Permutation Groups and the Solution of German Enigma Cipher

Jiří Tůma

tuma@karlin.mff.cuni.cz

Charles University, Prague, Czech Republic

How do cipher systems work?

Őluİouèký kùò. The sender starts with a **plain text**. Then with the help of a **key** he produces a **cipher text**. The cipher text is created from the plain text and the key by an algorithm. This process is called **encryption**.

How do cipher systems work?

Őluİouèký kùò. The sender starts with a **plain text**. Then with the help of a **key** he produces a **cipher text**. The cipher text is created from the plain text and the key by an algorithm. This process is called **encryption**.

The authorized addressee knows the encryption algorithm and the key and deciphers the plain text from the cipher text and the key. The reverse process is called **decryption**.

How do cipher systems work?

Őluİouèký kùò. The sender starts with a **plain text**. Then with the help of a **key** he produces a **cipher text**. The cipher text is created from the plain text and the key by an algorithm. This process is called **encryption**.

The authorized addressee knows the encryption algorithm and the key and deciphers the plain text from the cipher text and the key. The reverse process is called **decryption**.

An adversary may intercept the cipher text and attempt to recover the original plain text from it. This is called **solving the cipher**, informally **codebreaking**.

Maxims of cryptology

- **Never** use the same key to encrypt two different messages;

Maxims of cryptology

- **Never** use the same key to encrypt two different messages;
- **Never** encrypt the same message twice with two different keys;

Maxims of cryptology

- **Never** use the same key to encrypt two different messages;
- **Never** encrypt the same message twice with two different keys;
- **Always** assume that the adversary knows the encryption algorithm;

Maxims of cryptology

- **Never** use the same key to encrypt two different messages;
- **Never** encrypt the same message twice with two different keys;
- **Always** assume that the adversary knows the encryption algorithm;
- **Never** underrate the adversary.

Indicators

Security of a cipher system depends mainly on **key-exchange**, the way in which the sender and the authorized addressee exchange the message key.

Indicators

Security of a cipher system depends mainly on **key-exchange**, the way in which the sender and the authorized addressee exchange the message key.

They agree in advance on a position in the cipher text that will contain information from which the message key can be recovered. This information is called an **indicator**. The indicator is most often placed at the beginning of the cipher text. The indicator is usually not given in plain text but it is also enciphered in some way.

Indicators

Security of a cipher system depends mainly on **key-exchange**, the way in which the sender and the authorized addressee exchange the message key.

They agree in advance on a position in the cipher text that will contain information from which the message key can be recovered. This information is called an **indicator**. The indicator is most often placed at the beginning of the cipher text. The indicator is usually not given in plain text but it is also enciphered in some way.

Thus a cipher text usually has the form

```
indicator messagetext
```

Enigma, first contacts

From 1928 the German army *Wehrmacht* started to test a new cipher system. This caused panic in the ranks of the Polish Secret Service. After the end of the First World War France and Great Britain believed that Germany was no longer a threat to their security. However, Poland never shared this opinion.

Enigma, first contacts

From 1928 the German army *Wehrmacht* started to test a new cipher system. This caused panic in the ranks of the Polish Secret Service. After the end of the First World War France and Great Britain believed that Germany was no longer a threat to their security. However, Poland never shared this opinion.

Attempts to solve the new cipher had been completely unsuccessful for several years. Even parapsychology was involved but in vain. Finally, someone in the Polish Secret Service got the idea that mathematicians could be useful. A course in cryptanalysis was organized for students of mathematics at the University of Poznan.

Young Polish mathematicians

Three of the best graduates of the course,

Marian Rejewski (1905-1980),
Henryk Zygalski (1906-1978) and
Jerzy Rózycki (1907-1942)
then accepted the offer to work on cryptanalysis of the new cipher.

First results

Various statistical tests were applied to the intercepted cipher texts. As a result it became clear that the **first six letters** of each cipher text **formed the indicator**.

First results

Various statistical tests were applied to the intercepted cipher texts. As a result it became clear that the **first six letters** of each cipher text **formed the indicator**.

The statistical tests (mainly the **index of coincidence**) also suggested that the cipher is very probably a **polyalphabetic cipher**. This means that every letter of the plain text is replaced by a single corresponding letter in the cipher text. The cipher letter depends not only on the plain letter it replaces but also on its position in the plain text.

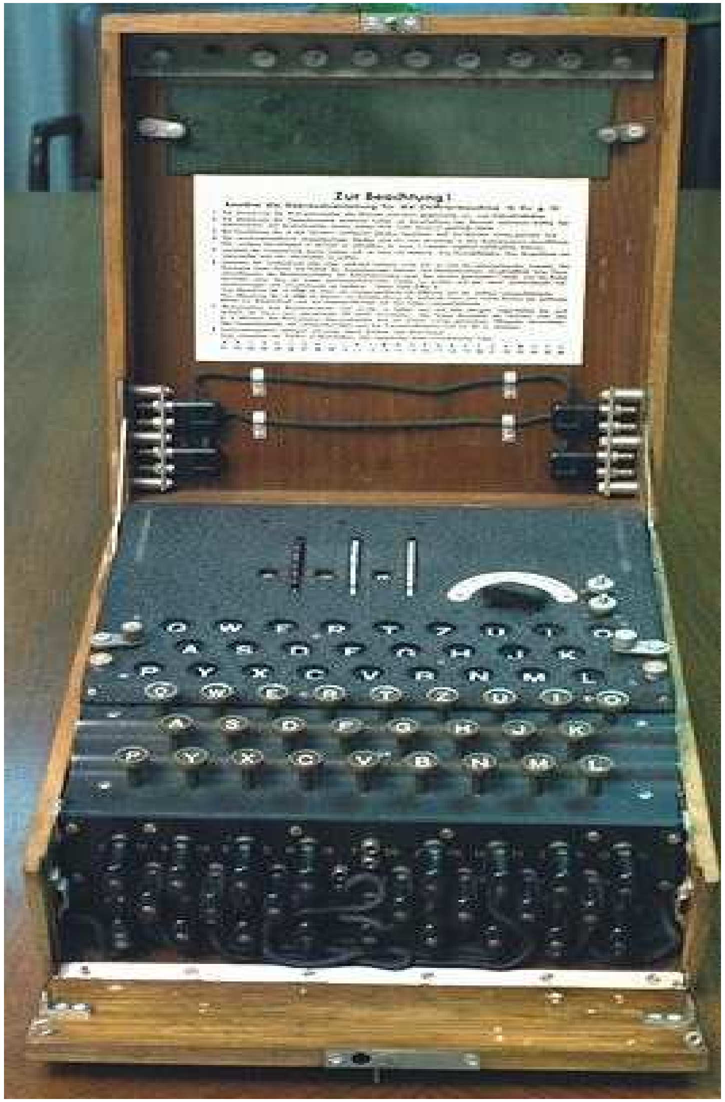
First results

Various statistical tests were applied to the intercepted cipher texts. As a result it became clear that the **first six letters** of each cipher text **formed the indicator**.

The statistical tests (mainly the **index of coincidence**) also suggested that the cipher is very probably a **polyalphabetic cipher**. This means that every letter of the plain text is replaced by a single corresponding letter in the cipher text. The cipher letter depends not only on the plain letter it replaces but also on its position in the plain text.

A similar cipher was produced by a commercial machine **Enigma** that had been on sale since 1926. So the Polish Intelligence Service hypothesized that the new cipher was produced by a military version of the **Enigma** machine.

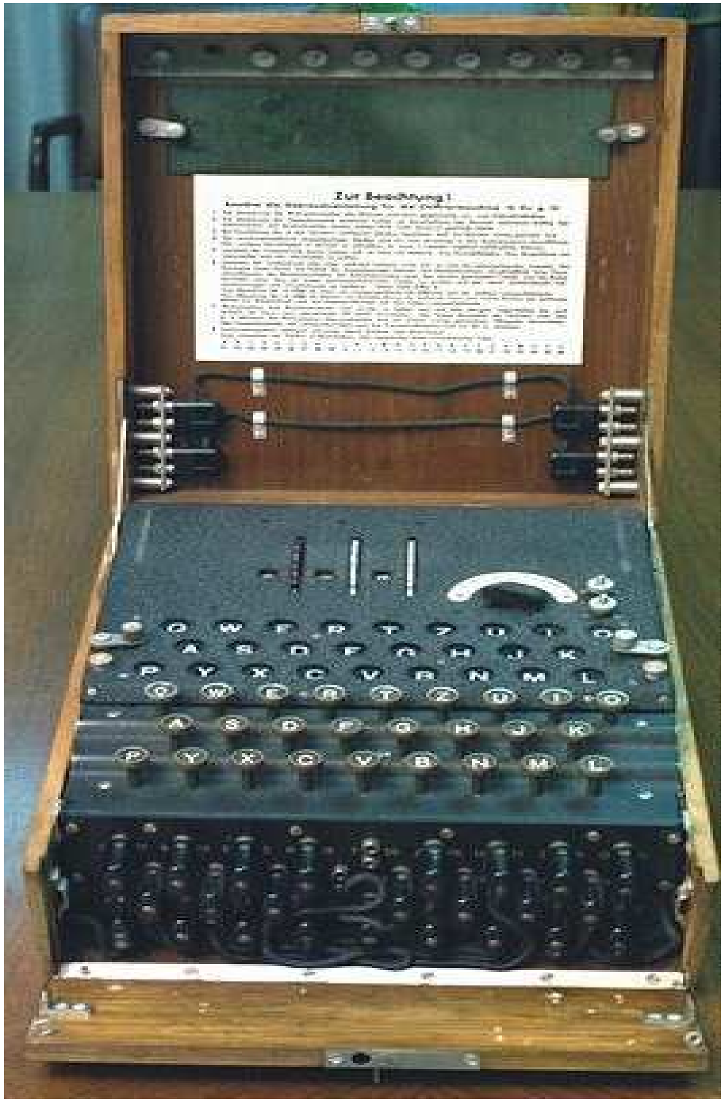
Military Enigma



Important parts of the machine are

- keyboard,

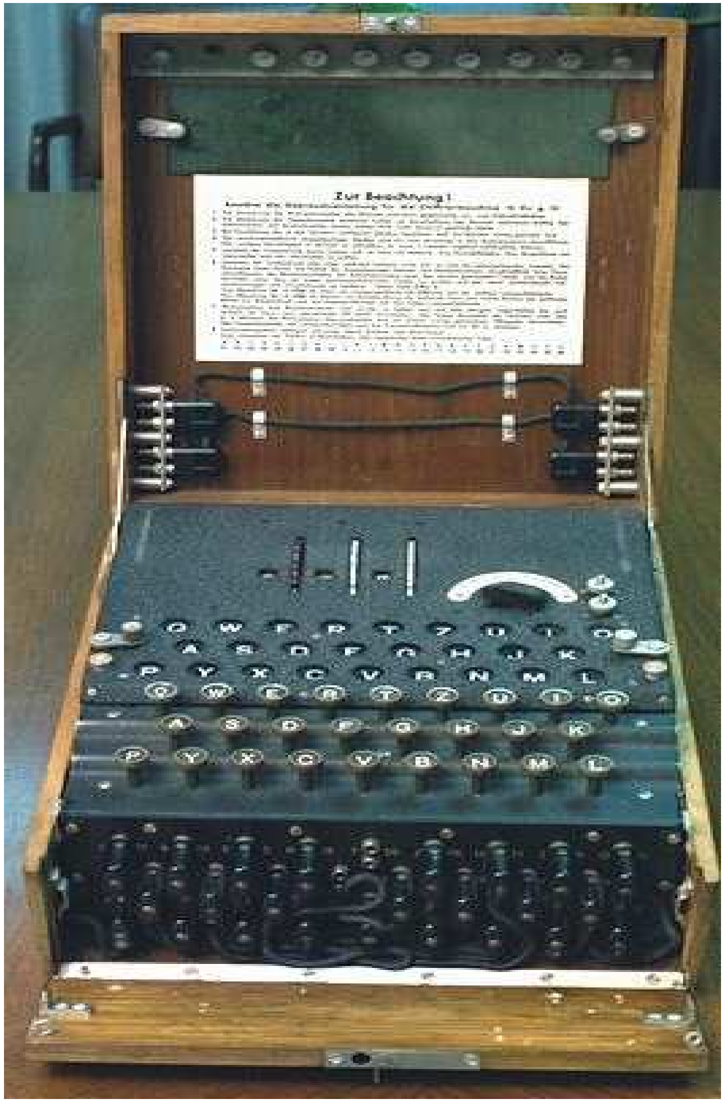
Military Enigma



Important parts of the machine are

- keyboard,
- bulbs,

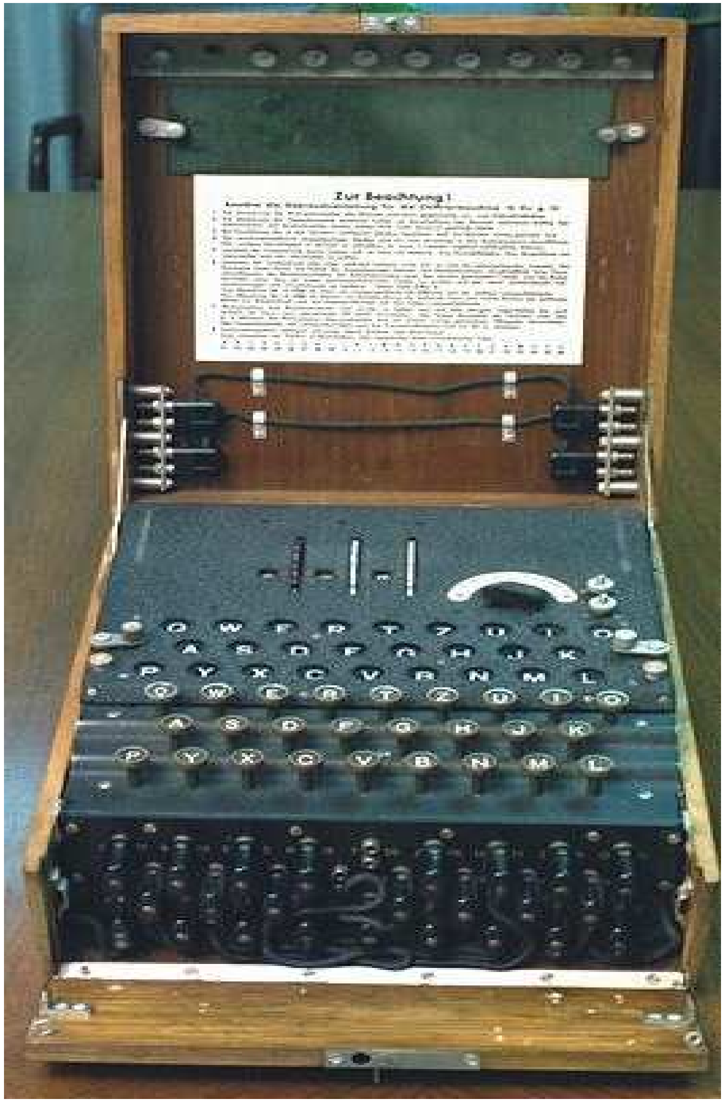
Military Enigma



Important parts of the machine are

- keyboard,
- bulbs,
- plug board (stecker board),

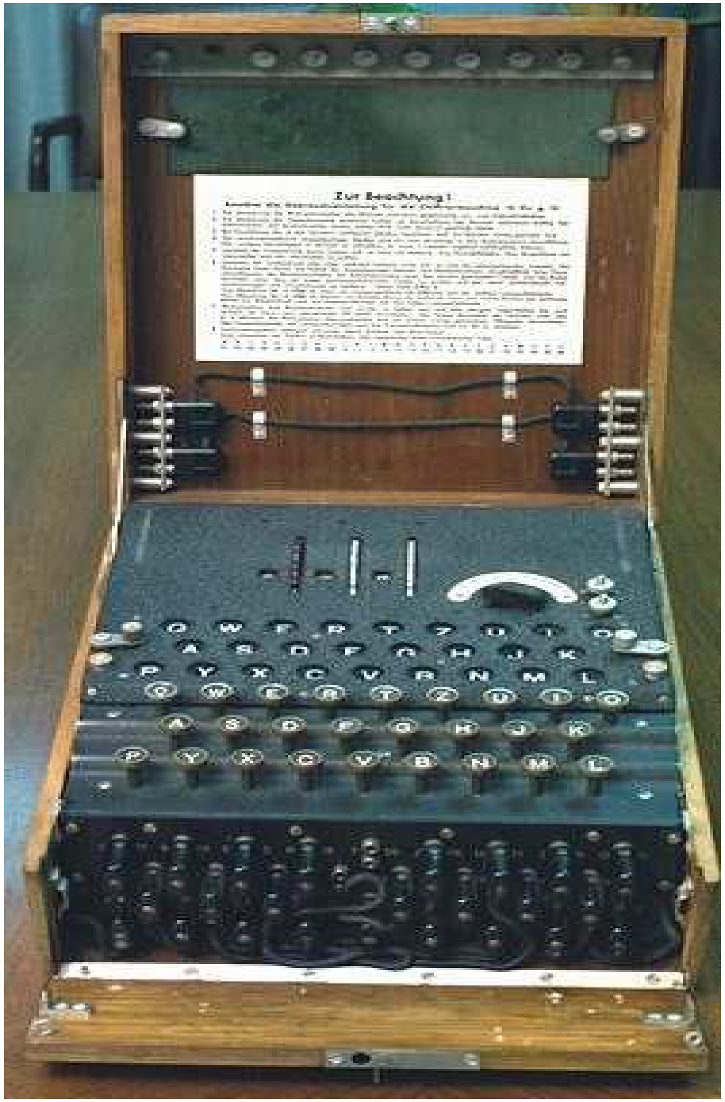
Military Enigma



Important parts of the machine are

- keyboard,
- bulbs,
- plug board (stecker board),
- scrambler,

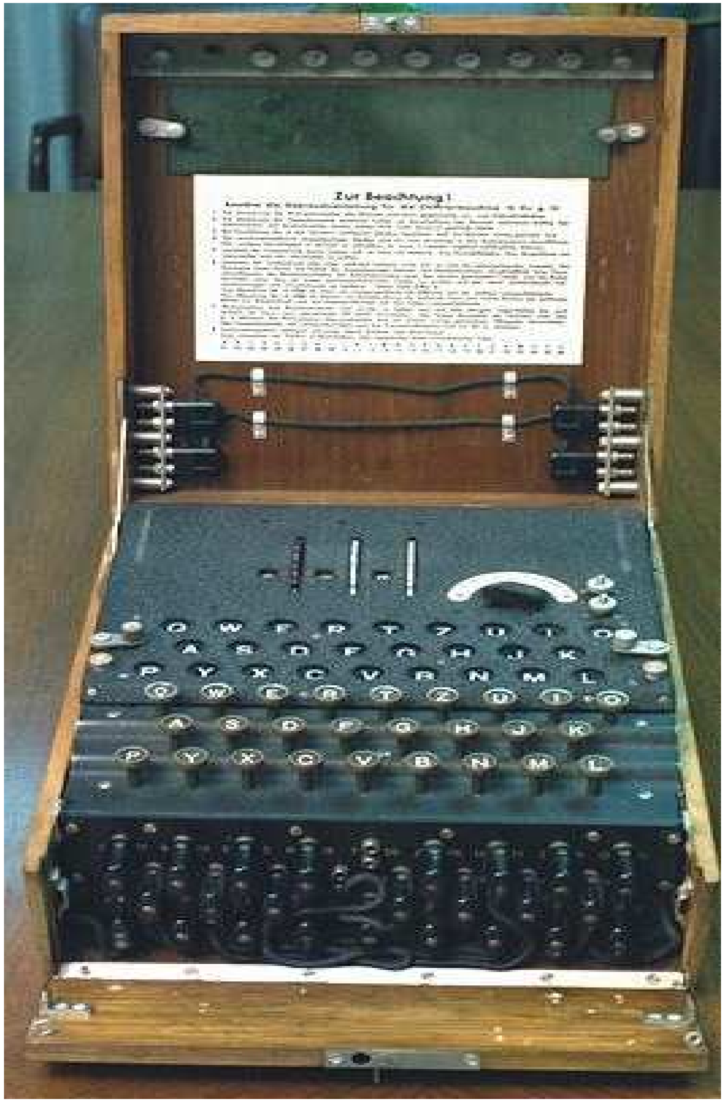
Military Enigma



Important parts of the machine are

- keyboard,
- bulbs,
- plug board (stecker board),
- scrambler,
- entry wheel,

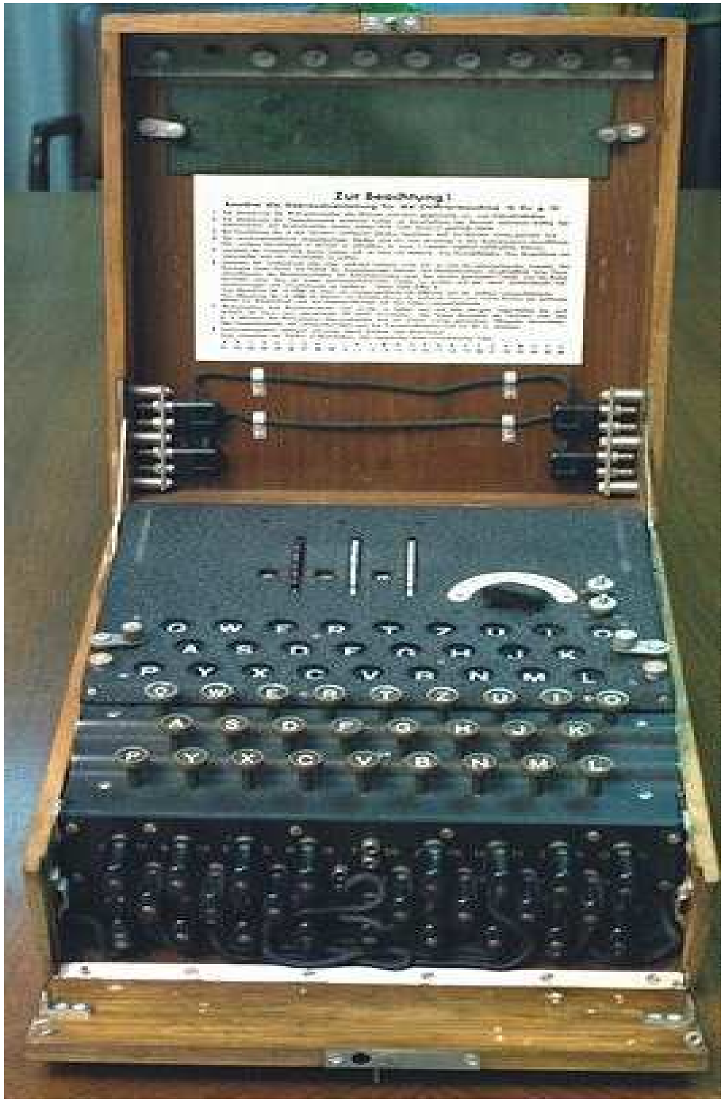
Military Enigma



Important parts of the machine are

- keyboard,
- bulbs,
- plug board (stecker board),
- scrambler,
- entry wheel,
- rotor,

