

Laporan Tugas Kecil 1 Seleksi Lab IRK
tahun 2022/2023
Implementasi Enkripsi dan Deskripsi Text dengan Enigma Machine



Disusun Oleh:

Mohammad Rifqi Farhansyah

13521166

**PROGRAM STUDI TEKNIK INFORMATIKA
SEKOLAH TEKNIK ELEKTRO DAN INFORMATIKA
INSTITUT TEKNOLOGI BANDUNG
2023**

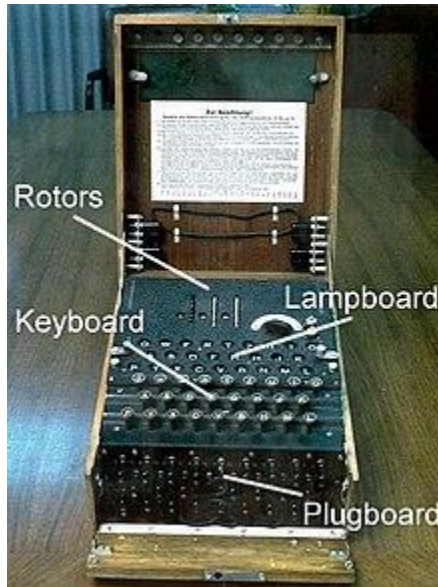
Daftar Isi

Daftar Isi	2
BAB I	3
BAB II	6
BAB III	8
BAB IV	10
BAB V	11

BAB I

Penjelasan Umum Enigma

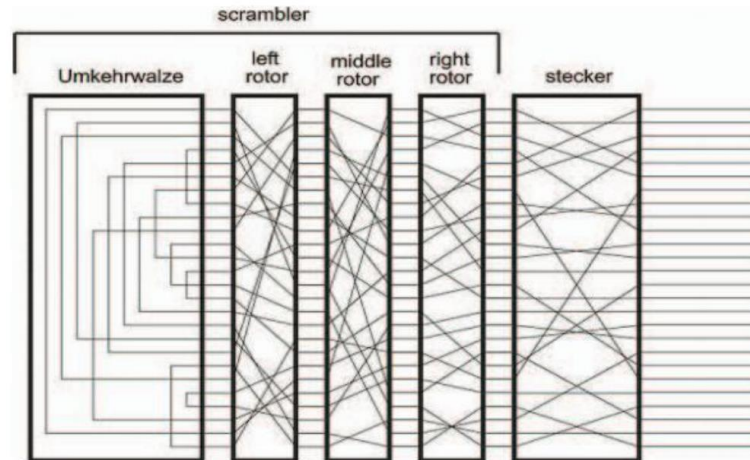
Enigma adalah sebuah mesin penyandi yang digunakan untuk mengenkripsikan dan mendekripsikan pesan rahasia. Enigma telah dipatenkan oleh insinyur Jerman yang bernama Arthur Scherbius. Mesin ini awalnya hanya digunakan untuk tujuan komersial, tetapi justru terkenal ketika digunakan oleh para tentara NAZI sebelum dan selama perang dunia II. Secara teknis, mesin enigma termasuk keluarga mesin rotor elektromekanik, yang memiliki berbagai model. Nama “Enigma” diambil dari kata latin *aenigma*, yang memiliki arti “teka-teki”. Pada Gambar 1.1.1 terlihat bahwa mesin enigma memiliki beberapa komponen utama yang terdiri atas: papan ketuk, lampu, steckerboard, scrambler, entry wheel, rotor, dan reflektor. Struktur umum inilah yang nantinya akan terus berkembang menjadi beberapa variasi lainnya.



