

LAPORAN TUGAS KECIL
SELEKSI LAB ILMU REKAYASA KOMPUTASI (IRK)
IMPLEMENTASI KRIPTOGRAFI “SEDERHANA++”
DALAM PENGENKRIPSAN PESAN



Disusun Oleh

Michael Leon Putra Widhi

(13521108)

Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
2023

A. Pengertian Enigma

Enigma adalah sebuah mesin enkripsi elektromekanis yang digunakan oleh Jerman Nazi selama Perang Dunia II. Mesin ini dirancang untuk mengamankan komunikasi militer Jerman agar tidak terbaca oleh pihak musuh. Enigma menggunakan konsep substitusi polialfabetik, yang berarti setiap huruf dalam teks yang dienkripsi digantikan oleh huruf lain berdasarkan pola yang rumit.

Mesin Enigma terdiri dari sebuah *keyboard* untuk memasukkan teks yang akan dienkripsi, lampu indikator yang menunjukkan huruf-huruf yang dienkripsi, serta sebuah rotor yang dapat diputar untuk mengubah substitusi huruf yang digunakan. Setiap kali sebuah huruf ditekan pada *keyboard*, sinyal listrik melalui rangkaian internal mesin Enigma dan mengalami serangkaian substitusi huruf berdasarkan konfigurasi rotor yang digunakan.

Enigma terdiri dari beberapa komponen utama yang bekerja secara bersama-sama untuk melakukan enkripsi dan dekripsi. Berikut adalah penjelasan mengenai komponen-komponen utama dari mesin Enigma.

1. *Keyboard* : *Keyboard* pada Enigma digunakan untuk memasukkan huruf-huruf yang akan dienkripsi atau didekripsi. Huruf-huruf ini mewakili teks yang ingin dikomunikasikan.
2. *Plugboard* : *Plugboard* adalah papan yang terdiri dari sejumlah konektor pasangan yang dapat dipasang dan dipasangkan. Pada awalnya, sinyal dari *keyboard* akan melewati *plugboard* dan mengalami substitusi huruf pertama. *Plugboard* memberikan tambahan substitusi awal sebelum masuk ke rotor and substitusi akhir setelah keluar dari rotor.
3. Rotor : Enigma menggunakan serangkaian rotor yang dapat diputar. Setiap rotor terdiri dari huruf-huruf yang mengelilingi sebuah poros. Ketika sebuah huruf dimasukkan melalui *keyboard*, sinyal melewati rotor-rotor ini dan mengalami substitusi huruf berdasarkan posisi rotor dan pengaturan internal yang kompleks. Setiap kali sebuah huruf dienkripsi, rotor-rotor ini berputar, mengubah substitusi huruf untuk huruf berikutnya.
4. *Reflector* : Setelah melewati rotor-rotor, sinyal akan memasuki *reflector*. *Reflector* adalah sebuah komponen khusus yang mengalirkan sinyal kembali melalui rotor-rotor yang sama, tetapi dalam arah yang berlawanan. Ini memberikan efek substitusi huruf

yang terbalik, sehingga memastikan bahwa mesin Enigma bersifat *reciprocating* (dalam artian, huruf A dienkripsi menjadi huruf B, dan huruf B dienkripsi menjadi huruf A).

5. *Lampboard* : *Lampboard* adalah sekelompok lampu indikator yang menunjukkan huruf-huruf yang dienkripsi. Ketika sebuah huruf dienkripsi, lampu yang sesuai akan menyala, memperlihatkan hasil enkripsi.

Selain komponen utama ini, Enigma juga memiliki mekanisme untuk mengatur posisi awal rotor (mulai dari posisi yang berbeda untuk setiap pesan) dan papan pengaturan untuk mengatur konfigurasi rotor yang digunakan. Dengan kombinasi yang berbeda dari rotor, pengaturan awal rotor, dan *plugboard*, Enigma dapat menghasilkan berbagai kemungkinan substitusi huruf yang rumit dan sulit diprediksi, membuatnya sulit untuk dipecahkan oleh pihak musuh.

B. Cara Kerja Enigma

Mesin Enigma memiliki cara kerja yang cukup kompleks. Berikut adalah penjelasan mengenai cara kerja Enigma secara umum.

1. Pengaturan Awal

Sebelum mengenkripsi atau mendekripsi pesan, pengguna mesin ini harus mengatur komponen-komponen mesin, termasuk rotor-rotor dan pengaturan awal rotor. Pengaturan ini memberikan konfigurasi awal substitusi huruf.

2. Masukan (*Input*)

Pengguna memasukkan huruf yang ingin dienkripsi melalui *keyboard*.

