Math 65S September 25, 2003

Enigma

The Enigma enciphering machine, so named by its inventor, Adolph Scherbius, was the first secure and practical mechanical encryption device. Invented as a means to store and protect commercial secrets, Enigma was not widely adopted until the German military, motivated in part by its embarrassing cryptographic failures both during and after WWI, bought the design in 1927 and later put it to use to secure the communications of its army, air force and, most famously, its Atlantic submarine fleet. Although conceptually not revolutionary, Enigma exploited available technology to mechanize encryption in an entirely new and effective way.

Part Ia: The machine

We will abbreviate "Enigma" or "Enigma machine" to EM. Its principal components were as follows (refer to the diagram on the following page):

Key board: an ordinary (German) keyboard.

Lamp board: similar, but with lamps in place of keys, on which were printed alphabetic characters which became visible when the corresponding lamps were illuminated

Switch board: single plug outlets, one for each alphabetic character, to be connected in six pairs with wire connectors. (This was not part of Scherbius' original design, but rather was added by the German military to increase security.)

Three (rotating) drums: removeable, coaxial insulated discs, also called *rotors*, with two sets of 26 contacts, one for each alphabetic character, arranged near the outer edge of the flat sides of the drums and wired together (through the discs) in pairs. The 26 alphabetic characters were inscribed along the round edge of each rotor, and a removeable plate enclosed the whole set of rotors, with small windows revealing the top-most letter so as to specify the (rotatable) position of the rotor.

Reflecting drum: a fixed insulated disc, with a single set of 26 contacts, wired together in pairs.

Wiring: connections between the keys and lamps, between the lamps and and fixed spring-loaded contacts to the first rotor, between fixed, spring-loaded contacts connecting the first and second rotors, the second and third rotors and the third and the reflecting drum.

Battery: to power the lamps.

All operators had identical machines to ensure interoperability. To initiate encryption of a message, an operator did two things. First he set the position of each rotor, both its order among the three available positions and its rotation (as seen through the small windows); then he chose six pairs of letters to be connected on the plug board. In practice, the operators did not themselves choose the rotor and plugboard settings: they were set by *code books* shared by all operators. At first, these settings were changed daily, later in WWII hourly in some cases. These settings constitute the key of the Enigma cryptosystem.

To encrypt a message, the operator pressed the key corresponding to the first letter of plaintext, thus closing the circuit and illuminating a lamp showing the first letter of ciphertext. One of the most important properties of EM is that this process is involutory: *if plain letter D (from the keyboard) was sent to cipher letter U (on the lampboard), then any other operator using the same plug and rotor settings typed in U and got D on the lampboard.* Thus, the enciphering and deciphering keys were the *same*.

Another feature of EM was that after each press of a key, the first rotor rotated to the next letter in the window; *i.e.* 1/26th of a complete turn. Every 26 presses, the second would also rotate 1/26th and every $26^2 = 676$ presses, the third rotor rotated through 1/26th of a complete turn. Thus, only after $26^3 = 17,576$ turns did the machine return to its initial setting. It could thus be expected that each setting of EM gave rise to 17,576 alphabets.

Part Ib: The protocol

All ciphertext was sent by radio and so was easily intercepted by the Allies. The Germans feared that with that a lot of ciphertext sent using the same day key, plus other information, an enemy might break EM. (In fact, Rejewski claims to have achieved such a break against a Swiss cipher machine in 1940.) So to avoid this possibility, the Germans adopted a protocol which set a different, operator specified *message key* for each message encrypted with EM. It is both surprising and ironic that this extra step, which was taken to enhance security, is exactly what allowed Polish mathematicians to break Enigma, as we will see.

To do this, an operator set the EM according to the day key, then sent a three-letter *message key*, randomly chosen by him, giving the three rotor settings for the coming message. The operator who received this three-letter encrypted code group then typed it into his EM, thus recovering the sender's three letters. Now the sender set the rotors on his EM to his three-letter choice and encrypted his message. Since the receiver had an identical machine and the correct setting of the rotors, he had only to type in the received ciphertext, in order to recover the plaintext. Notice that the involutory property of the key is being used here.

Radio transmission conditions were, however, often not optimal, resulting in the loss of some of the letters in this protocol. This is not even to mention that the life-and-death situations under which technicians sometimes had to operate could make accurate keying, reception and transcription difficult. If one of the first three letters, *i.e.* the message key, were lost, then the whole message that followed it would be unintelligible.