Gambar 1.1. Mesin Enigma

Sumber: https://id.wikipedia.org/wiki/Mesin_Enigma

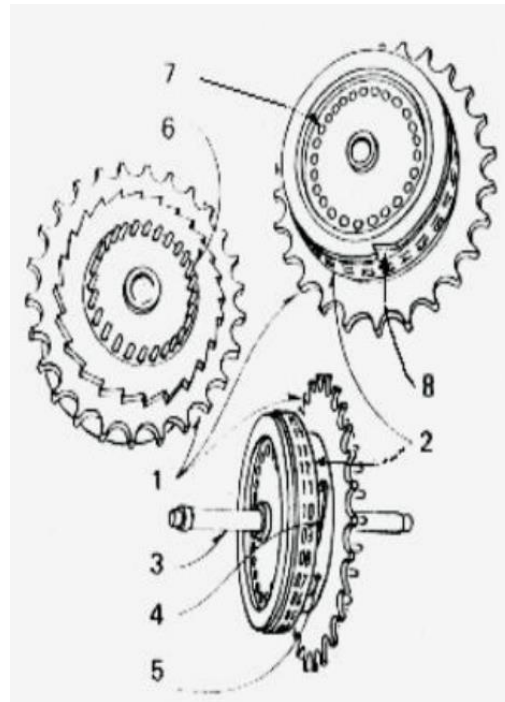
Versi Enigma yang paling terkenal adalah “Wehrmacht” milik tentara NAZI. Mesin ini mulai digunakan oleh tentara NAZI pada tahun 1928. Awalnya, mesin ini dianggap sebagai mesin kriptografi teraman di dunia, tetapi akhirnya dapat dipecahkan oleh pihak sekutu yang dipimpin oleh Alan Turing, sehingga mesin ini justru pada akhirnya merugikan pihak NAZI. Metode pemecahan (dekripsi) mesin ini pertama kali ditemukan pada tahun 1932 oleh beberapa kriptografer asal Polandia dari sebuah kantor sandi bernama Biuro Szyfrów. Marian Rejewski, Jerzy Różycki, dan Henryk Zygalski merupakan nama dari ketiga kriptografer tersebut. Namun pada tahun 1939, Jerman berhasil mendesain ulang mesin enigma, sehingga metode dekripsi dari mereka tidak dapat digunakan kembali. Berkat informasi dari Polandia, akhirnya Britania dan Prancis berhasil membuat sebuah mesin pemecah Enigma baru ini, yang diberi nama bombe. Informasi yang didapat Sekutu dari pemecahan enigma disebut sebagai ULTRA, yang terbukti amat penting bagi kemenangan sekutu pada perang dunia II. Menurut para ahli, perang dunia II dapat berakhir dua tahun lebih cepat berkat pemecahan enigma ini.



