

Laporan Tugas Seleksi Lab Ilmu Rekayasa Komputasi
“Implementasi Kriptografi Sederhana dalam Pengenkripsi Pesan
Menggunakan Mesin Enigma”



Oleh:
Puti Nabilla Aidira (13521088)

Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
2023

Daftar Isi

Daftar Isi	1
1. Enkripsi	2
2. Deskripsi Enigma	2
3. Cara Kerja Enigma	3
A. Plugboard	3
B. Rotor	4
C. Reflector	6
4. Contoh Tahapan Enkripsi dan Dekripsi Enigma	7
5. Perbandingan Hasil Program Buatan dengan Hasil Program di Internet	13

1. Enkripsi

Enkripsi adalah proses penyembunyian pesan/data dengan mengubahnya menjadi bentuk yang sulit dipahami orang lain. Proses pengubahan ini dilakukan menggunakan aturan-aturan tertentu. Orang yang menerima pesan terenkripsi dapat memahami pesan tersebut dengan melakukan dekripsi. Dekripsi adalah proses pengembalian pesan terenkripsi menjadi bentuk semula. Untuk melakukan dekripsi, seseorang perlu mengetahui aturan-aturan dekripsi untuk metode enkripsi tertentu. Terdapat banyak metode enkripsi, salah satunya adalah menggunakan mesin enigma.

2. Deskripsi Enigma

Enigma adalah sebuah mesin enkripsi elektromekanis yang dikembangkan oleh Jerman Nazi pada awal tahun 1920-an. Enigma digunakan secara luas sebagai alat pengamanan komunikasi selama Perang Dunia II. Enigma bekerja dengan mengubah suatu huruf masukan menjadi huruf lain.

Enigma terdiri dari 5 komponen utama: *keyboard*, 3 buah rotor, *reflector*, *plugboard*, dan *lampboard* (Gambar 1). Untuk melakukan enkripsi, operator biasanya akan mengetikan huruf pada *keyboard* kemudian mencatat huruf yang menyala pada *lampboard* sebagai pesan hasil enkripsi. Operator dapat mengubah konfigurasi rotor, *reflector*, dan *plugboard* untuk mengubah aturan enkripsi. Pengenkripsi mesin enigma adalah pengenkripsi simetris. Sehingga, untuk melakukan dekripsi, penerima pesan dapat kembali mengetikan pesan terenkripsi, kemudian mencatat huruf yang menyala pada *lampboard*. Dengan catatan, mesin enigma yang digunakan haruslah memiliki konfigurasi awal yang sama dengan mesin yang digunakan untuk mengenkripsi. Konfigurasi-konfigurasi yang dapat dilakukan pada mesin enigma dapat dilihat pada tabel 1.



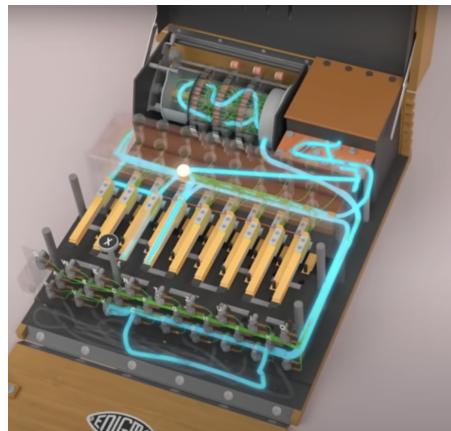
Gambar 1. Komponen Mesin Enigma
(<https://brilliant.org/wiki/enigma-machine/>)

Tabel 1. Konfigurasi Enigma

Komponen	Konfigurasi yang dapat dilakukan
Rotor	Tipe rotor (<i>wiring & notch</i>)
	Posisi <i>ring</i>
	Posisi (<i>offset</i>) plat huruf
Reflector	Tipe reflector (<i>wiring</i>)
Plugboard	Pasangan huruf/soket

3. Cara Kerja Enigma

Mesin enigma bekerja menggunakan serangkaian komponen elektromekanis. Secara umum, sesaat setelah suatu huruf diketikan, listrik akan mengalir dari *keyboard* melalui *plugboard* → *entry disk* → rotor 1 → rotor 2 → rotor 3 → *reflector* → rotor 3 → rotor 2 → rotor 1 → *entry disk* → *plugboard* → *lampboard* (lampa untuk huruf terenkripsi menyala) (Gambar 2.). *Entry disk* berfungsi sebagai pengatur kabel sebelum dan setelah melalui komponen rotor dan reflektor. *Entry disk* biasanya tidak melakukan perubahan huruf. Sebaliknya, pada masing-masing komponen lain terjadi mekanisme enkripsi yang akan dijelaskan pada poin-poin dibawah ini.



Gambar 2. Aliran Listrik pada Proses Enkripsi Mesin Enigma
(https://www.youtube.com/watch?v=ybkkiGtJmkM&ab_channel=JaredOwen)

A. Plugboard

Plugboard pada enigma merupakan panel yang berisi 26 soket, masing-masing merepresentasikan 26 huruf pada alfabet (Gambar 3). Fungsi utama *plugboard* adalah untuk menukar huruf-huruf tertentu sebelum aliran listrik melewati rotor-rotor. Dengan menghubungkan soket-soket yang sesuai dengan kabel, operator dapat mengatur pasangan huruf yang akan saling tukar. Misalnya, operator dapat menghubungkan soket 'A' dengan soket 'Q', yang berarti setiap kali huruf 'A' ditekan di *keyboard*, aliran listriknya akan melalui kabel dan keluar dari soket 'Q' begitu pula sebaliknya. Pada satu kali proses

enkripsi, aliran listrik akan melewati *plugboard* sebanyak 2 kali: sesaat setalah *keyboard* ditekan dan sesaat sebelum lampu *lampboard* menyala.



