# Mediterranean Enigma

by

Unknown Author

26 May 1943

## Abstract

An account of the procedure followed in Hut 8 in dealing with the Mediterranean Enigma ("Porpoise"). This has the "throw-on" type of indicator, and one recovers the Grundstellung alphabets by "boxing". (Sunfish and Seahorse also have this type of indicator; see Volume 2, Articles 3 and 5.

Source: NARA, College Park, Md., Record Group 38, Crane Collection, Box 172, RIP 610, ARC Identifier: 6921399, HMS/MLR Entry Number: A1 1025
https://catalog.archives.gov/id/6921399
Enigma Series Volume 8, Article 1

Editor: Frode Weierud, Crypto Cellar Research
Web Site: www.cryptocellar.org

Version: 29 May 2022

## MEDITERRANEAN ENIGMA

1. The bulk of this traffic, called "Sued" by the Germans and "Porpoise" by the Briti~~sh, i~~s enciphered on the 3-wheel naval enigma. The remainder, called "Henno", is believed to be a hand cipher like the R.H.V. The two types are indistinguishable by external characteristics; both are sent in 4-letter groups with the first two groups repeated at the end, and on the same frequency schedules. The users are surface craft and shore stations in the Mediterranean, Aegean, and Black Seas. The traffic averages about 120, 30 and 100 messages per day, respectively for the three areas; Henno probably 20-30.

The enigma keys are changed exactly as in Shark: wheels and rings usually last two days (sometimes only one and sometimes three), while the Stecker and Grundstellung change daily. Keys for the Offizier (called "Winkle") behave exactly as for Limpet. The system is not in the K-book family.

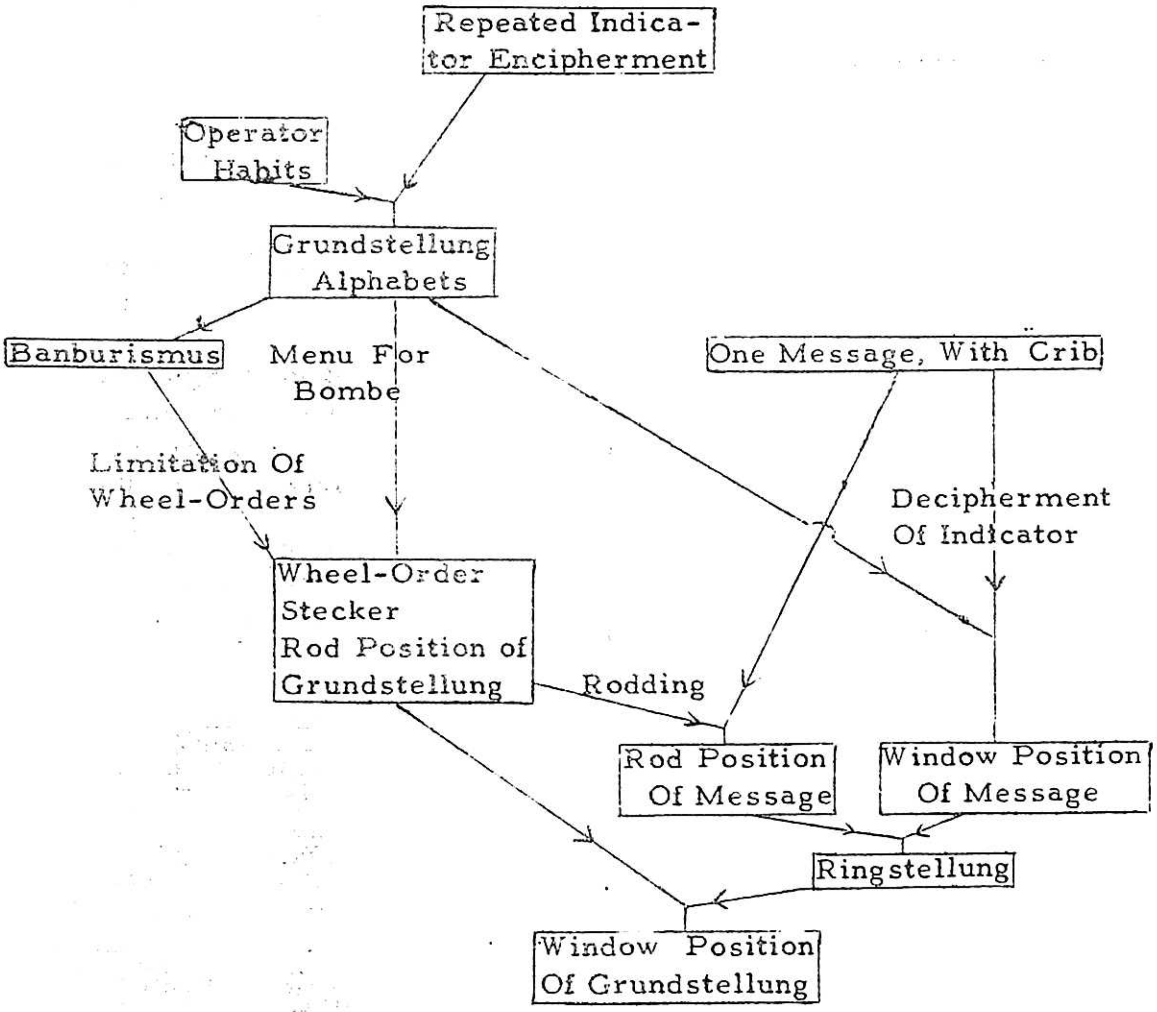
The operator selects a trigram at random, say PYX, at which to encipher the message, i.e. the left-hand wheel will be set at window position P, the middle at Y, and the right-hand wheel at X. To encipher the plain indicator PYX, the operator sets the machine at the Grundstellung in effect and enciphers PYXPYX, getting let us say RGYVMO. He then selects two letters, apparently at random, say U and S, and sends as the two-group indicator: URGY SVMO. Nothing is known about the significance, if any, of these beginning letters of the two indicator groups; it is possible they may serve to distinguish Porpoise from Henno.

