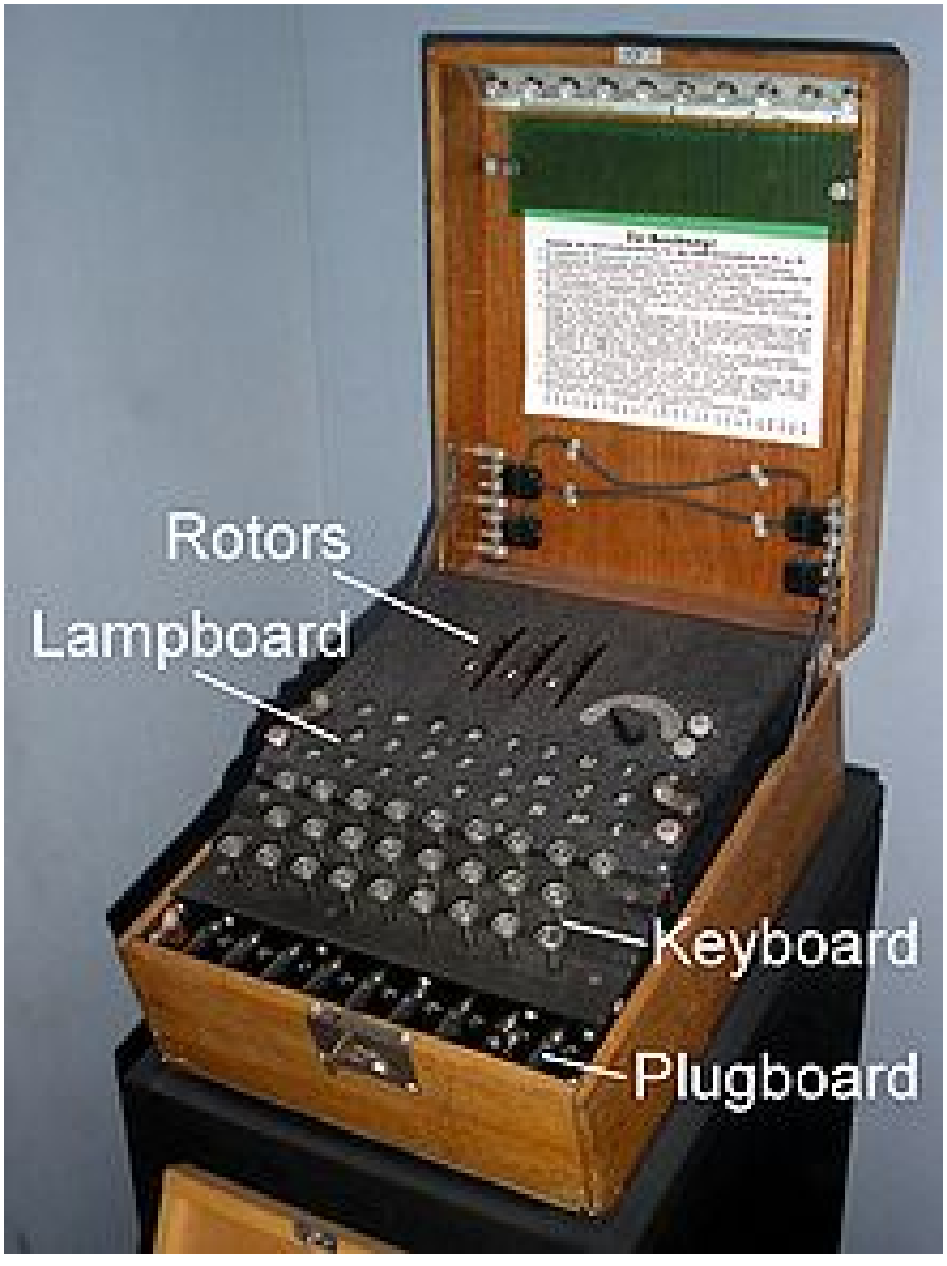
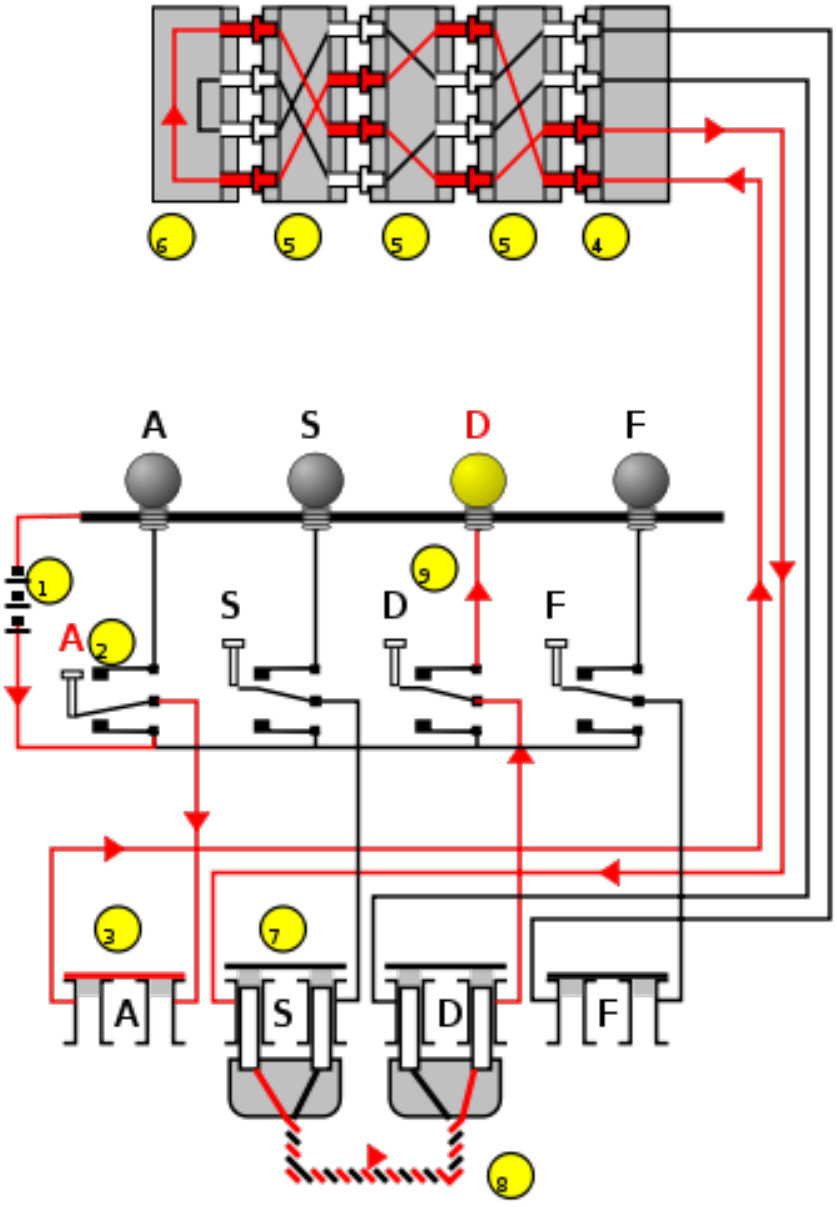
Cracking the Enigma