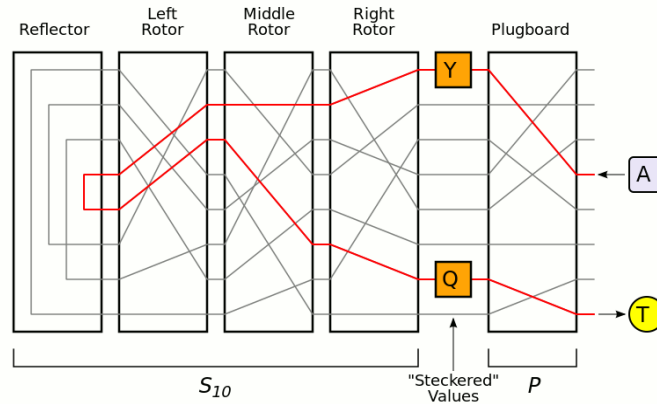
3. Plugboard Substitusi

Misalkan huruf yang dimasukkan adalah "A", maka huruf ini akan masuk ke dalam *plugboard* untuk kemudian dilakukan proses substitusi awal. Jika terdapat pasangan huruf yang dihubungkan di *plugboard*, misalnya $A \Leftrightarrow J$, maka huruf "A" dapat disubstitusi dengan huruf "J".

4. Melewati Rotor

Setelah melewati *plugboard*, sinyal huruf memasuki sekumpulan rotor yang telah dikonfigurasi sebelumnya. Rotor-rotor ini memiliki konfigurasi internal yang rumit

dan menggantikan huruf dengan huruf lain berdasarkan posisi rotor dan perputaran rotor yang terjadi. Berikut adalah salah satu contoh konfigurasi internal dan pemrosesannya.



Gambar 1. Contoh Pemrosesan Enigma pada Rotor dan *Plugboard*

Sumber : <https://github.com/voandy/enigma-machine>

5. *Reflector*

Setelah melewati sekumpulan rotor tersebut, sinyal huruf akan memasuki *reflector*. *Reflector* membalikkan arah sinyal, sehingga sinyal melewati rotor-rotor yang sama tetapi dalam arah yang berlawanan.

6. Kembali Melalui Rotor

Setelah melewati *reflector*, sinyal huruf kembali melalui sekumpulan rotor dalam arah yang berlawanan. Rotor-rotor tersebut akan menggantikan huruf dengan huruf lain berdasarkan konfigurasi internal dari masing-masing rotor.

7. *Plugboard* Substitusi Kedua

Selanjutnya, sinyal huruf akan kembali ke *plugboard*. Jika terdapat pasangan huruf yang dihubungkan di *plugboard*, maka substitusi terakhir akan terjadi.

8. Keluaran (*Output*)

Huruf terakhir yang dihasilkan akan menerangi lampu indikator yang sesuai di *lampboard* untuk menunjukkan huruf yang dienkripsi.

Setiap kali sebuah huruf dienkripsi, rotor-rotor tersebut akan berputar dan mengubah konfigurasi substitusi huruf. Kondisi ini yang membuat Enigma memiliki pola substitusi yang sangat kompleks dan sulit diprediksi sehingga memiliki tingkat keamanan yang tinggi. Lebih lanjut, proses dekripsi pesan dilakukan dengan prosedur yang sama, yaitu dengan

memberikan masukan teks yang akan didekripsi dan mengatur konfigurasi Enigma dengan pengaturan yang sesuai dengan proses enkripsi untuk menghasilkan huruf-huruf asli yang diinginkan.

Konfigurasi rotor yang diimplementasikan pada tugas ini adalah konfigurasi M3 menggunakan rotor I, II, dan III. *Entry disk* yang digunakan adalah ETW dengan menggunakan reflektor UKW-B. Berikut adalah penjelasan detail mengenai isi konfigurasi yang digunakan.

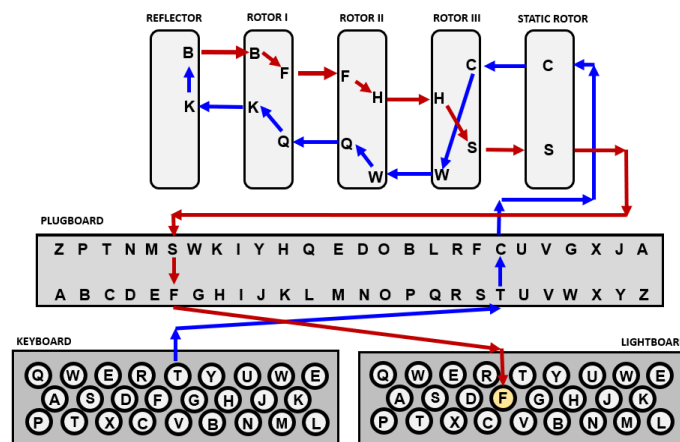
Tabel 1. Konfigurasi Mesin Enigma M3

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

Komponen	ABCDEFGHIJKLMNOPQRSTUVWXYZ	Titik putar
<i>Entry disk</i> ETW	ABCDEFGHIJKLMNOPQRSTUVWXYZ	-
Rotor I	EKMFLGDQVZNTOWYHXUSPAIBRCJ	Q
Rotor II	AJDKSIRUXBLHWTMCQGZNPYFVOE	E
Rotor III	BDFHJLCPRTXVZNIEUWGAQMUSQO	V
<i>Reflector</i> UKW-B	YRUHQSLDPXNGOKMIEBFZCWVJAT	-

C. Proses Enkripsi dengan Mesin Enigma

Berikut adalah contoh ilustrasi pemrosesan masukan dengan menggunakan Mesin Enigma.



