF OF STAFF WAR DEPARTMENT PAREN

/beginning of msg/ FROM GHQ SWPA SGD MACARTHUR CHARLIE TWO TWO FIVE NINE FOUR TO AGWAR REFERENCE YOUR WILLIAM XRAY THREE THREE SIX SIX FOUR APRIL SIXTEENTH AND WILLIAM FOUR FIVE ZERO SEVEN EIGHT MAY ELEVENTH PD

PAREN BOOK MESSAGE AGWAR CG MECAL CG AMMISCA CG AMMDEL CG SOUPAC CG CENTPAC MILITARY ATTACHE LONDON FROM GHQ SWPA SGD MACARTHUR CHARLIE XRAY TWO TWO FIVE NINE SEVEN PAREN

PAREN TOPSEC FROM GHQ SWPA SIGNED MACARTHUR TO CHIEF OF STAFF WAR DEPARTMENT FOR MARSHALL EYES ONLY CHARLIE TWO TWO FIVE NINE NINE PAREN

PAREN CHARLIE TWO TWO SIX ONE EIGHT FROM GHQ SWPA TO CHIEF OF STAFF WAR DEPARTMENT PAREN OPERATIONS REPORT SOWESPAC AREA PERIOD 1400z/15 TO 1400z/16 SIGNED MACARTHUR PD

FROM GHQ SWPA SGD MACARTHUR TO CHIEF OF STAFF WAR DEPARTMENT PERSONAL FOR MARSHALL CHARLIE TWO TWO SIX TWO ZERO PAREN

PAREN CHARLIE TWO TWO SIX TWO THREE FROM MACARTHUR GHQ SWPA TO CHIEF OF STAFF WASHINGTON DC PAREN

PAREN CHARLIE XRAY TWO TWO SIX TWO SEVEN CMA FROM GHQ SWPA SGD MACARTHUR TO AGWAR FOR ACTION TO COMGENSOPAC COMGENCENPAC FOR INFORMATION PAREN

REURAD PAW ZERO FOUR TWO FIVE DATED ONE FIVE MAY ONE NINE FOUR FOUR PAREN FROM GHQ SWPA SGD MACARTHUR TO COMGEN USAFICPA FOR RYAN ACTION AGWAR INFO CHARLIE XRAY TWO TWO SIX THREE SIX PAREN

PAREN FROM GHQ SWPA CHARLIE TWO TWO SIX THREE EIGHT TO CHIEF SIGNAL OFFICER WASHINGTON D C FOR GENERAL INGLES FROM GENERAL AKIN PAREN

~~SECRET~~

FROM SOUTHWEST PACIFIC AREA

PAREN FROM GHQ SWPA SIGNED MACARTHUR TO AGWAR CHARLIE TWO TWO SIX THREE NINE PD DILLER TO SURLES PD SEE YOUR FOUR SEVEN FOUR THREE THREE SEVENTEENTH PAREN
PAREN FROM GHQ SWPA SGD MACARTHUR TO AGWAR WASHINGTON CHARLIE TWO TWO SIX FOUR THREE REURAD WILLIAM TWO NINE SEVEN THREE FIVE DATED TWO NINE APRIL PAREN
PAREN FROM GHQ SWPA SGD MACARTHUR TO AGWAR WASHINGTON CHARLIE TWO TWO SIX FOUR FOUR ATTENTION REQUISITION AND RECORDS SECTION CLASSIFICATION AND REPLACEMENT BRANCH PAREN
PAREN FROM GHQ SWPA SGD MACARTHUR TO AGWAR WASHINGTON CHARLIE TWO TWO SIX FOUR FIVE PAREN
PAREN FM CG USAFFE SGD MACARTHUR TO AGWAR UNCLE THREE THREE ONE FIVE ONE PAREN
PAREN FROM GENERAL ARNOLD TO CHIEF SIGNAL OFFICER WASHINGTON PASS TO SIGNAL CORPS LIAISON OFFICER RADIO RESEARCH LABORATORY HARVARD UNIVERSITY CHARLIE TWO TWO SIX FIVE TWO PAREN
PAREN FROM MACARTHUR GHQ SWPA CHARLIE TWO TWO SIX FIVE THREE TO AGWAR PAREN
PAREN FROM GHQ SWPA SGD MACARTHUR CHARLIE TWO TWO SIX FIVE FOUR TO AGWAR WASHINGTON (DILLER TO SURLES) SEE YOUR THREE SEVEN FOUR THREE THREE DASH ONE SEVEN PAREN
PAREN FROM GHQ SWPA TO CHIEF OF STAFF WAR DEPARTMENT (CHARLIE TWO TWO SIX FIVE SEVEN) OPERATIONS REPORT SOWESPAC AREA PERIOD 1400z/16 TO 1400z/17 SGD MACARTHUR PAREN
PAREN CHARLIE TWO TWO SIX EIGHT FIVE FROM MACARTHUR GHQ SWPA TO AGWAR PAREN
PAREN CHARLIE XRAY TWO TWO SIX EIGHT EIGHT FROM MACARTHUR GHQ SWPA TO COMMANDING GENERAL ARMY SERVICE FORCES ACTION TO COMMANDER OF NAVAL OPERATIONS INFORMATION PAREN REURAD WILLIAM XRAY THREE SIX NINE ZERO THREE OF TWO THREE APRIL SIXTEEN FOUR ZERO NINE DOG BAKER PD