Rebecca Bellovin


Rotors
Lampboard
Keyboard
Plugboard


6
5
5
5
4
A
S
D
F
1
9
A
2
S
D
F
3
7
A
S
D
F
8

The Mechanism

The machine (in its simplest form) consisted of a keyboard, lamps (one for each letter), a plugboard, an entry drum, three rotors, and a reflector.

The Mechanism

The machine (in its simplest form) consisted of a keyboard, lamps (one for each letter), a plugboard, an entry drum, three rotors, and a reflector.
The cipher clerk presses a key, advancing the right-most rotor by one step and closing an electrical circuit. Current flows from the battery through the plugboard to the entry drum, from the entry drum to the rotors, through the rotors to the reflector, and then back through the rotors, entry drum, and plugboard, and lit up an appropriate lamp.

The Mechanism

The machine (in its simplest form) consisted of a keyboard, lamps (one for each letter), a plugboard, an entry drum, three rotors, and a reflector.

The cipher clerk presses a key, advancing the right-most rotor by one step and closing an electrical circuit. Current flows from the battery through the plugboard to the entry drum, from the entry drum to the rotors, through the rotors to the reflector, and then back through the rotors, entry drum, and plugboard, and lit up an appropriate lamp.

The entry drum, rotors, reflector, and plugboard are what scrambled the message.

Entry drum

The entry drum is a fixed part of the machine. It applies a fixed permutation, which was kept secret.

Rotors

There are three rotors in the machine at any given time. They can be removed and inserted in any order.

Rotors

There are three rotors in the machine at any given time. They can be removed and inserted in any order.
Each rotor is a disk, with 26 electrical contacts on one side and 26 pins on the other. There is internal wiring (which was kept secret) connecting each contact to a pin. The pins of each rotor touch the contacts of the rotor next to it, forming electrical circuits.

