Unit 180
Фиалка

Fialka, also known as *M-125*, or *Фиалка* in Russian, is a cipher machine used by the Soviet Union during the Cold War. It had ten rotors, irregular stepping, a reflector with special properties, and a punchcard reader for implementing an alphabetic permutation on the way into and out of the rotor assembly. Unlike Enigma and SIGABA, the Fialka's rotors permute the Russian alphabet, or at least most of it.

The Russian alphabet (a version of Cyrillic) is

АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ

Take note that Ы looks like two, but is a single letter. Russian cryptographers typically treat Е and Ё as the same letter; some Russian civilians do as well. The full alphabet has thirty-three letters, but the rotors and punchcard of Fialka are designed to handle only thirty. This is the modified alphabet used by the machine:

АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЫЬЮЯЙ

The letter Й ("short i" or "и краткое") has been moved to the end, probably so that the ten rotors of the machine could be labeled А-К without confusion. Letter Ё is understandably missing, but so are Ъ and Э. After one of the many Russian revolutions, there was an orthographic revision of the language, and Ъ ("hard sign" or "твёрдый знак" or "turdy snack" as one student may have called it) was dropped at the ends of words. It is now a rather rare letter, and I cannot even think of a word that contains it right now. Letter Э is also rare, and almost always appears in words derived from foreign words; a suitable replacement is Е.

Versions of the Fialka machine were used in different regions of the U.S.S.R. and countries in the Warsaw Pact, and we don't have complete information about every variation. They differed in their rotor wirings and in how keys on their keyboards could be used for Latin letters and symbols. To distinguish a set of rotors from another, a designation such as "3К" is stamped on them, along with the letter denoting which rotor we have from the set (А through К). In Tables 180.2, 180.3, 180.4, and 180.5 are the wirings for series 68, used in Russia; 3К, used in Poland; 5К, used in Hungary, and 6К, used in Czechoslovakia. For variants of keyboard mappings to Latin letters and symbols in Poland, East Germany, and Czechoslovakia, see Table 180.1. At the time that this book is being written, there is no information about other versions of rotors or keyboard layouts.

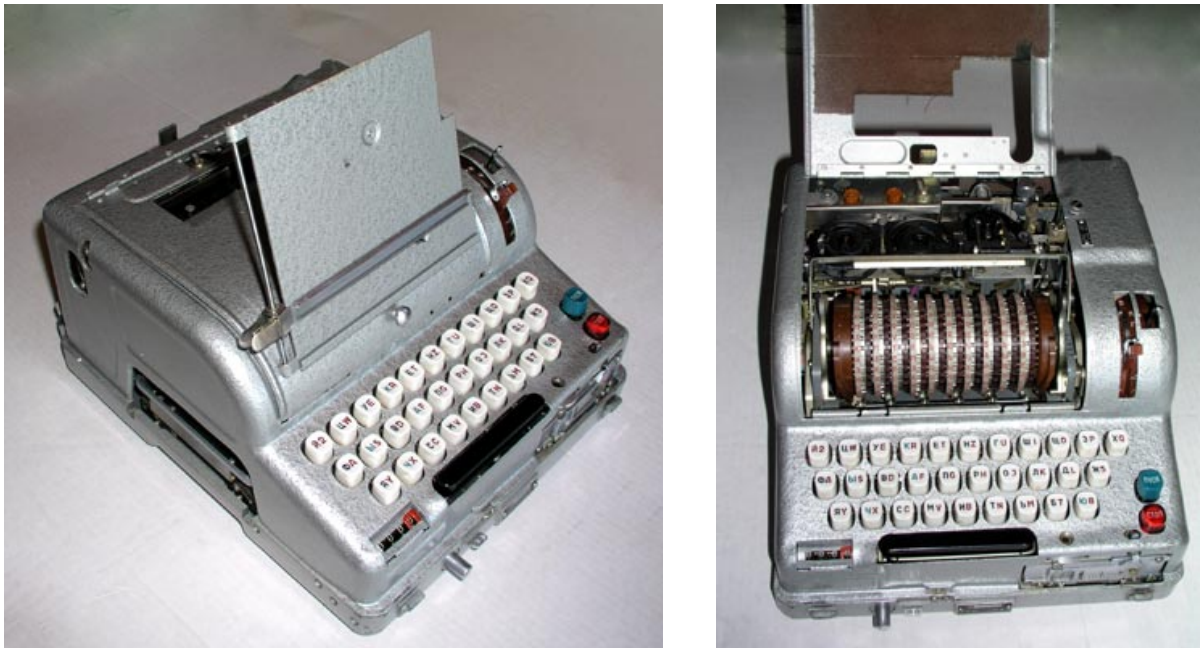


Figure 180.1: Fialka cipher machine. In the photo on the right, the cover is open and the rotors are visible. Photos from Tom Perera (EnigmaMuseum.com).

region	character set	Cyrillic key АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЫЬЮЯЙ
Poland	Latin: symbol:	FADULT5PBRKVZJGHCNE7QWXIOSM8Y2 Ą%-6)4 9?3(=5+ĘŁ:,2 01/78Ž.°'
East Germany	Latin: symbol:	F8DULT5PBRKVZ4GHCNEA327IOSM96J V:W6)4 9/3(X5JÄÜY,2 01F78Q.-Ö*
Czechoslovakia	Latin: symbol:	FADULT5PBRKVZJGHCNE7QWXIOSM8Y2 ŘÄČ6Ě4 9"3Ö=5ÜŽ+:,2 01/78Š.%-

Table 180.1: Substitutions for Latin letters and symbols used by Fialka. Ж *and* Ф *serve as symbol shift and letter shift, respectively. Non-Cyrillic letters were laid differently onto the keyboards in different regions of the U.S.S.R. In East Germany, the usual* Ä=AE, Ö=OE, Ü=UE, *and* ß=SS *or* SZ *can also be used.*

The Fialka cipher machine is very much like what an Enigma might have become if it had evolved under the control of the workers who have seized control of the means of production in order to lead the world into a brighter future. It has a keyboard, rotors, and reflector, but instead of the plugboard it has a punchcard reader for greater efficiency. The number of rotors has been increased to ten, and they have thirty contacts on each side. They are installed in any order into the machine beginning at the left end near the reflector (slot 1) and continuing to the end near the entry plate (slot 10). The reflector has been modified to avoid the weakness of Enigma that letters could not be enciphered to themselves. And the punchcard permutes the entire set of inputs, unlike Enigma's limit of the use of ten transpositions. We will now spend some time looking more closely at these components before we put the pieces together and see how a simulation might work.