2. From this encipherment of the repeated clear indicator, and the habits of operators choosing trigrams "at random", the six Grundstellung alphabets are found (paragraph 3 below), i.e. those in the first six positions after the Grundstellung. From these a strong menu can be built; in fact they need not be complete for this. Moreover, Banburismus (paragraph 4 below) enables one to find the middle and right-hand wheels, except that VI, VII and VIII cannot be distinguished since their notches are in the same place (after M and Z). Thus the number of wheel-orders to try can be limited to 6, 18 or 36 as the case may be.

The bombe gives the wheel-order and Stecker, of course, and the rod (i.e. core) position of the Grundstellung. Since we do not know the Ringstellung, the latter is as yet of no use. But all we need do is to rod one message, and the day is ours. For since we know the Grundstellung alphabets, we know at once from the indicator what the window setting of the message is, and this together with its rod position yields the rings.

A diagram of the daily procedure described above is given herewith. The entire job is usually finnished by 0600, leaving six current hours for the day. The paired day (paragraph 5 below) is usually out by 2000, leaving sixteen current hours.

DIAGRAM OF MEDITERRANEAN PROCEDURE


Repeated Indicator Encipherment
Operator Habits
Grundstellung Alphabets
Banburismus
Menu For Bombe
One Message, With Crib
Limitation Of Wheel-Orders
Decipherment Of Indicator
Wheel-Order Stecker Rod Position of Grundstellung
Rodding
Rod Position Of Message
Window Position Of Message
Ringstellung
Window Position Of Grundstellung

3. The first step in finding the Grundstellung alphabets is to make up a "throw-on" sheet (Exhibit 1.) Suppose the indicators of half a dozen messages are

| | | |
|---|---|---|
| 1. | AYZX | TDAB |
| 2. | VRFT | MXMK |
| 3. | CZKJ | LWTQ |
| 4. | RPOF | BCPG |
| 5. | UYAF | MDEG |
| 6. | VRMC | IXWV |

Recall that the significance of the 8 letters is schematically

| | |
|---|---|
| 123 | 456 |
| XLMR | XLMR |

Thus in message #1 the initial letters A and T are dummies (indicated by X); Y and D are the encipherments of the initial window position of the left-hand wheel (L) in the 1st and 4th Grundstellung alphabets; Z and A likewise for the middle wheel (M) in alphabets 2 and 5 respectively; X and B for the right-hand wheel (R) in 3 and 6. On the throw-on sheet one enters D in the Y-row and L-column, A in the Z-row and M-column, and B in the X-row and R-column. These have been starred in Exhibit 1.

From the 250 messages on May 17, all but three squares were filled, and these were readily found. The so-called "duds" - probably mostly Henno - do not fit the pattern, but they are easily eliminated by their failure to agree with the vast majority.

The second step is to "box" the throw-on sheet. This simply means to find the cyclic components of the three columns (separately). Thus for the L-column we get the cycles:

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

There must always be this pairings off into cycles of equal length. Perhaps the easiest way to see this is to take the correct answer (Exhibit 6) and work backwards. With reference to the L-alphabets 1 and 4 we see that

$$L \xrightarrow{1} R \xrightarrow{4} Z \xrightarrow{1} S \xrightarrow{4} W \xrightarrow{1} X \xrightarrow{4} L$$

It must take an even number of jumps to get back to the starting letter. Moreover, if we pick alternate letters we get L Z W AND R S X. These are the two cycles of length three, except that the second is reversed. This is clarified by breaking the above into two parts

$$L \xrightarrow{14} Z \xrightarrow{14} W \xrightarrow{14} L$$

$$R \xrightarrow{41} S \xrightarrow{41} X \xrightarrow{41} R$$

For the throw-on sheet is the effect of applying Grundstellung alphabet #1 and then #4, while applying first #4 and then #1 yields the inverse thereof.

But these considerations showing the origin of our paired cycles shows also what we must do to recover the constituent alphabets #1 and #4. One cycle must be reversed and larded into its mate. A convenient way of doing this is to write one down in double on one sheet of paper and the other reversed on another, and slide one under the other, thus:

A T Y D Q U G E I J A T Y D Q U G E I J

F N M K V H O C P B

In the above position we think

$$I \xrightarrow{1} F \xrightarrow{4} J \xrightarrow{1} N \xrightarrow{4} A \xrightarrow{1} \ldots \text{ etc.}$$

This is the "correct" position, as can be seen from Exhibit 6. In this way we can read plain-cipher pairings in alphabet #1 very readily - they are the vertical pairs IF, JN, AM, etc. Those in alphabet #4 are so obtained by sliding the bottom strip one place to the right: JF, AN, TM, etc.

