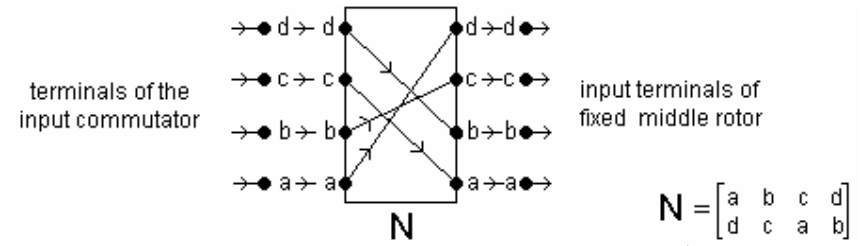
The Polish recovery of the Enigma Rotor wiring
(An application of the mathematics of permutations)

In 1932 the German Enigma operational procedure was to prescribe for each day a set of rotor starting positions to be used by all operators to doubly encipher their own message settings (resulting in six-letter indicators). This meant that there were some days when the middle and left-hand rotors did not move during these double encipherments.
The Polish mathematician Marian Rejewski showed that on such days the Enigma permutations generated at the six successive positions of the right-hand rotor could be represented by a set of six equations, which he hoped could be used to solve the problem of the finding the unknown wiring in the rotors. An explanation of his brilliant mathematical work is given below.

A preliminary note on the permutations due to the right-hand rotor:-

(an illustrative example using a simplified rotor with 4 terminals)

Let N be the permutation due to the right-hand rotor when at its initial starting position prior to the double encipherment of a message setting.

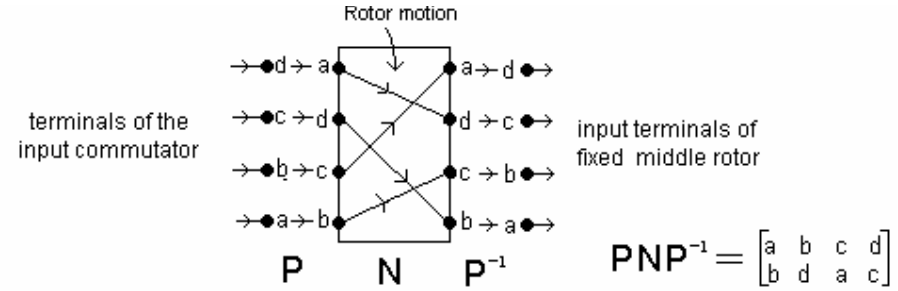


$$N = \begin{bmatrix} a & b & c & d \\ d & c & a & b \end{bmatrix}$$

Representing the permutation of the right-hand rotor when at the 1st position of the encipherment:-
Let P be the permutation between the commutator and the right hand rotor at this position

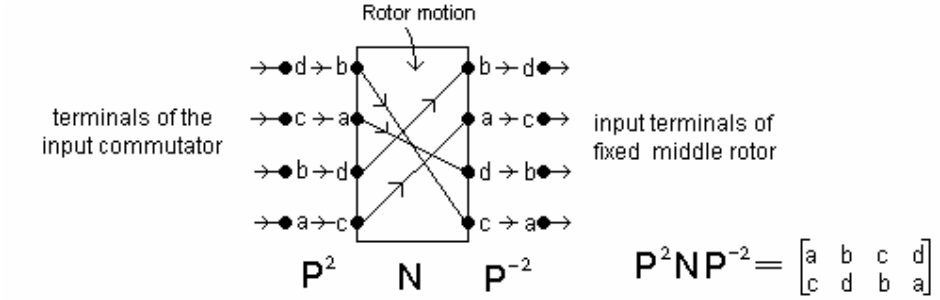
$$P = \begin{bmatrix} a & b & c & d \\ b & c & d & a \end{bmatrix} \quad \text{and} \quad P^{-1} = \begin{bmatrix} a & b & c & d \\ d & a & b & c \end{bmatrix}$$

Then at the 1st position as shown below the permutation of the right-hand rotor is $P.N.\ P^{-1}$



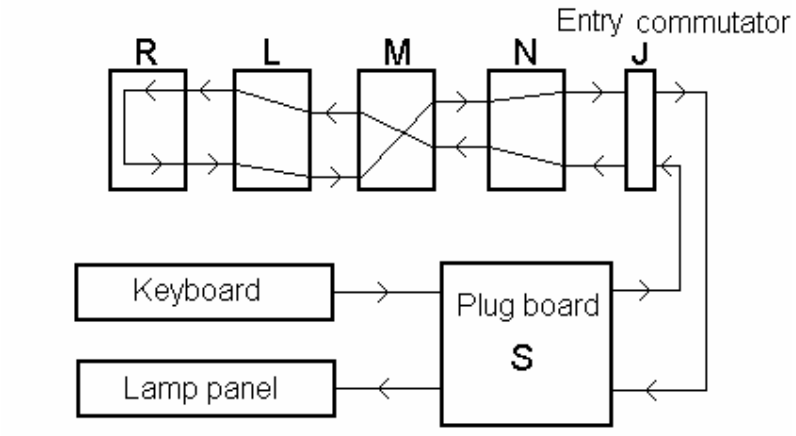
$$PNP^{-1} = \begin{bmatrix} a & b & c & d \\ b & d & a & c \end{bmatrix}$$

