Cryptologia
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/ucry20

FACTORING FOR THE PLUGBOARD - WAS REJEWSKI'S PROPOSED SOLUTION FOR BREAKING THE ENIGMA FEASIBLE?

John Lawrence [a]

[a] Department of Pure Mathematics and Centre for Applied Cryptographic Research, University of Waterloo, Waterloo, Ontario, CANADA N2L 3G1

Available online: 04 Jun 2010

To cite this article: John Lawrence (2005): FACTORING FOR THE PLUGBOARD - WAS REJEWSKI'S PROPOSED SOLUTION FOR BREAKING THE ENIGMA FEASIBLE?, Cryptologia, 29:4, 343-366

To link to this article: http://dx.doi.org/10.1080/0161-110591893924

FACTORING FOR THE PLUGBOARD – WAS REJEWSKI'S PROPOSED SOLUTION FOR BREAKING THE ENIGMA FEASIBLE?

John Lawrence

ADDRESS: Department of Pure Mathematics and Centre for Applied Cryptographic Research, University of Waterloo, Waterloo, Ontario, CANADA N2L 3G1.

ABSTRACT: We prove a generalization of a theorem of Rejewski. This theorem shows how one can solve an equation of the form $XY = \alpha$ in a symmetric group, where α is a given permutation and X and Y are each of order two with a specified number of disjoint transpositions. The number of solutions is also part of the theorem.

Using this theorem we outline what we believe was the Polish solution (or very close to it) to the Enigma assuming that one had no data from daily keys. With some assumptions on independence of events, we show that the Polish Cipher Bureau would probably have broken the Enigma in just over four years.

KEYWORDS: Enigma, plugboard, Rejewski.

1. INTRODUCTION AND HISTORICAL BACKGROUND

In 1933 Marian Rejewski, a young mathematician working for the Polish Cipher Bureau, broke the German Military Cipher machine—the Enigma. This remains one of the most stunning applications of mathematics to cryptoanalysis with far-reaching historical consequences. Rejewski did this by solving a system of six equations in the permutation group S_{26}. In solving the system of equations, he made use of specific plugboard settings for a sixty-day period, information supplied by the spy Hans Theo Schmidt through the French Cipher Bureau. Could Rejewski have solved for the wiring of the Enigma rotors without the material supplied by Schmidt?

In 1974 Colonel Mayer, the former head of the Polish Intelligence Service, wrote,

> "At the stage in which the research on the Enigma was at that time in the Polish cryptological section, these documents appeared not to be

indispensible for the final solution of the problem. But unquestionably, they facilitated it."[11]

To some extent this was confirmed by Rejewski when he wrote,

"However, it is known that this set (of equations) would be solvable if the cryptologist had cipher material for two different days; with different plug connections, but with the same or nearly the same settings of rotors." [13, p. 279]

"... the way to the goal would still be long and tedious, requiring the checking of many instances. In any case, a method of solving the equations existed, at least in theory. In reality, the necessary supplementary data were obtained by a different, far shorter way."[13]

"Admittedly another approach to the reconstruction of the rotor wiring was found in theory at any rate. But that approach is imperfect and laborious ...; therefore, finding the wiring of the rotors would depend on luck. In addition, it requires so many trials that it is not clear whether the director of the Cipher Bureau would have had enough patience to employ several workers for a long period without certain attainment of success or whether he would have once more discontinued work on the Enigma. Hence the conclusion is that the intelligence material furnished to us should be regarded as having been decisive to the solution of the machine." [6, pp. 87–88]

These comments by Rejewski suggest that although he had a general method in mind to solve for the rotors without the intelligence material supplied by Schmidt, only a very general idea existed as to the feasibility of the method.

It is clear that the above 'laborious method' was the only method that Rejewski had for solving for the wiring of the rotors without the Schmidt documents, for when he discussed the matter of solving a single system of equations, he stated, "To this day it is not known whether equation set (3) is solvable."[12, p. 258]

These statements led Gilbert Block to conclude, "Rejewski explicitly indicates that, without further information, it was impossible to solve the permutation equations."[3]

David Kahn discusses the ambiguity of Rejewski's statements and concludes that,

> "Only in the opinion that such a solution would have required a great deal of time—'a number of years,' he wrote in 'Enigma 1930–1940'—was he consistent. In any event, any answer to whether Rejewski would have solved the Enigma without Schmidt's documents would be hypothetical and thus impossible of proof." [6, p. 307]

One difficulty in understanding Rejewski's comments on the difficulty of solving the system of equations is that he is talking about two different problems. One problem is that of finding the wiring of the first rotor, given the equations coming from the first six permutations of the day. This is a problem of solving a single system of equations. But when Rejewski is discussing an alternate method of breaking the Enigma, he is talking about solving for the wiring of the rotors by using two systems of equations coming from two different days in which the rotor settings are the same. This still leaves open the question of whether a single system of equations can be solved efficiently.

Because Rejewski's proposed solution using two systems of equations from two different days is a much less direct method and requires time to gather the data required, the question of the feasibility of the method arises. That is what we look at in this paper.

In this paper we expand on Rejewski's rather brief explanation of his method, fill in gaps where particular theorems are needed and try to come to a conclusion as to whether the method would actually work without an exorbitant amount of calculations and time.

In Section 2 we discuss the collection of the data and the difficulties to be overcome.

The Section 3 we state and prove the theorems in algebra necessary to justify the method. The main theorem here is the one used to factor the plugboard.

In Section 4 of the paper we propose a method for solving the equations. There is an analysis of the amount of work required.

This leads to our conclusion in Section 5.

In looking at the number of calculations required, we have to have information on the number of solutions of certain group equations. This information is supplied in the tables at the end of the paper.

2. GATHERING THE DATA

The method that Rejewski briefly outlined requires time—not just time to do the calculations, but time to gather the data. Just how much time depends on

what we want to get from the data. If we require enough data to calculate the wiring of all three rotors (and the reflector), we need more time than if we only need enough data to calculate the wiring of two rotors and then find the wiring of the third rotor by another method.

In order to understand the method, let's go back to Rejewski's statements.

In [13, p. 279], Rejewski states that one could use the six equations to solve for the wiring of the first rotor if "the cryptologist had cipher material for two different days; with different plug connections, but with the same or nearly the same rotor settings." He also remarks that "... such a pair may be recognized by the fact that they have the same characteristic (but not the other way around ...)"[13, p. 279].

Recall that if on a given day the first six permutations are P_1, P_2, P_3, P_4, P_5, P_6, then the characteristic for that day is the triple of permutations (P_1P_4, P_2P_5, P_3P_6).

Let us call a pair of days in which we have the same initial position (as wired rotors—for the first permutation) a *collision* and a pair of days in which we have the same characteristic a *characteristic collision.*

If on a given day X_i, $i = 1, 2, 3, \ldots, 6$, denotes the first six permutations induced by the rotors and the reflector and V is the plugboard setting, then

$$P_i = V^{-1}X_iV, \quad i = 1, 2, \ldots, 6.$$

Therefore P_iP_{i+3} is conjugate to X_iX_{i+3}, $i = 1, 2, 3$.

If we have a second day in which the first six permutations induced by the rotors and reflector are also X_i, $i = 1, 2, 3, \ldots, 6$, and the first six permutations induced by the machine are $Q_1, Q_2, \ldots, Q_6$, then Q_iQ_{i+3} will also be conjugate to X_iX_{i+3}; hence Q_iQ_{i+3} will be conjugate to P_iP_{i+3} $(i = 1, 2, 3)$. Thus on the two days the characteristics will be the same.

Suppose that we have a period of n days. We will have $\frac{n(n+1)}{2}$ unordered pairs of days and we can expect for a given pair a probability of $(6 \times 26^3)^{-1}$ that the rotors will be in the same initial position. Therefore, over the period of n days we can expect about $\frac{n(n+1)}{12\times 26^3}$ collisions. Over a four-year period of about 1461 days we would expect about 10.1 collisions, while over a five-year period of about 1826 days we would expect about 15.8 collisions.

If A, B, C and D are each products of 13 disjoint transpositions, then the probability that AB and CD are conjugate is about $\frac{1}{10}$. (This calculation comes from our tables.) Therefore, given a pair of days, the probability that the two days will have the same characteristic is about $\frac{1}{1000}$. In a period of 1461 days

we would expect about 1067 characteristic collisions while over a period of 1826 days we would expect about 1666 characteristic collisions.

In general there are far more characteristic collisions than there are collisions.

One difficulty in finding the collisions is that the characteristic detects the collision only if the first six permutations induced by the rotors and the reflector are the same for the two days. If, for a pair of days, we have the same initial setting for the rotors, there is a $1-\left(\frac{21}{26}\right)^2 \approx .348$ chance that on one of those days the second rotor will move at some point in the remaining five permutations. In that case we will probably have different characteristics for the two days. Therefore we can expect that only about 65% of the collisions will be detected by characteristic collisions, but the ones that are detected will probably have the property that on the two days the first six permutations induced by the rotors and the reflector will be the same.

