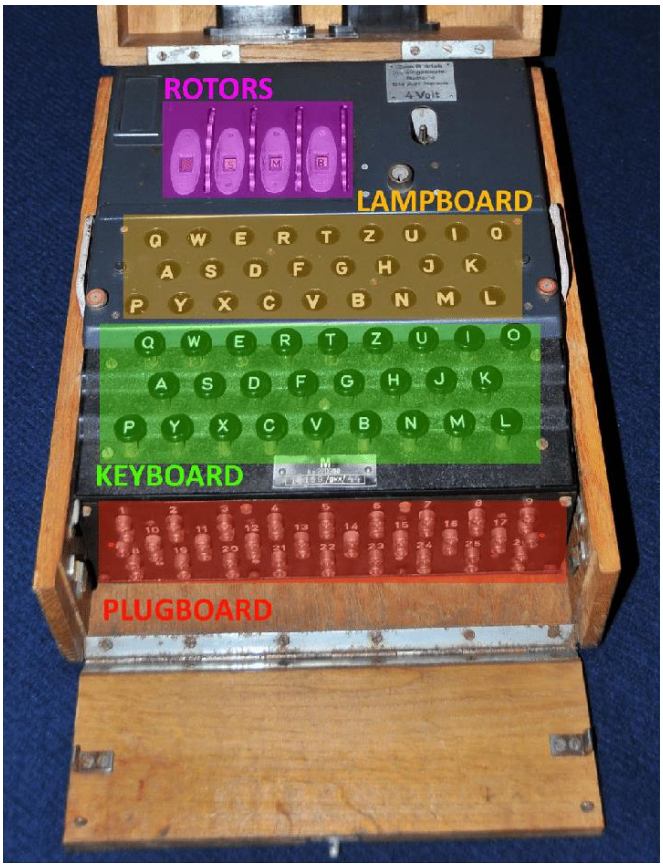
Apa itu Enigma



Sumber: https://www.researchgate.net/figure/The-four-main-components-of-the-Enigma-Four-rotors-a-lampboard-a-keyboard-and-a_fig1_339932418

Mesin enigma merupakan suatu mesin sandi yang dikembangkan dan digunakan pada awal hingga pertengahan abad ke-20. Mesin enigma ini digunakan secara massal oleh Nazi ketika perang dunia kedua. Proses enkripsi pada enigma menggunakan sinyal elektrik yang mengalir dari kabel ke kabel.

Enigma menggunakan penggantian substitusi, yaitu mengubah suatu huruf menjadi huruf lainnya. Akan tetapi, substitusi pada enigma bersifat dinamis karena setiap kali sebuah tombol pada enigma ditekan maka pemetaan hurufnya berubah disebabkan oleh pergerakan rotor pada enigma. Secara umum, enigma terdiri atas tiga bagian utama:

1. Rotor

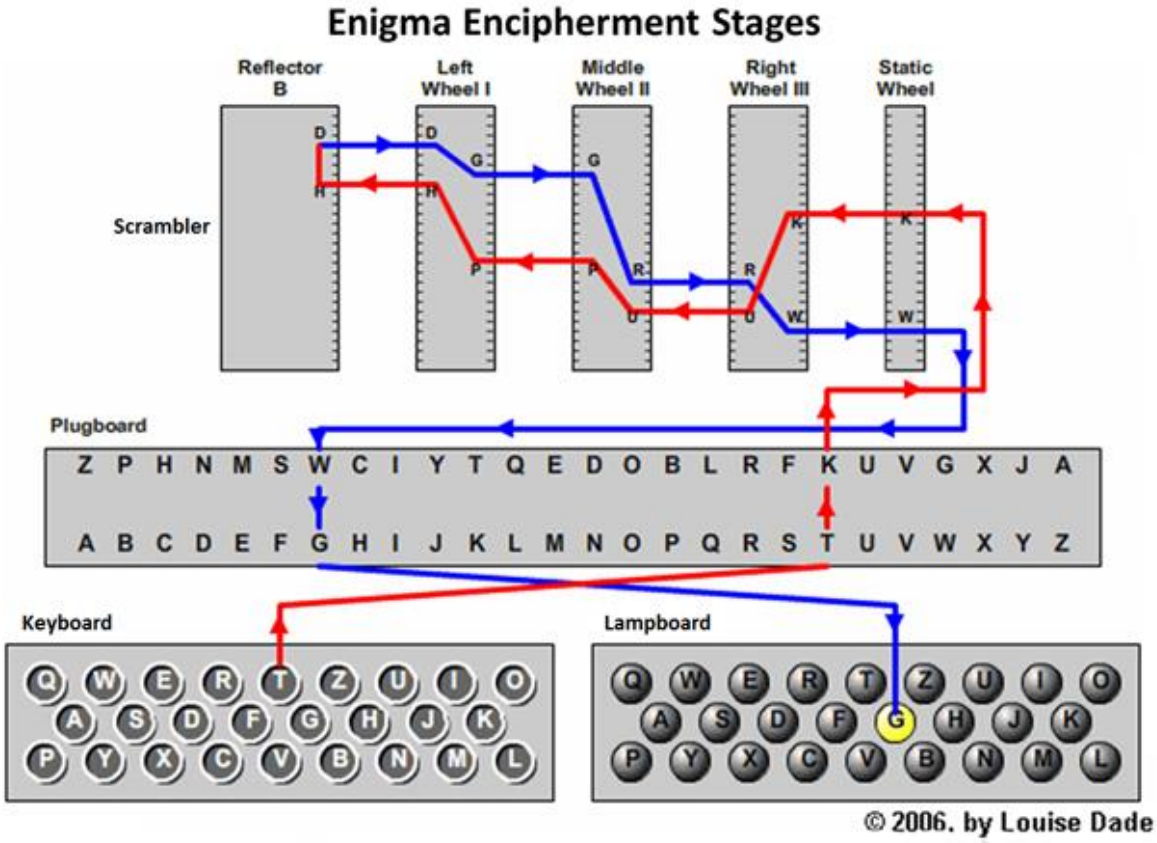
Sumber: https://arxiv.org/pdf/2004.09982.pdf