Likewise at the 2nd position as shown below the permutation is $P^2.N.\ P^{-2}$



$$P^2NP^{-2} = \begin{bmatrix} a & b & c & d \\ c & d & b & a \end{bmatrix}$$

(The permutation of the rotor at its n^{th} position is represented by the expression: $\mathbf{P^n\ N\ P^{-n}}$)



Let the Enigma permutations at the each of the six positions of the double encipherment of the message settings be:- position 1 2 3 4 5 6
Enigma permutation **A** **B** **C** **D** **E** **F**

Then with reference to the above diagram:-

A = $S.J.P.N.P^{-1}.M.L.R.L^{-1}.M^{-1}P.N^{-1}.P^{-1}.J^{-1}.S^{-1}$
B = $S.J.P^{2}.N.P^{-2}.M.L.R.L^{-1}.M^{-1}.P^{2}.N^{-1}.P^{-2}.J^{-1}.S^{-1}$
C = $S.J.P^{3}.N.P^{-3}.M.L.R.L^{-1}.M^{-1}.P^{3}.N^{-1}.P^{-3}.J^{-1}.S^{-1}$
D = $S.J.P^{4}.N.P^{-4}.M.L.R.L^{-1}.M^{-1}.P^{4}.N^{-1}.P^{-4}.J^{-1}.S^{-1}$
E = $S.J.P^{5}.N.P^{-5}.M.L.R.L^{-1}.M^{-1}.P^{5}.N^{-1}.P^{-5}.J^{-1}.S^{-1}$
F = $S.J.P^{6}.N.P^{-6}.M.L.R.L^{-1}.M^{-1}.P^{6}.N^{-1}.P^{-6}.J^{-1}.S^{-1}$

Where P = $\begin{bmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z & a \end{bmatrix}$

On a particular day the composite permutations **A.D** **B.E** and **C.F** were found from the intercepted messages (about 80 –100 were required for this purpose).
One example to show how this was done:- Suppose that an unknown message setting was $\alpha\beta\delta$ and that after its double encipherment the corresponding indicator was:- k t z s r f.
It follows that α.**A** = k and α.**D** = s. Given k = α**A**, and **A** is an Enigma permutation, it then follows that k.**A** = α**A.A** = α , and so k.**A.D** = α.**D** = s.
Thus one of the transpositions from the composite permutation **A.D** is (k s). In this way the transpositions in all of the composite permutations were found.

In order to determine the permutation produced by the right-hand rotor N it was first necessary to resolve the composite permutations **A.D**, **B.E** and **C.F** into the component Enigma permutations **A**, **B**, **C**, **D**, **E**, and **F**.
For this task Rejewski applied a theorem that states that:- '*The permutation cycles of the composite permutations always occur in pairs of equal length'.*
An illustrative example:-

A = $\begin{bmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ s & r & w & i & v & h & n & f & d & o & l & k & y & g & j & t & x & b & a & p & z & e & c & q & m & u \end{bmatrix}$

D = $\begin{bmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ s & w & r & j & p & t & q & k & v & d & h & x & o & z & m & e & g & c & a & f & y & i & b & l & u & n \end{bmatrix}$

A.D = $\begin{bmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ a & c & b & v & i & k & z & t & j & m & x & h & u & q & d & f & l & w & s & e & n & p & r & g & o & y \end{bmatrix}$

The composite permutation **A.D** contains the following cycles;-
C1 = (a) , C2 = (b c), C3 = (d v p f k x g z y o), C4= (e i j m u n q l h t),
C5= (r w), and C6= (s). It will be observed that the cycles occur in pairs of equal length. i.e. C1 & C6, C2 & C5, C3 & C4

The converse of Rejewski's theorem is also true:-'*If any permutation of even degree is composed of pairs of cycles of equal length then it can be resolved into two component permutations each of which is made up of pairs of transpositions'* (i.e. Enigma type permutations).
This justified the assumption that the composite permutation **A.D** could be resolved into its components **A** and **D**.