Any one of the 10 possible alignments gives a possible (partial) alphabet #1 (and #4), which can be completed by any one of the 3 possible alignments of the cycles of length 3, making 30 possibilities in all. Now comes the job of telling which one is right. This depends ultimately on operators' habits in "random" selection of the clear indicator trigrams. These habits are slightly different for the three classes of traffic: Mediterranean Proper (called "North Africa"), Black Sea, and Aegean.

In Exhibit 2 I have listed in the columns labelled "Cipher" the last three letters of the first indicator group of 100 North Africa messages (on this same day, May 17). (In the columns labelled "Plain" are the actual window settings obtained therefrom by the correct Grundstellung alphabets 1, 2, 3 in Exhibit 6). Exhibit 3 gives a frequency count of the enciphered indicator letters in Exhibit 2; for each of the three wheels L, M, and R. Although the I.C. is not used, I thought it of interest to compute it for each of the three counts: 1.28 (L), 1.12(M), and 0.98 (R).

Exhibit 5 is copied from their standard table showing the operators' preference for the various letters in each of the three positions. They keep a running frequency count of the clear indicator letters used, and modify the standard table periodically in accordance therewith. The table is expressed in "half decibans". Generally speaking, if x represents in some way the likelihood of a certain event, then this likelihood expressed in "decibans" is 10 log x, in "centibans" is 100 log x, in "half decibans" is 20 log x. In "bans" it would be log x, but this unit (like a farad) is seldom used. Thus if the odds are 2 to 1 that your wife will be waiting up for you after an evening with the boys, the likelihood of this event is approximately 3 decibans, 6 half decibans, or 30 centibans. In Exhibit 5, the number $g_i$ entered for the ith letter is actually

$$g_i = 20 \log \frac{f_i}{f} = 20 \log (26 f_i)$$

where $f_i$ is the relative frequency of the ith letter, and $\bar{f} = 1/26$ is the expected average (truly random) frequency. Thus the letter L occurs twice as often as it should by random for the L-wheel, i.e. $f_L - 1/13$, giving it a score of 6 half decibans in the L-column. Likewise J in the R-column occurs only half as often as it should, i.e. $f_j - 1/52$, giving it a score of -6 half decibans. Decibans (and family) provide not only an additive unit of likelihood but also a ready means (because of the +'s and -'s) of seeing whether an event is more likely or less likely than would normally be expected. Of course this idea per se is not new to us, as we used it in our work on transpositions, but we do not make such widespread use thereof.

The problem now is to select that one of the 30 possible alphabets which best matches the observed frequency (Exhibit 4) with the standard table (Exhibit 5). Taking the letters occurring in the two cycles of length three, we may classify them as high +, low -, or about average o.

| Observed (~~cipher~~) | Standard (plain) |
|---|---|
| + L R Z | + L R |
| o X | o S W Z |
| - S W | - X |

We have three possible alignments:

| | | | | | |
|---|---|---|---|---|---|
| (1) | L Z W | (2) | L Z W | (3) | L Z W |
| | R S X | | S X R | | X R S |

Omitting consideration of the average frequency letters,

(1) has three points in its favor: $L_c=R_p$, $R_c=L_p$, and $W_c=X_p$;
(2) has three points against it: $S_c=L_p$, $Z_c=X_p$, and $W_c=R_p$;
(3) has one point in its favor, $Z_c=R_p$, and one against, $L_c=X_p$.

There is thus no question but (1) is right.

Taking the pair of cycles of length 10, my technique was to encircle the standard highs and lows in black and red respectively, and put +'s and -'s for observed highs and lows, and count points for and against at each position. Thus at the position

```
+ + +   -   +   +   + + +   -   +
A T Ⓨ D Ⓠ Ⓤ Ⓖ Ⓔ I Ⓙ A T Ⓨ D Ⓠ Ⓤ Ⓖ Ⓔ I Ⓙ
        Ⓕ N Ⓜ Ⓚ V Ⓗ O C P Ⓑ
        - -     - + - - + -
```

there are 3 points for and 4 against. The winning position had 10 for and none against, though F opposite D gave a good score of 7 for with none against.

The actual technique employed is of necessity rougher and readier, as this is carried on as the traffic is coming in. None the less it is based fundamentally on matching frequencies of individual letters.

This point - technique of mine led to a dead heat between two positions for the R - alphabet. (Actually it seems surprising that any matching at all is possible with a count whose I.C. is 0.98, but it is!). After grubbing about in the intermediary frequencies, I arrived at a slight preference for one of them, and it turned out to be correct. However, such a choice can frequently be made by observing the final trigrams produced in each case.

In Exhibit 2 these are given in the columns marked "Plain". Those checked mean either that all three letters are near each other on the enigma keyboard (Exhibit 3), or that two are laterally adjacent. Notice the "straight keyboard" RTZ in the seventh message listed. Another habit is to form pronounceable trigrams. About 20% have the form consonant-vowel-consonant (19 such in our sample of 100)! Doubled letters rarely occur, and probably the EFE is unusual. I must say I can see small difference if the alternative R - alphabet is used. It spoils RTZ and turns LRH into the bad one LRR, but then it makes EFM out of EFE.

