SRIP 2026 Report:
Determining Absolute Rotor Wirings

Aaditya Rushabh Shah
Guided by Prof. Jyothi Krishnan

July 8, 2026

1 Introduction

Consider the rotor order of September to be L, M, N where L is the leftmost rotor, M is the middle rotor and N is the rightmost rotor. Now, the month of October has four possible rotor orders as stated below (because we know that rightmost rotor was changed from September to October) -

1. N, L, M
2. L, N, M
3. N, M, L
4. M, N, L

Observe the possible rotor orders N, L, M and M, N, L, they have no rotor in the same position compared to rotor order in September and thus, we call this the *No Rotor Fixed Case*. In case of L, N, M, the leftmost rotor is at same position, thus we call this the *Left Rotor Fixed Case* and in case of N, M, L, the middle rotor is at same position, thus we call this the *Middle Rotor Fixed Case*.
The aim is to solve for the exact internal rotor wirings for each of the rotors L, M, N on the basis of the data obtained for the months of September and October (we have the day key and intercepted messages along with an example containing both ciphertext and plaintext from the manual).
Rejewski's work covers finding internal rotor wirings for the two rotors that appear at rightmost position in the given months but up to the twist. Hence, we don't have the exact internal rotor wiring, the third rotor wiring and reflector. Below, this covers case-by-case how he possibly would have found the exact internal rotor wiring for the two rotors and wiring of third rotor which will then simply give us the reflector too.

2 No Rotor Fixed Case

Note: *We will be assuming that rotor order is N, L, M in October. Similar approach could be applied in case rotor order is M, N, L in October in which, one can apply methods used in September in this case to October and those in October to September.*
Consider a triplet of days from month of September (s_1, s_2, s_3) such that absolute rotor settings of left rotor are in A.P. $z_3 - z_2 = z_2 - z_1 = d$, $d \neq 0$ and $\gcd(d \mod 26, 26) = 1$, where (z_j, y_j, x_j) represent the absolute rotor settings for left, middle and right rotors on j-th day respectively for the first letter involution A_j (obtained using Rejewski's method for message keys). So, we know

$$A_j = S_j^{-1} P^{-x_j} N^{-1} P^{x_j} P^{-y_j} M^{-1} P^{y_j} P^{-z_j} L^{-1} P^{z_j} R P^{-z_j} L P^{z_j} P^{-y_j} M P^{y_j} P^{-x_j} N P^{x_j} S_j \tag{1}$$

where S_j are the plugboard settings for j-th day (which are known).

2.1 Finding the Right Rotor N's Twist

We know N and M up to twists, so $N = P^s\psi$, $M = P^t\phi$ where s is the twist for rotor N, ψ is one of the candidates, N is the true rotor wiring, and similarly, t is the twist for rotor M, ϕ is one of the candidates and M is the true rotor wiring.
Now, we define

$$A_j^* := P^{z_j}P^{-y_j}\phi P^{y_j}P^{-x_j}(P^s\psi)P^{x_j}SA_jS^{-1}P^{-x_j}(P^s\psi)^{-1}P^{x_j}P^{-y_j}\phi^{-1}P^{y_j}P^{-z_j} = P^{-t}L^{-1}P^{z_j}RP^{-z_j}LP^t \tag{2}$$

where A_j^* is a known (obtained by the product of the knowns as defined) except for twist s of N but we know $s \in \{0, 1, \ldots, 24, 25\}$.
Using equation (2) for $j = 1, 2, 3$, we get,

$$A_3^*A_2^* = (P^{-t}L^{-1}P^dLP^t)(A_2^*A_1^*)(P^{-t}L^{-1}P^{-d}LP^t) \tag{3}$$

Observe that $A_{j+1}^*A_j^*$'s cycle length is dependent upon the twist s of N (observe the known part in (2)), whereas the twist t of M does not affect their cycle length and thus does not affect the conjugacy relation obtained obtained in equation (3). Thus, this will help us to narrow down to possible values of s after trying them out, because conjugacy relation will not hold true for most incorrect values of s since they will result in different cycle lengths for $A_3^*A_2^*$ and $A_2^*A_1^*$. Also, the relation will hold true independent of the twist t for correct value of s. We can find such multiple triplets of days satisfying $z_3 - z_2 = z_2 - z_1 = k$ where k doesn't necessarily need to be same as d as we find values of s which satisfy the conjugacy relation and using this approach, we can narrow down to one value of twist s and obtain the true internal rotor wiring N.
Note: *We call this procedure as* ***right twist recovery****.*