The keyboard has thirty buttons for letters, of course, for the thirty letters listed above. But it also has a space bar, and it maps space to Й. Unfortunately, this means that yet another letter is unavailable. When Й is encountered in a plaintext, the output printer writes a space. The keyboard for machines used in various regions of the Soviet world had different substitutes for Latin letters. Those that are known are listed in Table 180.5. Between the keyboard and the punchcard reader the wiring of the machine carries a permutation which we call *S*:

$$S = (\text{СЩЙОЫХЕУАПЯФГЮШБЦЧТМЖДЬЗКИРНЛВ}) \tag{180.1}$$

The punchcard reader comes next. It holds a paper card with a 30×30 grid that unfortunately is not printed. Nevertheless, there can be exactly one hole punched in each row and exactly one in each column of this grid. Such a thing can be thought of like a 30×30 matrix with a single 1 in each row and column and 0 everywhere else (see Unit 123 for our introduction to matrices). Such a matrix, when multiplied by a column vector, performs a permutation on it. The punchcard reader takes the matrix defined by the holes in the card and applies the permutation to the thirty data lines coming to it from the keyboard (after passing through *S*). In Figure 180.2 is a reasonable facsimile of a Fialka punchcard. To read its permutation, look at the perforation (row of holes) near the top. If you discard the leftmost and rightmost holes of the perforation, then the remaining thirty define the columns of the grid. As you read from left to right, the letter that goes into writing down the permutation is which row is punched. In Figure 180.2, the first column has the fifth highest hole, so must be Д. The second column has the twenty-fourth highest hole, so must be Ш, etc. The permutation on this card is

$$P = (\text{ДШНЯЖЧВЙИБАЮХПЩТКГУСЫМЬЗФЕРОЛЦ})$$

As the signal leaves the punchcard reader and heads toward the rotors, it encounters another permutation built into the machine's wiring which we call *T*:

$$T = (\text{ЮОФШБРАКХЛСНУЙДЕЗПЧЩЬТВЯЮМЦЖИГ}) \tag{180.2}$$

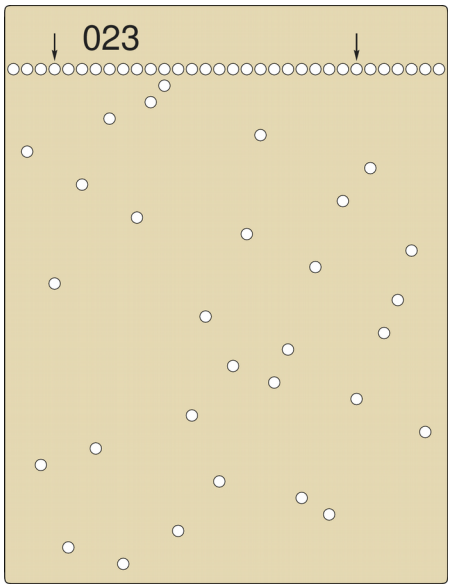


Figure 180.2: Facsimile of a punchcard for use in Fialka. The number indicates the day of the year in which it should be used. The arrows indicate the holes in the perforation through which alignment pins will protrude (pins are not placed symmetrically so that the card would not be placed in the machine upside-down). The permutation that this card represents has been randomly generated and should not be used in real-world communication.

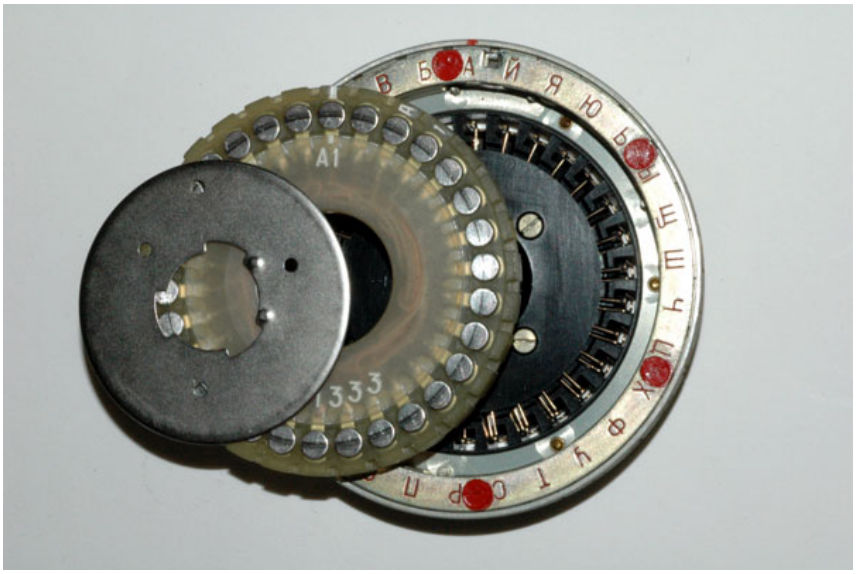


Figure 180.3: Disassembled configurable rotor from a Fialka machine. The red mark on the rim at the top is the indicator mark for the ring setting. The wiring core is A *and side 1 is showing. The white mark at the top of the wiring core is the indicator for its placement in the rotor frame. Photo from Tom Perera (EnigmaMuseum.com).*

