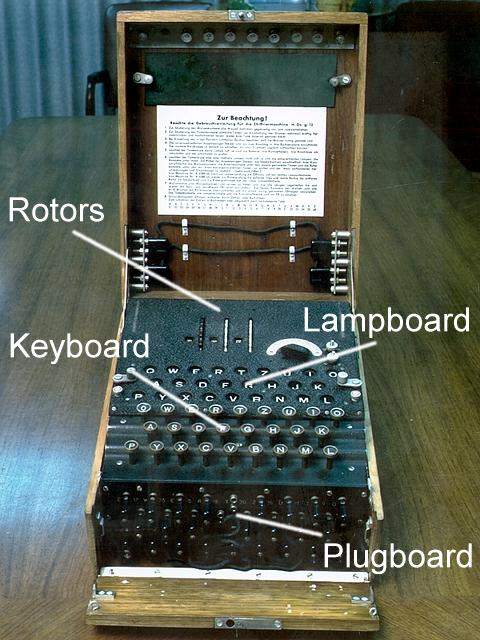
Laporan task 4 IRK

Nama: Haziq Abiyyu Mahdy

NIM: 13521170

1. Pengertian Enigma

Enigma adalah mesin yang digunakan oleh tentara dan pemerintah nazi pada perang dunia kedua untuk mengenkripsi atau mendekripsi pesan rahasia. Cara menggunakan Enigma cukup sederhana, yaitu dengan mengetikkan huruf yang akan dienkripsi pada keyboard, kemudian hasil enkripsi akan muncul pada lampboard di mana lampu pada huruf hasil enkripsi akan menyala.



Source: <https://id.wikipedia.org/wiki/Mesin_Enigma>

Secara umum, terdapat tiga bagian Enigma, yaitu keyboard yang berfungsi untuk memasukkan huruf yang akan dienkripsi, scrambler yang berfungsi untuk menentukan hasil enkripsi, serta lampboard yang berfungsi untuk menampilkan hasil enkripsi. Terdapat empat komponen pada scrambler, yaitu plugboard, entry disc, rotor, dan reflektor. Tiap komponen pada scrambler pada dasarnya memiliki tujuan yang sama, yaitu memetakan huruf input (huruf yang masuk ke komponen tersebut) menjadi huruf output (huruf yang keluar dari komponen tersebut) berdasarkan konfigurasi tertentu.

Perbedaan Enigma dengan enkripsi sederhana seperti sandi Caesar adalah, Enigma memiliki rotor yang berputar setiap kali keyboard ditekan, sehingga huruf yang sama dapat memiliki hasil enkripsi yang berbeda. Sedangkan pada sandi Caesar, tiap huruf akan dipetakan pada satu huruf lain berdasarkan pergeseran posisi huruf tersebut sebanyak k-kali dalam modulo 26.

Oleh karena itu, huruf yang sama akan menghasilkan sandi yang sama, sehingga tidak sulit untuk memecahkan sandi Caesar. Dengan mengetahui nilai k, kita dapat menerjemahkan kembali plaintext menjadi ciphertext denganrumus berikut

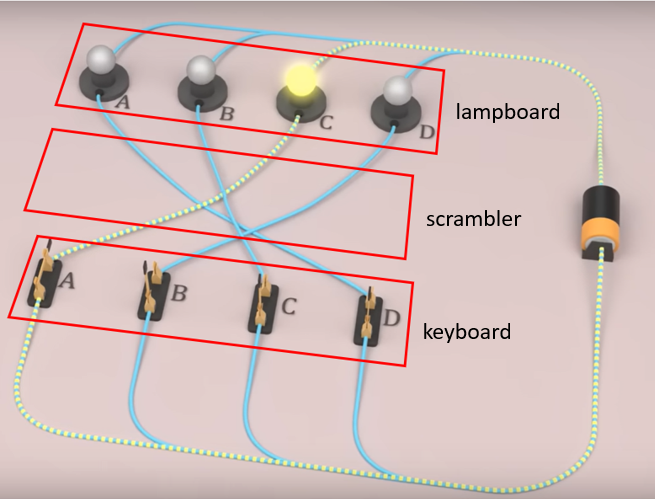
1. Penjelasan cara kerja Enigma
   1. Aliran listrik pada enigma

