<table>
<thead>
<tr>
<th>Sections</th>
<th>General Explanation</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The Right-Hand Wheel</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>Wheel Squares</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>Useful Aspect of a Cylindrical Message</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>Solution</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>Particular Solutions I</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td>When the wheels are Known</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Rectangles</td>
<td>23</td>
</tr>
<tr>
<td></td>
<td>Particular Solution II</td>
<td>27</td>
</tr>
<tr>
<td></td>
<td>When the wheels are not Known</td>
<td></td>
</tr>
<tr>
<td></td>
<td>General Remarks</td>
<td>36</td>
</tr>
</tbody>
</table>

**Figures:**

- Fig. 1: page 2
- Fig. 2: 30
- Fig. 3: 4
- Fig. 4: 5
- Fig. 5: End of book
- Fig. 6: 
- Fig. 7: Loose Sheet No. 1
- Fig. 8: No. 2
- Fig. 9: page 12
- Fig. 10: Loose Sheet No. 3
- Fig. 11: No. 4
- Fig. 12: No. 5
- Fig. 13: No. 6
- Fig. 14: No. 7
- Fig. 15: page 26
- Fig. 16: 26
- Fig. 17: 28
- Fig. 18: Loose Sheet No. 8
Sections

1. General Explanation
2. The Right-Hand Wheel
3. Wheel Squares
4. Useful Aspects of a Graphed Message
5. Solution
6. Particular Solution I
   When the wheels are known
7. Rectangles
8. Particular Solution II
   When the wheels are not known
9. General Remarks

Figures:

Fig. 1. page 2
Fig. 2. 30
Fig. 3. 4
Fig. 4. 4
Fig. 5. End of book
Fig. 6
Fig. 7. Loose Sheet No. 1
Fig. 8. " No. 2
Fig. 9. page 12
Fig. 10. Loose Sheet No. 3
Fig. 11. " No. 4
Fig. 12. " No. 5
Fig. 13. " No. 6
Fig. 14. " No. 7
Fig. 15. page 26
Fig. 16. 26
Fig. 17. 28
Fig. 18. Loose Sheet No. 8
Fig. 19. page 32
Fig. 20. Loose Sheet No. 9
The Reciprocal Enigma.

General Explanation:

1. (a) The cyphering is done by 26 keys, 26 lights and 4 wheels.

(b) Three of the wheels are through faces and the fourth causes a return (see fig 2) at end of book.

(c) In figure 2, each strip represents a wheel. The numbers indicate the connections. Thus the 1 on the right hand side of the wheel is connected electrically with the 1 on the left hand side. In wheel IV the 1 is connected with the 1 on the same side etc.

If the setting of the wheels (given by the numbers on the left hand side) is 8, 17, 22, 23 4, then order IV III II I, then I become T if the key I be pressed the light I shines or if the key T be pressed the light I shines (see fig 1).

(d) When a key is pressed, first the right hand wheel is moved round one place and then the electrical connection is made. Thus if the setting were III II I; 8, 17, 22, 23 and the key I were pressed first the wheel II would move from position 22 to 23 and then light I would shine.

(e) When any wheel comes into position 1 the wheel on the left is at the same time moved up one place. Thus with setting IV, III II I; 8, 17, 22, 23, if the key T is pressed this moves I to position 1 or I to position 23 or the light 2 shines. Similarly with the next wheel. Wheel IV, however, is never moved by the keys.

(f) The wheels I, II, III can be put on in any order.

(g) All the wheels have faces with marked with letters which can take
(b) Three of the wheels are thorough fares and the fourth causes a return (see fig. 2) at end of book.

(c) In figure 2, each strip represents a wheel. The numbers indicate the connections. Thus the 1 on the right hand side of the wheel is connected electrically with the 1 on the left hand side. In wheel IV the 1 is connected with the 7 on the same side, etc.

If the setting of the wheels (given by the numbers on the left hand side) is 8, 17, 22, 23 in first order IV III I II, then I become 1 if the key I be pressed, the light I shines or if the key I be pressed the light I shines (see fig. 1).

(d) When a key is pressed, first the right hand wheel is moved round one place and then the electrical connection is made. Thus if the setting were III I II; 8, 17, 22, 23 and the key I were pressed, first the wheel II would move from position 22 to 23 and then light I would shine.