Actually it is not necessary to complete the alphabets in order to make a good menu. About one and a half are said to be sufficient. Of course if L and half of R are known, we really know Grundstellung alphabets 1 and 4, and half of 2 and 5.

4. This section describes how the wheel-orders to try on the bombe are limited by the Banbury process. The day I worked on was May 20, not the same as in paragraph 3.

The first step is to punch Banbury sheets for the messages as they come in. Two such are enclosed as Exhibits 8A and 8B. These enable any two messages to be compared for coincidences at any desired position. (This could probably be done mechanically on 70 mm tape to good advantage, but the girls get very adept at it. It might be difficult to see trigrams and tetragrams on the I.C. machine, but its chief disadvantage to my mind is that slight uncertainty about position. In its application to Mediterranean, Banburismus compares messages at specified positions; it does not seek the best possible). The registration number and cipher trigram of the message are entered on the sheet at the time of punching it.

When the alphabets have been found, or even before they are complete, the clear trigram is written under the cipher one on the sheet. Bear in mind that the clear trigram gives the initial window setting of the message, and that the notches are on the rings, so the assumption of definite wheels in the M- and R- position leads to a definite conclusion as to what the distance is between two messages. Thus the distance from DGF to DJK (Exhibit 8) is 5 + (3x26) = 83 if the R-wheel has no turnover between F and K and is a single-notcher, but is 5 + (2x26) = 57 if it does have a turnover between F and K. If the R-wheel is a double-notcher, you cannot reach DJK from DGF; hence Banburying these two messages does not make a direct test on this hypothesis.

Comparing DGF and DJK at the interval 83 we find 6 coincidences in an overlap of 169, and at interval 57 we find 14 coincidences, including a bigram, in an overlap of 195. These results are entered on the Banburismus score sheet (Exhibit 7). Since wheel IV is the only one with a turnover between F and K, we enter 14 x over 195 in the column headed IV, the little x standing for a bigram. 6 over 169 is entered in columns I, II, III, and V. An X is placed in column VI (which means VII and VIII too, of course) meaning that the two-notchers are sitting this one out.

The remaining half dozen comparisons entered in Exhibit 7 are the only other fairly conclusive ones I found in about two days work. This stuff is like billiards - it is one thing to know the theory of impact and reflection, of draws and follows, reverse and running English, etc., and quite another to play the game with any degree of facility. In practice, anywhere from one to three of these score sheets are filled before your guess as to the R-wheel looks convincing, and then you must be ready with a second choice if the first "goes down" (i.e. fails, flops, fizzles) on the bombe. Generally the R-wheel is determined first by matching messages with first letter the same before the M-wheel is attempted. Otherwise you run into a multiplicity of intervals to compute and try.

The two-notchers are again inactive in the BNO/BON match, but the score of 11 in an overlap of 108, including a trigram (indicated by a little 3 encircled), looks so good that we are pretty sure the R-wheel is a single-notcher. TVL/TXK confirms this. GKM/GKZ and GUK/GZD make things look bright for II and IV. BLF/BNO looks very disappointing, since the expected number of coincidences in an overlap of 363 is 14. But here we observe that if the M-wheel is VI there would be a turnover between L and N, and on the strength of this my guess was that M = VI. The only direct confirmation of this(another day's work!) was AME/BON, and tests on other wheels gave negative results. For the R-wheel this gives a choice between IV and VI, and since IV was favored over II in DGF/DJK, my final guess was M = VI and R = IV. This proved to be correct.

I looked at the score sheets for a more recent day. There were three - one for R and two for M - all about full. There were two tetragraphic repeats, giving R and M both VI, and one score of 8 x /103 verifying the latter. The rest was absolute junk! The reason given is that there are increasingly many dummies. But they get it out regularly.

This brings us to ~~the final~~ point of "dummyismus". Each message is marked with a percentage (in Exhibit 8 both are 5%) indicating the probability that that message is a dummy, which is to be borne in mind when evaluating the Banbury score sheets. I give herewith excerpts from the table in present use, but which will shortly be brought up to date.

NORTH AFRICA

| | | | | | | |
|---|---|---|---|---|---|---|
| R | 3230 | 3236 | 3240 | 5907 | 5920 | 55% (0 to 12 hours)<br>20% (12 to 24 hours) |
| U | 3450 | 6520 | | | | 15% |
| L | 4040 | 5900 | 7485 | | | 15% |
| M | 3140 | 4600 | 4604 | 3750 | | 5% |
| K | 3620 | 4066 | 5065 | 8430 | | 5% |

AEGEAN

| | | | | |
|---|---|---|---|---|
| B | 3480 | 4850 | 4855 | Length: $0\,\frac{10\%}{35\%}\,30\,\frac{15\%}{45\%}\,40\,\frac{10\%}{35\%}\,50\,\frac{2\%}{6\%}$ |
| F | 402 | | | |
| G | 400 | | | (Use lower value if call sign not heard) |
| S | 3370 | 4350 | | |

BLACK SEA

Similar to North Africa, except that some stations are singled out. For example, for group P we find "AQH 40%, others 6%".

