How Polish Mathematicians Deciphered the Enigma

MARIAN REJEWSKI

The paper gives a personal view of work in the Polish Cipher Bureau From 1932 to 1939 as mathematicians worked to decipher the codes of the military version of the Enigma. The author, who was a participant. relates details of the device and the successes and frustrations involved in the work. He also describes mathematical principles that enabled him and his colleagues to break successive versions of the Enigma code and to construct technical devices (cyclometers and "bombs") that facilitated decipherment of Enigma-coded messages.

Keywords: Enigma, cryptology
***CR Category:** 1.2*

Introduction

At the end of 1927, or possibly at the beginning of 1928, a parcel containing radio equipment, according to the declaration, arrived from Germany at the customs house in Warsaw. Because the parcel had been sent erroneously in place of other equipment, a representative of a German firm very insistently demanded the return of the parcel to the German government before it was cleared through customs. His demands were so urgent that they awakened the suspicions of the customs officers, who informed the Cipher Bureau of the Second Department of the General Staff, an institution interested in every kind of innovation in the area of radio equipment. Since it happened to be Saturday afternoon, the employees delegated by the bureau had time to study the matter at leisure. The box was carefully opened, and it was determined that indeed it did not contain radio equipment; it contained a cipher machine. The machine was thoroughly examined, and then the box was carefully refastened.

You can easily surmise that this cipher machine was the Enigma--clearly the commercial version—because at that time the military version was not in use at all. The episode had no immediate significance, being simply the time the Cipher Bureau became interested in the Enigma machine and manifested that interest by the completely legal purchase of another unit of the commercial machine.

When the first machine-enciphered messages appeared on the air on July 15, 1928, transmitted by a German military station, Polish radio telegraphers working at monitoring stations began to pick up the transmissions. Polish cryptologists in the German section of the Cipher Bureau received orders to undertake an attempt to decipher them. But the effort was unsuccessful and after a time was terminated. Very minute traces of that work were left in the form of several sheets of paper densely filled with writing; the commercial version of the Enigma machine also was available.

This article was entitled "Jak matematycy polscy rozszyfrowali Enigmę" in the Annals of the Polish Mathematical Society. Series II, *Wiadomości Matematyczne*, Volume 23, 1980, 1–28, copyright © Państwowe Wydawnictwo Naukowe, Warsaw, 1980, translated by Joan Stepenske with the permission of the publisher. Translation © 1981 by the American Federation of Information Processing Societies. Inc. Permission to copy without fee all or part of this material is granted provided that the copies are not made or distributed for direct commercial advantage. the AFIPS copyright notice and the title of the publication and its date appear, and notice is given that copying is by permission of the American Federation of Information Processing Societies, Inc. To copy otherwise, or to republish, requires specific permission.
© 1981 AFIPS 0164-1239/81/030213-234$01.00/0

Editor's Note. We would like to thank Joan Stepenske for translating this article from the Polish. We also want to thank Zbigniew Semadeni and Wladyslaw M. Turski for their efforts in obtaining the article and in ensuring a faithful translation. We are grateful to Joanna Siemien for compiling bibliographic data.

Marian Rejewski

But the Cipher Bureau, whose chief at that time was Major F. Pokorny (related to the famous cryptologist of the Austrian army during World War I, Captain Herman Pokorny), did not give up. At the end of 1928, a course in cryptology was set up in Poznań for students who were completing their course of study in mathematics and were fluent in German. When the course ended, a temporary branch of the Cipher Bureau was formed in Poznań for some of the participants. Finally, on September 1, 1932, three math graduates employed in the agency were hired for permanent work at the Cipher Bureau in Warsaw, located on Saski Square in the General Staff Building, which is no longer standing.

There we three (Jerzy Różycki, Henryk Zygalski, and Marian Rejewski) received as our first independent assignment the task of solving a code of the German navy. To do this, knowledge of the German language was very helpful. But, as I will try to make clear later, knowledge of the language was not as useful as familiarity with mathematics. The great contribution of Major Pokorny, and also of his successors Lieutenant Colonel Karol G. Langer and Captain Maksymilian Ciężki, is that considerably earlier than their counterparts in other cipher bureaus they understood the usefulness of requiring cryptologists to be mathematics graduates as well as to know languages.

Marian Rejewski was born on August 16,1905, in Bydgoszcz, Poland, where he graduated from secondary school in 1923. He studied mathematics at the University of Poznań and after receiving the degree of Master of Philosophy in 1929 he spent a year in Göttingen specializing in the mathematics of insurance underwriting. From September 1930 to September 1932 he was a lecturer at the Institute of Mathematics at the University of Poznań. At the same time he worked at the Poznań branch of the Polish Cipher Bureau (the cipher bureau of the General Staff of the Polish army). He was transferred from that office to Warsaw where the events related in this article took place. After the war, Rejewski returned to Poland. For the next twenty years, until he retired in February 1967, he, worked in Bydgoszcz as a clerk in various firms. He died in Warsaw on February 13, 1980.

Here I will introduce another person, whom I will mention again, who played an absolutely exceptional role in breaking the Enigma cipher: General Gustav Bertrand of the French army, who died in 1976. In 1932 (at the rank of captain), as leader of the French intelligence section D, he procured and delivered to the Polish Cipher Bureau intelligence materials of tremendous significance; after that he repeatedly influenced the fate of the Polish cryptologists in a substantial way and eventually made their decisive role in breaking the Enigma cipher known to the world (Bertrand 1973).

It is not my purpose to describe the commercial or military machine in detail; I will briefly present only what is needed for the understanding of subsequent arguments. The machine (Figure 1) had the size and appearance of a portable typewriter, with 26 keys labeled with the letters of the Latin alphabet, but in place of typebars it had a platform with 26 electric lamps (the kind used in flashlights) labeled with the same letters as the keyboard. A battery provided electric current.

The most important parts of the machine were three rotating coaxial enciphering drums I, II, and III that could be mutually transposed (in Figures 1 and 4 these drums are in the positions denoted by the letters L, *M*, and *N*) as well as a fourth drum known *as reflecting drum R* (immovable in the military machine). A ring with the 26 letters of the alphabet engraved *on* the circumference was fixed to each enciphering drum, as illustrated in Figures 2 and 3. The letter positioned at the top could be seen through a small window located in the metal cover of the machine. The ring could be rotated with respect to the rest of the drum.

The central part of each drum was an ebonite *disk.* Twenty& stationary contacts were positioned concentrically along one side of the ring (visible on the right side of Figure 3) and connected irregularly by insulated wires to the 26 spring contacts located on the other side, also positioned concentrically (visible on the left side of Figure 3). The reflecting drum had 26 spring contacts on one side only; they were interconnected in an irregular fashion.

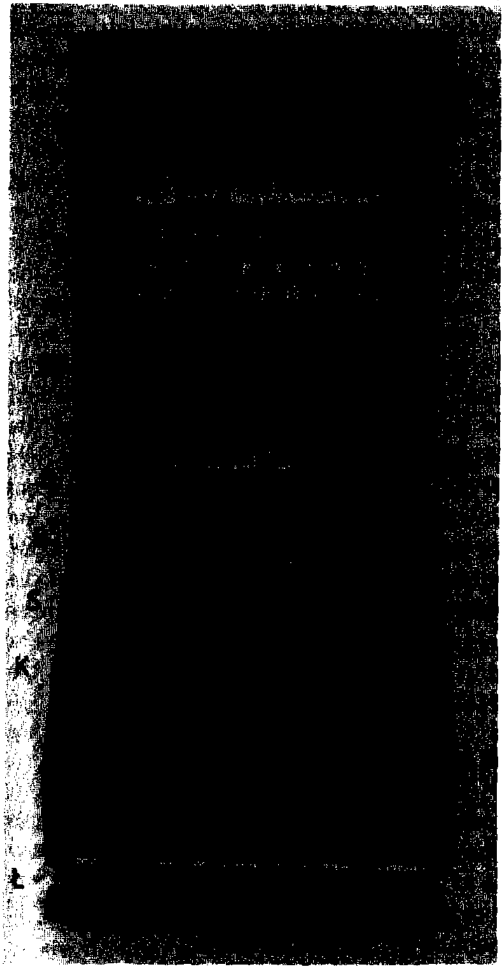


Figure 1. General view of the military Enigma.

W_d Wooden outside cover
W_m Metal lid covering drums and lamps
O_s Windows in the metal lid for viewing the lamps (the letter corresponding to each lamp is on the window)
O_p Windows for viewing letters on movable rings
B Drums (*R, L, M, N, H*)
D Lever fastening drums
S Lamps
K Keyboard
L Plug-type switchboard

When a key is pressed on the machine, enciphering drum N (that is, the drum at the **rightmost** position *N*) turns **1/26th** of the circumference. Current from the depressed key flows through the three enciphering drums, through the reflecting drum, again through the enciphering drums, and lights one of the **lamps** (Figure 4). When key u, for example, is **depressed,** a lamp labeled with another letter lights (differing from the depressed letter; in Figure 4 this is the letter d); at the next depression of the same key u, one **gets—as** a result of the rotations of the drums **performed** in the meantime—a different enciphered letter, **usually** a **different** lamp lights.

In *this* way, when a *series* of letters of **unenciphered** text **(called** plaintext) is keyed, the letters of the successively lighted lamps constitute the ***ciphertext.*** Conversely, when a series of cipher letters is keyed in the same way, the sequence of lighted **lamps generates** plaintext. In other words, under each **arrangement** of the drums, the actual cipher permutation is an involution, equivalent to the product of 13 **transpositions.**

Clearly, the number of enciphering drums with different interconnections is

$$26! = 403{,}291{,}461{,}126{,}605{,}635{,}584{,}000{,}000$$

and the number of different reflecting drums is

$$\frac{26!}{2^{13}\cdot 13!} = 7{,}905{,}853{,}580{,}025$$

Therefore, the **factory** making **these** Enigmas could provide **each** lot of **machines** that a customer ordered with different **drum connections.** This is **particularly** relevant for **the drums** of military **machines,** which obviously must have different **connections from** the drums **of any commercial** machine. **Every set of drums** for military- machines (numbering an estimated 100,000 to 200,000 during wartime) **had** the **same** connections,. so **cryptographers** from **any** military **unit could communicate** with **any** other unit, **as long as their** machines **were** set to the **same** key.

Figure 2. Enciphering drums (see Figures 1 and 4)

The key—the starting position for the drums--was a second secret of the military Enigma apart from the interconnections of the drums. Each enciphering drum can be set 26 different ways; therefore, three drums can be set 269 = 17,576 ways. Since a sequence of three drums on a shaft can again be arranged in six ways, the settings and ordering of the drums together result in 6 · 26^3 = 105,456 possibilities. That number seemed too low to the specialists from the German Cipher Bureau, so they added something in the nature of a telephone switchboard to the military version of the machine. This made it possible to interchange six pairs of letters freely, which created an additional

$$\frac{26!}{2^6 \cdot 6! \cdot 14!} = 100,391,791,500$$

new possibilities. So now the Germans figured that even if the enemy captured an actual military machine, perhaps as a result of military operations, without knowing the key they would be unable to decipher any messages. I will try to demonstrate that- the Germans were mistaken in this view.

The collection of settings imposed on cryptographers—the settings of the drums, their ordering, selected switchboard connections, and certain other settings, which I will not discuss for the time being—was called the daily *key* (although several elements of that key were changed more frequently than every 24 hours, especially during the last phase of the war; others were changed less frequently, particularly during the initial period of the machine's use). Cryptographers received the daily key in the form of a printed table for a period of an entire month.