(e) When any wheel moves into position 1, the wheel on the left is at the same time moved up one place. Thus with setting IV, III I II; 8, 15, 22, 75 the key I is pressed, this moves II to position 1 and I to position 23 and the light I shines. Similarly with the next wheel. Wheel IV, however, is never moved by the keys.

(f) The wheels I, II, III can be put on in any order.

(g) All the wheels have tyres and are marked with letters which can take up any position relative to the wheels. The Primary Setting is
<table>
<thead>
<tr>
<th></th>
<th>A1</th>
<th>A2</th>
<th>A3</th>
<th>A4</th>
<th>A5</th>
<th>A6</th>
</tr>
</thead>
<tbody>
<tr>
<td>B1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>B2</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
</tr>
<tr>
<td>B3</td>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>17</td>
<td>18</td>
</tr>
</tbody>
</table>

Pairs given by setting IV, II, I, II:
8, 17, 22, -

Pairs given by setting N, II, I, II:
8, 17, 23, -
|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |

|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |

**Pens given by setting IV, II, I, II:** 8, 17, 22, -.

**Pens given by setting IV, II, I, II:** 8, 17, 23, -.

**Pens given by setting IV, II, I, II:** 8, 17, 24, -.

**Pens given by setting IV, II, I, II:** 8, 17, 25, -.
consists of the setting of these types. Thus suppose that

Primary Setting were IV, III, I, II, MBAP. The wheels
would be put on in the order indicated and the types fixed to the wheels
so that in IV the M on the type was over the 1 on the wheel, in III the
B on the type was over the 1 on the wheel etc.

(b) The Secondary Setting refers to the letters on the type opposite
the red line in figure 2, e.g. Secondary Setting = TRVK

When M is opposite 1, T is opposite 8, when B is opposite 1, R is opposite 12
When A is opposite 1, V is opposite 12, when P is opposite 1, K is opposite 12.

So Primary Setting MBAP; secondary setting TRVK means that
The actual setting is K, 12, 23, 12.

(c) The Primary Setting could be used for a period of time and the Secondary
Setting could be different for each message and sent with it.

The Right Hand Wheel.

2. (a) One aspect of the method is given below.

(b) Consider only the right hand wheel as in figure 3A and consider the remaining
wheels in a lump. The coloured columns of figures give the pairs caused by
wheels IV III I in the positions indicated. It is sometimes convenient to think
of the right hand wheel moving against a system of pairs for 26 letters
and then "switched" over to another system of pairs.

(c) A Message with primary setting MBAP (IV III II) and secondary setting TRVK
could be replaced with the wheel II moving from 23 to 16 against the violet bearing.
(b) The Secondary Setting refers to the letters on the type opposite the red line in figure 2, e.g.: Secondary Setting: TRVK.

When M is opposite 1, T is opposite 8, when B is opposite 1, R is opposite 8.
When A is opposite 3, V is opposite 22, when P is opposite 2, K is opposite 22.

So Primary Setting MBAP; Secondary setting TRVK means that the actual setting is 5, 17, 22, 12.

(c) The Primary Setting could be used for a period of time and the Secondary Setting could be different for each message and sent with it.

---

The Right Hand Wheel.

2. (c) One aspect of the method is given below.

(4) Consider only the right hand wheel as in figure 3A, and consider the remaining wheels in a lump. The coloured columns of figures give the pairs caused by wheels IV III I in the positions indicated. It is sometimes convenient to think of the right hand wheel moving against a system of pairs for 26 letters and then "switched" over to another system of pairs.

(c) A message with primary setting MBAP (III II I) & secondary setting TRVK could be explained with the wheel II moving from 23 to 16 against the violet pair & moving from 15 to 8 against the red pair, then the blue pair & then the green pair.
6 (a) Given (b) The general idea of the machine with the order
of letters QWERTY etc.

(c) The connections in the wheels.

(d) A cypher message.

(e) The first 15 letters of the clear message "SITUATION REPORT".

(f) The secondary setting, KCS1 which was sent with
the cypher message in distinguishable form.

Find. (g) The rest of the message.

(h) The primary setting.

