CLASSICAL CRYPTOGRAPHY COURSE
BY LANAKI

04 JANUARY 1996
Revision 0

LECTURE 22

CIPHER MACHINES II

HEBERN'S "COMMERCIAL PORTABLE CODE" MACHINE AND THE ELECTRONIC CIPHER MACHINE MARK II (ECM MARK II or SIGABA)

SUMMARY

Lecture 21 opened up a hornet's nest. Lecture 22 (in response to student E-mail) covers cipher machine history and specifically, two more cipher machines - both electric rotor designs at different ends of the cryptosecurity scale : the simple one rotor Hebern "Commercial Portable Code Machine" and the Navy ECM Mark II (for Electronic Code Machine Version II designated SIGABA by Army) machine to illustrate further cryptographic principles surrounding the era of cipher machines. We develop our subject via a select group of references and assistance from the National Maritime Museum Association. [DEVO], [FR8], [NICH], [DAWS], [KULL] We will look at the ECM Mark II within the purview of the USS Pampanito (SS-383) and her place at war.

ACKNOWLEDGMENTS

Special acknowledgments for material excerpted in this lecture are made to Dr. Richard Pekelney, Dr. Cipher A. Deavours, Dr. Louis Kruh, Donald Dawson, U.S. National Archives and Records Administration (NARA), National Maritime Museum Association (NMMA), USS PAMPANITO (SS-383) and Director, NSA Cryptological Museum.

INTRODUCTION TO MACHINE CRYPTOGRAPHY

If we examine the 1,769 cryptography related patents issued between 1861 - 1980, we find that the 1920s were the most productive era. Six inventors shined. They were Arvid Gerhard Damm, Edward Hugh Hebern, Hugo Alexander Koch, Arthur Scherbius, Willi Korn, and Alexander von Kryha. 22 US patents are credited to this group during the decade. William F. Friedman's name joined the list in the 1930s. Herbern was the most prolific being credited with 9 US patents.

The first cryptographs produced under Damm's patent were clumsy and unreliable. The most important of Damm's cryptographic ideas was a rotor invention under US patent 1,502,376, July 22, 1924, but was never able to exploit fully.

The rotor principle was, in one form or another, the most widely used method of machine cryptography. The rotors took two forms: pinwheel rotors and wired rotors. We have looked at the pinwheel variety with 'active' and 'inactive' projecting positions in Lecture 21. The wired code-wheel is a disk constructed of some non- conducting material having on each face, a series of equally spaced contact studs which are interconnected so that the current entering on one face will be switched to exit from a different position on the other face of the rotor. Each face may have 26 studs (26 letters). The rotor acts as an electrical commutator (i.e. switch) and essentially causes a monoalphabetic substitution. By moving the rotors or employing a cascade of rotors, repeated substitutions can be obtained and varied to produce polyalphabetic ciphers of great complexity.

Boris Caesar Hagelin, an employee of Damm's, created the B-211 cryptograph which used two electrical rotors in conjunction with four pinwheel rotors to sell the first commercially successful cryptograph.

By the WWI, the wired rotor was an idea whose time had come. Without knowledge of each other, Damm and three others conceived of using the wired rotor for cryptographic machines. In 1917, Edward H. Hebern created his famous Electronic Code machine under patent 1,510,441 awarded on September 30, 1924. This machine influenced greatly the America cryptosecurity systems throughout WWII. Hebern's rotors had the 26 contact A-Z sequence. To Hebern must also go credit for the idea of wiring rotors according to the "interval method". Up to Hebern, designers randomly

connected the contacts to each face of the their rotors. Hebern chose his wiring to produce as flat a polyalphabetic frequency distribution as possible. The interval method of wiring rotors was used in the ECM.

An example of the interval procedure of wiring a rotor is:

Given:

Input Contact:

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

Output Contact:

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

The displacement which is defined for any input contact, measures the shift taken by the current traversing the rotor. So:

AG 06	BA 25	CD 01
DB 24	EO 10	FC 23
GT 13	HK 03	IN 03
JU 11	KZ 15	LX 12
MI 22	NW 09	OH 19
PF 16	QQ 00	RY 07
SL 17	TV 02	UP 21
VM 17	WE 08	XL 14
YS 20	ZR 18	

Of the 26 possible displacements values, 0 to 25, every displacement occurs in this set except 4, while displacement 17 occurs twice. This is the construction of the Hebern rotors.

The rotor machine destined to be the most famous of all time was fathered by Koch and Scherbius. It was named "Enigma." The machine attained its real potential in patents held by Korn. Korn explicitly set forth the idea of interchangeable rotors and allowed for reversability of the rotor turning. On October 29, 1929, Korn received US patent 1,733,886, which provided for a feed check apparatus to ensure correct rotor positioning and movement. In 1933 two more patents were issued for the Enigma in final form. (See Lecture 9)

During the same period, German cryptographers were altering Korn's commercial Enigma into a more secure form. In England, the British modified the Enigma for military use and called it the Typex. William F. Friedman started development on a tactical level rotor machine based on the Enigma. Friedman's machine, —325 failed to work well under field conditions and was not accepted. [This is William F. Friedman's only failure.]

The Enigma was such a commercial success that many countries bought the machine for use and study. The Japanese Enigma known as GREEN machine had rotors mounted on the top of the machine with characteristic Japanese design eccentricity.

Probably the most mechanically and cryptographically complex wired rotor machine was the American top-level machine, known as the ECM Mark II or SIGABA (also known as the M-134-C) in the Army and CSP - 888/889 in the Navy. The devise was based on an idea by Frank Rowlett and was considered insolvable, and that it was.

In 1924, Alexander von Kryha of Germany invented a simple spring driven arrangement of concentric disks which became widely used for 2 decades thereafter. European interests used many of the Kryha machines in banking, industrial and transportation industries.

During WWII, the Germans used the Kryha machine and the US cryptographic teams successfully analyzed intercepted diplomatic traffic. When proposed to be used in the US Army, Friedman, Rowlett, Kullback, and Sinkov, solved an untypically long test message of 1,135 letters to demonstrate the weakness of the machines ciphers. Statistical analysis was used extensively in the solution. (See Lecture 15.)

The Japanese actively pursued the development of machine ciphers during the 1920s and 1930s. Their RED ORANGE and PURPLE series were wired rotor machines based on the Hebern machine and German Enigma. Their RED machine had the distinction of being the first electromechanical cipher device to be broken by the American cryptanalysts.

While the German Enigma dominated the wired rotor market, Hagelin designed a series of machines first for the French and Russian Armies, the B-211, and then up with the idea for using variable pin rotors in conjunction with a cage of horizontal bars containing lugs to develop a new series of machines known as the 'C' machines whose variations and elaborations are still debated today. The most famous was the C-38 (the number indicates the year of release) which became the standard low echelon cryptograph for both the Army (M-209) and Navy (CSP1500).

During 1941-42, the Germans penetrated the C-38 traffic successfully in North Africa. This is why the Americans failed to maintain the tactical advantage in the earlier battles. After WWII Hagelin ran Damm's old Swedish organization and moved it to Switzerland under the name Crypto AG. Hagelin's lug and pin machines were very commonly used in embassies everywhere.

After 1931 the German's developed a series of cipher teleprinters dubbed the Geheimschreiber (secret writer). The story of the Polish attack -then British - then American attack on the Enigma has been well documented. The English expanded Friedman's coincidence calculations publishes decades earlier to attack the Enigma. (See Lecture 9).

In general, Axis code-breakers never scored regular penetration of the C-36 or M-209 systems. The Americans and British did a better job day-to-day on the details of cryptographic security. It has been demonstrated that failure to observe routine procedures in messages, changing keys, all pointed to disaster. The machine ciphers of the 1930s and 1940s were often more than adequate to defeat normal cryptanalysis if used with care. Even against today's computers, many of these machines could still prevail.

The role of computing technology in cryptanalysis has often been to aid in the rapid location of encipherment blunders in intercepted enemy traffic. The most fruitful cryptanalysis against the Russians in the 1980s and 90s has resulted from this approach rather than from any great conceptual advances caused by the development of computers. [NICH]

By 1950, the increasing appropriations and diminishing success of the US cryptanalytic effort in penetrating high level Soviet and Eastern bloc cryptosystems forced a reorganization of the communications intelligence (COMINT) activities. At that time there were four principal US cryptanalytical agencies: the Army Security Agency (ACA), the Naval Security Group, the Air Force security Services, and the Armed Forces security Agency (AFSA). In practice all these groups worked independently.

President Harry S. Truman directed the Secretary of Defense to establish a committee to survey COMINT activities in the US and to recommend actions. Based on this committees report the National Security Agency was formed via a secret executive order of October 24, 1952. The NSA was given clear responsibility over all US COMINT activities. The NSA has a military Director and a civil deputy Director.

Cryptography is virtually all electronic in the US. There is a tendency for our newer "sci.crypt" gurus to believe that faster and faster machines and larger storage devices could change the fundamental problems facing cryptanalysts after WWII. They tend to forget that the Third World's mail is the raison d'entre on NSA. These systems are usually easier to crack than those of the major powers and reveal much more information of highest priority and importance. That fact that cryptography is micro-computer based does not take away some of the conflicting system design aims just as decades ago.

HEBERN COMMERCIAL PORTABLE CODE MACHINE

The cryptanalysis of the one wire rotor Hebern machine follows along the lines of that discused in the CSP1500 in Lecture 21. There are some interesting differences. First of all, the setting up of the Rotor Generatrix Tableau is based on diagonalization of a sparse matrix rather than a horizontal or vertical solution.

Lets start with a one of Hebern's original rotors:

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

The output wiring is the straight A-Z sequence. As the plaintext letter S is entered from the keyboard (top), the electrical current enters the rotor at the 19th position of row two, which is wired to the 11 position, or to the letter K. This determines the output letter. Row two represents the permutation device. Thus if the rotor remains stationary, a simple substitution cipher is produced. For example, the plaintext SEND MORE AMMUNITION becomes KVLJ HROV FHHPLWBWRL.

To increase security, the rotor turns one position toward the operator before encipherment. In the diagram, rows two and three, simulating the rotor, shift one position to the right producing a second simple substitution cipher alphabet. Both row one and four never move during the encipherment process. The shift looks like this:

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

This time the letter S plain enters the keyboard row 1 and the electrical current enters the rotor at the 19 position which is now the letter B. the currents permutes to position 1 on row three. This results in letter A. We now have a polyalphabetic substitution problem because the rotor moves one position prior to entering the letter for each plaintext letter. The message SEND MORE AMMUNITION becomes:

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

          S E N D
  D -> E  E
  E -> F    Y
  F -> G      V
  G -> H        L

                  M O R E

  H -> I          H
  I -> J            X
  J -> K              J
  K -> L                J

  L -> M                    V
  M -> N                      L
  N -> O                        R
  O -> P                          O
  P -> Q                            T
  Q -> R                              H
  R -> S                                V
  S -> T                                  A
  T -> U                                    C
  U -> V                                      B
```

The real problem is to reduce the rotor ciphertext to monoalphabetic terms. Dawson (in a very badly edited book) describes the interesting procedure of matching diagonal alphabets or in chemical engineering optimization terms matrix reduction by diagonalization. The problem is easier if it is a sparse matrix. [NICH], [DAWS]

Lets look at the Dawson procedure:

Given the following cryptogram generated from a single rotor Hebern machine: (I have rewritten the original groups of 5 into 26 character lines "in depth")

```
XFSDOXIZYHSMDNJNJILAFINJLS
RZYTKIKQLVQFKKVLEJFDHIKIKR
AJPYLBTENHWCDESCLHXWTRIBJP
LWYUOEBLNSHRHHTPTJAETDOZQG
LMLJSIGLNNWAJHBLEOEMTVAEVD
XGGCZYWZNSLXYAHLLODDTDXCNJ
CKFLPIEZGZWCOGRHTEOXTDDGSN
LLQBLUAPQNQXPENHPSRXTDDGUS
XOMCJNWZSQFXIHVXPQLWYIEANL
DOWSSNPPTEEWJHZYRWZXITPUSZ
XUYISIGFVBCFIUBNJOVBSRAIGG
XXXLPHZLNSQXUKELTJAGKOYUSC
ROWHPYZDYUCAUBPPZARKFZDHSS
YXHIUDTYVZWFKQVJHZOMTVDHSS
GLTEZDKSOQFXEUEDTIAQVRTDZP
LLSEPHNDAQEXWMQSTEABFXKAIS
XHLPVPLPWHNDJUODMJOQHOOCGM
GLTQIHOLVNBMHORLRWRCFYPHQJ
CKGMZHZALMAWJBXXEQDATDMZNS
CRFGWHJSBKQHOARGBOULWVAJTX
UUEZPQKSBQEXMRPLWYGAURAASN
SXGGBBTBPNYMDXHHMIVDRRWAVZ
RHXDRNHZEHSXIKOAZUAGTLRGQK
LEADOZTBLHRWSIRPIZAGCXASGM
XFLDUHTSENIXUIRWUEOQTLMHTF
ZXEZUPAZXVCIOUTYRHKDTDOVWJ
SGMGBLTUPRWXONBDKNEUEYAEZJ
SEOYOPUZSLEPMTHDROSQFONJLW
OKYRDZTIVKAIPJRGYEATRTKITY
ZDSJUDTBZXFFRHTWTODDFIOATZ
MQPEAYGCGHPTIJUDKWDMBTUWVU
XKTIUIWZWVMXMPQPZPOXHLUNQL
QHZLPIJQNVRZPJHPZPOXHLUZVX
LWTJUBQQWSQWUYOPZPOXHLUZVX
YSPYOTNZTSBIPJHOZFKMWOOBZC
ZXQCXXNDWYNPOPXZBWBAQTXNFC
XHPCUDTGUGTRONUVNOFKJSXBNW
XFSBRLZUETHREEVWVYOVJRUCJF
XXPYOWGTGGLMBIHTEZLATYDGJJ
SKYISCTUVFNIMETYVYGXHJAINS
SKYISCTLNSQXIETPKWKYFXXMVA
```

```
GLTTOBNDGPNAPUUBZOZSFCMGGN
POQGLNNPYSWFNUNAWDMWHIAEIS
OQTBRLZDVKWCDUHPZSRZYOOGUS
DJTDUDTGYZVXDHTLUWFTFHRDBS
YJTRKILLVTTDEIHLUWZEFQBAFZ
UXMCBQTMLUTIOBPNHZALWVNGQC
ODYPIVIPZFEVJOKYRTRIFIIDIS
XUGVHXWZEHGXPKOARGRCYNAUSS
RXDCWHGQBFYAWKTNGNRETOXZVX
TXGCBAZABQTDCQVJASRJJJMUSZ
LEQBLEILLSRIYTHZXINYTTUGQL
MTSOXHAPYUQAWPXTZOVDJPIANA
RXQYRPJSFUACSOH
```

Each column therefore was enciphered by the same rotor position, implying monoalphabeticity.

Step 1: Rewrite the ciphertext into columns matching the turn-over position of the rotor movement. In the case the rotor alphabet is known to be English and therefore has a length of 26. If this information was unknown, we would use the PHI test (Lecture 15) to determine the length of the rotor alphabet. We verify:

Letter frequencies:

```
A  56   E  50   I 57   M  33   Q 47   U 58  Y 48
B  42   F  37   J 45   N  54   R 52   V 41  Z 68
C  33   G  52   K 36   O  62   S 66   W 52
D  60   H  63   L 67   P  61   T 81   X 72

Letters = 1393
Phi Values:
     Observed      =   77058
     Random        =   74653
     Non-Random    =  132621

Columns      Phi(o)     E(random)   E(plain)