Gambar 1.2. Komponen Mekanik dan Wiring Enigma

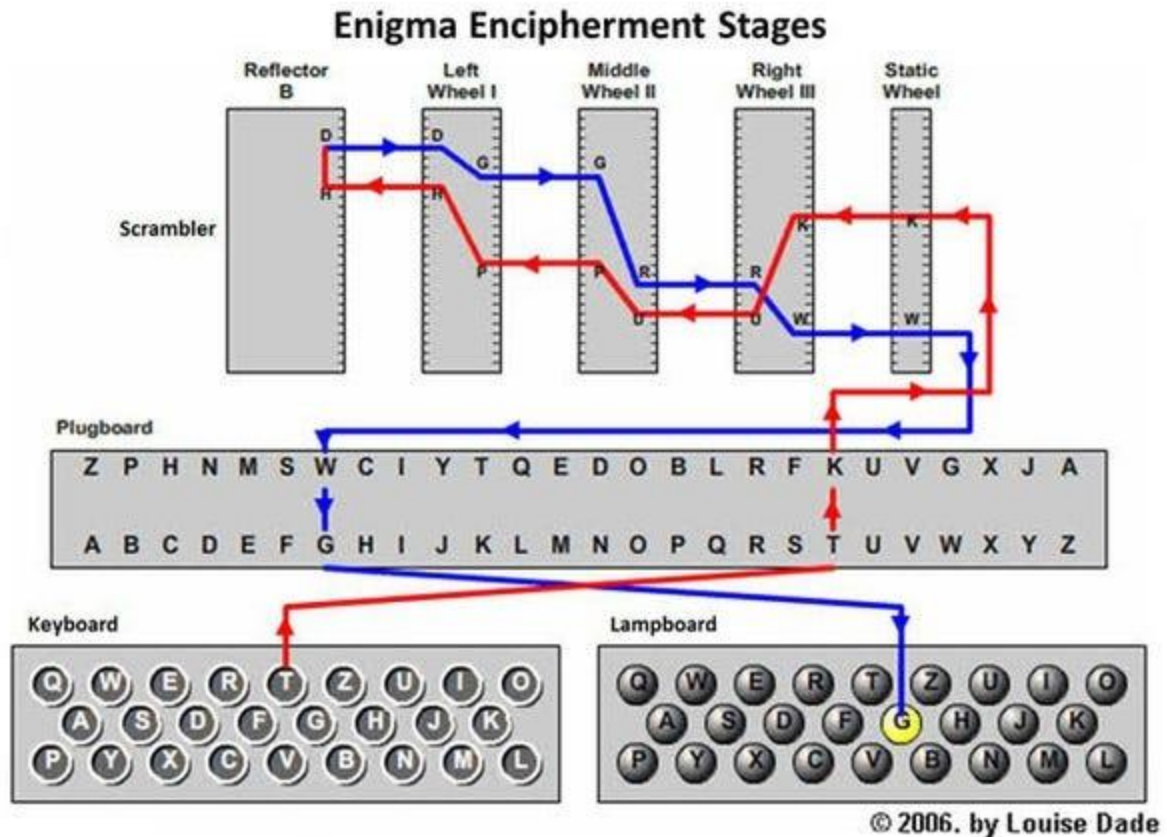
Sumber: https://id.wikipedia.org/wiki/Mesin_Enigma

Mesin enigma sesungguhnya merupakan kombinasi dari sistem mekanikal dan eletrikal. Sistem mekanikal mesin ini terdiri atas 4 buah rotor, yaitu: rotor kanan, rotor tengah, rotor kiri, serta rotor reflektor. Prinsip kerja mesin enigma adalah dengan mengalirkan arus listrik melalui rotor-rotor yang dapat berputar. Setiap rotor memiliki kontak elektrik di kedua sisi yang menghubungkan huruf-huruf pada keyboard dengan lampu-lampu pada lampboard. Ketika sebuah huruf pada keyboard ditekan, sinyal listrik akan mengalir melalui rotor-rotor dan reflektor, kemudian akan dihasilkan huruf yang telah terenkripsi pada lampboard.



Gambar 1.3. Komponen Rotor

Sumber: <https://fikirinotes.medium.com/cara-kerja-mesin-enigma-mesin-yang-digunakan-nazi-jerman-pada-perang-dunia-ke-2-e849335e4b23>



Gambar 1.4. Mekanisme Mesin Enigma

Sumber: <https://fikrinotes.medium.com/cara-kerja-mesin-enigma-mesin-yang-digunakan-nazi-jerman-pada-perang-dunia-ke-2-e849335e4b23>

Enigma menggunakan konfigurasi rotor yang dapat dipilih dan dikonfigurasi ulang untuk menghasilkan berbagai variasi enkripsi. Pengaturan rotor ini menjadikan enigma sangat sulit untuk dipecahkan oleh musuh, terutama karena pengaturan rotor dan konfigurasi yang berubah secara teratur.