This is not the last of the secrets of the military Enigma. Enciphering all messages on a given day with the same position of the drums would be tantamount to exposing those messages, *since* the first letters of all messages would then form a letter-for-letter substitution—that is, a very elementary ciphertext, easily solved when having enough materials; the second letters of all messages would determine another substitution, and so on. These are not merely theoretical considerations In France in 1940 we solved a Swiss cipher machine of the *Enigma* type exactly in this way. Because of this, selection of the setting of the drums at which encipherment of a given message began was left to the discretion of the German encipherer, who had to communicate that initial setting to his deciphering colleague so that the latter would know how to *set* the drums in order to read the message. This required sending three letters (the Germans believed they should be enciphered), and because radio did not always ensure good reception, the letters had to be sent twice, enciphered each time; thus six letters were inserted at the beginning of the given message. These three letters, freely chosen by the cryptographer, were called the *message key,* as distinct from the daily key, and they constituted the third secret of the military cipher Enigma.

Message Keys

In the autumn of 1932 I was separated from my colleagues up to that time, Różycki and Zygalski; I was assigned my own cubicle in the building of the General Staff and was instructed to resume the study of the Enigma that had been abandoned by my predecessors.

Today, after the passing of almost half a century, I no longer remember whether at that time I understood the differences in the structure of the military and commercial Enigmas. It is likely that I received this information somewhat later, but in any case it was not useful to me in the initial stage of my work. The

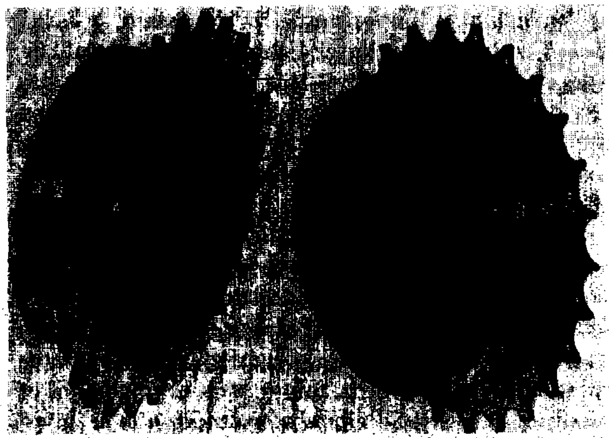


Figure 3. Two sides of an enciphering drum.

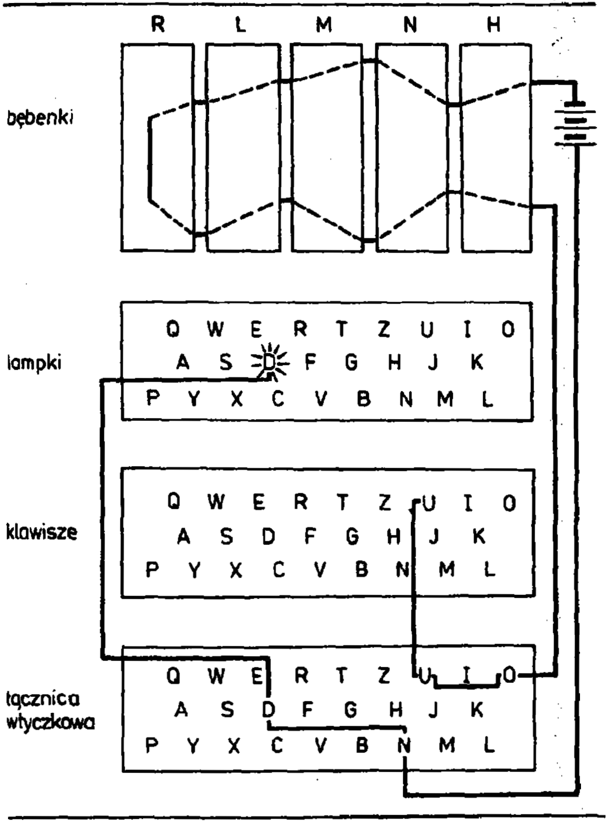


Figure 4. Diagram of the flow of current in the military Enigma.
bębenki = drums
lampki = lamps
klawisze = keyboard
łącznica wtyczkowa = plugboard

commercial machine we had purchased, as well as dozens of messages enciphered each day on the military Enigma, was placed at my disposal.

The fact that the first six letters of each message formed its three-letter key, twice enciphered, was obvious, and I will not dwell on the matter. But what else could be done? I will show how I proceeded at that time, and then I will try to justify my procedure.

I wrote down separately the first six letters of all messages from a given day—that is, their keys twice enciphered. Every key that had the same first letter also obviously had the same fourth letter. The same can be said about the second and fifth and the third and sixth.

I selected a key arbitrarily and wrote its first and fourth letters side by side. Then I looked for a key having the fourth letter of the previous key as its first letter. I wrote the fourth letter of this key beside the fourth letter of the previous key. Proceeding in this way, after a certain number of steps I encountered the first letter that I had written. The second time I did not copy this repeated letter, but enclosed the letters I had already written in parentheses. An example will illustrate my procedure more clearly. Let

dmq vbn

puy

puc fmq

be three somewhat artificially chosen enciphered keys of messages on a given day. For greater clarity I divided each key in half so that the first three letters were the key under the first encipherment and the next three letters were the second encipherment. Then I took the letter *d* from the first message and wrote the fourth, *v*, beside it. Next to it I wrote the fourth letter of the message starting with *v* (that is, *p)* and the fourth letter of the message starting with *p*. I got

dvpf

From the keys of subsequent messages it would turn out that a whole cycle of letters would emerge

dvpfkxgzyo

From the remaining keys other cycles would emerge. In this way the aggregate of cycles formed from the first and fourth letters could be seen as in the following example:

$$AD = (dvpfkxgzyo)(eijmunqlht)(bc)(rw)(a)(s)$$

I labeled the aggregate of cycles AD to signify that it arose from the first and fourth letters of the message keys of the given day. I proceeded in a similar way with the second and fifth as well as the third and sixth letters of the keys and came up with a representation like the following:

$$\begin{aligned} AD &= (dvpfkxgzyo)(eijmunglht)(bc)(rw)(a)(s)\\ BE &= (blfqveoum)(hjpswizrn)(axt)(cgy)(d)(k)\\ CF &= (abviktjgfcqny)(duzrehlxwpsmo) \end{aligned} \qquad (1)$$

This structure is most characteristic, and although the representation of such a structure was different each day, one trait was always the same: in each line the cycles of the same length always appeared in pairs. In view of the role this structure played, I named it the *characteristic structure*, or simply the *characteristic* of a given day.

How can one explain the origin of the characteristic structure? If I were to press each key in succession in such a way that the position of the enciphering drums did not change—by keeping one key depressed, for example—then different lamps would light continually. In this way a certain permutation of the letters would appear. Under a different setting of the drums, the permutation would clearly be different, but the reflecting drum would cause all permutations to be composed exclusively of the transpositions. For example, if striking key t would cause lamp *z* to light, then striking key *z* under the same setting of the drums would cause lamp *t* to light. (In the introduction I mentioned that plaintext yields ciphertext, and ciphertext yields plaintext.)

One can easily verify that if the six successive permutations arising from enciphering the message keys twice are denoted by the letters A to F, the products of the permutations AD, BE, and *CF* will be identical to the expressions constituting the characteristic of the given day, thereby justifying this notation.

Yes, but why in these expressions do cycles of the same length always appear in pairs? That also can be explained easily by proving the following theorem:

> If two permutations X and Y of the same degree consist exclusively of *disjoint* transpositions, then the number of disjoint cycles of the same length in the product XY is even.

One can also prove the following converse theorem:

> If in some permutation (of an even degree) different cycles of the *same* length appear *in* pairs, that *permutation* can be considered *as* the product XY of *two permutations* X and Y, each of them being *formed* by disjoint *transpositions* only.

A simple proof of these theorems is lengthy and will not be given. The following also can be shown:

1. Letters belonging to one and the *same transposition of permutation* X or Y always belong to *two* different cycles of the *same permutation* XY.
2. If two letters in two different cycles of the same *length of permutation XY belong to the same* transposition, their neighboring letters (one on *the right, the other on the left) also belong to* the *same* transposition.

An appropriate interpretation of these facts implies that it is sufficientto know the practices of cryptographers in order to reconstruct all message keys completely. As an example, cryptographers are inclined to choose three identical letters such as aaa, bbb, and the like as message keys. Let us examine the characteristic shown earlier (Equation 1). Because the letters a and s form one-letter cycles in the product AD, if the key *aaa* is to be found among the message keys, the encipherment of the first letter has to be *s*. Suppose that among the enciphered message keys of a given day there were three keys beginning with the letter s

sug smf

sjm spo

syx scw

The enciphered key *sug* snf could not come from the letters *aaa*, since the second letter *u* is found in the nine-letter cycle of the product BE, while a is found in the three-letter cycle of the same product. Similarly, the enciphered key sjm spo could not come from the letters *aaa*, since the letter j is also found in the nine-letter cycle. The enciphered key *syx scw* could result from the letters aaa, however, since *s* and a are found in two one-letter cycles of product AD, y and a belong to two different three-letter cycles of product BE, while *x* and a belong to two different thirteen-letter cycles of product CF.

The fact that the enciphered key *syx scw* really denotes the letters *aaa* under encipherment was confirmed by the fact that with this very assumption a great many other enciphered keys could be deciphered as sequences bbb and *ccc*.

Thus, one of the mysteries of the Enigma cipher, the secret of the message key, was solved. It is interesting that knowledge of neither the positions of the drums nor the daily keys—in other words, none of the remaining secrets of the Enigma cipher—was needed to attain this result. A sufficient number of messages from the same day were needed, around 60 specimens, for the characteristic structure AD, BE, *CF* to be established.

Besides this, a good knowledge of the practice of cryptographers regarding the selection of a message key was necessary. When I first assumed that,there would be many keys of the sort *aaa*, *bbb*, etc., it was only a hypothesis that luckily turned out to be true. The changing tastes of cryptographers were very carefully followed, and other predilections were uncovered. For example, when the use of three identical letters was forbiddeh, the cryptographers started avoiding even double repetitions of a given letter. That trait also was enough to determine what the message keys-were before encipherment.

These and several similar methods were developed. It is well known that 'a human being gifted with consciousness and memory does not have the ability to imitate chance in a faultless manner. Among other things, it is the task of a cryptologist to uncover and suitably make use of these deviations from chance.