FROM NORTH AFRICAN AREA

PAREN FOX SEVEN FOUR ZERO NINE EIGHT SIGNED DEVERS CITE NAGAP PAREN
PAREN FOX SEVEN FOUR ZERO NINE NINE SIGNED DEVERS CITE NAAGE TO AGWAR PAREN
PAREN FOX SEVEN FOUR ONE ZERO THREE SIGNED DEVERS CITE NAAGE TO AGWAR PAREN
PAREN FOX SEVEN FOUR ONE ZERO FIVE SIGNED DEVERS CITE NAAGE TO AGWAR PAREN
PAREN FOX SEVEN FOUR ONE ZERO SIX SIGNED DEVERS CITE NAAGE TO AGWAR PAREN
PAREN FOX SEVEN FOUR ONE THREE TWO SIGNED WILSON CITE FHENG TO AGWAR FOR ENGINEER FOR LOPER PAREN
PAREN FOX SEVEN FOUR ONE THREE THREE SIGNED WILSON CITE FHENG TO AGWAR FOR ENGINEER FOR ARMY MAP SERVICE PAREN
PAREN SIGNED DEVERS CITE NAGAP FOX SEVEN FOUR ONE THREE NINE PAREN
PAREN FOX SEVEN FOUR ONE FOUR ZERO SIGNED DEVERS CITE NAAGE TO AGWAR FOR CIPION AND PWB PRISONER OF WAR INFORMATION REURAD PAREN
PAREN FOX SEVEN FOUR ONE FOUR ONE SIGNED DEVERS CITE NAAGE TO AGWAR PAREN
PAREN FOX SEVEN FOUR ONE FOUR THREE SIGNED DEVERS CITE NAAGE TO AGWAR PAREN
PAREN FOX SEVEN FOUR ONE FIVE ONE TO AGWAR FOR CCS FOR CCAC REPEAT USFOR SIGNED WILSON CITE FOR BRITISH CHIEFS OF STAFF FHMOS