2.2 Finding the Left Rotor Wiring L up to twist

Now, in equation (3), we know t doesn't affect the conjugacy relation. So, once we obtain N, we treat $t = 0$ and obtain a conjugacy relation as follows

$$A_3^*A_2^* = (L^{-1}P^dL)(A_2^*A_1^*)(L^{-1}P^{-d}L) \tag{4}$$

which is a relation conjugated by $L^{-1}P^dL$.
Now, we find another triplet of days within the same month of September (s_4, s_5, s_6) such that $z_6 - z_5 = z_5 - z_4 = d$, that is the common difference of the A.P. formed shall remain the same as that of the triplet chosen earlier.
This time we know exact rotor wiring N. Thus, A_k^* for $k \in \{4, 5, 6\}$ are all knowns (here, A_k^* is similar to what we defined in (2)). Thus, we will obtain a relation,

$$A_6^*A_5^* = (L^{-1}P^dL)(A_5^*A_4^*)(L^{-1}P^{-d}L) \tag{5}$$

From equations (4), (5), we find the value of $\rho = L^{-1}P^dL$. Also, we had chosen d such that $d \mod 26$ is coprime to 26, and thus, we will obtain 26 possible values of L, that is, the rotor wiring of L up to its twist, say q, so $L = P^q\omega$ where ω is any one particular chosen value out of the 26 possible values.

2.3 Finding the Middle Rotor M's Twist

Now, we know rotor wiring L up to twist q. Thus, just like we did for finding twist s of rotor N, we apply right twist recovery in the month of October. We find triplet of days (o_1, o_2, o_3) such that $\gamma_3 - \gamma_2 = \gamma_2 - \gamma_1 = l$ where l need not be necessarily equal to d, $l \neq 0$, and $\gcd(l \mod 26, 26) = 1$. Now, consider B_m as the 1st letter involution of m-th day in October. We know,

$$B_m = S_m^{-1}P^{-\alpha_m}M^{-1}P^{\alpha_m}P^{-\beta_m}L^{-1}P^{\beta_m}P^{-\gamma_m}N^{-1}P^{\gamma_m}RP^{-\gamma_m}NP^{\gamma_m}P^{-\beta_m}LP^{\beta_m}P^{-\alpha_m}MP^{\alpha_m}S_m$$

where S_m are the plugboard settings for m-th day. We define B_m^* similar to that in (2),

$$B_m^* := P^{\gamma_m-\beta_m}\omega P^{\beta_m-\alpha_m}(P^t\phi)P^{\alpha_m}S_mA_mS_m^{-1}P^{-\alpha_m}(P^t\phi)^{-1}P^{\alpha_m-\beta_m}\phi^{-1}P^{\beta_m-\gamma_m} = P^{-q}N^{-1}P^{\gamma_m}RP^{-\gamma_m}NP^q$$

and obtain an equation similar to (3),

$$B_3^*B_2^* = (P^{-q}N^{-1}P^lNP^q)(B_2^*B_1^*)(P^{-q}N^{-1}P^{-l}NP^q) \tag{6}$$

This conjugacy relation will also not satisfy for most incorrect values of twist t of M, and will always satisfy independent of the value of twist q for correct twist t, and thus, using one or more triples like this in October, we can get to value of twist t and obtain the true internal rotor wiring M.

2.4 Finding the Left Rotor L's Twist

We can now use the triplet of October chosen earlier, and define

$$B_m^{**} := P^{-\gamma_m}NP^{\gamma_m-\beta_m}(P^q\omega)P^{\beta_m}P^{-\alpha_m}MP^{\alpha_m}S_mA_mS_m^{-1}P^{-\alpha_m}M^{-1}P^{\alpha_m-\beta_m}(P^q\omega)^{-1}P^{\beta_m-\gamma_m}N^{-1}P^{\gamma_m} = R \tag{7}$$

We check $B_2^{**} = B_1^{**}$ and $B_3^{**} = B_2^{**}$ and see that for which values of twist q do they hold true. We can apply this test on one or more triples if required and get to the correct value of q. From this, we obtain the true internal rotor wiring L.

2.4.1 Alternate Approach (Needs to be verified)

It seems that there is a much more straight forward way to find twist q of L. Observe (6), from which, it seems that q can be found once M is known by trying out all possible values of q, because twist q ensures that equality holds true whereas twist t of M was to ensure equal cycle lengths of $B_3^*B_2^*$.
Note: *There is an alternate approach to use similar strategy to find Middle Rotor M's twist too from a triplet used in month of September but the computation required increases slightly and thus I prefer the above stated methods.*