Interconnections of the Drums

It would have been better for the Germans if the message keys had not been enciphered at all because encipherment, as we have seen, not only did not guard against exposure but in addition supplied a bonus in the form of six successive permutations, A to F. As I will demonstrate, knowing them brought me closer to finding the drum connections of the military Enigma. First, I must describe what goes on inside the machine in terms of operations on permutations. I denoted by the letter S the permutation produced by the switchboard, by the letters L, M, and N permutations from the three enciphering drums, labeling them from left to right, and by the letter R permutations from the reflecting drum. Another drum should be mentioned: the initial drum, which was stationary and constituted a transition from the switchboard to drum N; I denoted this drum by the letter H. The path of the current could then be expressed in the following way:

$$SHNMLRL^{-1}M^{-1}H^{-1}S^{-1}$$

Because drum N rotated by 1/26th of its circumference with each stroke of a key, I had to introduce still another special permutation that would take this rotation into account. This permutation, which I will always denote by the letter P, changed each letter into the next letter in the alphabet: a to b, b to c, . . . , z to a. Permutations A through F could now be represented in terms of the following equations:

$$A = SHPNP^{-1}MLRL^{-1}M^{-1}PN^{-1}P^{-1}H^{-1}S^{-1}$$
$$B = SHP^2NP^{-2}MLRL^{-1}M^{-1}P^2N^{-1}P^{-2}H^{-1}S^{-1}$$
$$\cdot$$
$$\cdot$$
$$\cdot$$
$$F = SHP^6NP^{-6}MLRL^{-1}M^{-1}P^6N^{-1}P^{-6}H^{-1}S^{-1}$$

In writing these equations, I assumed that only the drum on the right, N, revolved, while drums L and M did not turn at all during the six successive keystrokes. This assumption is correct in 21 out of 26 cases on the average, which is sufficient to justify it. In such a case the expression $MLRL^{-1}M^{-1}$ is repeated in all 'the preceding equations and can be replaced temporarily by the letter Q, which denotes a fictitious reflecting drum.

$$Q = MLRL^{-1}M^{-1} \qquad (2)$$

This allows our set of equations to be simplified significantly.

$$A = SHPNP^{-1}QPN^{-1}P^{-1}H^{-1}S^{-1}$$
$$B = SHP^2NP^{-2}QP^2N^{-1}P^{-2}H^{-1}S^{-1}$$
$$\cdot$$
$$\cdot$$
$$\cdot$$
$$F = SHP^6NP^{-6}QP^6N^{-1}P^{-6}H^{-1}S^{-1} \qquad (3)$$

The actual problem lay in solving the above set of six equations with four unknown permutations S, H, N, and Q. Realizing the difficulty of the problem, I first tried to reduce the number of unknowns. Since in the commercial machine the connections of the initial drum had the form

$$H = \begin{pmatrix} qwertzuioasdfghjkpyxcvbnml \\ abcdefghijklmnopqrstuvwxyz \end{pmatrix}$$

(where the upper line of the permutation H represents the alphabet as given on the machine's keyboard), I originally assumed that permutation H had the same form on the military machine, because on both the commercial and military machines the letters were in the same order on the keyboard. I finally realized that this hypothesis was incorrect and had led to much needless work and considerable loss of time—so much that the study of the Enigma was almost discontinued once again. Thus, an unusual event had taken place here: the Cipher Bureau's purchase of a commercial machine with the intention of simplifying the breaking of the military Enigma cipher actually greatly impeded the task.

For the time being, however, I assumed that permutation H was known. So I had a set of six equations in three unknowns S, N, and Q. While I puzzled over how to solve that set of equations, on December 9, 1932, completely unexpectedly and at the most opportune moment, a photocopy of two tables of daily keys for September and October 1932 was delivered to me.

Now the situation changed radically. Since the table of keys also included a daily change in the connections of the switchboard, I could consider permutation S as given and transfer it, in the same way as the known permutation H, to the left side of the set of equations, which would take on the following form:

$$H^{-1}S^{-1}ASH = PNP^{-1}QPN^{-1}P^{-1}$$
$$H^{-1}S^{-1}BSH = P^2NP^{-2}QP^2N^{-1}P^{-2}$$
$$\vdots$$
$$H^{-1}S^{-1}FSH = P^6NP^{-6}QP^6N^{-1}P^{-6}$$

In this set of equations, all permutations on the left side are completely known, and on the right side only permutations N and Q are unknown. We again transform both sides of the first equation by the internal automorphism determined by P, the second equation by P^2, etc., and to be concise we denote the left sides by the letters U through Z.

$$U = P^{-1}H^{-1}S^{-1}ASHP = NP^{-1}QPN^{-1}$$
$$V = P^{-2}H^{-1}S^{-1}BSHP^2 = NP^{-2}QP^2N^{-1}$$
$$\vdots$$
$$Z = P^{-6}H^{-1}S^{-1}FSHP^6 = NP^{-6}QP^6N^{-1}$$

In addition, we will form new products by multiplying consecutive pairs of these equations.

$$UV = NP^{-1}(QP^{-1}QP)PN^{-1}$$
$$VW = NP^{-2}(QP^{-1}QP)P^2N^{-1}$$
$$\vdots$$
$$YZ = NP^{-5}(QP^{-1}QP)P^5N^{-1}$$

from which, by eliminating the common expression $QP^{-1}QP$, we get the set of four equations with only the single unknown NPN^{-1}.

$$VW = NP^{-1}N^{-1}(UV)NPN^{-1}$$
$$WX = NP^{-1}N^{-1}(VW)NPN^{-1}$$
$$XY = NP^{-1}N^{-1}(WX)NPN^{-1}$$
$$YZ = NP^{-1}N^{-1}(XY)NPN^{-1}$$

We see that the expression VW is transformed from the expression W by the use of permutation NPN^{-1}. Writing VW under W in all possible ways—and there are dozens of such ways—we get dozens of possible solutions for the expression NPN^{-1}. Similarly, WX is transformed from VW by using the same expression NPN^{-1}. Therefore, writing WX under VW we again get dozens of possible solutions for the expression NPN^{-1}. One of these solutions has to be identical to one of those previously obtained. That one is our desired NPN^{-1}. The last two equations in XY and YZ are already superfluous.

The rest is straightforward. It is sufficient to write the known permutation P in all 26 possible ways below the expression that was obtained for NPN^{-1} in order to obtain 26 variants for connections of drum N. Which of these variants we choose does not have great significance for the time being, since the choice of one or the other variants denotes only a greater or lesser rotation of the fixed-contact side relative to the spring-contact side in drum N. The final determination of the actual rotation can take place only later.

This is how the problem looked in theory, In practice, alas, it was different. From the above formulas it appears that the products W, VW, WX, XY, YZ all ought to be similar to each other. But that was not the case, and consequently it also was impossible to write those products beneath one another. And even though I carried out the same operation repeatedly on the material from different days, because I suspected that a shift of the middle drum occurred, the result was always negative. Carrying out the tests took a great deal of time, and the discontinuation of work on the Enigma was deliberated again, when I finally realized that the reason for my bad luck might be only an incorrect assumption regarding the connections of the initial drum.

A *small* digression here. I have every reason to believe the British cryptologists did not manage to solve the problem because of the difficulty caused by the connections of the initial drum. First, in July 1939, when representatives of Polish, French, and British cipher bureaus attended a meeting in Poland, the first question put forth by the British cryptologist Alfred Dillwyn Knox was: "What are the connections of the initial drum?' Second, Penelope Fitzgerald, Knox's niece, in her book, The *Knox* Brothers (1978), stated that Knox was furious when he realized how simple it Was.

What, then, were the connections of the initial drum? It turned out later that it was possible to find them using a deductive approach, but in December 1932, or perhaps *early* in 1933, I came up with the settings by guessing. I assumed that since the keys were riot-connected with successive contacts of the initial drum in the order of letters on the keyboard, very likely they were connected in alphabetical order;

that is, the permutation created by the initial drum was the identity, and it was possible to disregard it altogether. This time I was in luck. The hypothesis turned out to be correct, and the first test gave a positive result. As if under a magic spell, numbers denoting the settings of the drum N began flowing from my pencil. So that is how the settings of one drum, the right-hand one, at last became known.

How were the connections of the remaining drums found? Recall that I received a photocopy of daily keys for a period of two months, September and October 1932. At this time a change in the order of the drums on the shaft occurred every quarter. Because September and October belong to two different quarters they had different orderings of the drums, with different drums located on the right-hand side. Therefore, during both quarters I was able to employ exactly the same method for findingtheir connections. Finding the connections of the third drum and, in particular, the reflecting drum, did not present great difficulties by then. Likewise, there was no difficulty with the determination of either the exact rotation of the aides of the drums relative to each other or the moments when a revolution of the left-hand and center drums occurred.

In principle, the work required for settling these particulars consisted of attempts to decipher parts of several messages from this period and incorporating such corrections in the drum settings so that completely error-free segments would be obtained. Some simplification of this work was due to the German instructions for using the Enigma machine that were delivered together with the monthly tables of daily keys, In the instructions the plaintext of a certain message and its actual encipherment under a specified daily key and message key were provided as an example. In later editions of the same instructions, the example that was provided was always fictitious.

Because, as I have already stated, it turned out that the connections of the initial drum could be found by deduction and not just by guessing, the obvious next question was whether one could not also solve the set of equations (Equation 3) and in this way obtain the connections of the drums by a deductive approach, *without using intelligence material. To this day it* is not known whether Equation 3 is solvable. Admittedly, another approach to the reconstruction of the drum connections has been found, in theory at any rate. But that approach is imperfect and laborious. Even a superficial description would result in further lengthening of this article, so I will mention only that it requires the possession of messages from two days of identical or very similar connections of the drums; therefore, finding the connections of the drums would depend on luck. In addition, it requires so many tests 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.

Therefore, the conclusion is that procurement of intelligence material was the decisive factor in breaking the machine's secrets. Many y e . later I found that the source of the material was the already mentioned Captain Bertrand.

The Dally Keys

As soon as the connections of the drums became known, the search began for ways to discover the third and final secret of the *Enigma,* the daily keys. Earlier, a commercial machine was suitably remade m the technical section of the Cipher Bureau. I was told (probably at the beginning of January 1933) to let my two colleagues Henryk Zygalski and Jerzy Różycki in on the secret so they could read cipher material from the two months of September and October 1932 by making use of the daily keys that were delivered by French intelligence. I, however, had to remain in isolation until the conclusion of the assignment.

That the conclusion was not at all easy and could not be easy follows from the Germans' conviction that the cipher, even with the machine in hand, could not be broken without knowing the daily keys. I focused my attention on the fact that permutation S changed only six pairs of letters and thus fourteen letters remained unchanged.

Let us again examine the parts of Equation 3. We already know that permutation *His* the identity, so it can be omitted. For the time being we will assume that permutation *S* also is an identity. If we now transfer all permutations with the exception of the unknown permutation Q to the left-hand side, we obtain the following set of equations:

$$
\begin{aligned}
PN^{-1}P^{-1}APNP^{-1} &= Q \\
P^2N^{-1}P^{-2}BP^2NP^{-2} &= Q \\
&\vdots \\
P^6N^{-1}P^{-6}FP^6NP^{-6} &= Q
\end{aligned}
$$

The connections of drum *N* are indeed known; however, its setting is not known.