In our method we assume that for each of the pairs of days for which there is a collision, we can find the first six permutations for each of the days. The calcuation of these permutations is not just a mathematical problem (although Rejewski's Theorem cuts down the number of possible cases considerably). It also involves judgements made about the tendencies of individual encipherers. Rejewski discusses at some length how this was done. We quote part of his description.

> "A proper interpretation of the foregoing determination implies that it will suffice to know the habits of the encipherers in order to completely reconstruct the message keys." [14, p. 253]

In any case, when he described the method by which one could break the Enigma, it was clear that he assumed that these first six permutations were available. If one has the plugboard settings for a given day then it is must easier to check that a proposed list of six permutations is consistent, so there is added difficulty if the plugboard settings are not available. However, Rejewski makes it clear that in practice they were able, in most cases, to find the first six permutations without the aid of the plugboard settings.

3. SOME ALGEBRA THEOREMS NEEDED

In this section we state and prove our main theorem. This theorem is used to show how to factor for the plugboard and it gives the number of solutions in this factoring. The theorem is a fairly straightforward generalization of Rejewski's Theorem [12]. In order to make our description of the methods used as complete

as possible, we have also restated some basic theorems that we use which are proved elsewhere.

DEFINITION. Let m and n be integers with $n > 0$ and $m \geq 0$. Let $G(n, m)$ denote the set of elements of S_n which are products of m disjoint transpositions.

If we let $|G(n, m)|$ denote the number of elements of $G(n, m)$, then

$$|G(n, m)| = \frac{n!}{2^m m!(n - 2m)!}.$$

For example, $|G(26, 6)| \approx 10^{11}$, $|G(26, 7)| \approx 1.31 \times 10^{12}$, $|G(26, 10)| \approx 1.51 \times 10^{14}$ and $|G(26, 13)| \approx 7.9 \times 10^{12}$.

THEOREM 1 (FACTORING THEOREM). Let α be an element of S_n. Suppose that α has m_i i-cycles, $i = 1, 2, \ldots, n$, when written as a product of disjoint cycles. Let m be a positive integer with $2m \leq n$. Then the equation $XY = \alpha$ has a solution with X and Y both in $G(n, m)$ if and only if there is a n–$2m$ element subset S of cycles of α (we will assume that in S there are k_i i-cycles, $i = 1, 2, \ldots, n$) satisfying

(1) $m_i - k_i$ is even for all i,

and

(2) $t = \sum_{i \text{ even}} k_i$ is even.

With respect to a given subset S satisfying the above condition, the number of solutions of the equation is

$$\left(\frac{t!}{\left(\frac{t}{2}!\right)^2}\right) 2^{-t} \left[\prod_{j=1}^{n} \frac{j^{\frac{m_j + k_j}{2}} (m_j - k_j)!}{2^{\frac{m_j - k_j}{2}} \left(\frac{m_j - k_j}{2}\right)!}\right].$$

The total number of solutions of the equation is the sum of the above over all $n - 2m$ element subsets S satisfying the stated conditions.

PROOF. Suppose that the ℓ-cycle $(1\ 2 \ldots \ell)$ is one of the cycles in the decomposition of α with $\ell > 1$. We want to express α as a product XY of two elements of order 2. Suppose that the 1-cycle (1) is in the decomposition of X.

In α, $1 \rightarrow 2$, so we must have (1 2) as a cycle in Y. As $\ell \rightarrow 1$, we must have

$(2\ \ell)$ as a cycle in X. Continuing in this way we have two cases:

$$X = (1)(2\ \ell)(3\ \ell{-}1)\cdots\left(\frac{\ell}{2}\ \ \frac{\ell}{2}{+}2\right)\left(\frac{\ell}{2}{+}1\right)\cdots$$

and

$$Y = (1\ 2)(3\ \ell)(4\ \ell{-}1)\cdots\left(\frac{\ell}{2}{+}1\ \ \frac{\ell}{2}{+}2\right)\cdots$$

if m is even or

$$X = (1)(2\ \ell)(3\ \ell{-}1)\cdots\left(\frac{\ell{+}1}{2}\ \ \frac{\ell{+}3}{2}\right)\cdots$$

and

$$Y = (1\ 2)(3\ \ell)(4\ \ell{-}1)\cdots\left(\frac{\ell{+}1}{2}\ \ \frac{\ell{+}5}{2}\right)\left(\frac{\ell{+}3}{2}\right)\cdots$$

if m is odd.

Of course if $\ell = 1$, then $X = (1)\cdots$ and $Y = (1)\cdots$.

Notice that in all cases the cycle decompositions of X and Y are completely determined for the letters $1, 2, \ldots, \ell$ once we put the 1-cycle (1) in X. If ℓ is even, then we get two 1-cycles occurring in X (involving the letters $1, 2, \ldots, \ell$) and no 1-cycles occurring in Y, while if ℓ is odd, then we have one 1-cycle in each of X and Y. In both cases the total contribution of 1-cycles to X and Y involving the letters $1, 2, \ldots, \ell$ is 2.

Now the total number of 1-cycles in X and Y is $2(n - 2m)$ (for X and Y are both to lie in $G(n, m)$), so we must have at least $n - 2m$ cycles in the decomposition of α.

Let S be a $n-2m$-element set of cycles of α. When we express α as a product we want to choose the 1-cycles from letters that are in the cycles of S. If $(1\ 2\cdots\ell)$ is a member of S and ℓ is odd, then we can choose a 1-cycle for X in ℓ different ways and in each case we will get a 1-cycle for Y. If $(1\ 2\cdots\ell)$ is a member of S and ℓ is even, then we have $\frac{\ell}{2}$ different ways to choose a 1-cycle in X and each way will give us two 1-cycles in X. We could also choose a 1-cycle for Y in $\frac{\ell}{2}$ ways and each way will give us two 1-cycles in Y. In order to get n–$2m$ 1-cycles in both X and Y we will have to divide the set of even cycles of S into two equal parts and use one part to give us 1-cycles for X and one part to give us 1-cycles for Y. If the number of even cycles is t, then t is even and the number of ways of dividing these t cycles into two equal parts is $\frac{t!}{(\frac{t}{2}!)^2}$. Putting these parts together

we see that the number of ways of factoring these cycles in S is

$$\left[\frac{t!}{\left(\frac{t}{2}!\right)^2}\right]\left(\prod_{\substack{j\text{-cycle in } S\\ j \text{ even}}}\left(\frac{j}{2}\right)\right)\left(\prod_{\substack{j\text{-cycle in } S\\ j \text{ odd}}} j\right).$$

Suppose now that the ℓ-cycle $(1\ 2\cdots\ell)$ is not in S. When we factor this cycle we want no 1-cycles involving the letters $1,\ldots,\ell$ in either X or Y. If in X we have $(1\ u)$, then in Y we have $(2\ u)$, with $u \neq 1,2$. We then have $(2\ v)$ in X and so $(3\ v)$ in Y with $v \neq 1,2,3,u$. Continuing in this way we get

$$\begin{aligned} X &= (1\ u)(2\ v)(3\ w)\cdots(\ell\ t)\cdots \\ \text{and}\quad Y &= (2\ u)(3\ v)(4\ w)\cdots(1\ t)\cdots, \end{aligned}$$

with $u,v,w\cdots t \notin \{1,2,\ldots,\ell\}$. In the product $\alpha = XY$ we have the two ℓ-cycles $(1\ 2\cdots\ell)$ and $(t\cdots w\ v\ u)$. Therefore for these cycles of α which are not in S, the number of cycles of each length must be even. To factor those cycles of α that are not in S we pair off the cycles so that each pair consists of two cycles of the same length. If one cycle in a pair is $(1\ 2\cdots\ell)$, then we choose a letter, say u, from the other cycle and the factorization for that pair of cycles is completely determined. The number of such factorizations is the number of choices of u; thus there are ℓ factorizations.