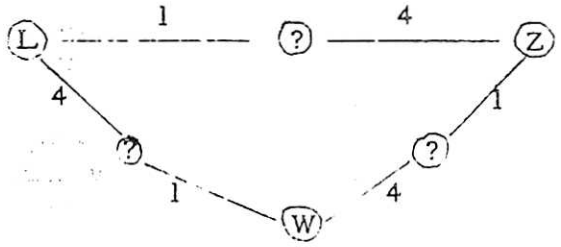
The letters are put on by Scarborough after the frequency, e.g. 3230R. Presumably they are groups of stations sending on the same frequency schedule. Note that in Aegean it is based solely on length, while mostly on groups in the other two. Incidentally, all North Africa call-signs begin with U, Aegean and Black Sea with A.

5. This completes the description of how the Grundstellung alphabets are found from the repeated indicator encipherment, with the aid of operators' habits, and how the wheel-orders to try on the bombe are limited by the Banbury process. The construction of menus out of

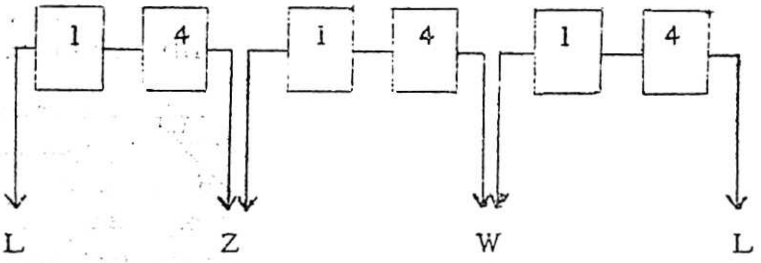
the alphabets is clear, and rodding a message with a crib is old stuff. But in connection with the latter, let me add that Banburismus may again play a part. For if tetragraphic repeats have been found, it is quite likely that one of these represents EINS. On the day mentioned above when two such were found, one of them failed but the other succeeded.

The remaining steps on the diagram page 3, are a matter of a minute or two, and should require no explanation.

A word, however, about getting out the paired day. While it would suffice to obtain the Grundstellung alphabets, these are not usually complete before midnight. But by 1800 enough of the throw-on sheet has been verified (by values occurring in more than one message) to form a "query" menu. If, for example, we had found the cycle (LZW) in the L-column of the throw-on sheet we could form the molecule



(This sort of thing occurs also in getting out the Grundstellung when the Bigram Tables are unknown.) The bombe is wired in exactly the same way as for an ordinary menu except that two machines separated by a query are wired directly to each other instead of via the diagonal board. Schematically, the wiring for the above portion of a menu would be thus:



There is also another feature worthy of note, namely that it is a so-called "hoppity" job. This term refers to any bombe job where the Ringstellung of the R-wheel is known, as it is in this case. It must be run on a bombe whose slowest wheel is the R-wheel, and in fact this is the reason for designing the newer models that way.

To illustrate the procedure, let us suppose that the core-position of the notch on the R-wheel is known to be between G and H, and let us suppose that we have a menu involving six successive positions, as would be the case here. The bombe would then be run in the following order.

|  | 1 | 2 - - - - | 21 | 22 | 23 | 24 | 25 | 26 |
|---|---|---|---|---|---|---|---|---|
| 1 | ZZH | ZZI | ZZB | ZZC | ZZD | ZZE | ZZF | ZZG |
| 2 | ZZI | ZZJ | ZZC | ZZD | ZZE | ZZF | ZZG | ZAH |
| 3 | ZZJ | ZZK | ZZD | ZZE | ZZF | ZZG | ZAH | ZAI |
| 4 | ZZK | ZZL | ZZE | ZZF | ZZG | ZAH | ZAI | ZAJ |
| 5 | ZZL | ZZM | ZZF | ZZG | ZAH | ZAI | ZAJ. | ZAK |
| 6 | ZZM | ZZN | ZZG | ZAG | ZAI | ZAJ | ZAK | ZAL |

The machines are originally set as indicated in column 1, i.e. each machine in position 1 is set at ZZH, each in position 2 at ZZI, etc. The bombe then runs through all 676 positions of the L- and M-wheels, after which the R-wheels all turn and we are in the position given by column 2. The bombe continues running until column 21 is complete. At this stage (at least formerly) the bombe is stopped and the M-wheel is advanced one notch in all machines pertaining to position 6. After 676 more positions, it is again stopped and the M-wheel advanced for position 5. This "hoppity" procedure is followed similarly through positions 4, 3, and 2. I understand that newer models are equipped with a device which does this automatically but this point must wait until my education reaches it. Presumably the wheels actually rotate in reverse direction, and the device paralyzes the carry-over mechanism at the proper time.

I believe it should be observed that there is no difference between a hoppity and an ordinary run if the crib is not broken by a turnover. It is in the latter case that the saving comes. For then (in the above example five additional runs of full length $26^3$ must be made if the Ringstellung of the R-wheel is not known or taken into account.

6. For possible future reference, a glossary of terms is appended herewith.

Banburismus: a method of finding coincidences between messages by punching them up on special (Banbury) sheets.

Box: a method of obtaining all possible constituent alphabets from the throw-on sheet by finding the paired cycles and sliding one under the reversal of its mate.