Resolving the composite permutation (**A.D**) into a pair of components **A** and **D**.
An examination of the cycles in **A.D** given above will show that the letters from the transpositions in the permutations **A** and **D** always appear in different cycles of the same length in the composite permutation **A.D**.
For example the transposition (b r) is from permutation **A** and it can be seen that b $\in$ C2 and r $\in$ C5 and that the two cycles C2 & C5 are of the same length.
Likewise the transposition (d j) is from the permutation **D** and d $\in$ C3 and j $\in$ C4 and that the two cycles C3 and C4 are of the same length.
Suppose that (α_1 α_2 α_3 α_4.....α_n) is one of the cycles of length n from **A.D**
If (α_1 β_1) is a transposition from **A** then there must be a transposition from **D** of the form (β_1 α_2) because of the cycle structure (α_1 α_2 …).
Likewise if (α_2 β_2) is another transposition from **A** then there must be a transposition from **D** of the form (β_2 α_3), because of the cycle structure (α_1 α_2 α_3 …)
This process can be continued with no loss of generality until the $(n + 1)^{th}$ step when $\alpha_{n+1} = \alpha_1$ (i.e. all the elements in the cycle have been used as first elements in the chosen transpositions).
This exhaustive process gives rise to the following two sets of transpositions.
Transpositions from **A**: (α_1 β_1) (α_2 β_2) (α_3 β_3) …… (α_{n-1} β_{n-1}) (α_n β_n)
Transpositions from **D**: (β_1 α_2) (β_2 α_3) (β_3 α_4) ……(β_{n-1} α_n) (β_n α_1)
Starting from the left hand side the following sequence of (n –1) pairs of transpositions generate the cycle (α_1 α_2 α_3 ...α_{n-1}.α_n) from **A.D** as is demonstrated below:

From **A**: ($\boldsymbol{\alpha_1}$ β_1) ($\boldsymbol{\alpha_2}$ β_2) ($\boldsymbol{\alpha_3}$ β_3) ……($\boldsymbol{\alpha_{n-1}}$ β_{n-1})
↓ ↓ ↓ ↓
From **D**: (β_1 $\boldsymbol{\alpha_2}$) (β_2 $\boldsymbol{\alpha_3}$) (β_3 $\boldsymbol{\alpha_4}$) …… (β_{n-1} $\boldsymbol{\alpha_n}$)

Starting from the right-hand side, another sequence of (n -1) pairs of transpositions (written in the alternative way), generate another cycle (β_n β_{n-1} β_{n-2} ..... β_2 β_1) of length n from **A.D**:-

From **A**: ($\boldsymbol{\beta_n}$ α_n) ($\boldsymbol{\beta_{n-1}}$ α_{n-1}) ($\boldsymbol{\beta_{n-2}}$ α_{n-2}) …….. ($\boldsymbol{\beta_2}$ α_2)
↓ ↓ ↓ ↓
From **D**: (α_n $\boldsymbol{\beta_{n-1}}$) (α_{n-1} $\boldsymbol{\beta_{n-2}}$) (α_{n-2} $\boldsymbol{\beta_{n-3}}$) ….. …… (α_2 $\boldsymbol{\beta_1}$)

Thus it is established that if **A.D** contains the cycle (α_1 α_2 α_3 ... α_{n-1} α_n) then it will also contain another cycle of the same length (β_n β_{n-1} β_{n-2} …… β_2 β_1)

It can be seen that if the elements in the second cycle are written in the **reverse order** below the elements of the first cycle, the vertical pairs of characters form the transpositions in permutation **A**:- (α_1 α_2 α_3 ... α_{n-1} α_n)
(β_1 β_2 β_3 ... β_{n-1} β_n)

A very similar procedure will lead to the transpositions in permutation **D**:-

$(\beta_1\ \beta_2\ \beta_3\ \ldots\ \ \beta_{n-1}\ \beta_n)$
$(\alpha_2\ \alpha_3\ \alpha_4\ \ldots\ldots\ \alpha_n\ \alpha_1)$

However if none of the individual transpositions are known then there will be many possible alignments of the permutation cycles from the composite **A.D** each leading to a different pair of solutions for permutations **A** and **D.** In the given example **A.D** contains pairs of cycles of lengths 1, 2 and 10 and consequently there are 2×10 possible pairs of solutions for **A** and **D**. To resolve the composite permutation **A.D** into the unique pair of the true original components, requires that each pair of cycles is vertically aligned in the correct relationship with one another, and to achieve this it is necessary to know some of the transpositions from **A** and **D** that involve letters from every cycle.