2.5 Alternative Approach to Determine Left Rotor Wiring L up to twist

This proposes an alternative approach to find the rotor wiring L using the data obtained from month of October and it is more efficient except for it doesn't help in determining twists of L, but works perfectly if the rightmost rotor, in this case M is known. Hence, if we use *middle twist recovery* in September or method similar to that in Section 2.3 and get rotor M up to twist, we can then apply the strategy described below. Consider two days (d_1, d_2) in month of October (since L is middle rotor in October) such that both of them contain a letter involution (other than 1st letter involution or double stepping) in which middle rotor turnover occurs. We choose two involutions C_j, D_j from d_j such that middle rotor turnover occurs in D_j, and suppose absolute rotor settings for C_1 are (z_1, y_1, x_1) whereas for C_2 are (z_2, y_2, x_2). Thus, we know the following:

$$C_1 = S_1^{-1}P^{-x_1}M^{-1}P^{x_1}P^{-y_1}L^{-1}P^{y_1}P^{-z_1}N^{-1}P^{z_1}RP^{-z_1}NP^{z_1}P^{-y_1}LP^{y_1}P^{-x_1}MP^{x_1}S_1$$

$$D_1 = S_1^{-1}P^{-(x_1+1)}M^{-1}P^{(x_1+1)}P^{-(y_1+1)}L^{-1}P^{(y_1+1)}P^{-z_1}N^{-1}P^{z_1}RP^{-z_1}NP^{z_1}P^{-(y_1+1)}LP^{y_1+1}P^{-(x_1+1)}MP^{(x_1+1)}S_1$$

because the right rotor steps as usual along with middle rotor too according to the data we find. We define, after shifting the knowns,

$$C_1^* := P^{y_1-x_1}MP^{x_1}S_1C_1S_1^{-1}P^{-x_1}M^{-1}P^{x_1-y_1} = L^{-1}P^{y_1-z_1}N^{-1}P^{z_1}RP^{-z_1}NP^{z_1-y_1}L \tag{8}$$

$$D_1^* := P^{y_1-x_1}MP^{(x_1+1)}S_1D_1S_1^{-1}P^{-(x_1+1)}M^{-1}P^{x_1-y_1} = L^{-1}P^{y_1-z_1+1}N^{-1}P^{z_1}RP^{-z_1}NP^{z_1-y_1-1}L \tag{9}$$

Substituting $N^{-1}P^{z_1}RP^{-z_1}N = P^{z_1-y_1}LC_1^*L^{-1}P^{y_1-z_1}$ (8) in (9), we get,

$$D_1^* = (L^{-1}PL)C_1^*(L^{-1}P^{-1}L) \tag{10}$$

and similarly,

$$D_2^* = (L^{-1}PL)C_2^*(L^{-1}P^{-1}L) \tag{11}$$

We can try to find as many such days as possible and that will definitely help us to get to one value of $L^{-1}PL$ if we don't get narrow down to one possibility from (10), (11) alone. Using the equations (10), (11), we obtain $\kappa = L^{-1}PL$ and hence, we find rotor wiring L up to twist q. The further procedure remains same as described in earlier sections.

3 Left Rotor Fixed Case

We could find the rotor wiring of N and M up to their twists s and t respectively. Next we aim to deduce the their twists to obtain true internal rotor wiring and then find L.

3.1 Finding the Right Rotor N's Twist

We use the method of *right twist recovery*. For this part, it is completely same method as used in Section 2.1. Thus, we find true internal rotor wiring N. Let's keep the naming conventions same as we had in Section 2.1

3.2 Finding the Middle Rotor M's Twist

Instead of finding left rotor wiring L up to twist first like we did earlier, we first determine middle rotor M's twist using *right twist recovery* as used in Section 2.1 for which we use a triplet of days in the month of October. The naming conventions used are similar to that in Section 2.3. Thus, from this, we get true internal rotor wiring M.

3.3 Finding the Left Rotor L up to twist

For finding left rotor L, we need any two triples from any of the months which have their leftmost rotor settings in A.P. of common difference d (which should be same for both triples), such that $d \neq 0$ and $\gcd(d \bmod 26, 26) = 1$. These triples can be same as the ones used in earlier sections if they satisfy the required conditions. Let's keep the naming conventions for 1-st letter involution in first triplet as A_j for $j \in \{4, 5, 6\}$ and 1-st letter involution in second triplet as B_k for $k \in \{4, 5, 6\}$. Depending on the month from which triplet is chosen, the exact expressions for A_j^* and B_k^* may differ but after manipulations similar to ones we did in Section 2.1, we will obtain a pair of equations as follows,

$$A_6^* A_5^* = (L^{-1} P^d L)(A_5^* A_4^*)(L^{-1} P^{-d} L) \tag{12}$$

$$B_6^* B_5^* = (L^{-1} P^d L)(B_5^* B_4^*)(L^{-1} P^{-d} L) \tag{13}$$

From the above pair of equations, we find $\rho = L^{-1} P^d L$ and thus obtain L up to twist q, that is, 26 possible candidates of L, with $L = P^q \omega$ where ω is one of those 26 possible candidates.