The number of i-cycles in the decomposition which are not in S is $m_i - k_i$. There are

$$\frac{(m_i-k_i)!}{2^{\frac{m_i-k_i}{2}}\left(\frac{m_i-k_i}{2}\right)!}$$

ways of pairing off these i-cycles and for each pair of i-cycles we have i factorizations. Therefore the total number of factorizations involving the letters of α which are not in the cycles of S is

$$\prod_{i=1}^{n}\left[\frac{i^{\frac{m_i-k_i}{2}}(m_i-k_i)!}{2^{\frac{m_i-k_i}{2}}\left(\frac{m_i-k_i}{2}\right)!}\right].$$

Thus for fixed S, the number of ways of factoring α is

$$\left[\frac{t!}{\left(\frac{t}{2}!\right)^2}\right]\left[\prod_{\substack{j \text{ cycle in } S\\ j \text{ even}}}\left(\frac{j}{2}\right)\right]\left[\prod_{\substack{j \text{ cycle in } S\\ j \text{ odd}}} j\right]\left[\prod_{j=1}^{n}\left(\frac{j^{\frac{m_j-k_j}{2}}(m_j-k_j)!}{2^{\frac{m_j-k_j}{2}}\left(\frac{m_j-k_j}{2}\right)!}\right)\right].$$

For fixed j, the number of j-cycles in S is k_j and $\sum_{\substack{j=1 \\ j \text{ even}}}^{n} k_j = t$, so we have

$$\prod_{\substack{j \text{ cycles of } S \\ j \text{ even}}} \left(\frac{j}{2}\right) = 2^{-t} \prod_{\substack{j=1 \\ j \text{ even}}}^{n} j^{k_j}$$

$$\text{and} \quad \prod_{\substack{j \text{ cycles of } S \\ j \text{ odd}}} j = \prod_{\substack{j=1 \\ j \text{ odd}}}^{n} j^{k_j}.$$

Thus our formula becomes

$$\frac{t!}{\left(\frac{t}{2}!\right)^2} \times \frac{1}{2^t} \left(\prod_{j=1}^{n} j^{k_j}\right) \left(\prod_{j=1}^{n} \frac{j^{\frac{m_j-k_j}{2}}(m_j-k_j)!}{2^{\frac{m_j-k_j}{2}}\left(\frac{m_j-k_j}{2}\right)!}\right)$$

$$= \frac{t!}{\left(\frac{t}{2}!\right)^2} \times 2^{-t} \left[\prod_{j=1}^{n} \frac{j^{\frac{m_j+k_j}{2}}(m_j-k_j)!}{2^{\frac{m_j-k_j}{2}}\left(\frac{m_j-k_j}{2}\right)!}\right].$$

This completes the proof of the theorem.

Rejewski's Theorem is the special case of the above theorem in which $2m = n$. In this case $k_j = 0$ for all j and so $t = 0$.

The conjugacy classes of the symmetric group S_n are in one-to-one correspondence with the partitions of n; thus a conjugacy class is completely determined by a partition (see Rotman [17]).

Example. Suppose that $\alpha \in S_{26}$ is given by the partition

$$26 = 4+3+3+2+2+2+1+1+1+1+1+1+1+1+1+1.$$

In α we have one 4-cycle, two 3-cycles, three 2-cycles and ten 1-cycles. Suppose we want to express α as a product XY with X and Y in $G(26,6)$. We must select for S fourteen cycles (out of sixteen). By the conditions of the theorem we can leave out two 3-cycles or leave out two 2-cycles or leave out two 1-cycles when we choose S.

Case 1. Suppose that S is the fourteen cycles of α leaving out the two 3-cycles. Therefore $k_1 = 10$, $k_2 = 3$, $k_3 = 0$, $k_4 = 1$; so $t = 4$. For the factoring of the cycles of S we have

$$\frac{4!}{(2!)^2} \times \left(\frac{2}{2}\right)^3 \times \left(\frac{4}{2}\right) \times (1)^{10} = 12 \text{ ways.}$$

For the factoring of the cycles of α that are not in S we have 3 ways. Therefore the number of ways of factoring α is 36.

Case 2. Suppose that S is fourteen cycles of α leaving out two 2-cycles. There are 3 ways of doing this. Now $k_1 = 10,\ k_2 = 1,\ k_3 = 2,\ k_4 = 1$ and $t = 2$.

For the factoring of the cycles of S we have

$$\frac{2!}{(1!)^2} \times \frac{4}{2} \times 3 \times 3 = 36 \text{ ways.}$$

Since there are 3 ways of choosing S this gives 108 factorizations. Finally there are 2 ways of factoring the cycles not in S. This gives 216 factorizations.

Case 3. Suppose that S is fourteen cycles of α leaving out two 1-cycles. There are $\binom{10}{2} = 45$ ways of doing this. In this case $k_1 = 8,\ k_2 = 8,\ k_3 = 2,\ k_4 = 1$ and $t = 4$. In the factoring of the cycles of S we have

$$\binom{4}{2} \times \binom{4}{2} \times 3^2 = 108 \text{ ways.}$$

Since there are 45 choices for S we have 4860 ways of factoring α in this case.

The total number of factorizations of α into XY with X and Y both in $G(26, 6)$ is $36 + 216 + 4860 = 5112$.

The size of the conjugacy class of α is

$$\frac{26!}{4 \times 3^2 \times 2! \times 2^3 \times 3! \times 10!} \approx 3.22 \times 10^{16}.$$

THEOREM 2. Let m and n be integers with $n \geq 1,\ m \geq 0$ and $n \geq 2m$. If n is even (odd) then $\alpha \in S_n$ can be expressed as a product XY with X and Y in $G(n, m)$ only if α is a product of an even (odd) number of disjoint cycles.

PROOF. The number of cycles in α is $\sum m_i$. If n is even (odd), then so is $n - 2m$ which is $\sum k_i$. As each $m_i - k_i$ is even, we have $\sum m_i$ even (odd).

COROLLARY. The equation $XY = \alpha,\ \alpha \in S_{26}$, has a solution with X and Y in $G(26, 6)$ only if α decomposes into an even number of at least fourteen cycles. So α must be a product of 14, 16, 18, 20, 22, 24 or 26 cycles.

THEOREM 3 ([5, Theorem 342]). The number of partitions of n into m parts equals the number of partitions of n into parts, the longest of which is m.

The number of partitions of 26 into 14 parts is thus the number of partitions of 26 into parts, the longest of which is 14. Such a partition has the form

14 + a partition of 12, so there are $p(12)$ (the number of partitions of 12) such partitions. Similarly the number of partitions of 26 into 16 parts is $p(10)$.

THEOREM 4. The number of conjugacy classes $[\alpha]$ of S_{26} for which the equation $XY = \alpha$ has a solution with X and Y in $G(26, 6)$ is 160.

PROOF. The element α decomposes into a product of 14, 16, 18, 20, 22, 24 or 26 cycles. The number of decompositions is

$$p(12) + p(10) + p(8) + p(6) + p(4) + p(2) + 1 = 77 + 42 + 22 + 11 + 5 + 2 + 1 = 160.$$

Therefore there are at most 160 conjugacy classes for which the equation has a solution of the required form.

Suppose on the other hand that we partition 26 into k parts with k even and greater than or equal to 14. There have to be at least $2(k - 13)$ ones involved in the partition. (If there are ℓ 1-cycles, then $26 \geq 2(k - \ell) + \ell = 2k - \ell$, so $\ell \geq 2(k - 13)$.) We can form the set S by omitting k–14 1-cycles. The number of cycles in S is then 14. As the number of odd cycles in the decomposition of α must be even, the number of even cycles must also be even and the conditions of Theorem 1 are satisfied.

The following is a rather technical theorem dealing with probabilities (counting) in finite groups.

THEOREM 5. Suppose that C is a conjugacy class of the finite group G. Then the following probabilities are equal.

1. If $(p_1, p_2, p_3, p_4, q_1, q_2, q_3, q_4) \in C^8$, the probability that p_1p_2 is conjugate to q_1q_2 and p_3p_4 is conjugate to q_3q_4.
2. If $(p_1, p_2, p_3, p_4, u, v) \in C^4 \times G^2$, the probability that p_1p_2 is conjugate to $u^{-1}p_1up_2$ and p_3p_4 is conjugate to $v^{-1}p_3vp_4$.
3. If $(p_1, p_2, p_3, p_4, u, v, w, x) \in C^4 \times G^4$, the probability that $u^{-1}p_1up_2$ is conjugate to $v^{-1}p_1vp_2$ and $w^{-1}p_3wp_4$ is conjugate to $x^{-1}p_3xp_4$.
4. If $(p_1, p_2, p_3, q_1, q_2, q_3, u, v, w, x) \in C^6 \times G^4$, the probability that $u^{-1}p_1up_2$ is conjugate to $v^{-1}q_1vq_2$ and $w^{-1}p_2wp_3$ is conjugate to $x^{-1}q_2xq_3$.
5. If $(p_1, p_2, p_3, p_4, p_5, p_6, q_1, q_2, q_3, q_4, q_5, q_6) \in C^{12}$ satisfies the conditions p_ip_{i+3} is conjugate to q_iq_{i+3}, $i = 1, 2, 3$, the probability that p_1p_2 is conjugate to q_1q_2 and p_2p_3 is conjugate to q_2q_3.