Rotor merupakan bagian yang berbentuk seperti roda yang memetakan suatu huruf ke huruf lainnya melalui pemetaan kabelnya. Setiap kali sebuah tombol pada keyboard

ditekan, maka rotor akan berputar (akan dijelaskan lebih lanjut di bagian cara kerja enigma)

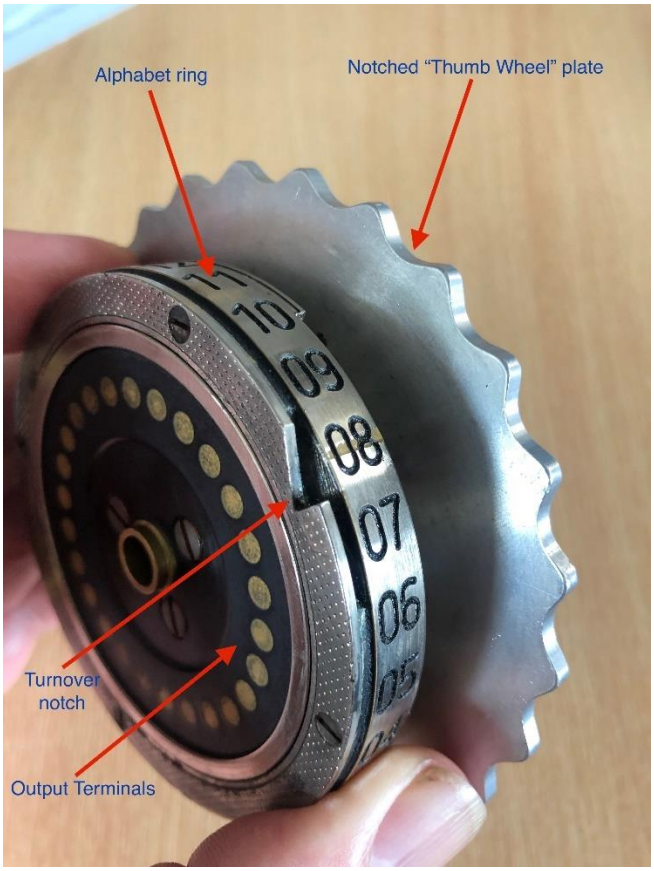
2. Plugboard
   Plugboard merupakan papan pemetaan sepasang huruf, yang memetakan suatu huruf ke huruf lainnya secara simetris. Pemetaan huruf pada plugboard menggunakan sebuah kabel yang ditancapkan ke dua huruf pada bagian plugboard untuk memetakan kedua huruf tersebut.
3. Reflektor
   Reflektor sesuai namanya memantulkan kembali sinyal elektrik yang mengalir dari rotor. Pada umumnya, sinyal elektrik pada enigma mengalir dari kanan ke kiri dan kemudian kiri ke kanan setelah melalui reflektor.

Cara Kerja Enigma



Sumber: https://www.mpoweruk.com/enigma.htm

Pada hakikatnya, mesin enigma merupakan pemetaan suatu huruf ke huruf lain secara berlapis. Pada umumnya, lapisan pemetaan tersebut adalah: dari Keyboard ke Plugboard, dari Plugboard ke Entrittswalze (ETW) atau Static Wheel, dari ETW ke Right Wheel, Right Wheel ke Middle Wheel, Middle Wheel ke Left Wheel, Left Wheel ke Reflector, Reflector ke Left Wheel, Left Wheel ke Middle Wheel, Middle Wheel ke Right Wheel, Right Wheel ke Plugboard, dan Plugboard ke Lampboard.