To take this into account, it is more *correct* to write

$$\begin{aligned}
P^{x}N^{-1}P^{-x}AP^{x}NP^{-x} &= Q\\
P^{x+1}N^{-1}P^{-x-1}BP^{x+1}NP^{-x-1} &= Q\\
&\cdot\\
&\cdot\\
&\cdot\\
P^{x+5}N^{-1}P^{-x-5}FP^{x+5}NP^{-x-5} &= Q
\end{aligned}$$

If permutation S actually were the identity, then by substituting the numbers 1 through 26 in succession for the variable x and after each substitution evaluating the left-hand side of the above set of equations, for a particular value of x we would obtain the same value for all expressions Q and in this way we would find the setting of drum N. Permutation S does exist, however, so for no x will the expressions Q be equal to each other, but among them there will be a certain similarity for a particular value of x, since permutation S does not change all of the letters. But carrying out the work described would be too laborious. I searched for a more practical method. I found it in the form I called the grid *method.*

For each of the three drums, the 31 permutations N, PNP^{-1}, P^2NP^{-2}, . . ., $P^{25}NP^{-25}$, N, PNP^{-1}, . . ., P^4NP^{-4} and the connections of the three drums are entered once and for all on a suitably sized sheet of paper in the following way:

N	*kjpzydtiohxcsgubrnwfmveqla*
PNP^{-1}	*ioyxcshngwbrftaqmveludpkzj*
P^2NP^{-2}	*nxwbrgmfvaqeszpludktcojyih*
.	
.	
.	
P^4NP^{-4}	*uzpekdtyocqxnjsbiramhwgflv*

On another chart with six slits, which I called *the grid*, the previously determined permutations A through F are entered in the following way:

$$A \quad \begin{pmatrix} abcdefghijklmnopqrstuvwxyz \\ srwivhnfdolkygjtxbapzecqmu \end{pmatrix}$$

$$\mathrm{F} \quad \begin{pmatrix} abcdefghijklmnopqrstuvwxyz \\ wxofkduihzevqscymtnrglabpj \end{pmatrix}$$

Next, the grid is moved along the paper on which the drum connections are written until it hits on a position where some similarities show up among the several expressions Q. In this position the upper and lower letters of each permutation A through F ought to be displaced so that all permutations Q become the same. In this way the setting of drum N and the changes resulting from permutation S are found simultaneously. This process requires considerable concentration since the similarities I mentioned do not always manifest themselves distinctly and can be very easily overlooked.

The task is still incomplete, for the unknown Q remains. Recall that Q is only an abbreviation (Equation 2) denoting a fictitious reflecting drum. At this point the connections of drums M, L, and R are already known. The positions of drums M and L are still not known; only drum R is stationary. Thus, it would be better to write

$$Q = P^{y}MP^{-y}P^{-z}LP^{-z}RP^{z}L^{-1p-z}P^{y}MP^{-y} \qquad (4)$$

where the variables y and z, analogous to the aforementioned variable x, can take on all values from 1 to 26. At the time (the beginning of 1933) the only means I could use to find y and z consisted of simply going through all possible $26^2 = 676$ positions of the drums M and L every day on the machine until I found their true positions. The work was quite tiresome, rather mechanical, but still not the end.

One must recall mother detail about the construction of the Enigma, which I pointed out earlier while describing the machine. On the circumferences of the enciphering drums L, M, and N movable rings were engraved with the letters of the alphabet. The *way* these rings had to be adjusted each day was delivered to the cryptographer along with the other components of the daily keys. Thus the setting of the rings was still to be found.

From the messages of September and October 1932 that were deciphered in the interim, it was learned that in principle all messages (of course, not taking into account succeeding parts of messages consisting of two or more parts) began with the letters *ANX*, from the word an (German for "to") and the spacer X. It was necessary to select an appropriate message beginning, for instance, with the letters *tuv*, and while continually striking key *t*, both turn the drums and simultaneously notice when lamp A lighted. Then it was necessary to strike key u and, if by chance lamp N lighted, also strike key v. If lamp X lighted, there was a high probability that we had found a good case; it was then necessary to adjust the rings accordingly. If not, it was necessary to search to the bitter end.

This method was very primitive and much more tiresome than that for finding the positions of drums L and M, since even in the most unfavorable case one had to go through all possible positions of the drums—$26^3 = 17{,}576$ of them. The method was nevertheless effective.

Thus, the results of the work accomplished during the course of merely a few months can be summarized as follows:

1. Reconstruction of the German military cipher machine Enigma.
2. Finding a method for the daily reconstruction of the message keys.
3. Finding a method for reconstructing the daily keys.

A Period of Relative Peace (1933–1935)

The first decision my superiors made when I informed them of my results was to issue an order to the AVA factory, which was under the control of the Cipher Bureau, to build a series of copies of the German military Enigma patterned after the commercial model. They were to use the drum connections I provided and take into account other differences in the construction of the two types of machines, first of all by adding a switchboard. Next, five or six young people were employed and assigned to a separate room with the exclusive task of deciphering the stream of messages for which daily keys soon began being delivered. Finally it was arranged for my two colleagues, Zygalski and Różycki, to work with me again, permanently from then on.

Now there were three of us instead of one. Using the methods that have been described, day after day we recovered the daily keys to be delivered to the decipherers. Since the Germans introduced no significant changes in the Enigma cipher in the three years until the end of 1935, we were able to devote some time to improving our methods of decryption. . ,

For example, for the six possible combinations of drums--I II, I III, II I, II III, III I, and 111 11—we created a catalog of all possible permutations Q according to Equation 4. It encompassed a total of $6 \cdot 26^2 = 4056$ positions. When it was ready, if we had already found the setting of drum N using the grid method, all we needed to do was look in the catalog for the simultaneously obtained permutation Q and in a moment we would already have the settings of drums L and M.

We made another improvement. When we turned the drums on the machine successively to all possible $26^3 = 17{,}576$ positions in order to find the settings of the rings using the ANX method, we soon noticed that if some part of the message was to begin with ANX, several positions of drum N would be impossible and should no longer be considered. Since there were a dozen or so messages every day in which one could expect to find the letters ANX at the beginning, it was usually possible to reject, purely by calculation, all impossible positions of drum N, leaving just one or two to consider. (I no longer remember which calculations had to be performed and on which theoretical principles they were based.)

During this period Różycki worked out a procedure he called the *clock method.* In a great many cases it allowed us to determine which of the three drums I, II, or III was drum N on a given day; that is, which drum was on the right-hand side of the machine. True, the order of the drums changed only once each quarter until the end of 1935, and thus the determination of the drum N was not yet too important. But starting on February 1, 1936, the change in the order of the drums occurred every month and starting on November 1,1936, every day. What was this method?

If we write two texts in German, one beneath the other, letter by letter—for example,

```
W E M G O T T W I L L R E C H T E G U N S T E R W E
U E B I M M E R T R E U U N D R E D L I C H K E I
```

then on the average two columns with identical letters can be found within a span of 26 letters. This feature will also be observed when we encipher both texts using the same key. If we encipher each text using a different key of the cipher machine, however, on the average only one column with identical letters will be found within a span of 26 letters. The reason for this phenomenon clearly lies in the unequal frequency of letters in German (and in other languages, too). In a span of 26 letters this phenomenon does not occur in a noticeable way. If, however, we have two messages, each 260 letters long, say, with this method we generally can decide whether the two messages were enciphered using the same key or different keys. We make use of this possibility in the following way. ,

Having a sufficient quantity of enciphered material at our disposal, we usually find a dozen or so pairs of messages such that in each pair the first two letters of their keys are identical, while the third letters are different. Now we write both messages of one pair one beneath the other so that letters enciphered by the same drum settings are directly beneath each other. There are two possible ways of writing one message beneath the other, depending on at which position of drum N the shift of the middle drum M occurs. These positions are known and are different for each of the three drums. For example, if drum I is located in the

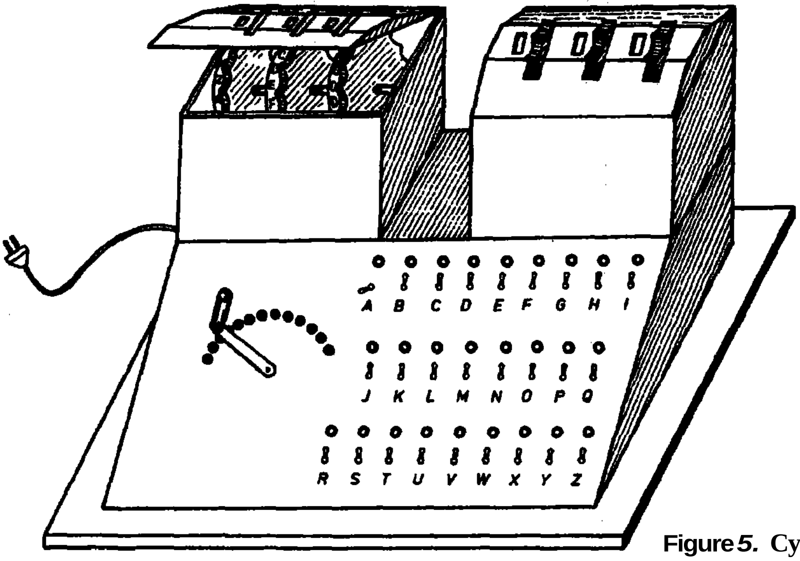


Figure 5. Cyclometer.

N place, the shift of drum M occurs when drum N shifts from letter Q to R in the window. If drum II is located in the *N* place, the shift occurs during the change from letter E to *F*, and if drum III is drum N, the shift occurs during the change from V to *W*. For each of the two possible ways of writing the messages beneath each other, it is sufficient to count the number of columns with identical letters in order to determine which way of writing the messages is correct and therefore to determine which of the three drums is located on the right-hand side.

Różycki's clock method, which simplified our work in a great many instances, also had an interesting property: of all the methods we discovered, it was the only one based on characteristics of the language—on the actual frequency of letters in the German language. As I have mentioned, in general the introduction of cipher machines influenced the change in the character of a cryptologist's work from linguistic to mathematical investigation.

The Period of Extensive Changes (1936 to August 1938)

The growing German military power brought about an expansion of the sphere of users of the Enigma machine. On August 1, 1935, the German air force had formed its own radio communication network with its own daily keys, but clearly employing the same Enigma. Gradually other military and paramilitary units joined in, and because they were also forming separate networks we had to recover more and more daily keys. I have already mentioned the ever more frequent changes of the order of the drums. But beginning on October 1, 1936, the number of modified pairs of letters on the switchboard was changed from six to anywhere from five to eight, which complicated the use of the grid method. So we searched for another method.

Our attention returned to the characteristics that had a rarely repeated form and for that reason labeled a given day to a certain degree. From the pattern

$$AD = SPNP^{-1}QPN^{-1}P^{3}NP^{4}QP^{4}N^{-1}P^{-4}S^{-1}$$

and the two analogous forms for BE and CF, it follows that permutation S as a transformation influences not the length of the cycles in the characteristic but only the letters in the cycles. So if we managed to invent a device that would produce the length of the cycles for each of the expressions of the type AD (again, these expressions are not numerous, since for each of the six possible sequences of the drums there are only 26^3 = 17,576 expressions), we would be able to make a chart of cycle lengths for expressions of the type AD and determine the drum setting by comparing the cycle lengths with the characteristic of a given day. We actually succeeded in inventing such a device, and it is unusually simple (Figure 5); we named it the cyclometer. It was produced by the AVA factory, the same factory that earlier had built copies of the military Enigma.

In essence the cyclometer consisted of two sets of drums (with drum *N* of the second set displaced by three letters in relation to drum *N* of the first set), an ebonite panel on which 26 flashlight lamps with switches were mounted, and a power source. When the flip of a switch at one of the lamps turned the current on, then not just the given lamp but all lamps belonging to the same cycle and to the other cycle of the same pair lighted. It remained to write the position of the drums and the number of lighted lamps on a card and to arrange these cards in a certain way—by cycle length, for example.

The work lasted a long time, over a year, since we worked on it along with our normal job of recovering daily keys with the aid of the grid. When all six card files were prepared, finding the daily key was an ordinary matter that took a mere 10 or 15 minutes. The drum positions were read off the card, the order of the drums was read from the box from which the card was retrieved, and permutation S was obtained by comparing the letters in the cycles of the characteristic with the letters in the cycles of permutations *AD*, *BE*, *CF*, which were found by typing them on the machine.