PROOF. 1) = 2). If $a \in G$ is chosen at random, the probability that $q_1 = a^{-1}p_1a$ is $|C|^{-1}$ (where $|C|$ = number of elements of C). Instead of thinking of p_1, p_2, q_1, q_2

being chosen at random, think of p_1 and p_2 being chosen at random in C and a and b being chosen at random in G. Let $q_1 = a^{-1}p_1a$ and $q_2 = b^{-1}p_2b$. Then $q_1q_2 = a^{-1}p_1ab^{-1}p_2b$ which is conjugate to $(ab^{-1})^{-1}p_1(ab^{-1})p_2$. But if a and b are chosen at random, then $u = ab^{-1}$ is also random (for the probability that $ab^{-1} = u$ for some specific u is $|G|^{-1}$). Thus the probability that p_1p_2 is conjugate to q_1q_2 is the same as the probability that p_1p_2 is conjugate to $u^{-1}p_1up_2$.

2) = 3) Straightforward.

3) = 4) Choose $a, b \in G$ at random and let $p_4 = a^{-1}p_2a$ and $q_4 = b^{-1}q_2b$. Let $a^{-1}w = w^*$ and $b^{-1}x = x^*$. Then $w^{-1}p_2wp_3 = w^{*^{-1}}a^{-1}p_2aw^*p_3 = w^{*^{-1}}p_4w^*p_3$ and $x^{-1}q_2xq_3 = x^{*^{-1}}b^{-1}q_2bx^*q_3 = x^{*^{-1}}q_4x^*q_3$. The probability that $u^{-1}p_1up_2$ is conjugate to $v^{-1}q_1vq_2$ and $w^{-1}p_2up_3$ is conjugate to $x^{-1}q_2xq_3$ is the same as the probability that $u^{-1}p_1up_2$ is conjugate to $v^{-1}q_1vq_2$ and $w^{*^{-1}}p_4w^*p_3$ is conjugate to $x^{*^{-1}}q_4x^*q_3$.

4) = 5) Consider the set C^{12} with the relation $\sim$ defined by

$$(p_1, p_2, p_3, p_4, p_5, p_6, q_1, q_2, q_3, q_4, q_5, q_6) \sim (p_1', p_2', p_3', p_4', p_5', p_6', q_1', q_2', q_3', q_4', q_5', q_6')$$

if there exist elements $u, v, w, x, y, z \in G$ such that

$$\begin{array}{lll} p_1' = u^{-1}p_1u & p_2' = v^{-1}p_2v & p_3' = w^{-1}p_3w \\ p_4' = u^{-1}p_4u & p_5' = v^{-1}p_5v & p_6' = w^{-1}p_6w \\ q_1' = x^{-1}q_1x & q_2' = y^{-1}q_2y & q_3' = z^{-1}q_3z \\ q_4' = x^{-1}q_4x & q_5' = y^{-1}q_5y & q_6' = z^{-1}q_6z. \end{array}$$

This relation is an equivalence relation.

Also note that if

$$(p_1, p_2, p_3, p_4, p_5, p_6, q_1, q_2, q_3, q_4, q_5, q_6) \sim (p_1', p_2', p_3', p_4', p_5', p_6', q_1', q_2', q_3', q_4', q_5', q_6')$$

and if p_ip_{i+3} is conjugate to q_iq_{i+3}, $i = 1, 2, 3$, then $p_i'p_{i+3}'$ is conjugate to $q_i'q_{i+3}'$, $i = 1, 2, 3$. Thus the property that p_ip_{i+3} is conjugate to q_iq_{i+3}, $i = 1, 2, 3$, is a property of the equivalence class.

Suppose that the above property holds in an equivalence class and that $p_1' = u^{-1}p_1u$, as before. Then $p_1'p_2'$ is conjugate to $q_1'q_2'$ and $p_2'p_3'$ is conjugate to $q_2'q_3'$ if and only if $(uv^{-1})^{-1}p_1(uv^{-1})p_2$ is conjugate to $(xy^{-1})^{-1}q_1(xy^{-1})q_2$ and $(vw^{-1})^{-1}p_2(vw^{-1})p_3$ is conjugate to $(yz^{-1})q_2(yz^{-1})q_3$.

But if u, v, w, x, y, z are chosen at random in G, then uv^{-1}, xy^{-1}, vw^{-1} and yz^{-1} are also random.

This completes the proof of the theorem.

We now state without proof two theorems that will be needed. The proofs can be found elsewhere.

THEOREM 6 (CONJUGACY THEOREM). Suppose that $\alpha, \beta \in S_n$. Then the equation $X^{-1}\alpha X = \beta$ has a solution in S_n if and only if α and β decompose with the same number of cycles of each length (α and β have the same cycle structure). Suppose that α (and β) is the product of m_i i-cycles, $i = 1, 2, \ldots, n$. Then the number of solutions of the equation $X^{-1}\alpha X = \beta$ is

$$\prod_{i=1}^{n} [i^{m_i} \times m_i!].$$

If this number is not "too large", then one can efficiently list all of the solutions.

See [8] for a reference.

THEOREM 7. Let n be a positive integer. Suppose that X and Y are chosen at random in $G(2n, n)$ (in S_{2n}). Then the probability that XY is in the conjugacy class consisting of these elements which decompose into products of $2m_i$ i-cycles, $i = 1, 2, \ldots, n$, is

$$\frac{2^{2n}(n!)^2}{(2n)!} \prod_{i=1}^{n} \left[\frac{1}{2^{m_i} \times m_i! \times i^{m_i}} \right].$$

See [8] for a proof.

Theorem 7 is used in calculating the tables at the end of the paper.

4. A POSSIBLE METHOD

We now put the results from the previous sections to work in a possible method for recovering the wiring of the rotors without the use of plugboard settings.

We assume that we have identified the characteristic collisions for a period of four to five years. Suppose that we have such a characteristic collision. Let $P_1, P_2, P_3, P_4, P_5, P_6$ be the first six permutations on one of the days and let $Q_1, Q_2, Q_3, Q_4, Q_5, Q_6$ be the first six permutations on the other day. In a period of four years we can expect about 1067 characteristic collisions while in a period of five years we can expect about 1826 characteristic collisions.

If the characteristic collision is a collision, then we must have P_1P_2 conjugate to Q_1Q_2 and P_2P_3 conjugate to Q_2Q_3. Using Theorem 5 we calculate that there is about 1 chance in 100 that a characteristic collision will satisfy this property.

Therefore, we expect to have no more than 20 characteristic collisions which will pass this test and these will include the true collisions.

Now given a characteristic collision which has passed the above test, once again let $P_1, P_2, P_3, P_4, P_5, P_6$ and $Q_1, Q_2, Q_3, Q_4, Q_5, Q_6$ be the first six permutations on the two days. Suppose that this is a collision. Let $X_1, X_2, X_3, X_4, X_5, X_6$ be the first six permutations induced by the rotors and the reflector. These are the same on the two days. Let V be the plugboard setting on one day and let V^* be the plugboard setting on the other day. Then

$$P_i = VX_iV^{-1}, \quad i = 1, 2, 3, 4, 5, 6,$$

and

$$Q_i = V^*X_iV^{*-1}, \quad i = 1, 2, 3, 4, 5, 6.$$

Therefore

$$Q_i = (V^*V^{-1})P_i(V^*V^{-1})^{-1},$$

so

$$Q_iQ_j = (V^*V^{-1})P_iP_j(V^*V^{-1})^{-1}.$$

As we have several choices for P_iP_j $(1 \leq i < j \leq 6)$ (more precisely several choices for $j - i$), we can assume that the number of solutions of the equation

$$Q_iQ_j = YP_iP_jY^{-1}$$

is at most 2500 (from the tables). This is justified since the weighted number of solutions for 75% of the cases of the Conjugacy Equation is less than 2500. From our twenty characteristic collisions, we will end up with at most 50,000 solutions to the Conjugacy Equation.

Of these roughly 50,000 solutions we want to find those that can be factored into a product of two elements of $G(26, 6)$. As the number of elements of $G(26, 6)$ is about 10^{11}, the probability that a permutation in S_{26} will factor into such a product is at most $\frac{10^{22}}{26!} \approx 2.47 \times 10^{-5}$. The permutations that do factor are members of 160 conjugacy classes (Theorem 4). From our (at most) 50,000 solutions we can expect at most 20 will pass the test.

We now use the Factoring Theorem to factor each of these permutations into a product of two elements of $G(26, 6)$. As the weighted mean for the number of solutions of $XY = \alpha$ for 90% of the products XY is less than 1200 (this comes from the tables), we can solve the equation $XY = \alpha$ for those α for which the number of solutions is at most 1200. If we started with eight equations (among the 20) for which we can solve for the plugboard settings, we may be only left

with seven such equations that we can solve. For the (at most) 20 equations we will have at most 24,000 factorings and, hence, 48,000 possible plugboard settings. Which of these are plugboard settings for the given days?