  23         140.1       138.9       246.8
  24         141.1       127.5       226.5
  25         115.4       117.4       208.6
  26         205.0       108.5       192.7
  27         104.4       100.5       178.6
  28          99.0        93.4       165.6
  29          85.8        87.0       154.5
```

Step 2: The Frequency Tableau

First we take a frequency count of each column. Part A: If the ciphertext was created by one of the Viggy's or variants, we can skip part B. we would start matching the columns based on the Viggy alphabets and relationships. In the case of a single rotor machine, this is not the case. Part B: Match alphabets instead of matching columns (as in the CSP1500 solution). We use diagonal alphabets for the matching. The single rotor cipher machine generate progressive alphabet sequences in the direction which the rotor turns. Some single rotor devices can reverse the direction of the turning rotor, in which case we would generate diagonals in downward sloping form. For third problem we will describe the standard rotor rotation which develops upward sloping diagonals.

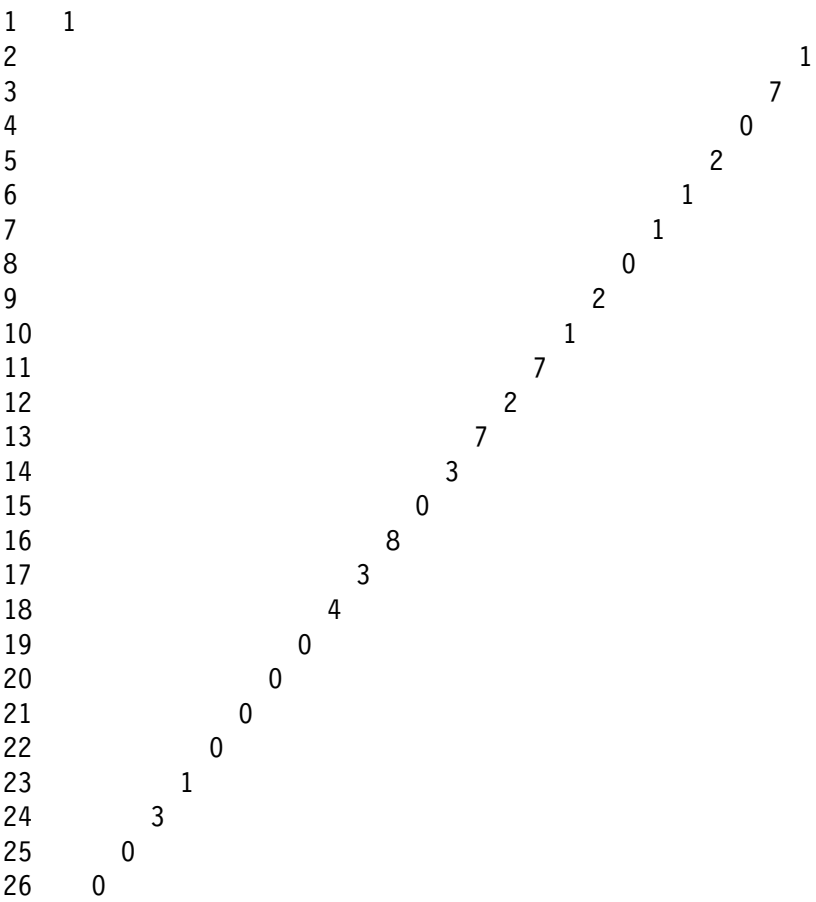
In order to make each of the 26 diagonal alphabets, the frequency count in the form of an upward sloping diagonals are used in place of the column frequency count. See Figure 22.1.

Figure 22-1

Col	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
1	1	0	3	2	0	0	3	0	0	0	0	7	2	0	3	1	1	5	5	1	2	0	012	3	3	
2	0	0	0	2	3	3	2	4	0	3	6	5	1	0	4	0	2	1	1	1	3	0	210	0	1	
3	1	0	0	1	2	2	5	1	0	0	0	3	3	0	1	5	5	0	5	8	0	0	2	2	7	1
4	0	4	7	5	3	0	5	1	5	2	0	3	1	0	1	2	1	2	1	2	1	1	0	0	5	2
5	1	4	0	1	0	0	0	1	2	1	2	4	0	0	7	6	0	4	5	0	8	1	2	2	0	3
6	1	4	2	5	2	0	0	8	7	0	0	3	0	4	0	4	2	0	0	1	1	1	1	3	3	2
7	3	1	0	0	1	0	4	1	3	3	3	2	0	5	1	1	1	0	014	1	0	4	0	0	6	
8	2	3	1	5	1	1	3	0	1	0	0	7	1	0	0	6	4	0	5	0	3	0	0	0	110	
9	1	4	0	0	4	1	3	0	0	0	0	5	0	7	1	2	1	0	2	3	1	7	4	1	5	2
10	0	1	0	0	1	3	2	7	0	0	3	1	1	5	0	1	5	1	8	2	4	4	0	1	1	3
11	3	2	3	0	5	3	1	2	1	0	0	2	1	4	0	1	7	3	2	4	0	1	7	0	2	0
12	5	0	4	3	0	5	0	1	6	0	0	0	4	0	0	2	0	3	0	1	0	1	414	0	1	
13	0	1	1	5	3	0	0	2	5	5	2	0	4	1	7	6	0	1	2	0	4	0	3	0	2	0
14	2	3	0	0	5	0	1	6	4	4	5	0	1	3	3	3	2	1	0	2	7	0	0	1	1	0
15	0	3	0	0	2	0	010	0	1	1	0	0	2	4	3	2	6	1	7	3	5	0	3	0	1	
16	3	1	1	5	0	0	2	3	0	2	0	8	0	4	1	8	0	0	1	2	0	1	3	2	4	2
17	1	2	0	0	4	0	1	2	1	2	3	2	2	1	0	2	0	6	0	6	3	2	2	1	1	9
18	1	0	0	1	4	1	1	2	4	4	0	0	0	2	9	3	2	0	3	1	1	0	7	0	3	4
19	8	1	0	4	2	3	2	0	0	0	3	3	1	1	8	0	0	8	1	0	1	3	0	1	0	3
20	5	2	2	6	3	0	3	0	1	1	2	2	4	0	0	0	4	0	1	2	1	1	3	7	2	1
21	0	1	1	0	111	0	7	1	4	1	0	0	0	0	0	0	1	3	113	1	1	3	0	3	0	
22	0	0	1	6	0	0	0	1	6	2	0	5	0	1	6	1	1	5	1	6	0	4	0	3	3	1
23	9	1	0	5	1	0	0	0	3	0	3	0	4	3	6	2	0	2	0	1	6	0	1	5	1	0
24	7	3	3	3	3	0	8	4	4	3	0	0	1	2	0	0	0	0	1	0	4	1	1	0	0	5
25	0	1	0	0	0	2	4	0	3	3	1	2	0	6	0	0	6	0	8	4	2	7	1	0	0	3
26	2	0	4	1	0	2	2	0	0	5	1	3	2	3	0	2	0	112	0	1	0	2	4	1	5	

For example, the diagonal row one would consist of the frequency of letter A from column 1, the frequency of letter B in column 26, the frequency of letter C in column 25, and onward to letter Z in column 2. This new frequency distribution for the first row is shown in Figure 22-2. The second diagonal row will begin with the frequency of the letter B of the first column. Then the frequencies for the rest of the second alphabetic frequency distribution follows the upward slope as did the first row. The same procedure is followed for all balance of the frequency distributions.

Figure 22-2



We can reevaluate the Phi values for each new diagonal alphabet:

Diagonal Row #1 letter frequencies:

A	1	E	1	I	0	M	0	Q	7	U	1	Y	7
B	0	F	0	J	4	N	3	R	1	V	1	Z	1
C	0	G	0	K	3	O	7	S	2	W	2		
D	3	H	0	L	8	P	2	T	0	X	0		

Letters = 54
Phi Values:
Observed = 218
Random = 110
Non-Random = 195

letter count and Phi values for 26 diagonal alphabets:

Row	# of letters	Actual Phi
1	54	218
2	54	196
3	41	74
4	56	196
5	52	138
6	53	220
7	76	318
8	46	150
9	56	294
10	52	196
11	37	78
12	52	168
13	47	144
14	58	286
15	51	134
16	49	154
17	59	238
18	51	232
19	59	230
20	55	196
21	37	100
22	63	272
23	59	228
24	57	254
25	54	228
26	65	388

Step 3: Match the diagonal alphabets

The next step is to match the diagonal frequency distributions. Several factors are considered in determining the base or stationary alphabet. We examine the Phi values and find the highest observed value occurs at alphabet 26 with a value of 388. This is usually the best place to begin, we check the observed Phi versus the observed Phi.

E(0r) = 0.0385 (65) (64) = 160
E(0p) = 0.0683 (65) (64) = 284

The observed Phi for this diagonal alphabet is noticeably higher than the expected value for a normal English plaintext alphabet. This is not as odd as it seems for a diagonal alphabet. The number of letters will vary from 37 to 73 letters and this makes the numbers skew somewhat high or low for observed values. We might copy the base alphabet into a 27th position and match all the remaining diagonal alphabets against it.

To match all the rest of the alphabets to the base, we select the next highest matching diagonal alphabet and combine their frequencies.

We start with the second highest observed Phi value and compute values for comparison. The observed value for row 7 is 318. So:

E(0r) = 0.0385 (76) (75) = 219
E(0p) = 0.0683 (76) (75) = 389

The observed Phi is approximately the midpoint of these two. We also take the third value from row 9 and calculate its Phi values.

E(0r) = 0.0385 (56) (55) = 118
E(0p) = 0.0683 (56) (55) = 210

The observed value of Phi is 294 is higher than the expected Phi for English text. Therefore this is a better choice (row 9) and is made the first alphabet to match to the base alphabet.

We can confirm this choice with the X test from Lecture 15. We match alphabets 27 vs 7 and 27 vs 9 for all 26 positions:

```
      27 vs 7
A   168      N  156
B   185      O  136
C   147      P  165
D   227      Q  182
E   167      R  241
F   192      S  178
G   353      T  207
H   166      U  202
I   180      V  266
J   228      W  238
K   169      X  136
L   169      Y  178
M   155      Z  149

    E(Xr) = 190
    E(Xp) = 337

      27 vs 9
A   128      N  131
B   173      O  169
C   100      P  130
D   128      Q  136
E   365      R  183
F   137      S  195
G   134      T  152
H   200      U  190
I   110      V  114
J    81      W  103
K   141      X   99
L    86      Y  154
M    48      Z   53

    E(Xr) = 140
    E(Xp) = 248
```

The results confirm that diagonal alphabet 9 is the best alphabet to join the base alphabet, which is the copy of the 26th alphabet. The base alphabet will remain stationary throughout the matching process. The results of the combined frequencies are as follows:

```
    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
26- 2 1 3 5 011 3 0 4 2 0 0 1 1 0 1 5 0 514 1 1 0 2 0 3
    E F G H I J K L M N O P Q R S T U V W X Y Z A B C D
9   0 0 5 4 0 5 1 0 4 1 0 0 0 0 0 2 3 0 314 2 3 1 3 0 5
=======================================================
    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
27: 2 1 8 9 016 4 0 8 3 0 0 1 1 0 3 8 0 828 3 4 1 5 0 8

    Total letters =   121       Random Phi = 559
    Observed Phi  =  1412       Plain phi  = 993
```

We add the frequencies of the individual letters to get a new total base component. As the total letters increases the probability of a correct match increases.

The matching process continues for every letter in the diagonal alphabets. The next addition would be row 7 and the best letter to match is G:

```
old 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
27- 2 1 8 9 016 4 0 8 3 0 0 1 1 0 3 8 0 828 3 4 1 5 0 8
    G H I J K L M N O P Q R S T U V W X Y Z A B C D E F
7   3 0 3 3 3 5 0 0 8 3 0 0 1 2 4 1 7 1 510 3 4 0 5 2 3
=======================================================
new 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
27: 5 11112 321 4 016 6 0 0 2 3 4 415 11338 6 8 110 211

    Total letters =   197       Random Phi = 1486
    Observed Phi  =  3062       Plain phi  = 2641
```

and so on for the balance of the diagonal alphabets.

Step 4: Construct the Reduction Tableau

The next step involves the construction of the reduction tableau from the results of matching the diagonal alphabets. We write out the base alphabet into the tableau starting at letter A and continuing in an upward sloping manner. All the other diagonal alphabets are written in the same way beginning with the matching letter to the base alphabet letter A. If the reversing rotor was used than the slope of the alphabet lines would be right and down. This tableau is the basis for reducing the polyalphabetic single rotor ciphertext into monoalphabetic terms. See Figure 22-3.

Figure 22-3

	1	2	3	4	5	6	7	8	9	10				15				20					26
Col	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
1	V	A	W	T	R	O	M	I	M	H	F	D	A	Q	Z	V	S	Q	N	L	T	J	G	E	C	Z
2	Z	V	S	Q	N	L	H	L	G	E	C	Z	P	Y	U	R	P	M	K	S	I	F	D	B	Y	U
3	U	R	P	M	K	G	K	F	D	B	Y	O	X	T	Q	O	L	J	R	H	E	C	A	X	T	Y
4	Q	O	L	J	F	J	E	C	A	X	N	W	S	P	N	K	I	Q	G	D	B	Z	W	S	X	T
5	N	K	I	E	I	D	B	Z	W	M	V	R	O	M	J	H	P	F	C	A	Y	V	R	W	S	P
6	J	H	D	H	C	A	Y	V	L	U	Q	N	L	I	G	O	E	B	Z	X	U	Q	V	R	O	M
7	G	C	G	B	Z	X	U	K	T	P	M	K	H	F	N	D	A	Y	W	T	P	U	Q	N	L	I
8	B	F	A	Y	W	T	J	S	O	L	J	G	E	M	C	Z	X	V	S	O	T	P	M	K	H	F
9	E	Z	X	V	S	I	R	N	K	I	F	D	L	B	Y	W	U	R	N	S	O	L	J	G	E	A
10	Y	W	U	R	H	Q	M	J	H	E	C	K	A	X	V	T	Q	M	R	N	K	I	F	D	Z	D
11	V	T	Q	G	P	L	I	G	D	B	J	Z	W	U	S	P	L	Q	M	J	H	E	C	Y	C	X
12	S	P	F	O	K	H	F	C	A	I	Y	V	T	R	O	K	P	L	I	G	D	B	X	B	W	U
13	O	E	N	J	G	E	B	Z	H	X	U	S	Q	N	J	O	K	H	F	C	A	W	A	V	T	R
14	D	M	I	F	D	A	Y	G	W	T	R	P	M	I	N	J	G	E	B	Z	V	Z	U	S	Q	N
15	L	H	E	C	Z	X	F	V	S	Q	O	L	H	M	I	F	D	A	Y	U	Y	T	R	P	M	C
16	G	D	B	Y	W	E	U	R	P	N	K	G	L	H	E	C	Z	X	T	X	S	Q	O	L	B	K
17	C	A	X	V	D	T	Q	O	M	J	F	K	G	D	B	Y	W	S	W	R	P	N	K	A	J	F
18	Z	W	U	C	S	P	N	L	I	E	J	F	C	A	X	V	R	V	Q	O	M	J	Z	I	E	B
19	V	T	B	R	O	M	K	H	D	I	E	B	Z	W	U	Q	U	P	N	L	I	Y	H	D	A	Y
20	S	A	Q	N	L	J	G	C	H	D	A	Y	V	T	P	T	O	M	K	H	X	G	C	Z	X	U
21	Z	P	M	K	I	F	B	G	C	Z	X	U	S	O	S	N	L	J	G	W	F	B	Y	W	T	R
22	O	L	J	H	E	A	F	B	Y	W	T	R	N	R	M	K	I	F	V	E	A	X	V	S	Q	Y
23	K	I	G	D	Z	E	A	X	V	S	Q	M	Q	L	J	H	E	U	D	Z	W	U	R	P	X	N
24	H	F	C	Y	Z	D	W	U	R	P	L	P	K	I	G	D	T	C	Y	V	T	Q	O	W	M	J
25	E	B	X	C	Y	V	T	Q	O	K	O	J	H	F	C	S	N	X	U	S	P	N	V	L	I	G
26	A	W	B	X	U	S	P	N	J	N	I	G	E	B	R	A	W	T	R	O	M	U	K	H	F	D

Note the diagonal symmetries.

The reduction tableau is used in a different manner than say a Viggy square. In the Viggy square, the intersections of the columns and rows are the ciphertext equivalents. This is not true for the rotor reduction tableau of Figure 22-3. Instead, the intersection of the diagonals and the columns are used to locate the ciphertext. For example, the letter E in the 25th row of column A is actually the letter E from the 21st row and the fifth column. While the V in the first row of column A is actually the letter V of the 6th row and the 22nd column. The actual work of reducing a single rotor ciphertext letter into a monoalphabetic letter is not the same.

The most important part of this tableau is the first letter in each diagonal alphabetic sequence of the first column labeled A. The is especially true in the case of a reversing rotor.

Step 5 . Monoalphabetic ciphertext

The value of each ciphertext letter needs to be clarified. Each letter contains two distinct values. The first value is known as the positional value and is based on the position of each letter in the alphabetic sequence, A=1, B=2...Z=26.

The second value is the displacement value and represents the distance from the first letter in the alphabetic sequence. D has a positional value of four and a displacement of three. Displacement values range from 0 - 25 in English. See Figure 22-4.

Figure 22-4

Positional Value	Letter	Displacement Value
1	A	0
2	B	1
3	C	2
4	D	3
5	E	4
6	F	5
7	G	6
8	H	7
9	I	8
10	J	9
11	K	10
12	L	11
13	M	12
14	N	13
15	O	14
16	P	15
17	Q	16
18	R	17
19	S	18
20	T	19
21	U	20
22	V	21
23	W	22
24	X	23
25	Y	24
26	Z	25

When addition or subtraction is performed during the reduction operation, it modulus 26. These two values along with modular (complete cycle) arithmetic, is used to find which diagonal alphabet is being used for the monoalphabetic equivalent. The correct selection of the diagonal alphabet is based on the position of the rotor and the letter's displacement value.

d = (r + cd) (mod 26) forward rotor eq 22-1

d = (r - cd) (mod 26) reverse rotor eq 22-2

Now the first letter in the cryptogram is X. Substituting the values from Figure 22-4.

d = (r + cd) (mod 26)
  = (1 + 23) (mod 26)
  = 24

The letter at the head of the 24th alphabet is H and has a positional value of 8. Next, follow this sloping diagonal alphabet up to the letter X to obtain the proper intersecting column which is Q at the head of the column.

This is also true by the following equation:

mp = (1 - D(dp)) + cp) (mod 26) eq 22-3

where: D(dp) is the positional value of the letter in row d, and cp is the positional value in the ciphertext letter in the text.

mp = (1 - 8 + 24) (mod 26) = 17 = Q

This equation also works for the reversing rotor.

We repeat this step until all the ciphertext letters are replaced by their monoalphabetic letters. A new frequency distribution and Phi test is calculated to verify the results.