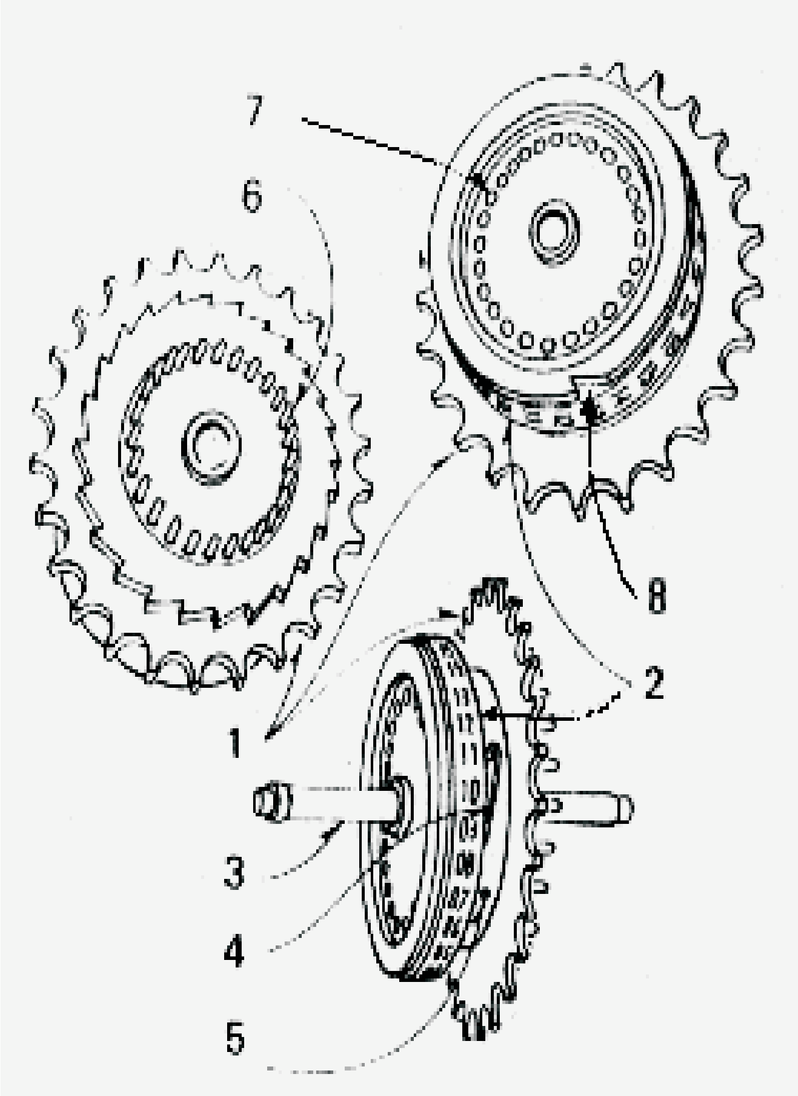
Military Enigma



Important parts of the machine are

- keyboard,
- bulbs,
- plug board (stecker board),
- scrambler,
- entry wheel,
- rotor,
- reflector (Umkehrwalze).

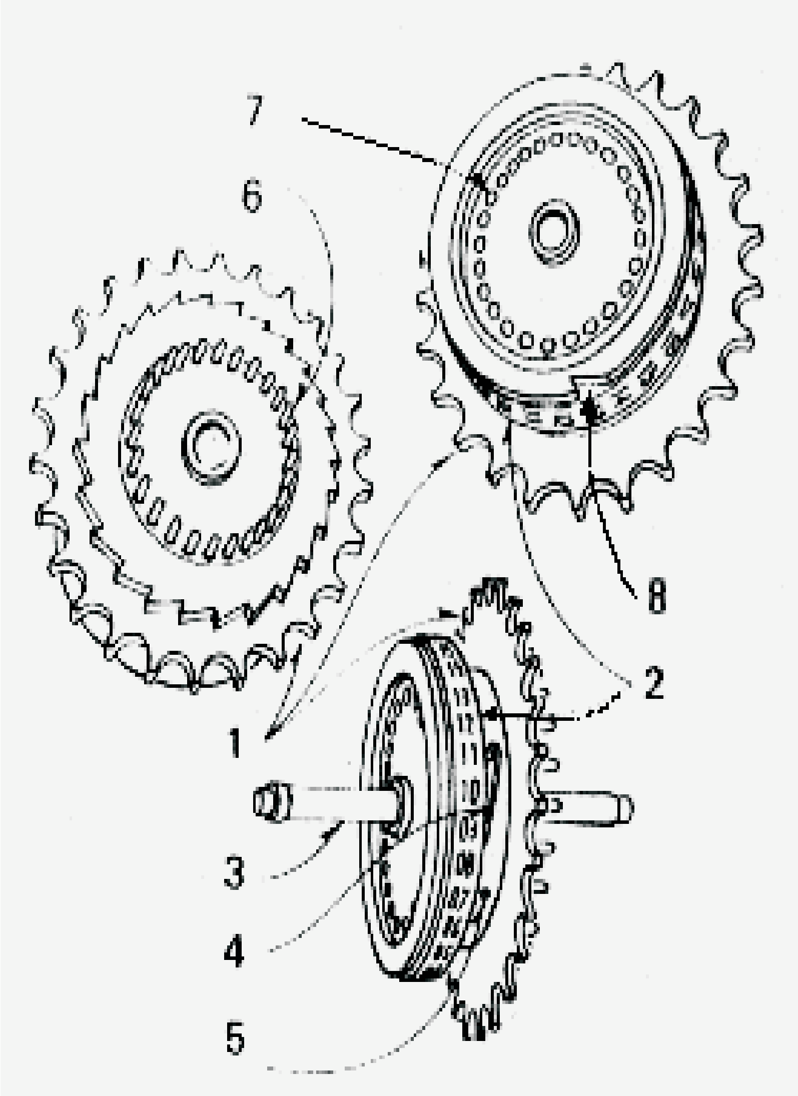
Rotors



Here is the structure of the rotors

- finger notches,

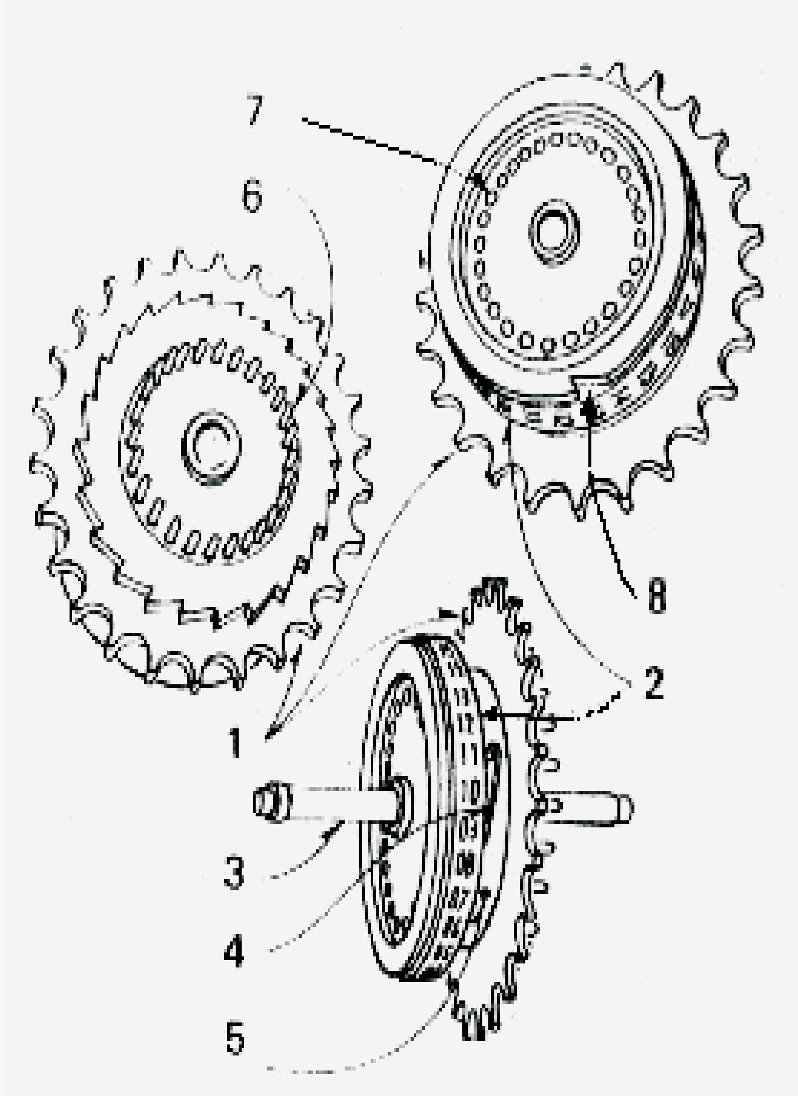
Rotors



Here is the structure of the rotors

- finger notches,
- alphabet ring,

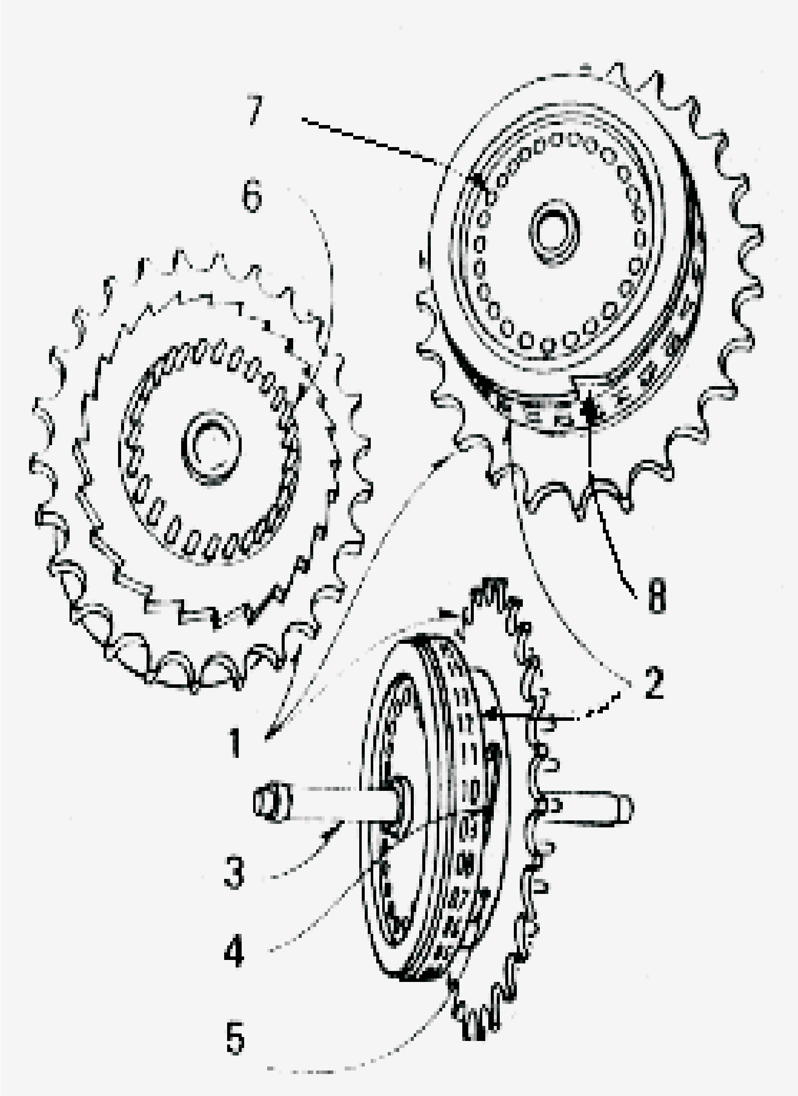
Rotors



Here is the structure of the rotors

- finger notches,
- alphabet ring,
- shaft,

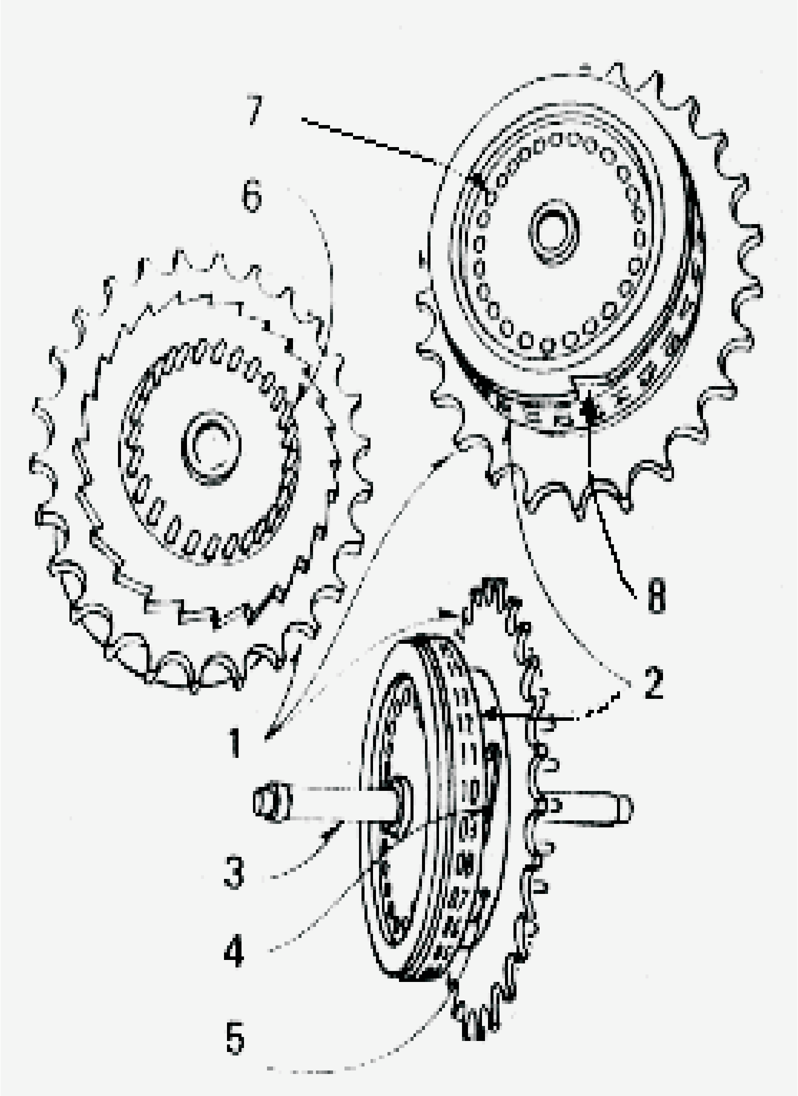
Rotors



Here is the structure of the rotors

- finger notches,
- alphabet ring,
- shaft,
- catch,

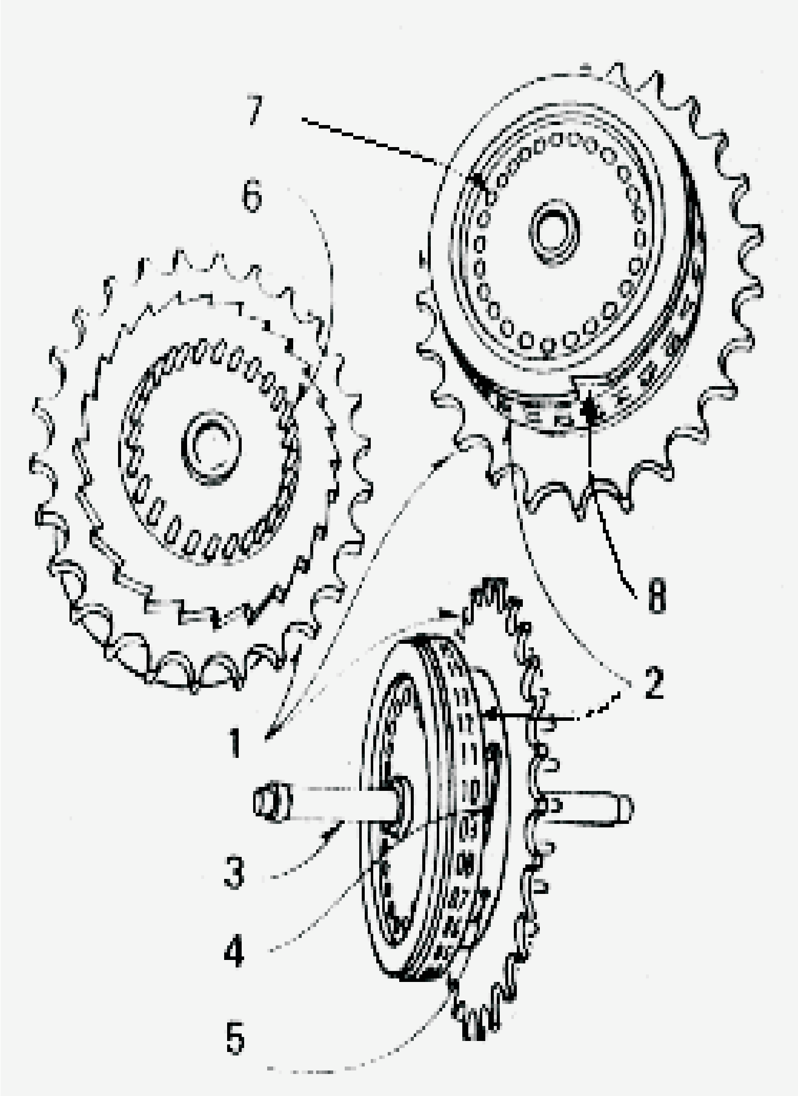
Rotors



Here is the structure of the rotors

- finger notches,
- alphabet ring,
- shaft,
- catch,
- core containing cross-wirings,

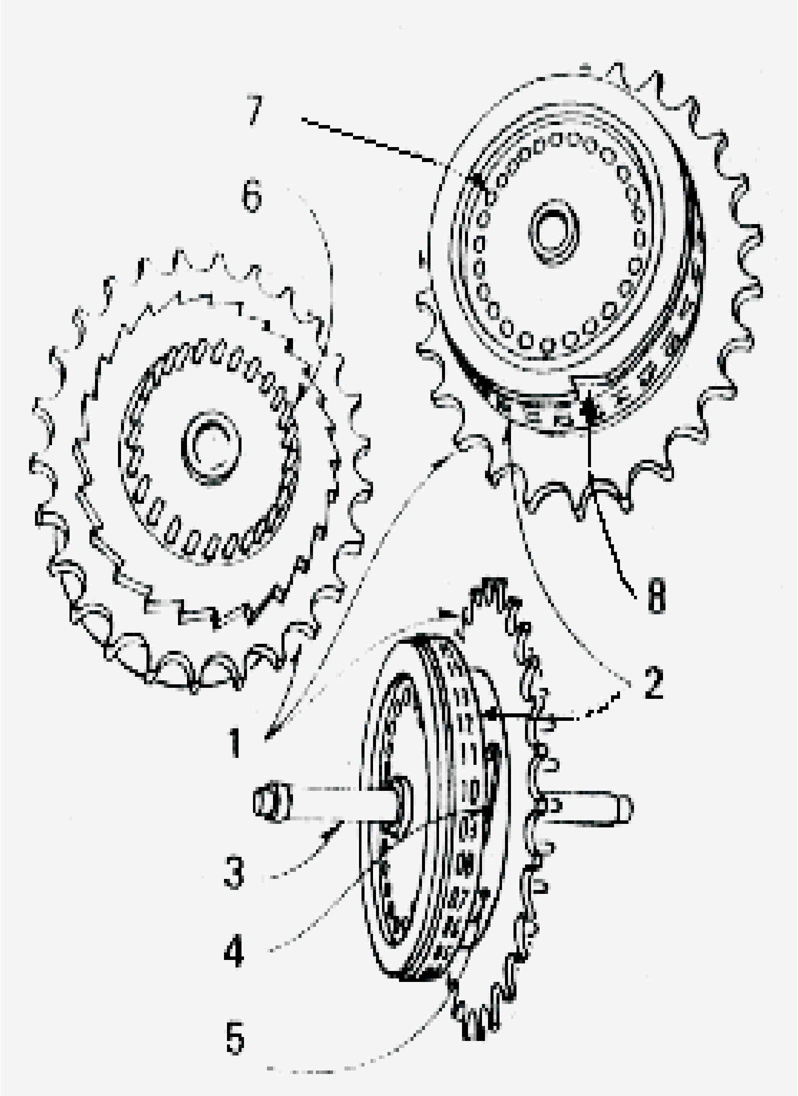
Rotors



Here is the structure of the rotors

- finger notches,
- alphabet ring,
- shaft,
- catch,
- core containing cross-wirings,
- spring loaded contacts,