Suppose that (V, V^*) is a factorization of X from the equation $Q_iQ_j = XP_iP_jX^{-1}$. Suppose, as before, that P_1, P_2, P_3, P_4, P_5 and P_6 are the first six permutations on one day and that $Q_1, Q_2, Q_3, Q_4, Q_5, Q_6$ are the first six permutations on the other day. If V is the plugboard setting for the first day and V^* is the plugboard setting for the second day, then

$$V^{-1}P_iVC^{-1}V^{-1}P_{i+1}VC$$

is conjugate to

$$V^{-1}P_{i+1}VC^{-1}V^{-1}P_{i+2}VC, \quad i = 1, 2, 3, 4,$$

and

$$V^{*-1}Q_iV^*C^{-1}V^*Q_{i+1}V^*C$$

is conjugate to

$$V^{*-1}Q_{i+1}V^*C^{-1}V^{*-1}Q_{i+2}V^*C, \quad i = 1, 2, 3, 4.$$

(See [8] in the discussion after Theorem 4.) As before, C is the 26-cycle $(1\ 2\ \cdots\ 26)$.

These conjugacy relations should be independent as they describe the internal workings of the Enigma machine through the permutations. Therefore, these eight conjugacy relations should happen with a probability of about 10^{-8} (recall that the probability of one holding is about one in ten). This allows us to reduce our 24,000 pairs to a few possible plugboard settings.

In Rejewski's system of equations there are six equations for the right-hand rotor for each plugboard setting. The estimate for the number of solutions for W, the right-hand rotor, in [8] suggests that it is likely that we will have only a few solutions for each rotor and a final determination of the correct wiring can be made empirically.

If we start with eight collisions and solve completely for seven, then there is better than an 82% probability that we will obtain the wiring for all three rotors. To have these eight collisions in the equations that we are solving we will need to have about 12 collisions (recall that only about 65% of collisions are detected by characteristic collisions). As we stated earlier, to have about 12 collisions should take somewhat more than four years.

5. CONCLUSIONS

The main limitation to Rejewski's proposed method for breaking the Enigma without initial setting is the time required to gather the data. Although a considerable amount of calculations have to be done, it appears that this amount is not unreasonably large. In order to have a reasonable likelihood of success, one probably wants about eight collisions (although this is not necessary) and to collect these would require about four or five years. This is an estimate of the time required to recover the wiring of all three rotors.

If one only needed to recover the wiring of two rotors, then less time would be required. In this case one would use some other method to recover the wiring of the third rotor.

6. THE TABLES

Two partial tables are provided to justify our calculations.

Table A deals with the conjugacy classes $[\alpha]$ of S_{26} for which the equation $XY = \alpha$ has a solution with $X, Y \in G(26, 13)$. Column I is the conjugacy class described by the number of cycles of each length. For example, $2\times\underline{8}+2\times\underline{3}+4\times\underline{1}$ means two 8-cycles, two 3-cycles and four 1-cycles. Column II is the approximate probability that if X and Y are chosen at random from $G(26, 13)$, then XY is in the conjugacy class. Column III is the number of solutions of the equation $Z^{-1}\alpha Z = \alpha$ for the conjugacy class $[\alpha]$. Column IV is the weighted number of solutions of the above equation. This is Column II times Column III. Column V is an approximation of the probability (Column II) squared. Column VI is the number of solutions of the equation $XY = \alpha$, with $X, Y \in G(26, 13)$.

Table B deals with the conjugacy classes $[\alpha]$ of S_{26} for which the equation $XY = \alpha$ has a solution with X and Y in $G(26, 6)$. Column I is the conjugacy class. Column II is the conjugate partition of the partition in I. Column III is the approximate size of the conjugacy class. Column IV is the number of solutions of $XY = \alpha$ with $X, Y \in G(26, 6)$. Column V is the approximate probability that if X and Y are chosen at random from $G(26, 6)$, then the product XY is in the conjugacy class.

Enigma Table A

I	II	III	IV	V	VI
$2 \times \underline{13}$	.248	338	83.8	.0616	13
$2 \times \underline{12} + 2 \times \underline{1}$	.134	576	77.2	.0181	12
$2 \times \underline{11} + 2 \times \underline{2}$	.073	1936	141.3	.0054	22
$2 \times \underline{11} + 4 \times \underline{1}$	.019	5808	110.4	.0004	33
$2 \times \underline{10} + 2 \times \underline{3}$	.054	3600	194.4	.0029	30
$2 \times \underline{10} + 2 \times \underline{2} + 2 \times \underline{1}$	.040	3200	128.0	.0016	20
$2 \times \underline{10} + 6 \times \underline{1}$	.007	144,000	1008.0	—	150
$2 \times \underline{9} + 2 \times \underline{4}$	.045	5184	233.3	.0020	36
$2 \times \underline{9} + 2 \times \underline{3} + 2 \times \underline{1}$	.030	5832	175.0	.0009	27
$2 \times \underline{9} + 4 \times \underline{2}$	.011	62,208	684.3	.0001	108
$2 \times \underline{9} + 2 \times \underline{2} + 4 \times \underline{1}$					54
$2 \times \underline{9} + 8 \times \underline{1}$					945
$2 \times \underline{8} + 2 \times \underline{5}$	.040	6,400	256.0	.0016	40
$2 \times \underline{8} + 2 \times \underline{4} + 2 \times \underline{1}$	.025	8,192	204.8	.0006	32
$2 \times \underline{8} + 2 \times \underline{3} + 2 \times \underline{2}$	.017	18,432	313.3	.0003	48
$2 \times \underline{8} + 2 \times \underline{3} + 4 \times \underline{1}$					72
$2 \times \underline{8} + 4 \times \underline{2} + 2 \times \underline{1}$					96
$2 \times \underline{8} + 2 \times \underline{2} + 6 \times \underline{1}$					240
$2 \times \underline{8} + 10 \times \underline{1}$					7,560
$2 \times \underline{7} + 2 \times \underline{6}$	.038	7,056	268.1	.0015	42
$2 \times \underline{7} + 2 \times \underline{5} + 2 \times \underline{1}$	.023	9,800	225.4	.0005	35
$2 \times \underline{7} + 2 \times \underline{4} + 2 \times \underline{2}$	.014	25,088	351.2	.0002	56
$2 \times \underline{7} + 2 \times \underline{4} + 4 \times \underline{1}$	.014	75,264	1053.0		84
$2 \times \underline{7} + 2 \times \underline{3} + 2 \times \underline{2} + 2 \times \underline{1}$	.001				42
$2 \times \underline{7} + 4 \times \underline{3}$	.013	190,512			189
$2 \times \underline{7} + 2 \times \underline{3} + 6 \times \underline{1}$					315
$2 \times \underline{7} + 6 \times \underline{2}$					840
$2 \times \underline{7} + 4 \times \underline{2} + 4 \times \underline{1}$					252
$2 \times \underline{7} + 2 \times \underline{2} + 8 \times \underline{1}$					1,470
$2 \times \underline{7} + 12 \times \underline{1}$					72,765
$4 \times \underline{6} + 2 \times \underline{1}$	.011	62,208	684.3	.0001	108
$2 \times \underline{6} + 2 \times \underline{5} + 2 \times \underline{2}$	.013	28,800	374.4	.0002	60
$2 \times \underline{6} + 2 \times \underline{5} + 4 \times \underline{1}$	.013				90
$2 \times \underline{6} + 2 \times \underline{4} + 2 \times \underline{3}$	.011	41,472	456.2	.0001	72
$2 \times \underline{6} + 2 \times \underline{4} + 2 \times \underline{2} + 2 \times \underline{1}$	.008	36,864	309.6		48