Gambar 3. *Plugboard*
(<https://www.wikidata.org/wiki/Q101516613>)

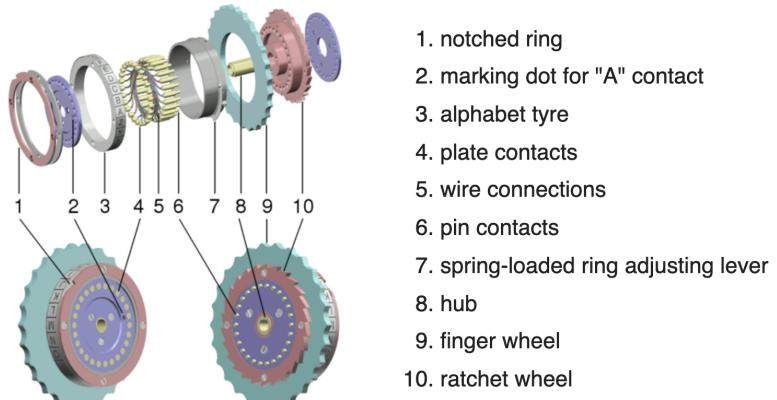
B. Rotor

Sebuah mesin enigma biasanya memiliki 3 buah rotor. Setiap rotor memiliki alfabet yang tercetak pada permukaannya, dan setiap huruf pada rotor dihubungkan ke huruf lain melalui kabel internal. Struktur lengkap dari sebuah rotor dapat dilihat pada Gambar 4. Tiga buah rotor terhubung melalui kontak pin.

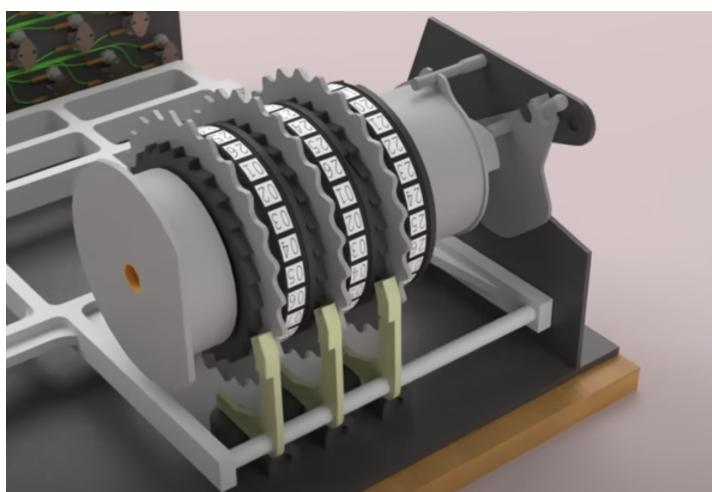
Terdapat berbagai macam tipe rotor yang masing-masing memiliki *wiring* (susunan kabel internal) dan posisi *notch* yang berbeda. Contohnya, untuk rotor tipe I memiliki *wiring* "EKMFLGDQVZNTOWYHXUSPAIBRCJ". Hal ini artinya, pada konfigurasi *default* (posisi plat huruf dan posisi *ring* di huruf yang sama) kabel untuk huruf masukan "A" akan keluar sebagai kabel untuk huruf "E", "B" sebagai "K" dan seterusnya. Namun, jika posisi plat huruf dan ring di huruf yang berbeda, misal plat huruf di "B" dan ring di "A", huruf masukan "A" akan masuk ke rotor sebagai huruf "B", sehingga keluar menjadi huruf "K" dan masuk ke rotor selanjutnya sebagai huruf "J". Selain melalui pengaturan konfigurasi awal, posisi (*offset*) plat huruf dari rotor 1 juga akan berubah setiap kali keyboard ditekan. Hal ini menambah kompleksitas enkripsi enigma. Untuk rotor 2, *offset* plat huruf akan bertambah setiap kali rotor 2 atau rotor 1 mencapai posisi *notch*. Untuk rotor 3, *offset* plat huruf akan bertambah setiap kali rotor 2 mencapai posisi *notch*. Pada praktiknya, selisih antara *offset* plat huruf relatif terhadap *offset ring* lah yang harus diperhitungkan. Selisih ini menentukan di mana aliran listrik masuk ke sebuah rotor dan di mana aliran listrik akan masuk ke rotor berikutnya, berdasarkan *wiring* tertentu.

Mekanisme pergerakan *offset* rotor menggunakan mekanisme Rachet and Pawl (Gambar 5). Dengan mekanisme ini, rotor hanya dapat bergerak 1 arah. Mekanisme *notch* bekerja dengan menghambat "lengan" Pawl selain pada posisi huruf yang ditentukan (disebut posisi *notch*) (Gambar 6).

