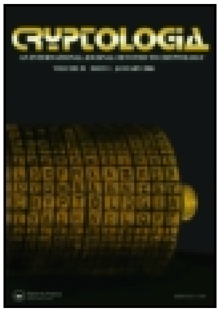

Cryptologia
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/ucry20

THE VERSATILITY OF REJEWSKI'S METHOD: SOLVING FOR THE WIRING OF THE SECOND ROTOR

John Lawrence [a]

[a] Department of Pure Mathematics, University of Waterloo, Waterloo, Ontario N2L 3G1 CANADA. jwlawren@math.uwaterloo.ca

Available online: 04 Jun 2010

THE VERSATILITY OF REJEWSKI'S METHOD: SOLVING FOR THE WIRING OF THE SECOND ROTOR

John Lawrence

ADDRESS: Department of Pure Mathematics, University of Waterloo, Waterloo, Ontario N2L 3G1 CANADA. jwlawren@math.uwaterloo.ca.

ABSTRACT: We show that the recovery of the wiring of the second rotor of the Enigma does not depend on the rotors being reordered.

KEYWORDS: Enigma, Rejewski, rotor.

The story of the breaking of the Enigma by the Polish Cipher Bureau is now well-known. Rejewski found a method of retrieving the first six permutations of the day (for most days) and set up six equations expressing relations among various components of the Enigma. After being supplied with the key settings for a two-month period, he was able to use the equations to solve for the wiring of the right-hand rotor. Rejewski states that after finding the wiring of the first rotor, he used the fact the period of the key settings that he was given straddled two yearly quarters. In these two quarters the rotors were in different orders, so he was able to solve for a second rotor which was now on the right-hand side in the second month.

Rejewski's description of how he discovered the wiring of the second rotor has led some authors to conclude that if the rotors had not been reordered or if the period of the key settings had not straddled two yearly quarters, then Rejewski would not have been able to find the wiring of a second rotor.

David Kahn, in his book 'Seizing the Enigma,' says, "Here the Poles had a stroke of luck. The Germans changed the order of the rotors every three months, or quarter of a year. Fortunately, the keys that Schmidt had supplied straddled two different quarters" [2, p. 66].

Stephen Budiansky, in his book 'Battle of Wits,' comments that "It was true irony that a procedure intended to enhance the Enigma's security had undermined it; were it not for the changes in the rotor order, Rejewski would have hit another impasse ..." [1, p. 102].

The purpose of this note is to show that even if the order of the rotors had not been changed over the two-month period of the supplied keys, Rejewski, with a small modification in his method, would have been able to solve for the wiring of the second rotor (as well as the third rotor and the reflector).

Among the documents which were stolen by Schmidt and eventually passed on to Rejewski was the 'Schlüsselanleitung für die Chiffriermaschine Enigma.' This gave the daily keying instructions for a two-month period. In particular it gave daily settings for (1) the initial rotor settings including the order of the rotors, (2) the ring settings for each rotor, and (3) the plugboard settings [2, pp. 60–62].

Let us suppose that we have the key settings for a two-month period of sixty days. Assume also that over that period, the ordering of the rotors remains the same.

As there are $\frac{60\times 59}{2} = 1770$ unordered pairs of distinct days in the sixty day period and the chance is $\frac{1}{26}$ that for a pair of days, the initial position of the third rotor is the same, we can expect to find about $\frac{1}{26}\times 1770 \approx 68$ pairs of days (D, D') where the initial position of the third rotor on day D is the same as the initial position of the third rotor on day D'. Denote the set of these pairs of days by T.