(i) First tabulate the cypher message and the first fifteen letters
of the clear message as was done in figure 8. (fig 10) House Sheet No.3

(j) Make a list of the four and first fifteen pairs as in 4(i) (p. 9).

1. 0 + 4, d + 1
2. a + 2, d + 2
3. i + 3, m + 3
4. o + 4, s + 4
5. h + 5, u + 5
6. s + 6, l + 6
7. h + 7, u + 7
8. w + 8, k + 8
9. u + 9, c + 9
10. o + 10, g + 10
11. o + 11, g + 11
12. r + 12, b + 12
13. u + 13, m + 13
14. a + 14, b + 14
15. o + 15, m + 5

(d) Assume that the right hand wheel is I

and that the first letter is cyphered with it

in the position 1. Substitute for the letters

the values given by the 1st column in fig 9

starting at the 26th line i.e. 9 = 3, w = 14 etc.

We get the pairs. 1. 26, 10

2. 23, 18

3. 21, 19

4. 3, 15

5. 7, 11

6. 17, 23

6. conflicts with 5 + 2; the assumption made
(4) The first 15 letters of its clear message "SITUATION REPORT".

(5) The secondary setting, KCS1, which was sent with the ciphered message in distinguishable form.

Find: (a) The rest of the message.

(b) The primary setting.

(c) First tabulate the ciphered message and the first fifteen letters of the clear message as was done in figure 8. (fig 10) loose sheet 146

(d) Make a list of the seven and first fifteen pairs as in 4(c) (p. 9)

1. o + 1, d + 1
2. a + 2, d + 2
3. i + 3, m + 3
4. o + 4, s + 4
5. h + 5, u + 5
6. s + 6, w + 6
7. h + 7, u + 7
8. w + 8, k + 8
9. u + 9, c + 9
10. o + 10, g + 10
11. o + 11, j + 11
12. r + 12, b + 12
13. v + 13, n + 13
14. a + 14, f + 14
15. c + 15, t + 15

(d) Assume that the right-hand wheel is 1 and that the first letter is deciphered with it in the position 1. Substitute for the letters the values given by the 15th column in fig 9 starting at the 26th line: ix. g = 3, w = 14 etc.

We get the pairs: 1. 26, 10
2. 23, 11
3. 21, 19
4. 3, 15
5. 7, 17
6. 17, 23

6. Conflicts with 5 + 2: The assumption made above is incorrect.
(b) The correct assumption is that Wheel II is in position 22 and Wheel IV in position 6.

(q) The secondary setting was KCSI. The actual setting is 6, 22, 9, 5.

.: The primary setting was F H K E. IV II III.

Rectangles.

7. (a) Before proceeding to the reconstruction of the wheels from a crib, it is necessary to say something about rectangles.

(b) There are two in figure 8 and one in figure 10. In the former, figure if we joined the pairs 2 + 3 to each other we at the corners of a rectangle whose length measured horizontally is one unit. The pairs 24 7 + 26 are at the corners of a rectangle of length 19 units. In the latter figure the pairs 10, 11 form a rectangle of length one unit.

(c) When two pairs form a rectangle

(i) They must have the same range

(ii) The number of units in the length of the rectangle must equal the difference between the values of the pairs (+ a multiple of 26).

(d) For example in figure 8. The pairs 2 + 3 are respectively valued at 25, 12 at 26, 13. They have the same range of the length, number of units in the length of the rectangle is equal to the difference between the values of the pairs. The pairs 22 7 + 26 are respectively valued at 26, 3 and 19, 22. The same remark applies to this rectangle.

(e) Suppose in figure 8, instead of pairs 8, 39, 13, 44, 11, we had had pairs a, b, c, d 4e. It will be seen that the pairs a 4b, c 4d, e 42.
Rectangles.

7. (a) Before proceeding to the reconstruction of the wheels from a crib, it is necessary to say something about rectangles.

(b) There are two in figure 8 and one in figure 10. In the former figure, if we join the pairs 2 + 3 to each other at the corners of a rectangle whose length measured horizontally is one unit. The pairs 26, 7 + 26 are at the corners of a rectangle of length 19 units. In the latter figure, the pairs 10 + 11 form a rectangle of length one unit.