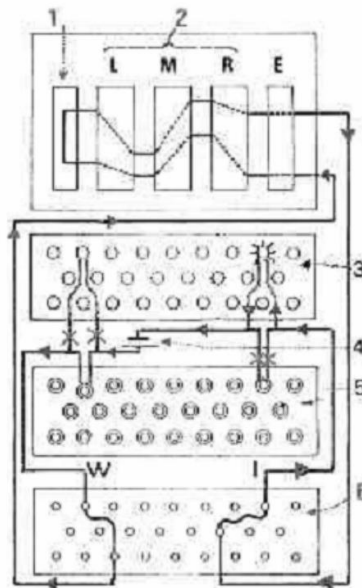
BAB II

Cara Kerja Enigma

Enkripsi yang dilakukan enigma sebenarnya merupakan sebuah proses substitusi, dimana sebuah huruf akan digantikan dengan tepat satu huruf juga. Akan tetapi, proses substitusi huruf dilakukan beberapa kali. Hal ini menyebabkan pesan akan sulit didekripsi kembali jika tidak dengan alat, pengaturan posisi, tipe substitusi, serta kode kunci yang sama. Seluruh proses tersebut sangat erat kaitannya dengan skema wiring pada tiap rotor seperti di Gambar 1.2.

Wiring pada mesin enigma berguna untuk mengalirkan listrik dari suatu rotor ke rotor lainnya, misalkan A pada rotor kiri terhubung dengan D pada rotor tengah, maka jika A pada rotor kiri dialiri arus listrik, maka D pada rotor tengah akan teraliri listrik juga. Secara sederhana, mekanisme wiring tersebut menunjukkan substitusi dari tombol yang ditekan dalam bentuk pemasangan lampu. Sesuai contoh sebelumnya, maka apabila tombol/saklar A ditekan, lampu D akan menyala. Hal tersebut akan dilakukan berulang-ulang namun dengan mengganti rotor yang sedang digunakan. Proses ini akan disertai dengan pergeseran rotor setiap kali ada tombol yang ditekan. Begitu seterusnya selama pesan diketik.

Reflektor pada mesin enigma akan ikut serta dalam proses enkripsi dengan membalikkan jalannya arus dari rotor kanan ke rotor kiri, yang efeknya akan meningkatkan kompleksitas dari substitusi huruf sebanyak 26 kali. Reflektor ini menyebabkan enigma tidak perlu mengubah state jika sedang ingin mengenkripsi sebuah pesan ataupun ingin mendeskripsikannya. Namun, reflektor menyebabkan enigma memiliki kelemahan, dimana dapat terjadinya resiprok. Resiprok adalah kondisi dimana huruf akan selalu dienkrpsi dengan pasangannya, sehingga tidak memungkinkan suatu huruf dienkrpsi menjadi dirinya sendiri, misalkan apabila huruf M dienkrpsi menjadi T, maka huruf T akan dienkrpsi menjadi huruf M pada rotor yang sama. Dengan demikian, huruf T tidak mungkin untuk dienkrpsi menjadi huruf T dan huruf M tidak mungkin dienkrpsi menjadi huruf M.



Gambar 2.1. Skema Mesin Enigma

Sumber: <https://fikrinotes.medium.com/cara-kerja-mesin-enigma-mesin-yang-digunakan-nazi-jerman-pada-perang-dunia-ke-2-e849335e4b23>

Sementara itu, terdapat beberapa tipe substitusi rotor yang tersedia untuk mesin enigma. Namun, pada setiap mesin enigma, hanya terdapat 3 tipe rotor yang dapat digunakan. Rotor-rotor tersebut akan dipasangan pada rotor kiri, tengah, dan kanan. Tipe-tipe rotor yang dapat digunakan antara lain:

Rotor	ABCDEFGHIJKLMNOPQRSTUVWXYZ
I	EKMFLGDQVZNTOWYHXUSPAIBRCJ
II	AJDKSIRUCBLHWTMCQGZNPYFVOE
III	BDFHJLCPRTXVZNYEIWGAKMUSQO
IV	ESOVZPJAYQUIRHXNLFTGKDCMWB
V	VZBRGITYUPSDNHLXAWMJQOFECK
VI	JPGVOUMFYQBENHZRDKASXLICTW
VII	NZJHGRCXMYSWBOUFAIVLPEKQDT
VIII	FKQHTLXOCBJSPDZRAMEWNIUYGV