In Rejewski's set of equations [4, p. 277], we already know the left side as well as S (the plugboard setting) and N (the wiring of the first rotor). Therefore if $(D, D') \in T$, then for day D we have an equation

$$A = P^kMP^{-k}LRL^{-1}P^kM^{-1}P^{-k}$$

and for day D' we have an equation

$$B = P^\ell MP^{-\ell}LRL^{-1}P^\ell M^{-1}P^{-\ell},$$

where A and B are known permutations. In these equations, M is the second rotor, L is the third rotor, R is the reflector and k and ℓ are integers between 1 and 26 which give the initial position of the second rotor on the respective days. The integers k and ℓ can be easily determined by looking up the ring settings and the rotor settings for the particular day.

Since

$$LRL^{-1} = P^kM^{-1}P^{-k}AP^kMP^{-k},$$

we have

$$B = P^\ell MP^{-\ell}P^kM^{-1}P^{-k}AP^kMP^{-k}P^\ell M^{-1}P^{-\ell},$$

so

$$P^{-\ell}BP^{-\ell} = (MP^{(k-\ell)}M^{-1})(P^{-k}AP^k)(MP^{-(k-\ell)}M^{-1}).$$

Both $P^{-\ell}BP^{\ell}$ and $P^{-k}AP^{k}$ are known, so we denote them by B^* and A^*, respectively. We assume that $k-\ell>0$ and denote it by a. The resulting equation is

$$B^* = MP^aM^{-1}A^*MP^{-a}M^{-1}$$

There are 12 positive integers less than 26 which are coprime to 26. Thus the probability of two equations having the above form with the same exponent a which is coprime to 26 is $\frac{12}{26^2}=\frac{12}{676}$. We have about $\frac{68\times 67}{2}=2278$ unordered pairs of equations, so we should expect about $2278\times\frac{12}{676}\approx 40$ pairs of equations such that for each pair we have the same exponent a in both equations and a is coprime to 26. Note, however, that we may have different a's for different pairs.

Choose such a pair of equations

$$\begin{aligned} B_1^* &= MP^aM^{-1}A_1^*MP^{-a}M^{-1} \\ B_2^* &= MP^aM^{-1}A_2^*MP^{-a}M^{-1}. \end{aligned}$$

Multiplying the two sides gives

$$B_1^*B_2^* = MP^aM^{-1}A_1^*A_2^*MP^{-a}M^{-1}.$$

We want $A_1^*A_2^*$ (and $B_1^*B_2^*$) to be in a conjugacy class of S_{26} for which the above equation has as few solutions as possible (for MP^aM^{-1}). The conjugacy class consisting of those elements of S_{26} which are a product of two disjoint 13-cycles is the best a[3]. In this case we get 338 solutions for MP^aM^{-1}. As a is coprime to 26, P^a has order 26, so we get $26\times 338=8788$ possible solutions for M—the wiring of the second rotor. To find the correct solution we must test the solutions of our equation in other equations of the form

$$B_3^*B_4^* = (MP^bM^{-1})A_3^*A_4^*(MP^bM^{-1}).$$

The same procedure is followed in solving for the wiring of the first rotor.

Of course, the above method can be modified to find the wiring of the third rotor as well.

One can see that the above method is just a variation on the method used by Rejewski to find the wiring of the first rotor. It is very hard to believe that he would not have thought of this variation had the need arisen.

With only a one-month supply of settings one could still attempt to use the above method but in order to get enough equations we would probably have to change the condition that the exponent a is coprime to 26 (although we would certainly want a to be coprime to 13). This would lead to a greater number of solutions to the final equation.

REFERENCES

1. Budiansky, S. 2000. *Battle of Wits, The Complete Story of Codebreaking in World War II*, New York: The Free Press.

2. Kahn, D. 1991. *Seizing the Enigma, The Race to Break the German U-Boat Codes 1939–1943*. Boston MA: Houghton Mifflin.

3. Lawrence, J. A study of Rejewski's equations. (Preprint.)

4. Rejewski, M. 1984. How Polish mathematicians broke Enigma. Appendix D, in *Enigma*, by W. Kozaczuk, pp. 246–271. Lanham MD: University Publications of America, Inc.

BIOGRAPHICAL SKETCH

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