Sumber: https://jgandrews.com/posts/the-enigma-machine/

Pemetaan dari wheel yang satu ke wheel yang lainnya menggunakan pemetaan dari rotor-rotor pada mesin enigma. Akan tetapi, pemetaan tersebut berubah terus menerus karena rotor akan berusaha untuk berputar setiap kali sebuah tombol pada keyboard ditekan. Setiap rotor hanya dapat berputar ketika rotor di sebelah kanannya sedang berada pada posisi yang mengakibatkan turnover notchnya pada posisi yang tepat (rotor kiri memerlukan rotor tengah pada posisi yang tepat, rotor tengah memerlukan rotor kanan pada posisi yang tepat, dan rotor kanan dapat berputar terus). Urutan pemutaran dilakukan dari rotor kiri terlebih dahulu, kemudian rotor tengah, dan terakhir rotor kanan.

Secara umum, cara menggunakan enigma adalah sebagai berikut:

1. Pengguna menggunakan konfigurasi tertentu, konfigurasi tersebut terdiri atas posisi awal rotor, ring rotor, jenis rotor pada setiap posisi, dan koneksi plugboard
2. Pengguna memasukkan teks yang ingin dienkripsi atau didekripsi pada keyboard
3. Pada setiap penekanan tombol keyboard, rotor akan berputar
4. Setelah rotor berputar, maka sinyal elektrik dari keyboard akan dialirkan ke ETW, rangkaian rotor, reflektor, kembali ke rangkaian rotor, dan ke lampboard
5. Ketika sinyal tiba di lampboard, maka lampu yang berkorespondensi dengan huruf hasil enkripsi akan menyala

Step Enkripsi dan Dekripsi Enigma

Rotor	ABCDEFGHIJKLMNOPQRSTUVWXYZ	Notch	Turnover	#
ETW	ABCDEFGHIJKLMNOPQRSTUVWXYZ			
I	EKMFLGDQVZNTOWYHXUSPAIBRCJ	Y	Q	1
II	AJDKSIRUXBLHWTMCQGZNPYFVOE	M	E	1
III	BDFHJLCPRTXVZNYEIWGAKMUSQO	D	V	1
IV	ESOVPZJAYQUIRHXLNFTGKDCMWB	R	J	1
V	VZBRGITYUPSDNHLXAWMJQOFECK	H	Z	1
VI	JPGVOUMFYQBENHZRDKASXLICTW	HU	ZM	2
VII	NZJHGRCXMYSWBOUFAIVLPEKQDT	HU	ZM	2
VIII	FKQHTLXOCBJSPDZRAMEWNIUYGV	HU	ZM	2
UKW-B	YRUHQSLDPXNGOKMIEBFZCWVJAT			
UKW-C	FVPJIAOYEDRZXWGCTKUQSBNMHL			

Sumber: https://www.cryptomuseum.com/crypto/enigma/wiring.htm#12

Enigma menggunakan enkripsi yang bersifat simetrik, yang berarti bahwa kunci untuk mengenkripsi dan mengdekripsi adalah sama. Yang dimaksud dengan kunci enkripsi simetrik berarti ketika A menjadi H pada saat enkripsi, maka saat dekripsi pengguna hanya perlu memasukkan kembali hasil enkripsi untuk mendekripsi karena H tersebut akan menjadi A. Step enkripsi dan dekripsi pada enigma adalah sebagai berikut:

1. Sinyal elektrik dari keyboard dialirkan ke plugboard
2. Apabila terdapat kabel yang memetakan huruf tertentu pada plugboard, maka huruf tersebut akan dipetakan pada plugboard, bila tidak maka akan sesuai dengan masukan pada keyboard
3. Hasil pemetaan huruf dari plugboard tersebut akan dialirkan ke ETW, pada umumnya ETW akan memetakan suatu huruf ke huruf itu sendiri
4. Ketika tahapan pemetaan huruf sebelum reflektor, akan terjadi forward mapping (semisal pada Rotor I maka A → E, B → K, dan seterusnya)
5. Ketika sinyal sampai pada reflektor, maka sinyal akan diforward mapping juga pada reflector yang digunakan (UKW-B atau UKW-C)
6. Setelah sinyal dipantulkan pada reflektor, maka sinyal-sinyal yang mengalir pada rotor akan direverse mapping (semisal pada Rotor I maka E → A, K → B, dan seterusnya)
7. Setelah sinyal keluar dari rotor paling kanan, maka sinyal akan mengalir ke plugboard yang akan memetakan kembali sesuai dengan tahapan kedua
8. Sinyal dari plugboard tersebut akan dialirkan ke lampu yang berkorespondensi

Berikut adalah pseudo-code untuk forward mapping dan reverse-mapping pada enigma

```
func forward_mapping (char)
        offset ← position – “A”  // menghitung jarak posisi alfabet rotor sekarang dari “A”
        mapped ← wiring[char + offset]
        res ← mapped – offset // mengurangi alfabet dengan offset
        ➔ res

func reverse_mapping(char)
```

```
        offset ← position – “A”  // menghitung jarak posisi alfabet rotor sekarang dari “A”
        mapped ← char + offset
        res ← wiring.reverse[mapped - offset]
        ➔ res

// pada forward mapping dan reverse mapping
// terdapat penambahan dan pengurangan offset
// hal tersebut terjadi karena sifat dari rotor yang berputar
// sehingga offset tersebut berpengaruh terhadap pemetaan rotor
```

Screenshot Perbandingan