Enigma dapat dianalogikan sebagai rangkaian listrik paralel yang memiliki 1 baterai, 26 saklar (A-Z) dan 26 lampu (A-Z) di mana kabel yang menghubungkan saklar dengan lampu di-scramble sedemikian rupa sehingga saklar dengan huruf plaintext akan menghidupkan lampu dengan huruf ciphertext-nya. Hal ini persis dengan cara kerja Enigma, di mana ketika huruf plaintext ditekan pada keyboard, maka lampu pada huruf ciphertext akan menyala pada lampboard. Berdasarkan analogi tersebut, menekan huruf pada keyboard Enigma analog (sebanding) dengan menghidupkan saklar pada rangkaian, sedangkan melepaskan huruf pada keyboard Enigma analog dengan mematikan saklar pada rangkaian. Perhatikan gambar berikut.

**Rangkaian listrik**

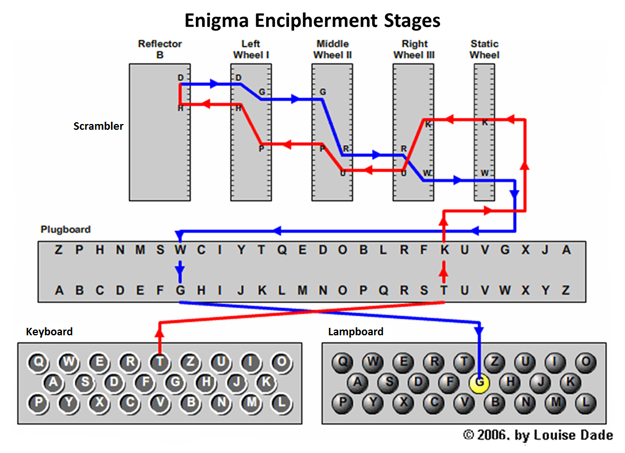


**“Enigma”**



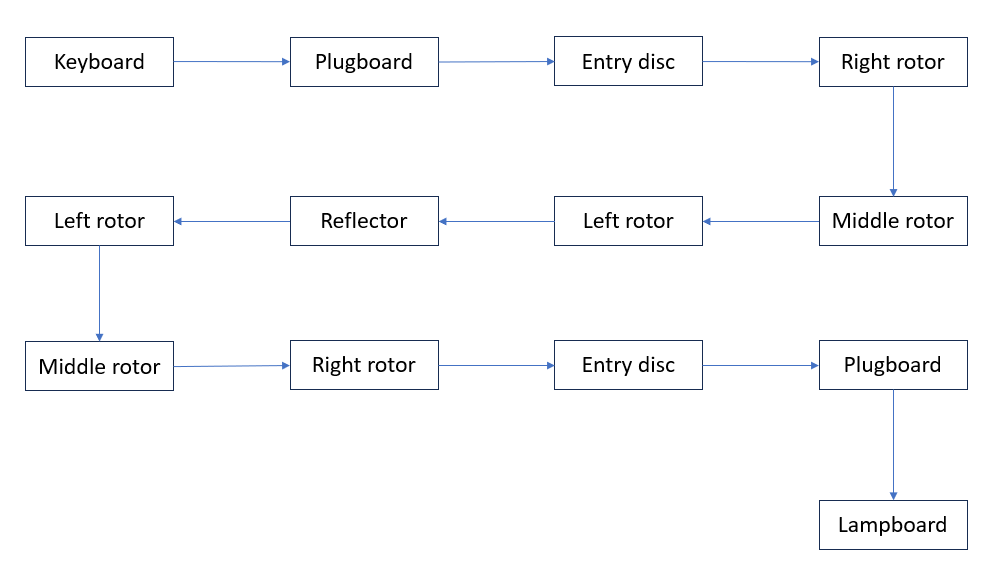
Source: <https://www.youtube.com/watch?v=ybkkiGtJmkM> dan sedikit modifikasi pribadi