```
letter frequencies:

A  31   E  28   I 109  M  17   Q 154  U 58  Y 22
B  14   F 121   J  42  N  18   R  11  V 94  Z 71
C  45   G  27   K   1  O  31   S  93  W  0
D  93   H   0   L   1  P  39   T 195  X 71

Letters = 1393
Phi Values:
     Observed      =  136660
     Random        =   74653
     Non-Random    =  132621
```

You might guess that the T = E and the Q = T ?

Figure 22-5 shows the first three ciphertext lines converted:

```
CT X F S D O X I Z Y H S M D N J N J I L A F I N J L S
MT Q Z T X T D X T S F Y F X S C T J I V I F S P D N T
P  T H E R E A R E N O B O R N D E C I S I O N M A K E
```

Where CT = ciphertext, MT = reduced to monoalphabetic terms, P = plain.

```
CT S E O Y O P U Z S L E P M T H D R O S Q F O N J L W
MT X V M Z T Q Z T X M T U I N T I Q F X S F Q P D N I
P  R S W H E T H E R W E L I K E I T O R N O T M A K I

CT R Z Y T K I K Q L V Q F K K V L E J F D H I K I K R
MT S E D J Z F I J T I V D A D X Q F O Y T I S E Z G P
P  N G A C H O I C E I S A P A R T O F B E I N G H U M
```

I leave the rest to the student to solve.

HISTORY OF THE ECM MARK II

The ECM Mark II (also known in the Navy as CSP-888/889 or SIGABA by the Army) is a cipher machine used for sensitive communications. According to the National Maritime Museum, it was used aboard USS Pampanito to encipher messages from plain text into cipher text under the control of a key (encipherment). A cryptographic system consists of the combination of cipher machine, operating procedures and management of keys. If the system is well designed and implemented correctly, cipher text can only be converted back to plain text (deciphered) by someone with all three elements of the system.

In early September 1944 U.S. Fleet Radio Unit Pacific (FRUPAC) in Hawaii recorded a Japanese cipher radio message that originated from Singapore. Unknown to the Japanese, U.S. forces had analyzed many Japanese messages and as a result of much brilliant and hard work were able to cryptanalyze their enemy's inadequately designed and implemented cryptographic system. FRUPAC deciphered the message that announced the route of an important Japanese convoy from Singapore to Japan. The timing and expected path of the convoy from the message was enciphered on an ECM in Hawaii and sent to Pampanito where it was deciphered on an ECM. Although Pampanito's crew did not know how FRUPAC got its information, they were able to go directly to the convoy's path and attack with great efficiency. Pampanito's attack was kept secret by the superior U.S. cryptographic system that revolved around the ECM Mark II.

The ECM Mark II based cryptographic system is not known to have ever been broken by an enemy and was secure throughout WWII. The system was retired by the U.S. Navy in 1959 because it was too slow to meet the demands of modern naval communications. Axis powers (primarily Germany) did however periodically break the lower grade systems used by Allied forces. Early in the war (notably during the convoy battle of the Atlantic and the North Africa campaign) the breaking of Allied systems contributed to Axis success. [Refer to my Lecture 9 for more details.]

In contrast, the Allies were able to break Axis communications for most of the war supplying many of the targets attacked by Pampanito. Intercepted messages provided not only the location of potential targets, but often insight into the thinking of enemy commanders. In the Pacific, this information was critical to success in the battles of Midway and the Coral Sea in 1942.

However, intelligence, including cryptanalysis, can be a double-edged sword. The intercepted message that directed Pampanito to attack the convoy during September 1944 did not indicate that 2000 Australian and British P.O.W.s were aboard the Japanese ships. The full story of this attack and Pampanito's rescue of 73 P.O.W.s is found in the Third War Patrol Report in Appendix 1.

The combination of secure U.S. cryptographic systems and vulnerable Axis systems directly contributed the success of the Allied powers during WWII thereby shortening the war by years and saving countless human lives.

TWO VIEWS OF THE ECM MARK II'S DEVELOPMENT:

This account is taken from the National Maritime Museum Association material:

The ECM Mark II's critical cryptographic innovation (the Stepping Maze) over Hebern's and other precursors was created by Army cryptologists Frank B. Rowlett and William F. Friedman shortly before 15 Jun 1935. During October and November of 1935 Friedman disclosed the details of the "Stepping Maze" to the Navy's cryptologists including Lt. Joseph N. Wenger. Aside from filing secret patent application No. 70,412 on 23 March 1936 little additional development was performed by either the Army or Navy until Lt. Wenger discussed the patent with Cmdr. Lawrence Safford during the winter of 1936-37. Cmdr. Safford recognized the potential of the invention and the Navy began sponsoring and financing a new machine including the "Stepping Maze".

Additional innovations by Cmdr. Safford, Cmdr. Seiler and the Teletype Corporation including Mr. Reiber and Mr. Zenner added to the security, reliability and manufacturability of the ECM Mark II. Prototypes were soon delivered, and in February 1940 the machine's details were disclosed to the Army. Amazing as it may seem, the Navy had kept its continuing development of the machine secret from the Army. With minor changes suggested by the Army the machine was accepted as the primary cipher machine for use by both Army and Navy.

The joint Army-Navy ECM Mark II cryptographic system became effective on 1 Aug 1941, and the two services had the common high-security cryptographic system in place and in use prior to the attack on Pearl Harbor. The use of a common system was of great military value, particularly during the early stages of the war when the distribution of machines and codewheels was incomplete. By 1943, over 10,000 machines were in use. The "Stepping Maze" and use of electronic control were a generation ahead of the systems employed by other countries before and after WWII. No other country is known to have ever broken the ECM Mark II cryptographic system.

[DEVO] has a slightly different take on the subject as taken from pages 78-80:

"While the US Army had Friedman, a cryptographic superstar, the Navy had the less flamboyant Lawrence F. Stafford, who in 1924 laid the foundations for the wartime Navy's excellent but underrated cryptologic organization Op-20-G. The Navy experimented with numerous cryptographic machines, many based on the Hebern's original machine, beginning about 1925. It was soon appreciated that 'to produce a more varied course of code wheel movement than any now known' was an imperative in the design of both wired rotor machines and Baudot tele-enciphers. In addition, numerous

design features: ac/dc operation, ball point rotor contacts, weather resistance, reliable rotor positioning, and stepping, were of prime importance for a field machine, which no matter how cryptographically sound, was useless unless it operated well under adverse conditions.

After the modified Hebern machine was shown to be less secure than thought, a new cryptograph was designed and developed by the Navy during the years 1932-34. This wired rotor machine had five rotors each of whose movement was controlled by a pinwheel of 25 pins each set to 'active' or 'inactive' position. Further a small plugboard, which transferred control among the five rotors, was suitably plugged.

During operation, one or more rotors would 'step' one position for each letter enciphered. At each encipherment the rotor's corresponding pinwheel would advance one step. When an active pin was sensed opposite the moving rotor, then that rotor ceased to move and control was passed to the rotor indicated by the plugboard connections. A rotor could pass control to itself if desired. All in all, it was a clever design which could be highly secure provided enough rotors were in use (The Navy used five chosen from a set of ten), and the pinwheel settings were selected with care. This machine was designated the Electronic Cipher Machine (ECM) Mark I and would be the main high level Naval cryptograph during WWII had not the Mark II version been developed. At this point, Navy cipher machine design was showing quite a bit of sophistication. The Mark I would have provided adequate security for the US communications during the wartime era.

The Navy was also instrumental in pushing for the development of what became the US's top-level cipher machine of the 1940's era, the ECM Mark II, or simply, ECM for short (designated SIGABA by the Army). The original idea for the ECM had come from Friedman's assistant, Frank Rowlett {ACA member} and resulted in a secret patent application filed by Friedman and Rowlett.

The Navy, with plenty of funds for cipher machine development, and the Army, with its skilled machine cryptanalysts, working closely together achieved the early development of a production design of a highly secure cipher machine which would fully satisfy the requirements of both services for enciphering their most secret communications. This was a most fortunate circumstance, because the ECM Mark II could not have possibly have become operational by the advent of America's entry into WWII without the full cooperation of the two services, nor would the high degree of cryptographic security required for both services and the reliability of supply so essential for such a vitally important equipment have been attained." [DEVO]

NAVY SYSTEMS

The Navy commenced WWII with three principle cryptographic systems (besides codes): The ECM (for high level communications); a Hagelin machine adapted from the C-36 (1936), the CSP 1500 (for medium level communications); and a strip cipher (for tactical level communications and sometimes higher level signals). The ECM was in use during Corregidor when immense quantities of enciphered poems, baseball scores, et cetera, were sent to provide artificially high traffic levels to confuse the Japanese.

ARMY SYSTEMS

The Army used the ECM (SIGABA) and the five rotor wired wheel M-134-A (SIGMYK), which was driven by a one-time Baudot tape to control its rotor movements. The two-tape Vernam system was also used, being later replaced by the M-228 (SIGCUM), a five rotor teletype machine. The Hagelin C-38 (1938) (M-209) was used for tactical communications along with a variety of hand systems. The strip system was used extensively for all levels of communications. [DEVO]

COMBINED US - BRITISH SYSTEM - CSP1700

During the war communication between US and British was paramount in importance. Don Seiler of the Navy designed the adaptor system for the British Typex and the US ECM. It was called the CSP1600. The hybrid machine was designated the CCM for Combined Cipher Machine or CSP1700. At the conclusion of WWII, the CSP1700 was adopted by the US State Department for its highest level ciphers. [DEVO] It stayed in place for more than 10 years. [NICH]

DESTRUCTION OF A NATIONAL TREASURE

After newer, faster cryptographic systems replaced the ECM Mark II the machines were systematically destroyed to protect the secrets of their design. Today only a few ECM's still exist. The National Cryptologic Museum (a part of the National Security Agency) has 4 machines, one of which is on display in their Fort George Meade, MD museum. The U.S. Naval Security Group has 2 machines, one of which is displayed aboard Pampanito in San Francisco, CA. When recently contacted the US Army historians did not believe they had any machines.

USS PAMPANITO (SS-383)

USS Pampanito (SS-383) was a World War II Balao class Fleet submarine that has been preserved as a National Historical Landmark located at San Francisco's Fisherman's Wharf. Pampanito made six patrols in the Pacific during World War II and sank six Japanese ships and damaged four others. It is operated by the National Maritime Museum Association.

The USS Pampanito was featured in the 1955 film Down Periscope. A self-guided tour is narrated by Captain Edward L. Beach, noted historian and author of the submarine classic Run Silent, Run Deep. The USS Pampanito has its own web site where you can take a closer look at the many issues involved in managing a tactical submarine:

http://www.maritime.org

The ECM Mark II aboard Pampanito is on loan from the Naval Security Group. After cleaning, lubrication and minor repair it was put on display in July of 1996. It is currently the only fully operable ECM Mark II in existence. This machine was built in June of 1943 as a CSP-889, and sometime circa 1950 it was modified into a CSP-889-2900. The minor modifications added one switch and a knob that allow operation compatible with CSP-889 machines, or enhanced security when operated as a CSP-2900.

CIPHER EQUIPMENT ABOARD PAMPANITO DURING 1944:

A Channel is the combination of all the equipment, instructions, key lists, etc. that are needed for two parties to communicate in a cipher system.

Before leaving on each war patrol, one officer and one enlisted man armed with a machine gun would draw the cipher equipment from its secure storage. There were two lists of cipher equipment and manuals, List A included an ECM Mark II and associated documents (Channel 105), List B did not include the ECM. For most patrols List A was used, if the patrol was particularly dangerous and in shallow waters List B was used. The CSP-1500 (Channel 110) would also be added as needed to either the List A or List B. The lists below was used by submarines in the Pacific during 1944.

Channel 105

CSP-888/889 = ECM Mark II = M-134-C = SIGABA. This was the high grade, electro-mechanical, rotor wheel cipher machine and the physical component of the primary cryptographic system used by the United States. High grade cryptographic systems are those that we believe cannot be broken by an enemy in a useful period of time even if they are in possession of the physical elements of the system, provided the other elements of the system are preserved (i.e. keys are kept secret, operating procedures are well designed and followed, number and size of messages per key are small, etc.)

The first 651 units built were the CSP-888 model that lacked plugs necessary for tandem operation, but were otherwise identical to the later CSP-889 model.

CSP-890 = CSP-890(A) = SIGHEK Plugboard rotor for use in the CSP-888/889.
CSP-1100 ECM Instructions
CSP-1122 ECM Wheels
CSP-1190 ECM Key Lists.
CSP-1941 SIGLUR-1 Instructions for CSP-890
ENG-108 Print unit for a CSP-889.
ENG-109 ECM spare parts kit. Metal Safe Locker Type #8 - Special safe built into the radio room for CSP-889

Channel 108

CSP-845 M138A = CSP-1088. This was a low-medium grade, paper strip cryptographic system that was used by U.S. Submarines when they were on such dangerous missions that they could not risk the capture of an ECM, or if the ECM broke down. It was also used to communicate with forces that did not have an ECM. Medium grade cryptographic systems can be read by an enemy in possession of the physical elements of the system, even if the other elements of the system are preserved. The related CSP-488 system was used until mid 1943 by Naval forces.

CSP-847 Instructions for use of CSP-845 strip cipher.
CSP-1247/8 Key lists for use with strip cipher.

Channel 135

CSP-1403/4 Key lists.

Channel 143

CSP-1286 Two card style authentication cipher. CSP-1521 Authentication Instructions.

Channel 144

CSP-1270 SIGMEN = SIGYAP Chart style authentication cipher.
CSP-1272 Instructions for CSP-1270.

Channel 171

CSP-1524 Call sign instructions.
CSP-1525/26 Emergency use call sign instructions.
CSP-1750 Call device MK 2 Call sign cipher. CSP-1751 are CSP-1750 instructions.
CSP-1756 Strip cipher compatable with CSP-1750. Made of mahogany.
CSP-1752 Key lists.

Channel Weather

CSP-1300 Weather cipher.
CSP- Weather Handbook for Submarines.

Channel 110

CSP-1500 M-209 = C-38. This was a low-medium grade, Hagelin derivative, mechanical cryptographic system. Over 140,000 of these were used by Allied forces during the war and they were regularly broken by the enemy, primarily when the instructions for use were not followed. Pampanito would have used this to communicate with forces that did not have an ECM. Low grade cryptographic systems can be broken by an enemy by purely cryptanalytical means without possession of any parts of the system.

"CSP" stands for Code and Signal Publication, its usage started during WW I. Refer to Appendix 3 for other cryptographic indicators.

DETAILS OF THE ECM MARK II CIPHER UNIT:

Prior to the ECM Mark II many cipher machines incorporated encipherment by means of an electric current passing through a series of cipher wheels or rotors. A character is typed on a keyboard, passed through the rotors and either printed or displayed in a light board for the operator. The rotors are thin disks with contacts on each side that are wired at random to the other side one wire per contact.

Typically a rotor will have 26 contacts on each side, each contact representing a letter of the alphabet. A current passing through the rotor disk might enter in the position of letter B and exit in the position of letter G. Encipherment occurs by passing the current through several rotors that are side by side and rotating one or more of the rotors between each character enciphered. If the deciphering machine starts with rotors of the same design and in the same positions as the enciphering machine, it will repeat the motion of the rotors thereby deciphering the text. The most important difference between previous machines and the ECM is how the enciphering rotors are stepped.

The "Stepping Maze" uses rotors in cascade formation to produce a more random stepping of the cipher rotors than existed on previous electromechanical cipher machines. The rotor on left was a Cipher or Control rotor, and on right it was an Index rotor.

The ECM has fifteen rotors arranged in three rotor banks. The five rotors in the rear are the cipher rotors that convert a plain-text letter into a cipher-text letter as they are irregularly stepped. Electrical currents passing first through the control (middle) rotor bank and then through the index (front) rotor bank determine which cipher rotor(s) step. The center three of five control rotors step in a metered fashion. Control rotor 3 is the fast rotor and steps once for each character typed. Control rotor 4 is the medium rotor and steps once each time control rotor 3 completes a full rotation. Control rotor

2 is the slow rotor and steps once each time control rotor 4 completes a full rotation. Control rotors 1 and 5 do not step. The index rotors are positioned once each day and do not move while operating. The 10 cipher and control rotors are large 26 contact rotors that may be used interchangeably in the cipher or control bank and are reversible. The five smaller, 10 contact, index rotors are only used in the index bank. Four contacts are energized on the first rotor of the control rotor bank. The connections between the last rotor of the 26 contact control bank and the first rotor of the 10 contact index bank are in 9 groups of between 1 and 6 wire(s) each. One of the index bank contacts is not used. The 10 outputs of the last index rotor are attached in pairs to 5 magnets that step cipher rotors when energized. Between 1 and 4 cipher rotors are stepped for each character enciphered.

To properly encipher a message, the three banks of rotors must be arranged and aligned in such a way that they can be reproduced by the deciphering operator. The particular arrangement and alignment of the rotors selected by the enciphering operator and transmitted to the deciphering operator in disguised form constitutes the keying instructions.

The design of the ECM limited the erratic stepping so that at least 1, and not more than 4 cipher rotors step at a time. Even so, a crude, exhaustive search would require an enemy to check around 10 to the 14th permutations of code, index and control rotor starting positions. The combination of modern algorithms and the availability of high speed computers mean this system is no longer secure, but during its term of service it provided an unprecedented level of security.

SIGABA GROUPING OF OUTPUT FROM CONTROL ROTORS TO INDEX ROTORS

Wiring from the keyboard and to the printer used the normal alphabet, from A-Z around the 26-contact rotors instead of the QWERTY...NM. However pressing the Z actually sent an X, and pressing the space bar, sent the real Z. This provided for word spacing.

As reported by researcher John Savard: the grouping of the output from the control rotors to the index rotors differed for two models of the SIGABA.

For the CSP-889, the grouping was:

1- B
2- C
3- DE
4- FGH
5- IJK
6- LMNO
7- PQRST
8- UVWXYZ
9- A

For the CSP-2900, the grouping was:

0- UV
1- B
2- C
3- DE
4- FGH
5- IJK
6- LMNO
7- ST
8- WXYZ
9- A

The SIGABA stepped from 1 to 4 of the five cipher rotors, the five 26-contact rotors through which the plaintext traveled. There were usually four live contacts entering the five 26-contact control rotors. This resulted in four of the 26 output being live.

After these outputs are grouped, the index rotors which take two of the groups to the mechanism that moves one of the five cipher rotors.

If every one of the four live contacts on the output control rotors goes to a different group, and each of these groups is taken to a different cipher rotor by the index rotor setting, which does not change during encipherment, then four cipher rotors move.

In the CSP-889, the only way that fewer than four rotors will move is when the one live output goes either to the same group, or to two groups connected by the index rotors to one cipher rotor's movement mechanism.

Some groups connect together as many as six outputs from the control rotors, and as few as one.

A bad index rotor setting might connect inputs 7 and 8 to the index rotors to one cipher rotor, and inputs 1 and 2 to another. Then the first cipher rotor, connected to 11 control rotor outputs would be moving most of the time - it might be the only rotor moving. The second cipher rotor is connected to 2 control rotor outputs. Thus, it can never be the only rotor moving.

The CSP-2900 corrects this problem. Since three of the control rotor outputs are discarded -only three- there may be as few as one live input. Therefore, any rotor can be the only one to move. The number of control rotor outputs connected to the index rotor input still varies.

The actual wirings used for the 10 contact rotors were:

7591482630 3810592764 4086153297 3980526174 6497135280

For the CSP-2900, P, Q, and R were not connected in the groups. The steppers of the five cipher rotors are connected to the ten outputs of the index rotors as follows:

1 : 0,9
2 : 7,8
3 : 5,6
4 : 3,4
5 : 1,2

Appendices 1 - 5 contain detail working information on the ECM MARK II.