**Deciban:** an additive (logarithmic) unit of likelihood.

**Dud:** no-come-out; it may be a message in a different system.

**Dummyismus:** The art of ascribing to each message a probability that it is a dummy.

**Henno:** the hand-cipher companion of Sued.

**Hoppity Job:** a bombe job with known Ringstellung of the R-wheel.

**Menu:** mutton, brussel sprouts, boiled potatoes and steamed pudding with jam sauce.

**Porpoise:** British name for Sued.

**Query Menu:** A menu with some letters unknown.

**Rod:** as a verb it means to apply what we call the click process, a click really meaning just a confirmation; rod-position of a wheel or message means core-position.

**Screed:** you have just read one - maybe.

**Straight Keyboard:** a setting like RTZ straight off the keyboard.

**Sued:** Mediterranean naval enigma traffic (sued = south, of course).

**Throw-On Sheet:** sheet made up from repeated indicator encipherment.

**Winkle:** British name for Sued Offizier.

EXHIBIT 1

Throw-On sheet
For 17 May Med.

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

* Values from Msg. #1 p4

EXHIBIT 4

Frequencies of Cipher Indic. Letters (exh. 2)

| | L | M | R |
|---|---|---|---|
| A | 7 | 3 | 3 |
| B | 1 | 1 | 4 |
| C | 1 | 5 | 5 |
| D | 4 | 1 | 7 |
| E | 2 | 2 | 7 |
| F | 1 | 3 | 4 |
| G | 6 | 2 | 0 |
| H | 7 | 7 | 4 |
| I | 7 | 6 | 0 |
| J | 4 | 1 | 2 |
| K | 2 | 3 | 6 |
| L | 11 | 5 | 5 |
| M | 3 | 5 | 7 |
| N | 1 | 7 | 4 |
| O | 1 | 4 | 4 |
| P | 5 | 8 | 5 |
| Q | 1 | 4 | 4 |
| R | 10 | 3 | 4 |
| S | 2 | 1 | 3 |
| T | 5 | 6 | 3 |
| U | 2 | 0 | 3 |
| V | 1 | 9 | 3 |
| W | 2 | 5 | 2 |
| X | 3 | 3 | 4 |
| Y | 5 | 0 | 5 |
| Z | 6 | 3 | 3 |

I. C. 1.28 .1.12 0.98

EXHIBIT 5

Standard Table* For North Africa Indicators

| | L | M | R |
|---|---|---|---|
| A | -4 | 2 | 1 |
| B | 4 | 0 | 3 |
| C | -3 | -2 | -2 |
| D | 2 | 3 | 1 |
| E | -8 | -2 | -8 |
| F | 4 | 3 | 0 |
| G | 5 | 3 | 1 |
| H | 5 | 2 | -1 |
| I | -7 | 0 | -4 |
| J | -8 | -7 | -6 |
| K | 5 | 4 | 3 |
| L | 6 | 3 | 5 |
| M | 3 | 1 | 3 |
| N | 2 | 1 | 3 |
| O | -9 | 0 | -3 |
| P | 1 | 2 | 2 |
| Q | -12 | -5 | -5 |
| R | 4 | 4 | 2 |
| S | 1 | 2 | 2 |
| T | 1 | 2 | 4 |
| U | -11 | -4 | -7 |
| V | -3 | -4 | -2 |
| W | -1 | 0 | -1 |
| X | -7 | -5 | -4 |
| Y | -11 | -8 | -6 |
| Z | -2 | 0 | 1 |

* In half decibans

EXHIBIT 6

CORRECT GRUNDSTELLUNG ALPHABETS FOR 17 MAY MEDITERRANEAN

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

| Plain | | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 4 | L | N | I | G | V | P | J | C | Q | B | F | Y | X | T | A | U | E | H | Z | W | M | O | D | S | L | K | R |
| 5 | M | X | G | S | Z | P | L | B | O | V | K | J | F | N | M | H | E | U | Y | C | W | Q | I | T | A | R | D |
| 6 | R | N | G | L | X | Y | P | B | O | Q | W | M | C | K | A | H | F | I | V | T | S | Z | R | J | D | E | U |

TOP SECRET
ULTRA
EXHIBIT 2

## ENCIPHERED AND PLAIN INDICATORS OF 100 NORTH AFRICA MESSAGES (17 MAY)

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

Those starred mean all three letters close to each other, or two laterally adjacent, on enigma keyboard.

## EXHIBIT 3

ENIGMA KEYBOARD:

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

EXHIBIT 7

## BANBURISMUS SCORE SHEET

| | I | II | III | IV | V | VI | I | II | III | IV | V | VI |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| BLF/BNO | | | | | | X | 16<br>363 | ------→ | | 9<br>368 | 16<br>363 | X |
| BNO/BON | | | | | | | 11③<br>108 | ----------------→ | | | | X |
| DGF/DJK (Exh.8) | | | | | | | 6<br>169 | ------→ | | $14^x$<br>195 | 6<br>169 | X |
| GKM/GKZ | | | | | | | X | $8^x$<br>84 | X | $8^x$<br>84 | $8^x$<br>84 | X |
| GUK/GZD | | | X | | | | 5<br>113 | $7^{xx}$<br>87 | 5<br>113 | $7^{xx}$<br>87 | 5<br>113 | X |
| TVL/TXK | | | X | | | | $11^x$③<br>148 | ----------------→ | | | | X |
| AME/BON | X ----------→ | | | | | | 3<br>108 | ------→ | | $7^x$<br>108 | 3<br>108 | $7^x$<br>108 |