In order to minimize this possibility, operators were instructed to send the message key *twice*. So if the message key were *hot*, then the sender set EM according to the day-key, typed *hothot*, read off the corresponding letters from the lampboard, say *duqraz*, reset

EM to *hot*, and typed in the message, reading off the corresponding cipher letters from the lamp board; this ciphertext , preceded by the six letters *duqraz*, were radioed to the receiver. Notice that because the rotors are turning each time a key is pressed, there is (in general) no repetition in the encipherment, *duqraz* of *hothot*. Again because of the involutory property of EM, when the receiver typed in *duqraz*, the lamps would give *hothot*, thus providing proof that the message key was *hot*.

Part II: Keys

The Germans believed EM was secure because of the size of the key space, which was so large as to be invulnerable to brute-force attack at the time. Let us look at this more closely.

Since there were three rotors, there were 3!=6 possibilities for their placement in the slots: 3 choices for the first slot, and, having placed one, 2 remaining rotors for the second. Then the third had only one place left to go. Once placed, each rotor could be rotated in its slot to any one of 26 positions. So there are $26^3 = 17,576$ possibilities for all three rotations. Altogether then, there are $6 \cdot 17,576 = 105,476$ possibilities for the placement of the rotors. In other words, there are 105,476 possible keys. This key space, which was what was available on Scherbius' commercial EM, seemed too small to the Germans, so they added the plugboard.

Now the number of ways of choosing a pair of letters to connect is the same as the number of two-element subsets of the set of 26 alphabetic characters, also known as "26-choose-2." This number is

$$\binom{26}{2} := \frac{26!}{24!2!} = \frac{26 \cdot 25}{2}$$

Once this has been done, there are 24 letters remaining, so

$$\frac{24 \cdot 23}{2}$$

ways of choosing two letters to connect. So it would seem there are altogether

$$\frac{26 \cdot 25}{2}\frac{24 \cdot 23}{2}\frac{22 \cdot 21}{2}\frac{20 \cdot 19}{2}\frac{18 \cdot 17}{2}\frac{16 \cdot 15}{2} = \frac{26!}{14!2^6}$$

ways to choose six pairs of letters to connect. However, this reasoning would count the choices

$$(A,S)(D,F)(G,H)(J,K)(L,O)(U,I)$$

and

$$(D,F)(A,S)(G,H)(J,K)(L,O)(U,I)$$

as being different, because their first pairs (A,S) and (D,F) are different, even though they differ only in the order in which they were chosen. Since there are 6! ways of ordering the six pairs of connections, there are in fact

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

possible plugboard configurations. So altogether, the size of the key space of the military EM is

$$26^3 \cdot 3! \cdot \frac{26!}{14!6!2^6} = 186,075,649,051,516,224,000$$

Keep in mind that, although very large, the size of this key space is close to 2^{56}, the size of the key space of DES, the former standard for secure private-key cryptosystems. In fact, the vulnerability of DES was due to the fact that machines could be built which were capable of searching its key space quickly. So if this were all the possible EM keys, then it could be broken with today's technology. But in practice there was a much larger key space.

Remember Kerckhoff's principle: one must assume that the enemy knows the cryptosystem, so only the key protects an encrypted message from being read. But in this case, the Poles (the enemy) had more than the key space to contend with: although they had a commercial EM, so that they knew exactly how EM functioned, they did not possess a military EM, whose internal wirings were different. This meant that they had to take the rotor wirings to be part of the key, making cryptanalysis both quantitatively and qualitatively much more difficult. Specifically, each rotor could be wired in any one of 26! ways: A on one side could be wired to any one of 26 letters on the other side of a rotor, then B to any of the remaining 25 letters, and so on. So there are

$$(26!)^3 = 65592937459144468297405473968303761468794234820105359750856704 \cdot 10^{18}$$

possible ways to wire the three rotors. By reasoning as we did when we computed the number of possible plugboard configurations, we see that the number of ways to wire the reflecting drum is

$$\frac{26!}{13!2^6} = 7,905,853,580,025$$

So the actual key space has size

$$518568159435733221862718182791346235984740553672610470234001015379171737 6 \cdot 10^{20}$$

times the number of rotor and plugboard settings we computed above, giving

$$\begin{aligned}&964929068444542065097252210287218695\\ &\qquad 981196905757970817178691444526584908808785585686708224 \cdot 10^{23}\end{aligned}$$

possible keys altogether. This is a number with 113 decimal digits, and a key space of this size is impossible to search on a modern computer. Rejewski certainly knew all this, and yet, in a brilliant series of attacks, was able to read EM-encrypted messages almost as fast as the intended receivers.