APPENDIX 1

USS PAMPANITO (SS-383)
THE THIRD WAR PATROL
AUGUST 17 - SEPTEMBER 28, 1944

On August 17, 1944 USS Pampanito was ready for sea. She had rendezvoused three weeks earlier with the submarine tender USS Proteus (AS-19) at Midway Island for repairs and supplies. During the standard refit period, which followed each war patrol, Pampanito was modified and repaired by the tender. Improvements included the installation of a radio key in the SJ radar circuit, a surface search device (so that the radar could also be used for communications), and the placement of charging equipment in the forward torpedo room which allowed the firing of Mark 18 electric torpedoes from the six forward tubes, an ability she already had in the after room. The brushes were replaced in all four of the 1600-horsepower electric main propulsion motors, and gaskets were replaced on the conning tower hatch, the main air induction valve, and the newly converted Fuel Ballast Tank #4A. Then final preparations were made for getting underway. Pampanito took on provisions, fuel, ammunition, and torpedoes.

Pampanito departed Midway again under the command of Lt. Commander Paul E. Summers and headed for her assigned patrol area in the Luzon Strait north of the Philippine Islands. This area was code named "Convoy College" because of the large number of Japanese convoys that converged there as they traveled north to Japan. Unlike her first two patrols when she operated alone, this time Pampanito traveled as part of a wolfpack which included USS Growler (SS-215), and USS Sealion II (SS-315). Wolfpacks became more common in the Pacific War as Japanese convoys became better organized and protected. Skippers used their radios sparingly, preferring to rendezvous regularly at pre-selected times using signal lights or megaphones instead. The structure of this pack, nicknamed "Ben's Busters" after tactical leader Commander T.B. "Ben" Oakley, included Oakley in Growler, Commander Eli T. Reich, second senior officer, in Sealion, and Summers in Pampanito.

En route to the patrol area the three boats exchanged recognition signals and tested communications via VHF radio. On August 19, Summers noted in his patrol report that he was having difficulty reaching Growler when the range exceeded

8,000 yards. He expressed doubts that successful communications could be maintained during a coordinated attack.

When "Ben's Busters" attacked a Japanese convoy in Bashi Channel off the southern tip of Formosa on August 30, they operated with another wolf-pack, "Ed's Eradicators". This group was comprised of tactical commander Captain Edwin Swineburne in USS Barb (SS-220), skippered by Commander Eugene Fluckey, and Commander Charles Loughlin in Queenfish (SS-393). While the two packs attacked the convoy, sinking seven ships and damaging others, Pampanito lookouts reported distant explosions and a burning ship over the moonlit horizon, followed by distant depth charges. No contact report was received from the two attacking wolfpacks, and Summers searched in vain for the remnants of the scattered convoy. Summers blamed communications problems for Pampanito's lack of participation in the attack.

During the next few days Pampanito developed a serious and perplexing mechanical problem. A loud air squeal had been heard up forward during a dive, and the diving officer reported 2000 pounds of water in the forward trim tank. No explanation could immediately be found because the noise was coming from inside the tank. On the night of September 4, Lt. Howard Fulton and Motor Machinist E.W. Stockslader, hoping to locate the source of the problem, volunteered to be sealed into the leaky tank while the boat dove. A signal system was set up, and Pampanito went down to 60 feet, yet the men in the tank found nothing. Summers took her deeper, to 200 feet, before the leak was finally found. The seal around the operating rod to torpedo tube #5 leaked as it passed through the forward bulkhead of the tank. The boat remained submerged during daylight hours for the next two days while blue prints were studied. Pampanito surfaced at night to allow the leak to be repaired. First Class Gunners Mate Tony Hauptman, an amateur diver, volunteered to perform the repair. He used shallow water diving apparatus to get below the waterline under the superstructure. During repeated dives, Hauptman fixed the noisy leak using a specially made wrench. Pampanito was then again able to maneuver silently while submerged, allowing the war patrol to resume without having to turn back to Midway for repair.

Pete Summers celebrated his thirty-first birthday at sea on September 6, 1944 , the same day an ill fated enemy convoy left Singapore bound through "Convoy College" to Japan. The convoy carried war production materials such as rubber and oil. It also carried over two thousand British and Australian prisoners of war being transported from Southeast Asia following the completion of the Burma-Thailand railroad.

This infamous "Railway of Death", as it became known, was used by the Japanese to move troops and supplies 250 miles through the mountainous jungles of Thailand and Burma connecting with other lines running through Southeast Asia and out to the South China Sea. The railway had been built at a huge cost of human life. An estimated 12,000 British, Australian, and many times that number of Asian prisoners died from jungle diseases, lack of medical care, starvation, abuse and overwork. The fittest of the railway survivors, known as the "Japan Party", were being relocated to work as forced labor in the copper mines of Japan. The POWs were openly worried about the likelihood of being torpedoed en route by American submarines and made what slim preparations they could for that strong possibility. Some formed teams and planned escape routes off the ship; others stockpiled meager rations or tested the effects of drinking small amounts of sea water. The Japanese could have requested safe passage for the transfer of prisoners, but no such request was received.

FRUPAC, the Fleet Radio Unit Pacific, intercepted and decoded a Japanese message detailing the course and estimated noon positions of the convoy along the route to Japan. On the night of September 9, the "Busters" were ordered to rendezvous on September 11, and to intercept the convoy. Later that night, the "Eradicators" were ordered to act as backstop and to move in on the convoy, as well. Growler, first to arrive at the meeting point on the night of the 11th, found light overcast and calm seas with rain on the horizon. Sealion surfaced nearby around 2000 hours, having just returned from Midway where her torpedoes, fired during the August 30th attack were replaced. Pampanito moved in an hour and a half later. The boats exchanged recognition signals with the SJ radar and moved within 100 yards of Growler to receive vocal instructions for the attack. The wolfpack moved to the expected position of the approaching convoy.

At 0130 on the morning of September 12, Pampanito's ace radar technician, George Moffett, picked up several pips on the screen at a range of over fifteen miles. A few minutes later, a contact report was received from Growler, but the message was garbled and could not be decoded. Summers went flank speed to maneuver ahead of the convoy and into attack position. Growler approached from the west and fired on the ships, causing the convoy's escorts to fan out in all directions. Growler's attack was a first and last in US submarine history. Oakley had been picked up on radar by the Japanese destroyer Shikinami as he moved in to attack. The destroyer charged the sub. Instead of diving his boat and taking evasive measures Oakley faced the oncoming escort bow to bow, firing three torpedoes at the vessel from a range of just over 1000 yards. The first torpedo hit, causing a violent explosion. The destroyer, listing badly, charged ahead, coming so close to Growler that Oakley felt the heat from the burning ship. Shikinami finally went under, sinking only 200 yards from Growler. This controversial bow to bow surface attack on a charging destroyer has never been successfully repeated and is considered to be unnecessarily dangerous. However, Growler escaped and went on to damage two other ships before moving out of range to reload her torpedo tubes.
A bright quarter moon had risen and, at 0230, Summers moved to the dark side of the scattered convoy. Sealion pulled

back to repair a jammed automatic gyro setter, a device which is used to set the angle of the torpedo run. Growler lost the track of the convoy temporarily, and "Ed`s Eradicators", Queenfish and Barb, were 80 miles to the north; since they had not received the contact reports alerting them to the battle taking place to the south. Pampanito and Sealion tracked the convoy for the remainder of the night, both boats moving into attack range just before dawn.

As Summers prepared to fire from a perfect position, Pampanito was jolted by a series of violent explosions which occurred as Sealion, to the west, fired two salvos of three torpedoes each at the convoy. The first salvo scored three hits on a large, heavily laden tanker which erupted into flames so bright they illuminated the second target, the transport Rakuyo Maru.

Rakuyo Maru was a 477-foot Japanese-built passenger-cargo vessel carrying a load of raw rubber and, unknown to the crews of the submarines, also carried over 1300 Allied prisoners of war. Two of Sealion's torpedoes hit the POW ship, one amidships and one in the bow. It took 12 hours for Rakuyo Maru to sink, which allowed the surviving POWs some time to make rafts and search the doomed ship for food and water. The Japanese guards had left the ship immediately after the attack using most of the lifeboats.

Sealion went deep to avoid the depth charging that followed the attack. The other two subs tracked the convoy as it zig-zagged radically to avoid being attacked. Growler caught up with and sank another Japanese escort, the frigate Hirado. The POWs, who were now in the water clinging to wreckage, had mixed feelings as the small escort instantly sank. Some cheered another score against their captors; others saw all chances of rescue sink with that ship. Tragically, many survivors of the initial attack were killed or badly wounded by shock waves caused by the explosions of Hirado's sinking, and the following depth charge attack on Sealion.

Pampanito again picked up the convoy on high periscope (using the periscope fully extended while on the surface to increase viewing range) at noon the next day, and tracked it westward. Just after dark, Summers moved in for a surface attack, but had to pull the sub back when he learned that the torpedo in tube #4 had moved forward in the tube and had a "hot run" (the torpedo engine was running inside the tube at high speed being held back by the closed outer door). Although the warhead of a torpedo was designed to be unarmed until it had run through the water for a few hundred feet, the crew knew that torpedoes could be temperamental.

Pampanito was pulled back to disengage a jammed gyro setter caused by the hot run. Summers then quickly moved in again to setup the attack with the dud torpedo still in tube #4. A few minutes later the boat was once again in position.

" 2240 Fired five torpedoes forward; three at large transport and two at large AK.... Swung hard right and at 2243 Fired four stern tubes; two at each of the two AK's in the farthest column. Saw three hits in large AP, two hits in large AK (Targets no. 1 and 2) and one hit in AK (farthest column) heard and timed, hit in fourth AK (leading ship in farthest column).... In all, seven hits out of nine torpedoes. From the bridge we watched both the large AP and the large AK (the one with two hits) sink within the next ten minutes, and saw the after deck house of the third ship, on which we saw one hit, go up into the air with the ship smoking heavily. The fourth ship could not be observed because of much smoke and haze in that direction. A short interval after the seven hits, the escorts started dropping depth charges at random, but for once we didn't mind."

Pampanito had sunk a 524 foot transport Kachidoki Maru, a captured American vessel built in New Jersey in 1921. First owned by the United States Ship Line, and later the Dollar Line, she had originally been named Wolverine State. After having been sold to American President Lines, she was renamed President Harrison. When captured off the China coast by the Japanese, she was given the name Kachidoki Maru. Like the Rakuyo Maru, the ship had been carrying raw materials to Japan. Also aboard were 900 Allied POWs.

Following the attack, Pampanito pulled away to eject the hot run torpedo and reload all tubes. An hour later, in another attack, Summers missed with three shots fired at a destroyer escort. He also observed two small ships, one of which had stopped, apparently to pick up survivors of the earlier attack. He decided they were too small to waste time and a torpedo on, and he moved on to rejoin the pack on the following night. No immediate attempt was made to track down the remaining stragglers from the convoy.

The wolfpack rendezvoused the night of September 13th. Growler moved south while Sealion and Pampanito spent the next day in vain looking for the rest of the convoy, then headed east toward the area of the September 12th attack on Rakuyo Maru. After diving to avoid a plane late in the afternoon of the 15th Pampanito surfaced to find much debris and floating wreckage.

" 1605 A bridge lookout sighted some men on a raft, so stood by small arms, and closed to investigate. 1634 The men were covered with oil and filth and we could not make them out. They were shouting but we couldn't understand what they were saying, except made out words "Pick us up please." Called rescue party on deck and took them off the raft. There were about fifteen (15) British and Australian Prisoner of War survivors on this raft from a ship sunk the night of 11-12 September, 1944. We learned they were enroute from Singapore to Formosa and that there were over thirteen hundred on the sunken ship."

These men were survivors of Rakuyo Maru, sunk earlier by Sealion. After four days of drifting on makeshift rafts they were in extremely bad shape. Most were covered with oil from the sunken tanker, and had long since used up what little food and water they had with them. Slowly, the story of what had occurred was unveiled by the survivors brought aboard Pampanito. Summers radioed Sealion, and Reich also moved in to pick up survivors. Again from the patrol reports:

"1634 As the men were received on board, we stripped them and removed most of the heavy coating of oil and muck. We cleared the after torpedo room and passed them below as quickly as possible. Gave all men a piece of cloth moistened with water to suck on. All of them were exhausted after four days on the raft and three years imprisonment. Many had lashed themselves to their makeshift rafts, which were slick with grease; and had nothing but lifebelts with them. All showed signs of pellagra, beri-beri, malaria, immersion, salt water sores, ringworm, etc. All were very thin and showed the results of under nourishment. Some were in very bad shape.... A pitiful sight none of us will ever forget. All hands turned to with a will and the men were cared for as rapidly as possible.

1701 Sent message to Sealion for help.
1712 Picked up a second raft with about nine men aboard.
1721 Picked up another six men.
1730 Rescued another six men.
1753 Picked up about eleven men.
1824 ...about six men.
1832 ...about five men.
1957 Light fading rapidly as we picked up a single survivor.
2005 Completely dark as we took aboard the last group of about ten men. Had made a thorough search of our vicinity with high periscope and kept the true bearings of all rafts sighted. Felt we had everyone in sight and knew we had all we could care for if not more. When finally we obtained an exact count, the number of survivors on board was 73. These together with 79 members of our crew plus 10 officers make us a little cramped for living space.
2015 Made final search and finding no one else set course for Saipan at four engine speed."

The crew of Pampanito spent four hours rescuing as many survivors as could be found. Under the direction of torpedo officer Lt. Ted Swain, volunteer teams were formed to get the almost helpless men aboard. Some of Pampanito's crew dove into the water with lines to attach to the rafts so hey could be brought in close enough for others, on deck and on the saddle tanks to carefully lift the men aboard. Among those crew members who swam out to rescue the former POWs, leaving the relative safety of the sub and risking being left behind if the boat had to dive, were Bob Bennett, Andrew Currier, Bill Yagemann, Gordon Hooper, Jim Behney, and Tony Hauptman. It was a tense and emotional moment as the shocked crew worked to save as many of the oil soaked survivors as possible. During the rescue many of the crew came topside to help. If a Japanese plane attacked at that time they would have been left on deck as Pampanito dove to avoid attack.

Personal cameras were not allowed on submarines. However, it was fortunate that a couple of contraband cameras were produced by the crew. Electrician Mate First Class Paul Pappas, Jr. was able to document the historic rescue with an amazing series of photographs and a 16mm film using the ship's movie camera.

During the five-day trip to Saipan, the nearest Allied port, the survivors were berthed in the crew's quarters amidships and on the empty torpedo skids and bunks in the after torpedo room where they were cared for by the crew. Some of the survivors were critically ill and in need of medical attention. Submarines carried no doctor on board, so the monumental task of treating these men became the responsibility of the only man on board with training in medicine, Pharmacist Mate First Class Maurice L. Demmers. With the help of crew members who fed the men and donated clothing, Demmers worked around the clock. Of the survivors, Britisher John Campbell, was the most seriously ill. Demmers worked continually in an attempt to save the delirious Campbell, but he died the next day, September 16. He was buried at sea following a somber ceremony; Paul Pappas read a heartfelt prayer. At one point, as Demmers tried to get a few hours sleep, several of the survivors took a turn for the worse, and he had to be awakened. Demmers continued his grueling work until he came dangerously close to total exhaustion. However, his efforts were rewarded; Campbell was the only casualty.

In a letter written after the war Demmers said "...as I examined and treated each one I could feel a deep sense of gratitude, their faces were expressionless and only a few could move their lips to whisper a faint 'thanks'. It was quite gratifying to see the happy expressions on their faces when they left the ship."

Before leaving for Saipan, Summers sent off a message to Pearl Harbor relaying what had happened, and requested that more subs be called in to continue the rescue. The only other boats in the area were Queenfish and Barb; they were ordered in as soon as possible. Both boats were 450 miles west in pursuit of a convoy, but when they received the new orders they dropped the track and headed full speed to the rescue area.

During the night of September 16th they encountered a convoy of large tankers and, among the escorts, a small aircraft carrier. The subs attacked the convoy and Barb quickly sank the carrier Unyo and an 11,000-ton tanker. After which they continued on to the rescue area.

Queenfish and Barb arrived at 0530 on the 17th to begin their search for rafts among the floating debris. Just after 1300 they located several rafts and began to pick up the few men still alive. They only had a few hours to search before a typhoon moved in, sealing the fate of those survivors not picked up in time. Before the storm hit, Queenfish found 18 men, and Barb found 14. The boats headed on to Saipan after a final search following the storm revealed no further survivors.

Of the 1,318 POWs on the Rakuyo Maru sunk by Sealion, 159 had been rescued by the four submarines; 73 on Pampanito, 54 on Sealion, and the 32 found by Queenfish and Barb. It was later learned that the Japanese had rescued 136 for a total of 295 survivors. Of the 900 POWs on the Kachidoki Maru sunk by Pampanito, 656 were rescued by the Japanese and taken to prison camps in Japan. Over 500 of these men were released by American troops in August, 1945 at the close of the war.

On September 18th, as Pampanito traveled to Saipan, she was met by the USS Case (DD 370) and took aboard a pharmacist mate, medical supplies, and a doctor. Yet, Maurice Demmers, who had saved so many lives, continued to care for the former POWs. On the morning of the 20th, Pampanito was met by the USS Dunlap (DD-84) which escorted Pampanito into Tanapag Harbor, Saipan, where she docked alongside the submarine tender USS Fulton (AS-11). Fresh fruit and ice cream were brought aboard for the survivors as preparations were made for off-loading them to the Fulton. The transfer was complete by 1100 that morning as Pampanito's crew bid farewell to the grateful and much improved former POWs.

Pampanito took on fuel and provisions and left for Hawaii at 1600 that afternoon. Pampanito arrived for refit at Submarine Base, Pearl Harbor on the 28th of September at 1000 hours. Summers and his crew were given high praises for their unprecedented rescue, unique in submarine history, and for a successful war patrol which had earned the combat insignia. The combined total tonnage sunk of the two wolfpacks was the highest to date in the war. Pampanito was credited with sinking three ships. Summers was awarded the Navy Cross, as were skippers Loughlin, Fluckey, Reich, and Swineburn. Fluckey went on to become the most highly decorated submariner of the war. The Navy and Marine Corps Medal was awarded to those who swam out during the rescue, as well as to pharmacist mate Demmers. The three men involved in the repair at sea of the leaky trim tank received Letters of Commendation.

APPENDIX 2

Replica Operating Instructions for ASAM 1 (a.k.a. ECM Mark II)

Below is a replica of the instructions for operating the ECM Mark II as written by the Army in 1949.

By 1949 the designation of the ECM Mark II by the Army was ASAM 1/1. The names of several of its parts were renamed as well, but these are generally obvious in their use. The normal keying shown here is essentially compatible with the final wartime keying. The emergency keying is not the same, during the war a CSP-890 was carried and it was used for emergency keying.

CONFIDENTIAL Reg. No. 30

Registered Cryptodocument

DEPARTMENT OF THE ARMY WASHINGTON

ASAM 1/1

CRYPTO-OPERATING INSTRUCTIONS FOR ASAM 1