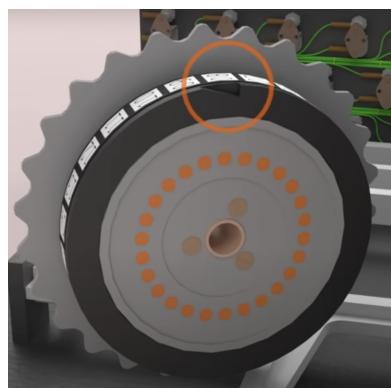
Dalam 1 kali proses enkripsi, aliran listrik akan melewati masing-masing rotor sebanyak 2 kali: melewati sisi kanan rotor (sebelum mencapai *reflector*) dan melewati sisi kiri rotor (setelah melewati *reflector*). Saat melewati sisi kiri rotor enkripsi menjadi terbalik, contohnya untuk *wiring* "EKMFLGDQVZNTOWYHXUSPAIBRCJ" huruf "E" akan menjadi huruf "A", "K" menjadi "B", dan seterusnya.



Gambar 4. Struktur Rotor
(https://en.wikipedia.org/wiki/Enigma_rotor_details)



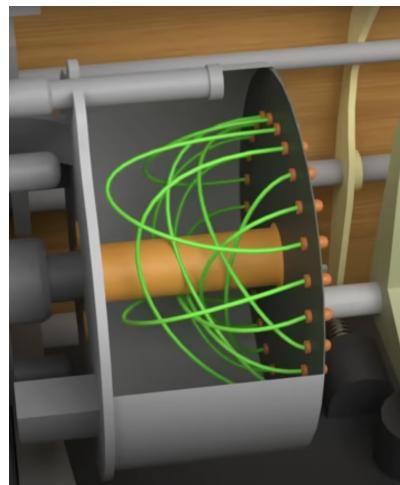
Gambar 5. Mekanisme Rachet and Pawl untuk Pergerakan Offset Rotor
(Youtube:[How did the Enigma Machine work?](#))



Gambar 6. Contoh notch pada rotor
(Youtube:[How did the Enigma Machine work?](#))

C. Reflector

Setelah melewati 3 rotor, aliran listrik akan memasuki reflektor untuk kemudian dialirkan kembali melewati rotor. *Reflector* berbentuk piringan dan memiliki sistem *wiring* yang mirip dengan rotor (Gambar 7). Namun, berbeda dengan rotor, *reflector* tidak bergerak sehingga enkripsi yang dilakukan pun bersifat statis. Enkripsi pada reflector menukar huruf secara berpasangan. Contohnya, reflector tipe B (UKW-B) dengan *wiring* "YRUHQSLDPXNGOKMIEBFZCWVJAT" akan mengenkripsi "A" menjadi "Y" begitu pula sebaliknya "Y" menjadi "A".



Gambar 7. *Reflector*
(Youtube:[How did the Enigma Machine work?](#))

4. Contoh Tahapan Enkripsi dan Dekripsi Enigma

Contoh 1

Konfigurasi:

Rotor 1 → I (*wiring*: EKMFLGDQVZNTOWYHXUSPAIBRCJ; *notch*: Y)

Rotor 2 → II (*wiring*: AJDKSIRUXBLHWWTMCQGZNPFVOE; *notch*: M)

Rotor 3 → III (*wiring*: BDFHJLCPTXVZNYEIWGAKMUSQO *notch*: D)

Reflector → UKW-B (*wiring*: YRUHQSLDPXNGOKMIEBFZCWVJAT)

Posisi plat huruf awal: "AAA" (berturut-turut untuk rotor 3, rotor 2, dan rotor 1)

Posisi *ring*: "AAA" (berturut-turut untuk rotor 3, rotor 2, dan rotor 1)

Plugboard: tidak dikonfigurasi

<i>Keyboard (input)</i>	<i>Plugboard</i>	Rotor 1	Rotor 2	Rotor 3	<i>Reflector</i>
A	A	J	B	D	H
- Rotor 1 step, plat huruf menjadi "AAB"		<ul style="list-style-type: none"> - Selisih <i>offset</i> plat huruf dengan ring = $B - A = 1$ - Saat masuk: sesuai <i>wiring</i> yang sejajar dengan A + 1 adalah K - Saat masuk ke rotor selanjutnya: huruf menjadi $K - 1 = J$ 	<ul style="list-style-type: none"> - Selisih <i>offset</i> plat huruf dengan ring = $A - A = 0$ - Saat masuk: sesuai <i>wiring</i> yang sejajar dengan J + 0 adalah B - Saat masuk ke rotor selanjutnya: huruf menjadi $B - 0 = B$ 	<ul style="list-style-type: none"> - Selisih <i>offset</i> plat huruf dengan ring = $A - A = 0$ - Saat masuk: sesuai <i>wiring</i> yang sejajar dengan B + 0 adalah D - Saat masuk ke reflector: huruf menjadi $D - 0 = D$ 	<ul style="list-style-type: none"> - Sesuai <i>wiring</i> D akan keluar sebagai H

<i>Lampboard (output)</i>	<i>Plugboard</i>	Rotor 1	Rotor 2	Rotor 3
F	F	F	C	D
		<ul style="list-style-type: none"> - Selisih <i>offset</i> plat huruf dengan ring = $B - A = 1$ - Saat masuk: sesuai <i>wiring</i> (terbalik) yang sejajar dengan C + 1 adalah G - Saat masuk ke entrydisk: huruf menjadi $G - 1 = F$ 	<ul style="list-style-type: none"> - Selisih <i>offset</i> plat huruf dengan ring = $A - A = 0$ - Saat masuk: sesuai <i>wiring</i> (terbalik) yang sejajar dengan D + 0 adalah C - Saat masuk ke rotor selanjutnya: huruf menjadi $C - 0 = C$ 	<ul style="list-style-type: none"> - Selisih <i>offset</i> plat huruf dengan ring = $A - A = 0$ - Saat masuk: sesuai <i>wiring</i> (terbalik) yang sejajar dengan H + 0 adalah D - Saat masuk ke rotor selanjutnya: huruf menjadi $D - 0 = D$