Sekilas Enigma terlihat sederhana karena mirip dengan rangkaian listrik paralel dengan susunan kabel yang diacak. Namun, kompleksitas Enigma terletak pada bagian scrambler. Scrambler memiliki 4 komponen yaitu plugboard, entry disc, rotor, dan reflektor. Tiap komponen akan memetakan huruf input menjadi huruf output, kemudian huruf output tersebut akan diteruskan pada komponen selanjutnya, sehingga proses enkripsi terjadi berulang kali.



Source: <https://www.mpoweruk.com/enigma.htm>

Berikut adalah alur pergerakan listrik/huruf dari keyboard menuju lampboard



Tiap komponen scrambler bertujuan memetakan huruf input menjadi huruf output, namun terdapat beberapa perbedaan pada tiap komponennya.

* + 1. Entry disc

Entry disc akan memetakan suatu huruf dengan huruf yang sama. (A 🡪 A, B 🡪B, dst.)

* + 1. Plugboard

Plugboard akan memetakan suatu huruf dengan huruf lainnya berdasarkan konfigurasi dari pengguna. Pengguna dapat memilih pasangan huruf-huruf yang akan dipetakan (misal W ↔ J, P ↔ X, dll). Terdapat maksimal 13 pasang huruf yang dapat dihubungkan dengan plugboard, dan huruf yang telah dimasukkan ke dalam plugboard tidak dapat dipilih lagi untuk dipasangkan dengan huruf lainnya (misal A ↔B, C ↔ A tidak valid). Misalkan terdapat konfigurasi plugboard W ↔ J. Maka, huruf W yang masuk akan dipetakan menjadi huruf J, dan huruf J yang masuk akan dipetakan menjadi huruf J. Pemasangan kabel pasangan huruf pada plugboard bersifat opsional, sehingga jika tidak ada pasangan huruf pada plugboard, maka tidak terjadi proses pemetaan pada plugboard.