This document consists of 27 numbered pages and cover

Verify upon receipt

1

ASAM 1/1

DEPARTMENT OF THE ARMY
Washington 25, D. C.
1 October 1949

1. This document, ASAM 1/1, "Crypto-operating Instructions for ASAM 1," is published for the information and guidance of all concerned.

2. Comments or recommendations concerning the instructions contained herein are invited and may be submitted to the Chief, Army Security Agency, The Pentagon, Washington 25, D. C., Attn: CSGAS-83. Direct communication for this purpose is authorized.

(AG 311.5 (30 Oct 43) OB-S-B)

BY ORDER OF THE SECRETARY OF THE ARMY:
OMAR N. BRADLEY
Chief of Staff

OFFICIAL:
EDWARD F. WITSELL
Major General
The Adjutant General

2

RECORD OF CHANGES

Change No.	Date Entered	Entered By
1	1 Nov 1949	M. Fishbow

3

(BLANK)

4

TABLE OF CONTENTS

CRYPTO-OPERATING INSTRUCTIONS FOR ASAM 1
SECTION I
GENERAL

1. Introduction.

a. This document, ASAM 1/1, "Crypto-operating Instructions for ASAM 1," is CONFIDENTIAL and registered, and will be handled accordingly. It contains basic instructions for the operation of ASAM 1, formerly Converter M-134-C (short title: SIGABA). Cryptosystems employing ASAM 1 are Category A.

b. Instructions concerning the processing of classified messages in a cryptocenter and information regarding general cryptographic procedures are contained in the document ASAG 2, "Cryptographic Operations."

c. No persons will be permitted to operate ASAM 1 unless they have been properly cleared for cryptographic duties in accordance with the provisions of current directives and have either read this document and ASAG 2 or been instructed by authorized personnel.

d. The document SIGKKK-2 should be consulted for detailed information relative to maintenance and power requirements of the machine and identification of mechanical parts.

2. Distribution.-This document is issued to holders of cryptosystems employing ASAM 1 with ASAM 1A as designated by the Department of the Army.

3. Accounting and Disposal.-Reports of possession, transfer, or destruction of this document will be forwarded as RESTRICTED correspondence, listing the document by the title ASAM 1/1 and register number only, to one of the following, whichever is applicable: (A) the Chief, Army Security Agency, The

Pentagon, Washington 25, D. C., Attn: CSGAS-82, (B) the Chief, Army Security Agency, Europe, Pacific, or Hawaii, or (C) the Signal Officer of the major

5

---

command headquarters which has been authorized by the Chief, Army Security Agency, Department of the Army, to act as command issuing office for this document in accordance with existing procedures Reports of loss or compromise will be made in accordance with the provisions of Chapter Five of the document ASAG 2. Instructions for the eventual disposal of this document will be issued at an appropriate time by the Chief, Army Security Agency, Washington D. C.

4. Effective Date.-This document is effective 1 October 1949 and at that time supersedes "Crypto-operating Instructions for Converter M-134-C" (short title: SIGQZF-3). One month after the effective date of this publication, SIGQZF-3 will be destroyed by burning and report of the destruction forwarded to the appropriate office of issue.

6

SECTION II
DESCRIPTION

5. Description and Use.-ASAM 1 is an electromechanical, transportable cipher machine to be used for automatically enciphering and deciphering messages, both tactical and administrative, with speed, accuracy, and security. The machine is CONFIDENTIAL and registered.

6. Component Parts.-The operator is directly concerned with the following component parts.

a. The keyboard resembles a typewriter keyboard and can be operated at a maximum speed of 45 to 50 words per minute (40 words per minute in tandem operation); if this speed is exceeded, characters may fail to print. The keyboard consists of 26 alphabet keys, 10 numeral keys, a "Repeat" key, a "Blank" key, a "Dash" key, a space bar and a dummy key. The "Blank" key permits advancing of the rotors without causing any resultant to be printed. The "Repeat" key permits continuous operation of the machine with or without printing.

b. The positions of the controller and their effect on the operation of the machine are as follows:

(1) Off Position ("O").-The power supply line is open and no current is supplied to the machine.

(2) Plain-text Position ("P").-All keys of the keyboard (except the dummy key) and the space bar are operative, and the machine will print plain text exactly as typed. The rotors remain motionless during typing.

(3) Reset Position ("R").-Only the numeral keys 1 to 5, inclusive, and the "Blank" and "Repeat" keys are operative. The rotors may be zeroized with the controller in this position and the zeroize-operate key in the "Zeroize" position (see par. 12a(3)). The tape will not feed while the controller is at "R." When the controller is moved to or through the "R" position, the tape-feed ratchet resets so that printing will begin on the first letter of a five- letter cipher group. Therefore, the tape may advance as many as five spaces.

(4) EnCipher Position ("E").-The alphabet, "Blank," and "Repeat" keys and the space bar are operative. Numeral and "Dash" keys are inoperative. The machine enciphers the letters struck on the keyboard and prints then resulting cipher text.

(5) Decipher Position ("D").-The alphabet, "Blank," and "Repeat" keys are operative. Numeral and "Dash" keys and the space bar are inoperative. The machine deciphers the letters struck on the keyboard and prints the resulting plain text.

7

---

c. The key located on the left front of the machine is the zeroize-operate key. The key is positioned at "Zeroize". when it is desired to align automatically all alphabet and stepping control rotors to the letter "0." The key is positioned at "Operate " at all other times.

d. The cipher unit ASAM 1A is detachable and consists of six upright bakelite separators which form a support for three rotor shafts. The unit supports the index, stepping control, and alphabet rotors in such relative positions that electrical circuits are formed through each row of rotors. The cipher unit, exclusive of rotors, is CONFIDENTIAL and registered.

e. The cipher unit ASAM IB is detachable and consists of six upright bakelite separators which form a support for one rotor shaft. Positions for five rotors are thus provided. The cipher unit, exclusive of rotors, is CONFIDENTIAL and registered; Instructions for the operation of ASAM 1 with cipher unit ASAM IB are contained in ASAM 5/1, "Crypto-operating Instructions for ASAM 5." The ASAM 1 with ASAM IB is referred to as the Combined Cipher Machine.

7. Rotors.

a. Sets of ten large rotors are issued for use with cryptosystems employing ASAM 1. The rotors are SECRET and registered. Each set of rotors is identified by a title and a number. In addition, each rotor is identified as belonging to a specific series by means of a letter-number pattern stamped on the rotor, usually opposite the letter "0." The pattern consists of any letter or any two-letter combination plus the numbers 1-10, 11-20, 21-30, etc. Each rotor bears a complete alphabet engraved in normal sequence on its periphery. The large rotors are all interchangeable and reversible.

(1) Five rotors are arranged in the middle row of the cipher unit and are known as the stepping control rotors. The two end rotors remain stationary during encipherment and decipherment.

(2) Five rotors are arranged in the rear row of the cipher unit and are known as they alphabet rotors. All five rotors advance in an irregular manner during encipherment and decipherment.

b. The five small rotors positioned in the front row of the cipher unit are known as index rotors. These rotors are a permanent part of the cipher unit and can be moved manually only. Each of the index rotors bears engraved on its periphery a sequence of numbers. One rotor is marked with the sequence 10 to 19 inclusive; another, the sequence 20 to 29 inclusive, etc. The complete set of five index rotors is numbered from 10 to 59 inclusive. The index rotors are always used in a fixed order in the five rotor positions (10-19, 20-29, 30-39, etc.). The index rotors are classified CONFIDENTIAL.

8. Power Requirements.-The machine is normally operated from a 105-125-volt a. c. (50 or 60 cycle) or d.c., power supply. Interchangeable motors are provided to utilize either type of power.

8

SECTION III
KEYING INSTRUCTIONS

9. Key List.-A key list, prepared in monthly editions and containing data essential to operation of ASAM 1, is used with each cryptosystem. The key list contains the following information:

a. Arrangement of the stepping control and alphabet rotors for each day of the month.

b. Alignment of index rotors for SECRET, CONFIDENTIAL, and RESTRICTED messages for each day of the month.

c. 26-30 check groups for SECRET, CONFIDENTIAL, and RESTRICTED classifications.

d. System indicators for SECRET, CONFIDENTIAL, and RESTRICTED messages.

Day of Month	ROTOR ARRANGEMENT (for all classifications) Stepping Control (Middle)	Alphabet (Rear)	SECRET Index(Front) Alignment	26-30 Check Group
1	OR 4 6 2R 7	1 8 5 9 3R	10 23 31 49 5	R N H V C
2	2 3R 9R 1 5	6 4R 8 7 0	14 25 33 46 59	S E M N O

Figure 1.-Sample Key List

Day of Month	CONFIDENTIAL Index(Front) Alignment	26-30 Check Group	RESTRICTED Index(Front) Alignment	26-30 Check Group
1	12 28 31 44 53	P W V M T	17 25 36 43 58	M C S D T
2	15 20 32 48 56	E H E W B	10 27 34 42 56	R S T H H

Figure 2.-Sample Key List

---

10. Rotor Arrangement.-The ten rotors used each day are arranged in the middle and rear positions of the cipher unit in accordance with the key list applicable to the cryptosystem. (See sample key list in fig. 1.) Single-digit numbers in the ROTOR ARRANGMENT column of the key list refer to the units digit of the number on the periphery of the rotors. The number 1 indicates that rotor number 1 (or 11 or

21, etc.) is to be used; the number 5, rotor number 5 (or 15, or 25, or 35, etc.); the number 0, rotor number 10 (or 20, or 30, etc.). The letter "R" appearing after a rotor number in the key list indicates that the rotor so designated is to be inserted in a reversed position, i. e., with the letters on the rotor appearing upside down to the operator as he faces the machine. Arrangement of the rotors may be illustrated by means of an example: In the sample key list, the rotor arrangement for the 2d of the month is 2 3R 9R 1 5 for the stepping control rotors and 6 4R 8 7 0 for the alphabet rotors. Rotors marked 2, 3, 9, 1, and 5 (disregarding the tens digits) will be inserted in the control position in that order, from left to right, as the operator face the converter, with rotors number 3 and 9 reversed. The remaining five rotors marked 6, 4, 8, 7, and 0 will be inserted in the alphabet position in that order from left to right, with rotor number 4 reversed.

CAUTION: Do not touch rotor contacts when arranging the rotors.

11. Alignment of Index Rotors.- The sets of numbers in the key list under INDEX (FRONT) ALIGNMENT designate the alignment of the index rotors. In three separate columns, each headed INDEX. (FRONT) ALIGNMENT, the key list give the daily alignment of the index rotors for each classification. The alignment of the index rotors is determined by the classification of the message and the day of the month. The index alignment for SECRET messages will also be used for messages classified TOP SECRET. Example: According to the sample key list (fig. 1), on the first day of the month the numbers of the index rotors should be aligned from left to right on the white reference mark at 10 23 31 49 50 for SECRET message; at 12 28 31 44 53 for CONFIDENTIAL messages; and at 17 25 36 43 58 for RESTRICTED messages.

12. 26-30 Check.-The key list contains 26-30 check groups by which the correctness of each rotor arrangement and index alignment and the operation of the machine are checked.

a. The 26-30 check is accomplished in the following manner:

(1) Insert the rotors according to the rotor arrangement for the specific date.

(2) Align the index rotors in accordance with the security classification and the specific date.

(3) Zeroize the rotors. This is accomplished by switching the zeroize-operate key to "Zeroize," turning the controller to "R," then pressing down the "Blank" and "Repeat" keys simultaneously until the letter "0" on each stepping control and alphabet rotor comes to rest at the reference mark.

(4) Set the stroke counter at zero.

(5) Switch the zeroize-operate key to "Operate" and turn the controller to "E."

(6) Press down the "Repeat" and "A" keys simultaneously and hold until 30 letters are printed.

(7) Compare the 26th through the 30th letters of the resultant encipherment with the appropriate 26-30 check group in the key list. For example, assume that the rotors of an appropriate set had been arranged and aligned in accordance

---

with the sample key list (fig. 2) for CONFIDENTIAL traffic for the second day of the month. If the 26-30 check procedure is followed correctly and the machine is operating properly, the 26th, 27th, 28th, 29th, and 30th letters will be E H E W B. Any deviation from the check group in the key list necessitates a complete recheck of the above procedure.

b. If the 26-30 check cannot be obtained, an error in the rotor arrangement, dirty contacts, or faulty mechanical operation may be the cause. If it appears that the error is caused by faulty mechanical operation, the machine should be checked by trained maintenance personnel.

NOTE : Care should be exercised whenever rotors are aligned to insure that the letter to be aligned on each rotor is directly in line with the white reference mark. If a rotor is off center, i. e., aligned halfway between two letters, the machine may not operate or monoalphabetic substitution encipherment may result.

c. The 26-30 check will be accomplished :
(1) After each change of the rotor arrangement.
(2) After each change of the index alignment.
(3) Each time the cipher unit is inserted in the machine prior to encipherment or decipherment.

13. System Indicator.-System indicators are the five-letter groups indicated in the key list for SECRET, CONFIDENTIAL, and RESTRICTED classifications. The system indicator identifies the specific ASAM 1 cryptosystem used to encipher a message, the classification of the message, and thereby the rotor arrangement and index rotor alignment to be used. The SECRET system indicator will also be used for messages classified TOP SECRET. The abbreviation TOPSEC will be buried near the beginning of the plain text during encipherment. The system indicator is never enciphered.

14. Message Indicator.-The message indicator consists of five letters selected at random by the operator. Bona fide five-letter words will not be used as message indicators even though such words occur by chance. The message indicator will be different for each message or part. When it is necessary, as in the case of a service, to reencipher a particular message or part, or any portion thereof, a different message indicator will be selected. The message indicator is used to determine the message rotor alignment as shown in paragraph 15.

15. Message Rotor Alignment.-The alignment of the stepping control and alphabet rotors at the beginning of encipherment or decipherment constitutes the message rotor alignment. The message rotor alignment is derived by the following procedure:.

a. Select five letters at random. The five letters will be the message indicator. Letters of the alphabet in proximity to the letter "O" i.e., L, M, N, or P, Q, R, will not be deliberately or consistently selected in the message indicator merely to reduce the number of steps required to align the letters of the message indicator on the stepping control rotors as explained below.

b. Zeroize the rotors(see par. 12a(3)).

c. Leave the controller at "R" and switch the zeroize- operate key to "Operate."

11

---

d. Strike the numeral "1" key the number of times required to align the first stepping control rotor (next to the left-end plate) to the first letter of the message indicator. The first stepping control rotor will advance one letter each time the "1" key is depressed.

e. Align the second stepping control rotor by striking the numeral "2" key, the third by striking the numeral "3" key, etc., until all five stepping control rotors are aligned to the five letters of the message indicator. The alphabet rotors will advance in an irregular manner with each operation of the numeral keys.

NOTE : If the letter "0" is to be aligned on any of the five stepping control rotors, it will be necessary to advance that rotor 26 times when setting up the message indicator.

f. If any rotor is advanced past the correct letter or if the rotors are not aligned in proper sequence, the entire process must be repeated from the zeroize position. Do not use the "Repeat" key with the numeral keys in aligning the message indicator and avoid a sharp, quick touch of the numeral keys. It is possible to strike the numeral keys too quickly so that the alphabet rotors will advance but the stepping control rotors will not, thus resulting in an incorrect alignment.

g. After the stepping control rotors have been aligned, check the alignment of the alphabet rotors to insure that all five are not aligned to the letter "0." The alphabet rotors should advance in an irregular manner while the stepping control rotors are being aligned. If all of the alphabet rotors remain aligned to the letter "O" it is an indication that the machine is not functioning properly or that the procedure outlined herein has not been followed correctly.

12

SECTION IV
OPERATING PROCEDURE

16. Division into Parts.-If the enciphered text of a message will exceed 350 five-letter groups, the plain text will be divided into parts so that no part will exceed 350 cipher- text groups. A different message indicator will be selected for each part.

17. Sequence of Operations in Encipherment.-After the message has been divided into parts, if necessary, and bisected, it will be enciphered according to the following sequence of operations.

a. Prepare the machine for operation in accordance with paragraphs 10, 11, and 12, referring to the appropriate effective key list to determine the correct rotor arrangement, the index rotor alignment for the classification of the message, and the 26-30 check.

b. Select at random the message indicator and determine the message rotor alignment in accordance with paragraph 15.

c. With the controller at "P," type the message heading, space several times, and type the system indicator and the message indicator. Phoneticize the message indicator.

d. With the rotors aligned to the message rotor alignment, turn the controller to "E" and set the stroke counter at zero.

e. Type the message text to be enciphered, employing variable spacing. If the last group of cipher text does not contain five letters, strike the space bar once and, if necessary, type enough different letters to complete the group.

f. Turn the controller to "P" and type the system indicator.

g. Press the right tape release marked "PRESS" and withdraw the tape until all printing has cleared the tape chute. Tear off the tape.

18. Sequence of Operations in Decipherment.

a. Prepare the machine for operation in accordance with paragraphs 10, 11, and 12, referring to the effective key list as designated by the system indicator for the correct rotor arrangement, the index rotor alignment for the classification of the message, and the 26-30 check.

b. Determine the message rotor alignment in accordance with paragraph 15.

c. With the rotors aligned to the message rotor alignment, turn the controller to "D" and set the stroke counter at zero.

d. Type the cipher text of the message, exclusive of indicators. Disregard spaces between groups; the space bar is inoperative while the controller is at "D." The

---

plain text will be printed on the tape in normal word lengths except where variable spacing was employed in encipherment. Note that X will always be printed in the place of Z, e.g:, ZERO will decipher as XERO, ZONE as XONE. In the event the deciphered text is garbled either from the beginning or after some plain text has been printed, attempt to determine the cause of the trouble by employing the procedure described

in section VI.

e. After the cipher text has been completely deciphered, press the right tape release marked "PRESS" and withdraw the tape, until all printing has cleared the tape chute. Tear off the tape.

NOTE: Every message that has been enciphered by means of ASAM 1 will be edited and appropriately marked before delivery to the addressee.

14

SECTION V
SPECIAL INSTRUCTIONS

19. Hand Operation.

a. If the main power supply fails, or other circumstances make motor operation impossible, the machine can be operated by use of the hand lever. A power supply of 24 volts d. c. is needed to operate the necessary magnets. Sixteen BA-23 cells in series, or equivalent, may be used for emergency power.

b. To shift from power operation to hand operation, proceed as follows:

(1) With the main power lead disconnected, interchange the positions of the motor plug (marked a. c. or d. c.) and the dummy plug so that the pointer of the dummy plug "24v."

(2) Raise the hand-lever pawl and slip the ring from under the pawl. Release the pawl to engage the hand-lever pinion.

(3) Connect the main power lead to any source of 24-volt d.c. If the voltage falls below 18, the magnet action will be unreliable; if more than 26 volts are used, injury to the magnets may result.

(4) After striking any key or the space bar, depress the hand lever fully and allow it to return completely to the top of its travel.

(5) To encipher or decipher a message, observe the normal operating procedures with the following exceptions:

(a) Zeroizing of the rotors can be accomplished with greater speed by moving the rotors manually to the "0" position.

(b) In determining the message rotor alignment, it is mandatory that each numeral key (1 through 5) be individually held in a depressed position until the downward motion of the hand lever has been completed. Failure to observe this requirement will prevent the stepping control rotors from advancing.

20. Tandem Operation.-Tandem operation provides an immediate automatic check of the encipherment of the message, a check on the operation of the enciphering machine, and an exact copy of the plain text of the message.

a. The machines have been provided with input and output tandem plug receptacles at the rear for tandem operation. Two machines can be connected so that one automatically deciphers the enciphered text produced by the other. When two machines are connected in tandem, errors will occur if only one machine is operated at a time or if the enciphering machine is operated faster than 40 words per minute. Tandem operation cannot be employed when emergency hand operation is used.