Rejewski succeeded in this task by identifying in the daily cipher traffic a significant number of repeats of the doubly enciphered message settings that he suspected were the result of operators using certain stereotype three-letter groups. With lower case letters representing the characters of the message settings he guessed correctly that these included 'aaa', 'bbb', 'ccc', and 'sss'. For example on a particular day the indicator letter sequence syx scw occurred five times and Rejewski guessed (correctly) that these were the result of the repeated use by the operators of 'aaa' as message settings, that implied:-
a.**A** = s , a.**B** = y, a.**C** = x, a.**D** = s, a.**E** = c and a.**F** = w. These results correspond to the transpositions (a s) in **A**, (a y) in **B**, (a x) in **C**, (a s) in **D**, (a c) in **E** and (a w) in **F**.

The three composite permutations found in this way by Rejewski are:-

A.D = (a) (s) (b c) (r w) (d v p f k x g z y o) (e i j m u n q l h t)

B.E = (d) (k) (a x t) (c g y) (b l f q v e o u m) (h j p s w i z r n)

C.F = (a b v i k t j g f c q n y) (d u z r e h l x w p s m o)

In attempting the task of decomposing these into their components the most straightforward one to consider first is **C.F** as it only contains two cycles. Writing these two cycles one above the other but with the second one in the reverse order gives:- (a b v i k t j g f c q n y)
(o m s p w x l h e r z u d)
However assuming that permutation **C** contains the transposition (a x), the correct alignment of the two cycles must be:- (**a** b v i k t j g f c q n y)
(**x** l h e r z u d o m s p w)
From this all of the thirteen transposition in permutation **C** can be readily found:-
(a x) (b l) (v h) (i e) (k r) (t z) (j u) (g d) (f o) (c m) (q s) (n p) (y w)

The transpositions in **F** can also be found from the original tabulation of the two cycles given above:- (a b v i k t j g f c q n y)
(o m s p w x l h e r z u d)
Assuming that **F** contains the transposition (a w), the correct alignment of the cycles is :-
(c q n y **a** b v i k t j g f)
(o m s p **w** x l h e r z u d)
Then from the correct alignment all the transpositions in permutation **F** can be found:-
(c o) (q m) (n s) (y p) (a w) (b x) (v l) (i h) (k e) (t r) (j z) (g u) (f d)

Another indicator letter sequence intercepted three times on the same day was 'sjm spo'
As it had been assumed that the permutation **A** contained the transposition (a s) then it could be inferred that the corresponding message setting was of the form 'a??'.

Moreover as it had been deduced that permutation **C** contained the transposition (c m) the message setting could be narrowed down to the form 'a?c'. (This hypothesis was reinforced by the occurrence of transposition (o c) in permutation **F** and of the transposition (a s) in permutation **D**). The assumption was made that the message setting was in fact 'abc', which inferred that the permutation **B** contains the transposition (b j) and the permutation **E** contains the transposition (b p); it has already been assumed that **B** contains the transposition (a y). These results can then be applied in the following way:-
First the pairs of cycles from **B.E** are written one above the other with the cycles in the second row in the reverse order:- (d) (a x t) (b l f q v e o u m)
(k) (y g c) (n r z i w s p j h)

The above transpositions can then be used to correctly align the cycles:-
(d) (**a** x t) (**b** l f q v e o u m)
(k) (**y** g c) (**j** h n r z i w s p)

From these alignments all of the transpositions in **B** are readily obtained:-
(d k) (a y) (x g) (t c) (b j) (l h) (f n) (q r) (v z) (e i) (o w) (u s) (m p)

All of the transpositions in **E** can also be found in the same way starting again with:-
(d) (a x t) (b l f q v e o u m)
(k) (y g c) (n r z i w s p j h)

The transpositions (a c) and (b p) from permutation **E** are used to make the correct alignments:- (d) (x t **a**) (q v e o u m **b** l f)
(k) (y g **c**) (n r z i w s **p** j h)

Hence all of the transpositions in **E** are:-
(d k) (x y) (t g) (a c) (q n) (v r) (e z) (o i) (u w) (m s) (b p) (l j) (f h)

It now remains to find the transpositions in the permutation **A.D**.
The indicator letter sequence ' r j l wpx' occurred four times, and by using the 'known' transpositions (b j) from permutation **B** and (b l) from permutation **C**, the form of the corresponding message setting was narrowed down to '?bb'. It was assumed that the message setting was in fact 'bbb' which in turn implied that permutation **A** contained the transposition (b r) and permutation **D** the transposition (b w). However these conclusions did not enable the two cycles of order ten to be correctly aligned and yet another intercepted letter sequence had to be identified for this purpose. The letter sequence 'ldr hde' occurred twice. By using transposition (k r) from permutation **C**, (e k) from permutation **F,** (d k) from permutation **B**, and (k d) from permutation **E** there was strong evidence to support the assumption that the corresponding message setting was 'kkk'.
This assumption in turn implied that the permutation **A** contained the transposition (l k) and the permutation **D** contained the transposition (h k). These conclusions were then used to correctly align the pairs of cycles from **A.D** in the way previously described.