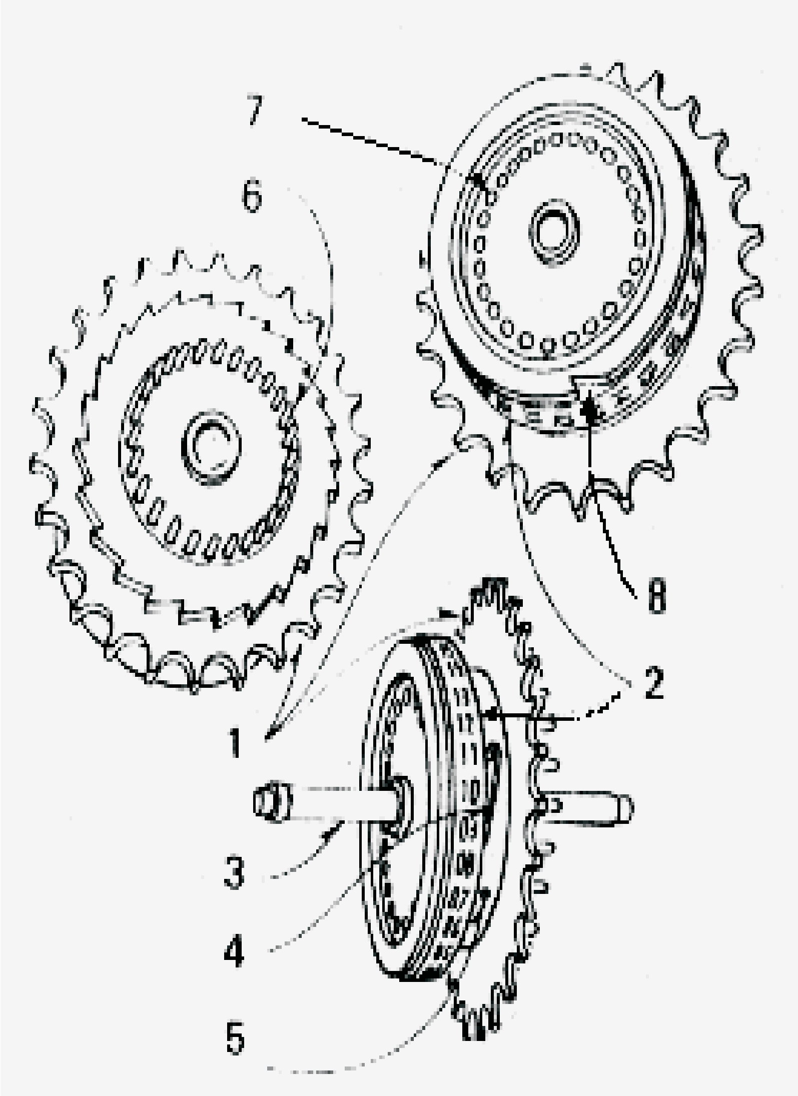
Rotors



Here is the structure of the rotors

- finger notches,
- alphabet ring,
- shaft,
- catch,
- core containing cross-wirings,
- spring loaded contacts,
- discs,

Rotors



Here is the structure of the rotors

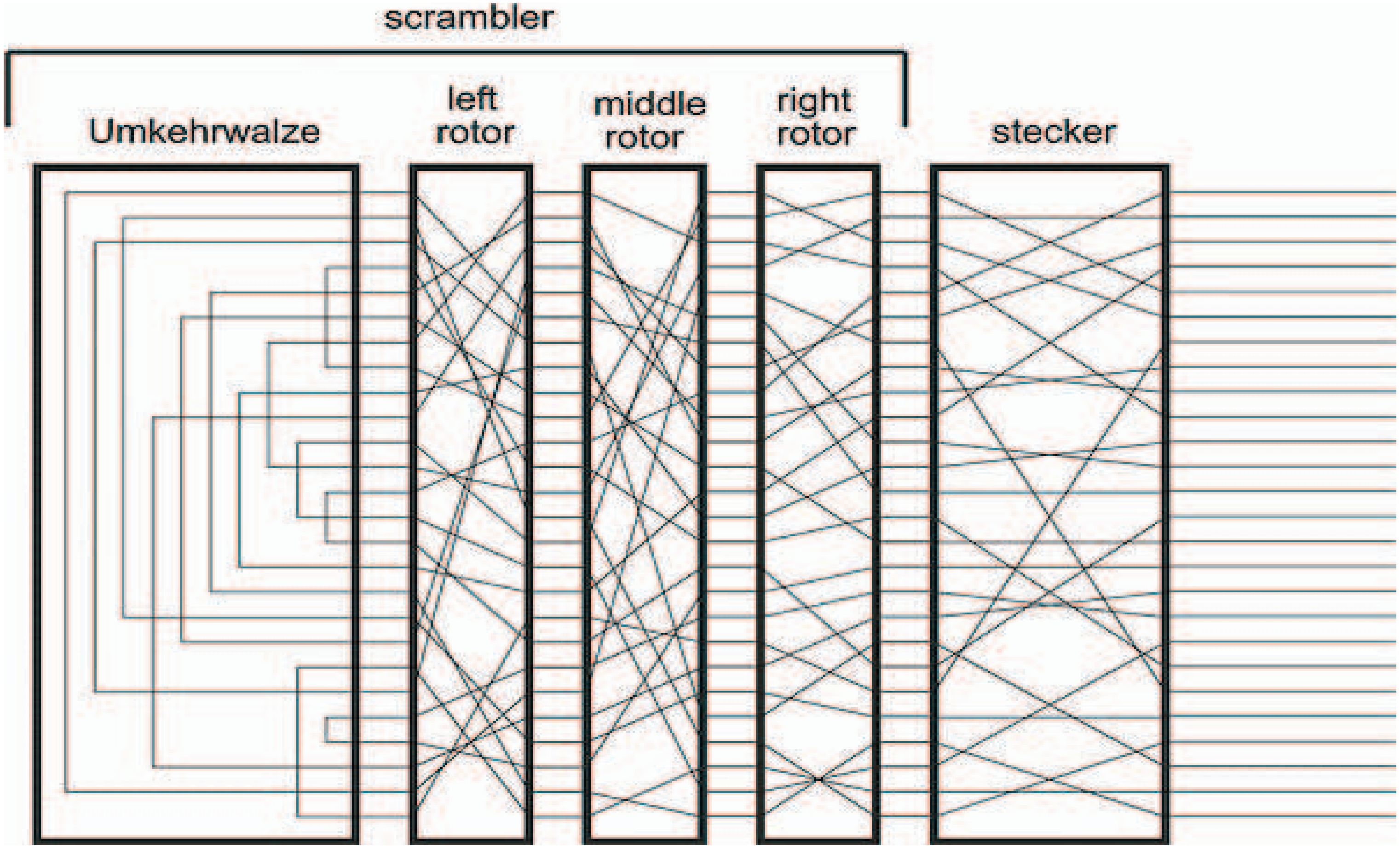
- finger notches,
- alphabet ring,
- shaft,
- catch,
- core containing cross-wirings,
- spring loaded contacts,
- discs,
- carry notch.

Wiring of Enigma

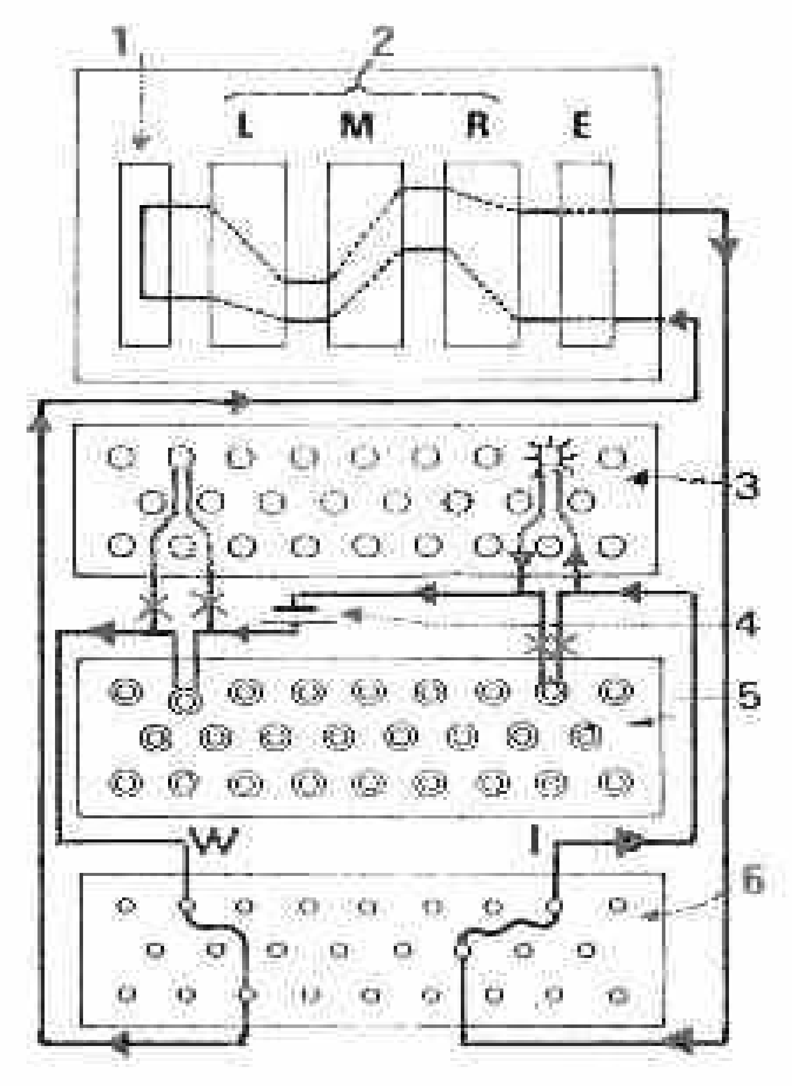
The wiring of the military version of the Enigma machine can be schematized in the following way.

Wiring of Enigma

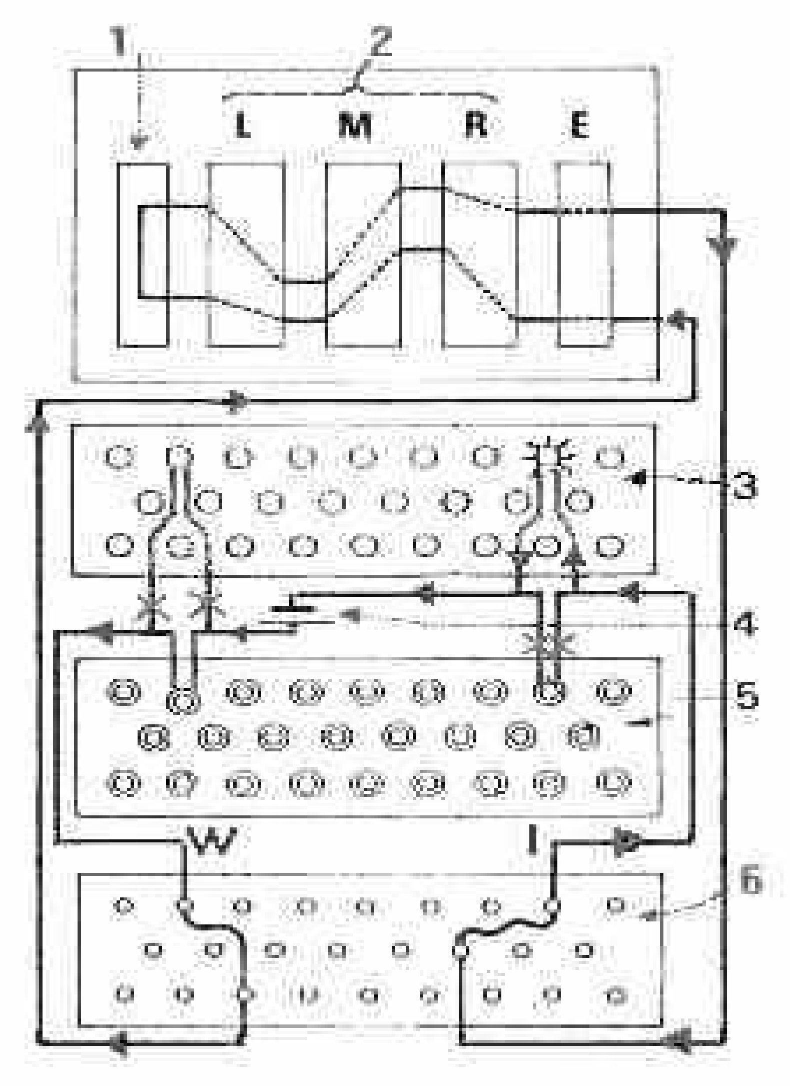
The wiring of the military version of the Enigma machine can be schematized in the following way.



Flow of current



Flow of current



This is how the current flows through the Enigma machine after pressing a key.

Operation manual

The operation manual was obtained through French espionage and passed to the Polish Intelligence Service in December 1932.

Operation manual

The operation manual was obtained through French espionage and passed to the Polish Intelligence Service in December 1932.

It contained the information needed to set up the machine using the **daily key**. The daily key consisted of

Operation manual

The operation manual was obtained through French espionage and passed to the Polish Intelligence Service in December 1932.

It contained the information needed to set up the machine using the **daily key**. The daily key consisted of

the order of the rotors: e.g. `II,III,I`;

Operation manual

The operation manual was obtained through French espionage and passed to the Polish Intelligence Service in December 1932.

It contained the information needed to set up the machine using the **daily key**. The daily key consisted of

the order of the rotors: e.g. `II,III,I`;

the position of the rings on the rotors: e.g. KUB;

Operation manual

The operation manual was obtained through French espionage and passed to the Polish Intelligence Service in December 1932.

It contained the information needed to set up the machine using the **daily key**. The daily key consisted of

the order of the rotors: e.g. `II,III,I`;

the position of the rings on the rotors: e.g. `KUB`;

the plug board connections: e.g. `AU,CR,DK,JZ,LN,PS`;

Operation manual

The operation manual was obtained through French espionage and passed to the Polish Intelligence Service in December 1932.

It contained the information needed to set up the machine using the **daily key**. The daily key consisted of

the order of the rotors: e.g. `II,III,I`;

the position of the rings on the rotors: e.g. `KUB`;

the plug board connections: e.g. `AU,CR,DK,JZ,LN,PS`;

the basic setting, letters visible in the little windows: e.g. `UFW`.

The message key

After setting up the machine with the use of the daily key, the operator was supposed to choose randomly three letters called the **message key**, e.g. HTS.

The message key

After setting up the machine with the use of the daily key, the operator was supposed to choose randomly three letters called the **message key**, e.g. `HTS`.

Then he wrote the message key twice, i.e. `HTS HTS`.

The message key

After setting up the machine with the use of the daily key, the operator was supposed to choose randomly three letters called the **message key**, e.g. `HTS`.

Then he wrote the message key twice, i.e. `HTS HTS`.

Then he encrypted these six letters by pressing the corresponding six keys on the keyboard and wrote down the cipher text. He obtained the cipher version of the message key, the indicator, e.g. the message key `HTS HTS` was encrypted as `NEV GWY.`

The message key

After setting up the machine with the use of the daily key, the operator was supposed to choose randomly three letters called the **message key**, e.g. HTS.

Then he wrote the message key twice, i.e. HTS HTS.

Then he encrypted these six letters by pressing the corresponding six keys on the keyboard and wrote down the cipher text. He obtained the cipher version of the message key, the indicator, e.g. the message key HTS HTS was encrypted as NEV GWY.

Then he turned the rotors to see the message key letters in the small windows, and continued with encrypting the message text from the position given by the message key.

The message key

After setting up the machine with the use of the daily key, the operator was supposed to choose randomly three letters called the **message key**, e.g. `HTS`.

Then he wrote the message key twice, i.e. `HTS HTS`.

Then he encrypted these six letters by pressing the corresponding six keys on the keyboard and wrote down the cipher text. He obtained the cipher version of the message key, the indicator, e.g. the message key `HTS HTS` was encrypted as `NEV GWY.`

Then he turned the rotors to see the message key letters in the small windows, and continued with encrypting the message text from the position given by the message key.

Thus the message `HELLO` was encrypted as `BPTQS`.

Violation of cryptological maxims

Finally, he passed the indicator and the cipher text to the radio operator. The whole encrypted message `HELLO` was thus transmitted as

`NEV GWY BPTQS`

Violation of cryptological maxims

Finally, he passed the indicator and the cipher text to the radio operator. The whole encrypted message `HELLO` was thus transmitted as

```
NEV GWY BPTQS
```

The rules violated two of the cryptological maxims.

Violation of cryptological maxims

Finally, he passed the indicator and the cipher text to the radio operator. The whole encrypted message `HELLO` was thus transmitted as

`NEV GWY BPTQS`

The rules violated two of the cryptological maxims.

All message keys during the same day were encrypted with the **same daily key**.

Violation of cryptological maxims

Finally, he passed the indicator and the cipher text to the radio operator. The whole encrypted message `HELLO` was thus transmitted as

`NEV GWY BPTQS`

The rules violated two of the cryptological maxims.

All message keys during the same day were encrypted with the **same daily key**.

Each particular message key was encrypted **twice with different keys**.

Violation of cryptological maxims

Finally, he passed the indicator and the cipher text to the radio operator. The whole encrypted message HELLO was thus transmitted as

NEV GWY BPTQS

The rules violated two of the cryptological maxims.

All message keys during the same day were encrypted with the **same daily key**.

Each particular message key was encrypted **twice with different keys**.

The violation of two cryptological maxims was the starting point of a mathematical analysis of the Enigma cipher. Could this open the door to solve the cipher?

The situation in December 1932

Let us summarize the information available to Marian Rejewski at that time:

The situation in December 1932

Let us summarize the information available to Marian Rejewski at that time:

a commercial version of the Enigma machine (without the plug board and certainly with different wirings inside the rotors and the reflector),

The situation in December 1932

Let us summarize the information available to Marian Rejewski at that time:

a commercial version of the Enigma machine (without the plug board and certainly with different wirings inside the rotors and the reflector),

the operation manual containing also an example of a plain text and its enciphered version with a given daily key and a message key,

The situation in December 1932

Let us summarize the information available to Marian Rejewski at that time:

a commercial version of the Enigma machine (without the plug board and certainly with different wirings inside the rotors and the reflector),

the operation manual containing also an example of a plain text and its enciphered version with a given daily key and a message key,

daily keys for September and October 1932. **Important:** the daily keys were from two different quarters of the year,

The situation in December 1932

Let us summarize the information available to Marian Rejewski at that time:

a commercial version of the Enigma machine (without the plug board and certainly with different wirings inside the rotors and the reflector),

the operation manual containing also an example of a plain text and its enciphered version with a given daily key and a message key,

daily keys for September and October 1932. **Important:** the daily keys were from two different quarters of the year,

and several dozens intercepted encrypted messages from each day of these two months.

Permutations

The (unknown) wiring inside a rotor (or the reflector) can be described by the mathematical concept of a **permutation**.

Permutations

The (unknown) wiring inside a rotor (or the reflector) can be described by the mathematical concept of a **permutation**.

Definition. A one-to-one mapping on a set X is called a **permutation** on the set X.

Permutations

The (unknown) wiring inside a rotor (or the reflector) can be described by the mathematical concept of a **permutation**.

Definition. A one-to-one mapping on a set X is called a **permutation** on the set X.

The value of a permutation P at a point x will be written as xP. Every permutation P on a set X uniquely defines the **inverse permutation** P^{-1}. This is determined by the property

$$(xP)P^{-1} = x$$

for every $x \in X$.

Product of permutations

Any two permutations P, Q on the same set X can be composed (as mappings) to get the **composition** or **product** PQ of the two permutations. Its value at a given element $x \in X$ is

$$x(PQ) = (xP)Q.$$

Product of permutations

Any two permutations P, Q on the same set X can be composed (as mappings) to get the **composition** or **product** PQ of the two permutations. Its value at a given element $x \in X$ is

$$x(PQ) = (xP)Q.$$

The **identity permutation** I on X is defined by

$$xI = x$$

for every $x \in X$.

Product of permutations

Any two permutations P, Q on the same set X can be composed (as mappings) to get the **composition** or **product** PQ of the two permutations. Its value at a given element $x \in X$ is

$$x(PQ) = (xP)Q.$$

The **identity permutation** I on X is defined by

$$xI = x$$

for every $x \in X$.

Thus $PP^{-1} = I = P^{-1}P$ for every permutation P on X.

Graph of a permutation

We can visualize permutations by drawing their **graphs**.