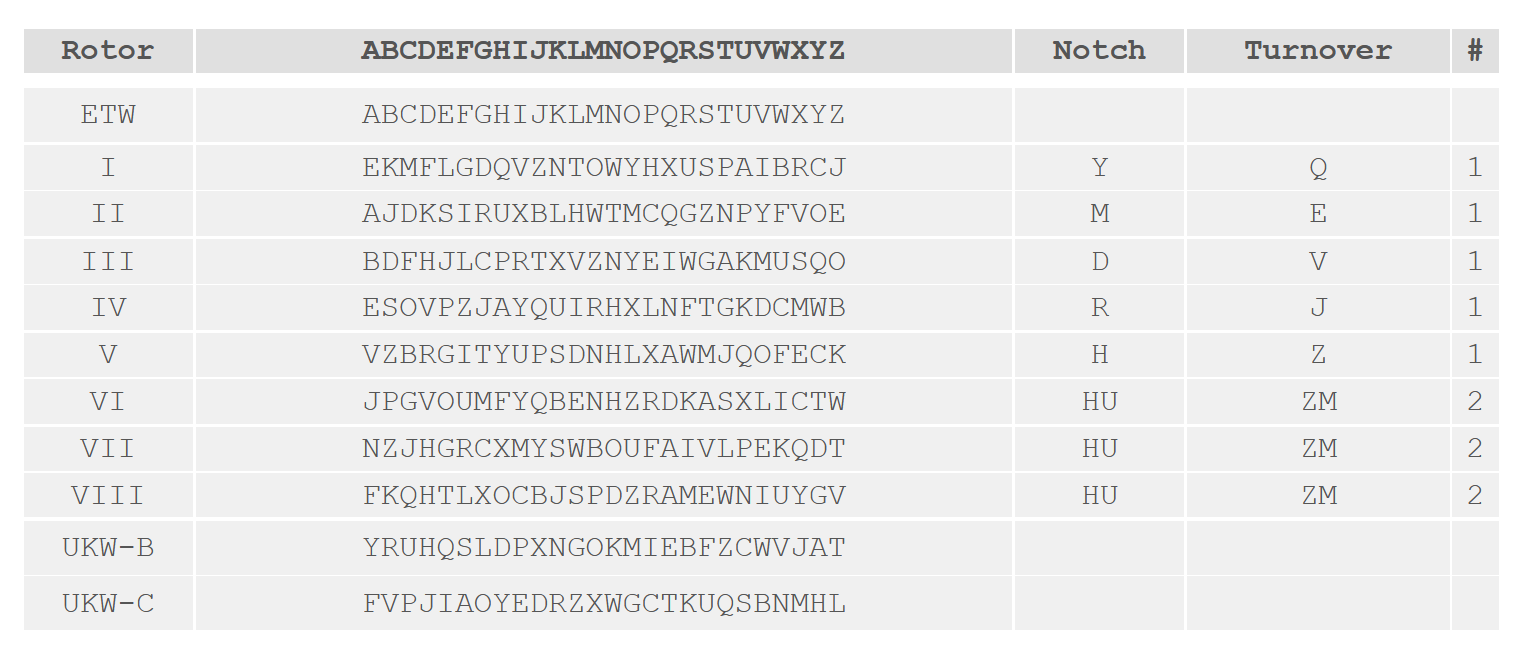
A close up of a machine

Description automatically generated

Source: <https://www.youtube.com/watch?v=ybkkiGtJmkM>

* + 1. Rotor

Berbeda dengan plugboard di mana pemetaan huruf ditentukan oleh pengguna, pemetaan huruf pada rotor bergantung pada jenis rotor yang dipilih. Pada Enigma jenis M3, terdapat delapan pilihan rotor yang dapat dipilih, yaitu rotor I, II, III, hingga VIII.



Source: <https://www.cryptomuseum.com/crypto/enigma/wiring.htm#12>

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Input | A | B | C | D | … | Z |
| Output | E | K | M | F | … | J |

Tabel mapping rotor I

Listrik akan melewati rotor dua kali, yaitu sebelum melewati reflektor dan setelah melewati reflektor. Sebelum listrik melewati reflektor, pemetaan dilakukan dengan maju (forward), misalnya pada jenis rotor I, huruf A akan dipetakan menjadi E, B dipetakan menjadi K, C menjadi M, dst. Setelah listrik melewati reflektor, pemetaan dilakukan dengan mundur (backward/inverse), misalnya pada jenis rotor I, huruf E akan dipetakan menjadi A, K menjadi B, dst.

A diagram of a diagram

Description automatically generated

Forward mapping dan backward mapping

* + 1. Reflector

A machine with a circular mechanism

Description automatically generated

Source: <https://www.youtube.com/watch?v=ybkkiGtJmkM> dan sedikit modifikasi pribadi

Seperti Rotor, pemetaan huruf pada reflector bergantung pada jenis reflector yang dipilih. Terdapat dua jenis reflector, yaitu UKW-B dan UKW-C. Huruf yang masuk dari left rotor akan dipetakan oleh reflektor dan diteruskan kembali ke left rotor.

* 1. Pengaruh perputaran rotor

Kompleksitas Enigma tidak berhenti pada enkripsi/mapping berulang yang dilakukan pada komponen-komponen scrambler. Rotor pada enigma dapat berputar setiap kali keyboard ditekan, sehingga dapat mengubah alur listrik/huruf yang masuk dan keluar dari rotor. Terdapat tiga rotor pada Enigma, yaitu right rotor, middle rotor, dan left rotor. Right rotor akan berputar (bergeser satu huruf) setiap kali keyboard ditekan. Pada salah satu huruf di right rotor, terdapat notch yang dapat menggerakkan middle rotor apabila right rotor berada pada posisi huruf tersebut. Pada salah satu huruf di middle rotor, terdapat pula notch yang dapat menggerakkan left rotor apabila middle rotor berada pada posisi huruf tersebut.