Rotors have thirty contacts on each side, and thirty Russian letters on the rims. They come in two varieties: adjustable/configurable and non-adjustable/non-configurable. Non-configurable rotors cannot be changed. They can be installed into different slots in the machine and rotated to different positions (i.e. so that they display a different letter to the operator), but they cannot be installed in reverse orientation and their alphabet ring cannot be shifted, etc. The permutations in Tables 180.1, 180.2, 180.3, and 180.4 are for the non-adjustable rotors in series 68, 3K, 5K, and 6K. Each series has ten rotors, designated with one of the Russian letters А, Б, В, Г, Д, Е, Ж, З, И, К. Each has thirty contacts on each side, so effects a permutation of the subset of the Russian alphabet with thirty letters given earlier. The permutations in the tables are for a signal entering on the righ-hand side of a rotor and exiting on the left-hand side. The permutation when the signal returns and passes left to right is the inverse. For dealing with the rotations of rotors with thirty positions, we need a new set of rotation permutations. The first is

$$R_1 \;=\; (\,\text{БВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЫЬЮЯЙА}\,)$$

The rest can be generated from it. As we have seen before, the permutation of a rotor W that has been turned by n steps is its unrotated permutation W sandwiched between two rotations:

$$R_{-n}\, W\, R_n \tag{180.3}$$

The configurable rotors have three components: a rotor frame, an alphabet ring, and a wiring-maze core. The frame has the thirty letters on its side, so that the alphabet ring and wiring core can each be aligned to one of those letters. In addition, the core can be flipped over so that one of two sides can be facing outward/leftward (sides “1” and “2”) (the frame cannot be installed into the machine in reverse orientation). Recall that in Unit 179 we saw that installing a rotor W into SIGABA in reverse orientation gave us $X\, W^{-1}\, X$, where X is a reflection about the axis that runs through letters A and N. With Fialka, when we place a wiring core into a rotor frame so that side 2 is facing outward, we do something similar, and we need the reflection about the axis that passes through (Russian letters) А and Р. So our new X is

$$X \;=\; (\,\text{АЙЯЮЬЫЩШЧЦХФУТСРПОНМЛКИЗЖЕДГВБ}\,) \tag{180.4}$$

Things are a little more complicated now, since the core can be rotated when placed in the frame as well as flipped over. Suppose we take a rotor in its base configuration $W_{\text{base}} = W(0, 0, 1)$, which is the same as the non-adjustable version, and which has the ring setting at А=0, the wiring-core indicator mark aligned to А=0, and the core with side 1 facing outward. The effective new rotor with ring setting r and core alignment m is

$$W(r, m, 1) \;=\; R_r^{-1}\, R_m\, W(0, 0, 1)\, R_m^{-1}\, R_r \tag{180.5}$$

When the core is flipped, the new rotor is

$$W(r, m, 2) \;=\; R_r^{-1}\, R_m\, X\, W(0, 0, 1)^{-1}\, X\, R_m^{-1}\, R_r \tag{180.6}$$

rotor	input АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЫЬЮЯЙ
А	ГИЖЬУЦШЙВДБТЛАФЧЫОЯЮКПЕХЩРЗНСМ
Б	ПЧЯДЗТЙКЮОЫЛХГФНЩМШВБСИЦАУЖРЕЬ
В	ДЩОГЯАЬНЦРЖЛФПЙБУЫСЧВКШЗМТЕИЮХ
Г	ФЧТХНПМАУЫСЙЖЩОКЯЗИГЦДЬРБЕЛЮШВ
Д	ДФЗКГОЧЬЙШИНЕЫМАЛЩБЖСВРТЮХЯПУЦ
Е	ЬТБДРКУЯЮМИГЫХЩАЛЕЖФСПНЙЦШОЧЗВ
Ж	ЫЙЯВРЕОЛКШБДЦУМЩХФЬЗНГИЮАПЖТЧС
З	ЗЫРМШЖЦКХЬПИГОТЩДНЯЕБФЛСАЧУВЮЙ
И	ТСДМБЮЫУРЧФВЯШПКЦХЖИЗГЬОАЩЛНЙЕ
К	КЗШЬБДЖЛГЕМЙЧТЫПЯНВЩЮРАЦОИХФУС

Table 180.2: Rotor wirings of Fialka for rotors in series 68 used in Russia. These wirings are for non-adjustable rotors and for a signal entering from the left. For the adjustable rotors, these wirings match the configuration in which the wiring maze and rotor frame have the same letter designation, А *on the ring is aligned with* А *on the rotor frame, the indicator mark on the wiring maze is aligned with* А *and side* 1 *faces outward.*

rotor	input АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЫЬЮЯЙ
А	ЧЦВЖГЗРЕКФПСШИЙМЩЛАЮЬДЯЫБТХОНУ
Б	ВШФБЕХЫЖТГСЧПУКЙНЮЯЛИЩАОЦЗЬДМР
В	ФДЖПХЬГАЦСЧНЙЕЫКРОУТЯШВМИЛБЮЗЩ
Г	РХЮЛЬВПМШЙИСГФЩЗАЯУТОКДЧЫЖЕЦБН
Д	ТПАЦУРЯЗСГВОЕЙЧДЫНЩКМХЬФЖЛШИБЮ
Е	ИОНФШЗБЕДУЛЮЙВТПЖЩРАМЧЬЯСКХГЦЫ
Ж	ЖИДЫЕГУВЗЮЦМХШЧКНАРЯБЩЬПТЛОСЙФ
З	ЯЬПНЗБЩМЕЧИТШАОХСКВЛЦЖРГУЫДЙЮФ
И	ДУБЬФЫЖЛРТВНГЧЮХЕШЯЙПСИМЗЦЩКАО
К	ФШЗЩУАСДПЬИМЦКТВРЙГОЖЧЛБЯЫЮХЕН