Enigma Table B

I	II	III	IV	x V			
$12\times\underline{2}+2\times\underline{1}$	$1\times\underline{14}+1\times\underline{12}$				1.03×10^{14}	924	9.52×10^{-6}
$1\times\underline{3}+10\times\underline{2}+3\times\underline{1}$	$1\times\underline{14}+1\times\underline{11}+1\times\underline{1}$				6.03×10^{15}	756	4.56×10^{-4}
$2\times\underline{3}+8\times\underline{2}+4\times\underline{1}$	$1\times\underline{14}+1\times\underline{10}+1\times\underline{2}$				9.04×10^{16}	630	5.70×10^{-3}
$1\times\underline{4}+9\times\underline{2}+4\times\underline{1}$	$1\times\underline{14}+1\times\underline{10}+2\times\underline{1}$				2.26×10^{15}	504	1.14×10^{-4}
$3\times\underline{3}+6\times\underline{2}+5\times\underline{1}$	$1\times\underline{14}+2\times\underline{9}+2\times\underline{3}$				4.50×10^{17}	540	2.43×10^{-2}
$1\times\underline{4}+1\times\underline{3}+7\times\underline{2}+5\times\underline{1}$	$1\times\underline{14}+2\times\underline{9}+2\times\underline{2}+2\times\underline{1}$				4.34×10^{17}	420	1.82×10^{-2}
$1\times\underline{5}+8\times\underline{2}+5\times\underline{1}$	$1\times\underline{14}+1\times\underline{9}+3\times\underline{1}$				6.51×10^{16}	350	2.28×10^{-3}
$4\times\underline{3}+4\times\underline{2}+6\times\underline{1}$	$1\times\underline{14}+1\times\underline{8}+1\times\underline{4}$				7.50×10^{17}	486	3.65×10^{-2}
$1\times\underline{4}+2\times\underline{3}+5\times\underline{2}+6\times\underline{1}$	$1\times\underline{14}+1\times\underline{8}+1\times\underline{3}+1\times\underline{1}$				2.03×10^{18}	360	7.31×10^{-2}
$2\times\underline{4}+6\times\underline{2}+6\times\underline{1}$	$1\times\underline{14}+1\times\underline{8}+4\times\underline{2}$				3.80×10^{17}	280	1.06×10^{-2}
$1\times\underline{5}+1\times\underline{3}+6\times\underline{2}+6\times\underline{1}$	$1\times\underline{14}+1\times\underline{8}+1\times\underline{2}+2\times\underline{1}$				8.10×10^{17}	300	2.43×10^{-2}
$1\times\underline{6}+7\times\underline{2}+6\times\underline{1}$	$1\times\underline{14}+1\times\underline{8}+4\times\underline{1}$				1.45×10^{17}	210	3.05×10^{-3}
$5\times\underline{3}+2\times\underline{2}+7\times\underline{1}$	$1\times\underline{14}+1\times\underline{7}+1\times5$				3.43×10^{17}	486	1.67×10^{-2}
$1\times\underline{4}+3\times\underline{3}+3\times\underline{2}+7\times\underline{1}$	$1\times\underline{14}+1\times\underline{7}+1\times\underline{4}+1\times\underline{1}$				2.57×10^{18}	324	8.33×10^{-2}
$2\times\underline{4}+1\times\underline{3}+4\times\underline{2}+7\times\underline{1}$	$1\times\underline{14}+1\times\underline{7}+1\times\underline{3}+1\times\underline{2}$				2.17×10^{18}	240	5.21×10^{-2}
$1\times\underline{5}+2\times\underline{3}+4\times\underline{2}+7\times\underline{1}$	$1\times\underline{14}+1\times\underline{7}+1\times\underline{3}+2\times\underline{1}$				2.32×10^{18}	270	6.26×10^{-2}
$1\times\underline{5}+1\times\underline{4}+5\times\underline{2}+7\times\underline{1}$	$1\times\underline{14}+1\times\underline{7}+2\times\underline{2}+1\times\underline{1}$				1.04×10^{18}	200	2.08×10^{-2}
$1\times\underline{6}+1\times\underline{3}+5\times\underline{2}+7\times\underline{1}$	$1\times\underline{14}+1\times\underline{7}+2\times\underline{2}+3\times\underline{1}$				1.16×10^{18}	180	2.09×10^{-2}
$1\times\underline{7}+6\times\underline{2}+7\times\underline{1}$	$1\times\underline{14}+1\times\underline{7}+5\times\underline{1}$				2.48×10^{17}	140	3.47×10^{-3}
$6\times\underline{3}+8\times\underline{1}$	$1\times\underline{14}+2\times\underline{6}$				1.91×10^{16}	729	1.39×10^{-3}
$1\times\underline{4}+4\times\underline{3}+1\times\underline{2}+8\times\underline{1}$	$1\times\underline{14}+1\times\underline{6}+1\times\underline{5}+1\times\underline{1}$				7.15×10^{16}	162	1.15×10^{-3}
$2\times\underline{4}+2\times\underline{3}+2\times\underline{2}+8\times\underline{1}$	$1\times\underline{14}+1\times\underline{6}+1\times\underline{4}+1\times2$				2.17×10^{18}	216	4.69×10^{-2}
$1\times\underline{5}+3\times\underline{3}+2\times\underline{2}+8\times\underline{1}$	$1\times\underline{14}+1\times\underline{6}+1\times\underline{4}+2\times\underline{1}$				1.54×10^{18}	270	4.16×10^{-2}

	I	II	III	IV	x V			
$1\times\underline{5}+1\times\underline{4}+1\times\underline{3}+3\times\underline{2}+8\times\underline{1}$	$1\times\underline{14}+1\times\underline{6}+1\times\underline{3}+1\times\underline{2}+1\times\underline{1}$					3.47×10^{18}	180	6.25×10^{-2}
$3\times\underline{4}+3\times\underline{2}+8\times\underline{1}$	$1\times\underline{14}+1\times\underline{6}+2\times\underline{3}$					5.43×10^{17}	160	8.69×10^{-3}
$1\times\underline{6}+2\times\underline{3}+3\times\underline{2}+8\times\underline{1}$	$1\times\underline{14}+1\times\underline{6}+1\times\underline{3}+3\times\underline{1}$					1.93×10^{18}	162	3.13×10^{-2}
$2\times\underline{5}+4\times\underline{2}+8\times\underline{1}$	$1\times\underline{14}+1\times\underline{6}+3\times\underline{2}$					5.21×10^{17}	150	7.82×10^{-3}
$1\times\underline{6}+1\times\underline{4}+4\times\underline{2}+8\times\underline{1}$	$1\times\underline{14}+1\times\underline{6}+2\times\underline{2}+2\times\underline{1}$					1.09×10^{18}	120	1.31×10^{-2}
$1\times\underline{7}+1\times\underline{3}+4\times\underline{2}+8\times\underline{1}$	$1\times\underline{14}+1\times\underline{6}+1\times\underline{2}+4\times\underline{1}$					1.24×10^{18}	126	1.56×10^{-2}
$1\times\underline{8}+5\times\underline{2}+8\times\underline{1}$	$1\times\underline{14}+1\times\underline{6}+6\times\underline{1}$					3.26×10^{17}	40	1.30×10^{-3}
$2\times\underline{4}+3\times\underline{3}+9\times\underline{1}$	$1\times\underline{14}+2\times\underline{5}+1\times\underline{2}$					2.14×10^{16}	54	1.15×10^{-4}
$1\times\underline{5}+4\times\underline{3}+9\times\underline{1}$	$1\times\underline{14}+2\times\underline{5}+2\times\underline{1}$					1.14×10^{17}	135	1.54×10^{-3}
$3\times\underline{4}+1\times\underline{3}+1\times\underline{2}+9\times\underline{1}$	$1\times\underline{14}+1\times\underline{5}+1\times\underline{4}+1\times\underline{3}$					4.82×10^{17}	144	6.94×10^{-3}
$1\times\underline{5}+1\times\underline{4}+2\times\underline{3}+1\times\underline{2}+9\times\underline{1}$	$1\times\underline{14}+1\times\underline{5}+1\times\underline{4}+1\times\underline{2}+1\times\underline{1}$					1.54×10^{18}	180	2.77×10^{-2}
$1\times\underline{6}+3\times\underline{3}+1\times\underline{2}+9\times\underline{1}$	$1\times\underline{14}+1\times\underline{5}+1\times\underline{4}+3\times\underline{1}$					5.72×10^{17}	162	9.27×10^{-3}
$1\times\underline{5}+2\times\underline{4}+2\times\underline{2}+9\times\underline{1}$	$1\times\underline{14}+1\times\underline{5}+2\times\underline{3}+1\times\underline{1}$					8.68×10^{17}	120	1.04×10^{-2}
$2\times\underline{5}+1\times\underline{3}+2\times\underline{2}+9\times\underline{1}$	$1\times\underline{14}+1\times\underline{5}+1\times\underline{3}+2\times\underline{2}$					9.26×10^{17}	150	1.39×10^{-2}
$1\times\underline{6}+1\times\underline{4}+1\times\underline{3}+2\times\underline{2}+9\times\underline{1}$	$1\times\underline{14}+1\times\underline{5}+1\times\underline{3}+1\times\underline{2}+2\times\underline{1}$					1.93×10^{18}	108	2.08×10^{-2}
$1\times\underline{7}+2\times\underline{3}+2\times\underline{2}+9\times\underline{1}$	$1\times\underline{14}+1\times\underline{5}+1\times\underline{3}+4\times\underline{1}$					1.10×10^{18}	126	1.39×10^{-2}
$1\times\underline{6}+1\times\underline{5}+3\times\underline{2}+9\times\underline{1}$	$1\times\underline{14}+1\times\underline{5}+3\times\underline{2}+1\times\underline{1}$					7.72×10^{17}	90	6.95×10^{-3}
$1\times\underline{7}+1\times\underline{4}+3\times\underline{2}+9\times\underline{1}$	$1\times\underline{14}+1\times\underline{5}+2\times\underline{2}+3\times\underline{1}$					8.27×10^{17}	84	6.95×10^{-3}
$1\times\underline{8}+1\times\underline{3}+3\times\underline{2}+9\times\underline{1}$	$1\times\underline{14}+1\times\underline{5}+1\times\underline{2}+5\times\underline{1}$					9.65×10^{17}	72	6.95×10^{-3}
$1\times\underline{9}+4\times\underline{2}+9\times\underline{1}$	$1\times\underline{14}+1\times\underline{5}+7\times\underline{1}$					3.22×10^{17}	54	1.74×10^{-3}
$4\times\underline{4}+10\times\underline{1}$	$1\times\underline{14}+3\times\underline{4}$					1.81×10^{16}	96	1.74×10^{-4}
$1\times\underline{5}+2\times\underline{4}+1\times\underline{3}+10\times\underline{1}$	$1\times\underline{14}+2\times\underline{4}+1\times\underline{3}+1\times\underline{1}$					2.32×10^{17}	120	2.78×10^{-3}
$2\times\underline{5}+2\times\underline{3}+10\times\underline{1}$	$1\times\underline{14}+2\times\underline{4}+2\times\underline{2}$					1.23×10^{17}	225	2.77×10^{-3}
$1\times\underline{6}+1\times\underline{4}+2\times\underline{3}+10\times\underline{1}$	$1\times\underline{14}+2\times\underline{4}+1\times\underline{2}+2\times\underline{1}$					2.57×10^{17}	108	2.78×10^{-3}
$1\times\underline{7}+3\times\underline{3}+10\times\underline{1}$	$1\times\underline{14}+2\times\underline{4}+4\times\underline{1}$					9.80×10^{16}	189	1.85×10^{-3}

