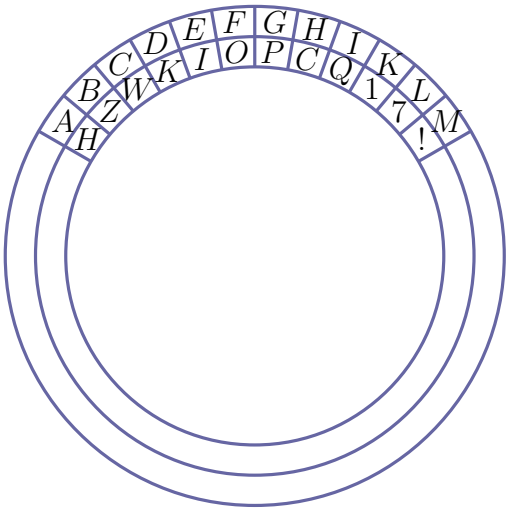
POLITECHNIKA BIAŁOSTOCKA
WYDZIAŁ INFORMATYKI
Bezpieczeństwo sieci komputerowych

PRACOWNIA SPECJALISTYCZNA 3
DR INŻ. MACIEJ BRZOZOWSKI

TEMAT: KRYPTOSYSTEMY SYMETRYCZNE - ALGORYTM ENIGMA.

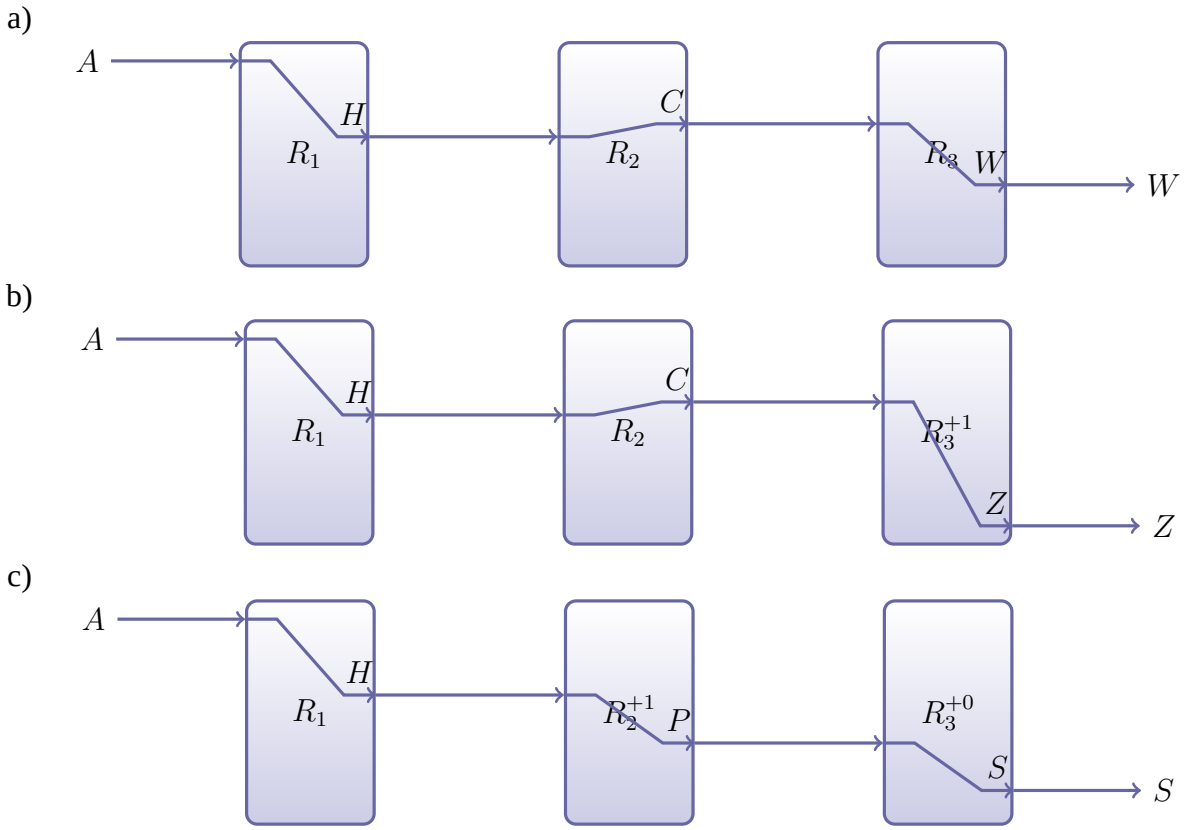


Rysunek 1: Pojedyńczy rotor systemu Enigma

Zasada działania: Na Rysunku 2 przedstawiono zasadę działania systemu Enigma. Każda litera poddawana jest permutacji na każdym rotorze (Rysunku 2.a). Po ukończeniu kodowania każdej litery następuje rotacja na ostatnim rotorze (Rysunku 2.b). Jeżeli rotor dokona pełnego obrotu wymusza to przesunięcie rotora następnego w kolejności po nim (Rysunku 2.c) a rotor wraca do ustawienia startowego.

Zadania:

1. Zaimplementuj system Enigma dla rotorów o 256 komórkach i N rotorach wraz z reflektorem.
2. Zweryfikuj poprawność działania w/w systemu.
3. System ma zapewniać możliwość szyfrowania tekstu/plików binarnych przy powtarzalności szyfrowania/deszyfrowania.
4. System winien umożliwiać wprowadzanie klucza użytkownikowi.



Rysunek 2: Przykład działania systemu Enigma bez reflektora dla kolejek: a) 0, b) 1, c) 256