~~SECRET~~

FROM NORTH AFRICAN AREA

PAREN FOX SEVEN FOUR ONE FIVE FIVE SIGNED DEVERS CITE NAGAP
PAREN AAI FOR CSC TROOPERS FOR SIGS SEVEN A AGWAR CITE SPSOL NAAF FOR AIR SIGNAL OFFICER IN CHIEF MID EAST FOR SIGS FROM AFHQ CITE FESIG FOX SEVEN FOUR ONE SIX FOUR ONE SEVEN MAY
PAREN FOX SEVEN FOUR ONE EIGHT ZERO PWB TO OWI SIGNED WILSON CITE FHPWO ALWAE ONE SEVEN NINE THREE ZERO PAREN
PAREN FOX SEVEN FOUR ONE NINE FOUR TO AGWAR FOR SURLEE SIGNED WILSON CITE FHINC PAREN
PAREN SIGNED DEVERS CITE NATPN TO AGWAR FOR ACTION TO CG SOS NATOUSA AND CO MBS INFORMATION FOX SEVEN FOUR TWO ZERO FIVE PAREN
PAREN FOX SEVEN FOUR TWO TWO FOUR TO AGWAR FOR CCS FOR CCAC RPTD ETOUSA FOR BCS SIGNED WILSON CITE FHMGS PAREN
PAREN FOX SEVEN FOUR ONE FIVE ZERO TO AGWAR FOR CCS AND CCAC RPTD USFOR FOR BCS SIGNED WILSON CITE FHMGS PD THIS IS LOVE ABLE CHARLIE FOUR ZERO TWO PAREN
REFERENCE OUR F.46725 OF 16 MAY (.) FOX SEVEN FOUR TWO ZERO SEVEN TO AGWAR FOR CCS, USFOR FOR BRITISHCHIEFS OF STAFF, UNITY LONDON, FAIRBANKS, FROM FREEDOM,
PAREN CITE NAAGP FOX SEVEN FOUR TWO TWO FIVE SIGNED DEVERS TO AGWAR INFORMATION OG CBI PAREN
X SIGNED WILSON CITE FHORB FOX SEVEN FOUR TWO SEVEN TWO. AFHQ FOR ACTION MILSTAF WASHINGTON FROM MOUNTFORD FOR HARDY X
X (FOX SEVEN FOUR TWO EIGHT SIX) ACTION AGWAR WAR SHIPPING ADMINISTRATION FOR GADDESS SIGNED WILSON CITE KALLOCH NAVS 323 X
NAVS 324 REFERENCE WSNA 767 X(FOX SEVEN FOUR TWO EIGHT SEVEN) ACTION AGWAR FOR GADDESS WAR SHIPPING ADMINISTRATION WASHINGTON SIGNED WILSON CITE KALLOCH
X (FOX SEVEN FOUR TWO EIGHT EIGHT) ACTION AGWAR FOR GILLESPIE AMERICAN EXPORT LINES 25 BROADWAY NEW YORK SIGNED WILSON CITE KALLOCH X
X (FOX SEVEN FOUR TWO EIGHT NINE) ACTION AGWAR FOR GILLESPIE AMERICAN EXPORT LINES 25 BROADWAY NEW YORK SIGNED WILSON CITE KALLOCH X
X (FOX SEVEN FOUR TWO NINE ONE) ACTION AGWAR WAR SHIPPING ADMINISTRATION FOR CONWAY SIGNED WILSON CITE KALLOCH NAVS 322 X
X (FOX SEVEN FOUR THREE TWO SIX) TO AGWAR CITE NAAGO SIGNED DEVERS X
X (FOX SEVEN FOUR THREE THREE TWO) ACTION AGWAR PASS TO ANPB FOR LIEUTENANT COLONEL MORGAN CITE FHPET SIGNED WILSON X
PAREN TO AGWAR TO GEORGE FOR IRELAND PASS TO SURLEE FROM HAUCH SIGNED WILSON FOX SEVEN FOUR THREE THREE SEVEN PAREN
PAREN FOX SEVEN FOUR THREE THREE EIGHT FROM SWITZER FOR BISSELL SIGNED WILSON PAREN
PAREN (FOX SEVEN FOUR THREE FOUR NINE) FROM SAVERIDGE SIGNED DEVERS CITE NAGAP TO AGWAR PERSONAL FOR WHITE PAREN