These columns refer to the M-wheel

These columns refer to the R-wheel

TOP SECRET
ULTRA

EXHIBIT 8A

MESSAGE D G F

| 5 | | | 6 | | | | | | | | | | 7 | | | | | | | | | | 8 | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 7 | 8 | 9 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| A | ⊘ | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A |
| B | B | B | B | B | B | B | B | B | B | B | B | B | B | B | B | B | ⊘ | B | B | B | B | B | B | B | B | B | ⊘ | ⊘ | B |
| C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C |
| D | D | D | D | D | D | D | D | D | ⊘ | D | D | D | D | D | D | D | D | D | D | D | D | D | D | D | D | D | D | D | D |
| E | E | E | E | E | E | E | E | E | E | E | F | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E |
| F | F | F | F | F | F | F | ⊘ | F | F | F | F | F | F | F | F | F | F | F | F | F | F | F | F | F | F | F | F | F | F |
| G | G | G | G | G | G | G | G | G | G | G | G | G | G | G | G | G | G | G | G | G | G | G | G | G | G | G | G | G | G |
| H | H | H | H | ⊘ | H | H | H | H | H | H | H | H | H | H | ⊘ | H | H | H | H | H | H | H | H | H | H | H | H | H | H |
| I | I | I | I | I | I | I | I | I | I | I | I | I | I | I | I | ⊘ | I | I | ⊘ | I | I | I | I | I | ⊘ | I | I | I | I |
| J | J | ⊘ | J | J | J | J | J | J | J | J | J | J | J | J | J | J | J | J | J | J | J | J | J | J | J | J | J | J | J |
| K | K | K | K | K | K | ⊘ | K | K | K | K | K | K | K | K | K | K | K | K | K | K | K | K | K | K | K | K | K | K | K |
| L | L | L | L | L | L | L | L | L | L | L | L | L | L | L | L | L | L | L | L | L | L | L | ⊘ | L | L | L | L | L | L |
| M | M | M | M | M | M | M | M | M | M | M | M | M | M | M | M | M | M | M | M | M | M | M | M | M | M | ⊘ | M | M | M |
| N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N |
| O | O | O | O | O | O | O | O | O | O | ⊘ | O | O | O | O | O | O | O | O | O | O | O | O | O | O | O | O | O | O | O |
| P | P | P | P | P | P | P | P | P | P | P | P | P | P | P | P | P | P | P | P | P | ⊘ | P | P | P | P | P | P | P | P |
| Q | Q | Q | Q | Q | Q | Q | Q | Q | Q | ⊘ | Q | Q | Q | Q | Q | Q | Q | Q | Q | Q | Q | Q | Q | Q | Q | Q | Q | Q | Q |
| R | R | R | ⊘ | R | R | R | R | R | R | R | R | R | R | R | R | R | R | R | R | R | R | R | R | R | R | R | R | R | R |
| S | S | S | S | S | S | S | S | S | S | S | S | S | ⊘ | S | S | S | S | S | S | S | ⊘ | S | ⊘ | S | S | S | S | S | S |
| ⊘ | T | T | T | T | T | T | T | T | T | T | ⊘ | T | T | T | T | T | T | T | T | T | T | T | T | ⊘ | T | T | T | T | T |
| U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U |
| V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V |
| W | W | W | W | W | W | W | W | W | W | W | W | W | W | ⊘ | W | W | W | W | W | W | W | W | W | W | W | W | W | W | W |
| X | X | X | X | X | X | X | X | X | X | X | ⊘ | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | ⊘ | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | |
| Z | Z | Z | Z | Z | ⊘ | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z |