Table 180.3: Rotor wirings of Fialka for rotors in series 3K used in Poland. These wirings are for non-adjustable rotors and for a signal entering from the left. For the adjustable rotors, these wirings match the configuration in which the wiring maze and rotor frame have the same letter designation, А *on the ring is aligned with* А *on the rotor frame, the indicator mark on the wiring maze is aligned with* А *and side* 1 *faces outward.*

rotor	input АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЫЬЮЯЙ
А	НЛКПАФШБГИЬСЫВМЗДРУЦЧЮОЩТЕЙЯЖХ
Б	ЕУЦАХНЮЫЙКИЖМЧСШЩЗФРГБПДТЯВЬЛО
В	ЩПЮЖУТОКШЕРИГФВЬЦДЗЯАМХЧСЫНБЙЛ
Г	ЧВШНГЫТПЛЕЯЦЩЖИХФБОСУЙЗКМАРЮДЬ
Д	РЦИБЕДАМГСОХТПЮЬЗЛЯВЩКУЫЧНШФЖЙ
Е	КЕЗФЧЬЫГЯТСХШЛОЮАДНМЦВРУЖИЩЙБП
Ж	ХЙЫВРЮФИЩАЖСКЕЬЧМБЦШОЛЗГУДНПЯТ
З	ШСЛФЙЯУКЖХЕТБАДНЬМПЩГЧОЮИВЫРЗЦ
И	СИБГФЬРКХЖПЯЫЩТОЛЙЦМЮЧНЗАЕДВШУ
К	БМДЗНЯКУЩШРЖЦЬЫЮЙЕГИЛТСЧАВОФПХ

Table 180.4: Rotor wirings of Fialka for rotors in series 5K used in Hungary. These wirings are for non-adjustable rotors and for a signal entering from the left. For the adjustable rotors, these wirings match the configuration in which the wiring maze and rotor frame have the same letter designation, А *on the ring is aligned with* А *on the rotor frame, the indicator mark on the wiring maze is aligned with* А *and side* 1 *faces outward.*

rotor	input АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЫЬЮЯЙ
А	НЦЗТФМЮГПЬВДРОЧЫАЩСЛЙКШЖЕХЯБИУ
Б	ФЗДПГЮХАШНЯМОЧЩЖИЙЬВЛТСУЦКБЫЕР
В	ЯЛГЦШРТБЧВСЗФДЮМПЫЙЖХУНКЬЩИАОЕ
Г	ГМУЯШЧЖЙПАФОТБРЬКЩСЮЕХЛЗЦДИВЫН
Д	ТБПЖФЮЗНЧМУЬГШКОЛЕЙВСЫЦАЯЩРХДИ
Е	РГОШЧУЙВАЗЬНИДЯКПЫЦЖЩСФЛБЕХЮТМ
Ж	ЫЧЖДНЗШЙЯФЦИМКЩРВХУТГАЮЬЕБПСЛО
З	РЦОЙШПСФГЖЬМЕНЩХАДЫЗЛЧЯЮВТКУБИ
И	МАСЯЕГЖЛПВХЩИЫЙНЦФКШЬОЮЧБДУТРЗ
К	ИХЗРЩДФЦГЬОУАПЙБКСЖШМТЯВЧЕНЮЫЛ

Table 180.5: Rotor wirings of Fialka for rotors in series 6K used in Czechoslovakia. These wirings are for non-adjustable rotors and for a signal entering from the left. For the adjustable rotors, these wirings match the configuration in which the wiring maze and rotor frame have the same letter designation, А *on the ring is aligned with* А *on the rotor frame, the indicator mark on the wiring maze is aligned with* А *and side* 1 *faces outward.*

Stepping of the rotors occurs after each letter is enciphered and is irregular. Rotors in slots 1, 3, 5, 7, and 9 (counting from left to right) are ganged together, and their motions are interrelated. They only rotate in the forward direction, i.e., so that the letter describing its positions changes to the following one in the thirty-letter subset of the alphabet (with wrap-around). The rotor in slot 9 steps every time. The rotors in slots 1, 3, 5, and 7 cannot rotate if an advancement-blocking pin is present on the rotor in slot 9 at a position 20 further than its current position. If the pin is not present, then the rotor in slot 7 steps. The rotors in slots 1, 3, and 5 cannot rotate if a pin is present on the rotor in slot 7 at a position 20 further than its current position. Without that pin, the rotor in slot 5 steps. The same behavior continues, so we see that a rotor in an odd-numbered slot cannot advance if it is blocked by a pin on a rotor in any other odd-numbered slot to its right. Rotors in slots 2, 4, 6, 8, and 10 work together and rotate in the reverse direction, i.e., so that the letter indicating its current position changes to the one preceding it in the alphabet. The rotor in slot 2 is the one that steps every time. Each of the others is blocked from stepping if there is a pin in a position 17 further than the current position of any rotor in an even-numbered slot to its left. The positions of the stepping-inhibiting pins for series 68, 3K, 5K, and 6K are in Tables 180.6, 180.7, 180,8, and 180.9.