Contoh 2

Konfigurasi:

Rotor 1 → I (*wiring*: EKMFLGDQVZNTOWYHXUSPAIBRCJ; *notch*: Y)

Rotor 2 → II (*wiring*: AJDKSIRUXBLHWTMCGZNPFVOE; *notch*: M)

Rotor 3 → III (*wiring*: BDFHJLCPRTXVZNYEIWGAKMUSQO *notch*: D)

Reflector → UKW-B (*wiring*: YRUHQSLDPXNGOKMIEBFZCWVJAT)

Posisi plat huruf awal: "AAQ" (berturut-turut untuk rotor 3, rotor 2, dan rotor 1)

Posisi *ring*: "AAA" (berturut-turut untuk rotor 3, rotor 2, dan rotor 1)

Plugboard: A ↔ B, N ↔ X

<i>Keyboard (input)</i>	<i>Plugboard</i>	Rotor 1	Rotor 2	Rotor 3	<i>Reflector</i>
A	B	B	C	F	S
<ul style="list-style-type: none"> - Posisi plat huruf Q adalah ketika notch rotor 1 berada pada posisi Y, Rotor 2 step, plat huruf menjadi "ABQ" - Rotor 1 step, plat huruf menjadi "ABR" 	<ul style="list-style-type: none"> - A ditukar dengan B 	<ul style="list-style-type: none"> - Selisih offset plat huruf dengan ring = $R - A = 17$ - Saat masuk: sesuai <i>wiring</i> yang sejajar dengan $B + 17$ adalah S - Saat masuk ke rotor selanjutnya: huruf menjadi $S - 17 = B$ 	<ul style="list-style-type: none"> - Selisih offset plat huruf dengan ring = $B - A = 1$ - Saat masuk: sesuai <i>wiring</i> yang sejajar dengan $B + 1$ adalah D - Saat masuk ke rotor selanjutnya: huruf menjadi $D - 1 = C$ 	<ul style="list-style-type: none"> - Selisih offset plat huruf dengan ring = $A - A = 0$ - Saat masuk: sesuai <i>wiring</i> yang sejajar dengan $C + 0$ adalah F - Saat masuk ke reflector: huruf menjadi $F - 0 = F$ 	<ul style="list-style-type: none"> - Sesuai <i>wiring</i> F akan keluar sebagai S

<i>Lampboard (output)</i>	<i>Plugboard</i>	Rotor 1	Rotor 2	Rotor 3
X	X	N	U	X
	<ul style="list-style-type: none"> - N ditukar dengan X 	<ul style="list-style-type: none"> - Selisih offset plat huruf dengan ring = $R - A = 17$ - Saat masuk: sesuai <i>wiring</i> (terbalik) yang sejajar dengan $U + 17$ adalah E - Saat masuk ke entrydisk: huruf menjadi $E - 17 = N$ 	<ul style="list-style-type: none"> - Selisih offset plat huruf dengan ring = $B - A = 1$ - Saat masuk: sesuai <i>wiring</i> (terbalik) yang sejajar dengan $X + 1$ adalah V - Saat masuk ke rotor selanjutnya: huruf menjadi $V - 1 = U$ 	<ul style="list-style-type: none"> - Selisih offset plat huruf dengan ring = $A - A = 0$ - Saat masuk: sesuai <i>wiring</i> (terbalik) yang sejajar dengan $S + 0$ adalah X - Saat masuk ke rotor selanjutnya: huruf menjadi $X - 0 = X$

Contoh 3

Konfigurasi:

Rotor 1 → III (*wiring*: BDFHJLCPRTXVZNYEIWGAKMUSQO; *notch*: D)

Rotor 2 → II (*wiring*: AJDKSIRUXBLHWWTMCQGZNPFVOE; *notch*: M)

Rotor 3 → I (*wiring*: EKMFLGDQVZNTOWYHXUSPAIBRCJ *notch*: Y)

Reflector → UKW-B (*wiring*: YRUHQSLDPXNGOKMIEBFZCWVJAT)

Posisi plat huruf awal: "AAA" (berturut-turut untuk rotor 3, rotor 2, dan rotor 1)

Posisi *ring*: "BBB" (berturut-turut untuk rotor 3, rotor 2, dan rotor 1)

Plugboard: tidak dikonfigurasi

<i>Keyboard (input)</i>	<i>Plugboard</i>	Rotor 1	Rotor 2	Rotor 3	<i>Reflector</i>
A	A	B	B	F	S
- Rotor 1 step, plat huruf menjadi " AAB "		<ul style="list-style-type: none"> - Selisih <i>offset</i> plat huruf dengan <i>ring</i> = $B - B = 0$ - Saat masuk: sesuai <i>wiring</i> yang sejajar dengan A + 0 adalah B - Saat masuk ke rotor selanjutnya: huruf menjadi $B - 0 = B$ 	<ul style="list-style-type: none"> - Selisih <i>offset</i> plat huruf dengan <i>ring</i> = $A - B = -1$ - Saat masuk: sesuai <i>wiring</i> yang sejajar dengan B - 1 adalah A - Saat masuk ke rotor selanjutnya: huruf menjadi $A + 1 = B$ 	<ul style="list-style-type: none"> - Selisih <i>offset</i> plat huruf dengan <i>ring</i> = $A - B = -1$ - Saat masuk: sesuai <i>wiring</i> yang sejajar dengan B - 1 adalah E - Saat masuk ke reflector: huruf menjadi $E + 1 = F$ 	<ul style="list-style-type: none"> - Sesuai <i>wiring</i> F akan keluar sebagai S

