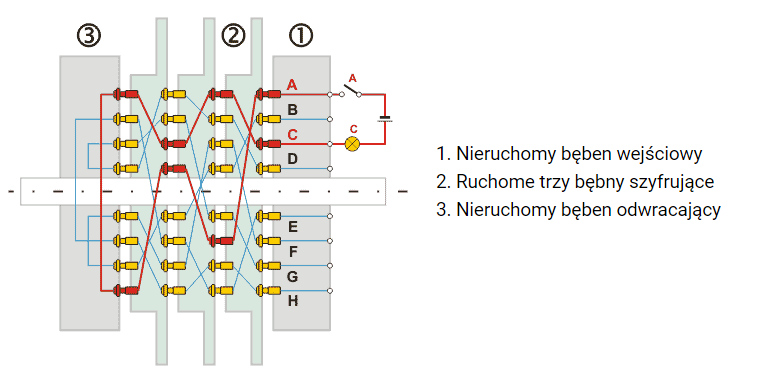
1. **Działanie enigmy**

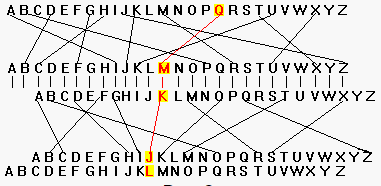
W skład enigmy wchodzą trzy bębny szyfrujące, bęben wejściowy oraz bęben odwracający.



Sygnał (litera) była wprowadzana do bębna wejściowego. Przekazywał on sygnał dalej do prawego bębna szyfrującego. Zadaniem bębnów szyfrujących była podmiana określonych liter. Przykładową podmianę widać na rysunku poniżej:



Każdy bęben szyfrujący miał na stałe ustalone podmiany liter. Dlatego stworzono 5 typów bębnów szyfrujących (5 różnych podmian liter) i zmieniano ich kolejność w maszynie. Dodatkowo bębny szyfrujące obracały się wokół wspólnej osi, przez co generowane mogły być nowe kombinacje szyfrów. Przykładowy obrót widać na poniższym rysunku.

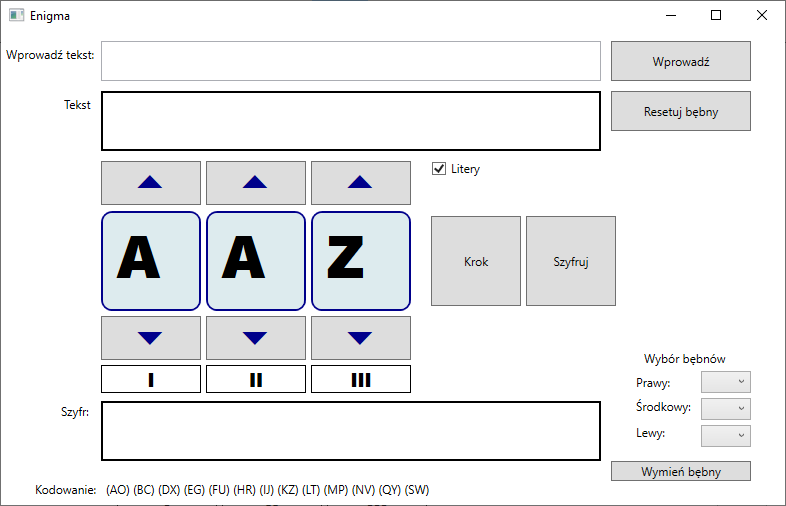


Zamiast wykorzystywać wyjścia styków z trzeciego bębna jako szyfr litery wejściowej, wyjścia te podłączano do nieruchomego bębna odwracającego. Zadaniem bębna była prosta wymiana pary znaków. Sygnał wyjściowy był z powrotem kierowany do bębnów szyfrujących w odwrotnym kierunku i pojawiał się na bębnie wejściowym, lecz na innym styku. Dzięki zastosowaniu bębna odwracającego możliwe było wygenerowanie większej liczby alfabetów podstawieniowych. Minusem tego rozwiązania było to, że kod był odwracalny. Jeżeli np. „A” było kodowane przez „C”, to również „C” było kodowane przez „A”. Można więc było dla danego ustawienia bębnów w prosty sposób przedstawić cykl permutacyjny np.:

(AU) (BE) (CJ) (DO) (FT) (GP) (HZ) (IW) (KN) (LS) (MR) (QV) (XY).

Prawy bęben szyfrujący przed każdym wprowadzeniem nowej litery wykonywał 1/26 obrotu. Bębny szyfrujące posiadały nacięcia, przez co przy środkowy bęben obracał się o 1/26 obrotu przy odpowiednim ułożeniu prawego bębna (analogicznie lewy przy odpowiednim ułożeniu bębna środkowego). Obroty bębnów szyfrujących sprawiały, że każda nowa litera szyfrowana była innym cyklem permutacyjnym.

1. **Działanie programu**



Na samej górze znajduje się miejsce do wprowadzania tekstu. Po kliknięciu przycisku „Wprowadź” tekst zostaje poddany konwersji. Małe litery są zamieniane na wielkie, a wszystkie inne znaki są usuwane. Użyto trzech bębnów szyfrujących, oraz nieruchomego bębna odwracającego, którego nie widać w interfejsie graficznym. Przyciski ze strzałkami pozwalają na ręczne obracanie bębnów szyfrujących. Przycisk „Resetuj bębny” ustawia je w pozycji początkowej (AAZ – dzięki temu pierwsza litera szyfrowana jest ustawieniem AAA). Przycisk „Wymień bębny” pozwala na użycie dowolnych trzech z pięciu dostępnych bębnów. Ustawienia dostępnych bębnów znajdują się poniżej:

|  |  |  |
| --- | --- | --- |
| Numer bębna | Podstawienia dla kolejnych liter alfabetu | Punkt przeniesienia obrotu |
| I | EKMFLGDQVZNTOWYHXUSPAIBRCJ | R |
| II | AJDKSIRUXBLHWTMCQGZNPYFVOE | F |
| III | BDFHJLCPRTXVZNYEIWGAKMUSQO | W |
| IV | ESOVPZJAYQUIRHXLNFTGKDCMWB | K |
| V | VZBRGITYUPSDNHLXAWMJQOFECK | A |

Przycisk „Szyfruj” szyfruje cały wprowadzony tekst, przycisk „Krok” szyfruje po jednym znaku. Po jego użyciu niektóre funkcje nie są dostępne, aż nie zaszyfruje się całego wprowadzonego tekstu do końca. Na samym dole wyświetlane są podstawienia liter dla danego ustawienia bębnów.