Rotors

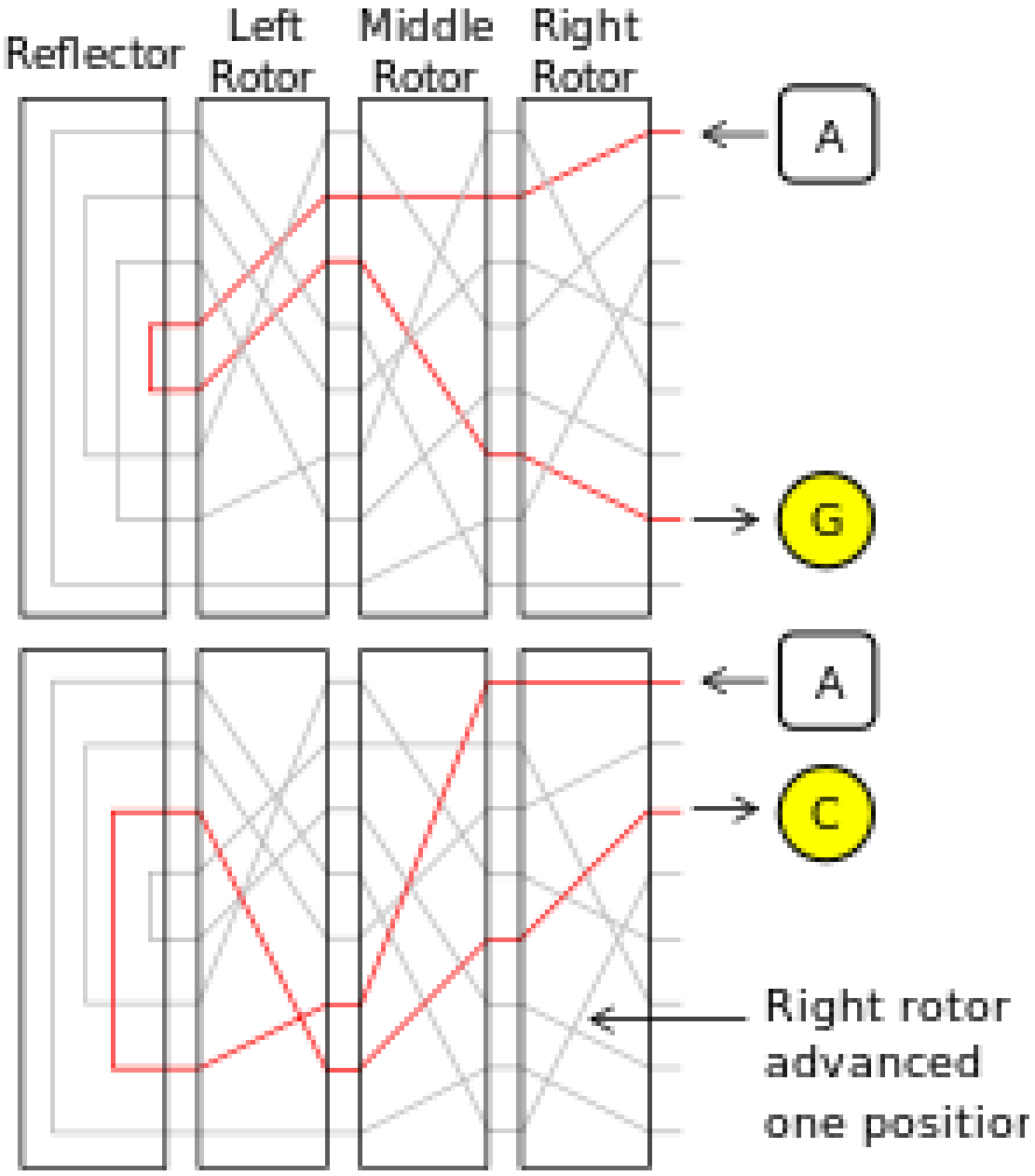
There are three rotors in the machine at any given time. They can be removed and inserted in any order.
Each rotor is a disk, with 26 electrical contacts on one side and 26 pins on the other. There is internal wiring (which was kept secret) connecting each contact to a pin. The pins of each rotor touch the contacts of the rotor next to it, forming electrical circuits.
Thus, each rotor applies a (different) permutation to the input from the entry drum. The rotors rotate during operation of the machine.

Rotors

There are three rotors in the machine at any given time. They can be removed and inserted in any order.
Each rotor is a disk, with 26 electrical contacts on one side and 26 pins on the other. There is internal wiring (which was kept secret) connecting each contact to a pin. The pins of each rotor touch the contacts of the rotor next to it, forming electrical circuits.
Thus, each rotor applies a (different) permutation to the input from the entry drum. The rotors rotate during operation of the machine.
At every keystroke, the right-most rotor advances one step. When it has made one full revolution, the middle rotor advances one step. When the middle rotor has made one full revolution, the left-most rotor advances one step.

