

Podstawowa wersja Enigmy używała trzech z 8 możliwych wirników, każdy z nich miał 26 liter alfabetu łacińskiego w kolejności od A-Z. Różniły się one jedynie miejscem, w którym wirnik obracał następny oraz połączeniem między literami. Oprócz trzech wirników mamy jeszcze reflektor, który odwraca naszą literę i przesyła ją ponownie przez wirniki.

Użyjmy I, II i III wirnika - pierwszy obraca następny wirnik po literze "Q", drugi po "E", a trzeci po "V". Możemy również ustawić litery początkowe - ja wybrałem "B", "K" i "P". Poniżej znajduje się układ połączeń między literami pierwszych pięciu wirników oraz reflektorów.

Numer wirnika	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
I	E	K	M	F	L	G	D	Q	V	Z	N	T	O	W	Y	H	X	U	S	P	A	I	B	R	C	J
II	A	J	D	K	S	I	R	U	X	B	L	H	W	T	M	C	Q	G	Z	N	P	Y	F	V	O	E
III	B	D	F	H	J	L	C	P	R	T	X	V	Z	N	Y	E	I	W	G	A	K	M	U	S	Q	O
IV	E	S	O	V	P	Z	J	A	Y	Q	U	I	R	H	X	L	N	F	T	G	K	D	C	M	W	B
V	V	Z	B	R	G	I	T	Y	U	P	S	D	N	H	L	X	A	W	M	J	Q	O	F	E	C	K
REFLEKTOR (UKW) B	Y	R	U	H	Q	S	L	D	P	X	N	G	O	K	M	I	E	B	F	Z	C	W	V	J	A	T
REFLEKTOR (UKW) C	F	V	P	J	I	A	O	Y	E	D	R	Z	X	W	G	C	T	K	U	Q	S	B	N	M	H	L

Spróbujmy teraz zakodować prostą wiadomość - musimy jednak pamiętać, że klasyczna Enigma nie używa polskich znaków. Niech tą przykładową wiadomością będzie "Cześć" czyli "Czesc" dla naszej maszyny.

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Spróbujmy zaszyfrować pierwszą literę tej wiadomości:

0. Na początek musimy znać kolejność z jaką nasza litera przechodzi przez maszynę. Zaczynamy od ostatniego wirnika, idąc ku pierwszemu. Tam uruchamia się reflektor, który przekształca naszą literę i wysyła z powrotem od pierwszego do ostatniego wirnika.

1. Litera "C" przesuwa nasz ostatni (trzeci) wirnik mechanicznie o 1 miejsce do przodu na literę Q (dla każdej nowej litery ostatni wirnik przewraca się o jedną pozycję dalej), a sygnał idzie na trzecie miejsce od tej litery („Q” + „C” = 18 = „S”) czyli "S". "S" łączy się zgodnie z naszą tabelką z "G".

2. Teraz cofamy tą literę o 6 miejsc, czyli na "A" w wirniku drugim, która w tabelce odpowiada literze "A". Robimy tak, ponieważ różnica miejsc w wirniku drugim względem trzeciego wynosi -6 ("K" - "Q" = -6).

3. Przechodząc do wirnika pierwszego znowu musimy się cofać aż o 9 miejsc ("B" - "K" = -9) do litery "R", która łączy się z "U".

4. Dotarliśmy do momentu użycia reflektora, który odbije nam tę literę. Na początek musimy oczywiście cofnąć "U" o 1 miejsce do "T", ponieważ reflektor jest zawsze ustawiony na pozycji zerowej ("A" - "B" = -1). "T" zmienia nam się

w "Z" i wraca do wirników.

5. "Z" łąduje w wirniku 1 i przechodzi o jedno miejsce do przodu ("B" - "A" = 1), stając się "A".

6. Teraz odwracamy naszą tabelkę, czyli szukamy pożądanej litery wśród liter wirnika i dopasowujemy jej literę z górnego (uporządkowanego) alfabetu.

7. Patrzymy, która literka w alfabecie ma połączenie z literą "A" z wirnika 1. Tą literką jest "U". Z nią przechodzimy do wirnika 2.

8. Stosujemy teraz stare, dobre przesunięcie ("K" - "B" = 9). "U" zmienia się w "D", które jest łączeniem "C". Lecimy do wirnika 3.

9. Litera "C" jest tutaj przesuwana o 6 miejsc ("Q" - "K" = 6) i staje się "I", która jest łączeniem litery "Q".

10. Teraz wystarczy się cofnąć do pozycji zerowej, jaką jest "A" ("A" - "Q" = -16). Okazuje się, że to "A" jest naszym wynikiem. Poniżej widzimy całą zakodowaną wiadomość:

"C" -> "A"

"Z" -> "B"

"E" -> "B"

"S" -> "H"

"C" -> "I"

Możemy ją odkodować, wpisując wynik ("ABBHI" <-> "CZESC").

Żeby nie męczyć się z pisemnym szyfrowaniem wiadomości, stworzyłem program w C++, który robi to za mnie w ułamku sekundy.