Part III: Rejewski

Rejewski's attack on EM began with the determination of all the message keys on a given day from 60-80 intercepted repeated encipherments of message keys. He did this without knowledge of the day keys used to encipher the message keys and without knowing the wirings of the drums.

His procedure was as follows:

(1) First collect the six letter twice-enciphered message keys, say

$$\begin{array}{ll} duq & raz \\ lmr & dek \\ haf & mxj \\ zxl & itm \\ rch & lpo \end{array}$$

and so on.

(2) Next take the first and fourth letters from each group,

$$\begin{array}{ll} d & r \\ l & d \\ h & m \\ z & i \\ r & l \end{array}$$

and look for chains constructed as follows. Write down the first and fourth letter of one of these groups; then if this fourth letter is the first letter of another group, write down the fourth letter of that group; then if this fourth letter is the first letter of another group, write down the fourth letter of that group, and so on until the the circle is complete: a fourth letter is reached which was the very first letter. Call the resulting collection of letters a *cycle*. For instance, with the collection of first and fourth letters above we would get the cycle

$$d \to r \to l \to d$$

We denote this cycle

$$(drl)$$

Clearly, if we had started with the pair, $r \to l$, of first and fourth letters, we would have gotten the cycle (rld), so we regard the cycles (drl), (rld) and (ldr) as identical for this procedure. Each is called a *cyclic permutation* of the others.

(3) Keep doing this until you run out of letters. It turns out in fact that these cycles are disjoint and exhaustive: if you find another cycle with d, l or r in it, it has to be (dlr) or a cyclic permutation of it; and (with enough intercepts) every letter will eventually appear in one of these cycles. Thus you find all the letters of the alphabet, divided into disjoint cycles.

(4) Now do the same thing for the second and fifth and then for the third and sixth letters.

This procedure produces three lists of cycles, each of which gives a complete irredundant list of the letters in the alphabet. These lists have some remarkable properties. For instance, each collection of cycles occurs in pairs of equal length. So where we have a cycle (dlr) as above, we must have another 3-letter cycle.

From this and other properties like it, plus some skill and intuition, Rejewski was able to deduce all the message keys from the intercepts he used to produce the three lists of cycles. To see how he did this we must study the mathematical tool he used, the theory of permutations.

Part IV: Permutations

Fix a set X of n distinct objects. For instance, X might be the alphabetic characters

$$\mathcal{A} := \{a, b, \ldots, z\},$$

where n=26. Another example is the set of the first n integers

$$\mathbf{n} := \{1, 2, \ldots, n\}$$

for some integer n. A *permutation* of X is a one-to-one function $\pi : X \to X$, meaning that if $x \neq y$, then $\pi(x) \neq \pi(y)$.

For instance, for each setting of EM, we get a permutation of $\mathcal{A}$. In fact, *the set of encryption functions for monoalphabetic ciphers (which use the letters from $\mathcal{A}$) is the same as the set of permutations of $\mathcal{A}$.*

For another example, if the cards in a deck are numbered top to bottom from 1 to 52, then shuffles of the deck are the same as permutations of **52**. For instance, the permutation π of **6** given by

$$\pi(1) = 1$$

$$\pi(2) = 3$$

$$\pi(3) = 5$$

$$\pi(4) = 2$$

$$\pi(5) = 4$$

$$\pi(6) = 6$$

is often called a "perfect shuffle": cut the deck in half and interleave the cards.

An interesting property of this shuffle, indeed of any shuffle or even any permutation, is that if it is repeated often enough, the cards (or letters or numbers) will return to their original order. We will see later why this is so.

Here are some abstract properties of permutations, together with their crypto-counterparts.

(1) If π_1 and π_2 are permutations, so is the composition $\pi_2 \circ \pi_1$. *Doing two monoalphabetic encipherments in succession is still a monoalphabetic cipher.*

(2) The function $\epsilon : X \to X$, $\epsilon(x) = x$, is a permutation such that $\epsilon \circ \pi = \pi = \pi \circ \epsilon$. It is called the *identity* permutation. *The non-cipher!*