Rotors (pictures)

Rotors (pictures)



Reflector

The reflector is a fixed piece of hardware in contact with the left-most rotor. It connects letters in pairs, and its wiring was kept secret.
This has two important consequences:

- Encryption is a transposition. So if (for some key setting) A encrypts to T, then (for the same key setting) T encrypts to A. So as long as the key is known, the same machine both encrypts and decrypts.

Reflector

The reflector is a fixed piece of hardware in contact with the left-most rotor. It connects letters in pairs, and its wiring was kept secret.
This has two important consequences:

- Encryption is a transposition. So if (for some key setting) A encrypts to T, then (for the same key setting) T encrypts to A. So as long as the key is known, the same machine both encrypts and decrypts.
- No letter can be enciphered to itself.

Plugboard

The plugboard (or *steckerboard*, or *steckerbrett*) swaps pairs of letters. The wiring is variable, and the cipher clerk swaps pairs of letters by plugging in a wire connecting them. Originally, six pairs of letters were swapped.

Summary

A key consists of

- A choice and ordering of three rotors.

Summary

A key consists of

- A choice and ordering of three rotors.
- A choice of six pairs of letters to be swapped via the plugboard.

Summary

A key consists of

- A choice and ordering of three rotors.
- A choice of six pairs of letters to be swapped via the plugboard.
- An initial rotor setting.

The internal wiring of the rotors, the wiring of the reflector, and the wiring of the entry drum were all difficult to change.

Permutations

Definition

A *permutation* on a set S is a bijection $f : S \to S$.

We are interested in permutations on the set of 26 letters.

Permutations

Definition

A *permutation* on a set S is a bijection $f : S \to S$.

We are interested in permutations on the set of 26 letters.
We can write a permutation as a product of disjoint cycles, in a unique way. For example, $(abcd)(e)(fg)(h)(i)(j)(k)(lmnop)\ldots$.

Permutations

Definition

A *permutation* on a set S is a bijection $f : S \to S$.

We are interested in permutations on the set of 26 letters.
We can write a permutation as a product of disjoint cycles, in a unique way. For example, $(abcd)(e)(fg)(h)(i)(j)(k)(lmnop)\ldots$.
Enigma's encryption can be represented as a composition of permutations

$$(\text{Plug})(\text{Ent})(\text{R1})(\text{R2})(\text{R3})(\text{Ref})(\text{R3})^{-1}(\text{R2})^{-1}(\text{R1})^{-1}(Ent)^{-1}(\text{Plug})^{-1}$$

Permutations

Definition

A *permutation* on a set S is a bijection $f : S \to S$.

We are interested in permutations on the set of 26 letters.
We can write a permutation as a product of disjoint cycles, in a unique way. For example, $(abcd)(e)(fg)(h)(i)(j)(k)(lmnop)\ldots$.
Enigma's encryption can be represented as a composition of permutations

$$(\text{Plug})(\text{Ent})(\text{R1})(\text{R2})(\text{R3})(\text{Ref})(\text{R3})^{-1}(\text{R2})^{-1}(\text{R1})^{-1}(Ent)^{-1}(\text{Plug})^{-1}$$

If the right-most rotor advances (and the middle and right-most rotor do not), the new encryption permutation is

$$(\text{Plug})(\text{Ent})(\rho\text{R1}\rho^{-1})(\text{R2})(\text{R3})(\text{Ref})(\text{R3})^{-1}(\text{R2})^{-1}(\rho\text{R1}\rho^{-1})^{-1}(Ent)^{-1}(\text{Pl}$$

where ρ is the cyclic permutation $(abcdefghijklmnopqrstuvwxyz)$.

Permutations (cont'd)

Note that Enigma encryption is of the form $Q(Ref)Q^{-1}$ for some permutation Q. This motivates the following definition.

Definition

Two permutations P, P' are said to be *conjugate* if there is a third permutation Q such that $P' = QPQ^{-1}$.

Permutations (cont'd)

Note that Enigma encryption is of the form $Q(Ref)Q^{-1}$ for some permutation Q. This motivates the following definition.

Definition

Two permutations P, P' are said to be *conjugate* if there is a third permutation Q such that $P' = QPQ^{-1}$.

Theorem

If P and P' are conjugate, their cycle decompositions have cycles of the same lengths, with the same multiplicities.

Permutations (cont'd)

Note that Enigma encryption is of the form $Q(Ref)Q^{-1}$ for some permutation Q. This motivates the following definition.

Definition

Two permutations P, P' are said to be *conjugate* if there is a third permutation Q such that $P' = QPQ^{-1}$.

Theorem

If P and P' are conjugate, their cycle decompositions have cycles of the same lengths, with the same multiplicities.