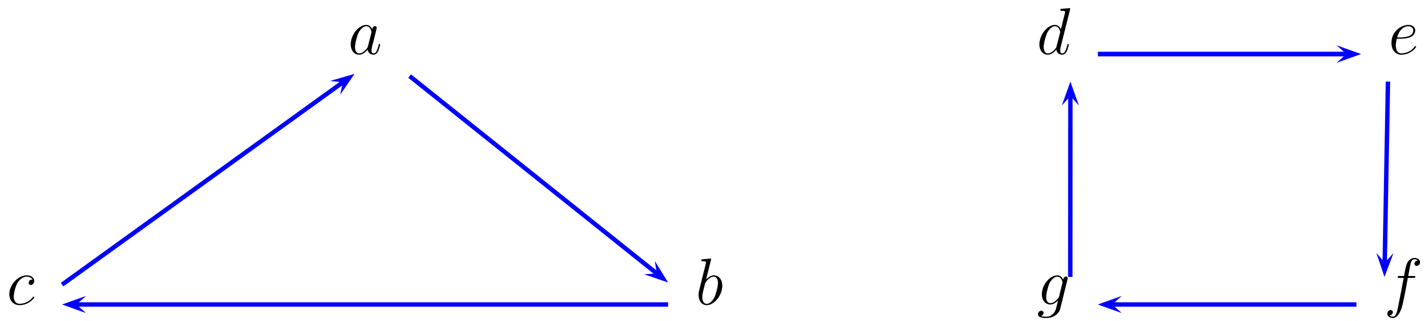
Graph of a permutation

We can visualize permutations by drawing their **graphs**.

For example, the permutation P on the set $\{a, b, c, d, e, f, g\}$ defined by

$$aP = b, bP = c, cP = a, dP = e, eP = f, fP = g, gP = d,$$

can be visualized as

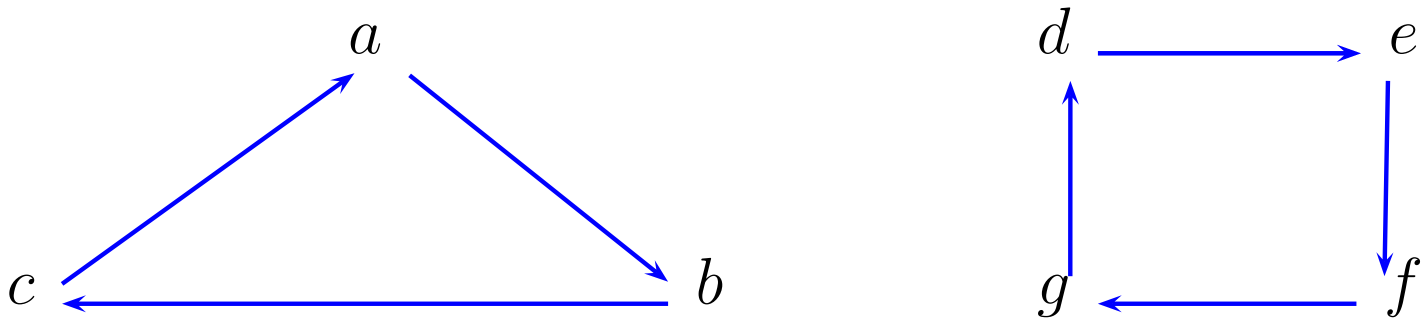


Graph of the composition

If we want to find the graph of the product PQ of the permutation p with another permutation Q defined by

$$aQ = d, bQ = a, cQ = g, dQ = f, eQ = e, fQ = b, gQ = c,$$

we first draw the graph of P.



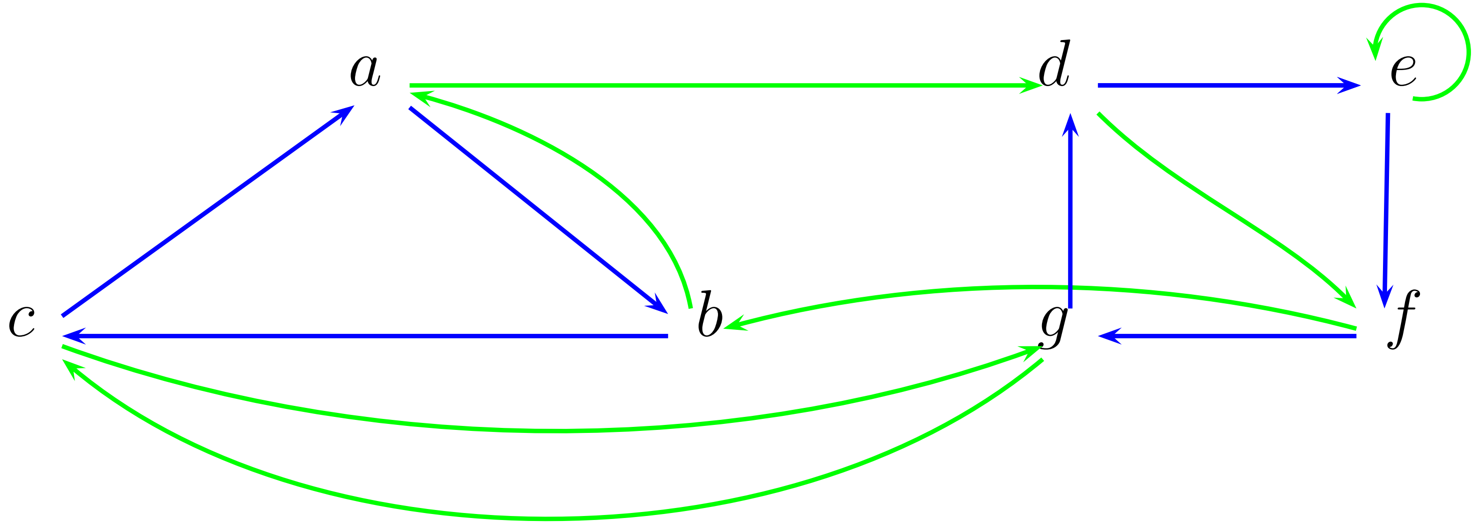
Graph of the composition

If we want to find the graph of the product PQ of the permutation p with another permutation Q defined by

$$aQ = d, bQ = a, cQ = g, dQ = f, eQ = e, fQ = b, gQ = c,$$

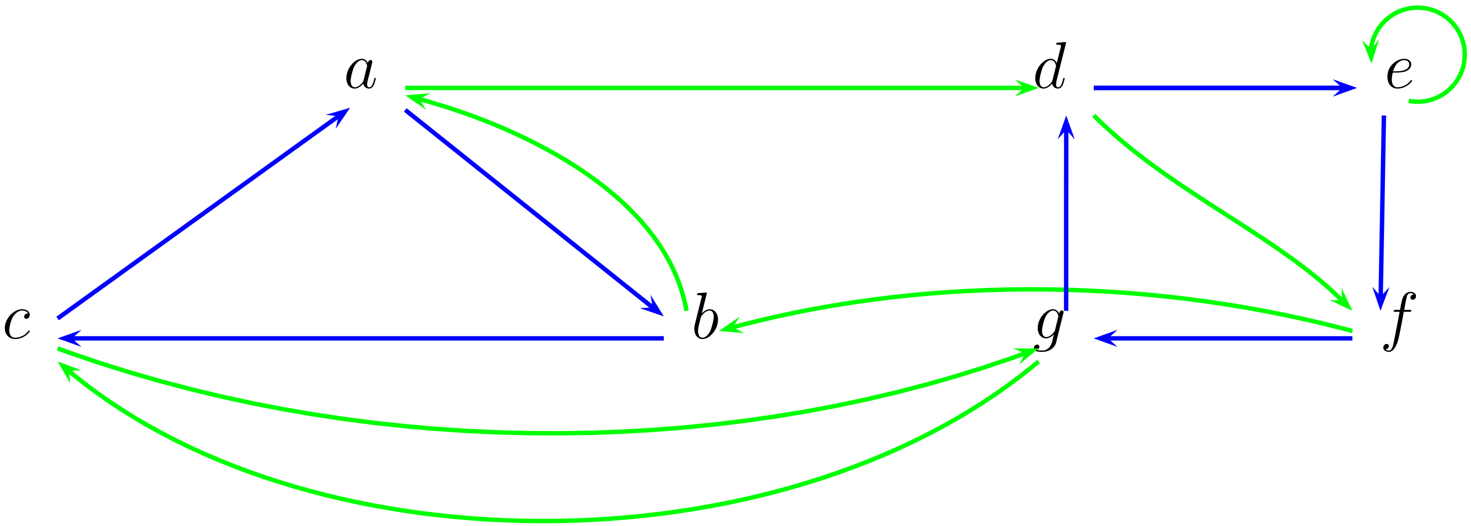
we first draw the graph of P.

Then we draw the graph of Q to it.



Graph of the composition - cont.

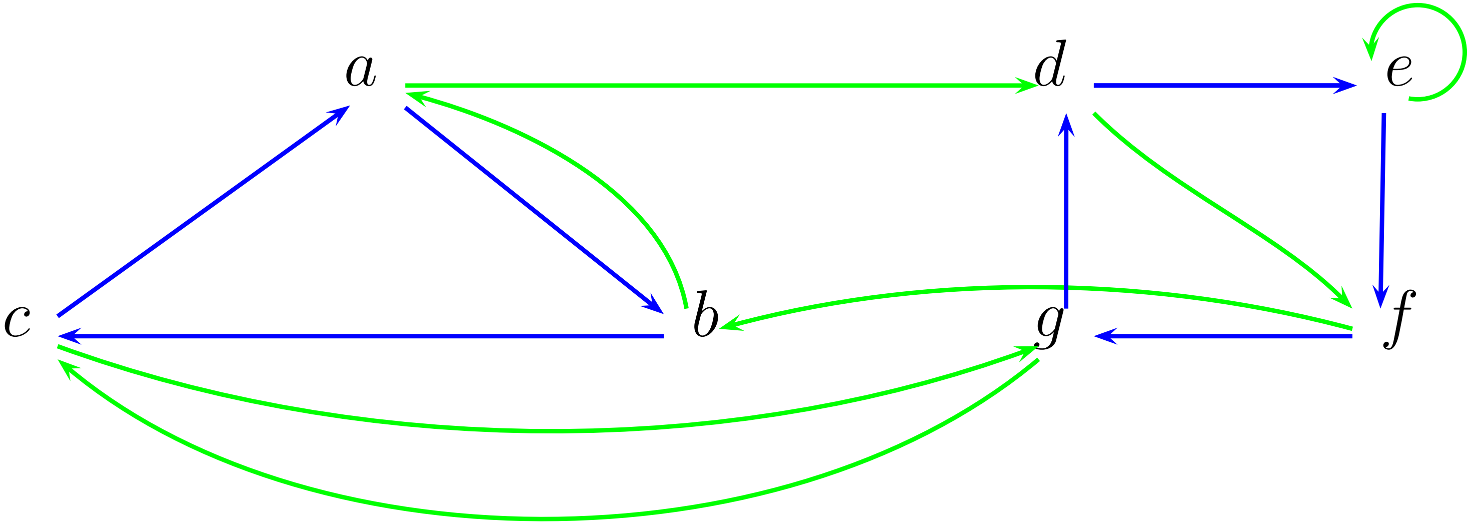
To get an arrow in the graph of the product PQ from a given element, we first follow the arrow of P and then continue with the arrow of Q.



Graph of the composition - cont.

To get an arrow in the graph of the product PQ from a given element, we first follow the arrow of P and then continue with the arrow of Q.

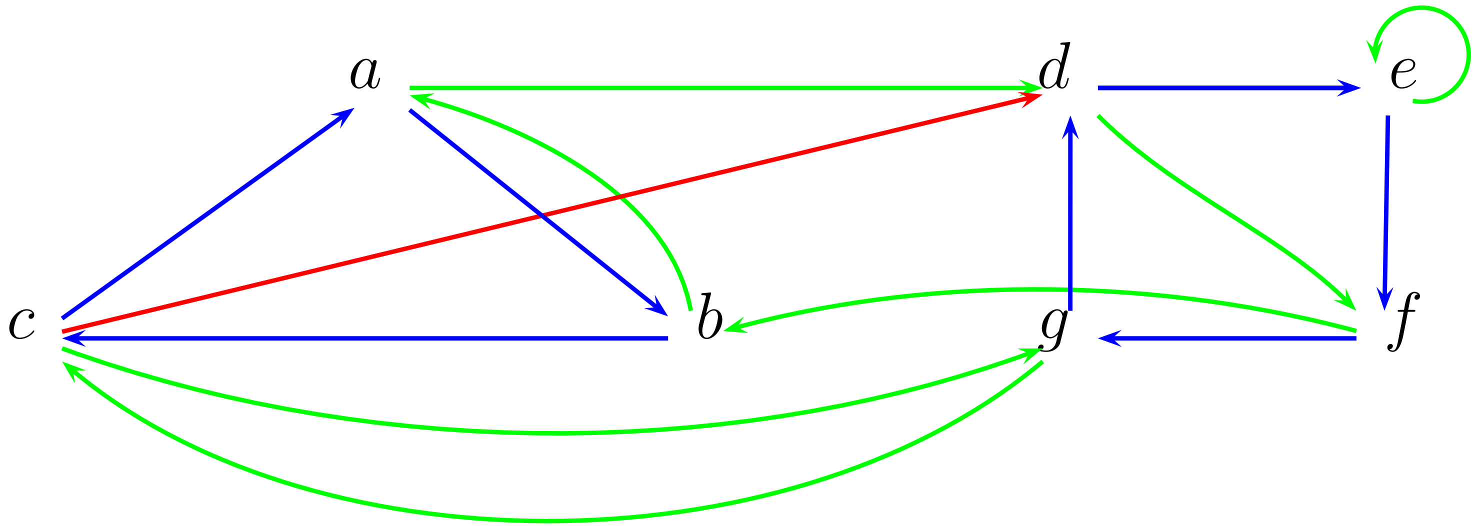
Here is how it works for the element c.



Graph of the composition - cont.

To get an arrow in the graph of the product PQ from a given element, we first follow the arrow of P and then continue with the arrow of Q.

Here is how it works for the element c.

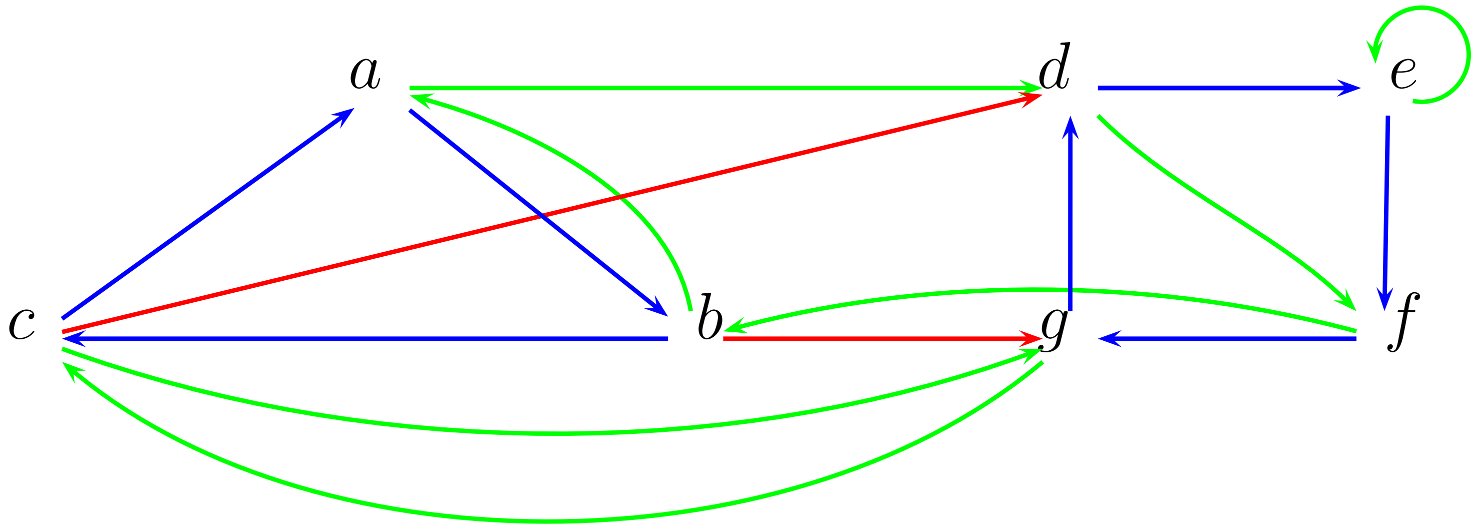


Graph of the composition - cont.

To get an arrow in the graph of the product PQ from a given element, we first follow the arrow of P and then continue with the arrow of Q.

Here is how it works for the element c.

And for the element b.



Math. model of rotors and reflector

If we take a rotor, we may denote the spring contacts on one side of the rotor by letters of the alphabet $a, b, c, \ldots, x, y, z$. Opposite to each spring contact there is a disc, through which the current flows out of the rotor. We denote it by the same letter as the opposite spring contact. Thus the **wires inside the rotor define** a one-to-one mapping, or **a permutation**, on the alphabet $\{a, b, c, \ldots, x, y, z\}$.

Math. model of rotors and reflector

If we take a rotor, we may denote the spring contacts on one side of the rotor by letters of the alphabet $a, b, c, \dots, x, y, z$. Opposite to each spring contact there is a disc, through which the current flows out of the rotor. We denote it by the same letter as the opposite spring contact. Thus the **wires inside the rotor define** a one-to-one mapping, or **a permutation**, on the alphabet $\{a, b, c, \dots, x, y, z\}$.

Let us denote the permutations that describe the wirings of the left, middle and right rotors by L, M and N.

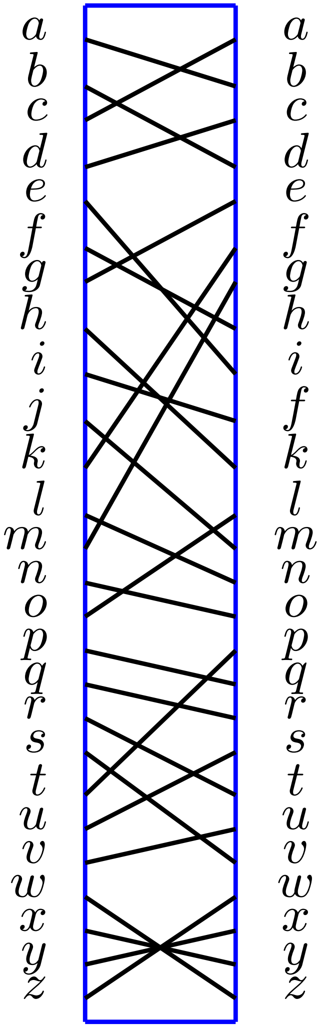
Math. model of rotors and reflector

If we take a rotor, we may denote the spring contacts on one side of the rotor by letters of the alphabet $a, b, c, \ldots, x, y, z$. Opposite to each spring contact there is a disc, through which the current flows out of the rotor. We denote it by the same letter as the opposite spring contact. Thus the **wires inside the rotor define** a one-to-one mapping, or **a permutation**, on the alphabet $\{a, b, c, \ldots, x, y, z\}$.

Let us denote the permutations that describe the wirings of the left, middle and right rotors by L, M and N.

There are also thirteen wires inside the reflector, each connecting two springs. Thus the wiring inside the **reflector can be described by** another **permutation** R on the alphabet $\{a, b, c, \ldots, x, y, z\}$. This time the permutation R is not arbitrary but has to have 13 cycles of length 2.

Math. model of a rotor


a b c d e f g h i j k l m n o p q r s t u v w x y z
a b c d e f g h i f k l m n o p q r s t u v w x y z

If we take a rotor, we may denote the spring contacts on one side of the rotor by the letters of the alphabet $a, b, c, \ldots, x, y, z$. Opposite to each spring contact there is a disc, through which the current flows out of the rotor. We denote it by the same letter as the opposite spring contact. Thus the wires inside the rotor define a permutation on the alphabet $\{a, b, c, \ldots, x, y, z\}$.

More permutations

Let us denote the permutations that describe the wirings of the left, middle and right rotors by L, M and N.

More permutations

Let us denote the permutations that describe the wirings of the left, middle and right rotors by L, M and N.

There are also thirteen wires inside the reflector, each connecting two springs. Thus the wiring inside the reflector can be described by another permutation R on the alphabet $\{a, b, c, \ldots, x, y, z\}$. This time the permutation R is not arbitrary but has to have 13 cycles of length 2.

More permutations

Let us denote the permutations that describe the wirings of the left, middle and right rotors by L, M and N.

There are also thirteen wires inside the reflector, each connecting two springs. Thus the wiring inside the reflector can be described by another permutation R on the alphabet $\{a, b, c, \ldots, x, y, z\}$. This time the permutation R is not arbitrary but has to have 13 cycles of length 2.

And the wires between the plugboard and the entry wheel define yet another permutation H on the alphabet $\{a, b, c, \ldots, x, y, z\}$.