Pada setiap rotor tersebut dikenal adanya istilah Turnover, yaitu posisi dimana sebuah rotor mulai bergerak menggeser rotor yang berada di sampingnya. Rotor kanan akan selalu bergerak 1 huruf setiap kali tombol ditekan serta apabila turnover dari rotor R tersebut adalah S, maka rotor R akan menggeser rotor M sejauh 1 huruf jika sudah mencapai posisi turnover-nya (posisi di huruf S). Setiap jenis rotor mempunyai turnover masing-masing. Sementara itu terdapat versi lain yang mengatakan bahwa turnover merupakan pergerakan posisi rotor setelah rotor di sebelahnya mencapai posisi notch. Posisi notch adalah posisi khusus pada rotor di mesin enigma dimana rotor tersebut mulai bergerak untuk menggeser rotor di sebelahnya. Setiap rotor memiliki satu atau beberapa notch yang ditempatkan pada posisi tertentu. Ketika rotor mencapai posisi notch, rotor di sebelahnya akan bergerak satu langkah.

Selain itu, adapula peran besar yang disumbangkan oleh komponen lainnya bernama plugboard. Plugboard sendiri adalah sebuah papan yang mengganti arus dari huruf awal ke huruf yang diinginkan dengan cara meneruskan arus tersebut dengan kabel, seperti pada Gambar 1.1. Plugboard akan menambahkan substitusi tergantung pada pasangan yang ditentukan dalam proses wiring.

BAB III

Enkripsi Enigma

Enkripsi pada enigma sebenarnya merupakan sebuah operasi permutasi yang cukup panjang, yaitu: $E = PRMLUL^{-1}M^{-1}R^{-1}P^{-1}$, dengan R adalah rotor kanan, M adalah rotor tengah, L adalah rotor kiri, P adalah plugboard, U adalah reflektor, serta E adalah hasil enkripsi. Seluruh operasi permutasi tersebut ditentukan oleh ketentuan Jerman yang berbeda-beda untuk tiap jaringan dan hari tertentu. Hal tersebut dilakukan Jerman dengan cara memberikan sebuah buku sebagai standar untuk masing-masing operator. Adapun hal-hal yang diatur adalah : pilihan rotor, peletakan posisi rotor, pemilihan huruf awal setiap rotor, posisi plug pada plugboard, dan tipe reflektor. Sebagai contoh, pada suatu hari standar yang disebarkan oleh kurir-lurir Jerman ke setiap operator enigma mereka adalah sebagai berikut:

25

I III V

B M X

DM OA MR IS NE IL KI UN

Artinya kode tersebut dikeluarkan pada tanggal 25 bulan itu, kemudian rotor yang digunakan untuk rotor kiri adalah I, rotor tengah adalah III, dan rotor kanan adalah V. Baris berikutnya merupakan penanda posisi awal untuk masing-masing rotor, jadi B adalah posisi awal dari rotor I, M adalah posisi awal dari rotor III, dan X adalah posisi awal dari rotor V. Sementara itu, baris terakhir berisi huruf-huruf yang perlu disambungkan pada plugboard.

Berikut ini adalah salah satu contoh langkah-langkah enkripsi dari mesin enigma:

	Rotor Kiri = I	Rotor Tengah = II	Rotor Kanan = III
Initial Position	A	A	A
Ring	A	A	A
Reflektor	UKW-B= YRUHQSLDPXNGOKMIEBFZCWVJAT		
Plugboard	AB		
InputText	AKU		
Entry	= ABCDEFGHIJKLMNOPQRSTUVWXYZ		
Rotor I	= EKMFLGDQVZNTOWYHXUSPAIBRCJ		
Rotor II	= AJDKSIRUXBLHWTMCQGZNPYFVOE		
Rotor III	= BDFHJLCPRXTXVZNYEIWGAKMUSQO		

1. Huruf A sebagai masukan karakter pertama akan diubah oleh plugboard menjadi huruf B, sesuai kabel yang terhubung pada plugboard.
2. B akan diubah menjadi huruf E oleh rotor kanan.
3. Huruf E masuk ke rotor tengah dan diubah menjadi huruf S.
4. S akan masuk ke rotor kiri dan berubah menjadi huruf F.
5. Reflektor kemudian mengubah huruf S menjadi F.