<i>Lampboard (output)</i>	<i>Plugboard</i>	Rotor 1	Rotor 2	Rotor 3
E	E	E	J	Y
		<ul style="list-style-type: none"> - Selisih <i>offset</i> plat huruf dengan <i>ring</i> = $B - B = 0$ - Saat masuk: sesuai <i>wiring</i> (terbalik) yang sejajar dengan J + 0 adalah E - Saat masuk ke entrydisk: huruf menjadi $E - 0 = E$ 	<ul style="list-style-type: none"> - Selisih <i>offset</i> plat huruf dengan <i>ring</i> = $A - B = -1$ - Saat masuk: sesuai <i>wiring</i> (terbalik) yang sejajar dengan Y - 1 adalah I - Saat masuk ke rotor selanjutnya: huruf menjadi $I + 1 = J$ 	<ul style="list-style-type: none"> - Selisih <i>offset</i> plat huruf dengan <i>ring</i> = $A - B = -1$ - Saat masuk: sesuai <i>wiring</i> (terbalik) yang sejajar dengan S - 1 adalah X - Saat masuk ke rotor selanjutnya: huruf menjadi $X + 1 = Y$

Contoh 4

Konfigurasi:

Rotor 1 → III (*wiring*: BDFHJLCPRTXVZNYEIWGAKMUSQO; *notch*: D)

Rotor 2 → II (*wiring*: AJDKSIRUXBLHWTCQGZNPFVOE; *notch*: M)

Rotor 3 → I (*wiring*: EKMFLGDQVZNTOWYHXUSPAIBRCJ *notch*: Y)

Reflector → UKW-B (*wiring*: YRUHQSLDPXNGOKMIEBFZCWVJAT)

Posisi plat huruf awal: "AEV" (berturut-turut untuk rotor 3, rotor 2, dan rotor 1)

Posisi *ring*: "AAA" (berturut-turut untuk rotor 3, rotor 2, dan rotor 1)

Plugboard: A ↔ R

<i>Keyboard (input)</i>	<i>Plugboard</i>	Rotor 1	Rotor 2	Rotor 3	<i>Reflector</i>
A	R	R	A	J	X
<ul style="list-style-type: none"> - Posisi plat huruf E adalah ketika notch rotor 2 berada pada posisi M, Rotor 3 step, plat huruf menjadi "BEV" - Posisi plat huruf V adalah ketika notch rotor 1 berada pada posisi D, Rotor 2 step, plat huruf menjadi "BFV" - Rotor 1 step, plat huruf menjadi "BFW" 	<ul style="list-style-type: none"> - A ditukar dengan R 	<ul style="list-style-type: none"> - Selisih <i>offset</i> plat huruf dengan ring = $W - A = 22$ - Saat masuk: sesuai <i>wiring</i> yang sejajar dengan $R + 22$ adalah N - Saat masuk ke rotor selanjutnya: huruf menjadi $N - 22 = R$ 	<ul style="list-style-type: none"> - Selisih <i>offset</i> plat huruf dengan ring = $F - A = 5$ - Saat masuk: sesuai <i>wiring</i> yang sejajar dengan $R + 5$ adalah D - Saat masuk ke rotor selanjutnya: huruf menjadi $F - 5 = A$ 	<ul style="list-style-type: none"> - Selisih <i>offset</i> plat huruf dengan ring = $B - A = 1$ - Saat masuk: sesuai <i>wiring</i> yang sejajar dengan $A + 1$ adalah K - Saat masuk ke reflector: huruf menjadi $K - 1 = J$ 	<ul style="list-style-type: none"> - Sesuai <i>wiring</i> J akan keluar sebagai X

<i>Lampboard (output)</i>	<i>Plugboard</i>	Rotor 1	Rotor 2	Rotor 3
P	P	P	Z	N
		<ul style="list-style-type: none"> - Selisih <i>offset</i> plat huruf dengan ring = $W - A = 22$ - Saat masuk: sesuai <i>wiring</i> (terbalik) yang sejajar dengan $Z + 22$ adalah L - Saat masuk ke entrydisk: huruf menjadi $L - 22 = P$ 	<ul style="list-style-type: none"> - Selisih <i>offset</i> plat huruf dengan ring = $F - A = 5$ - Saat masuk: sesuai <i>wiring</i> (terbalik) yang sejajar dengan $N + 5$ adalah E - Saat masuk ke rotor selanjutnya: huruf menjadi $E - 5 = Z$ 	<ul style="list-style-type: none"> - Selisih <i>offset</i> plat huruf dengan ring = $B - A = 1$ - Saat masuk: sesuai <i>wiring</i> (terbalik) yang sejajar dengan $X + 1$ adalah O - Saat masuk ke rotor selanjutnya: huruf menjadi $O - 1 = N$

Contoh Enkripsi Pesan

Konfigurasi:

Rotor 1 → III (*wiring*: BDFHJLCPRTXVZNYEIWGAKMUSQO; *notch*: D)

Rotor 2 → II (*wiring*: AJDKSIRUXBLHWTCQGZNPFVOE; *notch*: M)