(3) For every permutation π, there is a permutation σ such that $\sigma \circ \pi = \epsilon = \pi \circ \sigma$. This uses two things: first the Pidgeonhole Principle to conclude that every $y \in X$ is $\pi(x)$ for some x; and second the one-to-one-ness of π to conclude that there is only one such x. So if we define

$$\sigma(y) = x$$

then because $\pi(x) = y$, we have what we want. *If $\pi : \mathcal{A} \to \mathcal{A}$ is an enciphering rule, then there is a deciphering counterpart σ which "undoes" the encipherment of a plaintext letter: $\sigma(\pi(p)) = p$*

(4) Given permutations π and σ, it's not always true that $\pi \circ \sigma = \sigma \circ \pi$. For instance, the permutations of **3**

$$\begin{aligned} \pi(1) &= 2 \quad & \sigma(1) &= 2 \\ \pi(2) &= 3 \quad & \sigma(2) &= 1 \\ \pi(3) &= 1 \quad & \sigma(3) &= 3 \end{aligned}$$

satisfy

$$\pi \circ \sigma(2) = 2 \text{ but } \sigma \circ \pi(2) = 3$$

Take care with the order of repeated encipherment.

(5) There are $n!$ permutations of X. *There are 26! monoalphabetic ciphers.*

A very simple sort of permutation is a *cycle*, which we introduce by example. From **6** choose a subset, say 1, 6, 4. Then define a permutation $\gamma : \mathbf{6} \to \mathbf{6}$ which takes 1 to 6, 6 to 4 and 4 to 1:

$$\begin{aligned} \gamma(1) &= 6 \\ \gamma(2) &= 2 \\ \gamma(3) &= 3 \\ \gamma(4) &= 1 \\ \gamma(5) &= 5 \\ \gamma(6) &= 4 \end{aligned}$$

Notice that 2, 3, and 5 are fixed. A convenient notation for this permutation is

$$\gamma = (164)(2)(3)(5)$$

or just

$$(164),$$

called a *3-cycle.* Since the notation means that 1 is taken to 6, 6 to 4 and 4 to 1, we have

$$(164) = (641) = (416);$$

but

$$(164) \neq (614)!$$

Now looking back at the definition of a perfect shuffle, we see it is the 4-cycle

$$(2354)$$

Recall we said above that the order of composition of permutations matters: for permutations π and σ, $\pi \circ \sigma \neq \sigma \circ \pi$ in general. Some exceptions to this “inequality” were noted there. Another is that *the order of composition of disjoint cycles doesn't matter.* For instance,

$$(164) \circ (235) = (235) \circ (164)$$

It's easy to see why this is so: because the subsets $\{1, 6, 4\}$ and $\{2, 3, 5\}$ are disjoint, it doesn't matter in which order you move them around, first $\{1, 6, 4\}$ then $\{2, 3, 5\}$, or vice-versa. Notice that the permutations π and σ in property (4) were not moving disjoint sets around.

The second important property of disjoint cycles is that they are everywhere. For example, let's take the example γ above and change it slightly, by changing the values of $\gamma(2)$ and $\gamma(3)$:

$$\gamma'(1) = 6$$

$$\gamma'(2) = 3$$

$$\gamma'(3) = 2$$

$$\gamma'(4) = 1$$

$$\gamma'(5) = 5$$

$$\gamma'(6) = 4$$

Then

$$\gamma' = (164)(23)$$

meaning that γ' takes 1 to 6, 6 to 4 and 4 to 1; *and* 2 to 3 and 3 to 2. The way this was done should remind you of the procedure Rejewski used to find his cycles in Part III: γ sends 1 to 6, then 6 to 4 and finally 4 back to 1; next take a number not among those in (164), say 2, and find that 2 goes to 3 and 3 back to 2; finally, the remaining number, 5, is not moved by γ'.

We say that γ' *contains* the cycles (164) and (23) and sometimes write

$$(164) \in \gamma' \quad \text{and} \quad (23) \in \gamma'$$

Notice that the two cycles (164) and (23) are disjoint. In fact, this procedure can be carried out for any permutation:

Theorem. *Every permutation can be decomposed uniquely (in only one way) into disjoint cycles.*

This explains why every shuffle, repeated often enough, returns the deck to its original order. Suppose the shuffle σ is decomposed into disjoint cycles

$$\sigma = \gamma_1 \gamma_2 \dots \gamma_m$$

Since the order of composition of the γ's does not matter, if we compose σ with itself k times (*i.e.*, repeat the shuffle γ k times), then we get

$$\sigma^k = (\gamma_1)^k (\gamma_2)^k \dots (\gamma_m)^k$$

Now if, say, γ is a 4-cycle, then it's easy to see that $\gamma^4 = \epsilon$, the identity permutation. So if k is chosen carefully

$$\sigma^k = \epsilon$$

meaning that the deck has been returned to its original order.