For example, suppose $S = \{1, 2, 3, 4, 5\}$, $P = (12)(345)$, and $Q = (12345)$. Then

$$P' := QPQ^{-1} = (12345)(12)(345)(54321) = (15)(234)$$

Permutations (cont'd)

Note that Enigma encryption is of the form $Q(Ref)Q^{-1}$ for some permutation Q. This motivates the following definition.

Definition

Two permutations P, P' are said to be *conjugate* if there is a third permutation Q such that $P' = QPQ^{-1}$.

Theorem

If P and P' are conjugate, their cycle decompositions have cycles of the same lengths, with the same multiplicities.

For example, suppose $S = \{1, 2, 3, 4, 5\}$, $P = (12)(345)$, and $Q = (12345)$. Then

$$P' := QPQ^{-1} = (12345)(12)(345)(54321) = (15)(234)$$

Definition

A *transposition* is a permutation with only length two cycles.

Consequences

Corollary

Engima encryption is a transposition with no fixed points.

Consequences

Corollary

Engima encryption is a transposition with no fixed points.

Proof.

Recall that Enigma encryption can be written $Q(Ref)Q^{-1}$, where Q is some permutation and (Ref) is the permutation induced by the reflector. But the reflector connects pairs of letters, and does not fix any of them, so its cycle decomposition is 13 cycles of length two. Therefore, the cycle decomposition of Enigma encryption is 13 cycles of length two. $\square$

The first problem

Polish intelligence assigned the mathematician Marian Rejewski the task of breaking Enigma.

The first problem

Polish intelligence assigned the mathematician Marian Rejewski the task of breaking Enigma.
The first problem was discovering the internal wiring of the rotors, the reflector, and the entry drum.

The first problem

Polish intelligence assigned the mathematician Marian Rejewski the task of breaking Enigma.
The first problem was discovering the internal wiring of the rotors, the reflector, and the entry drum.
Rejewski had access to months of intercepted messages, two months of daily keys (provided by French intelligence), and commercial models of Enigma.

How Enigma was used

A list of daily keys was distributed every month, specifying rotor choice and order, plugboard settings, and initial rotor settings. The rotor choice and order was only changed every three months.

How Enigma was used

A list of daily keys was distributed every month, specifying rotor choice and order, plugboard settings, and initial rotor settings. The rotor choice and order was only changed every three months.
To send a message, a cipher clerk first set his machine to the daily key. He then chose a new rotor setting, the message key, and typed it twice. Then he reset the rotors to the message key and typed the actual message.

Example

Example

The cipher clerk might choose the message key ASD. He would type ASDASD, which might be enciphered as FRSMIE.
A cryptanalyst seeing a message begin with FRSMIE knew that F and M, R and I, and S and E were examples of the same letter encrypted with different rotor settings.

Message keys

Let A, B, C, D, E, F denote the first six permutations applied by Enigma (on any given day). Then given sufficiently many messages from the same day, we can find the permutations AD, BE, and CF.

Message keys

Let A, B, C, D, E, F denote the first six permutations applied by Enigma (on any given day). Then given sufficiently many messages from the same day, we can find the permutations AD, BE, and CF.

Example

Suppose DMQ VBN, VON PUY, and PUC FMQ are three sets of enciphered message keys from the same day. Then $AD = (DVPF\ldots)\ldots$. In Rejewski's example,

$$\begin{aligned} AD &= (DVPFKXGZYO)(EIJMUNQLHT)(BC)(RW)(A)(S) \\ BE &= (BLFQVEOUM)(HJPSWIZRN)(AXT)(CGY)(D)(K) \\ CF &= (ABVIKTJGFCQNY)(DUZREHLXWPSMO) \end{aligned}$$

Why?

Because Enigma encrypts with transpositions! The permutation AD applied to the (enciphered message key) letter D is just the permutation D applied to the (plaintext) first letter of the message key.

Why?

Because Enigma encrypts with transpositions! The permutation AD applied to the (enciphered message key) letter D is just the permutation D applied to the (plaintext) first letter of the message key.
The permutations AD, BE, and CF are called the *characteristic set* of the day.