rotor	pin locations																													
	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Ю	Я	Й
А		×	×		×			×		×	×		×	×	×			×	×			×	×	×			×	×	×	
Б	×		×	×	×	×		×	×			×	×	×	×	×		×	×	×	×		×	×	×	×	×		×	×
В					×			×		×				×			×		×			×	×	×		×	×			
Г		×		×	×	×	×		×	×		×	×	×	×	×		×			×	×	×				×		×	×
Д			×	×		×	×				×		×									×								
Е	×						×		×	×	×	×			×		×	×	×	×	×			×	×			×	×	×
Ж	×	×	×	×					×				×		×	×						×	×		×	×		×		
З						×				×								×		×					×	×			×	
И		×					×	×	×	×		×								×				×	×			×	×	
К		×	×		×	×	×					×		×	×		×						×			×				

Table 180.6: Locations of stepping-inhibiting pins on the rotors in series 68.

rotor	pin locations АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЫЬЮЯЙ
А	× × ××× × × ×× ×× × × ×
Б	× × × × × ××××× ×× × ×××
В	× × × × × × ×
Г	× ××××× ×× × ×××× ×××××× ××× ×
Д	× × ×× × × ×
Е	× × × ×××× × ×××× ×
Ж	× ×××××× ×××××× × ×××× ×××× ×
З	× ××× × × ×
И	×××× × × ×× × × ××××× ×
К	× × × ××× ×× ×× ×××

Table 180.7: Locations of stepping-inhibiting pins on the rotors in series 3K.

rotor	pin locations АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЫЬЮЯЙ
А	×××× × ×× ×× × ×
Б	× × × × × × ×
В	× × × × × × ××
Г	× × × × × × ×
Д	× × × × ××× × × × ×
Е	×××× × × × × × ××
Ж	× ×× ××× × × ×× × ××
З	×× × × ×××× ×× ×× × ×××× ××
И	×× ×× ×××× × × ×××× ×××
К	×× × ××××× ××× ××× ×× ××

Table 180.8: Locations of stepping-inhibiting pins on the rotors in series 5K.

rotor	pin locations АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЫЬЮЯЙ
А	××× × × × ×× ×× ×× ×××× × ××
Б	× × × × × × ×× × ×
В	× × × × × × × ×
Г	× × ××× ×××××× ×××× × ××× ×
Д	× × × × × × ×
Е	× ××× ××× ×××××× ××× × ×
Ж	××× ××× ××× × ×××××× ×
З	×× ×× × × ××××××
И	× ×× × × × × ×
К	××× ×× ××× ×××××× ××× ××× ×× ××

Table 180.9: Locations of stepping-inhibiting pins on the rotors in series 6K.

Unlike Enigma, Fialka has only one reflector. It is permanently installed in the machine; it cannot be removed; it cannot be rotated. And to improve on the Enigma, it has some innovations. While most of the connections are wired in pairs, like in any other self-respecting reflector, a signal on connector 12 (counting from zero) indicates that a plaintext letter should be enciphered to itself. This eliminates the weakness that Enigma had in its inability to do this. In Fialka, since one connector has this property, any given plaintext letter has a one in thirty probabililty of being its own ciphertext letter; this is just what would be expected from a process that randomly assigns ciphertext letters. Since it is impossible to send a signal back again on the same connector, some circuitry in the reflector instead sends a signal back to the keyboard to tell it to bypass the entire encryption process and send the plaintext letter to the output. Nevertheless, when we are creating a simulation of the Fialka, we can ignore this physical impossibility and simply allow the reflector's permutation to map Н to Н. But now we have another problem: with one connection used for itself, there is an odd number remaining. We cannot map another connection to itself, because that would spoil the appearance of randomness. To solve this problem, the makers of the Fialka introduced another bit of circuitry that performs a 3-cycle on connections 15, 17, and 23. This breaks the self-reciprocity of the reflector, so some more circuitry must be added to reverse this 3-cycle when the machine is in decryption mode. Here is the permutation of the reflector during encryption. We call it *U* as we did for Enigma. Above it we write the rotor alphabet so that we can see the 3-cycle more easily.

$$\begin{array}{c} \text{АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЫЬЮЯЙ} \\ U = (\,\text{ЧЕФЮОБМСЦЛКЖНДЯТЗШЬВЩИАРХЙУГПЫ}\,) \end{array} \qquad (180.7)$$

Notice the 1-cycle (Н) and the 3-cycle (РТШ). All other letters are in 2-cycles.

We are finally ready to put all of the pieces together. In Figure 180.4 is an overview of the Fialka cipher machine. When a letter is processed, these things happen:

1. A key for the letter is pressed on the keyboard. If the key is the space bar and the machine is in encryption mode, then the character is changed to Й by the keyboard. The signal leaves the keyboard.
2. The signal passes through permutation S (Equation 180.1).
3. The signal passes through permutation P of the punchcard reader.
4. The signal passes through permutation T (Equation 180.2).
5. At the entry plate to the rotor assembly, there is a rotation by 3 because the letters indicating the positions of the rotors are not centered in the machine.
6. The signal passes through the ten rotors in reverse order (right to left, slot 10 to slot 1). Despite the reversal of rotor order, the permutation of each is in its forward direction.
7. Between the rotor assembly and the reflector is a rotation by −3. See number (5) above.
8. The signal passes through permutation U (Equation 180.7) if the machine is in encryption mode. If the machine is in decryption mode, the permutation is U^{-1}.
9. A rotation by 3 when entering the rotor assembly.
10. The signal passes through the ten rotors in forward order (left to right, slot 1 to slot 10). The permutation of each is the inverse of the permutation in step (6).
11. Rotation by −3 at the entry plate.
12. Permutation T^{-1}.
13. Permutation P^{-1}.
14. Permutation S^{-1}.
15. If the machine is in decryption mode and the resulting signal is Й, then the printer outputs a space. Otherwise, it prints the letter that it receives.