I	II	III	IV	k	V			
$2\times\underline{5}+1\times\underline{4}+1\times\underline{2}+10\times\underline{1}$	$1\times\underline{14}+1\times\underline{4}+2\times\underline{3}+1\times\underline{2}$					2.78×10^{17}	100	2.78×10^{-3}
$1\times\underline{6}+2\times\underline{4}+1\times\underline{2}+10\times\underline{1}$	$1\times\underline{14}+1\times\underline{4}+2\times\underline{3}+2\times\underline{1}$					2.89×10^{17}	72	2.08×10^{-3}
$1\times\underline{6}+1\times\underline{5}+1\times\underline{3}+1\times\underline{2}+10\times\underline{1}$	$1\times\underline{14}+1\times\underline{4}+1\times\underline{3}+2\times\underline{2}+1\times\underline{1}$					6.17×10^{17}	90	5.55×10^{-3}
$1\times\underline{7}+1\times\underline{4}+1\times\underline{3}+1\times\underline{2}+10\times\underline{1}$	$1\times\underline{14}+1\times\underline{4}+1\times\underline{3}+1\times\underline{2}+3\times\underline{1}$					6.62×10^{17}	84	5.56×10^{-3}
$1\times\underline{8}+2\times\underline{3}+1\times\underline{2}+10\times\underline{1}$	$1\times\underline{14}+1\times\underline{4}+1\times\underline{3}+5\times\underline{1}$					3.86×10^{17}	72	2.28×10^{-3}
$2\times\underline{6}+2\times\underline{2}+10\times\underline{1}$	$1\times\underline{14}+1\times\underline{4}+4\times\underline{2}$					1.93×10^{17}	54	1.04×10^{-3}
$1\times\underline{7}+1\times\underline{5}+2\times\underline{2}+10\times\underline{1}$	$1\times\underline{14}+1\times\underline{4}+3\times\underline{2}+2\times\underline{1}$					3.97×10^{17}	70	2.78×10^{-3}
$1\times\underline{8}+1\times\underline{4}+2\times\underline{2}+10\times\underline{1}$	$1\times\underline{14}+1\times\underline{4}+2\times\underline{2}+4\times\underline{1}$					4.34×10^{17}	48	2.08×10^{-3}
$1\times\underline{9}+1\times\underline{3}+2\times\underline{2}+10\times\underline{1}$	$1\times\underline{14}+1\times\underline{4}+1\times\underline{2}+6\times\underline{1}$					5.15×10^{17}	54	2.78×10^{-3}
$1\times\underline{10}+3\times\underline{2}+10\times\underline{1}$	$1\times\underline{14}+1\times\underline{4}+8\times\underline{1}$					2.32×10^{17}	30	6.96×10^{-4}
$3\times\underline{5}+11\times\underline{1}$	$1\times\underline{14}+4\times\underline{3}$					1.35×10^{16}	125	1.69×10^{-4}
$1\times\underline{6}+1\times\underline{5}+1\times\underline{4}+11\times\underline{1}$	$1\times\underline{14}+3\times\underline{3}+1\times\underline{2}+1\times\underline{1}$					8.42×10^{16}	60	5.05×10^{-4}
$1\times\underline{7}+2\times\underline{4}+11\times\underline{1}$	$1\times\underline{14}+3\times\underline{3}+3\times\underline{1}$					4.51×10^{16}	56	2.53×10^{-4}
$2\times\underline{6}+1\times\underline{3}+11\times\underline{1}$	$1\times\underline{14}+2\times\underline{3}+3\times\underline{2}$					4.68×10^{16}	54	2.53×10^{-4}
$1\times\underline{7}+1\times\underline{5}+1\times\underline{3}+11\times\underline{1}$	$1\times\underline{14}+2\times\underline{3}+2\times\underline{2}+2\times\underline{1}$					9.62×10^{16}	105	1.01×10^{-3}
$1\times\underline{8}+1\times\underline{4}+1\times\underline{3}+11\times\underline{1}$	$1\times\underline{14}+2\times\underline{3}+1\times\underline{2}+4\times\underline{1}$					1.05×10^{17}	48	5.04×10^{-4}
$1\times\underline{9}+2\times\underline{3}+11\times\underline{1}$	$1\times\underline{14}+2\times\underline{3}+6\times\underline{1}$					6.24×10^{16}	81	5.30×10^{-4}
$1\times\underline{7}+1\times\underline{6}+1\times\underline{2}+11\times\underline{1}$	$1\times\underline{14}+1\times\underline{3}+4\times\underline{2}+1\times\underline{1}$					1.20×10^{17}	42	5.04×10^{-4}
$1\times\underline{8}+1\times\underline{5}+1\times\underline{2}+11\times\underline{1}$	$1\times\underline{14}+1\times\underline{3}+3\times\underline{2}+3\times\underline{1}$					1.26×10^{17}	40	5.04×10^{-4}
$1\times\underline{9}+1\times\underline{4}+1\times\underline{2}+11\times\underline{1}$	$1\times\underline{14}+1\times\underline{3}+2\times\underline{2}+5\times\underline{1}$					1.40×10^{17}	36	5.04×10^{-4}
$1\times\underline{10}+1\times\underline{3}+1\times\underline{2}+11\times\underline{1}$	$1\times\underline{14}+1\times\underline{3}+1\times\underline{2}+7\times\underline{1}$					1.68×10^{17}	30	5.04×10^{-4}
$1\times\underline{11}+2\times\underline{2}+11\times\underline{1}$	$1\times\underline{14}+1\times\underline{3}+9\times\underline{1}$					1.15×10^{17}	22	2.53×10^{-4}
$2\times\underline{7}+12\times\underline{1}$	$1\times\underline{14}+6\times\underline{2}$					8.59×10^{15}	49	4.21×10^{-5}
$1\times\underline{8}+1\times\underline{6}+12\times\underline{1}$	$1\times\underline{14}+5\times\underline{2}+2\times\underline{1}$					1.75×10^{16}	24	4.20×10^{-5}
$1\times\underline{9}+1\times\underline{5}+12\times\underline{1}$	$1\times\underline{14}+4\times\underline{2}+4\times\underline{1}$					1.87×10^{16}	45	8.42×10^{-5}