FROM EUROPEAN AREA

PD FOR SPPES REURAL WAR TWO EIGHT FOUR SEVEN NINE FROM COBRA SOSFD SIGNED EISENHOWER EASY EIGHT TWO TWO FIVE ONE PD

~~SECRET~~

PAREN FOR SPFER FROM COBBS SOSFD S GNRD EISENHOWER EASY EIGHT TWO TWO FIVE ZERO PAREN
PAREN FOR SOMERVELL FROM LEE SIGNED EISENHOWER EASY EIGHT TWO TWO FIVE TWO PAREN
PAREN FROM LEE SIGNED EISENHOWER EASY EIGHT TWO TWO FIVE SEVEN PAREN
PD TO KERR FROM LEE SIGNED EISENHOWER EASY EIGHT TWO TWO SIX ZERO PD
PAREN TO KERR FROM LEE SIGNED EISENHOWER EASY EIGHT TWO TWO SIX ZERO PAREN
PAREN FOR SPSRB FOR CG AAF FOR HANSHAW FOR TEAGUE FOR HALLEY FROM POTTER FROM LEE SIGNED EISENHOWER EASY EIGHT TWO TWO SIX ONE PAREN
PAREN SIGNED EISENHOWER EASY EIGHT TWO TWO SEVEN ZERO PAREN
PD FOR SPXPR SIGNED EISENHOWER EASY EIGHT TWO TWO SEVEN ONE PD
PD FOR SPPAM FROM COBBS SOSPD SIGNED EISENHOWER EASY EIGHT TWO SEVEN THREE PD
PD EASY EIGHT TWO TWO SEVEN FOUR FROM LEE SIGNED EISENHOWER PD
PD TO ARNOLD FROM SPAATZ EASY EIGHT TWO TWO SEVEN FIVE SIGNED EISENHOWER PD
PAREN FROM DOOLITTLE TO ARNOLD FROM SPAATZ (EASY EIGHT TWO TWO SEVEN EIGHT) SIGNED EISENHOWER REFERENCE WARX THREE ZERO THREE SEVEN FIVE MAY FIRST PAREN
PAREN FOR SPPAM FROM COBBS SIGNED EISENHOWER EASY EIGHT TWO TWO SEVEN NINE SOSPD PAREN
PAREN SIGNED EISENHOWER EASY EIGHT TWO TWO EIGHT ONE PAREN
PAREN FOR SOMERVELL FOR GREGORY FROM LEE SIGNED EISENHOWER EASY XRAY TWO EIGHT TWO EIGHT THREE PAREN
PAREN SIGNED EISENHOWER EASY EIGHT TWO TWO EIGHT FIVE PAREN
PAREN CITE SOSOD FROM LEE REFERENCE NUMBER EASY EXRAY TWO EIGHT TWO EIGHT SIGNED EISENHOWER REFERENCE YOUR WILLIAM ABLE ROGER THREE SEVEN FOUR NINE FIVE PAREN
PAREN SIGNED EISENHOWER EASY EIGHT TWO TWO EIGHT SEVEN PAREN
PAREN SIGNED EISENHOWER EASY EXRAY EIGHT TWO TWO EIGHT NINE PAREN
PAREN TO INGLES FOR SPSCO DASH L FROM LEE SIGNED EISENHOWER EASY EXRAY EIGHT TWO TWO NINE ZERO CITE SOSSC
PD FROM LEE SIGNED EISENHOWER EASY EXRAY EIGHT TWO TWO NINE TWO PD
PAREN TO SOMERVELL FOR BOONE FROM LEE SIGNED EISENHOWER EASY EXRAY EIGHT TWO TWO NINE THREE CITE ETOCE PAREN
FROM ROBERTSON FROM LEE (EASY EXRAY EIGHT TWO TWO NINE FOUR) SGD EISENHOWER CITE SOSSC TO SPSAS
PAREN FOR SPXPR SIGNED EISENHOWER EASY EIGHT TWO TWO NINE FIVE PAREN
PAREN BRERETON TO ARNOLD FOR LEACH CHIEF OPERATIONS ANALYSIS DIVISION FOR SPAATZ SIGNED EISENHOWER (EASY EIGHT TWO NINE ZERO SIX) PAREN
PAREN SPAATZ CITE EASY EIGHT TWO TWO NINE EIGHT TO ULIO INFO CG AAF SGD EISENHOWER PAREN
PAREN TO DUNLOP SPGAR INFO ARNOLD FROM SPAATZ CITE EASY EIGHT TWO TWO NINE NINE SIGNED EISENHOWER CITE WAR TWO SEVEN EIGHT TWO ZERO MARCH TWO NINE PAREN
PAREN TO ARNOLD FROM SPAATZ SIGNED EISENHOWER CITE EASY EIGHT TWO THREE ZERO ZERO WARX THREE SIX TWO ONE ONE MAY THIRTEEN PAREN
PAREN FOR GRONINGER INFO IRELAND FROM LEE SIGNED EISENHOWER REF NO EASY XRAY EIGHT TWO THREE FOUR SIX PAREN REFERENCE CABLE WAR TWO NINE NINE NINE FOUR DATED FOUR MAY PD