Static model of the scrambler

The passage of the electrical current through the scrambler now can be described as the composition of permutations

$$NMLRL^{-1}M^{-1}N^{-1}.$$

Static model of the scrambler

The passage of the electrical current through the scrambler now can be described as the composition of permutations

$$NMLRL^{-1}M^{-1}N^{-1}.$$

If we include the connections between the plugboard and the entry wheel, then the passage of the current from the plugboard through the scrambler and back to the plugboard is described by the permutation

$$HNMLRL^{-1}M^{-1}N^{-1}H^{-1}.$$

Static model of the scrambler

The passage of the electrical current through the scrambler now can be described as the composition of permutations

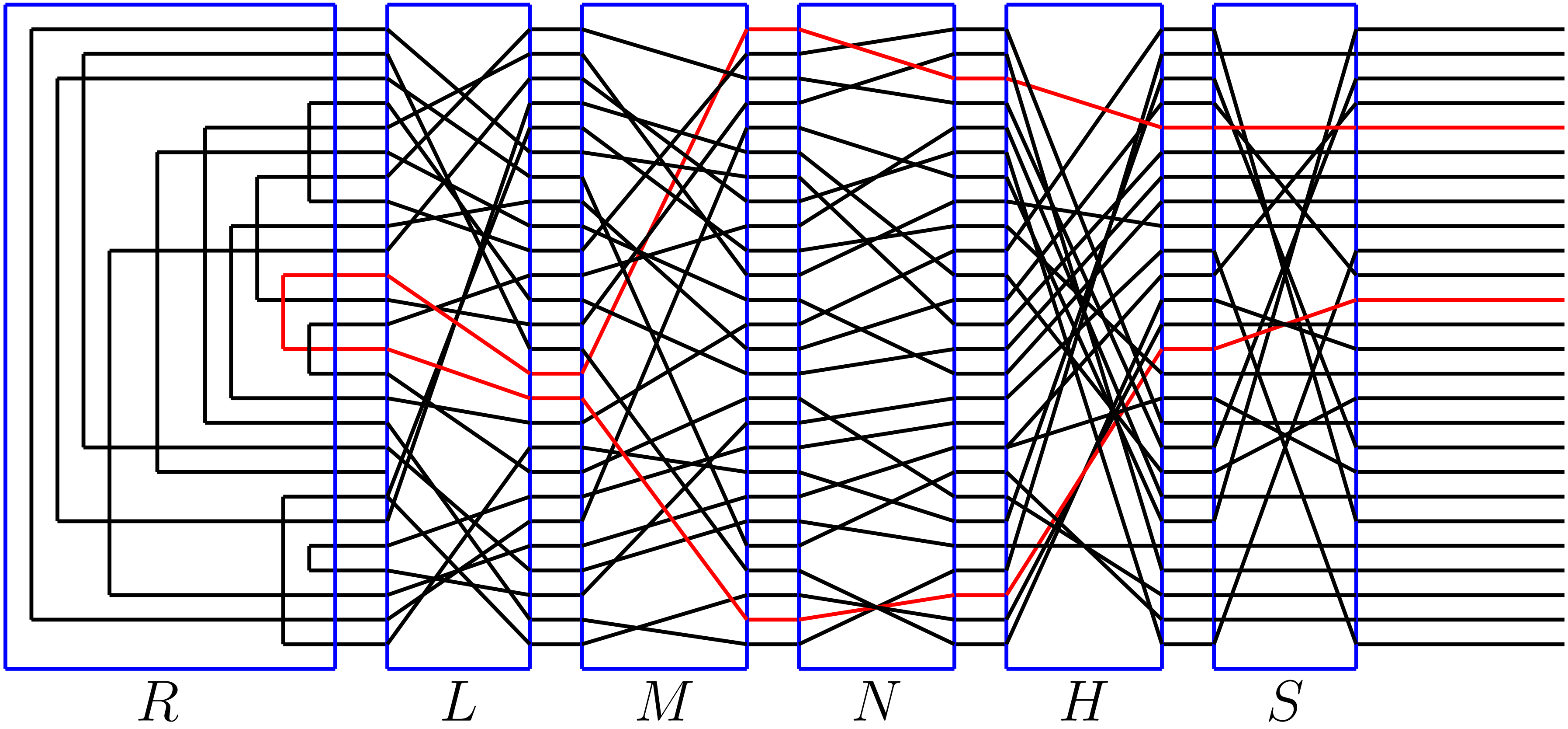
$$NMLRL^{-1}M^{-1}N^{-1}.$$

If we include the connections between the plugboard and the entry wheel, then the passage of the current from the plugboard through the scrambler and back to the plugboard is described by the permutation

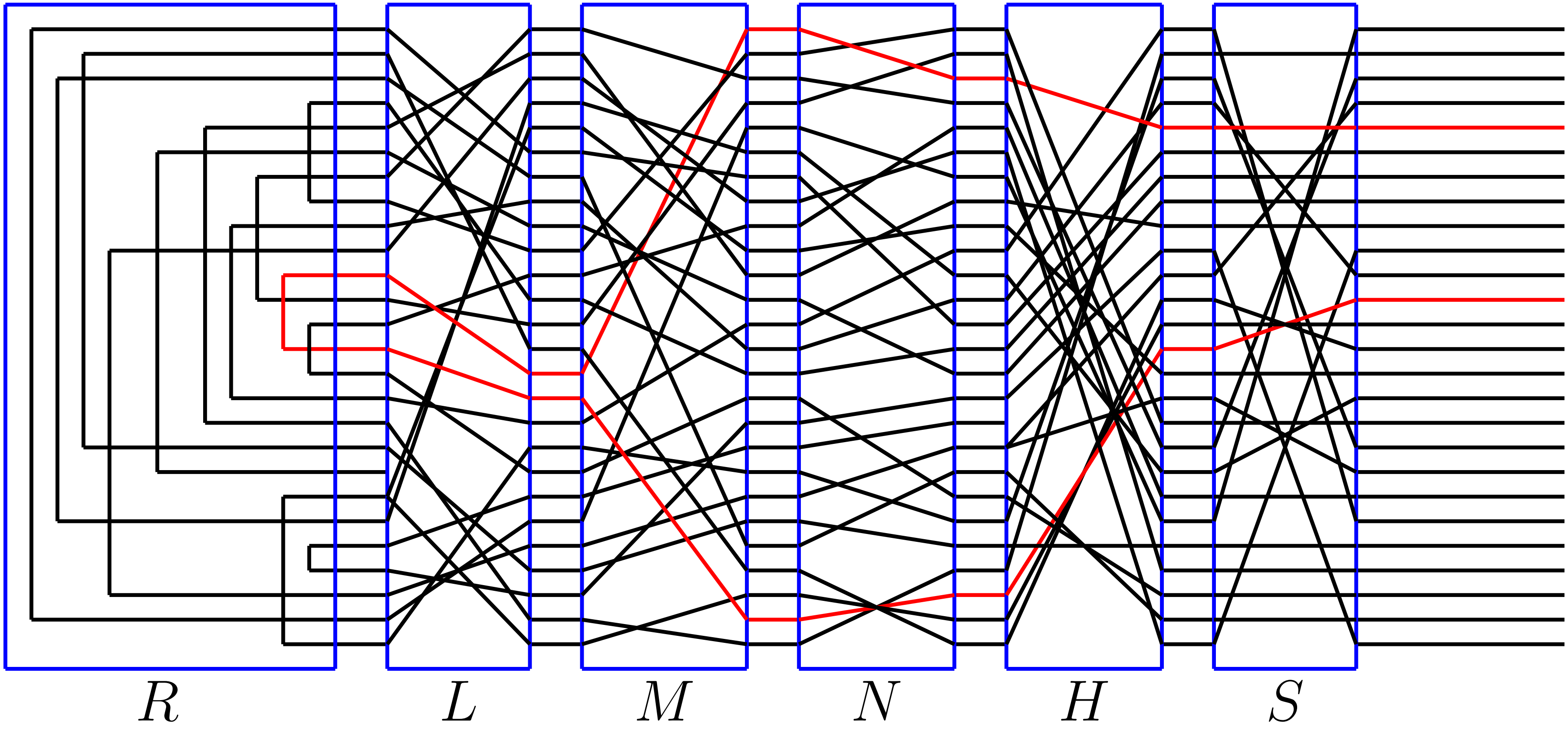
$$HNMLRL^{-1}M^{-1}N^{-1}H^{-1}.$$

And we also have to take into account the cables in the plugboard defining a permutation S.

Static model of Enigma



Static model of Enigma



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

Dynamic model of the scrambler

If the right rotor moves first, then the current from the disc a of the entry wheel does not flow to the spring a of the right rotor, but to the spring b of the right rotor. Similarly, from the disc b of the entry wheel it flows to the spring c of the right rotor, etc.

Dynamic model of the scrambler

If the right rotor moves first, then the current from the disc a of the entry wheel does not flow to the spring a of the right rotor, but to the spring b of the right rotor. Similarly, from the disc b of the entry wheel it flows to the spring c of the right rotor, etc.

We denote by P the cyclic permutation

$$\begin{tikzcd}
a \arrow[r] & b \arrow[r] & c \arrow[r] & d & \cdots & x \arrow[r] & y \arrow[r] & z \arrow[lllllll, bend left]
\end{tikzcd}$$

It maps every letter of the alphabet $\{a, b, c, \ldots, x, y, z\}$ to the subsequent one and the last letter z to the first letter a.

Dynamic model of the scrambler

But we have to take into account also the fact that after pressing a key the right rotor moves first and only then the current flows through the plugboard, entry wheel and the scrambler. So the current from the disc a of the entry wheel does not flow to the spring a of the right rotor, but to the spring b of the right rotor. Similarly, from the disc b of the entry wheel it flows to the spring c of the right rotor, etc.

Dynamic model of the scrambler

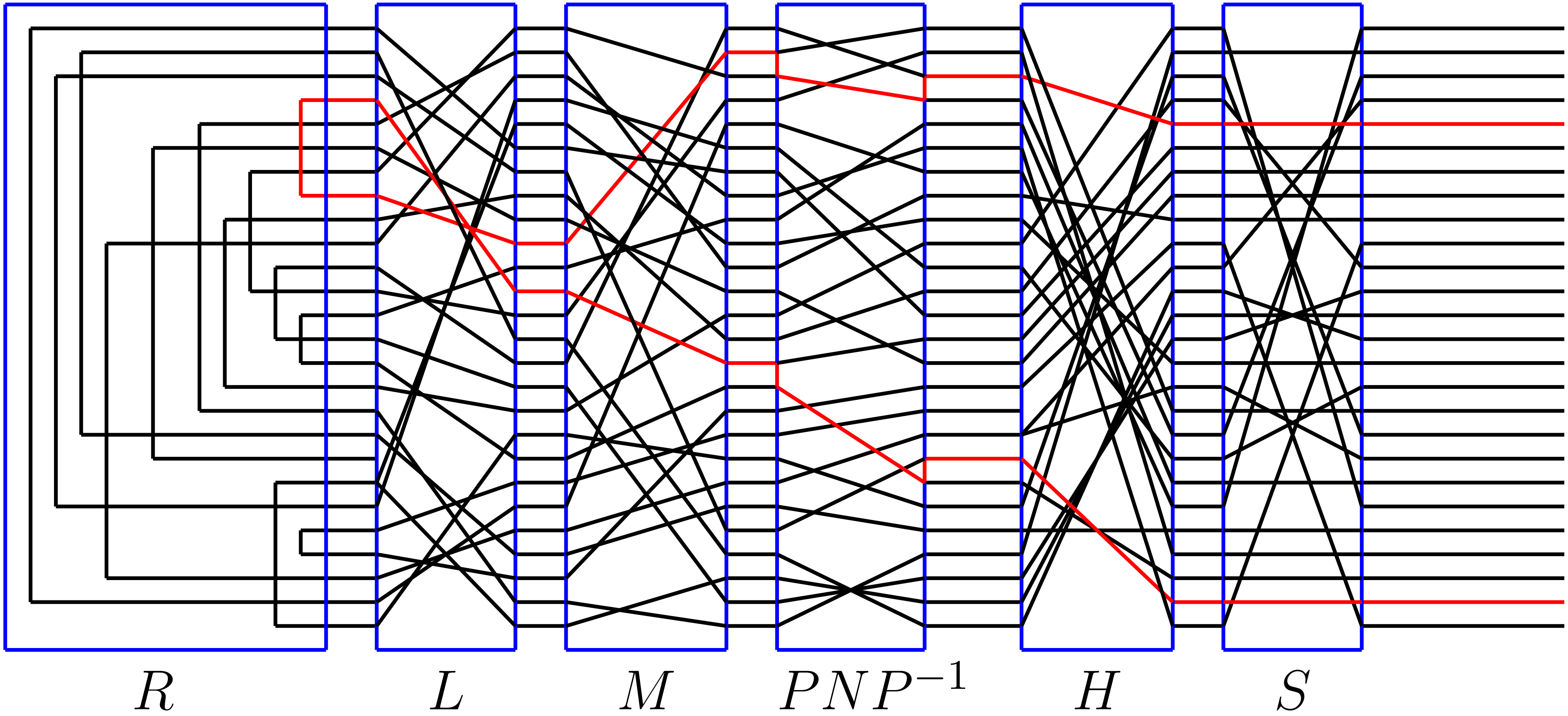
But we have to take into account also the fact that after pressing a key the right rotor moves first and only then the current flows through the plugboard, entry wheel and the scrambler. So the current from the disc a of the entry wheel does not flow to the spring a of the right rotor, but to the spring b of the right rotor. Similarly, from the disc b of the entry wheel it flows to the spring c of the right rotor, etc.

We denote by P the cyclic permutation

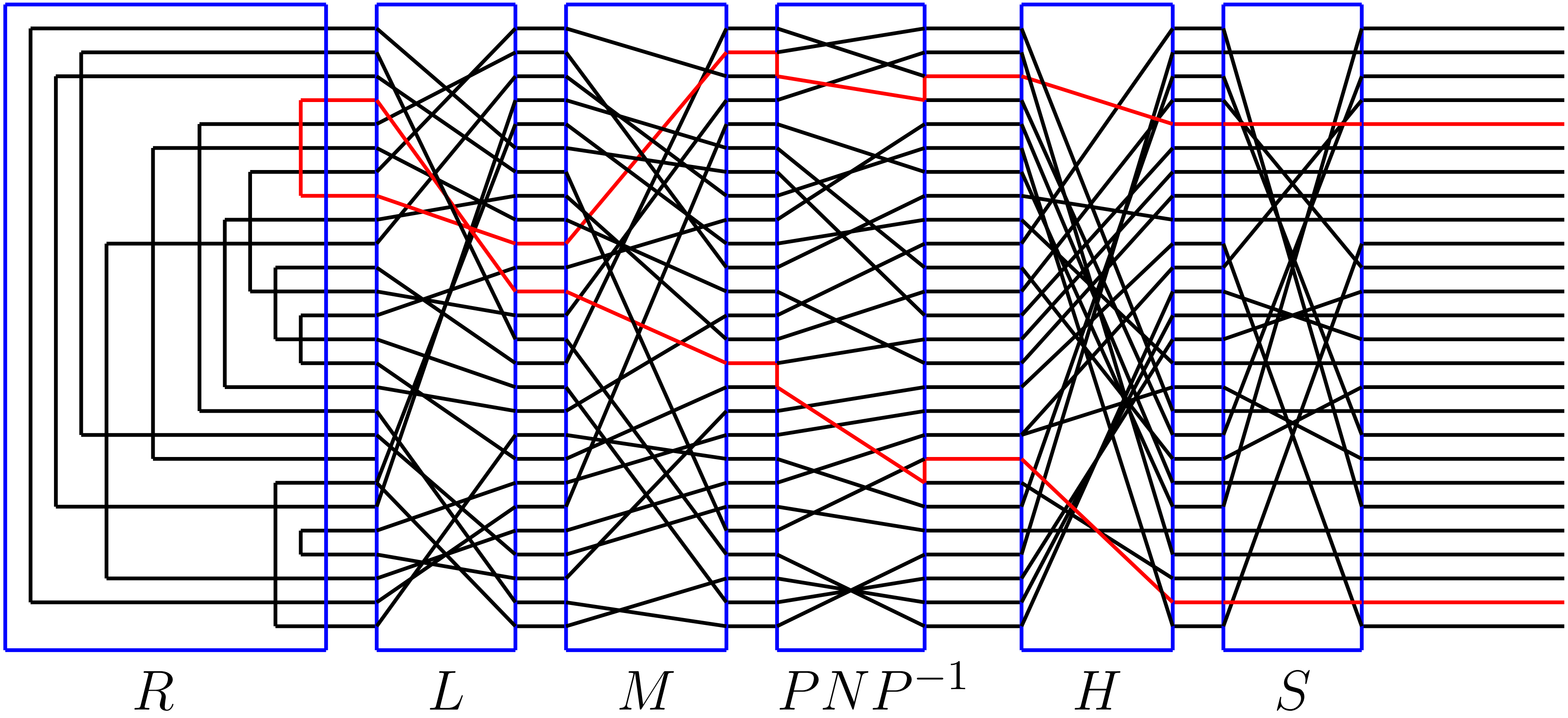
$$\begin{tikzcd}
a \arrow[r] & b \arrow[r] & c \arrow[r] & d & \cdots & x \arrow[r] & y \arrow[r] & z \arrow[llllllll, bend left]
\end{tikzcd}$$

It maps every letter of the alphabet $\{a, b, c, \ldots, x, y, z\}$ to the subsequent one and the last letter z to the first letter a.

Dynamic model of Enigma



Dynamic model of Enigma



$$SH(PNP^{-1})MLRL^{-1}M^{-1}(PN^{-1}P^{-1})H^{-1}S^{-1}$$

Complete model

Thus the whole dynamic model of the operation of the Enigma machine can be described by the permutation

$$SHPNP^{-1}MLRL^{-1}M^{-1}PN^{-1}P^{-1}H^{-1}S^{-1}.$$

Complete model

Thus the whole dynamic model of the operation of the Enigma machine can be described by the permutation

$$SHPNP^{-1}MLRL^{-1}M^{-1}PN^{-1}P^{-1}H^{-1}S^{-1}.$$

The cyclic permutation P is known, the unknown permutations L, M, N and H describe the unknown internal structure of the Enigma machine. The permutation S changes day by day and is given by the corresponding daily key.

Permutations of the day

The first six letters of each message transmitted during the same day were encrypted by the same key given by the setup of the machine for that day. So we can denote by A the permutation of the first letters of messages transmitted that day.

Permutations of the day

The first six letters of each message transmitted during the same day were encrypted by the same key given by the setup of the machine for that day. So we can denote by A the permutation of the first letters of messages transmitted that day.

Similarly, we denote by B the permutation of the second letters of messages transmitted the same day, by C the permutation of the third letters, by D, E and F the permutations of the fourth, fifth and sixth letters.

Permutations of the day

The first six letters of each message transmitted during the same day were encrypted by the same key given by the setup of the machine for that day. So we can denote by A the permutation of the first letters of messages transmitted that day.

Similarly, we denote by B the permutation of the second letters of messages transmitted the same day, by C the permutation of the third letters, by D, E and F the permutations of the fourth, fifth and sixth letters.

All the six permutations A, B, C, D, E, F were also unknown. We may call them the **permutations of the day**.

Connection to the dynamic model

We have already found another description of the permutation determined by the setup of the machine for the day. It was

$$SHPNP^{-1}MLRL^{-1}M^{-1}PN^{-1}P^{-1}H^{-1}S^{-1}.$$

Connection to the dynamic model

We have already found another description of the permutation determined by the setup of the machine for the day. It was

$$SHPNP^{-1}MLRL^{-1}M^{-1}PN^{-1}P^{-1}H^{-1}S^{-1}.$$

So we get the equation

$$A = SHPNP^{-1}MLRL^{-1}M^{-1}PN^{-1}P^{-1}H^{-1}S^{-1}.$$

Connection cont.

We can find a similar expression for the second permutation of the day B. We only have to take into account that after pressing the second key the right rotor has already turned twice. So the equation is

$$B = SHP^2NP^{-2}MLRL^{-1}M^{-1}P^2N^{-1}P^{-2}H^{-1}S^{-1}.$$

Connection cont.

We can find a similar expression for the second permutation of the day B. We only have to take into account that after pressing the second key the right rotor has already turned twice. So the equation is

$$B = SHP^2NP^{-2}MLRL^{-1}M^{-1}P^2N^{-1}P^{-2}H^{-1}S^{-1}.$$

The remaining four permutations of the day can be expressed as

$$\begin{aligned}
C &= SHP^3NP^{-3}MLRL^{-1}M^{-1}P^3N^{-1}P^{-3}H^{-1}S^{-1},\\
D &= SHP^4NP^{-4}MLRL^{-1}M^{-1}P^4N^{-1}P^{-4}H^{-1}S^{-1},\\
E &= SHP^5NP^{-5}MLRL^{-1}M^{-1}P^5N^{-1}P^{-5}H^{-1}S^{-1},\\
F &= SHP^6NP^{-6}MLRL^{-1}M^{-1}P^6N^{-1}P^{-6}H^{-1}S^{-1}.
\end{aligned}$$

products

Conjugated permutations

It should be emphasized that these equations are valid only under the assumption that the only rotor that moved during the encryption of the six letters of the message keys during the given day was the right one. But this happened on average in 20 out of 26 days. Quite often.

Conjugated permutations

It should be emphasized that these equations are valid only under the assumption that the only rotor that moved during the encryption of the six letters of the message keys during the given day was the right one. But this happened on average in 20 out of 26 days. Quite often.

All the permutations in the previous expressions of the permutations of the day were unknown except P. But something important was known!

Conjugated permutations

It should be emphasized that these equations are valid only under the assumption that the only rotor that moved during the encryption of the six letters of the message keys during the given day was the right one. But this happened on average in 20 out of 26 days. Quite often.

All the permutations in the previous expressions of the permutations of the day were unknown except P. But something important was known!

Before we proceed let us state an important definition.

Definition. Two permutations K, L on the same set X are called **conjugated** if there exists another permutation T on the set X such that

$$K = TLT^{-1}.$$

The theorem that won WWII

And one more definition.

Definition. The list of lengths of all cycles in a permutation K is called the **cyclic structure** of the permutation K.

The theorem that won WWII

And one more definition.

Definition. The list of lengths of all cycles in a permutation K is called the **cyclic structure** of the permutation K.