First by writing them one above the other with those in the second row in the reverse order:-
(a) (b c) (d v p f k x g z y o)
(s) (w r) (t h l q n u m j i e)

and then using the transpositions to align them correctly:-
(a) (**b** c) (d v p f **k** x g z y o)
(s) (**r** w) (i e t h **l** q n u m j)

Thus all of the transpositions in **A** are:-
(a s) (b r) (c w) (d i) (v e) (p t) (f h) (k l) (x q) (g n) (z u) (y m) (o j)

Finally all of the transpositions in **D** were found by starting again with:-

(a) (b c) (d v p f k x g z y o)
(s) (w r) (t h l q n u m j i e)

and using the transpositions (b w) and (h k) from permutation **D** to correctly align them:-

(a) (**b** c) (f **k** x g z y o d v p)
(s) (**w** r) (t **h** l q n u m j i e)

From this alignment all of the transpositions in **D** were recovered:-

(a s) (b w) (c r) (f t) (k h) (x l) (g q) (z n) (y u) (o m) (d j) (v i) (p e)

The transpositions of the six Enigma permutations **A**, **B**, **C**, **D**, **E**, and **F**, now written in a particular order, were:-

A = (a s) (b r) (c w) (d i) (e v) (f h) (g n) (j o) (k l) (m y) (p t) (q x) (u z)
B = (a y) (b j) (c t) (d k) (e i) (f n) (g x) (h l) (m p) (o w) (q r) (s u) (v z)
C = (a x) (b l) (c m) (d g) (e i) (f o) (h v) (j u) (k r) (n p) (q s) (t z) (w y)
D = (a s) (b w) (c r) (d j) (e p) (f t) (g q) (h k) (i v) (l x) (m o) (n z) (u y)
E = (a c) (b p) (d k) (e z) (f h) (g t) (i o) (j l) (m s) (n q) (r v) (u w) (x y)
F = (a w) (b x) (c o) (d f) (e k) (g u) (h i) (j z) (l v) (m q) (n s) (p y) (r t)

Having determined these transpositions the next stage of the work was to find, by means of the set of equations given on page 2, the required permutation N.

Rejewski first simplified these equations by means of the following substitutions:-

$Q = M\,LR\,L^{-1}\,M^{-1}$ $\quad U = N\,P^{-1}Q\,PN^{-1}$
$V = N\,P^{-2}Q\,P^{2}\,N^{-1}$ $\quad W = N\,P^{-3}Q\,P^{3}\,N^{-1}$
$X = N\,P^{-4}Q\,P^{4}\,N^{-1}$ $\quad Y = N\,P^{-5}Q\,P^{5}\,N^{-1}$
$Z = N\,P^{-6}Q\,P^{6}\,N^{-1}$ $\quad H = N\,PN^{-1}$

Then making these substitutions in the original equations:-

$\mathbf{A} = SJ\,P\,N\,P^{-1}Q\,PN^{-1}\,P^{-1}J^{-1}\,S^{-1} \Rightarrow \mathbf{A} = SJPU\,P^{-1}\,J^{-1}\,S^{-1}$
$\mathbf{B} = SJP^{2}\,N\,P^{-2}Q\,P^{2}\,N^{-1}\,P^{-2}\,J^{-1}\,S^{-1} \Rightarrow \mathbf{B} = SJP^{2}V\,P^{-2}J^{-1}S^{-1}$
$\mathbf{C} = SJP^{3}\,N\,P^{-3}Q\,P^{3}\,N^{-1}\,P^{-3}\,J^{-1}\,S^{-1} \Rightarrow \mathbf{C} = SJP^{3}W\,P^{-3}J^{-1}S^{-1}$
$\mathbf{D} = SJP^{4}\,N\,P^{-4}Q\,P^{4}\,N^{-1}\,P^{-4}\,J^{-1}\,S^{-1} \Rightarrow \mathbf{D} = SJP^{4}X\,P^{-4}J^{-1}S^{-1}$
$\mathbf{E} = SJP^{5}\,N\,P^{-5}Q\,P^{5}\,N^{-1}\,P^{-5}\,J^{-1}\,S^{-1} \Rightarrow \mathbf{E} = SJP^{5}Y\,P^{-5}J^{-1}S^{-1}$
$\mathbf{F} = SJP^{6}\,N\,P^{-6}Q\,P^{6}\,N^{-1}\,P^{-6}\,J^{-1}\,S^{-1} \Rightarrow \mathbf{F} = SJP^{6}Z\,P^{-6}J^{-1}S^{-1}$