Rotor 3 → I (*wiring*: EKMFLGDQVZNTOWYHXUSPAIBRCJ *notch*: Y)

Reflector → UKW-B (*wiring*: YRUHQSLDPXNGOKMIEBFZCWVJAT)

Posisi plat huruf awal: "AEV" (berturut-turut untuk rotor 3, rotor 2, dan rotor 1)

Posisi *ring*: "AAB" (berturut-turut untuk rotor 3, rotor 2, dan rotor 1)

Plugboard: A ↔ B, S ↔ X, N ↔ J

Keyboard	E	N	I	G	M	A
<i>Plugboard</i>	E	J	I	G	M	A
Rotor 1	T	P	O	L	W	B
Rotor 2	J	K	I	L	E	M
Rotor 3	M	S	Y	N	F	V
<i>Reflector</i>	O	F	A	K	S	W
Rotor 3	S	E	V	D	K	P
Rotor 2	D	W	V	A	P	C
Rotor 1	T	B	A	Q	A	G
<i>Plugboard</i>	T	P	A	Q	A	G
Lampboard	T	P	A	Q	A	G

Contoh Dekripsi Pesan

Konfigurasi:

Rotor 1 → III (*wiring*: BDFHJLCPRTXVZNYEIWGAKMUSQO; *notch*: D)

Rotor 2 → II (*wiring*: AJDKSIRUXBLHWTCQGZNPFVOE; *notch*: M)

Rotor 3 → I (*wiring*: EKMFLGDQVZNTOWYHXUSPAIBRCJ *notch*: Y)

Reflector → UKW-B (*wiring*: YRUHQSLDPXNGOKMIEBFZCWVJAT)

Posisi plat huruf awal: "AEV" (berturut-turut untuk rotor 3, rotor 2, dan rotor 1)

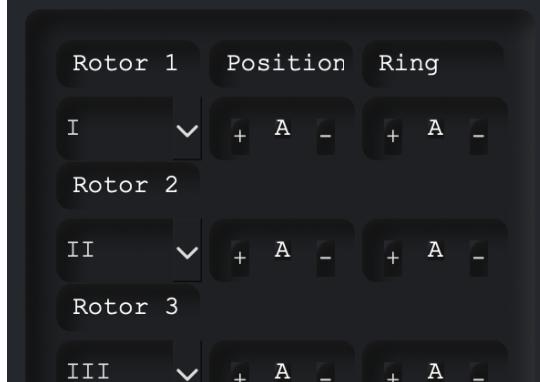
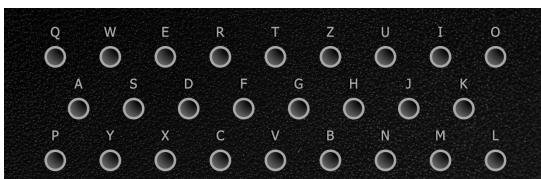
Posisi *ring*: "AAB" (berturut-turut untuk rotor 3, rotor 2, dan rotor 1)

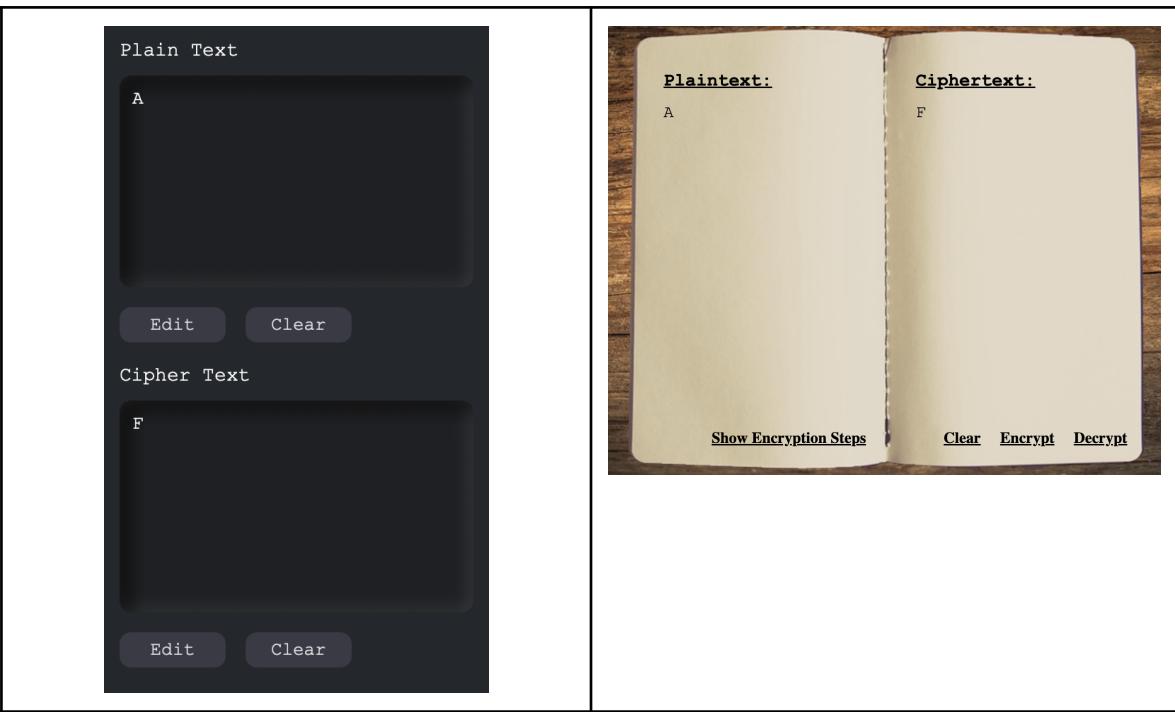
Plugboard: A ↔ B, S ↔ X, N ↔ J

Keyboard	T	P	A	Q	A	G
<i>Plugboard</i>	T	P	A	Q	A	G
Rotor 1	T	B	A	Q	A	G
Rotor 2	D	W	V	A	P	C
Rotor 3	S	E	V	D	K	P
<i>Reflector</i>	O	F	A	K	S	W
Rotor 3	M	S	Y	N	F	V
Rotor 2	J	K	I	L	E	M
Rotor 1	T	P	O	L	W	B
<i>Plugboard</i>	E	J	I	G	M	A
Lampboard	E	N	I	G	M	A