Gambar 2. Skema Pemrosesan Mesin Enigma

Sumber :

<https://www.une.edu.au/info-for/visitors/museums/museum-of-antiquities/exhibitions-and-programs/codebreaker-challenge/enigma>

Misalkan terdapat sebuah mesin Enigma M3 yang menggunakan urutan rotor I, II, dan III, *Entry Disk* ETW, dan *Reflector* UKW-B dengan konfigurasi seperti yang telah dijelaskan pada Tabel 1. Digunakan pula sebuah *Plugboard* dengan pasangan kunci “HA RD” Karakter yang akan dienkripsi adalah “HELLO WORLD” dengan konfigurasi awal rotor berada pada posisi A-A-A untuk setiap rotor terkait. Proses enkripsi berlangsung sebagai berikut.

1. Mengatur konfigurasi mesin enigma sesuai ketentuan diatas.
2. Melakukan pemrosesan untuk setiap karakter. Untuk setiap karakter yang dimasukkan, lakukan hal berikut :
 - a. Putar rotor sesuai kondisi. Rotor paling kanan berputar untuk setiap karakter yang masuk. Ketika rotor paling kanan menyelesaikan satu putaran penuh, maka rotor di sebelah kirinya akan terpicu untuk berputar. Rotor tengah akan berputar satu kali untuk setiap putaran penuh rotor paling kanan. Demikian pula, rotor paling kiri berputar satu kali untuk setiap putaran penuh rotor tengah.
Pada iterasi pertama, posisi rotor menjadi A-A-B.
 - b. Gunakan *plugboard* untuk melakukan substitusi pertama. Karakter “H” dapat disubstitusi dengan “A” dengan menggunakan konfigurasi *plugboard* yang telah dijelaskan sebelumnya.
 - c. Lakukan penggantian substitusi pada setiap rotor, dimulai dari rotor paling kanan (dalam hal ini, rotor III). Karena rotor III sudah berputar, maka posisi A tidak lagi berada pada paling depan, melainkan Z karena arah putaran yang berlawanan arah jarum jam. Berikut proses pencocokannya

Rotor III

Normal : Z A BCDEFGHIJKLMNOPQRSTUVWXYZ

Rotor III : B D FHJLCPRTXVZNYEIWGAKMUSQO

Diperoleh hasil rotor III = $D - 1 = C$ (1 berasal dari jumlah rotasi rotor yang telah terjadi dengan modulo 26)

Rotor II

Normal : A B C DEFGHIJKLMNOPQRSTUVWXYZ

Rotor II : A J D KSIRUXBLHWTMCQGZNPYFVOE

Diperoleh hasil rotor II = $D - 0 = D$

Rotor I

Normal : ABC D EFGHIJKLMNOPQRSTUVWXYZ

Rotor I : EKM F LGDQVZNTOWYHXUSPAIBRCJ

Diperoleh hasil rotor I = F - 0 = **F**

- d. Setelah melalui semua rotor, maka sinyal akan tiba di *reflector*. Dengan menggunakan konfigurasi *reflector* yang telah dijelaskan sebelumnya, proses dilakukan sebagai berikut.

Reflector UKW-B

Normal : ABCDE F GHIJKLMNOPQRSTUVWXYZ

Reflector : YRUHQ S LDPXNGOKMIEBFZCWXVJAT

Diperoleh hasil *reflector* = **S**

- e. Setelah melalui *reflector*, maka sinyal akan kembali melewati sekumpulan rotor dengan arah yang berlawanan. Pemrosesan pun dilakukan dengan melakukan invers terhadap pencarian rotor. Lebih lengkap proses dilaksanakan sebagai berikut.

Rotor I

Normal : ABCDEFGHIJKLMNOPQR S TUVWXYZ

Rotor I : EKMFLGDQVZNTOWYHXU S PAIBRCJ

Diperoleh hasil rotor I = S - 0 = **S**

Rotor II

Normal : ABCD E FGHJKLMNOPQRSTUVWXYZ

Rotor II : AJDK S IRUXBLHWTMCQGZNPYFVOE

Diperoleh hasil rotor II = E - 0 = **E**

Rotor III

Normal : Z A BCDEFGHIJKLMNOPQRSTU VWXY

Rotor III : B D FHJLCPRTXVZNYEIWGAKMUSQO

Diperoleh hasil rotor III = A + 1 = **B** (Catatan, D diperoleh dari E - 1, kemudian hasil ditambahkan kembali dengan 1 untuk melakukan invers).