b. Two lengths of tandem cables are available. By using the longer cable it is possible to connect two machines in tandem after they have been installed in Chests CH-76

15

---

if the upper shelves are fully extended. When the shelf of a CH-76 is fully extended, a support should be placed under the front edge of the shelf to prevent its possible collapse.

c. The machines will be prepared for tandem operation as follows:

(1) Determine which machine has the slower speed. This may be accomplished by preparing the two machines for individual operation and turning the controller to the same position on both; i.e., if one machine is set at "P," set the second machine at "P" also. Set the stroke counter on each machine at zero. Press simultaneously the "Repeat" and "Blank" keys of both machines, holding them down approximately one minute. Release the keys simultaneously and note the counter readings. The machine showing the higher reading should be chosen as the deciphering machine and should be placed at the right of the other. The SLOWER machine will be the enciphering machine.

(2) Disconnect the power lead of the deciphering machine and tape or tie it so that it cannot accidentally be plugged into a source of power, but leave the ground clip connected. Should both machines be connected to a source of power while operating in tandem, fuses may be blown and damage may result.

(3) Check fuses in the master machine and replace with 10-ampere if equipped with 5-ampere. Five-ampere fuses are insufficient to start both motors at once.

(4) Using the tandem cable supplied, connect from the output on the enciphering machine to the input of the deciphering machine. Plugs are so constructed that they will fit only one way. The plugs must be completely inserted or improper operation may result. Care must be exercised in connecting the tandem cable in order to prevent bending the plug contacts or breaking the fiber insulators on either the tandem cable or the receptacles of the machine. A twisting motion should not be used in either inserting the plugs or removing them. A light coat of oil on the contacts will facilitate insertion and removal of plugs without interfering with the operation of the machines.

d. Tandem operation is accomplished as follows:

(1) Turn the controller of the enciphering machine to "R" and the deciphering machine to "P." Determine the message rotor alignment for the enciphering machine in accordance with paragraph 15.

2) Turn the controller of the enciphering machine to "P" and the deciphering machine to "R" and align the rotors to the same message rotor alignment in accordance with paragraph 15.

(3) Turn the controller of the deciphering machine to "P" and type the necessary plain text, the system indicator, and the message indicator.

(4) Set the enciphering machine at "E" and the deciphering machine at "D." Proceed in accordance with normal operating procedure The enciphering machine will print the enciphered text, while the second machine will print the decipherment of the enciphered text, i.e., a duplicate of the plain text as typed.

16

SECTION VI
AIDS FOR DECIPHERING GARBLED MESSAGES

21. Introductory Information.

a. A detailed explanation of certain errors which may occur in messages enciphered by means of ASAM 1 is

listed below in paragraphs 22 and 23 under the headings "When No Plain Text Appears" and "When Some Plain Text Appears." The errors are listed according to the frequency of their occurrence and the time necessary to correct them. Corrective measures are given for each error below the listing of the error. It is suggested that the corrections be tried in the order in which they are listed. Before trying any of the suggestions given below, the deciphering operator should check his own work to see that he has not deviated from prescribed procedure or made careless errors.

b. All errors, except typing errors, should be brought to the attention of the crypto-security officer.

22. When No Plain Text Appears.

a. Missing or additional groups at the beginning of the message.

CORRECTION PROCEDURE.-If checking the group count given in the message heading against the actual number of groups indicates that one or more groups are missing, or have been added, align the rotors to the message rotor alignment.

(1) If one or more groups are missing, turn the controller to "D" and advance the rotors by striking the "Blank" key as many times as there are missing letters. Decipher, beginning with the first group of the message.

(2) If one or more groups have been added, omit the indicated number of letters and decipher.

b. Wrong system.

CORRECTION PROCEDURE.

(1) Try deciphering the message using any other ASAM 1 cryptosystem held in common with the enciphering station.

c. Failure to zeroize and realign if a rotor is advanced beyond the proper alignment in aligning the message rotor alignment.

CORRECTION PROCEDURE.

(1) Zeroize the machine.

17

---

(2) When beginning to realign the rotors, advance the first rotor 26 characters beyond the letter to which it should be aligned, i.e., if the letter "B" has been selected as the first letter of the message indicator, advance that rotor until "B" appears on the white reference mark a second time and proceed to decipher. (The other four rotors will be aligned to normal positions.)

(3) If plain text does not result, zeroize the machine again and continue the process, advancing each rotor, in turn; an extra cycle. Four of the rotors must always be aligned correctly.

d. Message received with wrong date-time group or without date-time group.

CORRECTION PROCEDURE.

(1) Try the rotor arrangement and the index alignment for the date preceding and the date following the date appearing in the message.

(2) If no date appears in the message, try to decipher the message using the rotor arrangement and index alignment for the date following and the date preceding the date of receipt.

(3) Try the rotor arrangement and index alignment for the same day of the month preceding and the month following the current one.

(4) If the date appearing in the message is different from the date of receipt, try the date of receipt (if not tried in (1) above).

e. Failure to align to message indicator.

CORRECTION PROCEDURE-Zeroize the machine and begin decipherment without aligning the rotors to the indicator.

f. Transposition of letters of message indicator in the alignment of rotors.

Examples:
LEFLU aligned LEFUL
LKMNS aligned MKLNS
ALIFE aligned FAILE

(The enciphering operator is likely to exchange the position of two letters when the result forms a pronounceable group or when the two letters are often seen in reverse.)

CORRECTION PROCEDURE.

(1) Transpose adjacent letters in the message indicator and attempt to decipher the message.

(2) Transpose letters separated by only one letter and attempt to decipher. For example, transpose the 1st and 3d letters of the indicator and attempt to decipher.

(3) Try aligning the rotors to various other arrangements of the letters in the indicator

g. Incorrect alignment of index rotors.

CORRECTION PROCEDURE.

(1) If the system indicator is for CONFIDENTIAL messages, try the SECRET index rotor alignment, and then the RESTRICTED index alignment. Use the same idea for messages of other classifications.

(2) Use the index rotor alignment for the date preceding and the date following the date appearing in the message.

18

---

h. Incorrect alignment of stepping control and alphabet rotors.

CORRECTION PROCEDURE.

(1) Decipher, using the system indicator as the message indicator.

(2) Decipher, using the 26-30 check group as the message indicator.

(3) If the message is divided into parts, use as the beginning alignment the reading left on the machine after decipherment of the previous part.

(4) If the letter "0" is to be aligned, do not advance the rotor 26 times in aligning the message indicator

(5) Align stepping control rotors to letters of message indicator which might have been misread, e.g., Q and 0, N and M, W and M (reversed).

(6) Align stepping control rotors to letters which are adjoining letters of message indicator.

i. Incorrect rotor arrangement, the operator having failed to make the 26-30 check.

CORRECTION PROCEDURE

(1) Check the daily rotor arrangement table for "R" (reverse) designations which are faint enough to be overlooked.

(2) Try consecutively each of the reversed rotors in the normal position; then all of the reversed rotors in the normal position.

(3) Exchange positions of the 6 and 9 rotors.

(4) Exchange the positions of the last two alphabet rotors on the right.

j. Additional groups at the beginning of the message when group count checks. (This sometimes occurs when the operator makes an enciphering error and realigns to the message indicator without tearing off the cipher letters already printed on the tape.)

CORRECTION PROCEDURE.

(1) Align the stepping control rotors to the message indicator and decipher, dropping the 1st, 4th, and 7th groups, etc., through approximately the 28th group.

(2) When plain text results, realign the rotors to the indicator and decipher, omitting the same number of groups dropped in the above procedure.

k. An incomplete group or complete groups lost at the beginning of the message when the group count checks.

CORRECTION PROCEDURE.

(1) Align the stepping control rotors to the message indicator; strike the "Blank" key once and decipher the first three groups; strike the "Blank" key again and decipher the 4th, 5th, and 6th groups; strike the "Blank" key and continue this process up to the 13th group. Check the tape for plain text. The number of blanks required to obtain plain text represents the number of missing letters.

(2) If no plain text results from the above procedure, without realigning the rotors, decipher the next group (13th) six or eight times. Check for plain text after each decipherment of the group and if in doubt decipher the next group (14th); if plain text still does not appear, decipher the 14th group six or eight times, checking for plain text.

19

---

l. Alignment of index rotors displaced.

CORRECTION PROCEDURE.

(1) Turn the index rotors forward one position, one at a time, and attempt to decipher the message each time a rotor is moved. (Four of the rotors will remain in the original position.)

(2) If the above procedure does not result in plain text, turn the index rotors backward one at a time and follow the same procedure

m. Index rotor off center.
(This will result in monoalphabetic substitution cipher text and should be reported to the cryptosecurity officer immediately.)

CORRECTION PROCEDURE.- Place any index rotor in a halfway position, i.e., halfway between two numbers. Align the message indicator and decipher the message. The alphabet rotors will not advance

n. Overstepping of an alphabet rotor.

CORRECTION PROCEDURE.

(1) With the rotors aligned to the message rotor alignment, advance the 1st alphabet rotor one position and decipher the first one or two groups. Check the tape for plain text.

(2) If plain text does not result, retard the 1st rotor one position and advance the 2d rotor one position; decipher the next two groups.

(3) If plain text still does not appear, follow the same procedure for the 3d, 4th, and 5th rotors.

(4) When plain text results, realign the rotors to the message rotor alignment, advance the correct rotor, and decipher.

o Failure of stepping control rotor to advance when a key is depressed during alignment of message indicator on enciphering machine.

CORRECTION PROCEDURE.- Align the rotors to the message rotor alignment, and then advance the alphabet rotors one at a time and in all possible combinations. Each time, decipher one or two groups. Check the tape for plain text.

23. When Some Plain Text Appears.

a. Deletion of one or more groups.

CORRECTION PROCEDURE.

(1) Check the actual number of groups in the message against the group count appearing in the message heading. Realign to the message rotor alignment. With the controller at "D," advance the rotors to the point of garble by means

---

of the "Blank" key. Record the rotor alignment and counter reading. Strike the "Blank" key the same number of times as there are missing letters, and then continue with the decipherment of the message.

(2) If the above procedure does not result in plain text, align the alphabet and control rotors manually to the alignment at the point of garble as recorded in (1) above. With the controller at "D," decipher the group following the point of garble as many times as necessary (without realigning the rotors) until plain text appears, checking for plain text after each decipherment. For example, if the garbled text starts at a counter reading of 95 (19 groups), decipher the 20th group as many times as necessary (without realigning the rotors) until plain text appears.

b. Added or repeated groups.

CORRECTION PROCEDURE.

(1) If a check of the group count shows that one or more groups have been added or repeated, realign to the message rotor alignment. With the controller at "D," advance the rotors to the point of garble by means of the "Blank" key. Record the rotor alignment and counter reading. Omit the indicated number of groups and continue to decipher.

(2) If the above procedure does not result in plain text, decipher the 11th group following the garble as many times as necessary (without realigning the rotors) until plain text appears. Check each decipherment of the group for readable text. For example, if the recorded letter count at the point of garble is 205 (41 groups), decipher the 52d group as many times as necessary (without realigning the rotors) until plain text appears. If there are not 11 groups following the point of garble, decipher the next to the last group of the message (exclusive of indicators) as many times as necessary (without realigning rotors) until plain text appears. (3) The number of extra groups can be determined by subtracting from 11 the number of times the 11th group was deciphered to produce plain text.

c. One letter of a six-letter group (made by defective spacing of the machine) is lost in handling.

CORRECTION PROCEDURE.-Realign to the message rotor alignment. With the controller set at "D," advance the rotors to the point of garble, strike the "Blank" key once to replace the missing letter, and then decipher normally.

d. Cipher group consisting of only four letters.

CORRECTION PROCEDURE.-Record the rotor alignment and counter reading immediately before deciphering the four letter group. Strike the "Blank" key once to replace the missing letter, and then continue to decipher.

NOTE: In case an important word remains garbled in C or d above, realign to the point immediately preceding the group yielding garbles and decipher, striking the "Blank" key in a different position until a logical word is obtained. If necessary, consult a Morse error chart for two-letter combinations commonly transmitted as one letter. Substitute such letters in the cipher text and decipher.

e. Cipher group consisting of six letters. (Occasionally a six letter group will be printed because of a machine fault, in which case all six letters will be required to get plain text.)

21

CORRECTION PROCEDURE.

(1) Record the rotor alignment and counter reading immediately before deciphering the six letter group; then decipher all six letters of the group and continue to decipher several groups. If the result is a garble, decipher only the first five letters of the group, dropping the 6th, and continue to decipher several groups. If there is still a garble, drop other letters of the group one at a time until plain text results.

(2) Consult a Morse chart, if applicable, for single letters commonly transmitted as two letters, and substitute in the cipher. text.

f. Two or more letters garbled in transmission causing an important word to be partially garbled.

CORRECTION PROCEDURE.

(1) Consult a Morse error chart or a teletypewriter garble table for letters commonly garbled in transmission. Substitute such letters in the cipher text and decipher.

(2) Realign the rotors to the message rotor alignment Set the counter at zero and the controller at "E," and by means of the "Blank" key, advance the rotors to the point of garble; then encipher the assumed word, Compare the result with the cipher text received. If the difference is justified by common transmission errors, the assumed word is probably correct. (In this event the operator must deliver to the officer in charge of the cryptocenter the text which was actually deciphered as well as the correction.)

g. One hand of the enciphering operator misplaced on the keyboard. (Note that words when deciphered retain their correct length even though garbled) Example: AIRCRAFT REOIRTED IOERATUBG IVER SOUTHERN AREA. (In this example the right hand of the enciphering operator was placed one position over from the correct position.)

CORRECTION PROCEDURE.-Observe the text as it appears on the tape. Fit in probable plain-text words and try to justify them by a particular incorrect position of the operator's hand.

h. One hand of teletypewriter operator misplaced on keyboard in transmission. (Note that words do not necessarily retain their correct length.) Example: BOMBED AIRCLJFTWR GCBRTXDWOPERMXHJTYION GIAVER SOUTHERN AREA.

CORRECTION PROCEDURE.- Assume a specific incorrect position of the operator's hand. Replace the incorrect cipher letters with the assumed correct ones and decipher the result.

i. Stepping control rotors advancing incorrectly on the enciphering machine.

CORRECTION PROCEDURE. - Realign the rotors and decipher slowly, at the point of garble, observing the stepping of the rotors. As "0" on the 3d stepping control rotor passes the white reference mark, the 4th rotor should advance once; as "0" on the 4th rotor passes the white reference mark, the 2d rotor should advance once. In case one of these rotors fails to advance at the proper time move it forward by hand before striking the next key. Then proceed to decipher the message.

22

---

j. Stepping control rotors advancing incorrectly on the enciphering machine.

CORRECTION PROCEDURE.

(1) If the 2d, 3d, and 4th stepping control rotors advance at the point of garble, move back the 2d rotor one position, and continue decipherment. If plain text does not result, realign, move back the 2d and 4th rotors when they advance, and continue decipherment. Then realign, move back all three rotors one position, and continue decipherment.

(2) If only the 3d and 4th rotors advance at the point of garble, move back the 4th rotor one position and decipher. Then realign, if necessary, move back both the 3d and 4th rotors one position, and decipher.

(3) If only the 3d rotor advances at the point of garble, realign the rotors. Advance the rotors to the last letter yielding plain text; record the alignment of the rotors. Move back the 3d control rotor one position and decipher, beginning with the last correct letter. Check the tape for plain text.

(4) If plain text does not result, return to the recorded alignment, advance the 4th rotor one position and decipher; if plain text still does not appear, follow the same procedure for the 2d, 1st, and 5th rotors.

k. One alphabet rotor missing a step.

CORRECTION PROCEDURE.-To check for this fault on the enciphering machine, realign the rotors and at the point of garble move back the 1st alphabet rotor one position and decipher three groups. If no plain text results, advance the 1st alphabet rotor one position and move back the 2d alphabet rotor one position . Then decipher three more groups. If no plain text results, repeat this process for each of the five alphabet rotors. (If the last good letter of the text can be determined, only the alphabet rotors which advance during the decipherment of that letter need be tried.)

l. Overstepping of an alphabet rotor on the enciphering machine.

CORRECTION PROCEDURE.-Repeat the process outlined in paragraph 23k above, but this time advance the rotors one at a time and attempt to decipher. (If the last good letter of the text can be determined, only the alphabet rotors which did not advance during the decipherment of that letter need be tried.)

23

SECTION VII
OPERATION IN AN EMERGENCY

24. General.-The procedure for operation of ASAM 1 during an emergency created by the compromise of all keying materials in use or held in reserve by individual holders is described in paragraphs 25 through 29. The procedure provides a method whereby the data normally contained in the key list is supplied to each holder by a classified message in order that normal communications may be maintained until uncompromised key lists and rotors can be distributed.

25. Notification of Compromise.

a. Upon determination of a compromise the Chief, Army Security Agency, The Pentagon, Washington 25, D. C., or the Chief, Army Security Agency, Europe, Pacific, or Hawaii, whichever is applicable, will inform each holder of ASAM 1 of the compromise by means of an emergency message which will contain keying data for a period of five days. The emergency message will be identified by a special indicator reserved for that purpose only.

b. The emergency message will be enciphered with the currently effective rotors of the system. However, the rotor arrangement and index rotor alignment used will be based upon the emergency key phrase in effect at the time of the compromise.

26. Emergency Key Phrase.

a. Emergency key phrase will be supplied each holder of ASAM 1 in a sealed envelope which will not be opened before the date indicated on the envelope. Each emergency key phrase will be effective for a period of two months, at the end of which time a new phrase will become effective. The emergency key phrase will be used only in connection with the encipherment and decipherment of the emergency message. It will be used to determine for that message:

(1) The stepping control and alphabet rotor arrangement.

(2) The index rotor alignment.

b. After the sealed envelope is opened, the emergency key phrase will be memorized and the letter containing it will be destroyed. No report of destruction is required. To insure knowledge of the phrase at all times, it will be memorized by the crypto-security officer and each trick chief. Under no circumstances will the emergency key phrase be recorded nor will the letter be retained. Written evidence of the phrase would defeat the purpose of the emergency system.

24

---

27. Use of the Emergency Key Phrase.-The emergency key phrase will be used for arranging and aligning the rotors as follows:

a. Each key phrase will be at least 16 letters in length, e.g., CAPTAIN JOHN SMITH

b. The first 10 letters will be numbered 1 through 0 according to their relative sequence in the normal alphabet. Thus,