6. Lalu dikembalikan ke rotor kiri menjadi huruf D.
7. Huruf D diubah menjadi huruf C oleh rotor tengah.
8. C akan masuk ke rotor kanan dan diubah menjadi huruf A.
9. Terakhir, plugboard akan kembali merubah huruf A menjadi B, sehingga huruf B akan menyala pada lampboard.
10. Hal serupa akan dilakukan pada huruf K dan U dari string masukan.
11. Hasil enkripsi adalah BFF.

BAB IV

Dekripsi Enigma

Kode hasil enkripsi mesin enigma yang telah serumit itu dan bahkan diklaim oleh Jerman tidak mungkin dipecahkan tersebut ternyata tetap saja mempunyai kelemahan-kelemahan yang pada akhirnya berakhir pada terpercakannya kode enkripsi oleh pihak musuh. Akan tetapi secara umum, proses enkripsi dan dekripsi dari sebuah mesin enigma adalah sejalan, asalkan seluruh syarat terpenuhi, yaitu: rotor, initial position, ring, reflektor, serta plugboard yang digunakan sama.

Berikut ini adalah salah satu contoh langkah-langkah dekripsi dari mesin enigma:

	Rotor Kiri = I	Rotor Tengah = II	Rotor Kanan = III
Initial Position	A	A	A
Ring	A	A	A
Reflektor	UKW-B= YRUHQSLDPXNGOKMIEBFZCWVJAT		
Plugboard	AB		
InputText	BFF		
Entry = ABCDEFGHIJKLMNOPQRSTUVWXYZ			
Rotor I = EKMFLGDQVZNTOWYHXUSPAIBRCJ			
Rotor II = AJDKSIRUXBLHWTMCQGZNPYFVOE			
Rotor III = BDFHJLCPRCTXVZNYEIWGAKMUSQO			

1. Huruf B sebagai masukan karakter pertama akan diubah oleh plugboard menjadi huruf A, sesuai kabel yang terhubung pada plugboard.
2. A akan diubah menjadi huruf C oleh rotor kanan.
3. Huruf C masuk ke rotor tengah dan diubah menjadi huruf D.
4. D akan masuk ke rotor kiri dan berubah menjadi huruf F.
5. Reflektor kemudian mengubah huruf F menjadi S.
6. Lalu dikembalikan ke rotor kiri menjadi huruf S.
7. Huruf S diubah menjadi huruf E oleh rotor tengah.
8. E akan masuk ke rotor kanan dan diubah menjadi huruf B.
9. Terakhir, plugboard akan kembali merubah huruf B menjadi A, sehingga huruf A akan menyala pada lampboard.
10. Hal serupa akan dilakukan pada huruf F dan F dari string masukan.
11. Apabila telah selesai dilakukan, maka hasil dekripsi adalah AKU yang notabennya sama dengan contoh enkripsi pada Bab III hanya saja proses yang dilakukan dibalik urutannya.


BAB V

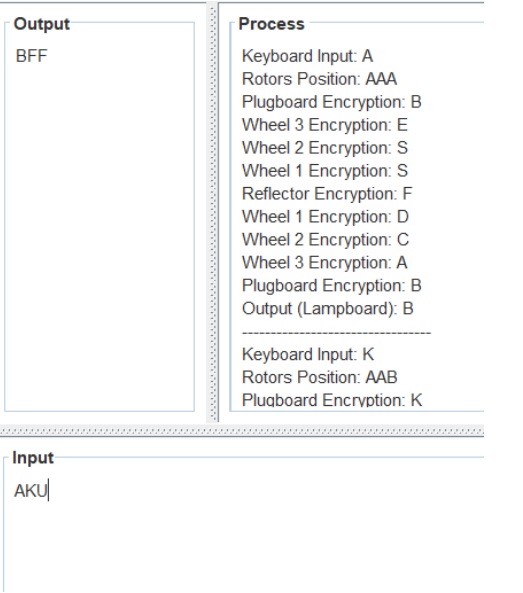
Perbandingan Program dengan Enigma Internet