(c) When two pairs form a rectangle ① they must have the same range. ② The number of units in the length of the rectangle must equal the difference between the values of the pairs ( + a multiple of 26).

(d) For example in figure 8. The pairs 2 + 3 are respectively valued at 25, 12 & 26, 13. They have the same range. The number of units in the length of the rectangle is equal to the difference between the values of the pairs. The pairs 17 + 26 are respectively valued at 26, 3 and 19, 22. The same remark applies to this rectangle.

(e) Suppose in figure 8, instead of pairs 8, 3; 13, 4; 11, we had had pairs a, b, c, d & e. It will be seen that the pairs a + c, c + e, e + 42 form rectangles of length 31 units.
<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>Column</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td>Row</td>
<td>A</td>
<td>B</td>
<td>C</td>
<td>D</td>
<td>E</td>
<td>F</td>
<td>G</td>
<td>H</td>
<td>I</td>
</tr>
<tr>
<td>V</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IV</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>III</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>II</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MBAP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Secondary Setting TRVK.


Cyphered with wheels IV III I in position TRV.

Cyphered with wheels IV III I in position TRW.

Cyphered with wheels IV III I in position TRX.
Cyphered with wheels IV III I in position TRY.

" " " " " in position TRW.

" " " " " in position TRX.

" " " " " in position TRY.
8 (a) Given: 1) The general idea of the machine with the order of letters QWERTYD

2) A cypher message with a crib of 180 letters.

3) The secondary setting, sent in distinguishable form.

Find: 1) The 'relative values' of the connections in the wheels.

2) The primary setting.

(b) In the message given only the 'relative values' of the connections of only the two right-hand wheels can be found and the primary setting only of the right-hand wheel.

(c) The message and crib are tabulated on Horse Sheet No. 6 and the values of the pairs on Horse Sheet No. 7. (Figures 13 and 14 respectively)

(d) In figure 13 the rectangles are indicated.

(e) In figure 15 we enter the rectangles that might possess an inherent likeness. N.B. If the 'switch' occurs between the first pairs or between the second pairs of rectangles then there can be no 'inherent' likeness. The converse of this is not true.

(f) From figure 16 we can say that switch probably occurs at 12/13, 13/14, 14/15 or 16/17 and that the likenesses of 2 and 3 are least likely to be inherent.

(9) Consider 2 and 3 in Fig 15. If in 2, \( o - e = k - l = 14 \). Then in 3

\[ o - e = k - l = 8 \]

from 2 we get \( o - e + k - l = 38 \) by adding

\[ o - e + k - l = 38 \quad \text{and from 2} \]

\[ o - e + k - l = 38 \quad \text{which conflict. Similarly if in 3 we started with} \]

\[ o - e = k - l = 14 \quad \text{we should reach the same contradiction.} \]
Find the relative values of the connections in the figure.

2. The primary setting.

(6) In the message given only the 'relative values' of the connections of only the two right hand wheels can be found and the primary setting only of the right hand wheel.

(6) The message and crib are tabulated in House Sheet No. 6 and the values of the pairs on House Sheet No. 7. (Figures 13 and 14 respectively.)

(6) In figure 13 the rectangles are indicated.

(6) In figure 15 are entered the rectangles that might possess an inherent likeness. N.B. If the 'switch' occurs between the first pairs or between the second pairs of rectangles then there can be no inherent likeness. The converse of this is not true.

(6) From figure 16 we can say that switch probably occurs at 12/13, 12/14, 14/15 or 16/17 and that the likenesses of (2) and (5) are least likely to be inherent.

(6) Consider (6) and (6) in Fig. 15. If in (6) \( a - e = k - l = 19 \). Then in (6) 
\[
0 - l = k - e = 4. \quad \text{from (6) we get} \quad 0 - l + k - e = 8 \quad \text{by adding}
\]
\[
0 - e + k - l = 38 \quad \text{from (6) } \quad 0 - e + k - e = 8 \quad \text{which conflict. Similarly if in (6) we started with} \quad 0 - l = k - e = 14 \quad \text{we should reach the same contradiction.}
\]

At 12/13 only one pair of rectangles \((12,13)\) needs to have only a fortuitous likeness.

If a 'switch' occurs as 12/13 8 sets of rectangles have only a fortuitous likeness.