Unfortunately,on November 2,1937, when the card files were ready, the Germans changed the reflecting drum that had been used up to that time (which they denoted by A) to a different drum B. We had to redo all the work, starting with the reconstruction of the connections of drum B.

In September 1937, and thus several weeks before the change of the reflecting drum, a new network appeared on the air. We soon learned it was the network of the party security staff, the so-called *Sicherheitsdienst* (SD). I would like to devote a few words to the role our reading of this network played in the work on the Enigma several months later.

The method of encipherment by the SD did not differ in principle from the method used in other networks. When, for the first time, one day's characteristic from that network was formed, it was found in our files with no difficulty. Consequently, the order and positions of the drums as well as permutation S were determined, but when method ANX was tried in order to establish the settings of the rings, difficulties were encountered. Obviously none of the messages considered started with *ANX*. So we selected a fragment from the middle of one of the messages and began to type it on the machine under all possible drum settings in the hope of recovering a fragment of the content. We had good luck and recovered the letters *ein* after a relatively short time. It could have been a fragment of the content or it also could have been a completely accidental occurrence of just those letters. When the entire message was typed in at those drum positions we did not find any other fragment in German.

After a more thorough analysis of this apparently senseless series of letters, we could make out definite repetitions of letters; these repetitions formed four-letter groups, and the space between them was a multiple of four; in other words, it was possible to divide the entire message (leaving out the word *ein*) into four-letter code groups. Thus we were faced with so-called double encoding. First, the sender of the message, undoubtedly an officer, encoded the text of the message using a codebook of four-letter code groups and wrote the word *ein* only because he did not find it in the codebook. Only then did he turn the prepared message over to cryptographers for further encipherment by machine.

Thanks to such a slip—mixing plaintext with code—and also to a bit of luck, it became possible to recover the entire daily key as well as the ring settings. Luckily the code also turned out to be easy to solve, although clearly one can never recover a codebook 100% in such instances, since not all code groups appear in the messages.

Early in 1938, the head of our intelligence department, Colonel Stefan Mayer, ordered that statistics be gathered for a period of two weeks to measure the quantity of deciphered material against all Enigma-enciphered material picked up by the radiotelegraphers. It turned out that there was a 75%success rate. Peter Calvocoressi, former employee of the British Cipher Bureau, in a talk broadcast on British radio on January 18,1977, stated that no one else on earth had attained such result. Obviously, he was thinking of later times since in 1938 no one except the Poles had read a single message enciphered on the German military Enigma. Moreover, the 75%of messages that had been deciphered did not define the limits of our capabilities. With a slight increasein personnel we could havedeciphered90% of the messages. (A certain quantity of enciphered material, because of faulty transmission, faulty reception, or various other reasons, always remains unread.),

The Greatest Changes (September 1938 to September 1939)

As of September 15, 1938, the Germans, changing nothing in the machine itself and adding nothing to it, changed the way of sending the message keys. From this date on, the cryptographer was required to choose three arbitrary letters to be placed at the head of the message without being enciphered. He then set the drums to these letters, chose three other letters as a message key, and, as before, after enciphering them twice, placed them at the beginning of the message. Then he set the drums to the message key and began the actual encipherment of the message itself.

The changes in the transmission of the message key were implemented in all military units but were not carried out in the SD network. All we had produced up to that time for the recovery of daily keys and message keys—the card files and grid method-came to naught with regard to the military units, because there were no more characteristics. We could solve and read only the SD network.

In a very short time, perhaps a week or two, we came up with two ideas—or rather, since this is more important, we found ways to carry them out. I will attempt to summarize the ideas and their execution.

With the earlier method of transmitting the key, we presented the key in the form of two three-letter groups. Now we had to present it as three groups—for example,

SHP, CHV PZT

The first group, separated by a comma from the rest, is not enciphered, and the other two groups make up the message key enciphered two times. With enough cipher material it can happen that on a given day three messages will be found with keys as in the following example:

RTJ, WAH WIK
HPN, RAW KTW
DQY, *DWJ MWR*

where the first and fourth, the second and fifth, or the third and sixth letters in the keys of all three messages are the same. In this case it is the letter W, but it could also be any other letter, just so it is the same in all three messages. Let us assume for the time being that permutation S was the identity. If the ring setting was also identical and if we knew the order of the drums on the shaft, it would be sufficient to set the drums at position *RTJ*; then by striking key W three times in a row, the same lamp would light. The same would happen in drum positions *HPN* and *DQY*. The setting of the rings makes the positions of the drums at which this would happen unknown to us, but the differences in the positions will be maintained and thus are known.

One need only construct a device that in principle would consist of sets of drums from six Enigmas and that, preserving the known mutual differences in the positions of the drums, would turn the drums synchronously. After passing through all possible 26^3 = 17,576 positions in a specified time (about two hours), the machine would indicate when three pairs of lamp (the same lamp in each pair) lighted.

The order of the drums is unknown, so it would be better to build six such devices from the start, one for each possible ordering. But we must deal with permutation S. During this period, permutation S consisted of five to eight transpositions; that is, it changed half the letters on the average. One could therefore expect that a letter that is repeated six times in three messages (the letter W in this case) would not be changed by permutation S at least every second time.

I have just presented the operating principle. The AVA factory built six such devices in an unbelievably short time—it was only November 1938. For lack of a better name we called them bombs. Our success was thanks to the exceptional service of the factory's director, Antoni Palluth, who was not a regular employee of the Cipher Bureau, but worked closely with it. Beii a cryptologist himself, he understood the needs of the bureau very welt

The second idea, which originated at practically the same time as the idea of the bomb, was based on apparently *similar*, but actually completely different assumptions. As with the bomb, we also had to possess enough suitable cipher material. Out of this material we could expect about ten messages with keys such as

KTL, *WOC DRC*
SVW, DKR IKC
BWK, *TCL TSD*
EDV, *PRS ZRT*
GRN, *UST* UQA

GRA, FDR *YDP*
MDO, CTW YZW
AGH, *SLM PZM*
JBR, *LPS* TOS
ITY, APO ZPD

In these keys either the first and fourth, the second and fifth, or the third and sixth letters are the same, but the identical pairs could be different in each key. If we recall the characteristic shown in Equation 1, we should also remember that the identical letters in corresponding place8 in the key represent one-letter cycles in the characteristic. But permutation *S* does not, after all, influence the length of cycles in the characteristic and therefore does not influence the fact of the occurrence or nonoccurrence of cycles one letter long.

Thus, in place of the card file of cycle lengths in all products of the type *AD*, we had to produce a card file of the positions of all those products of the type AD in which 'one-letter cycles occurred and then compare them with the one-letter cycles occurring in message keys for a given day. But how could the comparison be carried out? In this process, as in the previous one, only the relative distances of one-letter cycles discovered in the message keys of a given day are known It was here that Zygalski pointed out a way to carry out the comparison.

For each of the 26 possible positions of drum L, a square partitioned into 51 x 51 smaller squares is drawn on a large sheet of paper (about 60 × 60 cm). The square is labeled with the consecutive letters of the alphabet: the letters *A* through Z followed by A through Y are written along the sides, on the top, and on the bottom of each square. This was, as it were, a coordinate system in which the abscissa and ordinate denoted consecutive possible positions of drums *M* and *N*, and each small square denoted a permutation with or without one-letter cycles corresponding to that position. Squares with one-letter *cycles* were perforated.

The work was vast, all the more because the instances with one-letter cycles had to be perforated four times. When these sheets of paper were placed on top of each other according to a precisely defined program, in proper order and properly displaced with respect to each other, the number of perforations showing through gradually decreased. If an adequate number of keys with one-letter cycles were at hand, at the end one perforation remained showing through all the sheets of paper, most likely corresponding to a good case.

The order of the drums was derived from the identity of the set to which the sheets of paper belonged. From the position of the perforation and the letter on the paper, we could compute the settings of the rings, and by comparing the letters of the keys with the letters in the machine, we could obtain permutation *S*—that is, the entire daily key. Still, as I mentioned, the work was vast, since we had to cut out about a thousand perforations in each sheet of paper, each complete set contained 26 sheets, and six sets had to be made. We carried out this work in addition to our normal activities; that is why we managed to produce only two complete sets by December 15,1938.

Meanwhile, the Germans instituted new changes in the Enigma cipher by adding two more drums, IV and V, to the three original drums in the machines used by all units, including the SD. There were still only three drums on the shaft, but now the three were to be chosen from a set of five; instead of six possible orderings there were sixty. Besides the tenfold increase in the number of possible orderings of the drums, there were the unknown connections of the drums. How could they be obtained? Under the new system of encipherment there was no longer any characteristic; the cyclometer and the card files were worthless. Luckily we had the SD network, which, although it introduced the drums IV and V, remained under the old system of encipherment. Using the grid method we looked for and found a day on which drum *N* was one of the original—and therefore known—drums. We assumed that one of the drums L or *M* belonged to the knowns and the other to the unknowns. We found the connections of the unknown drum the same way we had found the connections of the third drum in 1932.

In this way we obtained the connections of all five drums and were able to read messages of the SD network. It was not easy, however. We sometimes knew which drum was at position N as a result of Różycki's *clock* method, but the grid method, the only one we could now apply to the SD network, sometimes failed. It failed because on January 1, 1939, the Germans again increased the number of pairs of letters modified by permutation S from seven to ten. Nevertheless, we did read messages of the SD network Calvocoressi wrongly stated (1077) that at this time no one on earth was able to read messages enciphered on a five-drum Enigma.

Reading messages of military units was a different problem- Although we had found the connections of drums IV and V through the SD network, these drums had to be incorporated into our bomb and into our perforated sheets of paper. The AVA factory did supply a small number of the drums IV and V for the machines used by the decipherers to read the messages of the SD network, but each bomb required 36 pairs of drums IV and V. Since the work using the bombs had to go on around the clock, several additional operators would have to be employed. As for the perforated papers—we would have to make 58 complete sets in addition to the two we already had. We developed methods that, in certain cases, helped us establish with a high degree of probability which drum was at position N. Nonetheless, all sets of the papers were needed. This was the situation: aside from messages of the SD network, we only read military messages when it happened that the three original drums were on the *shaft,* which averaged out to one time out of ten The introduction of drums IV and V meant a change in the quantity but not in the quality of our work. When the SD network also changed to a new way of specifying the daily key on July 1, 1939, the grid method became useless here, too.

Conclusion

On July 25 and 26, 1939, the Poles called representatives of the British, French, and Polish intelligence agencies together for a meeting in Warsaw. At that meeting we told everything we knew and showed everything we had. We provided Major Bertrand with two five-drum Enigmas we haid-made. He undertook the obligation to hand one of the machines over to the.