Theorem. Two permutations K, L on the same set X are conjugated if and only if they have the same cyclic structure.

The theorem that won WWII

And one more definition.

Definition. The list of lengths of all cycles in a permutation K is called the **cyclic structure** of the permutation K.

Theorem. Two permutations K, L on the same set X are conjugated if and only if they have the same cyclic structure.

We can get an idea why the theorem is true by drawing the graphs of permutations. So assume that permutations K, L are conjugated and let T be a permutation such that

$$K = TLT^{-1}.$$

Proof

Now choose an arbitrary element $x \in X$ and look at the following part of the graphs of the three permutations. The arrows of the permutation K are blue, the arrows of L are green, and the arrows of T are red.

Proof

Now choose an arbitrary element $x \in X$ and look at the following part of the graphs of the three permutations. The arrows of the permutation K are blue, the arrows of L are green, and the arrows of T are red.

$$\begin{tikzcd}
x \arrow[r] \arrow[d] & xT \arrow[d] \\
xK \arrow[r] & xTL = xKT
\end{tikzcd}$$

Proof cont.

Thus the permutation T maps each cycle of the permutation K to a cycle of the permutation L of the same length. Conjugated permutations must have the same cyclic structures.

Proof cont.

Thus the permutation T maps each cycle of the permutation K to a cycle of the permutation L of the same length. Conjugated permutations must have the same cyclic structures.

Now assume conversely that two permutations K, L have the same cyclic structure. Choose a cycle in the permutation K and a cycle in the permutation L of the same length. Further, choose an element x in the chosen cycle of K and an element y in the chosen cycle of the permutation L. Try to set $xT = y$.

Proof cont.

Thus the permutation T maps each cycle of the permutation K to a cycle of the permutation L of the same length. Conjugated permutations must have the same cyclic structures.

Now assume conversely that two permutations K, L have the same cyclic structure. Choose a cycle in the permutation K and a cycle in the permutation L of the same length. Further, choose an element x in the chosen cycle of K and an element y in the chosen cycle of the permutation L. Try to set $xT = y$.

We search for a permutation T satisfying the equation

$$K = TLT^{-1}.$$

Proof cont.

Look at the following part of the graphs of all three permutations.

Proof cont.

Look at the following part of the graphs of all three permutations.

$$\begin{tikzcd}
x \arrow[r] \arrow[d] & y = xT \arrow[d] \\
xK \arrow[r, dashed] \arrow[d] & yL \arrow[d] \\
xK^2 \arrow[r, dashed] \arrow[uu, dotted, bend left] & yL^2 \arrow[uu, dotted, bend left]
\end{tikzcd}$$

End of the proof

Thus the choice of x and y uniquely determines the values of the permutation T at all elements of the chosen cycle of the permutation K.

End of the proof

Thus the choice of x and y uniquely determines the values of the permutation T at all elements of the chosen cycle of the permutation K.

Observe also that this method enables us to find all possible permutations T that satisfy the equation

$$K = TLT^{-1}$$

if the given permutations K, L have the same cyclic structure.

Characteristics of the day

The permutation R describing the wiring of the reflector has all cycles of length 2. This is the reason why $R^2 = I$, or $R^{-1} = R$.

Characteristics of the day

The permutation R describing the wiring of the reflector has all cycles of length 2. This is the reason why $R^2 = I$, or $R^{-1} = R$.

All permutations A, B, C, D, E, F of the day are conjugated to R. So they all have only cycles of length 2. Thus we get

$$A^2 = B^2 = C^2 = D^2 = E^2 = F^2 = I,$$

or stated otherwise, each of the six permutations is equal to its inverse.

Characteristics of the day

The permutation R describing the wiring of the reflector has all cycles of length 2. This is the reason why $R^2 = I$, or $R^{-1} = R$.

All permutations A, B, C, D, E, F of the day are conjugated to R. So they all have only cycles of length 2. Thus we get

$$A^2 = B^2 = C^2 = D^2 = E^2 = F^2 = I,$$

or stated otherwise, each of the six permutations is equal to its inverse.

We do not not the permutations A, B, C, D, E, F yet. But we do know the products AD, BE, CF if there are enough intercepted messages for the day. Rejewski called them the **characteristics of the day**.

Finding characteristics

You will recall that the intercepted indicators were obtained by enciphering message keys twice. Stated otherwise, by enciphering messages of the form

$$\mathtt{xyzxyz},$$

where x, y, z can be arbitrary letters.

Finding characteristics

You will recall that the intercepted indicators were obtained by enciphering message keys twice. Stated otherwise, by enciphering messages of the form

$$\mathtt{xyzxyz},$$

where x, y, z can be arbitrary letters.

If $\mathtt{x}A = \mathtt{u}$ and $\mathtt{x}D = \mathtt{v}$, then we get

$$\mathtt{u}AD = \mathtt{v},$$

since $A^{-1} = A$.

Finding characteristics

You will recall that the intercepted indicators were obtained by enciphering message keys twice. Stated otherwise, by enciphering messages of the form

$$\mathtt{xyzxyz},$$

where x, y, z can be arbitrary letters.

If $\mathtt{x}A = \mathtt{u}$ and $\mathtt{x}D = \mathtt{v}$, then we get

$$\mathtt{u}AD = \mathtt{v},$$

since $A^{-1} = A$.

But various pairs of the letters $u, v = uAD$ are known! They are the first and fourth letters of the intercepted messages.

A busy manoeuver day

So if there are enough intercepted messages from a given day, we do know the characteristics AD, BE and CF of the day.

A busy manoeuver day

So if there are enough intercepted messages from a given day, we do know the characteristics AD, BE and CF of the day.

As an example, we find the characteristics of a busy manoeuver day, when the following indicators were intercepted. This is a made up example taken from the notes written by Marian Rejewski in 1967.

A busy manoeuver day

So if there are enough intercepted messages from a given day, we do know the characteristics AD, BE and CF of the day.

As an example, we find the characteristics of a busy manoeuver day, when the following indicators were intercepted. This is a made up example taken from the notes written by Marian Rejewski in 1967.

The following table shows 64 intercepted characteristics from the same day. There are enough of them to find all three permutations AD, BE and CF.

A busy manoeuver day cont.

1. AUQ AMN
2. BNH CHL
3. BCT CGJ
4. CIK BZT
5. DDB VDV
6. EJP IPS
7. GPB ZSV
8. GPB ZSV
9. HNO THD
10. HNO THD
11. HXV TTI
12. IKG JKF
13. IKG JKF
14. IND JHU
15. JWF MIC
16. JWF MIC
17. KHB XJV
18. KHB XJV
19. LDR HDE
20. LDR HDE
21. MAW UXP
22. MAW UXP
23. NXD QTU
24. NXD QTU
25. NLU QFZ
26. OBU DLZ
27. PVJ FEG
28. QGA LYB
29. QGA LYB
30. RJL WPX
31. RJL WPX
32. RJL WPX
33. RJL WPX
34. RFC WQQ
35. SYX SCW
36. SYX SCW
37. SYX SCW
38. SYX SCW
39. SYX SCW
40. SJM SPO
41. SJM SPO
42. SJM SPO
43. SUG SMF
44. SUG SMF
45. TMN EBY
46. TMN EBY
47. TAA EXB
48. USE NWH
49. VII PZK
50. VII PZK
51. VQZ PVR
52. VQZ PVR
53. WTM RAO
54. WTM RAO
55. WTM RAO
56. WKI RKK
57. XRS GNM
58. XRS GNM
59. XOI GUK
60. XYW GCP
61. YPC OSQ
62. ZZY YRA
63. ZEF YOC
64. ZSJ YWG

back

back back

Characteristics of the manoeuver day

From the first indicator we find for example that

$$\mathtt{a}AD = \mathtt{a}, \quad \mathtt{u}BE = \mathtt{m}, \quad \mathtt{q}CF = \mathtt{n}.$$

Characteristics of the manoeuver day

From the first indicator we find for example that

$$\mathtt{a}AD = \mathtt{a}, \quad \mathtt{u}BE = \mathtt{m}, \quad \mathtt{q}CF = \mathtt{n}.$$

Similarly, the second indicator gives

$$\mathtt{b}AD = \mathtt{c}, \quad \mathtt{n}BE = \mathtt{h}, \quad \mathtt{h}CF = \mathtt{l}.$$

Characteristics of the manoeuver day

From the first indicator we find for example that

$$\mathtt{a}AD = \mathtt{a}, \quad \mathtt{u}BE = \mathtt{m}, \quad \mathtt{q}CF = \mathtt{n}.$$

Similarly, the second indicator gives

$$\mathtt{b}AD = \mathtt{c}, \quad \mathtt{n}BE = \mathtt{h}, \quad \mathtt{h}CF = \mathtt{l}.$$

The following table lists the cycles of all three characteristics of the manoeuver day.

$$\begin{aligned} AD &= (\mathtt{a}), (\mathtt{s}), (\mathtt{bc}), (\mathtt{rw}), (\mathtt{dvpfkxgzyo}), (\mathtt{eijmunqlht}), \\ BE &= (\mathtt{axt}), (\mathtt{blfqveoum}), (\mathtt{cgy}), (\mathtt{d}), (\mathtt{hjpswizrn}), (\mathtt{k}), \\ CF &= (\mathtt{abviktjgfcqny}), (\mathtt{duzrehlxwpsmo}). \end{aligned}$$

More equations

By multiplying the corresponding pairs of the earlier found equations for the permutations A, B, C, D, E, F of the day we get the following system of equations:

$$\begin{aligned}
AD &= SHPNP^{-1}MLRL^{-1}M^{-1}PN^{-1}P^3NP^{-4}MLRL^{-1}\\
&\quad M^{-1}P^4N^{-1}P^{-4}H^{-1}S^{-1},\\
BE &= SHP^2NP^{-2}MLRL^{-1}M^{-1}P^2N^{-1}P^3NP^{-5}MLRL^{-1}\\
&\quad M^{-1}P^5N^{-1}P^{-5}H^{-1}S^{-1},\\
CF &= SHP^3NP^{-3}MLRL^{-1}M^{-1}P^3N^{-1}P^3NP^{-6}MLRL^{-1}\\
&\quad M^{-1}P^6N^{-1}P^{-6}H^{-1}S^{-1}.
\end{aligned}$$

back

How to simplify the system?

Now, not only the cyclic permutation was known, but also the three characteristics of the day on the left hand sides of the equations. But the system is certainly unsolvable for the unknown wirings of the three rotors and the reflector.

How to simplify the system?

Now, not only the cyclic permutation was known, but also the three characteristics of the day on the left hand sides of the equations. But the system is certainly unsolvable for the unknown wirings of the three rotors and the reflector.

The system can be formally simplified by substituting $Q = MLRL^{-1}M^{-1}$ into the three equations. The permutation Q is the wiring of a virtual reflector consisting of the reflector and the left and middle rotors that were fixed during the day. The substitution only leads to a slightly simplified system of equations on the next slide.

A slightly simplified system

$$\begin{aligned}
AD &= SHPNP^{-1}QPN^{-1}P^3NP^{-4}QP^4N^{-1}P^{-4}H^{-1}S^{-1},\\
BE &= SHP^2NP^{-2}QP^2N^{-1}P^3NP^{-5}QP^5N^{-1}P^{-5}H^{-1}S^{-1},\\
CF &= SHP^3NP^{-3}QP^3N^{-1}P^3NP^{-6}QP^6N^{-1}P^{-6}H^{-1}S^{-1}.
\end{aligned}$$

A slightly simplified system

$$\begin{aligned}
AD &= SHPNP^{-1}QPN^{-1}P^3NP^{-4}QP^4N^{-1}P^{-4}H^{-1}S^{-1},\\
BE &= SHP^2NP^{-2}QP^2N^{-1}P^3NP^{-5}QP^5N^{-1}P^{-5}H^{-1}S^{-1},\\
CF &= SHP^3NP^{-3}QP^3N^{-1}P^3NP^{-6}QP^6N^{-1}P^{-6}H^{-1}S^{-1}.
\end{aligned}$$

This system is still certainly unsolvable for the unknown wirings N, Q even if all the other permutations are known. It has to be further simplified.

A slightly simplified system

$$\begin{aligned}
AD &= SHPNP^{-1}QPN^{-1}P^3NP^{-4}QP^4N^{-1}P^{-4}H^{-1}S^{-1}, \\
BE &= SHP^2NP^{-2}QP^2N^{-1}P^3NP^{-5}QP^5N^{-1}P^{-5}H^{-1}S^{-1}, \\
CF &= SHP^3NP^{-3}QP^3N^{-1}P^3NP^{-6}QP^6N^{-1}P^{-6}H^{-1}S^{-1}.
\end{aligned}$$

This system is still certainly unsolvable for the unknown wirings N, Q even if all the other permutations are known. It has to be further simplified.

Now comes the first of Marian Rejewski's ingenious ideas.

Blunders of German operators

When studying the tables of intercepted message keys he observed that the message keys were certainly not chosen randomly as the manual stated. There were too many repeated indicators.

Blunders of German operators

When studying the tables of intercepted message keys he observed that the message keys were certainly not chosen randomly as the manual stated. There were too many repeated indicators.

But if the operators did not choose the message keys randomly, what were the probable non random choices? Which stereotypes were probably used by the operators?

Blunders of German operators

When studying the tables of intercepted message keys he observed that the message keys were certainly not chosen randomly as the manual stated. There were too many repeated indicators.

But if the operators did not choose the message keys randomly, what were the probable non random choices? Which stereotypes were probably used by the operators?

Marian Rejewski first proved the following simple theorem that helped him to understand the relationship between the two permutations A, D of a day and their composition, the characteristic AD of the same day. You will remember that each of the two permutations A and D contained only cycles of length 2.

One more theorem on permutations

Theorem. A permutation K on a set Z can be expressed as the composition of two permutations X, Y with all cycles of length two if and only if it contains an even number of cycles of each length.

One more theorem on permutations

Theorem. A permutation K on a set Z can be expressed as the composition of two permutations X, Y with all cycles of length two if and only if it contains an even number of cycles of each length.

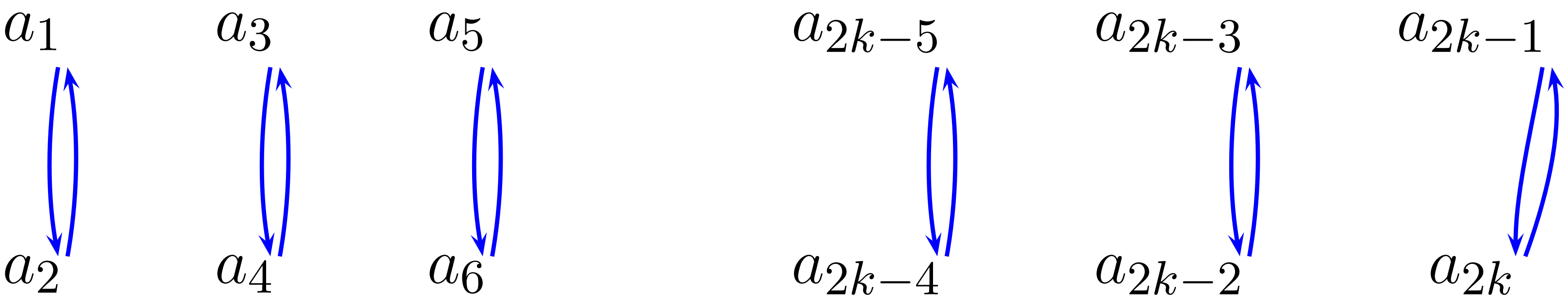
In order to understand why the theorem holds we first assume that $K = XY$ where both permutations X and Y have all cycles of length two.

Proof

We take a cycle (a_1, a_2) of the permutation X and investigate what are the lengths of the cycles of the product XY containing the elements a_1 and a_2. A picture will help.

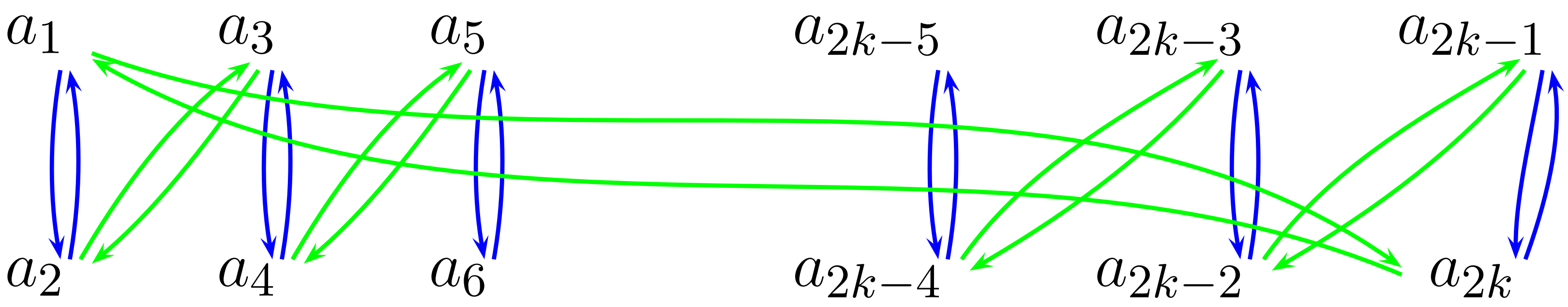
Proof

We take a cycle (a_1, a_2) of the permutation X and investigate what are the lengths of the cycles of the product XY containing the elements a_1 and a_2. A picture will help. We first draw the graph of X



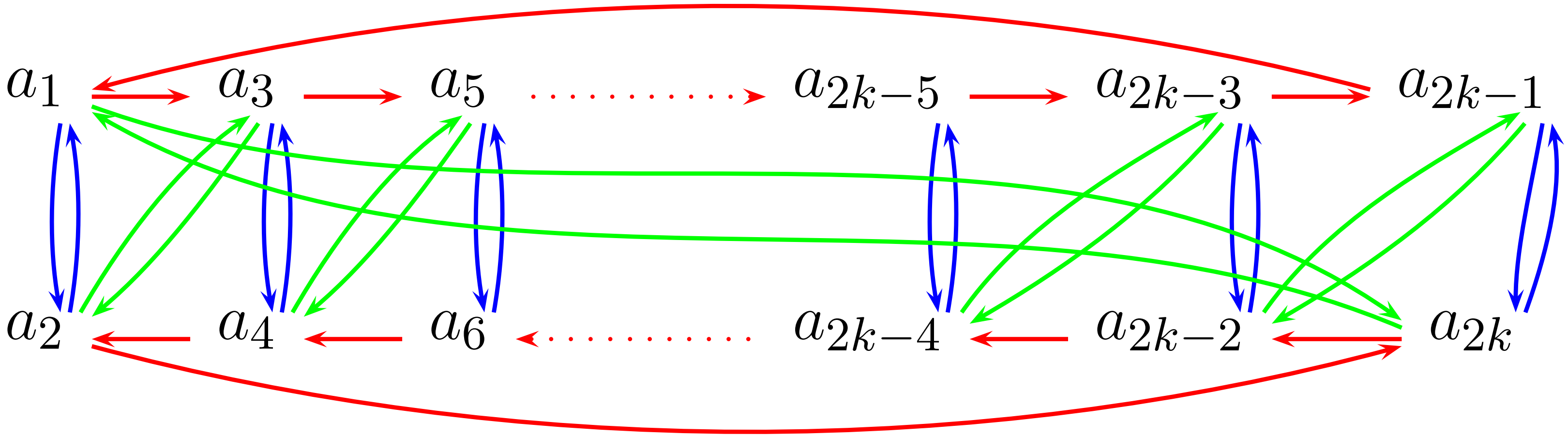
Proof

We take a cycle (a_1, a_2) of the permutation X and investigate what are the lengths of the cycles of the product XY containing the elements a_1 and a_2. A picture will help. We first draw the graph of X and then the graph of Y.



Proof

We take a cycle (a_1, a_2) of the permutation X and investigate what are the lengths of the cycles of the product XY containing the elements a_1 and a_2. A picture will help. We first draw the graph of X and then the graph of Y. Finally, we draw the graph of XY.



Proof cont.

We see that the elements a_1 and a_2 belong to two different cycles of the same length. They are $(a_1a_3\cdots a_{2k-3}a_{2k-1})$ and $(a_2a_{2k}a_{2k-2}\cdots a_4)$.

Proof cont.

We see that the elements a_1 and a_2 belong to two different cycles of the same length. They are $(a_1 a_3 \cdots a_{2k-3} a_{2k-1})$ and $(a_2 a_{2k} a_{2k-2} \cdots a_4)$.

Thus the composition XY has always even number of cycles of any given length.

Proof cont.

We see that the elements a_1 and a_2 belong to two different cycles of the same length. They are $(a_1 a_3 \cdots a_{2k-3} a_{2k-1})$ and $(a_2 a_{2k} a_{2k-2} \cdots a_4)$.

Thus the composition XY has always even number of cycles of any given length.

To prove the converse we assume that a permutation K has even number of cycles of any given length. We will show how to find all possible expressions of K as a composition XY of two permutations which have all cycles of length 2.

Proof cont.

We see that the elements a_1 and a_2 belong to two different cycles of the same length. They are $(a_1 a_3 \cdots a_{2k-3} a_{2k-1})$ and $(a_2 a_{2k} a_{2k-2} \cdots a_4)$.

Thus the composition XY has always even number of cycles of any given length.

To prove the converse we assume that a permutation K has even number of cycles of any given length. We will show how to find all possible expressions of K as a composition XY of two permutations which have all cycles of length 2.

We choose two cycles of the same length, say k, and an arbitrary element a_1 in one of the cycles and an element a_2 in the other cycle. We may assume that $(a_1 a_2)$ is one of the cycles in X.

