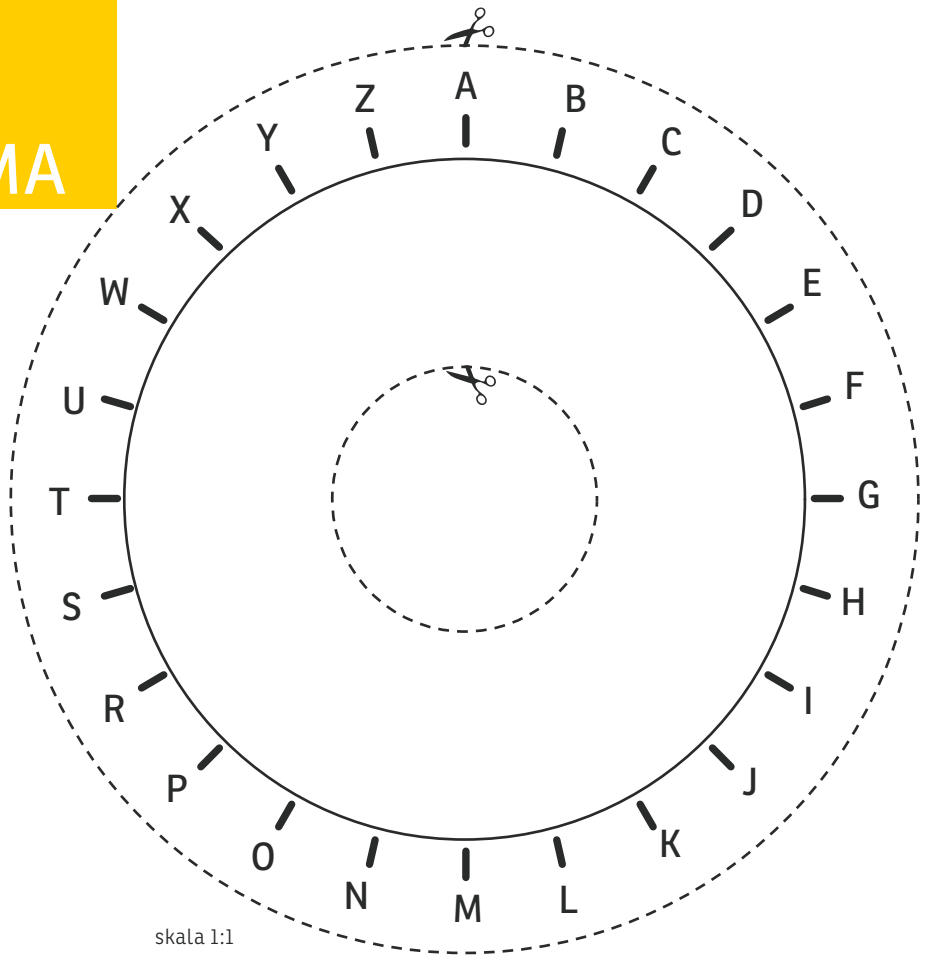


ENIGMA



skala 1:1

Któż nie słyszał tej nazwy? Osławiona maszyna szyfrująca, skonstruowana w czasie drugiej wojny światowej służy wywiadowi niektórych państw do dziś. To chyba najefektowniejsze praktyczne zastosowanie permutacji. Zasada szyfrowania tekstu tak, jak to robi Enigma, jest prosta:

1. Utwórz sieć sztywnych, wzajemnie jednoznacznych przypisań litera szyfrowana - litera szyfrująca.
2. Zaszifruj pierwszy znak tekstu.
3. Dokonaj przesunięcia całej sieci przypisań o stały krok, np. o dwie jednostki.

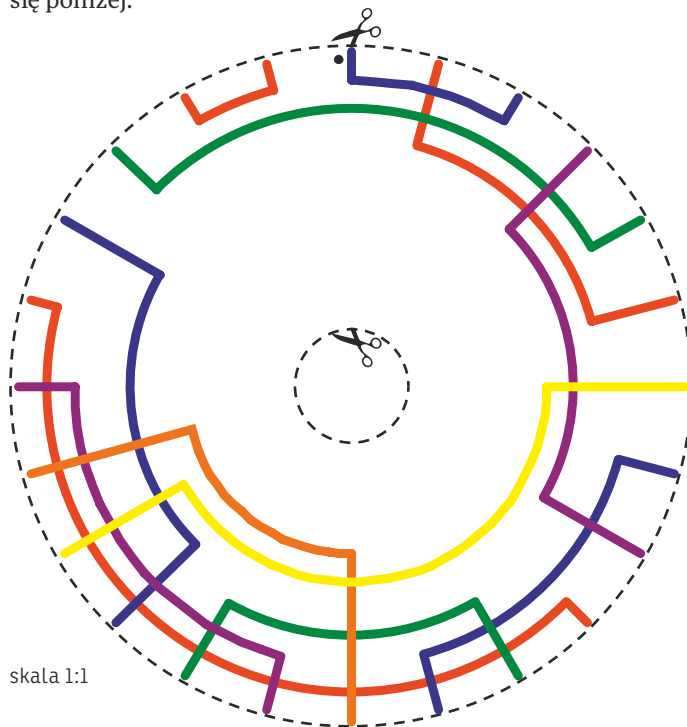


4. Zaszzyfruj następny znak tekstu.
5. Powtarzaj cyklicznie punkty 3 i 4 aż do zaszzyfrowania całego tekstu.

Jak to zrobić w praktyce? Najprostszy model maszyny szyfrującej na takiej samej zasadzie, jak robiła to Enigma, możesz zbudować z tekturki i pudełka po płycie CD w kilkanaście minut. Skopiuj i wydrukuj rysunek widoczny na stronie obok.

Należy umieścić go w pudełku płyty CD tak, by wydruk widoczny był wewnątrz. Szczegóły uwidocznione są na zdjęciach.

To jest pole kodująco-dekodujące. Składa się z umieszczonych w okręgu liter alfabetu. Ich położenia są niezmiennie. Jest ono „klawiaturą” i „wyświetlaczem” równocześnie naszej maszyny szyfrującej. Teraz tarcza kodująca. Jej wzór, przykładowy, znajduje się poniżej:



skala 1:1