I	II	III	IV	V			
$1\times\underline{10}+1\times\underline{4}+12\times\underline{1}$					2.10×10^{16}	20	4.20×10^{-5}
$1\times\underline{11}+1\times\underline{3}+12\times\underline{1}$					2.55×10^{16}	33	8.42×10^{-5}
$1\times\underline{12}+1\times\underline{2}+12\times\underline{1}$					3.51×10^{16}	12	4.21×10^{-5}
$1\times\underline{13}+13\times\underline{1}$					4.98×10^{15}	13	6.47×10^{-6}
$10\times\underline{2}+6\times\underline{1}$					1.51×10^{14}		
$1\times\underline{3}+8\times\underline{2}+7\times\underline{1}$					2.58×10^{15}		
$2\times\underline{3}+6\times\underline{2}+8\times\underline{1}$					1.21×10^{16}	6,720	8.13×10^{-3}
$1\times\underline{4}+7\times\underline{2}+8\times\underline{1}$	$1\times\underline{16}+1\times\underline{8}+2\times\underline{1}$				3.88×10^{15}		
$3\times\underline{3}+4\times\underline{2}+9\times\underline{1}$	$1\times\underline{16}+1\times\underline{7}+1\times\underline{3}$				1.79×10^{16}	6,642	1.19×10^{-2}
$1\times\underline{4}+1\times\underline{3}+5\times\underline{2}+9\times\underline{1}$	$1\times\underline{16}+1\times\underline{7}+1\times\underline{2}+1\times\underline{1}$				2.41×10^{16}	5,040	1.21×10^{-2}
$1\times\underline{5}+6\times\underline{2}+9\times\underline{1}$	$1\times\underline{16}+1\times\underline{7}+3\times\underline{1}$				4.82×10^{15}		
$4\times\underline{3}+2\times\underline{2}+10\times\underline{1}$	$1\times\underline{16}+1\times\underline{6}+1\times\underline{4}$				7.15×10^{15}		
$1\times\underline{4}+2\times\underline{3}+3\times\underline{2}+10\times\underline{1}$	$1\times\underline{16}+1\times\underline{6}+1\times\underline{3}+1\times\underline{1}$				3.22×10^{16}	5,112	1.65×10^{-2}
$2\times\underline{4}+4\times\underline{2}+10\times\underline{1}$	$1\times\underline{16}+1\times\underline{6}+2\times\underline{2}$				9.04×10^{15}		
$1\times\underline{5}+1\times\underline{3}+4\times\underline{2}+10\times\underline{1}$	$1\times\underline{16}+1\times\underline{6}+1\times\underline{2}+2\times\underline{1}$				1.93×10^{16}	4,410	8.51×10^{-3}
$1\times\underline{6}+5\times\underline{2}+10\times\underline{1}$	$1\times\underline{16}+1\times\underline{6}+4\times\underline{1}$				4.82×10^{15}		
$5\times\underline{3}+11\times\underline{1}$	$1\times\underline{16}+2\times\underline{5}$				3.46×10^{14}		
$1\times\underline{4}+3\times\underline{3}+1\times\underline{2}+11\times\underline{1}$	$1\times\underline{16}+1\times\underline{5}+1\times\underline{4}+1\times\underline{1}$				7.80×10^{15}		
$2\times\underline{4}+1\times\underline{3}+2\times\underline{2}+11\times\underline{1}$	$1\times\underline{16}+1\times\underline{5}+1\times\underline{3}+1\times\underline{2}$				1.32×10^{16}	4,032	5.32×10^{-3}
$1\times\underline{5}+2\times\underline{3}+2\times\underline{2}+11\times\underline{1}$	$1\times\underline{16}+1\times\underline{5}+1\times\underline{3}+2\times\underline{1}$				1.40×10^{16}	5,070	7.10×10^{-3}
$1\times\underline{5}+1\times\underline{4}+1\times\underline{3}+1\times\underline{2}+11\times\underline{1}$	$1\times\underline{16}+1\times\underline{5}+2\times\underline{2}+1\times\underline{1}$				1.05×10^{16}	3,420	3.59×10^{-3}
$1\times\underline{6}+1\times\underline{3}+3\times\underline{2}+11\times\underline{1}$	$1\times\underline{16}+1\times\underline{5}+1\times\underline{2}+3\times\underline{1}$				1.17×10^{16}	3,078	3.60×10^{-3}
$1\times\underline{5}+1\times\underline{4}+1\times\underline{3}+1\times\underline{2}+12\times\underline{1}$	$1\times\underline{16}+1\times\underline{4}+1\times\underline{3}+1\times\underline{2}+1\times\underline{1}$				7.02×10^{15}	3,960	2.78×10^{-3}
$1\times\underline{3}+6\times\underline{2}+11\times\underline{1}$	$1\times\underline{18}+1\times\underline{7}+1\times\underline{1}$				7.31×10^{13}	392,580	2.87×10^{-3}
$1\times\underline{5}+1\times\underline{4}+1\times\underline{2}+15\times\underline{1}$	$1\times\underline{18}+1\times\underline{3}+2\times\underline{2}+1\times\underline{1}$				7.71×10^{12}	491,400	3.78×10^{-4}

I	II	III	IV	k	V
$1\times\underline{6}+1\times\underline{3}+1\times\underline{2}+15\times\underline{1}$		$1\times\underline{18}+1\times\underline{3}+1\times\underline{2}+3\times\underline{1}$		8.57×10^{12}	$442{,}260$	3.78×10^{-4}
$1\times\underline{9}+17\times\underline{1}$		$1\times\underline{18}+8\times\underline{1}$		1.26×10^{11}	$257{,}040$	3.24×10^{-6}
$1\times\underline{5}+21\times\underline{1}$		$1\times\underline{22}+4\times\underline{1}$		$1{,}578{,}720$	$106{,}832{,}250$	1.69×10^{-7}
$2\times\underline{2}+22\times\underline{1}$		$1\times\underline{24}+1\times\underline{2}$		$44{,}850$	$1{,}289{,}312{,}640$	5.77×10^{-8}
$1\times\underline{3}+23\times\underline{1}$		$1\times\underline{24}+2\times\underline{1}$		$5{,}200$	$3{,}243{,}427{,}110$	1.69×10^{-9}
$26\times\underline{1}$		$1\times\underline{26}$		1	$100{,}391{,}791{,}500$	1.00×10^{-11}

REFERENCES

1. Bertrand, G. 1973. *Enigma, ou la plus grande énigme de la guerre* 1939–1945. Paris, Plon.

2. Bloch, G. 1988. *Enigma Avant Ultra*, Paris (privately printed). Translated by C. A. Deavours in *Cryptologia.*

3. Bloch, G. 1987. Enigma before ultra. Polish work and the French contribution. *Cryptologia.* 11(3): 142–155.

4. Bloch, G. 1987. Enigma before ultra. The Polish success and check (1933–1939). *Cryptologia.* 11(4): 227–234.

5. Hardy, G. H. and E. M. Wright. 1965. *The Theory of Numbers.* 4th Ed., New York: Oxford University Press.

6. Kahn, D. 1983. The spy who most affected WWII. In *Kahn on Codes.* pp. 76–88. New York: Macmillan.

7. Kozaczuk, W. 1967. *Bitwa o tajemnice: Stużby wywiadoweze Polski i Rzerzy Niemieckief 1922–1939*. Warwaw Ksiaźkai Wiedza.

8. Lawrence, J. A study of Rejewski's equations. *Cryptologia.* 29(3): 233-247.

9. Lisicki, T. 1979. Die Leistung des polnischen Entzifferung sdienstes bei der Lösung des Verfahrens der deutschen 'Enigma-Funkschlüsselmachine', in Jüngen Rohwer and Eberhard Jäckel, eds., *Die Funkaufklärung und ihre Rolle im 2. Weltkreig.* Stuttgart. pp. 166–186.

10. Lyndon, R. 1980. Equations in groups. *Bol. Soc. Brasiliero de Mathematics.* 11: 79–102.

11. Mayer, S. 1974. The breaking up of the German ciphering machine 'Enigma' by the cryptological section in the 2nd Department of the Polish Armed Forces General Staff, manuscript, Pifsudski Institute of America, New York. 9 pp. Written May 31, 1974.

12. Rejewski, M. 1984. How the Polish mathematicians broke Enigma, Appendix D. In *Enigma*, by W. Kozaczuk. Bethesda MD: University Publications of America, Inc. 246–271.

13. Rejewski, M. 1984. The mathematical solution of the Enigma cipher, Appendix E. In *Enigma*, by W. Kozaczuk. Bethesda MD: University Publications of America, Inc. 272–290.

14. Rejewski, M. Enigma 1930–1940. Methoda i historia rozwi zania niemieckiego szyfru maszynowego (w. zarysie), 31 pp. Available at the website `www.spybooks.pl/en/enigma.html`.

15. Rejewski, M. Czy bez dokument w uzyskanych drog wywiadu by o mo liwe

rozwi zanie "Enigmy"? (Was it possible to break Enigma code without Asche's documents?), 1 page. Available at website `www.spybooks.pl/en/enigma.html`.

16. Rejewski, M. Szkic methody zomania szy fru Enigma bez pomocy materiau wywiado wczeo (How to break Enigma cipher without any outside assistance), 2 pages. Available at website `www.spybooks.pl/en/enigma.html`.

17. Rotman, J. 1984. *An Introduction to the Theory of Groups.* Upper Saddle River NJ: Allyn and Bacon.

18. Welchman, G. 1982. *The Hot Six Story. Breaking the Enigma Codes.* New York: McGraw-Hill Book Co.

BIOGRAPHICAL SKETCH

John Lawrence is a graduate of Carleton University and McGill University. He teaches mathematics at the University of Waterloo.