Perubahan posisi rotor akan menyebabkan diperlukannya penyesuaian saat huruf masuk dan keluar dari rotor. Apabila rotor berada pada posisi ke-0 (huruf A), maka tidak perlu dilakukan penyesuaian saat huruf masuk dan keluar dari rotor. Namun apabila rotor berada pada posisi ke-n, dengan 0 < n < 26, maka sebelum huruf masuk ke dalam rotor, huruf yang masuk harus di-shift maju sebanyak n kali dalam modulo 26, kemudian dilakukan mapping pada rotor, kemudian hasil mapping akan di-shift mundur sebanyak n kali dalam modulo 26.

Hal ini dapat diilustrasikan dengan Enigma pada gambar berikut yang memiliki tiga alphabet (A, B, C) dengan mapping (A 🡪 C, B 🡪 A, C 🡪 B). Pada gambar di bawah, kotak hijau melambangkan rotor, kotak biru melambangkan posisi rotor, garis hitam menggambarkan mapping rotor, dan panah merah menggambarkan posisi huruf input dan output rotor.

Rotor pada posisi ke-0 (A)

A diagram of a diagram

Description automatically generated

Rotor pada posisi ke-1 (B)

A diagram of a diagram

Description automatically generated

Pada posisi ke-0 (A), huruf pada kabel output sama dengan hasil mapping huruf pada kabel input. Namun pada posisi ke-1 (B), huruf pada kabel output dimajukan sebanyak satu kali, kemudian di-mapping, lalu hasil mapping akan dimundurkan sebanyak satu kali. Hal ini disebabkan hanya rotor saja yang berputar, bukan posisi kabel input/outputnya. Sebagai contoh, saat rotor berada pada posisi ke-1 (B), huruf C (2) yang masuk dari kabel input akan digeser maju sebanyak satu kali menjadi (2 + 1) mod 3 = 0 = A. Kemudian A di-mapping menjadi C, dan huruf C akan digeser mundur sebanyak satu kali menjadi (2 – 1) mod 3 = 1 = B.

* 1. Simpulan cara kerja Enigma
* Pengguna menentukan konfigurasi enigma: plugboard, jenis rotor, posisi awal rotor, jenis reflektor
* Pengguna menekan keyboard
* Right rotor akan bergerak, dan jika right rotor berada pada posisi notch, middle rotor akan bergerak, dan jika middle rotor berada pada posisi notch, left rotor akan bergerak
* Listrik mengalir dari baterai ke keyboard
* Listrik diteruskan dari keyboard ke plugboard
* Plugboard akan melakukan mapping huruf dan meneruskannya ke right rotor, middle rotor, kemudian left rotor dengan forward mapping. Huruf yang masuk ke dalam rotor akan disesuaikan terlebih dahulu berdasarkan posisi rotor, kemudian di-mapping dan hasil mapping akan disesuaikan berdasarkan posisi rotor
* Huruf akan diteruskan ke reflektor, kemudian reflektor melakukan mapping dan meneruskan kembali ke left rotor, middle rotor, dan right rotor dengan backward mapping (penyesuaian tetap dilakukan seperti langkah sebelumnya)
* Huruf diteruskan ke plugboard, di-mapping oleh plugboard, kemudian diteruskan ke lampboard. Lampu pada huruf hasil enkripsi akan menyala pada lampboard
* Listrik diteruskan kembali ke baterai

1. Contoh langkah-langkah enkripsi

Kondisi awal:

- Left rotor: rotor I, posisi awal: A

- Middle rotor: rotor II, posisi awal: A

- Right rotor: rotor II, posisi awal: A

- Reflektor: UKW-B

- Plugboard: AP, LS

* 1. Pengguna menekan huruf A
  2. Posisi rotor berubah menjadi AAB
  3. Huruf A masuk ke plugboard, di-mapping menjadi P
  4. Huruf P masuk ke entry disc (tidak berubah)
  5. Huruf P masuk ke right rotor. Karena posisi right rotor = 1 (B), maka P harus digeser maju sebanyak satu kali menjadi Q, kemudian Q akan di-mapping menjadi I. I akan digeser mundur sebanyak satu kali menjadi H.
  6. Huruf H masuk ke middle rotor. Karena posisi middle rotor = 0, maka H tidak perlu digeser maju dan dapat langsung di-mapping menjadi U. U tidak perlu digeser mundur.
  7. Huruf U masuk ke left rotor. Karena posisi left rotor = 0, maka H tidak perlu digeser maju dan dapat langsung di-mapping menjadi A. A tidak perlu digeser mundur.
  8. Huruf A masuk ke reflektor, kemudian di-mapping menjadi Y
  9. Huruf Y masuk ke left rotor. Karena posisi left rotor = 0, maka Y tidak perlu digeser maju dan dapat langsung di-mapping (menggunakan backward mapping) menjadi O. O tidak perlu digeser mundur.
  10. Huruf O masuk ke middle rotor. Karena posisi middle rotor = 0, maka O tidak perlu digeser maju dan dapat langsung di-mapping (menggunakan backward mapping) menjadi Y. Y tidak perlu digeser mundur.
  11. Huruf Y masuk ke right rotor. Karena posisi right rotor = 1 (B), maka Y harus digeser maju sebanyak satu kali menjadi Z, kemudian Z akan di-mapping (menggunakan backward mapping) menjadi M. M akan digeser mundur sebanyak satu kali menjadi L.
  12. Huruf L masuk ke plugboard, di-mapping menjadi S.
  13. Huruf S akan menyala pada lampboard

1. Contoh dekripsi

Untuk melakukan dekripsi, konfigurasi awal Enigma harus sama dengan konfigurasi awal sebelum melakukan enkripsi. Sehingga, Kondisi awal:

- Left rotor: rotor I, posisi awal: A

- Middle rotor: rotor II, posisi awal: A

- Right rotor: rotor II, posisi awal: A

- Reflektor: UKW-B

- Plugboard: AP, LS

Huruf S apabila didekripsi dengan konfigurasi di atas, akan mengasilkan huruf A. Berikut adalah langkah-langkahnya.

1. Pengguna menekan huruf S
2. Posisi rotor berubah menjadi AAB
3. Huruf S masuk ke plugboard, di-mapping menjadi L
4. Huruf L masuk ke entry disc (tidak berubah)
5. Huruf L masuk ke right rotor. Karena posisi right rotor = 1 (B), maka L harus digeser maju sebanyak satu kali menjadi M, kemudian M akan di-mapping menjadi Z. Z akan digeser mundur sebanyak satu kali menjadi Y.
6. Huruf Y masuk ke middle rotor. Karena posisi middle rotor = 0, maka Y tidak perlu digeser maju dan dapat langsung di-mapping menjadi O. O tidak perlu digeser mundur.
7. Huruf O masuk ke left rotor. Karena posisi left rotor = 0, maka O tidak perlu digeser maju dan dapat langsung di-mapping menjadi Y. Y tidak perlu digeser mundur.
8. Huruf Y masuk ke reflektor, kemudian di-mapping menjadi A
9. Huruf A masuk ke left rotor. Karena posisi left rotor = 0, maka A tidak perlu digeser maju dan dapat langsung di-mapping (menggunakan backward mapping) menjadi U. U tidak perlu digeser mundur.
10. Huruf U masuk ke middle rotor. Karena posisi middle rotor = 0, maka U tidak perlu digeser maju dan dapat langsung di-mapping (menggunakan backward mapping) menjadi H. H tidak perlu digeser mundur.
11. Huruf H masuk ke right rotor. Karena posisi right rotor = 1 (B), maka H harus digeser maju sebanyak satu kali menjadi I, kemudian I akan di-mapping (menggunakan backward mapping) menjadi Q. Q akan digeser mundur sebanyak satu kali menjadi P.
12. Huruf P masuk ke plugboard, di-mapping menjadi A.
13. Huruf A akan menyala pada lampboard
14. Screenshot hasil program dan perbandingan dengan contoh Enigma di internet. (source: <https://cryptii.com/pipes/enigma-machine>)
    1. Contoh 1.