The examples of greatest interest to us are the permutations (encryptions) effected by EM. Remember its involutory property: if, say, EM(a)=s, then EM(s)=a. So given a setting of EM, its encryption rule looks like

$$(as)(rz)(bl)(rh)\ldots$$

Now 2-cycles like these are important enough to have their own name: *transpositions*. So we have shown

- *EM encryptions are decomposed into disjoint transpositions*

Part V: Rejewski Redux

Now finally we can see what Rejewski was doing when he constructed his chains. Using his notation (from the handout) let A, B, C, D, E and F denote the first six permutations (encryptions) effected by EM; it is using these to encrypt the repeated 3-letter message keys. These permutations will be used to encrypt every message key on a given day. Suppose

$$A = (as)(rz)(bl)(dh)\ldots,$$

the permutation above, and D is

$$D = (tk)(rh)(bd)(zl)\ldots,$$

so that if the message key were *hot*, so that the sender typed *hothot*, then since

$$A(h) = d \text{ and } D(h) = r$$

the first and fourth letters of ciphertext would be d and r. Now since $A(h) = d$, $A(d) = h$. So for the composition $D \circ A$, we have

$$D \circ A(d) := D(A(d)) = D(h) = r$$

Next suppose the message key were chosen (for another message) to be *zip*. Then the first and fourth letters of the encryption of *zipzip* would be

$$A(z) = r \text{ and } D(z) = l,$$

so that

$$D \circ A(r) := D(A(r)) = D(z) = l$$

If a third intercept were an encryption of *bbbbbb*, then the first and fourth letters of the enciphered version would be

$$A(b) = l \text{ and } D(b) = d,$$

so that

$$D \circ A(l) = d$$

So the first-to-fourth letter cycle Rejewski would build from these intercepts is

$$(drl)$$

which is also a part of the cycle decomposition of the permutation $D \circ A$. So

• *Rejewski's first-to-fourth letter cycle decomposition of the set $\mathcal{A} = \{a, b, \ldots, z\}$ of alphabetic characters is the same as the cycle decomposition of the permutation $D \circ A$ of $\mathcal{A}$. In other words, by determining this decomposition, he was determining the composite permutation $D \circ A$.*

Of course what he wanted was A or D: with these, he could take any intercepted encryption of a message key and find the first plain letter by applying A to the first cipher letter, or D to the fourth cipher letter. So here is the

Goal. *Given $D \circ A$ (which has been determined from a large collection of intercepts) find A or D.*

Rejewski reached this goal with a combination that is very common in successful attacks on cryptosystems: mathematics and intuition, *i.e.*, guessing. Since we're on the subject, we discuss the mathematics first.

We won't reach our goal directly, instead discovering some of the hidden structure of composed permutations like $D \circ A$ first.

Suppose the transposition $(a_1 a_2)$ were in A. Then the letter a_2 would have to appear in some transposition in D, say $(a_2 a_3)$. If $a_3 = a_1$, stop. Otherwise, a_3 is in some transposition (other than $(a_1 a_2)$) in A, say $(a_3 a_4)$ is in A. Now a_4 is somewhere in D, say $(a_4 a_5)$ is in D. Here is a summary:

$$(a_1 a_2) \in A \quad \text{and} \quad (a_2 a_3) \in D$$

then if $a_3 \neq a_1$,

$$(a_3 a_4) \in A \quad \text{and} \quad (a_4 a_5) \in D$$

and if $a_5 \neq a_1$, ... eventually

$$(a_{2k-1} a_{2k}) \in A \quad \text{and} \quad (a_{2k} a_1) \in D$$

That is, we get back to a_1.

Here is what it looks like schematically:

$$a_1 \xrightarrow{A} a_2 \xrightarrow{D} a_3 \xrightarrow{A} a_4 \xrightarrow{D} a_5 \ldots a_{2k-1} \xrightarrow{A} a_{2k} \xrightarrow{D} a_1$$

For instance, if A and D are

$$A = (as)(rz)(bl)(dh)\ldots \quad \text{and} \quad D = (tk)(rh)(bd)(zl)\ldots$$

as at the beginning of this section, then this chain starting at d is

$$d \xrightarrow{A} h \xrightarrow{D} r \xrightarrow{A} z \xrightarrow{D} l \xrightarrow{A} b \xrightarrow{D} d$$