The overall permutation effected by the machine during encryption is (ignoring the bits about space bar and Й)

$$F = S^{-1}\, P^{-1}\, T^{-1}\, R_{27} \prod W_i^{-1}\, R_3\, U\, R_{27} \prod W_i\, R_3\, T\, P\, S \tag{180.8}$$

Remember that operators act on what comes to them from the right and so this product of operators works from right to left. We have used $\prod W_i$ and $\prod W_i^{-1}$ as shorthand for

$$\begin{aligned} \prod \mathrm{W}_i &= \mathrm{W}_1\, W_2\, W_3\, W_4\, W_5\, W_6\, W_7\, W_8\, W_9\, W_{10} \\ \prod W_i^{-1} &= W_{10}{}^{-1}\, W_9{}^{-1}\, W_8{}^{-1}\, W_7{}^{-1}\, W_6{}^{-1}\, W_5{}^{-1}\, W_4{}^{-1}\, W_3{}^{-1}\, W_2{}^{-1}\, W_1{}^{-1} \end{aligned}$$

where W_i is the permutation of whatever rotor is in slot i in whatever position it currently is in. A configurable rotor is constructed as in Equations 180.5 and 180.6. All rotors are rotated to their current positions according to Equation 180.3.

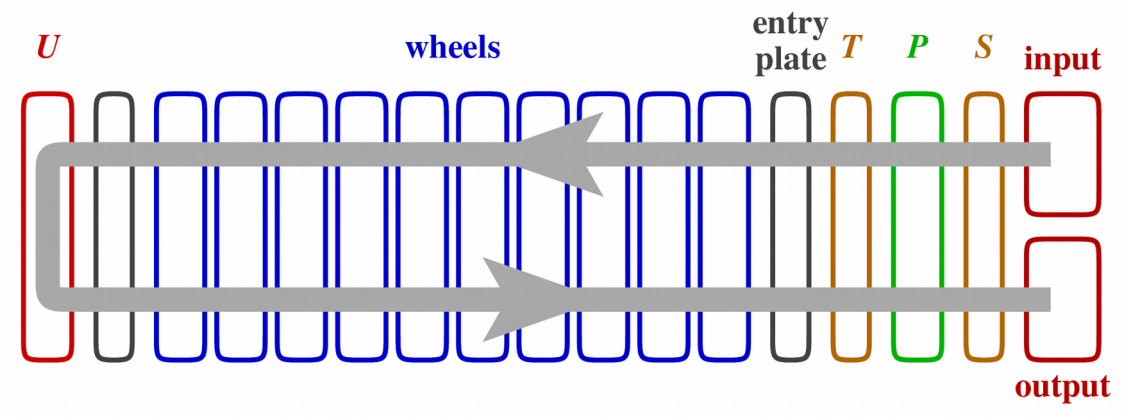


Figure 180.4: Functional overview of the Fialka cipher machine. Input from the keyboard (30 wires) passes through permutation S, the punchcard reader P, permutation T, a rotation for the entry plate, ten wheels, a rotation between the wheels and reflector, the reflector U, and back again in reverse to the output.

The internal settings of the Fialka machine form the daily key. For machines with rotors with fixed wiring, the daily key is a list of ten rotors in the order in which they are installed on the spindle, from left to right (from the reflector toward the punchcard). For machines equipped with configurable rotors, the specific contents of the daily key are five lists of ten items and the punchcard. The first item in each list describes what is placed in the first slot, etc. The lists describe

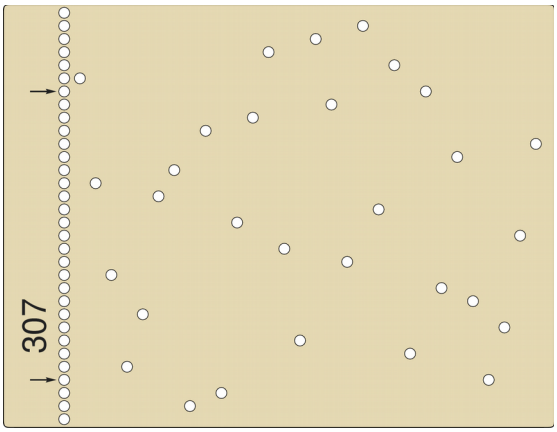
- the choice of rotor frame (Russian letter)
- the ring setting (Russian letter)
- the identity of the wiring core (Russian letter)
- whether the wiring core is installed upside-up or upside-down (digit 1 or 2)
- the position of the indexing mark on the wiring core (Russian letter)

The initial positions of the rotors serve as the message key.

For example, if we are working with a machine with non-configurable rotors from series 3K, and our key is this one, which was randomly generated:

daily key: ЕЗКАВ ИГЖДБ

message key: ВЫДЮЛ ЗХСКЧ



The permutation given by the punchcard is

$$P = (\text{ЗКЬГЦПЮДЫШВТОЯЛФЕБЖЩЙИМСЧАХНРУ})$$

Here is a typical message that we can encrypt:

THIS MESSAGE IS ENCRYPTED WITH FIALKA

The first thing to do is rewrite the message in Russian, with Й in place of spaces.