* Left rotor: III, position: L
* Middle rotor: I, position: C
* Right rotor: II, position: F
* Plugboard: -
* Plaintext: HELLO WORLD
* Ciphertext: sqwyp qcvis
* Contoh Enigma di internet:

A screenshot of a computer

Description automatically generated

* Konfigurasi Enigma

A screenshot of a computer

Description automatically generated

* Input

A screenshot of a computer

Description automatically generated

* Output

A screenshot of a computer

Description automatically generated

* Kondisi akhir Enigma

A screenshot of a computer

Description automatically generated

* 1. Contoh 2.
* Left rotor: II, position: B
* Middle rotor: II, position: Z
* Right rotor: II, position: Q
* Plugboard: PR JW CM LT
* Plaintext: LABORATORIUMILMUREKAYASAKOMPUTASI
* Ciphertext: UQXIZJZUXCHKUCWTUNDUHJBMXIHHAWDHO
* Contoh Enigma di internet:

A screenshot of a computer

Description automatically generated

* Konfigurasi Enigma

A screenshot of a computer

Description automatically generated

* Input

A screenshot of a computer

Description automatically generated

* Output

A screenshot of a computer

Description automatically generated

* Kondisi akhir Enigma

A screenshot of a computer

Description automatically generated

* Steps

|  |
| --- |
| Keyboard input: U  Rotor positions: BZR  Plugboard encryption: U  Wheel 3 encryption: Q  Wheel 2 encryption: D  Wheel 1 encryption: R  Rotor encryption: B  Wheel 1 encryption: O  Wheel 2 encryption: U  Wheel 3 encryption: T  Plugboard encryption: L  ============================  Keyboard input: Q  Rotor positions: BZS  Plugboard encryption: Q  Wheel 3 encryption: F  Wheel 2 encryption: T  Wheel 1 encryption: O  Rotor encryption: M  Wheel 1 encryption: S  Wheel 2 encryption: H  Wheel 3 encryption: A  Plugboard encryption: A  ============================  Keyboard input: X  Rotor positions: BZT  Plugboard encryption: X  Wheel 3 encryption: X  Wheel 2 encryption: G  Wheel 1 encryption: T  Rotor encryption: Z  Wheel 1 encryption: Z  Wheel 2 encryption: W  Wheel 3 encryption: B  Plugboard encryption: B  ============================  Keyboard input: I  Rotor positions: BZU  Plugboard encryption: I  Wheel 3 encryption: J  Wheel 2 encryption: Y  Wheel 1 encryption: D  Rotor encryption: H  Wheel 1 encryption: E  Wheel 2 encryption: D  Wheel 3 encryption: O  Plugboard encryption: O  (dan seterusnya (terlalu panjang untuk dimasukkan ke dalam laporan) |

* 1. Contoh 3.
* Left rotor: III, position: S
* Middle rotor: II, position: O
* Right rotor: I, position: A
* Plugboard: AS DF GH JK LQ WE RT YU IO PZ XC VB NM
* Plaintext: Lorem ipsum dolor sit amet consectetur adipiscing elit In elementum tortor ac ligula viverra tincidunt Mauris bibendum finibus felis non ultricies erat condimentum ut Sed blandit molestie nunc ut gravida risus Nam bibendum lectus nec lacinia tristique dui ante dictum odio eget congue urna dolor id risus Morbi a elementum arcu Proin dolor purus auctor ut ullamcorper non aliquet eu metus Quisque in augue tellus Sed in porttitor libero id ullamcorper nulla In est turpis consectetur vel tristique dictum tempus non arcu Integer nisl erat pellentesque quis metus et commodo commodo tortor Ut posuere est quam eget hendrerit leo molestie eu Nam pellentesque cursus porta
* Ciphertext:
* Contoh Enigma di internet:

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

* Konfigurasi Enigma

A screenshot of a computer

Description automatically generated

* Input

A screenshot of a text input

Description automatically generated

* Output

A screenshot of a computer screen

Description automatically generated

* Kondisi akhir Enigma