The equation $\mathbf{A} = SJPU\,P^{-1}J^{-1}S^{-1}$ can be rewritten as $\mathbf{A}SJP = SJPU$
and hence $U = P^{-1}J^{-1}S^{-1}\mathbf{A}SJ\,P$ In a similar way:- $V = P^{-2}\,J^{-1}S^{-1}\mathbf{B}SJ\,P^{2}$

$W = P^{-3}\,J^{-1}S^{-1}\mathbf{C}SJ\,P^{3}$ $\quad X = P^{-4}\,J^{-1}S^{-1}\mathbf{D}SJ\,P^{4}$
$Y = P^{-5}\,J^{-1}S^{-1}\mathbf{E}SJ\,P^{5}$ $\quad Z = P^{-6}\,J^{-1}S^{-1}\mathbf{F}SJ\,P^{6}$

To make further progress it was necessary to find the unknown permutations J and S. The permutation S was known for the day in question from the Enigma settings that had been obtained by espionage. The discovery of the permutation J was less straightforward. At first Rejewski had assumed that it was the same as for the 'commercial ' Enigma machine that the Polish Cipher Bureau had purchased, but as he states '*I later found this hypothesis was mistaken, and its adoption caused much unnecessary work and considerable loss of time, so that we nearly broke off the studies of Enigma.'* He also wrote:- *'I obtained those connections by guessing. I assumed that since the keyboard keys were not connected with the successive contacts in the entry commutator in the order of the letters on the keyboard* (i.e. Q W E R T Z ..) *then maybe they were connected up in alphabetical order'.*

So Rejewski assumed (correctly) that the permutation J was equal to the identity permutation:-

$$I = \begin{bmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \end{bmatrix}$$

This meant that the term J could be removed from the equations, and with S known the permutations U, V, W, X, Y and Z could be determined. Then using the composite permutations UV, VW, WX, XY and YZ Rejewski derived another set of equations from which it was possible to determine the permutation N.
The derivation of these equations required considerable algebraic manipulation in order to eliminate the unknown expression $Q\ P^{-1}Q\ P$ (Q represented the unknown composite permutation of the reflector together with middle and left-hand rotors).

Consider the composite UV:-
As $U = P^{-1}S^{-1}\mathbf{A}SP$ and $V = P^{-2}S^{-1}\mathbf{B}SP^2$ $\quad UV = P^{-1}S^{-1}\mathbf{A}SP\ P^{-2}S^{-1}\mathbf{B}SP^2$

$= P^{-1}S^{-1}\mathbf{A}SP^{-1}S^{-1}\mathbf{B}SP^2$

Then as $\mathbf{A} = S\ P\ N\ P^{-1}Q\ PN^{-1}\ P^{-1}\ S^{-1}$ and $\mathbf{B} = S\ P^2\ N\ P^{-2}Q\ P^2\ N^{-1}\ P^{-2}\ S^{-1}$

after making these substitutions (shown in heavy type):-

$UV = P^{-1}S^{-1}(\mathbf{S\ P\ N\ P^{-1}Q\ PN^{-1}\ P^{-1}\ S^{-1}})SP^{-1}S^{-1}(\mathbf{S\ P^2\ N\ P^{-2}Q\ P^2\ N^{-1}\ P^{-2}\ S^{-1}})SP^2$

$= N\ P^{-1}Q\ PN^{-1}\ P^{-1}S^{-1}SP^{-1}S^{-1}S\ P^2\ N\ P^{-2}Q\ P^2\ N^{-1}$

$= N\ P^{-1}Q\ PN^{-1}\ P^{-2}\ P^2\ N\ P^{-2}Q\ P^2\ N^{-1}$

$= N\ P^{-1}Q\ P^{-1}Q\ P^2\ N^{-1}$

Hence $UV = N\ P^{-1}(Q\ P^{-1}Q\ P)P\ N^{-1}$ or alternatively $Q\ P^{-1}Q\ P = PN^{-1}UVNP^{-1}$

In a similar way it can be shown that $V\ W = N\ P^{-2}(Q\ P^{-1}Q\ P)P^2\ N^{-1}$

and $WX = N\ P^{-3}(Q\ P^{-1}Q\ P)P^3\ N^{-1}$

The expression $Q\ P^{-1}Q\ P$ can be eliminated by the substitution $Q\ P^{-1}Q\ P = PN^{-1}UVNP^{-1}$
so that expression for V W can be rewritten as $N\ P^{-2}\ (PN^{-1}UVNP^{-1})P^2N^{-1}$

so that $V\ W = N\ P^{-2}\ PN^{-1}(UV)NP^{-1}P^2\ N^{-1}$

$= NPN^{-1}(UV)NPN^{-1}$

Leading finally to $V\ W = H^{-1}(U\ V)\ H$ (since $H = NPN^{-1}$)

Likewise $W\ X = H^{-1}(V\ W)\ H$

$X\ Y = H^{-1}(W\ X)\ H$

$Y\ Z = H^{-1}(X\ Y)\ H$

As the composite permutations UV, VW, WX, XY had been found this final set of equations could be used to determine H.

