tertransformasi ke karakter "B" di $i = 1$ dan tertransformasi ke karakter "C" di $i = 3$. Oleh karena itu, sandi *rotor* mendekati kerahasiaan sempurna karena statistik pada teks asli tidak muncul pada statistik pada teks sandi.

Keamanan Mesin Rotor

Pemecahan mesin rotor dengan *brute force* hampir tidak mungkin karena ruang kunci mesin rotor sama dengan $26!^n$ dengan n adalah jumlah gigi rotor. Sedangkan serangan statisktik terhadap teks sandi juga tidak bisa dilakukan karena statistik kemunculan karakter pada teks asli tidak ada pada teks sandi.

Mesin Enigma

Mesin rotor merupakan mesin penyandian yang populer pada zaman sebelum perang dunia ke-2. Jerman pada perang ke-2 membuat mesin penyandi Enigma untuk membuat pesan rahasia. Mesin Enigma merupakan mesin penyandi yang menggunakan prinsip sandi rotor. Bentuk fisik mesin enigma serupa dengan mesin ketik biasa namun memiliki tambahan rangkaian elektronik untuk mewujudkan penyandian. Blok diagram mesin Enigma diberikan oleh Gambar 2.12.

Mesin Enigma terdiri dari beberapa bagian yaitu:

1. Papan ketik tempat pengguna memasukkan satu karakter "A .. Z".

2. *Plugboard* tempat penyambungan manual antara papan ketik dan lampu indikator (output). Dalam penggunaannya *plugboard* diubah tiap saat.

3. Mesin rotor yang terdiri dari 3 rotor: rotor kiri, rotor tengah dan rotor kanan serta 1 reflektor. Rotor kanan selalu berputar (mengganti fungsi substitusi) pada tiap input satu karakter. Jika rotor kanan telah mengalami 1 putaran penuh rotor tengah naik satu. Jika rotor tengah telah mengalami 1 putaran penuh rotor kiri naik satu. Reflektor hanya mengembalikan dengan cara mencerminkan input dan output yaitu $0 - 25, 1 -$