```
3 1 9 0 2 5 7 6 8 4
C A P T A I N J O H N S M I T H
```

Note that repeated letters, such as A in this example, are numbered according to the order of their occurrence in the key, from left to right. The last letter to be numbered becomes 0, denoting the rotor numbered 0 in the set.

c. Stepping control (middle) rotors will be arranged in the cipher unit according to the first five numbers of the key. Any number associated with a vowel (A, E, I, 0, or U) indicates a "reversed" rotor. In this example, the arrangement of the stepping control rotors would be: 3, 1R, 9, 0, 2R.

d. The alphabet (rear) rotors will be arranged in the cipher unit according to the sixth through tenth numbers of the key. Any number associated with a vowel indicates a "reversed" rotor. In this example, the arrangement of the alphabet rotors would be: 5R, 7, 6, 8R, 4.

e. The index (front) rotor alignment will be derived by taking the alternate numbers in the key, beginning with the second number and proceeding through the tenth. In this example, the numbers are 1 0 5 6 4. The numbers indicate the "units" digit of the number to be aligned on each index rotor. Thus the index alignment in this example would be 11, 20, 35, 46, 54.

f. After arranging and aligning the rotors as described above, normal operating procedure for ASAM 1 will be observed in enciphering and deciphering the emergency message.

28. Emergency Message.

a. An emergency message, enciphered according to the above outlined procedure, will be sent to all holders of the compromised system. It will contain keying data for a five-day period and will bear three indicators, as follows:

(1) A special indicator which will indicate that it is an emergency message. This indicator will be KINSL.

(2) The system indicator for the SECRET classification of the compromised system.

(3) The message indicator.

b. The message will include the following items:

(1) Identification of the compromised system.

(2) Keying data arranged in the following order: date of the month; stepping control rotor arrangement; alphabet rotor arrangement; SECRET index rotor alignment and 26-30 check; CONFIDENTIAL index rotor alignment and 26-30 check; RESTRICTED index rotor alignment and 26-30 check.

c. A sample emergency message is illustrated below. "REV" appearing after a rotor number indicates that rotor is to be inserted in a reversed position.

SYSTEM NINE SIX FIVE THREE COMPROMISED PD FIFTEENTH
MIDDLE FIVE TWO SIX NINE ZERO REAR SEVEN ONEREV EIGHT
FOUR THE SEC

24

FOUR EIGHT FIVE ZERO ONE CHECK MIKE KING LOVE OBOE
CHARLIE CONF THREE SEVEN FIVE FOUR ONE CHECK NAN GEORGE
TARE VICTOR ZEBRA RESTR FOUR EIGHT TWO ZERO SEVEN CHECK
DOG GEORGE OBOE WILLIAM YOKE PD SIXTEENTH MIDDLE TWOREV
NINE SEVEN FOUR ONE REAR THREE FIVE SIXREV EIGHT ZERO
SEC FOUR TWO EIGHT SEVEN ONE CHECK CHARLIE BAKER FOX
WILLIAM VICTOR CONF EIGHT TWO SIX FIVE THREE CHECK TARE
UNCLE OBOE PETER KING RESTR ZERO NINE TWO EIGHT SIX
CHECK QUEEN ZEBRA FOX UNCLE NAN PD SENTEENTH MIDDLE
ONEREV SEVEN NINE FOURREV TWO REAR EIGHT THREE SIXREV
FIVE ZERO SEC SEVEN FIVE TWO ONE SIX CHECK GEORGE VICTOR
BAKER JIG QUEEN CONF ONE FIVE ZERO EIGHT TWO CHECK TARE
SUGAR UNCLE OBOE DOG RESTR FIVE TWO NINE THREE SEVEN
CHECK OBOE FOX CHARLIE KING PETER PD EIGHTEENTH MIDDLE
FOUR SEVENREV TWO FIVE ZERO REAR THREE NINE SIX EIGHT
ONE SEC TWO THREE EIGHT ZERO FOUR CHECK HOW YOKE FOX
CHARLIE JIG CONF FIVE NINE TWO ONE ZERO CHECK GEORGE
WILLIAM PETER OBOE ITEM RESTR SEVEN ONE FIVE EIGHT NINE
CHECK DOG ITEM KING ROGER BAKER PD NINETEENTH MIDDLE SIX
TWOREV EIGHTREV ONE FOURREV REAR FIVE ZERO SEVEN THREE
NINE SEC NINE FOUR SEVEN ZERO ONE CHECK JIG HOW DOG FOX
ITEM CONF SEVEN ZERO FIVE THREE EIGHT CHECK LOVE GEORGE
MIKE PETER EASY RESTR NINE THREE SIX ONE FIVE CHECK MIKE
LOVE HOW GEORGE LOVE

d. The enciphered message, including the indicators, will be arranged as follows:

```
EXAMPLE: KINSL RLMCR DOG TARE JIG XRAY LOVE MRWTX .....GDLJC
           1      2               3                      4
```

l. Special indicator for Key-changing message.
2. System indicator for SECRET classification of the compromised system.
3. Message indicator.
4. Text.

e. The emergency message will always contain keying data for the day on which it is sent, regardless of the time.

f. The keying data derived from the emergency key phrase will not be employed for enciphering or deciphering any other message. After deciphering the emergency message, each holder will prepare the ASAM 1 for operation using the data supplied in the message in conjunction with the currently effective rotors of the compromised system.

g. The deciphering copy of the emergency message will be retained in the cryptocenter where it will be safeguarded in the manner prescribed for registered SECRET material. It will be destroyed five days after the last date for which the keying data is contained therein. In the event that an emergency destruction of crypto- material is necessary, the plain text of the emergency message will be the first item destroyed.

h. In the event that replacement key lists and rotors cannot be distributed to all holders within five days, additional keying data will be supplied each holder by classified message. This message will resemble a normal message and will be enciphered by means of the keying data supplied for the last date in the emergency message.

24

---

29. Normal Traffic.

a. The system indicators contained in the key list will be used for all ASAM 1 traffic enciphered during the emergency period. The special indicator KINSL is reserved for the original emergency message only.

b. Operation of the ASAM 1 employing the keying data supplied in the emergency message will conform to the normal operating procedure for the machine.

APPENDIX 3

KEYING (OPERATING) THE ECM MARK II

This outline of the June 1945 (SIGQZF-2) keying procedure describes how key lists were used to assemble and align the rotors before enciphering a message. The first instructions from July 1941 (SIGQZF) were changed in June 1945 (SIGQZF-2) and again November 1945 (SGIQZF-3). For example, SIGQZF-3 uses a totally different method of determining message indicators that eliminated the need for a daily rotor alignment of the control and cipher rotors. Changes were made to minimize operator errors, enhance security and speed up the operation. A sample Army manual from 1949 is available online.

Although the index rotors were reassembled (changing the order of the rotors) once a day during most of the war (SIGQZF), starting with SIGQZF-2 they were kept in a fixed order not requiring daily reassembly. The operator consults the secret daily keylist and aligns (rotates) the index rotor wheels differently for secret, confidential and restricted messages. The index rotor alignment is only changed when either the day ends, or the classification of message to be encrypted changes.

Control and cipher rotors are also reassembled once a day from the secret daily keylist, their alignment however, was changed with each message. After the daily assembly of all rotors and the alignment of the index rotors, a check group is used to verify the initialization and operation of the machine before any real messages are encrypted. The rotors are zeroized, (cipher and control rotors positioned on "O") and the letter A is repeatedly encrypted until 30 cipher text characters are printed. Then the 26th-30th letters are matched with the check group supplied in the secret daily keys.

For each message, the secret daily keylist is consulted, and the control and cipher rotors are aligned to an initial position depending on the classification of the message. Now the operator selects a group of any five letters, except Z, at random to be the internal message indicator. This internal message indicator is then enciphered and the external message indicator (enciphered internal message indicator) is printed on the tape and transmitted with the message. The control and cipher rotors are then aligned without printing to the internal message indicator. The rotors are never aligned to the external message indicator (the letters printed on the tape), but always to the internal message indicator. Now the body of the message may be enciphered and transmitted with the external message indicator. If the plain text exceeds 350 5-letter groups, the plain text must be divided into 2 or more equal parts so that no part exceeds 350 groups. For each part a new internal message indicator is selected.

APPENDIX 4

COMPLIANCE WITH OPERATING PROCEDURES:

The security of a cryptographic system relies as much on the operation of the cipher machine as the machine itself. During WWII the U.S. created organizations to formally train operators and to monitor U.S. operators compliance with procedure. When an error was found the first response was often a memorandum such as the one replicated below. It provides a list of the most common errors that could compromise the security of the cryptographic system.

Navy Department
Office of Chief of Naval Operations
Washington, D.C.

CLASSIFICATION: CONFIDENTIAL Date: 27 Dec 1943

MEMORANDUM
COMMUNICATION IMPROVEMENT ITEM

From: Director Naval Communications
To: Commandant, Twelfth Naval District

The principles of communication security cannot be overstressed, for such security is vital to the success of operations. Errors which seem minor in themselves may, when accumulated, offer to the enemy an entering wedge for the eventual compromise of a system. The object of this memorandum is to enlist your cooperation in protecting our cipher systems and hence our national security.

THE PRICE OF SECURITY IS ETERNAL VIGILANCE.

A communication such as COM 112 222105 DECEMBER may endanger our interests because it appears to violate security principles in the following respect(s):

DRAFTING: Plain language reference to encrypted dispatches.

No reply to this memorandum is necessary, but your cooperation in suppressing dangerous communication practices is earnestly solicited.

CARELESS COMMUNICATIONS COST LIVES

The following is a list of some of common violations of security principles:

DRAFTING:

Unnecessary word repetition
Unnecessary or improper punctuation
Plain language reply to encrypted dispatch
Classification too high
Precedence too high
Cancellation in plain language of an encrypted dispatch

ENCRYPTION:

"XYX" or "X"'s for nulls
"XX" & "KK" to separate padding from text
Same letters at both ends to separate padding from text
Continuity of padding
Seasonal and stereotyped padding
Repetition of generatrices (Ed. Note: CSP-845)
Systematic selection of generatrices (CSP-845)
Using plain text column for encryption (CSP-845)
Proper strips not eliminated as prescribed by internal
indicator (CSP- 845)
Improper set-up according to date
Using system not held by all addressees
Failing to use system of narrowest distribution

CALLS:

Enciphering indefinite call sign
Enciphering call signs of shore activities

CODRESS might have been used

TRANSMISSION:

Classified dispatch transmitted in plain language by wire or radio, when not specifically authorized. Dispatch might have gone to some or all addressees by mail.

APPENDIX 5

ECM MARK II SPECIFICATIONS

Input: Keyboard or electric via tandem plug.
Output: Printed tape or electric via tandem plug.
Speed: 45 to 50 Words per minute.
Power Supply: 40/70 cycle, 105-125 VAC or 105-125 VDC or 24 VDC 2 amps at 120 volts AC or DC, 3 amps at 24 VDC.

Approximate Size:
In operation: 15" x 19.25" x 12" or 2.1 cubic feet
In carrying case: 17.125" x 23" x 15.5" or 3.5 cubic feet
Packed for long term: 19.5" x 27.5" x 18" or 5.6 cubic feet

Approximate Weight:
In operation: 93.5 lbs.
In carrying case: 133.5 lbs.
Packed for long term: 195 lbs.

Cost:
By 1943, 10, 060 ECM Mark II's were purchased at an estimated cost of $2,040 a piece. This does not include the cost of spare parts; additional code wheel sets, code wheel wiring that was done by the military; modifications and upgrades, precursor machine development, etc.

ADDITIONAL REFERENCES

[ASSA] Army Signal Security Agency (1946) History Of Converter M-134-C (Sigaba) Vol I, II And III: available from the US National Archives and Records Administration (NARA); NSA Historical Collections 190/37/7/1, Box 799, F: 2292, pp 468.

[ASA] Army Security Agency (1948) Historical and Cryptologic Summary of Cryptosystems; ASAG 23; Vol 1.

[DOA1] Department of the Army (1945) Crypto-Operating Instructions for Converter M-134-C (short title: SIGQZF-2)

[DOA2] Department of the Army (1946) Crypto-Operating Instructions for Converter M-134-C (short title: SIGQZF-3)

[DOA3] Department of the Army (1949) ASAM 1/1 Crypto-Operating Instructions for ASAM 1. Note the new designation of ASAM 1 for the ECM Mark II after the war.

[OCNO] Office of Chief of Naval Operations (1943) Memorandum Communication Improvement Item. available from the NARA, Pacific Sierra Regional Archive, RG 181-58-3224, 12th ND Commandants Office General Correspondence, A6-2(1) Complaints -Discrepancies, Security-etc.

[SAS-] Descriptions of the Authentication Systems may be found in: Survey Of Authentication Systems 1942-45 (1945), NARA; NSA Historical Collections 190/37/7/1, NR 3526 CBRK24 12960A 19420728.

[SAFF] Safford, L.F. (1943) History of Invention And Development of the Mark II ECM (Electric Cipher Machine) available from NARA. SRH-360 in RG 0457: NSA/CSS Finding Aid A1, 9020 US Navy Records Relating to Cryptology 1918- 1950 Stack 190 Begin Loc 36/12/04 Location 1-19. In Feb 1996 the version at NARA was redacted, but the full document is now declassified.

[SFUS] Submarine Force U.S. Pacific Fleet (1944) Cryptographic Aids Check-Off List: available from NARA, Pacific Sierra Regional Archive, 181-58-3201, S1313, S372, A6-3/N36 Cryptographic Aids.

[USNA] US Naval Administration in WW II, History of Naval Communications, 1939-1945. Op-20A-asz, A12, Serial 00362P20, 7 Apr 1948. available from the Naval Historical Center; WW II Command File CNO; Communications History; Microfiche No. F3561.

[WDO] War Department Office of The Chief Signal Officer (1941) Operating Instructions for Converter M-134-C (short title: SIGBWJ)

[WDO1] War Department Office of The Chief Signal Officer (1941) Operating Instructions for Converter M-134-C (short title: SIGLVC) Department of the Army (1941) Crypto-Operating Instructions for Converter M-134-C (short title: SIGQZF)

[WDM1] War Department (1942) Maintenance Instructions for Converter M-134-C (short title: SIGKKK)

[WDM2] War Department (1945) Maintenance Instructions for Converter M-134-C (short title: SIGKKK-2) SIGQZF, SIGBWJ, SIGLVC, SIGKKK, SIGKKK-2 are available from NARA; NSA Historical Collections 190/37/7/1, NR 2292 CBLL36 10622A 19410300.

[WDG1] War Department (1945) General Instructions For Converter M-134-C (short title: SIGBRE-1) available from NARA; NSA Historical Collections 190/37/7/1, NR 4588 ZEMA35 13909A 19450600