Second and third observations

Theorem

- *Let X and Y be two permutations whose cycle decompositions are composed only of disjoint transpositions (in our case, thirteen two-cycles). Then if (AB) is a cycle of either X or Y, A and B appear in different cycles of the same length of the permutation XY.*
- *If A and B appear in different cycles of XY of the same length and (AB) is a cycle of Y, then $\left((XY)^{-1}(A)(XY)(B)\right)$ (the letter to the left of A and the letter to the right of B) is also a cycle of Y. Similarly when (AB) is a cycle of X (or when A and B are replaced by arbitrary letters).*

Second and third observations

Theorem

- *Let X and Y be two permutations whose cycle decompositions are composed only of disjoint transpositions (in our case, thirteen two-cycles). Then if (AB) is a cycle of either X or Y, A and B appear in different cycles of the same length of the permutation XY.*
- *If A and B appear in different cycles of XY of the same length and (AB) is a cycle of Y, then $\left((XY)^{-1}(A)(XY)(B)\right)$ (the letter to the left of A and the letter to the right of B) is also a cycle of Y. Similarly when (AB) is a cycle of X (or when A and B are replaced by arbitrary letters).*

Furthermore, cipher clerks often chose bad message keys, such as AAA. Guessing even a few message keys often permitted the reconstruction of the individual permutations A, B, C, D, E, and F.

Example

Suppose we are in Rejewski's example, with

$$\begin{aligned} AD &= (DVPFKXGZYO)(EIJMUNQLHT)(BC)(RW)(A)(S) \\ BE &= (BLFQVEOUM)(HJPSWIZRN)(AXT)(CGY)(D)(K) \\ CF &= (ABVIKTJGFCQNY)(DUZREHLXWPSMO) \end{aligned}$$

and we suspect that some cipher clerk on this day chose the message key AAA. Since the singletons in AD are (A) and (S), we are looking for a message whose first and fourth letters are S.

Example

Suppose we are in Rejewski's example, with

$$\begin{aligned} AD &= (DVPFKXGZYO)(EIJMUNQLHT)(BC)(RW)(A)(S) \\ BE &= (BLFQVEOUM)(HJPSWIZRN)(AXT)(CGY)(D)(K) \\ CF &= (ABVIKTJGFCQNY)(DUZREHLXWPSMO) \end{aligned}$$

and we suspect that some cipher clerk on this day chose the message key AAA. Since the singletons in AD are (A) and (S), we are looking for a message whose first and fourth letters are S. Suppose we have three messages beginning with SUG SMF, SJM SPO, and SYX SCW. The first two cannot have come from AAA AAA, since U and J appear in nine-letter cycles of BE, whereas A appears in a three-letter cycle of BE (so neither (AU) nor (AJ) could be a transposition of B). But if we consider our third enciphered message key, Y and C both appear in three-letter cycles of BE (as does A), and X and W both appear in 13-letter cycles of CF (as does A).

Example (cont'd)

We assume the transposition (AY) is a cycle in B, and (AC) is a cycle in E. Then (XG) and (TC) are also cycles of B, and (TG) and (XC) are cycles of E.

Example (cont'd)

We assume the transposition (AY) is a cycle in B, and (AC) is a cycle in E. Then (XG) and (TC) are also cycles of B, and (TG) and (XC) are cycles of E.
Moreover, we assume that (AX) is a transposition of C and (AW) is a transposition of F. Then $C = (AX)(BL)(VH)(IE)(KR)(TZ)(JU)(GD)(FO)(CM)(QS)(NP)(YW)$ and so on for F.

Finding the rotors

On any given day, we may now assume we know the six permutations

$$A = (\mathrm{P})(\mathrm{E})(\mathrm{R1})(\mathrm{R2})(\mathrm{R3})(\mathrm{Ref})(\mathrm{R3})^{-1}(\mathrm{R2})^{-1}(\mathrm{R1})^{-1}(\mathrm{E})^{-1}(\mathrm{P})^{-1}$$
$$B = (\mathrm{P})(\mathrm{E})(\rho\mathrm{R1}\rho^{-1})(\mathrm{R2})(\mathrm{R3})(\mathrm{Ref})(\mathrm{R3})^{-1}(\mathrm{R2})^{-1}(\rho\mathrm{R1}\rho^{-1})^{-1}(\mathrm{E})^{-1}(\mathrm{P})^{-1}$$
$$C = (\mathrm{P})(\mathrm{E})(\rho^{2}\mathrm{R1}\rho^{-2})(\mathrm{R2})(\mathrm{R3})(\mathrm{Ref})(\mathrm{R3})^{-1}(\mathrm{R2})^{-1}(\rho^{2}\mathrm{R1}\rho^{-2})^{-1}(\mathrm{E})^{-1}(\mathrm{P})$$
$$D = (\mathrm{P})(\mathrm{E})(\rho^{3}\mathrm{R1}\rho^{-3})(\mathrm{R2})(\mathrm{R3})(\mathrm{Ref})(\mathrm{R3})^{-1}(\mathrm{R2})^{-1}(\rho^{3}\mathrm{R1}\rho^{-3})^{-1}(\mathrm{E})^{-1}(\mathrm{P})$$
$$E = (\mathrm{P})(\mathrm{E})(\rho^{4}\mathrm{R1}\rho^{-4})(\mathrm{R2})(\mathrm{R3})(\mathrm{Ref})(\mathrm{R3})^{-1}(\mathrm{R2})^{-1}(\rho^{4}\mathrm{R1}\rho^{-4})^{-1}(\mathrm{E})^{-1}(\mathrm{P})$$
$$F = (\mathrm{P})(\mathrm{E})(\rho^{5}\mathrm{R1}\rho^{-5})(\mathrm{R2})(\mathrm{R3})(\mathrm{Ref})(\mathrm{R3})^{-1}(\mathrm{R2})^{-1}(\rho^{5}\mathrm{R1}\rho^{-5})^{-1}(\mathrm{E})^{-1}(\mathrm{P})$$