ЕРШЫЙЬУЫЫБПУЙШЫЙУТСКЯЗЕУВЙЦШЕРЙАШБДЛБ

The machine is loaded with non-configurable rotors such that rotor Е is in the first slot, rotor З in the second, К in the third, etc. The rotors are initial set to the positions given by the message key: the first at В, the second at Ы, etc. The resulting permutation from Equation 180.8 is

УЛНЮЫЙПФСЩБЧВХЖШИТАЗОРМЦКДЯГЬЕ

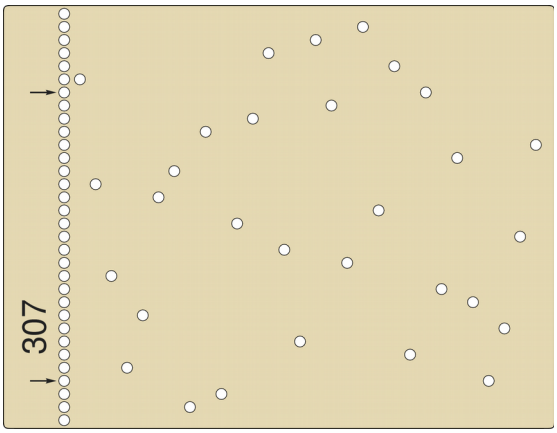
This permutation maps the plaintext letter Е to Й. Next, since there is a steeping-inhibiting pin at Н on rotor З in slot 2 (17 steps ahead of its current position, Ы) (Table 180.7), the rotors in slots 4, 6, 8, and 10 do not step at this time. There are no pins blocking the rotors in slots 7 and 5 from stepping, but those in slots 3 and 1 cannot step. So the rotor positions go from ВЫДЮЛЗХСКЧ to ВЩДЮМЗЦСЛЧ and we are ready for the second letter of the text. We continue until we have the full ciphertext:

ЙЩНШВЯХГЬЛЮЫЧЮРФУЧЙМКЗЛЕНШЕРЙГЦЫЮЗМДБ

Now let's expand the daily key for a machine with configurable rotors. The new settings were also randomly generated.

daily key: ЕЗКАВ ИГЖДБ
ШЖВЙМ ЛПХЦЕ
БЗГКИ АДЖВЕ
21121 11221
ВЧЩЫР ЯЛПБИ

message key: ВЫДЮЛ ЗХСКЧ



The first slot contains a rotor comprised of the Е frame with the Б wiring core installed with side 2 facing outward, ring setting Ш=23, and core alignment В=2. The other slots contain rotors configured according to the respective columns in the key. The permutation on the punchcard is the same as before. With this key, the same plaintext becomes this ciphertext:

МТЧЬГДХМАБФПЬЫОСФЕГЯУЮТЩОРШЦЧЛРЧЛПГИТ

Reading and references

Thomas B. Perera and David Hamer, “General Introduction: Russian Cold War Era M-125 and M-125-3MN Fialka Cipher Machines,” 2005, http://w1tp.com/enigma/mfialka.htm

Thomas B. Perera and David Hamer, “Rotor Technical Descriptions and Wiring and Stepping Data for the M-125-MN and M-125-3MN/-3MP3 Russian Fialka Cipher Machines,” 2005, http://w1tp.com/enigma/mfr.htm

Paul Reuvers and Marc Simons, Fialka M-125: Detailed description of the Russian Fialka cipher machines, version 2.0, 2009-06-22, https://www.cryptomuseum.com/pub/files/Fialka_200.pdf

If you see “36” in the table for the rotor wirings of series 5K, it should be “26”.

Crypto Museum pages on the Fialka:

main page:	https://www.cryptomuseum.com/crypto/fialka/index.htm
functional overview:	https://www.cryptomuseum.com/crypto/fialka/block.htm
rotors:	https://www.cryptomuseum.com/crypto/fialka/wheels.htm
rotor wirings:	https://www.cryptomuseum.com/crypto/fialka/wiring.htm
reflector:	https://www.cryptomuseum.com/crypto/fialka/magic.htm
punchcards:	https://www.cryptomuseum.com/crypto/fialka/card.htm

Python tips

Python version 3 does everything in eight-bit Unicode by default, so there is nothing special that you need to do (in Python 2 you needed to set the encoding of your files in a special comment). Printing to console may be a problem if you don’t have that set up right.

The Russian letters are at these Unicode points (in hexadecimal):

А-Я	U+0410 through U+042F
а-я	U+0430 through U+044F
Ё	U+0401
ё	U+0451

Of course, it may be easier to just open this document in software that allows you to copy and paste this alphabet:

АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ

Remember that ы is one letter and that often, Е and Ё are treated as the same letter.

The string methods `.upper()` and `.lower()` work on Russian, too.

Programming tasks

1. Simulate the Fialka in Python. This can be a good exercise in using a non-English alphabet and creating files in Unicode.

2. If you are ambitious, try installing the `Pillow` package in Python and use it to create a punchcard reader that takes a graphic file and outputs the permutation. Specifications for the physical size and positions of the holes can be found in the reference by Reuvers and Simons. For information about `Pillow`, you might start here: https://pillow.readthedocs.io/en/stable

Exercises

1. Use a Fialka with series-3K non-configurable rotors and the Polish keyboard to encrypt this English text with the given key. Use the punchcard in Figure 180.2. Discard punctuation but retain spaces, which become Й before encryption. Express the ciphertext in two ways: as Cyrillic output and as Latin output.

   daily key: ИЗГЖВ БКДАЕ
   message key: ИЫШЬЮ ГДФХЯ

   There was once an emperor, very great and mighty, and he ruled over an empire so large that no one knew where it began and where it ended. But if nobody could tell the exact extent of his sovereignty everybody was aware that the emperor's right eye laughed, while his left eye wept. One or two men of valour had the courage to go and ask him the reason of this strange fact, but he only laughed and said nothing; and the reason of the deadly enmity between his two eyes was a secret only known to the monarch himself.