5. Perbandingan Hasil Program Buatan dengan Hasil Program di Internet

Program buatan dapat diakses di <https://github.com/Putinabillaa/EnigmaM3Simulator>. Program di internet yang dijadikan referensi dapat diakses pada <https://www.101computing.net/enigma-machine-emulator/>. Sebagai catatan, penomoran rotor pada program buatan dimulai dari kanan ke kiri (aliran listrik pertama kali melewati rotor 1 dan kembali ke rotor 1). Sedangkan, pada program internet penomoran rotor dimulai dari kiri ke kanan (aliran listrik pertama kali melewati rotor 3 dan kembali ke rotor 3).

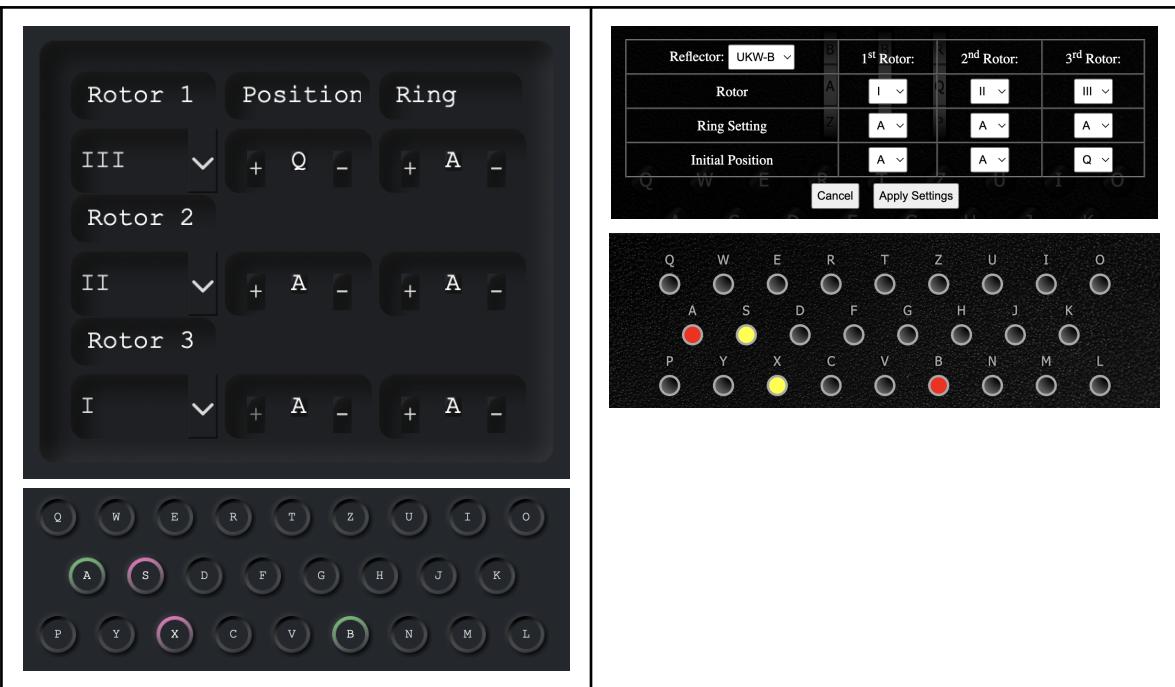
Program Buatan	Program Internet
Contoh 1	
Konfigurasi	
 	
Input - Output	



Langkah	
Input: A Plugboard: A Rotor 1: J Rotor 2: B Rotor 3: D Reflector: H Rotor 3: D Rotor 2: C Rotor 1: F Output (Plugboard): F	Keyboard Input: A Rotors Position: AAB Plugboard Encryption: A Wheel 3 Encryption: J Wheel 2 Encryption: B Wheel 1 Encryption: D Reflector Encryption: H Wheel 1 Encryption: D Wheel 2 Encryption: C Wheel 3 Encryption: F Plugboard Encryption: F Output (Lampboard): F

Contoh 2

Konfigurasi



Input-Output

Plain Text

```
HAI
```

Cipher Text

```
WSD
```

Plaintext:

```
HAI
```

Ciphertext:

```
WSD
```

Show Encryption Steps **Clear** **Encrypt** **Decrypt**

Langkah

Input: H
Plugboard: H
Rotor 1: Z
Rotor 2: E
Rotor 3: L
Reflector: G
Rotor 3: F
Rotor 2: W
Rotor 1: W
Output (Plugboard): W

Input: A
Plugboard: B
Rotor 1: I
Rotor 2: X
Rotor 3: R
Reflector: B
Rotor 3: W
Rotor 2: M
Rotor 1: X
Output (Plugboard): S