I abbreviate Plug with P and Ent with E.

Finding the rotors

On any given day, we may now assume we know the six permutations

$$A = (\mathrm{P})(\mathrm{E})(\mathrm{R1})(\mathrm{R2})(\mathrm{R3})(\mathrm{Ref})(\mathrm{R3})^{-1}(\mathrm{R2})^{-1}(\mathrm{R1})^{-1}(\mathrm{E})^{-1}(\mathrm{P})^{-1}$$
$$B = (\mathrm{P})(\mathrm{E})(\rho\mathrm{R1}\rho^{-1})(\mathrm{R2})(\mathrm{R3})(\mathrm{Ref})(\mathrm{R3})^{-1}(\mathrm{R2})^{-1}(\rho\mathrm{R1}\rho^{-1})^{-1}(\mathrm{E})^{-1}(\mathrm{P})^{-1}$$
$$C = (\mathrm{P})(\mathrm{E})(\rho^2\mathrm{R1}\rho^{-2})(\mathrm{R2})(\mathrm{R3})(\mathrm{Ref})(\mathrm{R3})^{-1}(\mathrm{R2})^{-1}(\rho^2\mathrm{R1}\rho^{-2})^{-1}(\mathrm{E})^{-1}(\mathrm{P})$$
$$D = (\mathrm{P})(\mathrm{E})(\rho^3\mathrm{R1}\rho^{-3})(\mathrm{R2})(\mathrm{R3})(\mathrm{Ref})(\mathrm{R3})^{-1}(\mathrm{R2})^{-1}(\rho^3\mathrm{R1}\rho^{-3})^{-1}(\mathrm{E})^{-1}(\mathrm{P})$$
$$E = (\mathrm{P})(\mathrm{E})(\rho^4\mathrm{R1}\rho^{-4})(\mathrm{R2})(\mathrm{R3})(\mathrm{Ref})(\mathrm{R3})^{-1}(\mathrm{R2})^{-1}(\rho^4\mathrm{R1}\rho^{-4})^{-1}(\mathrm{E})^{-1}(\mathrm{P})$$
$$F = (\mathrm{P})(\mathrm{E})(\rho^5\mathrm{R1}\rho^{-5})(\mathrm{R2})(\mathrm{R3})(\mathrm{Ref})(\mathrm{R3})^{-1}(\mathrm{R2})^{-1}(\rho^5\mathrm{R1}\rho^{-5})^{-1}(\mathrm{E})^{-1}(\mathrm{P})$$

I abbreviate Plug with P and Ent with E.
This is *only* true if the middle and left-most rotors did not move while the first six letters were pressed. But this is a reasonable assumption since it is true in 21 cases out of 26.

Simplifications

We would like to know what $R1$, $R2$, $R3$, and Ref are.

Simplifications

We would like to know what $R1$, $R2$, $R3$, and Ref are.
The information from French intelligence gave the daily value of Plug for two months.

Simplifications

We would like to know what $R1$, $R2$, $R3$, and Ref are.
The information from French intelligence gave the daily value of Plug for two months.
Rejewski guessed the wiring in the entry drum (letters were connected in alphabetical order), giving Ent.

Simplifications

We would like to know what $R1$, $R2$, $R3$, and Ref are.
The information from French intelligence gave the daily value of Plug for two months.
Rejewski guessed the wiring in the entry drum (letters were connected in alphabetical order), giving Ent.
Writing $Q = (\mathrm{R2})(\mathrm{R3})(\mathrm{Ref})(\mathrm{R3})^{-1}(\mathrm{R2})^{-1}$, we now have six equations

$$\begin{aligned}
A' &= (\mathrm{R1})Q(\mathrm{R1})^{-1} \\
B' &= (\rho\mathrm{R1}\rho^{-1})Q(\rho\mathrm{R1}\rho^{-1})^{-1} \\
C' &= (\rho^2\mathrm{R1}\rho^{-2})Q(\rho^2\mathrm{R1}\rho^{-2})^{-1} \\
D' &= (\rho^3\mathrm{R1}\rho^{-3})Q(\rho^3\mathrm{R1}\rho^{-3})^{-1} \\
E' &= (\rho^4\mathrm{R1}\rho^{-4})Q(\rho^4\mathrm{R1}\rho^{-4})^{-1} \\
F' &= (\rho^5\mathrm{R1}\rho^{-5})Q(\rho^5\mathrm{R1}\rho^{-5})^{-1}
\end{aligned}$$