3.4 Finding the Left Rotor L's Twist

We are now left with 26 possible combinations for $N/M/L$. It must be noted though that we have deduced true internal wiring of N and M completely and thus, a lot of terms are known. But, this just is bad for us. I could not think of any clear possibility to deduce the exact twist of L. It seems that until any of the two rotor orders is maintained, one could never deduce true internal rotor wiring of L using any simple/trivial or non-laborious method because it will always have 26 possibilities of Enigma ($N/M/L/R$) and only when rotor order changes can one check for it. We don't face similar issues in any other case because in all those cases, each rotor has to contribute to something which makes a difference whereas here L doesn't contribute to anything along with the fact its effect can be adjusted with reflector. This leads to another Enigma in itself to crack just with one rotor but no data except that we know 26 possible rotor wirings.
Hence, if this was the case Rejewski dealt with, and also deduced true internal rotor wiring L, he must have used the example from the manual which must have contained an example with rotor order other than L, M, N and L, N, M. Even slightest of information with any other rotor order could help us true L.

Note: *One may argue that he might have waited for another quarter where rotor order would have changed and would have found third rotor wiring from it. Even though its possible, as far as what I read, Rejewski had deduced all the wirings completely by end of December and according to that information, he didn't wait for the next quarter.*

4 Middle Rotor Fixed Case

We know the rotor wiring for N and L up to twist s and q respectively, such that $N = P^s\psi$, $L = P^t\omega$

4.1 Finding the Middle Rotor M up to twist

Now, we use the middle rotor turnover method as described in Section 2.5.
Consider two days (d_1, d_2) in September (though one can choose any month for any day as the final pair of equations will be similar and help to solve, but choosing a pair in same month is more helpful as possibilities of twists are reduced) such that both of them contain a letter involution (other than 1-st letter involution or double stepping) in which middle rotor turnover occurs. We choose two involutions C_j, D_j from d_j such that middle rotor turnover occurs in D_j and C_j is the preceding letter involution. Let's assume the absolute rotor settings for C_j to be (z_j, y_j, x_j). So, we know the following,

$$C_j = S_j^{-1}P^{-x_j}N^{-1}P^{x_j}P^{-y_j}M^{-1}P^{y_j}P^{-z_j}L^{-1}P^{z_j}RP^{-z_j}LP^{z_j}P^{-y_j}MP^{y_j}P^{-x_j}NP^{x_j}S_j$$

$$D_j = S_j^{-1}P^{-(x_j+1)}N^{-1}P^{(x_j+1)}P^{-(y_j+1)}M^{-1}P^{(y_j+1)}P^{-z_j}L^{-1}P^{z_j}RP^{-z_j}LP^{z_j}P^{-(y_j+1)}MP^{y_j+1}P^{-(x_j+1)}NP^{(x_j+1)}S_j$$

$$C_j^* := P^{y_j-x_j}\psi P^{x_j}S_jC_jS_j^{-j}P^{-x_j}\psi^{-1}P^{x_j-y_j} = P^{-s}M^{-1}P^{y_j-z_j}L^{-1}P^{z_j}RP^{-z_j}LP^{z_j-y_j}MP^s \tag{14}$$

$$D_j^* := P^{y_j-x_j}\psi P^{(x_j+1)}S_jD_jS_j^{-1}P^{-(x_j+1)}\psi^{-1}P^{x_j-y_j} = P^{-s}M^{-1}P^{y_j-z_j+1}L^{-1}P^{z_j}RP^{-z_j}LP^{z_j-y_j-1}MP^s \tag{15}$$

From (14), (15), we get,

$$P^sD_j^*P^{-s} = (M^{-1}PM)(P^sC_j^*P^{-s})(M^{-1}P^{-1}M) \tag{16}$$

Using $j = 1, 2$ and choosing any value of s, probably $s = 0$ (it doesn't give wrong possibilities of M because one can observe that s essentially has no effect on the equation by observing known part of C_j^* of D_j^*), from (16) or analyze for more days if required, we obtain $\kappa = M^{-1}PM$ which helps us to find M up to twist say t, that is, $M = P^t\phi$.

4.2 Finding the Right Rotor N's twist

Approach this problem just like we did in Section 2.1 for *No Rotor Fixed Case* using a triplet from month of September, from which we find the twist s of rotor N and thus we know the true internal rotor wiring N.

4.3 Finding the Left Rotor L's twist

At this point, the problem has become very much similar to that in case of *No Rotor Fixed Case*. We use the approach described in Section 2.3 by choosing a triplet in October and thus obtain true internal rotor wiring of L.
Note: *If the claim made in Section 2.4.1 is correct, we can simply use that to find the correct twists (t, q) and obtain true internal rotor wiring for M and L also.*

4.4 Finding the Middle Rotor M's twist

Again, we approach the problem in a similar fashion as shown in Section 2.4 (if the one in Section 2.4.1 doesn't work), such that we find triplet from any of the months and find twist t of M to obtain true internal rotor wiring of M.