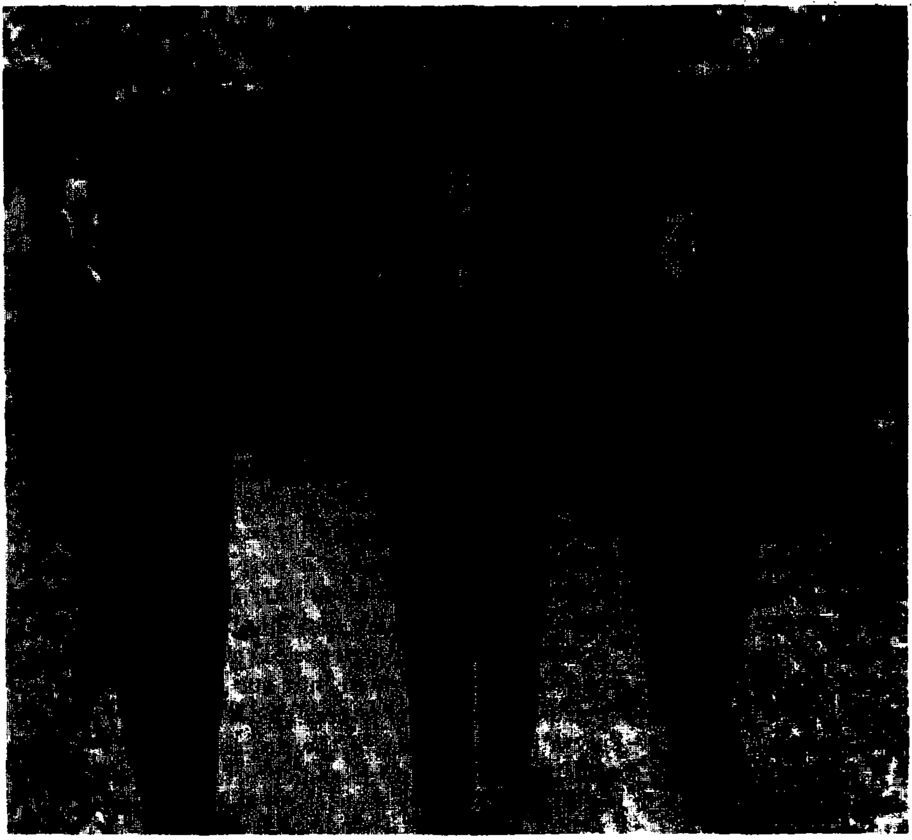


Figure 6. In the gardens of the castle Les Fouzes in southern France in 1941. Left to right: Henryk Zygalski, Jerzy Różycki, and Marian Rejewski.

British, which he did. We learned nothing from our guests. Neither the British nor the French had managed to get past the first difficulties. They did not have the drum connections. They had no methods whatsoever.

The meeting did have far-reaching effects. Shortly thereafter, the Germans, without a declaration of war, invaded Poland. The General Staff, and with it the Cipher Bureau, fled to Rumania. Major Bertrand then brought 15 employees of the bureau, including the chief, his assistant, my two colleagues, and me, to France where he had created a workshop for us in the castle at Vignolles about 40 kilometers from Paris. But how could we work there? All of the materials, equipment, and machines (with the exception of two Enigmas transported across the border in Lt. Col. Langer's car) had been carefully destroyed before leaving Poland so that no trace of our work would fall into German hands. At that point the British sent us the entire collection of 60 sets of 26 perforated Zygalski sheets.

The completion of an enormous amount of work in a relatively short time was nothing extraordinary for the British. They had many people at their disposal. In Bletchley, a town situated about 60 kilometers north of London, where the British cipher bureau was then located, 60 cryptologists were employed already at the beginning of the war, and later there were far more. It is not surprising that when we began to recreate the daily keys using the perforated sheets and send the keys back and forth to each other across the English Channel, out of every 100 keys that were recovered 83 came from the British, and only 17 came from the Poles.

When the French signed a truce with the Germans in June 1940, Major Bertrand arranged for us to flee to Algeria In the fall of the same year, when we returned to the unoccupied zone of France in order to work clandestinely under the leadership of Major Bertrand, we discovered that the Germans had again' changed the way of specifying the daily key, thereby rendering Zygalski's sheets useless. We took up the solution of ciphers other than the Enigma. As Calvocoressi has aptly stated (1977), two things were needed in order to break the Enigma type of cipher: mathematical theory and mechanical aid. As the Germans perfected ways to transmit messages, the mechanical support needed to break the cipher became more and more complicated and costly. The amount of intercepted traffic needed to break a cipher grew correspondingly. Under the conditions we had in France, in zones that were unoccupied but controlled by the Germans, we obtained little intercepted traffic. We could not even dream about concocting a plan to build—much less to actually construct—the complex and costly machines that would have been useful

By 1940 the British in Bletchley had reworked the 1938 Polish bombs to correspond with changed requirements, preserving the name *bomb* and their electromechanical character. Then they built more and more complicated machines to break the Enigma cipher until finally one of them, which came into use at the very end of 1943, was, as Calvocoressi (1977) asserted, the first real electronic computer built in the world.

On November 8, 1942, when the Allies landed in North Africa and in retaliation the Germans crossed into the unoccupied zone of France, Major Bertrand hurriedly evacuated all of us to the Côte d'Azur, from where he organized a plan for us to go in small parties over the Pyrenees to Spain and on to Great Britain. The crossing did not prove successful, however. While crossing the Spanish border three of the persons mentioned in this work fell into German hands: Lt. Col. Langer, Major Ciężki, and Palluth. Palluth died in a labor camp on April 19, 1944, when he was struck by a fragment of a bomb the Allies dropped during an air raid on the camp. Langer and Ciężki were placed in prisoner-of-war camps from which they were freed by the Allies in May 1945. Jerzy Różycki perished earlier, on January 9,1942, in a shipwreck as he was crossing the Mediterranean Sea. Only Henryk Zygalski and I made it to Great Britain. There we became part of a Polish military unit and after a while we again became involved with breaking German ciphers (but not the Enigma) until our unit was disbanded on the strength of relevant Soviet-British agreements.

REFERENCES

Bennett, Ralph. 1979. *Ultra in the West.* London, Hutchinson.

Bertrand, Gustav. 1973. *Enigma ou la Plus Grande Enigme de la Guerre 1939–1945 (Enigma: The Greatest Riddle of World War II).* Paris, Librarie Plon

Brown, Anthony Cave. 1975. *Bodyguard of Lies.* New York, Harper & Row.

Calvocoressi, Peter. 1977. "The Secrets of the Enigma." *The Listener.* London, January 20, January 27, February 3, 1977.

Garliński, Józef. 1979. *Intercept: Secrets of the Enigma War.* London, Dent. (Editor's note: see also Garliński, J., and T. Lisicki, *Enigma War*, New York, Scribner's, 1980.)

Hinsley, F. H., et al. 1979. "The Polish, French and British Contributions to the Breaking of the Enigma." *British Intelligence in the Second World War*, Volume *I*, Appendix 1. London, H.M.S.O.

Johnson, Brian. 1978. *The Secret War*. London, British Broadcasting Corporation.

Kahn, David. 1967. *The Code-Breakers.* New York, Mac-

Kozaczuk, Władysław. 1967. *Bitwa o Tajemnice (Battle for Secrets).* Warsaw, Książka i Wiedza.

Kozaczuk, Władysław. 1976. *Złamany Szyfr (Broken Cipher)*. Warsaw, Wydawnictwo MON.

Kozaczuk, Władysław. 1977. *Wojna w Eterze* (*War on the Airwaves*). Warsaw, Wydawnictwa Radia i Telewizji.

Kozaczuk, Władysław. 1979. *W Kręgu Enigmy* (*Around the Enigma*). Warsaw, Książka i Wiedza.

Lewin, Ronald. 1979. *Ultra Goes to War: The Secret Story.* New York, McGraw-Hill.

Lisicki, T. 1979. Die Leistung des polnischen Entzifferungsdienstes bei der Lösung des Verfahrens der deutschen "Enigma-Funkschlüsselmaschinen." In: Rohwer, J., and E. Jäckel, 1979.

Marinkowić, Ilija. 1977. "*Enigma*" *do Pobjede* ("*Enigma*" *on the Way to Victory*). Zagreb.

Rejewski, Marian. 1980. An application of the theory of permutations in breaking the Enigma cipher. *Applicationes Math. 16*, 4, 543–559.

Rohwer, J., and E. Jäckel (eds.). 1979. *Die Funkaufklärung* (*Radio Reconnaissance*). Bonn-Stuttgart, Motorbuch Verlag.

Stevenson, Williams. 1976. *A Man Called Intrepid: The Secret War*. New York, Harcourt, Brace Jovanovich.*.

Strumph-Wojtkiewicz, Stanisław. 1978. *Sekret Enigmy cret of the Enigma*). Warsaw, Iskry.

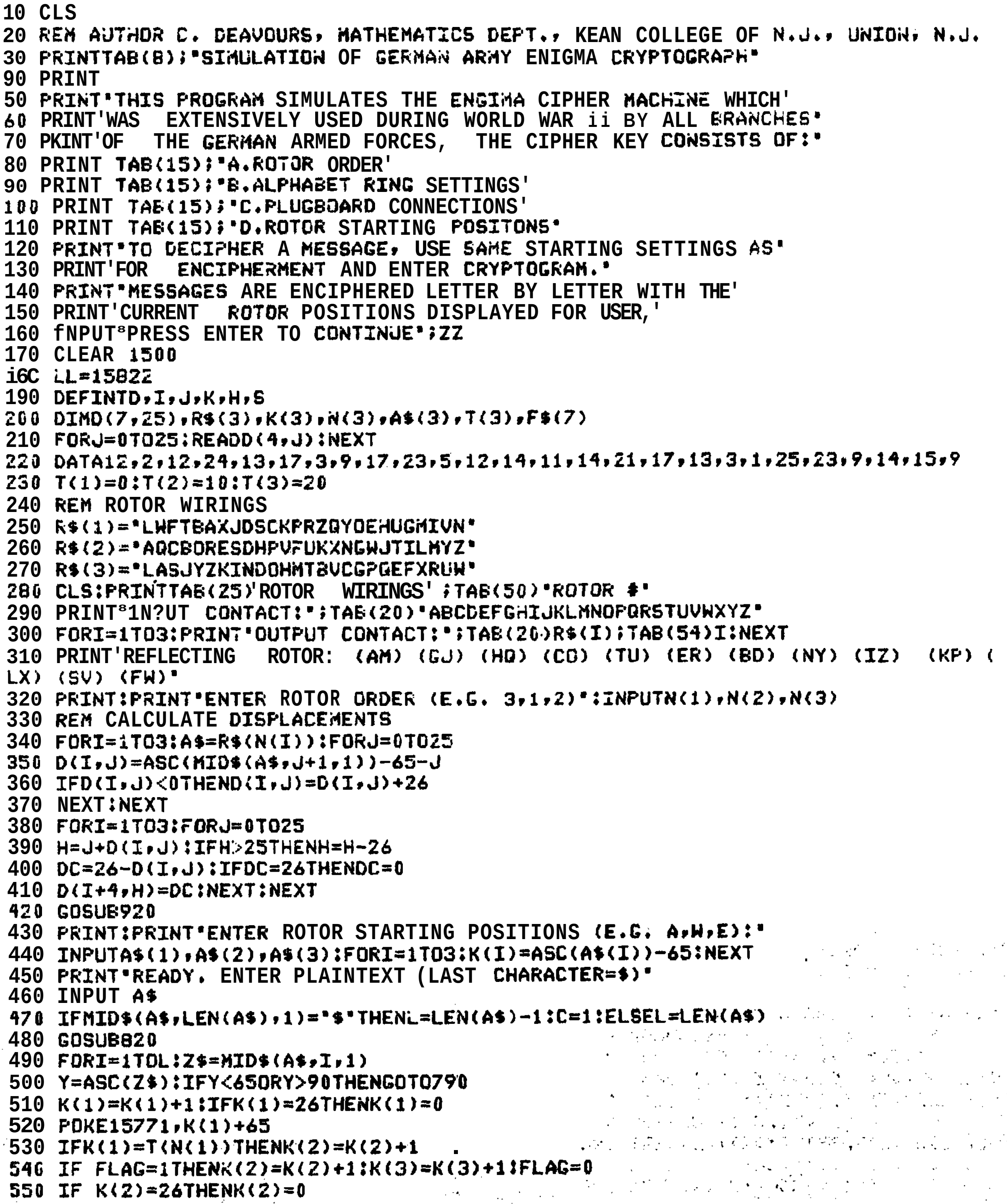
Winterbotham, E. W. 1974. The *Ultra Secret,* New York, Harper & Row.