   (from “The Fairy of the Dawn” in *The Violet Fairy Book* by Andrew Lang)

2. Use a Fialka with series-68 non-configurable rotors to encrypt this Russian text with the given key. Use the punchcard in Figure 180.2. Discard punctuation and spaces. The lower-case Russian letters almost always look like their upper-case counterparts; the only ones that do not are Аа, Бб, Ее, Ёё, and even then б is the only weird one.

   daily key: ВИКАБ ГЖДЕЗ
   message key: ДЩСЧИ СХЫРС

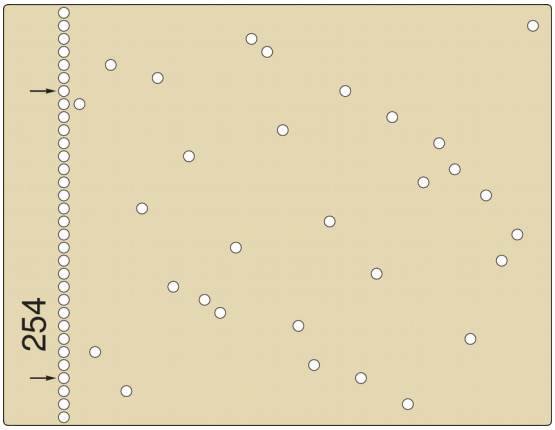
   Возможно ль? вместо роз, Амуром
   насажденных,
   Тюльпанов, гордо наклоненных,
   Душистых ландышей, ясминов и лилей,
   Которых ты всегда любила
   И прежде всякий день носила
   На мраморной груди твоей—
   Возможно ль, милая Климена?

   (from «Красавице, которая нюхала табак» by Aleksandr Sergeevich Pushkin)

3. Decrypt this ciphertext which was prepared with a Fialka using the series-6K configurable rotors and the Czech keyboard. The key is given, and the punchcard is shown below. Spaces, but not punctuation, were kept in the English plaintext.

daily key: ИДАЖЕ ЗВБКГ
ДЧВЩЫ НЫСАЕ
ГИДВБ ЕЗКАЖ
12112 11212
ЛВЩВФ ХАРВТ

message key: ЬЙФШЯ ЬЦЫНЦ

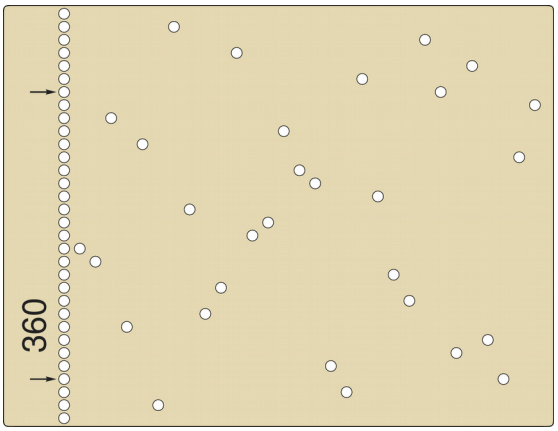


ШЙРЙНАЖТМРВТПЩЛШЯДЦСОСХТЛЖБСХПЮИХЧФЛАЧРКНЯЩГНЛОИНКЙБВСПМШЧЕЫ
ДИШЙЗНЕВДЬВЕЯЬСРТХКШЖФМЫЬЯЬЗЧРКНБШОЖЧЩВПЗДНТЦЫСБЗЧУЬРОХЛПХДФ
АСУГЗЖЗХРЫЖДЩУЙСЙИЫСДЙВРТНБАСКУАЛВМКЛНЦЗТЙКТРМЖЩФАЕФМУХЖИЫШР
ЧБЦОЫЛИТМЛЩЮНВМАМТРСШТКЗПЦЦНЙФЖЗЗТСНШЗБГКЬЛЬЕФПКОЕИЮЖХГЧДЖМБ
ШУХЬСТМЫБДВХУЫРРШСЫПЮЧЮЩФКГЫДЬЯПЕБСЮЖСИРЛБТФХПТЦЖСЬЕЦУЖКФЫАМ
ЦЯФЦЬХВБЧТОЬХПРПЮЫНОИЖФЬЖЧНХДКУОМРЙСЯВГХХНЖВЧЖХБШАНКМЖХЖФЩЦЛ
ВОСЦЗЮЗЮРЧЮАЙЛБАДЛШБЧЖЗЬИЖАЮЬЙЗЯПВХГГЩЖЮГВКПРФАЕХСЦРРЛЕЮШТНФ
ССЧЮПУМЙЛВЯДЮЗВАФЩАУЩЖАФРСУЩОФЯФБ

4. Find the missing parts of the message key. The text is in English using the Polish keyboard mapping. Spaces, but not punctuation, were retained in the plaintext. The rotor set is from series 3K. The punchcard is shown below.

daily key: КГБДИ ЖЗАВЕ

message key: ПШХГБ ?????



ТТТАГЩЖБШПТИЯЯСЕХДЮИКЛАПДЮОЗОМЩДСЛМФОФЛАЧТЗУЯЖЬДГЫДЙМАНСАЩРФ
ЯРВЮШДТХДФЫЫЧВРЮРАЛЗКЗШШГЬХДЩГРНЙПУЖЦНЙЯУСАЬФСИЧЬУИХЖТШКСТЯМ
АДРЖТОЩМПОЬФЙЙАДТРИОЫХРХБСШЕЯВЬЕУВЮЕТШЖГПЧОЖАХГШЬЯЬНМЬКПЖЬНЮ
ГФНОШАЕИЩЖЛЙЧЖФУОВФВКЧЧМГХРЖНААБЫДЧЯЮЬЕЙЬТЖХЛКДКЙЕКЬЗБЛЫУРНФ
МЕКДУПРЧЦБЬСЕХЩОШАННЗИЗБУГШЮЛЙПУЙСВКЬЖЮДФЬЧУААЩНЩИИЛМСУФЧДТГ
ЯЗТХЮУЦЦУНМГЬВЫНБЗЖЬФХМУРБАФЧОЕАЕЯВНЧРЮОЗЕЧРРЙУГФШУЧЛМЯТСМЮЕ
ИАЧББЮЗЮРТЕБФЗУМЧЫЬТДЬМПВЫБШБ

5. Learn the Russian language.
6. Используй твою симуляцию Фиалки чтобы зашифровать сообщение Кремлю.