Going back to the general picture, we see that

$$(a_1 a_3 \ldots a_{2k-1}) \in D \circ A$$

and, starting at a_{2k} and going backward,

$$(a_{2k} a_{2k-2} \ldots a_2) \in D \circ A$$

as well. In our example these two cycles in $D \circ A$ are (drl) and (bzh). We have thus proved:

Rejewski's Theorem. *Let A and D be two permutations composed solely of disjoint transpositions. Then*

(1) *The cycles in $D \circ A$ appear in pairs of equal length.*
(2) *The two letters in any transposition in A or D appear in different cycles of $D \circ A$ of the same length.*
(3) *Suppose in (2) that (ab) is in A, that a is in the cycle γ_1 of $D \circ A$ and that b is in the cycle γ_2 of $D \circ A$. Let c be the letter just before a in γ_1 and let d be the letter just after b in γ_2. Then (cd) is in A.*

That's the mathematical side of the story. It tells us that if we can discover just one $(ab) \in A$ for each pair of equal length cycles in $D \circ A$ (remember we know $D \circ A$ from intercepts), as in part (2) of Rejewski's Theorem, then part (3) says we get all of the transpositions in A, *i.e.*, we get all of A. But how does one find that first $(ab) \in A$? One can't be a successful cryptanalyst without a sense for how real people will use a machine like Enigma, and in this Rejewski shows his second, equally brilliant, but completely different skill: intuition.

Let's follow the example he gives on p.218 of the handout. Suppose we have from intercepts that

$$D \circ A = (dvpfkxgzyo)(eijmunglht)(bc)(rw)(a)(s)$$

$$E \circ B = (blfqveoum)(hjpswizrn)(axt)(cgy)(d)(k)$$

$$F \circ C = (abviktjgfcqny)(duzrehlxwpsmo)$$

By Part (2) of Rejewski's Theorem, we know right away that (as) is in both A and D, because the two letters of each transposition in A or D have to appear in cycles of equal length in $D \circ A$. Now Rejewski makes the remarkable observation that "...cryptographers are inclined to choose three identical letters..." for their message keys, in spite of the fact that the protocol calls on them to choose three random letters. And it turns out he's right!

For example, let's see whether one of the senders of the intercepts of encrypted message keys

$$sug \quad smf$$

$$sjm \quad spo$$

$$syx \quad scw$$

could have been using aaa as his message key. We've chosen to try out aaa because s appears as both first and fourth letters of these intercepts, and we know that these s's decrypt to a.

Look at the first intercept. If u had been an encryption of a, then we would have had

$$B(a) = u$$

or, in other words

$$(au) \in B$$

However, a is in a 3-cycle and u in a 9-cycle of $E \circ B$, so by Part (2) of Rejewski's theorem, (au) couldn't have been in B. So the first intercept is not an encryption of aaa.

For the second intercept to be a repeated encryption of aaa, (aj) must be in B. But since j is in a 9-cycle of $E \circ B$, this is again impossible

However, in the third intercept we have y and c in the second and fifth positions, so they could well be encryptions of a, because it is in one of the 3-cycles of $E \circ B$ while y and c are in the other. Moreover, in $F \circ C$, we find a in the left 13-cycle and both x and w in the right 13-cycle. Although this doesn't prove that *syc scw* is the encryption of *aaa aaa*, it is strong evidence.

How does Rejewski test whether this evidence is conclusive? For this he uses Part (3) of his theorem: the assumption that $(ax) \in C$ leads to the complete determination of C! Similarly, the assumption that $(ay) \in B$ means that $(xg) \in B$ and $(tc) \in B$, so B has been partly determined, and if we knew (or guessed) one other transposition in $E \circ B$ in the 9-cycles of B, we'd have B completely. And this would be done by guessing other three-letter message keys and seeing whether these guesses fit into a coherent determination of A, B and C. As Rejewski says (p.218) : "...a good knowledge of the practice of cryptographers regarding the selection of message keys was necessary...The changing tastes of cryptographers were very carefully followed, and other predilections were uncovered."

This then is the second half of the story of Rejewski's break into the first secret of Enigma, the message keys. He and his co-workers went on to determine the day keys (the configuration of the rotors and plugboard) and even the wirings of the rotating and fixed drums, again using information from the encrypted message keys. Like the discovery of the message keys, the rest of Enigma was broken into pieces, in spite of its appearance as an integral whole. All this was done without anything but a model of Enigma.

And it was all made possible, not by a design flaw in Enigma, but rather by the German decision to repeatedly encrypt the message keys.