Afterwords

Editor's Note: We solicited two responses to Rejewski's article—one from Cy Deavours, an amateur cryptanalyst who has written about the work in Poland, and one from Jack Good, who worked with Turing during the war.

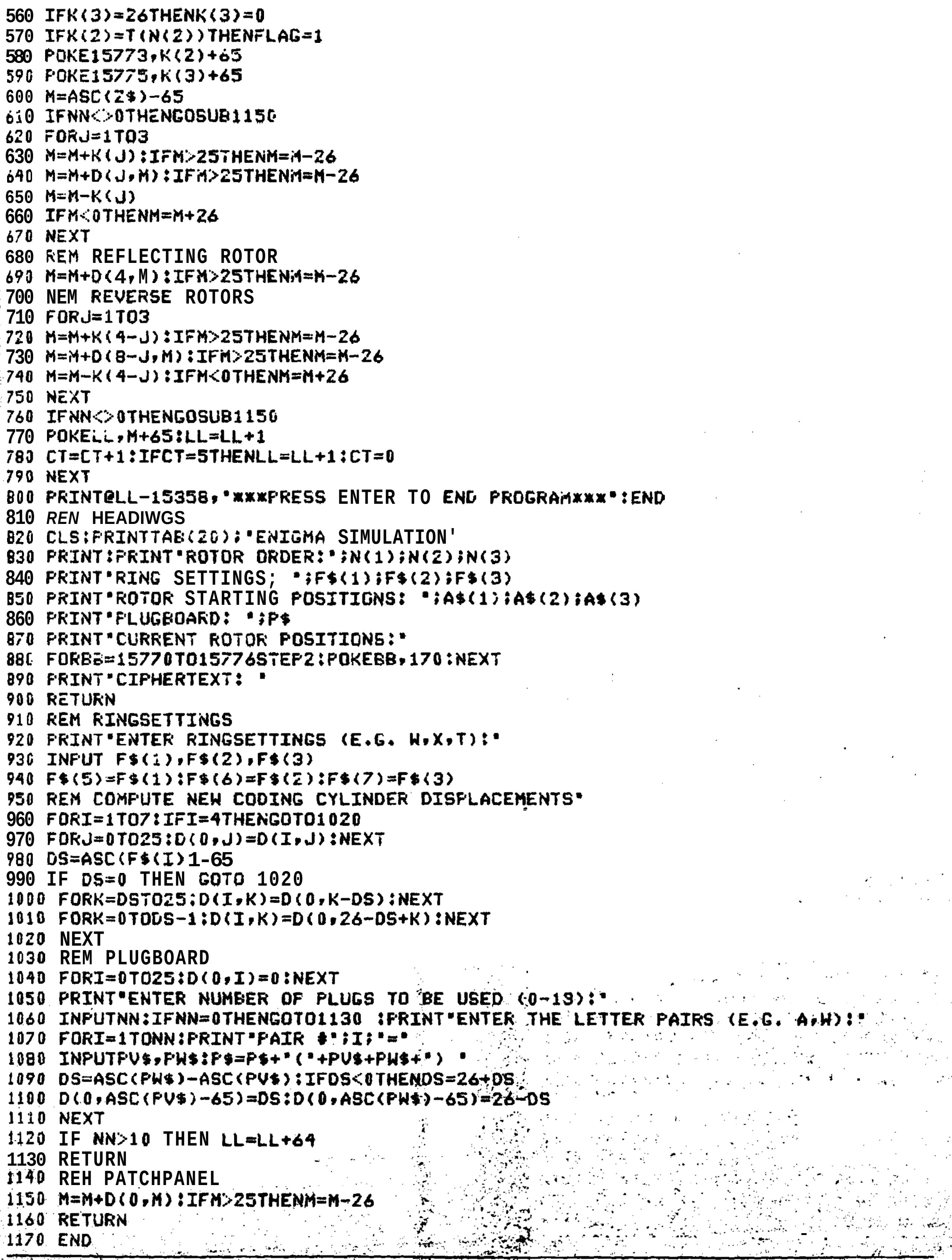
□ Cryptanalysis is an exciting combination of mathematics, statistics, linguistics, computational agility, and inspired guesswork. If one needed convincing of this, the Rejewski article should do it. After all, how many applications of group theory and computer science read like spy thrillers?

Polish penetration into the secrets of the Enigma began in earnest when Rejewski realized the applicability of a simple property of permutations—namely, that if G and P are permutations, then the permutation defined by PGP^{-1} has the same cycle structure as the permutation G. This elementary result along with the ill-conceived German message keying systems was enough to do the job. No doubt practitioners of group



```
10 CLS
20 REM AUTHOR C. DEAVOURS, MATHEMATICS DEPT., KEAN COLLEGE OF N.J., UNION, N.J.
30 PRINTTAB(8);"SIMULATION OF GERMAN ARMY ENIGMA CRYPTOGRAPH"
90 PRINT
50 PRINT"THIS PROGRAM SIMULATES THE ENGIMA CIPHER MACHINE WHICH'
60 PRINT'WAS  EXTENSIVELY USED DURING WORLD WAR ii BY ALL BRANCHES"
70 PKINT'OF  THE GERMAN ARMED FORCES,  THE CIPHER KEY CONSISTS OF:"
80 PRINT TAB(15);"A.ROTOR ORDER'
90 PRINT TAB(15);"B.ALPHABET RING SETTINGS'
100 PRINT TAB(15);'C.PLUGBOARD CONNECTIONS'
110 PRINT TAB(15);'D.ROTOR STARTING POSITONS"
120 PRINT"TO DECIPHER A MESSAGE, USE SAME STARTING SETTINGS AS"
130 PRINT'FOR  ENCIPHERMENT AND ENTER CRYPTOGRAM."
140 PRINT"MESSAGES ARE ENCIPHERED LETTER BY LETTER WITH THE'
150 PRINT'CURRENT  ROTOR POSITIONS DISPLAYED FOR USER,'
160 fNPUT°PRESS ENTER TO CONTINUE";ZZ
170 CLEAR 1500
i6C LL=15822
190 DEFINTD,I,J,K,H,S
200 DIMD(7,25),R$(3),K(3),N(3),A$(3),T(3),F$(7)
210 FORJ=0TO25:READD(4,J):NEXT
220 DATA12,2,12,24,13,17,3,9,17,23,5,12,14,11,14,21,17,13,3,1,25,23,9,14,15,9
230 T(1)=0:T(2)=10:T(3)=20
240 REM ROTOR WIRINGS
250 R$(1)="LWFTBAXJDSCKPRZQYOEHUGMIVN"
260 R$(2)="AQCBORESDHPVFUKXNGWJTILMYZ"
270 R$(3)="LASJYZKINDOHMTBVCGPGEFXRUW"
280 CLS:PRINTTAB(25)'ROTOR  WIRINGS' ;TAB(50)"ROTOR #"
290 PRINT°1N?UT CONTACT:";TAB(20)"ABCDEFGHIJKLMNOPQRSTUVWXYZ"
300 FORI=1TO3:PRINT"OUTPUT CONTACT:";TAB(20)R$(I);TAB(54)I:NEXT
310 PRINT'REFLECTING  ROTOR: (AM) (GJ) (HQ) (CO) (TU) (ER) (BD) (NY) (IZ)  (KP) (
LX) (SV) (FW)"
320 PRINT:PRINT"ENTER ROTOR ORDER (E.G. 3,1,2)":INPUTN(1),N(2),N(3)
330 REM CALCULATE DISPLACEMENTS
340 FORI=1TO3:A$=R$(N(I)):FORJ=0TO25
350 D(I,J)=ASC(MID$(A$,J+1,1))-65-J
360 IFD(I,J)<0THEND(I,J)=D(I,J)+26
370 NEXT:NEXT
380 FORI=1TO3:FORJ=0TO25
390 H=J+D(I,J):IFH>25THENH=H-26
400 DC=26-D(I,J):IFDC=26THENDC=0
410 D(I+4,H)=DC:NEXT:NEXT
420 GOSUB920
430 PRINT:PRINT"ENTER ROTOR STARTING POSITIONS (E.G. A,W,E):"
440 INPUTA$(1),A$(2),A$(3):FORI=1TO3:K(I)=ASC(A$(I))-65:NEXT
450 PRINT"READY. ENTER PLAINTEXT (LAST CHARACTER=$)"
460 INPUT A$
470 IFMID$(A$,LEN(A$),1)="$"THENL=LEN(A$)-1:C=1:ELSEL=LEN(A$)
480 GOSUB820
490 FORI=1TOL:Z$=MID$(A$,I,1)
500 Y=ASC(Z$):IFY<65ORY>90THENGOTO790
510 K(1)=K(1)+1:IFK(1)=26THENK(1)=0
520 POKE15771,K(1)+65
530 IFK(1)=T(N(1))THENK(2)=K(2)+1
540 IF FLAG=1THENK(2)=K(2)+1:K(3)=K(3)+1:FLAG=0
550 IF K(2)=26THENK(2)=0
```

Simulation of Enigma cryptograph.



```
560 IFK(3)=26THENK(3)=0
570 IFK(2)=T(N(2))THENFLAG=1
580 POKE15773,K(2)+65
590 POKE15775,K(3)+65
600 M=ASC(Z$)-65
610 IFNN<>0THENGOSUB1150
620 FORJ=1TO3
630 M=M+K(J):IFM>25THENM=M-26
640 M=M+D(J,M):IFM>25THENM=M-26
650 M=M-K(J)
660 IFM<0THENM=M+26
670 NEXT
680 REM REFLECTING ROTOR
690 M=M+D(4,M):IFM>25THENM=M-26
700 NEM REVERSE ROTORS
710 FORJ=1TO3
720 M=M+K(4-J):IFM>25THENM=M-26
730 M=M+D(8-J,M):IFM>25THENM=M-26
740 M=M-K(4-J):IFM<0THENM=M+26
750 NEXT
760 IFNN<>0THENGOSUB1150
770 POKELL,M+65:LL=LL+1
780 CT=CT+1:IFCT=5THENLL=LL+1:CT=0
790 NEXT
800 PRINT@LL-15358,"***PRESS ENTER TO END PROGRAM***":END
810 REN HEADIWGS
820 CLS:PRINTTAB(20);"ENIGMA SIMULATION'
830 PRINT:PRINT"ROTOR ORDER:";N(1);N(2);N(3)
840 PRINT"RING SETTINGS; ";F$(1);F$(2);F$(3)
850 PRINT"ROTOR STARTING POSITIONS: ";A$(1);A$(2);A$(3)
860 PRINT"PLUGBOARD: ";P$
870 PRINT"CURRENT ROTOR POSITIONS:"
880 FORBB=15770TO15776STEP2:POKEBB,170:NEXT
890 PRINT"CIPHERTEXT: "
900 RETURN
910 REM RINGSETTINGS
920 PRINT"ENTER RINGSETTINGS (E.G. W,X,T):"
930 INPUT F$(1),F$(2),F$(3)
940 F$(5)=F$(1):F$(6)=F$(2):F$(7)=F$(3)
950 REM COMPUTE NEW CODING CYLINDER DISPLACEMENTS"
960 FORI=1TO7:IFI=4THENGOTO1020
970 FORJ=0TO25:D(0,J)=D(I,J):NEXT
980 DS=ASC(F$(I)1-65
990 IF DS=0 THEN GOTO 1020
1000 FORK=DSTO25:D(I,K)=D(0,K-DS):NEXT
1010 FORK=0TODS-1:D(I,K)=D(0,26-DS+K):NEXT
1020 NEXT
1030 REM PLUGBOARD
1040 FORI=0TO25:D(0,I)=0:NEXT
1050 PRINT"ENTER NUMBER OF PLUGS TO BE USED (0-13):"
1060 INPUTNN:IFNN=0THENGOTO1130 :PRINT"ENTER THE LETTER PAIRS (E.G. A,W):"
1070 FORI=1TONN:PRINT"PAIR #";I;"="
1080 INPUTPV$,PW$:P$=P$+"("+PV$+PW$+") "
1090 DS=ASC(PW$)-ASC(PV$):IFDS<0THENDS=26+DS
1100 D(0,ASC(PV$)-65)=DS:D(0,ASC(PW$)-65)=26-DS
1110 NEXT
1120 IF NN>10 THEN LL=LL+64
1130 RETURN
1140 REH PATCHPANEL
1150 M=M+D(0,M):IFM>25THENM=M-26
1160 RETURN
1170 END
```