~~SECRET~~

PAREN 02 DAILY CABLE MAY TWENTY SEVENTH EIGHT ZERO ZERO TO WDGBI FROM RTGBI FROM CONRAD SIGNED EASY EIGHT TWO THREE FIVE TWO EISENHOWER PAREN
PAREN CITE SOSTC NINE TWO FIVE FOUR FROM ROSS FROM LEE SIGNED EISENHOWER EASY EIGHT TWO THREE FIVE FIVE PAREN
PD CITE SOSTC NINE ONE FIVE FIVE FROM ROSS FROM LEE SIGNED EISENHOWER RHF NR EASY EIGHT TWO THREE SIX ZERO (MY PASS TO OSD) PD
PAREN CITE SOSTC NINE ONE FIVE SEVEN FROM ROSS FROM LEE SIGNED EISENHOWER EASY XRAY EIGHT TWO THREE SIX ONE PAREN
PAREN EASY EIGHT TWO THREE SIX TWO TO SURLES FROM LAWRENCE SIGNED EISENHOWER REUR WAR FOUR SEVEN TWO ZERO NINE PAREN
PAREN EASY EIGHT TWO FOUR TWO SIX FOR SPXPR SIGNED EISENHOWER PAREN
PAREN FOR ORDINGER FROM LEE SIGNED EISENHOWER RHF NR EASY EIGHT TWO FOUR FOUR ZERO TO GOT WASH D CATH LT COL A G STRAN PAREN

~~SECRET~~

~~SECRET~~

NAVY STYLE

FROM COMDESLANT ACTION CTF SIX FOUR AND CTG TWO TWO DOT FOUR INFO CINCLANT
RABBITT OFFERS COMSLSVEN
X GRIFFIN ORIGINATOR DEPARTED X
X SAYS COMEASTSEAFROM MYDIS ONE FOUR ZERO SIX HUNDRED X
X NAVY YARD NEW YORK HAS FOR ACTION SHIP PASS TO CHARLIE TARE FOX SIX SIX FOR INFO X
X HERE COMES DE DISBURSING OFFICE NEW YORK WITH CTS TWO ZERO ONE FIVE TWO FOUR X
X SENT BY CINCLANT ACTION TASK FORCES SIX EIGHT SIX FOUR SIX THREE SIX TWO COMSERVLANT
FOX AFLF OBOES AT BOSTON NEW YORK AND CHARLESTON X
X THIS FROM CINCLANT ACTION OFF TWO FOUR INFO COMNAVEU X
XCOMNAVNAVREERCTPHERBCI'CMEDZEROEIGHTTWELVEHUNDREDX
X COMDESLANT TELLING ACTION BUPERS INFO CINCLANT X
X USNO PHILA SINGS X
X HANCOCK SPEAKING ACTION CINCPAC RDO WASHN PASS TO NSD MECHANICSBURG X
X SAYS CTU ZERO TWO POINT NINE DOTTED X
PUSHIPS SLIPS THIS ONE OUT TO NSD ORAN
PUSHIPS SPEAKS TO NAV OBOE BAKER NORFOLK
MARPACSHOUTSTOMA-CORPS
CORINCH YELLS TO CINCPAC X YOUR ONE TWO ZERO SEVEN FOUR TWO X
XNAESEVENCHIESTONOBPEARLX
COMCARIBSEAFROM TAKES GREAT PLEASURE IN PRESENTING HIS TWENTY HUNDRED POS

~~SECRET~~

BRITISH STYLE (TYPE I)