Finally the equation $H = NPN^{-1}$ was used to determine N.

<u>A note on 'Similar permutations'</u>
The last two stages of the work described above involve permutation equations of the form $K = T\ LT^{-1}$ where K, T, and L are permutations on the same set of elements.
and from which solutions for T are required for given permutations K and L.
The permutations K and L are an example of a pair of '*similar permutations*' and in order to solve his final equations Rejeweski used the following theorem relating to such permutations:-
Two permutations K and L on the same set of elements are similar if and only if they have the same cycle structure.

A proof: (part i) Suppose that $K = T\ LT^{-1}$ and let x be an element of a cycle of length n from the permutation L, so that x, $x.L$, $x.L^2$, $x.L^3$ … will form the sequence of elements in the cycle. Then by definition $x.\ L^n = x$ (since the cycle is of length n)

Let $y.T = x$ so that $y = x.T^{-1}$ (continued below)

Consider the expression y. $K^n = y.(T\,LT^{-1})^n$

$= y.(T\,LT^{-1}\,T\,LT^{-1}\,T\,LT^{-1}\ldots\ldots)$ (n terms)

$= y.T\,L^nT^{-1}$

$= x.L^n\,T^{-1} = x.T^{-1} = y$

Thus the permutation K (= TLT^{-1}) also contains a cycle of length n, thus establishing that the cycles in the two permutations can be matched into pairs of the same length.

Proof (part ii). Suppose that the permutations K and L have the same cycle structure and that x is an element of a chosen cycle of length n from K, and y is an element from a corresponding cycle of length n from L.
consider the following sequences of elements from these two cycles:
Elements of the cycle of K:- $x \quad x.K \quad x.K^2 \quad x.K^3 \quad x.K^4 \ldots\ldots\ldots\ldots x.K^{n-1}$
Elements of the cycle of L:- $y \quad y.L \quad y.L^2 \quad y.L^3 \quad y.L^4 \ldots\ldots\ldots\ldots y.L^{n-1}$

Let T be the permutation formed by the vertical pairs of elements from the two cycles.
Then it follows from the first two pairs that x.T = y and x.KT = y.L.
Hence x.KT = x.TL $\Rightarrow$ KT = TL from which $K = TLT^{-1}$. The same outcome is obtained from any two adjacent vertical pairs of elements. In a similar way the permutation T can be extended to cover all of the pairs of cycles in K and L.
Note: this approach enables all possible forms of the permutation T to be determined.
A mini example:

Given permutations K and L to find a permutation T so that $K = TLT^{-1}$

$$K = \begin{bmatrix} a & b & c & d & e \\ c & e & d & a & b \end{bmatrix} \qquad L = \begin{bmatrix} a & b & c & d & e \\ c & a & b & e & d \end{bmatrix}$$

Cycle structure of K: (a c d) (b e)

Cycle structure of L: (a c b) (d e)

By first aligning the elements of the K cycles above an arbitrary ordering of the elements of the corresponding L cycles:-

(a c d) (b e)
(b a c) (e d)

a solution for T is then found by re-ordering the vertical pairs $T = \begin{bmatrix} a & b & c & d & e \\ b & e & a & c & d \end{bmatrix}$

A direct verification of this result is as follows:-

$$T^{-1} = \begin{bmatrix} a & b & c & d & e \\ c & a & d & e & b \end{bmatrix} \quad \text{hence} \quad TLT^{-1}$$

$$= \begin{bmatrix} a & b & c & d & e \\ b & e & a & c & d \end{bmatrix} \begin{bmatrix} a & b & c & d & e \\ c & a & b & e & d \end{bmatrix} \begin{bmatrix} a & b & c & d & e \\ c & a & d & e & b \end{bmatrix}$$

$$= \begin{bmatrix} a & b & c & d & e \\ a & d & c & b & e \end{bmatrix} \begin{bmatrix} a & b & c & d & e \\ c & a & d & e & b \end{bmatrix}$$

$$= \begin{bmatrix} a & b & c & d & e \\ c & e & d & a & b \end{bmatrix} = K$$

There are as many solutions for T as there are ways of writing the elements of the cycles of permutation L in a correct cyclic order below the corresponding cycles of K.
Thus in general the equation $K = TLT^{-1}$ has multiple solutions for T.