theory should introduce this property of permutations to students as "the theorem that won World War II." Of course, actually solving the Enigma traffic via statistical analysis, table lookups, or mechanical computation (the Poles used all these methods) was an immense undertaking—one that no other country was up to at that period of history. At the same time Rejewski and his compatriots were busting Enigma traffic on an ongoing basis, the only cryptanalytic technique available was a method known as "cliques on the rods" to the British or the "baton" method to the French. This technique was perfected during the Spanish Civil War and was really useful only for the nonplugboard model of the Enigma that was used in that conflict.

A salient point made by Rejewski that differs markedly from accounts contained in popular histories is that the rotor wirings were reconstructed by Polish cryptographers using the commercial model of the machine as an aid as well as the "Asche" documents. Thus, no military model of the device was available to the Poles, as has been claimed by some authors.

The Polish computational aids, the cyclometer and bombs, were in no sense computers but did hasten the advent of later British electronic calculators such as the Colossus and Heath Robin devices, which became operational around 1943. Rejewski gives the impression that these later machines were also used to solve Enigma messages, but this is not the case since the system being attacked was a series of machines called *Geheimschreibers* ("secret writers") whose complexity generally exceeded that of the Enigma.

One point that should be made is that the British machines called Bombes were not merely high-speed improvements of the Polish bombs but performed Enigma solutions by radically different methods involving known plaintext and parallel processing in testing plugboard permutations. The architects of these British Enigma solvers were Alan M. Turing and Gordon Welchman.

Some minor technical points:

1. The rotor movement of the Enigma was not precisely that of an odometer, at certain positions the second rotor could step two steps in succession so that the rotor period was $26 \cdot 25 \cdot 26$ instead of 26^3.

2. Besides the addition of a plugboard, the rotor alphabet rings of the military Enigma were differently constructed from those of the commercial model. This led to some important differences in solution techniqes. Additionally, the reflecting rotor, as Rejewski indicates, was not rotatable on the military Enigma.

The Germans constantly revised and modified their use of the Enigma during the war. More rotors were introduced from which to choose the three that were used in the machine. A four-rotor model with a much better keying system was adopted for naval use. Message-indicator systems were altered, etc. Polish and later British cryptanalysts managed to keep up with these changes. Eventually, the Germans must have sensed the vulnerabilities of the Enigma became a new cipher machine was being introduced on the front lines when the war ended. Ironically, this new machine would have been even easier for the Allies to penetrate than had been the older Enigmas.

Cipher A. Deavours
Mathematics Department
Kean College of New Jersey
Union, NJ 07083

□ The editor has requested my reactions to Rejewski's paper describing the cryptanalytic work on the German Enigma by three Polish mathematicians. My relevant experience was as a cryptanalyst during World War II, especially in the attack on the German naval Enigma when I was the chief statistical assistant to A. M. Turing and later to the famous chess player C. H. O'D. Alexander in Bletchley Park in the section called Hut 8. I arrived at Bletchley Park on May 24, 1941, which happened to be the day the *Bismarck* was sunk. In October 1943 I became the main statistical assistant and first mathematical assistant to M. H. A. Newman, F.R.S., who was in charge of machine attacks on the cryptographic machine called the Geheimschreiber. At the time Newman had one other cryptanalytic assistant, Donald Michie, now a professor of machine intelligence in Edinburgh.

Because of the security principle of the "need to know" I was not aware, during the war, of the details of the Polish work, although I knew they had made a contribution to the breaking of the Enigma. It was therefore an eye-opener for me when I read Rejewski's paper. The Polish mathematicians, with the help of French intelligence, certainly did an outstanding job.

It would be a pity, however, if the publication of Rejewski's paper should cause anyone to belittle the British cryptanalytic e&*. In my opinion a balanced view can be obtained from Appendix I (p. 495) of Hinsley (1979). It appears from Hinsley's account that some months were gained in the British reading of the German air force Enigma traffic, owing to the Polish contribution, but "The regular solution of German naval and army Enigma keys [by the British] began so much later than the beginning of 1941, and was the outcome of so many other developments, that it is unlikely that the Polish contribution made any difference to the dates from which they were mastered."

The security of the German usage of the Enigma gradually increased, with the result that the Polish cryptanalytic resources became inadequate before the outbreak of the war. The Germans made the following cryptographic improvements in the use of the naval Enigma.

In 1939 the number of distinct rotors used by the German navy increased to eight. The Poles had read much traffic when there were only three rotors in the set—that is, six possible wheel orders. They recovered the wirings of five rotors, but $5\cdot4\cdot3 = 60$ wheel orders for the military Enigma were too many for their resources. With eight wheels in the set there were $8\cdot7\cdot6 = 336$ possible wheel orders for the three-wheel machine, and later there were $8\cdot7\cdot6\cdot5 = 1680$ for the four-wheel (U-boat) machine. Moreover, ten pairs of letters were plugged into the Stecker board so there were only six "self-steckers" or nonplugged letters instead of the fourteen previously available. Six self-steckers were too few to be readily exploited by the cryptanalyst. Finally, the indicator system for the naval Enigma, for the initial settings of individual messages, was made more sophisticated. (The settings were enciphered at a setting called the *Grundstellung*, which was fixed for the day and had to be recovered cryptanalytically.)

Part of the stock-in-trade of the cryptanalyst is a search for repeats (Saccho 1951, p. 186; Friedman 1922). Różycki's "clock method," mentioned by Rejewski, is an application of such a search. Różycki aligned two messages, one under the other, in "depth," if the number of pairs of repeated cipher letters (such as an X underneath an *X*) was large enough. Several such alignments led to the identification of the right-hand rotor. We used an elaboration of this procedure, which we called *Banburismus*, but it was logically much more complex because of the nature of the system for indicating the initial settings of the rotors for each message. Information was derived from long repeats, such as pentagraphs, found by sorting all the traffic, and by short repeats, such as monographs and digraphs, found by *sliding* one message against another. Not all tetragraph repeats, for example, were of equal value. By subdividing the population one could improve the accuracy of one's scoring system. The process of using the more accurate scores was called ROMSing, where ROMS meant "resources of modern science." The entire repeat pattern between two messages gives probabilistic evidence for or against the hypothesis that the two messages are correctly aligned "in depth" at a certain stagger (Good 1973). Of course, the sliding process can be carried out more easily with the help of punched paper than by sliding written or printed messages.

The punched forms of the messages were called Banbury sheets because they were printed in the town of Banbury. The punching was done laboriously by scores of young women known as "the girls." The repeat patterns were scored up, using "weights of evidence" (logarithms of Bayes factors) measured in "decibans." The names *deciban* and ban were invented by Turing. If f is a Bayes factor then $10 \log_{10} f$ is the corresponding number of decibans. For more discussion of this terminology see Good (1950), although in that book I made the retrograde step of *calling* decibans "decibels."

One of my early contributions in Hut 8 was the intellectually modest one of proposing the half deciban (hdb) as the unit, to be rounded to the nearest integer. Previously the "girls" had been compiling large tables of scores such as 3.7, meaning 3.7 decibans. My first reaction was to think that the decimal point should be dropped, the unit then being a centiban, but then a calculation showed that the use of half decibans would lose little accuracy, and writing 7 should be adequate. This saved a great deal of writing, arithmetic, and eyestrain and therefore saved hours every Banburismus day, which for a time was roughly every second day. Some ideas are very useful without being very clever.

The probabilistic information obtained from numerous pairs of messages all had to be fitted together to make a consistent story concerning the simple substitution applied to the third letter of each trigraphic indicator group as a consequence of its encipherment at the Grundstellung. It would take too long to go into further details. Banburismus was a game that required much skill and judgment, because it involved numerous little pieces of probabilistic information, and it is not *surprising* that the chess champion Hugh Alexander-was also the champion at this game. The game went further than the identitication of the right-hand wheel, which was the application mentioned by Rejewski. The information obtained from Banburismus or from cribs, or both, was fed to the Bombes for finding more information about the daily keys. The output from the Bombes was then returned to the cryptanalysts to complete the daily job.

It was in connection with Banburismus that Turing had a number of new or fairly new statistical ideas, such as sequential analysis and the nontrivial form of empirical Bayes. For a rapid rundown of these ideas see *Good* (1979*a*).

As Rejewski surmises, our Bombes were much more elaborate and sophisticated than the Polish *Bombas*, both in their basic logic and in their engineering design.--Bath the Bombas and the Bombes were electromagnetic. The Colossus, which was electronic, was not related to nor derived from the Bombe nor to Polish cryptanalysis. Thus Rejewski's penultimate paragraph is misleading. For further information about the Colossi see Johnson (1978, p. 338), Randell (1980), and Good (1979*b*).

REFERENCES

Friedman, W. F. 1922. The index of coincidence and its applications in cryptography. Geneva, Ill., Riverbank Laboratories. Available at the Library of Congress.

Good, I. J. 1950. *Probability and the Weighing of Evidence*. London, Griffin.

Good, I. J. 1973. The joint probability generating function for run-lengths in regenerative binary Markov chains, with applications. *Annals* of *Statistics* 1, 933–939.

Good, I. J. 1979*a*. Early work on computing at Bletchley. *Annals of the History of Computing 1*, No. 1, 38–48.

Good, I. J. 1979*b*. Studies in the history of probability and statistics XXXVII. A. M. Turing's statistical work in World War II. *Biometrika* 66, 393–396.

Hinsley, F. H., et al. 1979. *British Intelligence in the Second World War*. Vol. 1, London, H.M.S.O.

Johnson, Brian. 1978. *The Secret War*. London, British Broadcasting Corporation.

Randell, Brian. 1980. "The Colossus." In *A History of Computing in the Twentieth Century*, N. Metropolis, J. Howlett, and Gian-Carlo Rota, eds. New York, Academic Press.

Saccho, L. 1951. *Manuel de Cryptographie* (French ed. by J. Bres, from the Italian). Paris, Payot.

I. J. Good
Department of Statistics
Virginia Polytechnic Institute and State University
Blacksburg, VA 24061