((( AIRMIS WHALL AGWAR FROM HQ MAAF. AF308(308 2(2 MAY. MED ALLIED AIR FORCES OPSUM 336(336. MEDITERRANEAN ALLIED )))
((( AIR MINISTRY WHITEHALL A WAR FROM HQ [illegible] FOX 337(337 15/5(14/5 SECRET. MEDITERRANEAN ALLIED AIR FORCES OPSUM 446(446 ABLE CONTINUATION OF ABLE FOX 334(334. MEDITERRANEAN ALLIED TACTICAL AIR FORCE. CORRECTION OPSUM 547(547. AMEND )))
PART FIVE AND FINAL PART OF ABLE FOX 340(340 16(16 MAY
((( AAA AGWAR FROM HQMAAF AF 341(341 17(51TH MAY SECRET. IMMEDIATE. MEDITERRANEAN ALLIED AIR FORCES OPSUM 551(551 )))
((( AAA AGWAR FROM HQ MAAF AF343(343 18(18 MAY SECRET MEDITERRANEAN ALLIED AIR FORCES OPSUM 552(552 MASAF(MASAF.
(( PAR TWO OF ABLE FOX TITLE FOUR THREE EIGHTEENTH MAY SECRET ))
( PART SIX AND FINAL MY AF343(343 181813(181912 B FROM HQ MAAF)
0.4822(0.4822 TO COSTTINTREP ADDRESSEES (FREEDOM PASS C IN C MED ALGIERS AND 7(7) ARMY. UNITY (SHAEF) PASS EXFOR TAC EXFOR AND 2(2) TAC AIR FORCE) INFO 2(2) DISTRICT (PASS 15(15 AIR FORCE (3) DISTRICT (1) DISTRICT FROM HQ AAI SIGNED WILSON CITE FHOCT(OCT) FHOCT(OCT) AND FHOBI(OBI) MAY 182235. SECRET. COSTTINTREP NO. 412(412) TO 1800(1800) BRS 16(16) MAY. PART ONE. SECTION ONE. INTELLIGENCE.
SECRET. THIRD CIPHER PART OF HQ AAI(AAI) COSTTINTREP NUMBER 413(413) 172230 ORIG NUMBER 04829(4829)
END OF PART SIX OF NUMBER 04829(4829) OF COSTTINTREP NUMBER 413(413 172230(172230) PART SEVEN AND LAST FOLLOWS
SEVENTH CIPHER PART OF COSTTINTREP NUMBER 413(413) SECRET FROM HQ AAI(AAI) ORIG NUMBER 04829(4829) THREE ENDS. SIGNED WILSON CITE FHOCT(OCT) AND FHOBI(OBI). SECTION 0.4835(4835) 182250(182250 B FROM AAI(AAI) TO COSTT INTREP ADDRESSEES. AFHQ (PASS C IN C MED ALGIERS) UNITY (SHAEF) (PASS EXFOR TAC EXFOR AND (2) TACTICAL AIR FORCE INFO 2(2) DISTRICT (PASS 15(15) AIR FORCE) 3(3) DISTRICT 1(1) DISTRICT (PASS 7(7) ARMY). SIGNED WILSON CITE FHOCT AND FHOBI. SECRET. COSTTINTREP NUMBER 414(414) TO 1800(1800) BRS 18(18) MAY. PART ONE. SECTION ONE.
FIFTH AND LAST CIPHER PART OF COSTTINTREP NUMBER 414(414) FROM HQ AAI

## APPENDIX II

### FILE DATE/TIME

The file date/time group which appears in clear in the preamble of messages usually signifies the date and time put on by the writer upon finishing the composition of his message or the time in which the writer files his message in the message center. It infrequently designates the time a message leaves message center on its way to radio operator.

What are the relative advantages and disadvantages in keeping the file date/time in clear as at present, omitting it altogether, or enciphering it internally?

(1) The date/time group in clear allows deductions from the correlation of date/time and type of traffic. Thus, air traffic at a certain time may mean planes arriving, departic, etc. Water transport traffic may refer to a situation report or convoy movements, etc. Removing the date/time group from the preamble of message would not eliminate ability to make this deduction, for transmittal or intercept time could function just as well.

(2) File date/time group allows collecting of parts of same message. Intercept time functions just as well.

(3) File date/time group can be used for correlation with internal message numbers.

Intercept date/time and cryptographic date function just as well.

(4) Can the file date/time be omitted altogether?

The file date/time allows the recipient to evaluate the contents of a message; and provides a check on the communications interval. This may be very important. The recipient is informed that at a

given hour, the contents of the message are valid. If two rather contradictory messages are received, it is important to know the sequence in which they were written. Omission of file date/time would also make the servicing of messages difficult. The file date/time cannot be omitted.

(5) Should the file date/time be enciphered internally?

Encipherment of date/time is insecure cryptographically, for correlations are possible between intercept date and file date. It would also be difficult to identify messages for servicing.

Since intercept date/time will function in most cases as validly as file date/time, and since it is not feasible to encipher date/time group from security viewpoint; since file date/time provides a communication check which cannot be provided by any other means.....,there seems little reason to discontinue the present practice of clear file date/time group in preamble.