This statement can be applied to the equations of this form derived by Rejewski that were given earlier. The details of his solutions of these equations are given below:-

The permutation S due to the plug-board on the particular day (six transpositions) was included in the information supplied to the Poles by French Intelligence.

S = (a p) (b l) (c z) (f h) (j k) (q u)

Using the known transpositions A, B, C, D, E, F and S combined with the appropriate powers of P the permutations U, V, W, X, were determined (Y and Z were not required).

Rejewski quotes the following results:-

U = (a x) (b u) (c k) (d r) (e j) (f w) (g i) (l p) (m s) (n z) (o h) (q t) (v y)
V = (a r) (b v) (c o) (d h) (f l) (g k) (i z) (j p) (m n) (q y) (s u) (t w) (x e)
W = (a s) (b z) (c p) (d q) (e o) (f w) (g j) (h l) (i y) (k r) (m u) (n t) (v x)
X = (a p) (b f) (c u) (d v) (e i) (g r) (h o) (j n) (k y) (l x) (m z) (q s) (t w)

The three composite permutations derived from these were:-

UV = (a e p f t y b s n i k o d) (r h c g z m u v q w l j x)

VW = (a k j c e v z y d l w n u) (s m t f h q i b x o p g r)

WX = (a q v l o i k g n w b m c) (p u z f t j r y e h x d s)

Note that these three composite permutations have the same cycle structure.
This can be explained in the following way:-
A consequence of the two equations $VW = H^{-1}(UV)H$ and $WX = H^{-1}(VW)H$
is that the three composite permutations UV, VW and WX are similar and so must have the same cycle structure.

To determine all possible values of H from the equation $VW = H^{-1}(UV)H$ permutation VW would be written below permutation UV in every possible way to obtain a set of solutions for H each satisfying the equation $VW = H^{-1}(UV)H$. In the same way another set of solutions for H would be obtained from the equation $WX = H^{-1}(VW)H$.
The required solution for H is the only one that is common to both of these sets, and this was subsequently used to solve the equation $H = NPN^{-1}$ for N.

In a paper written by Rejewski he states that although this was theoretically the correct procedure to use it was '*rather tedious*' and that it was shortened by the use of various undisclosed '*tricks and technical means*'. However he gives the true alignment between the pairs of cycles as:-

UV = (a e p f t y b s n i k o d) (r h c g z m u v q w l j y)
VW = (y d l w n u a k j c e v z) (i b x o p g r s m t f h q)

VW = (y d l w n u a k j c e v z) (i b x o p g r s m t f h q)
WX = (u z f t j r y e h x d s p) (c a q v l o i k g n w b m)

From these two pairs of composite permutations a common solution for H was obtained:-

H = (a y u r i c x q m g o v s k e d z p l f w t n j h b)

Since $H = NPN^{-1}$ a similar procedure was then used to solve for N^{-1}
One obvious possible alignment of the pairs of permutation cycles is:-

H = (a y u r i c x q m g o v s k e d z p l f w t n j h b)
P = (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)

After reordering the upper row into alphabetical order a solution for N:-

$$N = \begin{bmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ a & z & f & p & o & t & j & y & e & x & n & s & i & w & k & r & h & d & m & v & c & l & u & g & b & q \end{bmatrix}$$

The above solution is however only one from a total of 26 possible alternatives, and the question remained of how was the correct one was to be found.

In his paper Rejewski states:-: '*All the other alternative solutions for N are not fundamentally different from this one. The only consequence of selecting one or another solution is that in effect the right-hand face of rotor N is turned by a greater or smaller angle with respect to the left-hand face'.*

He also states that:- '*Which of these variants we select is not of great importance for the moment'*

In coming to a decision on which permutation N is to be accepted as the true one, he states that:-'*Those details may only be established following the basic reconstruction of the connections to all the rotors'* (see the final paragraph).

Rekewski gives an outline description of the procedure used to recover '*those details*'. This appears to have depended largely on 'trial and error'. Included in the intelligence material supplied to the Poles at the time by French Intelligence were several examples of plaintext messages together with the corresponding cipher-text obtained with given Enigma keys. The Germans had produced these to help in the training of their operators. It would seem that the Poles made use these examples by making repeated attempts to recover the known plaintext from the known cipher-text, trying out different orientations of the right-hand faces of the rotors until finally success was achieved!

The intelligence information supplied to the Poles included the setting sheets that covered a two-month period during which there was a change in the rotor occupying the right-hand position in the machine. Using the technique described, the permutation (N) for this rotor was also recovered. Rejewski states that it then became possible deduce the corresponding permutation for the remaining rotor and also that of the reflector.
(In 1932 the German Enigma machines were only equipped with three rotors.)

F.L.C March 2005

.