Proof cont.

We denote the two cycles $(a_1 a_3 \cdots a_{2k-3} a_{2k-1})$ and $(a_2 a_{2k} a_{2k-2} \cdots a_4)$, and draw them one under another and in the opposite direction.

.

Proof cont.

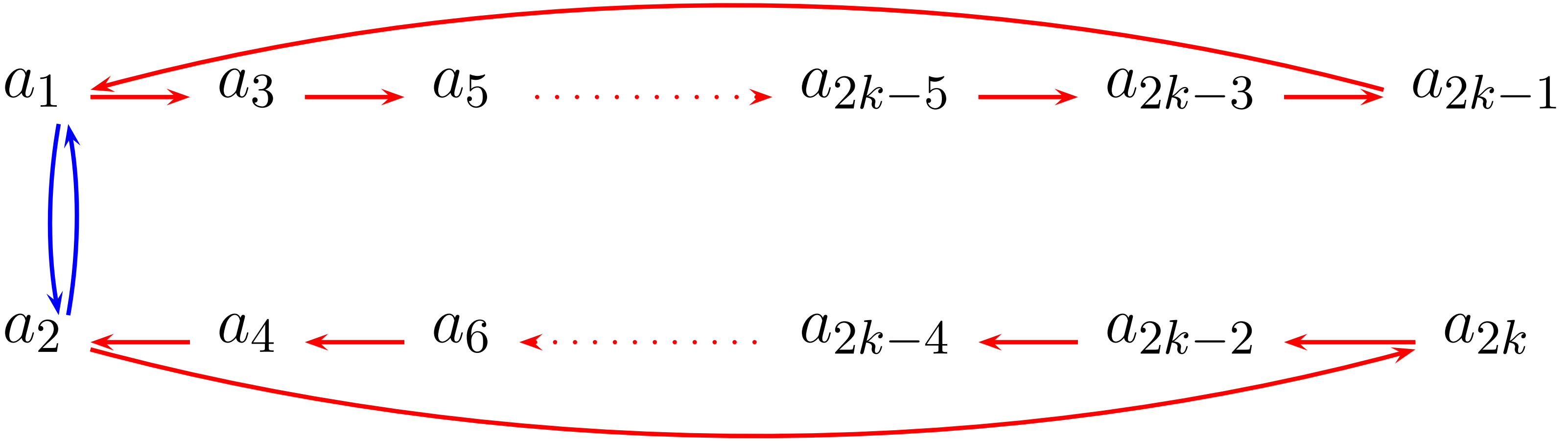
We denote the two cycles $(a_1 a_3 \cdots a_{2k-3} a_{2k-1})$ and $(a_2 a_{2k} a_{2k-2} \cdots a_4)$, and draw them one under another and in the opposite direction.

.

$$\begin{tikzcd}
a_1 \arrow[r] & a_3 \arrow[r] & a_5 \arrow[r, dotted] & a_{2k-5} \arrow[r] & a_{2k-3} \arrow[r] & a_{2k-1} \arrow[lllll, bend right] \\
a_2 \arrow[rrrrr, bend right] & a_4 \arrow[l] & a_6 \arrow[l] & a_{2k-4} \arrow[l, dotted] & a_{2k-2} \arrow[l] & a_{2k} \arrow[l]
\end{tikzcd}$$

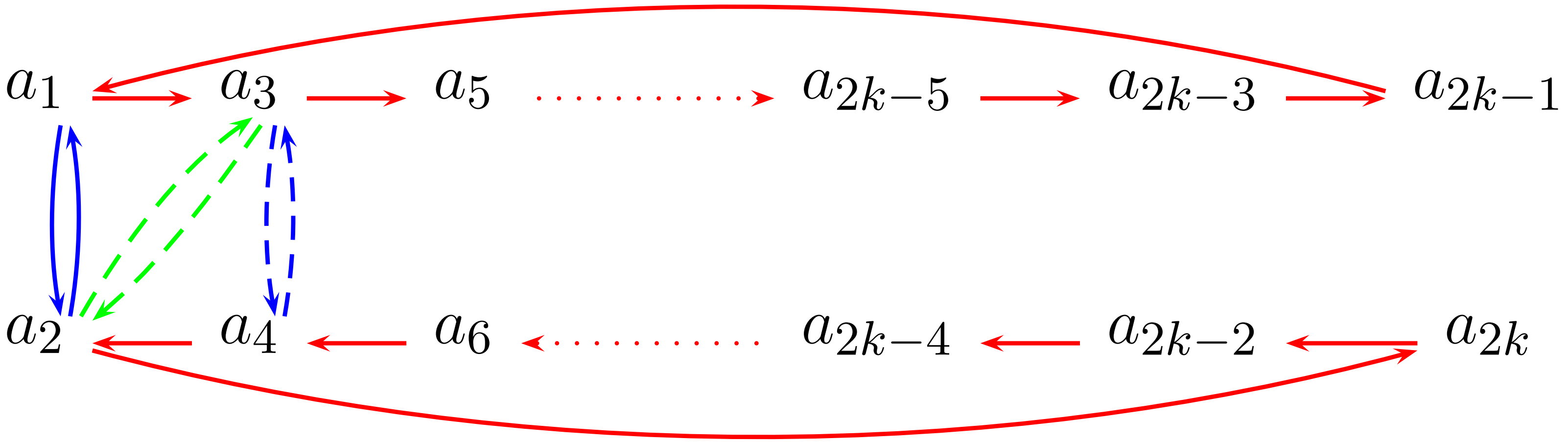
Proof cont.

We denote the two cycles $(a_1 a_3 \cdots a_{2k-3} a_{2k-1})$ and $(a_2 a_{2k} a_{2k-2} \cdots a_4)$, and draw them one under another and in the opposite direction. Then we add the chosen cycle $(a_1 a_2)$ of permutation X.



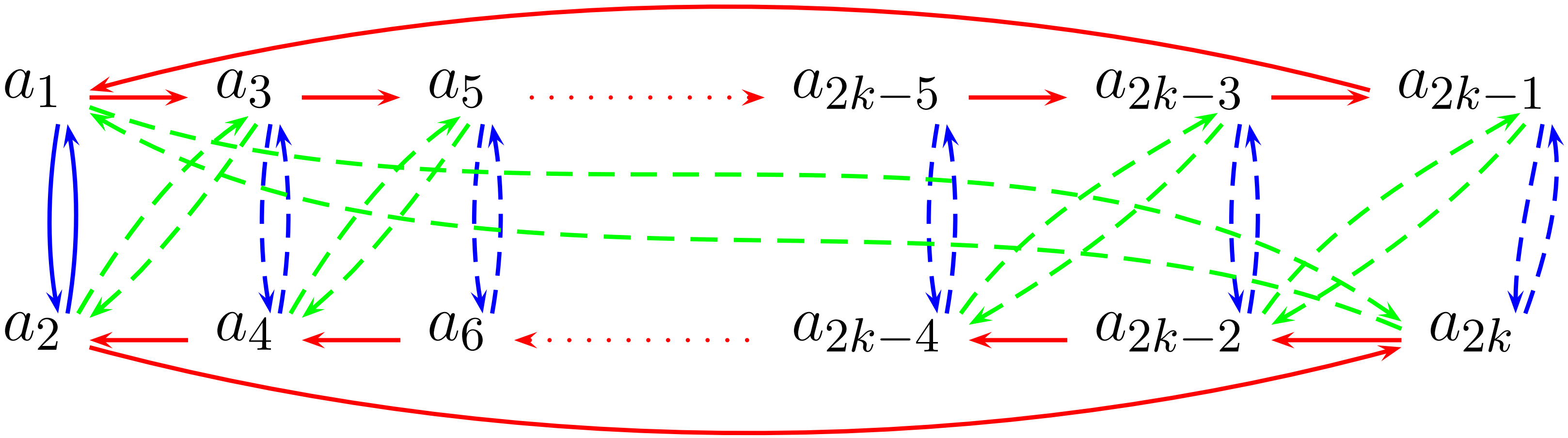
Proof cont.

We denote the two cycles $(a_1 a_3 \cdots a_{2k-3} a_{2k-1})$ and $(a_2 a_{2k} a_{2k-2} \cdots a_4)$, and draw them one under another and in the opposite direction. Then we add the chosen cycle $(a_1 a_2)$ of permutation X. Since we want to have $K = XY$, the permutation Y must map the element a_2 to a_3. From the same reason, a_4 must be mapped to a_3 in X.



Proof cont.

We denote the two cycles $(a_1a_3 \cdots a_{2k-3}a_{2k-1})$ and $(a_2a_{2k}a_{2k-2} \cdots a_4)$, and draw them one under another and in the opposite direction. Then we add the chosen cycle (a_1a_2) of permutation X. Since we want to have $K = XY$, the permutation Y must map the element a_2 to a_3. From the same reason, a_4 must be mapped to a_3 in X. And so on.



End of the proof

This procedure can be used for any pair of cycles of the same length. And since the permutation K has an even number of cycles of any given length, we may define in this way the permutations X and Y on all elements of the set Z.

End of the proof

This procedure can be used for any pair of cycles of the same length. And since the permutation K has an even number of cycles of any given length, we may define in this way the permutations X and Y on all elements of the set Z.

Note also that this procedure gives us a method how to find all decompositions of K as the product $K = XY$ of permutations with all cycles of length 2.

The number of possibilities

For example, the three characteristics of the Rejewski's example

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

give 13 possibilities for the permutations C and F, 3×9 possibilities for the permutations B and E and 2×10 possibilities for the permutations A and D. All together $20 \times 27 \times 13 = 7020$ possibilities for the permutations of the day given these three characteristics of the day.
back

Reducing the number of possibilities

To reduce the number of possibilities Marian Rejewski guessed that the operators had probably chosen message keys consisting of the same three letters or perhaps three neighbouring letters on the keyboard.

Reducing the number of possibilities

To reduce the number of possibilities Marian Rejewski guessed that the operators had probably chosen message keys consisting of the same three letters or perhaps three neighbouring letters on the keyboard.

From the form of the characteristic he could find that the permutation A has to map the letter a to the letter s. So if an operator had chosen triple AAA as the message key, its enciphered version had to start with the letter S. There were only a few possibilities.

Reducing the number of possibilities

To reduce the number of possibilities Marian Rejewski guessed that the operators had probably chosen message keys consisting of the same three letters or perhaps three neighbouring letters on the keyboard.

From the form of the characteristic he could find that the permutation A has to map the letter a to the letter s. So if an operator had chosen triple AAA as the message key, its enciphered version had to start with the letter S. There were only a few possibilities.

When he tried the possibility that the pattern `SYX SCW` was in fact the encryption of the message key AAA doubled, all of a sudden he was able to reconstruct the permutations A, B, C, D, E, F that gave very many stereotyped plain indicators.

A miracle

This assumption means that $\mathtt{a}A = \mathtt{s}$, $\mathtt{a}B = \mathtt{y}$ and $\mathtt{a}C = \mathtt{x}$.

A miracle

This assumption means that $\mathtt{a}A = \mathtt{s}$, $\mathtt{a}B = \mathtt{y}$ and $\mathtt{a}C = \mathtt{x}$.

Since the characteristic CF has only two cycles of length 13, the assumption determines uniquely the permutations C and F.

A miracle

This assumption means that $\mathtt{a}A = \mathtt{s}$, $\mathtt{a}B = \mathtt{y}$ and $\mathtt{a}C = \mathtt{x}$.

Since the characteristic CF has only two cycles of length 13, the assumption determines uniquely the permutations C and F.

Since the elements a and y belong to different cycles of the same length 3 in the characteristic BE, this guess also determines the values of B and E on the six elements of the two cycles. The letters a and s form cycles of length 1 in AD, thus the cycle $(\mathtt{as})$ belongs to both A and D.

A miracle

This assumption means that $\mathtt{a}A = \mathtt{s}$, $\mathtt{a}B = \mathtt{y}$ and $\mathtt{a}C = \mathtt{x}$.

Since the characteristic CF has only two cycles of length 13, the assumption determines uniquely the permutations C and F.

Since the elements a and y belong to different cycles of the same length 3 in the characteristic BE, this guess also determines the values of B and E on the six elements of the two cycles. The letters a and s form cycles of length 1 in AD, thus the cycle $(\mathtt{as})$ belongs to both A and D.

With another two guesses of this form Marian Rejewski was eventually able to reconstruct all message keys used during the day. They are listed in the following table.

The message keys

AUQ AMN:	sss	IKG JKF:	ddd	QGA LYB:	xxx	VQZ PVR:	ert
BNH CHL:	rfv	IND JHU:	dfg	RJL WPX:	bbb	WTM RAO:	ccc
BCT CGJ:	rtz	JWF MIC:	ooo	RFC WQQ:	bnm	WKI RKK:	cde
CIK BZT:	wer	KHB XJV:	lll	SYX SCW:	aaa	XRS GNM:	qqq
DDB VDV:	ikl	LDR HDE:	kkk	SJM SPO:	abc	XOI GUK:	qwe
EJP IPS:	vbn	MAW UXP:	yyy	SUG SMF:	asd	XYW GCP:	qay
FBR KLE:	hjk	NXD QTU:	ggg	TMN EBY:	ppp	YPC OSQ:	mmm
GPB ZSV:	nml	NLU QFZ:	ghj	TAA EXB:	pyx	ZZY YRA:	uvw
HNO THD:	fff	OBU DLZ:	jjj	USE NWH:	zui	ZEF YOC:	uio
HXV TTI:	fgh	PVJ FEG:	tzu	VII PZK:	eee	ZSJ YWG:	uuu

The message keys

AUQ AMN:	sss	IKG JKF:	ddd	QGA LYB:	xxx	VQZ PVR:	ert
BNH CHL:	rfv	IND JHU:	dfg	RJL WPX:	bbb	WTM RAO:	ccc
BCT CGJ:	rtz	JWF MIC:	ooo	RFC WQQ:	bnm	WKI RKK:	cde
CIK BZT:	wer	KHB XJV:	lll	SYX SCW:	aaa	XRS GNM:	qqq
DDB VDV:	ikl	LDR HDE:	kkk	SJM SPO:	abc	XOI GUK:	qwe
EJP IPS:	vbn	MAW UXP:	yyy	SUG SMF:	asd	XYW GCP:	qay
FBR KLE:	hjk	NXD QTU:	ggg	TMN EBY:	ppp	YPC OSQ:	mmm
GPB ZSV:	nml	NLU QFZ:	ghj	TAA EXB:	pyx	ZZY YRA:	uvw
HNO THD:	fff	OBU DLZ:	jjj	USE NWH:	zui	ZEF YOC:	uio
HXV TTI:	fgh	PVJ FEG:	tzu	VII PZK:	eee	ZSJ YWG:	uuu

With the exception of two message keys `abc` and `uvw` all the remaining ones are either triples of the same letters or triples of letters on neighbouring keys on the Enigma keyboard. And these two message keys are also far from being random.

A simplified system of equations

The psychological insight into the habits of German operators enabled Rejewski to return to the original system of equations.

A simplified system of equations

The psychological insight into the habits of German operators enabled Rejewski to return to the original system of equations.

$$\begin{aligned}
A &= SHP^1NP^{-1}QP^1N^{-1}P^{-1}H^{-1}S^{-1}\\
B &= SHP^2NP^{-2}QP^2N^{-1}P^{-2}H^{-1}S^{-1}\\
C &= SHP^3NP^{-3}QP^3N^{-1}P^{-3}H^{-1}S^{-1}\\
D &= SHP^4NP^{-4}QP^4N^{-1}P^{-4}H^{-1}S^{-1}\\
E &= SHP^5NP^{-5}QP^5N^{-1}P^{-5}H^{-1}S^{-1}\\
F &= SHP^6NP^{-6}QP^6N^{-1}P^{-6}H^{-1}S^{-1}.
\end{aligned}$$

But now the permutations A, B, C, D, E, F were known.

back

The daily keys were known!

In fact, Marian Rejewski reconstructed the message keys from a day in September 1932 and he moreover had the daily keys from this month. So he knew also the permutation S. He could move it to the left hand sides of the equations among the already known permutations. It gave him the following system.

The daily keys were known!

In fact, Marian Rejewski reconstructed the message keys from a day in September 1932 and he moreover had the daily keys from this month. So he knew also the permutation S. He could move it to the left hand sides of the equations among the already known permutations. It gave him the following system.

$$\begin{aligned}
S^{-1}AS &= HP^{1}NP^{-1}QP^{1}N^{-1}P^{-1}H^{-1} \\
S^{-1}BS &= HP^{2}NP^{-2}QP^{2}N^{-1}P^{-2}H^{-1} \\
S^{-1}CS &= HP^{3}NP^{-3}QP^{3}N^{-1}P^{-3}H^{-1} \\
S^{-1}DS &= HP^{4}NP^{-4}QP^{4}N^{-1}P^{-4}H^{-1} \\
S^{-1}ES &= HP^{5}NP^{-5}QP^{5}N^{-1}P^{-5}H^{-1} \\
S^{-1}FS &= HP^{6}NP^{-6}QP^{6}N^{-1}P^{-6}H^{-1}.
\end{aligned}$$

Germans like order

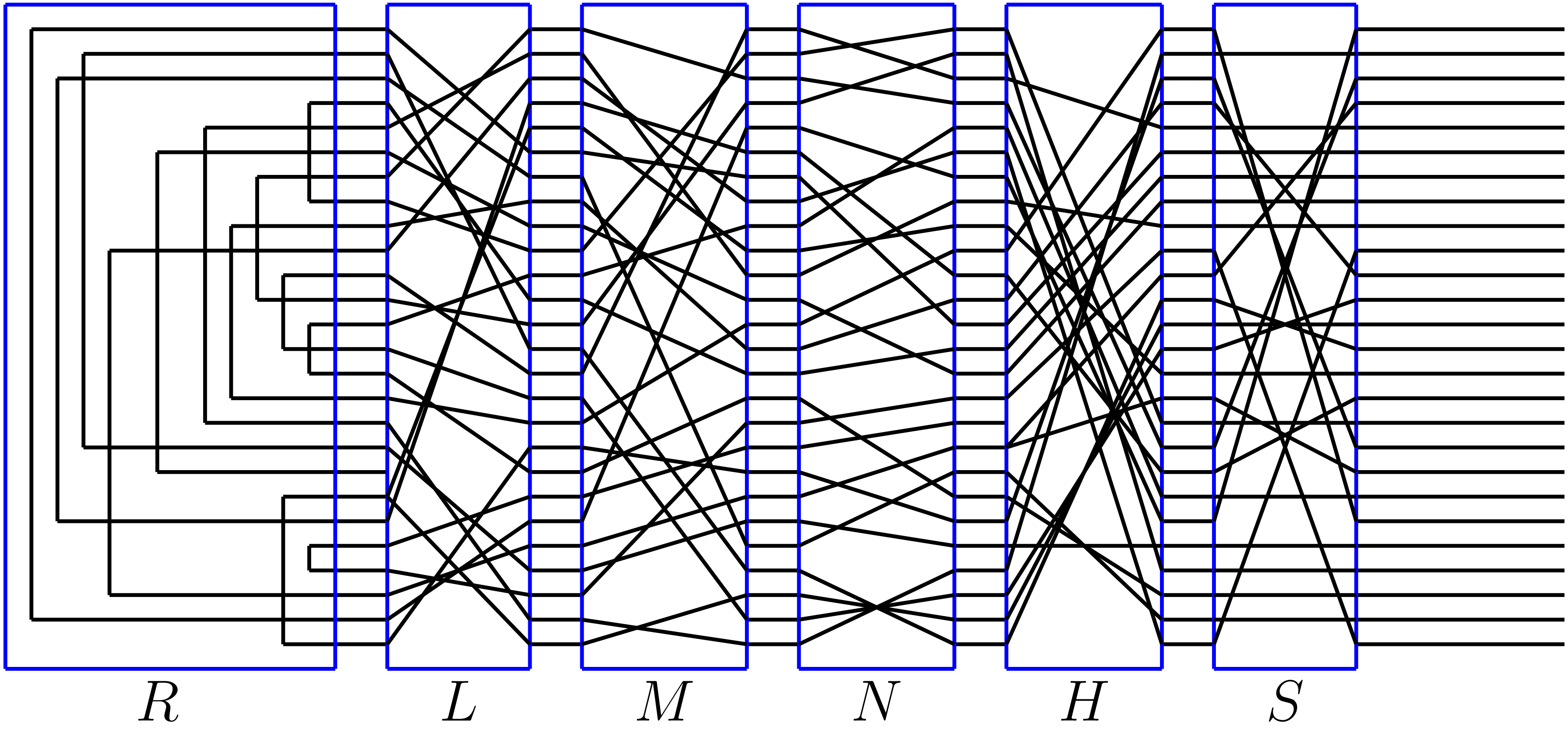
Now only the permutations H, N and Q were unknown. Rejewski first tried the same wiring between the plug board and the entry wheel that was used in the commercial Enigma. But it went nowhere.