Input: I
Plugboard: I
Rotor 1: K
Rotor 2: L
Rotor 3: T
Reflector: Z
Rotor 3: J
Rotor 2: B
Rotor 1: D
Output (Plugboard): D

Keyboard Input: H
Rotors Position: AAR
Plugboard Encryption: H
Wheel 3 Encryption: Z
Wheel 2 Encryption: E
Wheel 1 Encryption: L
Reflector Encryption: G
Wheel 1 Encryption: F
Wheel 2 Encryption: W
Wheel 3 Encryption: W
Plugboard Encryption: W
Output (Lampboard): W

Keyboard Input: A
Rotors Position: AAS
Plugboard Encryption: B
Wheel 3 Encryption: I
Wheel 2 Encryption: X
Wheel 1 Encryption: R
Reflector Encryption: B
Wheel 1 Encryption: W
Wheel 2 Encryption: M
Wheel 3 Encryption: X
Plugboard Encryption: S
Output (Lampboard): S

Keyboard Input: I
Rotors Position: AAT
Plugboard Encryption: I
Wheel 3 Encryption: K
Wheel 2 Encryption: L
Wheel 1 Encryption: T
Reflector Encryption: Z
Wheel 1 Encryption: J
Wheel 2 Encryption: B
Wheel 3 Encryption: D
Plugboard Encryption: D
Output (Lampboard): D

Contoh 3

Konfigurasi

Reflector:	UKW-B	1 st Rotor:	I	2 nd Rotor:	II	3 rd Rotor:	III
Rotor	A	I	II	III			
Ring Setting	A	A	A	B			
Initial Position	A	E	E	V			

Cancel Apply Settings

Input-Output

Plain Text

ENIGMA

Cipher Text

TABQBN

Edit **Clear**

Plaintext:

ENIGMA

Ciphertext:

TABQBN

Show Encryption Steps **Clear** **Encrypt** **Decrypt**

Langkah

Input: E
Plugboard: E
Rotor 1: T
Rotor 2: J
Rotor 3: M
Reflector: O
Rotor 3: S
Rotor 2: D
Rotor 1: T
Output (Plugboard): T

Input: N
Plugboard: J
Rotor 1: P
Rotor 2: K
Rotor 3: S
Reflector: F
Rotor 3: E
Rotor 2: W
Rotor 1: B
Output (Plugboard): A

Input: I
Plugboard: I
Rotor 1: O
Rotor 2: I
Rotor 3: Y
Reflector: A
Rotor 3: V
Rotor 2: V
Rotor 1: A
Output (Plugboard): B

Keyboard Input: E
Rotors Position: BFW
Plugboard Encryption: E
Wheel 3 Encryption: T
Wheel 2 Encryption: J
Wheel 1 Encryption: M
Reflector Encryption: O
Wheel 1 Encryption: S
Wheel 2 Encryption: D
Wheel 3 Encryption: T
Plugboard Encryption: T
Output (Lampboard): T

Keyboard Input: N
Rotors Position: BFX
Plugboard Encryption: J
Wheel 3 Encryption: P
Wheel 2 Encryption: K
Wheel 1 Encryption: S
Reflector Encryption: F
Wheel 1 Encryption: E
Wheel 2 Encryption: W
Wheel 3 Encryption: B
Plugboard Encryption: A
Output (Lampboard): A

Keyboard Input: I
Rotors Position: BFY
Plugboard Encryption: I
Wheel 3 Encryption: O
Wheel 2 Encryption: I
Wheel 1 Encryption: Y
Reflector Encryption: A
Wheel 1 Encryption: V
Wheel 2 Encryption: V
Wheel 3 Encryption: A
Plugboard Encryption: B
Output (Lampboard): B

Keyboard Input: G
Rotors Position: BFZ
Plugboard Encryption: G
Wheel 3 Encryption: L
Wheel 2 Encryption: L
Wheel 1 Encryption: N
Reflector Encryption: K
Wheel 1 Encryption: D
Wheel 2 Encryption: A
Wheel 3 Encryption: Q
Plugboard Encryption: Q
Output (Lampboard): Q

Input: G
Plugboard: G
Rotor 1: L
Rotor 2: L
Rotor 3: N
Reflector: K
Rotor 3: D
Rotor 2: A
Rotor 1: Q
Output (Plugboard): Q

Input: M
Plugboard: M
Rotor 1: W
Rotor 2: E
Rotor 3: F
Reflector: S
Rotor 3: K
Rotor 2: P
Rotor 1: A
Output (Plugboard): B

Input: A
Plugboard: B
Rotor 1: D
Rotor 2: S
Rotor 3: O
Reflector: M
Rotor 3: J
Rotor 2: T
Rotor 1: J
Output (Plugboard): N

Keyboard Input: M
Rotors Position: BFA
Plugboard Encryption: M
Wheel 3 Encryption: W
Wheel 2 Encryption: E
Wheel 1 Encryption: F
Reflector Encryption: S
Wheel 1 Encryption: K
Wheel 2 Encryption: P
Wheel 3 Encryption: A
Plugboard Encryption: B
Output (Lampboard): B

Keyboard Input: A
Rotors Position: BFB
Plugboard Encryption: B
Wheel 3 Encryption: D
Wheel 2 Encryption: S
Wheel 1 Encryption: O
Reflector Encryption: M
Wheel 1 Encryption: J
Wheel 2 Encryption: T
Wheel 3 Encryption: J
Plugboard Encryption: N
Output (Lampboard): N