Simplifications (cont'd)

We write

$$\begin{aligned} U &= A' = (\mathrm{R1})Q(\mathrm{R1})^{-1} \\ V &= \rho^{-1}B'\rho = (\mathrm{R1}\rho^{-1})Q(\mathrm{R1}\rho^{-1})^{-1} \\ W &= \rho^{-2}C'\rho^{2} = (\mathrm{R1}\rho^{-2})Q(\mathrm{R1}\rho^{-2})^{-1} \\ X &= \rho^{-3}D'\rho^{3} = (\mathrm{R1}\rho^{-3})Q(\mathrm{R1}\rho^{-3})^{-1} \\ Y &= \rho^{-4}E'\rho^{4} = (\mathrm{R1}\rho^{-4})Q(\mathrm{R1}\rho^{-4})^{-1} \\ Z &= \rho^{-5}F'\rho^{5} = (\mathrm{R1}\rho^{-5})Q(\mathrm{R1}\rho^{-5})^{-1} \end{aligned}$$

so that we have the products

$$\begin{aligned} UV &= (\mathrm{R1})(Q\rho^{-1}Q\rho)(\mathrm{R1})^{-1} \\ VW &= (\mathrm{R1})\rho^{-1}(Q\rho^{-1}Q\rho)\rho(\mathrm{R1})^{-1} \\ WX &= (\mathrm{R1})\rho^{-2}(Q\rho^{-1}Q\rho)\rho^{2}(\mathrm{R1})^{-1} \\ XY &= (\mathrm{R1})\rho^{-3}(Q\rho^{-1}Q\rho)\rho^{3}(\mathrm{R1})^{-1} \\ YZ &= (\mathrm{R1})\rho^{-4}(Q\rho^{-1}Q\rho)\rho^{4}(\mathrm{R1})^{-1} \end{aligned}$$

Simplifications (cont'd)

Now we can eliminate Q from our equations to get the system

$$\begin{aligned} VW &= (\mathrm{R1})\rho^{-1}(\mathrm{R1})^{-1}(UV)(\mathrm{R1})\rho(\mathrm{R1})^{-1} \\ WX &= (\mathrm{R1})\rho^{-1}(\mathrm{R1})^{-1}(VW)(\mathrm{R1})\rho(\mathrm{R1})^{-1} \\ XY &= (\mathrm{R1})\rho^{-1}(\mathrm{R1})^{-1}(WX)(\mathrm{R1})\rho(\mathrm{R1})^{-1} \\ YZ &= (\mathrm{R1})\rho^{-1}(\mathrm{R1})^{-1}(XY)(\mathrm{R1})\rho(\mathrm{R1})^{-1} \end{aligned}$$

We know every quantity in these equations except (R1), and if our guesses were right (about the entry drum wiring and that only the right-most rotor moved), we can solve these equations for (R1).

Simplifications (cont'd)

Now we can eliminate Q from our equations to get the system

$$\begin{aligned} VW &= (\mathrm{R1})\rho^{-1}(\mathrm{R1})^{-1}(UV)(\mathrm{R1})\rho(\mathrm{R1})^{-1} \\ WX &= (\mathrm{R1})\rho^{-1}(\mathrm{R1})^{-1}(VW)(\mathrm{R1})\rho(\mathrm{R1})^{-1} \\ XY &= (\mathrm{R1})\rho^{-1}(\mathrm{R1})^{-1}(WX)(\mathrm{R1})\rho(\mathrm{R1})^{-1} \\ YZ &= (\mathrm{R1})\rho^{-1}(\mathrm{R1})^{-1}(XY)(\mathrm{R1})\rho(\mathrm{R1})^{-1} \end{aligned}$$

We know every quantity in these equations except (R1), and if our guesses were right (about the entry drum wiring and that only the right-most rotor moved), we can solve these equations for (R1). Since the order of the rotors changed the following month, Rejewski could run these calculations again for (R2), then for (R3) and (Ref).

Daily keys

Knowing the wiring of Enigma was only the beginning. Rejewski needed some way of discovering daily keys without fortuitous deliveries from French intelligence.