Germans like order

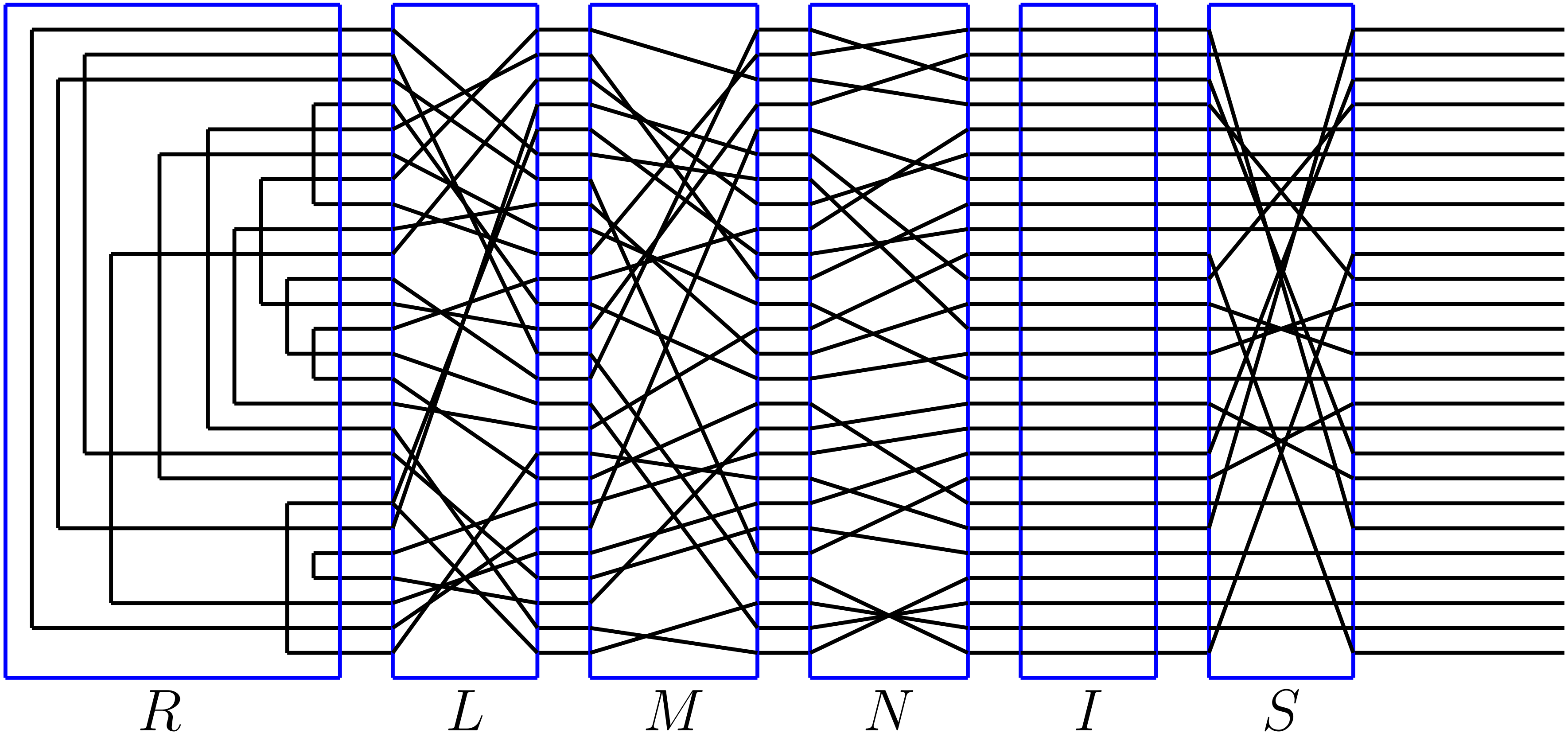
Now only the permutations H, N and Q were unknown. Rejewski first tried the same wiring between the plug board and the entry wheel that was used in the commercial Enigma. But it went nowhere.

This unsuccessful attempt led him to the second ingenious insight into the psychology, this time of the constructors of the Enigma machine. Rejewski observed that the wiring between the plugboard and the entry wheel in the commercial Enigma machine was very regular. The plugs were connected to the entry wheel in the order of the keys on the keyboard. So he tried another regular wiring, this time in the order of the alphabet.

Real connections to the entry wheel



Real connections to the entry wheel



Thus the second try was $H = I$, the identity permutation.

Number of unknowns is getting smaller

Now only two permutations N and Q remained unknown. Rejewski rewrote the system of six equations in the following form.

Number of unknowns is getting smaller

Now only two permutations N and Q remained unknown. Rejewski rewrote the system of six equations in the following form.

$$\begin{aligned}
T &= P^{-1}S^{-1}ASP^{1} = NP^{-1}QP^{1}N^{-1}, \\
U &= P^{-2}S^{-1}BSP^{2} = NP^{-2}QP^{2}N^{-1}, \\
W &= P^{-3}S^{-1}CSP^{3} = NP^{-3}QP^{3}N^{-1}, \\
X &= P^{-4}S^{-1}DSP^{4} = NP^{-4}QP^{4}N^{-1}, \\
Y &= P^{-5}S^{-1}ESP^{5} = NP^{-5}QP^{5}N^{-1}, \\
Z &= P^{-6}S^{-1}DSP^{6} = NP^{-6}QP^{6}N^{-1}.
\end{aligned}$$

The moment of the truth

By multiplying the pairs of subsequent equations he obtained the following system of five equations in the two unknowns N and Q.

The moment of the truth

By multiplying the pairs of subsequent equations he obtained the following system of five equations in the two unknowns N and Q.

$$\begin{aligned}
TU &= NP^{-1}(QP^{-1}QP)PN^{-1}, \\
UW &= NP^{-2}(QP^{-1}QP)P^2N^{-1}, \\
WX &= NP^{-3}(QP^{-1}QP)P^3N^{-1}, \\
XY &= NP^{-4}(QP^{-1}QP)P^4N^{-1}, \\
YZ &= NP^{-5}(QP^{-1}QP)P^5N^{-1}.
\end{aligned}$$

Only one unknown remained

From this system he eliminated the common expression $QP^{-1}QP$ and obtained the following system of four equations in one unknown N, or still better, in the unknown $V = NP^{-1}N^{-1}$.

Only one unknown remained

From this system he eliminated the common expression $QP^{-1}QP$ and obtained the following system of four equations in one unknown N, or still better, in the unknown $V = NP^{-1}N^{-1}$.

$$\begin{aligned}
UW &= NP^{-1}N^{-1}(TU)NPN^{-1} = V(TU)V^{-1}, \\
WX &= NP^{-1}N^{-1}(UW)NPN^{-1} = V(UW)V^{-1}, \\
XY &= NP^{-1}N^{-1}(WX)NPN^{-1} = V(WX)V^{-1}, \\
YZ &= NP^{-1}N^{-1}(XY)NPN^{-1} = V(XY)V^{-1}.
\end{aligned}$$

Only one unknown remained

From this system he eliminated the common expression $QP^{-1}QP$ and obtained the following system of four equations in one unknown N, or still better, in the unknown $V = NP^{-1}N^{-1}$.

$$
\begin{aligned}
UW &= NP^{-1}N^{-1}(TU)NPN^{-1} = V(TU)V^{-1}, \\
WX &= NP^{-1}N^{-1}(UW)NPN^{-1} = V(UW)V^{-1}, \\
XY &= NP^{-1}N^{-1}(WX)NPN^{-1} = V(WX)V^{-1}, \\
YZ &= NP^{-1}N^{-1}(XY)NPN^{-1} = V(XY)V^{-1}.
\end{aligned}
$$

Moreover, all four equations have the familiar form

$$K = TLT^{-1}.$$

The solution

From the proof of the theorem that won the WWII we already know how to find all solutions V of each of the four equations. There must be a common solution V of the four equations that is a cyclic permutation, since it is conjugated to the the cyclic permutation P^{-1}. Hence he could also find all twenty six solutions for the permutation N.

The solution

From the proof of the theorem that won the WWII we already know how to find all solutions V of each of the four equations. There must be a common solution V of the four equations that is a cyclic permutation, since it is conjugated to the the cyclic permutation P^{-1}. Hence he could also find all twenty six solutions for the permutation N.

The wiring of one of the rotors thus became known. In those times the German army changed the order of rotors in daily keys every quarter of the year. Since September and October are in different quarters of the year, the same method led to the discovery of the wiring of another rotor. This was the rotor used as the right (fast) rotor in the other quarter of the year 1932 from which the daily keys were known.

Third rotor and reflector

Then it was possible to calculate the wiring of the remaining rotor and also of the reflector. Rejewski is very sketchy in this respect. Let us try to figure out how it could had been done.

Third rotor and reflector

Then it was possible to calculate the wiring of the remaining rotor and also of the reflector. Rejewski is very sketchy in this respect. Let us try to figure out how it could had been done.

The first month the rotors were in the order L, M, N, from which the wiring N of the right rotor was calculated.

Third rotor and reflector cont.

Let us keep the notation also for the other month. The rotors were in a different order, certainly the right rotor had changed. This gives us four possibilities for the order of rotors in the other month:

- M, N, L, from which L can be calculated,

Third rotor and reflector cont.

Let us keep the notation also for the other month. The rotors were in a different order, certainly the right rotor had changed. This gives us four possibilities for the order of rotors in the other month:

- M, N, L, from which L can be calculated,
- N, L, M, from which M could be calculated,

Third rotor and reflector cont.

Let us keep the notation also for the other month. The rotors were in a different order, certainly the right rotor had changed. This gives us four possibilities for the order of rotors in the other month:

- M, N, L, from which L can be calculated,
- N, L, M, from which M could be calculated,
- L, N, M, from which M could be calculated,

Third rotor and reflector cont.

Let us keep the notation also for the other month. The rotors were in a different order, certainly the right rotor had changed. This gives us four possibilities for the order of rotors in the other month:

- M, N, L, from which L can be calculated,
- N, L, M, from which M could be calculated,
- L, N, M, from which M could be calculated,
- N, L, M, from which again M could be calculated.

Third rotor and reflector cont.

Let us keep the notation also for the other month. The rotors were in a different order, certainly the right rotor had changed. This gives us four possibilities for the order of rotors in the other month:

- M, N, L, from which L can be calculated,
- N, L, M, from which M could be calculated,
- L, N, M, from which M could be calculated,
- N, L, M, from which again M could be calculated.

In the first three of these cases the unknown rotor appears in at least one of the two month as the slowest left rotor.

Third rotor and reflector cont.

When calculating the wiring inside the fast right rotor, Rejewski used only intercepted messages from one day of the month. But he had at his disposal several dozens intercepted messages from each day of the month.

Third rotor and reflector cont.

When calculating the wiring inside the fast right rotor, Rejewski used only intercepted messages from one day of the month. But he had at his disposal several dozens intercepted messages from each day of the month.
So we may safely assume that in the tables of daily keys from the month he could find four days in which the positions of the left rotor formed an arithmetic sequence modulo 26. That means that the initial positions of the left rotor were

$$P^{x}LP^{-x}, P^{x+d}LP^{-x-d}, P^{x+2d}LP^{-x-2d}, P^{x+3d}LP^{-x-3d}$$

for some $x, d \in \{0, 1, 2, \ldots, 25\}$, preferably d odd.

Third rotor and reflector cont.

For each of these four days we take the equation expressing the first permutation of the day.

Third rotor and reflector cont.

For each of these four days we take the equation expressing the first permutation of the day.

So we get the system of equations

$$A_i = S_i N_i M_i P^{x+id} L P^{-x-id} R P^{x+id} L^{-1} P^{-x-id} M_i^{-1} N_i - 1 S_i^{-1}$$

for $i = 0, 1, 2, 3$ in the unknowns L, R. Here we have set $N_i = P^{y_i} N P^{-y_i}$ and $M_i = P^{z_i} M P^{-z_i}$ to simplify the notation. Moreover, the permutations S_i describe the plug board connections valid for the four chosen days.

Third rotor and reflector cont.

For each of these four days we take the equation expressing the first permutation of the day.

So we get the system of equations

$$A_i = S_i N_i M_i P^{x+id} L P^{-x-id} R P^{x+id} L^{-1} P^{-x-id} M_i^{-1} N_i - 1 S_i^{-1}$$

for $i = 0, 1, 2, 3$ in the unknowns L, R. Here we have set $N_i = P^{y_i} N P^{-y_i}$ and $M_i = P^{z_i} M P^{-z_i}$ to simplify the notation. Moreover, the permutations S_i describe the plug board connections valid for the four chosen days.

The rest of the calculation can be done in the way discovered by Rejewski.

Third rotor and reflector cont.

First we transfer as many of the known permutations as possible to the left hand side and obtain the equations

$$P^{-x-id}M_i^{-1}N_i^{-1}S_i^{-1}A_iS_iN_iM_iP^{x+id} = LP^{-x-id}RP^{x+id}L^{-1}$$

for i=0,1,2,3.

Third rotor and reflector cont.

First we transfer as many of the known permutations as possible to the left hand side and obtain the equations

$$P^{-x-id}M_i^{-1}N_i^{-1}S_i^{-1}A_iS_iN_iM_iP^{x+id} = LP^{-x-id}RP^{x+id}L^{-1}$$

for i=0,1,2,3.

Then we change the notation for the left hand sides to get

$$U_i = LP^{-x-id}RP^{x+id}L^{-1}.$$

Third rotor and reflector cont.

First we transfer as many of the known permutations as possible to the left hand side and obtain the equations

$$P^{-x-id}M_i^{-1}N_i^{-1}S_i^{-1}A_iS_iN_iM_iP^{x+id} = LP^{-x-id}RP^{x+id}L^{-1}$$

for i=0,1,2,3.

Then we change the notation for the left hand sides to get

$$U_i = LP^{-x-id}RP^{x+id}L^{-1}.$$

Then we multiply pairs of subsequent equations and get for $i = 0, 1, 2$

$$U_iU_{i+1} = LP^{-x-id}RP^{-d}RP^dP^{x+id}L^{-1}.$$

Third rotor and reflector end

By eliminating the common expression $RP^{-d}RP^{d}$ from the three equations we get two equations for the unknown $LP^{d}L^{-1}$

$$U_iU_{i+1} = (LP^{d}L^{-1})U_{i+1}U_{i+2}(LP^{-d}L^{-1})$$

for $i = 0, 1$.

Third rotor and reflector end

By eliminating the common expression $RP^{-d}RP^{d}$ from the three equations we get two equations for the unknown $LP^{d}L^{-1}$

$$U_iU_{i+1} = (LP^dL^{-1})U_{i+1}U_{i+2}(LP^{-d}L^{-1})$$

for $i = 0, 1$.

From these two equations the unknown $LP^{d}L^{-1}$ can be calculated. Provided the joint solution of tese two equations is unique we subsequently get 26 possibilities for the unknown wiring L in case d is odd and 13×13 possibilities for L in case d is even.

Choice of the right wirings L, M, N

Then the wiring R inside the reflector can be easily and uniquely calculated from the equation

$$A = SP^1NP^{-1}MLRL^{-1}M^{-1}P^1N^{-1}P^{-1}S^{-1}$$

used earlier.

Choice of the right wirings L, M, N

Then the wiring R inside the reflector can be easily and uniquely calculated from the equation

$$A = SP^1NP^{-1}MLRL^{-1}M^{-1}P^1N^{-1}P^{-1}S^{-1}$$

used earlier.

As a result of these calculations Rejewski received at least $26 \times 26 \times 26 = 17576$ possibilities for the internal wirings of the Enigma machine. To choose the right one he was greatly helped by the example of a plain text and its real cipher version given in the operation manual.

Choice of the right wirings L, M, N

Then the wiring R inside the reflector can be easily and uniquely calculated from the equation

$$A = SP^1NP^{-1}MLRL^{-1}M^{-1}P^1N^{-1}P^{-1}S^{-1}$$

used earlier.

As a result of these calculations Rejewski received at least $26 \times 26 \times 26 = 17576$ possibilities for the internal wirings of the Enigma machine. To choose the right one he was greatly helped by the example of a plain text and its real cipher version given in the operation manual.

And finally, he found the position of the carry notches on the alphabet ring of each rotor.

How it was possible to calculate H

In his notes written in France probably in 1940 Rejewski mentions that it was also possible to calculate the permutation H describing the wiring between the plug board and the entry wheel. You will recall that Rejewski made a wild guess that H was the identity permutation and the guess proved to be true.

How it was possible to calculate H

In his notes written in France probably in 1940 Rejewski mentions that it was also possible to calculate the permutation H describing the wiring between the plug board and the entry wheel. You will recall that Rejewski made a wild guess that H was the identity permutation and the guess proved to be true.

To this end it was sufficient to find two days during the same month, in which the positions P^jNP^{-j} of the right rotor were the same. Since there were 26 possible positions and at least 30 days in the month, such two days always existed.

How it was possible to calculate H

In his notes written in France probably in 1940 Rejewski mentions that it was also possible to calculate the permutation H describing the wiring between the plug board and the entry wheel. You will recall that Rejewski made a wild guess that H was the identity permutation and the guess proved to be true.

To this end it was sufficient to find two days during the same month, in which the positions P^jNP^{-j} of the right rotor were the same. Since there were 26 possible positions and at least 30 days in the month, such two days always existed.

We will denote the permutations defined by the virtual reflectors $M_1L_1RL_1^{-1}M_1^{-1}$ and $M_2L_2RL_2^{-1}M_2^{-1}$ in these two days by Q_1 and Q_2 respectively.

Calculating H cont.

The equations describing the permutations of the day in terms of the internal structure of the machine were for the first day

$$A_i = S_1 H P^{j+i} N P^{-j-i} Q_1 P^{j+i} N^{-1} P^{-j-i} H^{-1} S_1^{-1},$$

i=1,2,. . . ,6, and for the other day

$$B_i = S_2 H P^{j+i} N P^{-j-i} Q_2 P^{j+i} N^{-1} P^{-j-i} H^{-1} S_2^{-1},$$

i=1,2,. . . ,6.

Calculating H cont.

The equations describing the permutations of the day in terms of the internal structure of the machine were for the first day

$$A_i = S_1 H P^{j+i} N P^{-j-i} Q_1 P^{j+i} N^{-1} P^{-j-i} H^{-1} S_1^{-1},$$

i=1,2,. . . ,6, and for the other day

$$B_i = S_2 H P^{j+i} N P^{-j-i} Q_2 P^{j+i} N^{-1} P^{-j-i} H^{-1} S_2^{-1},$$

i=1,2,. . . ,6.
Transferring the known permutations S_1 and S_2 to the left hand sides and multiplying the corresponding pairs of equations led to the equations ($i = 1, 2, \ldots, 6$)

$$S_1^{-1} A_i S_1 S_2^{-1} B_i S_2 = H P^{j+i} N P^{-j-i} Q_1 Q_2 P^{j+i} N^{-1} P^{-j-i} H^{-1}.$$

Calculating H end

By eliminating the common part Q_1Q_2 from all equations and by another use of the theorem that won WWII it was possible to find the permutations

$$HP^{j+i}(PN^{-1}P^{-1}N)P^{-j-i}H^{-1}$$

for $i = 1, 2, \ldots, 6$.

Calculating H end

By eliminating the common part Q_1Q_2 from all equations and by another use of the theorem that won WWII it was possible to find the permutations

$$HP^{j+i}(PN^{-1}P^{-1}N)P^{-j-i}H^{-1}$$

for $i = 1, 2, \ldots, 6$.

And eliminating the common expression $PN^{-1}P^{-1}N$ and another application of the same theorem would give the permutation HPH^{-1}. From this we would get once more 26 possible values of the permutation H.

Calculating H end

By eliminating the common part Q_1Q_2 from all equations and by another use of the theorem that won WWII it was possible to find the permutations

$$HP^{j+i}(PN^{-1}P^{-1}N)P^{-j-i}H^{-1}$$

for $i = 1, 2, \ldots, 6$.

And eliminating the common expression $PN^{-1}P^{-1}N$ and another application of the same theorem would give the permutation HPH^{-1}. From this we would get once more 26 possible values of the permutation H.

Rejewski estimates that the lucky guess $H = I$ shortened the reconstruction of the Enigma machine by 3 months. Without this guess he would have to check not only $26^3 = 17576$ possibilities but $26^4 = 456976$ possibilities.

A replica of Enigma was built

The guess $H = I$ enabled to built a replica of the military Enigma machine already at the end of January 1933.

A replica of Enigma was built

The guess $H = I$ enabled to built a replica of the military Enigma machine already at the end of January 1933.

Hitler came to power in Germany in January 1933. From almost the same time the Polish Intelligence Service was able to read most of the top secret German army communications.

A replica of Enigma was built

The guess $H = I$ enabled to built a replica of the military Enigma machine already at the end of January 1933.

Hitler came to power in Germany in January 1933. From almost the same time the Polish Intelligence Service was able to read most of the top secret German army communications.

In July 1939, when it became clear that a new war in Europe was inevitable, the Polish Intelligence Service organized a meeting near Warsaw. There it passed the replicas and all other information to its French and British counterparts. This is how the first replica of the military Enigma machine got to Bletchley Park, the center of the British cryptanalysis of that time.

References

Rejewski, Marian, *An application of the theory of permutations in breaking the Enigma cipher*, Applicationes Mathematicae **16**, No. 4, Warsaw 1980, mad.home.cern.ch/frode/crypto/rew80.pdf

Rejewski, Marian, *How Polish mathematicians broke the Enigma cipher*, IEEE Annals of the history of computing, July 1981, 213-234,

Kozaczuk, Wladyslaw, *Enigma*, London: Arms and Armour, 1984,

Bauer, Friedrich L., *Decrypted Secrets, Methods and Maxims of Cryptology*, 2nd ed. Springer-Verlag, Berlin Heidelberg 2000.

http://www.spybooks.pl/en/enigma.html, a large collection of various notes written by Marian Rejewski, mainly in Polish.

Enigma simulators

Enigma simulators can be found e.g. at

www.xat.nl/enigma/

www.ugrad.cs.jhu.edu/ russell/classes/enigma/

frode.home.cern.ch/frode/crypto/simula/m3/