Note: J X P T Y

EXHIBIT 8B

## MESSAGE D J K

| | | | | | | | | | 1 | | | | | | | | | | 2 | | | | | | | | | | 3 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 |
| A | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A |
| B | B | B | B | B | B | B | B | B | B | B | B | B | B | B | B | B | B | B | B | B | B | B | B | B | B | B | B | B | B |
| C | C | C | C | C | C | C | C | C | C | C | C | C | C | ⊘ | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C |
| D | D | D | D | D | D | D | D | D | D | D | D | D | D | D | D | D | D | D | D | D | D | D | D | D | D | D | D | D | D |
| E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | ⊘ | E | E | E | E | E | E | E | E | E | E | E | E | E |
| F | F | F | F | F | F | F | F | ⊘ | F | F | F | F | F | F | F | F | F | F | F | F | F | F | F | ⊘ | F | F | F | F | F |
| G | G | G | G | G | G | G | G | G | G | G | G | G | G | G | G | G | G | G | G | G | G | G | G | G | G | G | G | G | G |
| H | H | H | H | H | H | H | H | H | H | H | H | H | H | H | H | H | H | H | H | H | H | H | H | H | ⊘ | H | H | H | H |
| I | I | I | ⊘ | I | I | ⊘ | I | I | I | I | I | I | I | I | I | I | I | I | I | ⊘ | I | I | I | I | I | I | I | I | I |
| J | ⊘ | J | J | J | J | J | J | J | J | J | J | J | J | J | J | J | J | J | J | J | J | J | J | J | J | J | J | J | J |
| K | K | K | K | ⊘ | K | K | K | K | K | K | ⊘ | K | K | K | K | K | K | K | K | K | K | K | K | K | K | K | ⊘ | K | K |
| L | L | L | L | L | L | L | L | L | L | L | L | ⊘ | L | L | L | L | L | L | L | L | L | L | L | L | L | L | L | L | L |
| ⊘ | M | ⊘ | M | M | M | M | M | M | M | M | M | M | M | M | ⊘ | M | M | M | M | M | M | M | M | M | M | M | M | M | M |
| N | N | N | N | N | ⊘ | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N |
| O | O | O | O | O | O | O | O | O | O | O | O | O | O | O | O | O | O | O | O | O | O | O | O | O | O | O | O | O | O |
| P | P | P | P | P | P | P | P | P | P | P | P | P | P | P | P | P | P | P | ⊘ | P | P | P | P | P | P | P | P | P | P |
| Q | Q | Q | Q | Q | Q | Q | Q | Q | Q | Q | Q | Q | Q | Q | Q | Q | ⊘ | Q | Q | Q | ⊘ | Q | Q | Q | Q | Q | Q | Q | Q |
| R | R | R | R | R | R | R | R | R | R | R | R | R | ⊘ | R | R | R | R | R | R | R | R | R | R | R | R | R | R | R | R |
| S | S | S | S | S | S | S | S | S | S | S | S | S | S | S | S | S | S | ⊘ | S | S | S | S | S | S | S | ⊘ | S | S | S |
| T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | ⊘ | T | T | T | T | T | ⊘ |
| U | U | U | U | U | U | U | U | U | U | ⊘ | U | U | U | U | U | U | U | U | U | U | U | ⊘ | U | U | U | U | U | U | U |
| V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V |
| W | W | W | W | W | W | W | | W | W | W | W | W | W | W | W | W | W | W | W | W | W | W | W | W | W | W | W | W | W |
| X | X | X | X | X | X | X | X | X | X | ⊘ | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | ⊘ | Y |
| Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z |
| Note: | | | J | | | | | | | X | | | | | | | | | P | | | | T | | | | | Y | |

TOP SECRET
CREAM
EXHIBIT 80

*SUPER-POSITION OF MESSAGES D G F & D J K*

| | | | | | | | | | 1 | | | | | | | | | | 2 | | | | | | | | | | 3 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 |
| A | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A |
| B | B | B | B | B | B | B | B | B | B | B | B | B | B | B | B | B | B | B | B | B | B | B | B | B | B | B | B | B | B |
| C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C |
| D | D | D | D | D | D | D | D | D | D | D | D | D | D | D | D | D | D | D | D | D | D | D | D | D | D | D | D | D | D |
| E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E |
| F | F | F | F | F | F | F | F | F | F | F | F | F | F | F | F | F | F | F | F | F | F | F | F | F | F | F | F | F | F |
| G | G | G | G | G | G | G | G | G | G | G | G | G | G | G | G | G | G | G | G | G | G | G | G | G | G | G | G | G | G |
| H | H | H | H | H | H | H | H | H | H | H | H | H | H | H | H | H | H | H | H | H | H | H | H | H | H | H | H | H | H |
| I | I | I | I | I | I | I | I | I | I | I | I | I | I | I | I | I | I | I | I | I | I | I | I | I | I | I | I | I | I |
| J | // | J | J | J | J | J | J | J | J | J | J | J | J | J | J | J | J | J | J | J | J | J | J | J | J | J | J | J | J |
| K | K | K | K | K | K | K | K | K | K | K | K | K | K | K | K | K | K | K | K | K | K | K | K | K | K | K | K | K | K |
| L | L | L | L | L | L | L | L | L | L | L | L | L | L | L | L | L | L | L | L | L | L | L | L | L | L | L | L | L | L |
| M | M | M | M | M | M | M | M | M | M | M | M | M | M | M | M | M | M | M | M | M | M | M | M | M | M | M | M | M | M |
| N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N |
| O | O | O | O | O | O | O | O | O | O | O | O | O | O | O | O | O | O | O | O | O | O | O | O | O | O | O | O | O | O |
| P | P | P | P | P | P | P | P | P | P | P | P | P | P | P | P | P | P | P | // | P | P | P | P | P | P | P | P | P | P |
| Q | Q | Q | Q | Q | Q | Q | Q | Q | Q | Q | Q | Q | Q | Q | Q | Q | Q | Q | Q | Q | Q | Q | Q | Q | Q | Q | Q | Q | Q |
| R | R | R | R | R | R | R | R | R | R | R | R | R | R | R | R | R | R | R | R | R | R | R | R | R | R | R | R | R | R |
| S | S | S | S | S | S | S | S | S | S | S | S | S | S | S | S | S | S | S | S | S | S | S | S | S | S | S | S | S | S |
| T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | // | T | T | T | T | T | T | T |
| U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U |
| V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V |
| W | W | W | W | W | W | W | W | W | W | W | W | W | W | W | W | W | W | W | W | W | W | W | W | W | W | W | W | W | W |
| X | X | X | X | X | X | X | X | X | X | // | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | // | Y |
| Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z |