Terdapat beberapa contoh screenshot yang diambil, untuk tiap kasus diberikan settingan yang digunakannya dalam bentuk tabel:

1. Kasus 1

	Rotor Kiri = I	Rotor Tengah = II	Rotor Kanan = III
Initial Position	A	A	A
Ring	A	A	A
Reflektor	UKW-B= YRUHQSLDPXNGOKMIEBFZCWVJAT		
Plugboard	AB		
InputText	AKU		





Keduanya menghasilkan output yang sama yaitu BFF

2. Kasus 2

	Rotor Kiri = I	Rotor Tengah = II	Rotor Kanan = III
Initial Position	A	A	A
Ring	A	A	A
Reflektor	UKW-B= YRUHQSLDPXNGOKMIEBFZCWVJAT		
Plugboard	AB CD GH IJ		
InputText	MAU		

Output

CIF

Process

Plugboard Encryption: U
 Wheel 3 Encryption: P
 Wheel 2 Encryption: C
 Wheel 1 Encryption: M
 Reflector Encryption: O
 Wheel 1 Encryption: M
 Wheel 2 Encryption: O
 Wheel 3 Encryption: F
 Plugboard Encryption: F
 Output (Lampboard): F

Input

MAU

Keduanya menghasilkan output yang sama yaitu CIF

3. Kasus 3

	Rotor Kiri = I	Rotor Tengah = II	Rotor Kanan = III
Initial Position	A	A	A
Ring	A	A	A
Reflektor	UKW-C= FVPJIAOYEDRZXWGCTKUQSBNMHL		
Plugboard	AB CD GH IJ		
InputText	MASUK		

Output

RXDBN

Process

Plugboard Encryption: K
 Wheel 3 Encryption: Z
 Wheel 2 Encryption: E
 Wheel 1 Encryption: L
 Reflector Encryption: Z
 Wheel 1 Encryption: J
 Wheel 2 Encryption: B
 Wheel 3 Encryption: N
 Plugboard Encryption: N
 Output (Lampboard): N

Input

MASUK

Keduanya menghasilkan output yang sama yaitu RXDBN

4. Kasus 4

	Rotor Kiri = I	Rotor Tengah = II	Rotor Kanan = III
Initial Position	B	C	E
Ring	A	A	A
Reflektor	UKW-B= YRUHQSLDPXNGOKMIEBFZCWVJAT		
Plugboard	AB CD GH IJ		
InputText	LAB		

Plaintext:

LAB

Ciphertext:

WWO

Show Encryption Steps

Clear Encrypt Decrypt

Encryption Steps:

Keyboard Input: L
Rotors Position: BCF
Plugboard Encryption: L
Wheel 3 Encryption: D
Wheel 2 Encryption: G
Wheel 1 Encryption: F
Reflector Encryption: I
Wheel 1 Encryption: Y
Wheel 2 Encryption: Y
Wheel 3 Encryption: W
Plugboard Encryption: W
Output (Lampboard): W

Output

WWO

Process

Plugboard Encryption: A
Wheel 3 Encryption: I
Wheel 2 Encryption: J
Wheel 1 Encryption: M
Reflector Encryption: O
Wheel 1 Encryption: S
Wheel 2 Encryption: F
Wheel 3 Encryption: O
Plugboard Encryption: O
Output (Lampboard): O

Input

LAB

Kesimpulannya, keseluruhan hasil dengan settingan yang berbeda tetap menghasilkan pesan enkripsi yang sama.