- f. Selanjutnya sinyal kembali tiba di *plugboard*, gunakan untuk melakukan substitusi terakhir. Karakter “B” tidak dapat disubstitusi dengan apapun dalam konfigurasi, maka karakter akan tetap dinyatakan dalam “B”.

- g. Proses karakter selesai dilaksanakan, tambahkan ke dalam *string* solusi.

Dengan menjalankan prosedur diatas, maka karakter “H” akan dikodekan menjadi “B”. Jika proses enkripsi dilanjutkan untuk setiap karakter, maka akan dihasilkan sebuah *string* dengan hasil “BLBRH HMUHX”.

D. Proses Dekripsi dengan Mesin Enigma

Proses dekripsi memiliki mekanisme yang sama dengan proses enkripsi. Hal yang perlu dilakukan untuk melakukan dekripsi adalah memastikan bahwa konfigurasi awal dari proses dekripsi sama dengan proses enkripsi untuk mendapatkan pesan yang ingin disampaikan. Dengan menggunakan konfigurasi yang sama seperti pada bagian sebelumnya, akan didekripsi sebuah *string* “BLBRH HMUHX”. Proses dekripsi berlangsung sebagai berikut.

1. Mengatur konfigurasi mesin enigma sesuai ketentuan pada bagian kondisi awal proses enkripsi.
2. Melakukan pemrosesan untuk setiap karakter. Untuk setiap karakter yang dimasukkan, lakukan hal berikut :
 - a. Putar rotor sesuai kondisi. Rotor paling kanan berputar untuk setiap karakter yang masuk. Ketika rotor paling kanan menyelesaikan satu putaran penuh, maka rotor di sebelah kirinya akan terpicu untuk berputar. Rotor tengah akan berputar satu kali untuk setiap putaran penuh rotor paling kanan. Demikian pula, rotor paling kiri berputar satu kali untuk setiap putaran penuh rotor tengah.
Pada iterasi pertama, posisi rotor menjadi A-A-B.
 - b. Gunakan *plugboard* untuk melakukan substitusi pertama. Karakter “B” tidak dapat disubstitusi dengan menggunakan konfigurasi *plugboard* yang telah dijelaskan sebelumnya, sehingga nilainya akan tetap “B”.
 - h. Lakukan penggantian substitusi pada setiap rotor, dimulai dari rotor paling kanan (dalam hal ini, rotor III). Karena rotor III sudah berputar, maka posisi A tidak lagi berada pada paling depan, melainkan Z karena arah putaran yang berlawanan arah jarum jam. Berikut proses pencocokannya

Rotor III

Normal : Z A B C D E F G H I J K L M N O P Q R S T U V W X Y

Rotor III : B D F H J L C P R T X V Z N Y E I W G A K M U S Q O

Diperoleh hasil rotor III = F - 1 = **E** (1 berasal dari jumlah rotasi rotor yang telah terjadi dengan modulo 26)

Rotor II

Normal : A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Rotor II : A J D K S I R U X B L H W T M C Q G Z N P Y F V O E

Diperoleh hasil rotor II = S - 0 = **S**

Rotor I

Normal : A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Rotor I : E K M F L G D Q V Z N T O W Y H X U S P A I B R C J

Diperoleh hasil rotor I = S - 0 = **S**

- i. Setelah melalui semua rotor, maka sinyal akan tiba di *reflector*. Dengan menggunakan konfigurasi *reflector* yang telah dijelaskan sebelumnya, proses dilakukan sebagai berikut.

Reflector UKW-B

Normal : A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Reflector : Y R U H Q S L D P X N G O K M I E B F Z C W V J A T

Diperoleh hasil *reflector* = **F**

- j. Setelah melalui *reflector*, maka sinyal akan kembali melewati sekumpulan rotor dengan arah yang berlawanan. Pemrosesan pun dilakukan dengan melakukan invers terhadap pencarian rotor. Lebih lengkap proses dilaksanakan sebagai berikut.

Rotor I

Normal : A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Rotor I : E K M F L G D Q V Z N T O W Y H X U S P A I B R C J

Diperoleh hasil rotor I = D - 0 = **D**

Rotor II

Normal : A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Rotor II : A J D K S I R U X B L H W T M C Q G Z N P Y F V O E

Diperoleh hasil rotor II = C - 0 = C

Rotor III

Normal : Z ABCDEFGHIJKLMNOPQRSTUVWXYZ

Rotor III : B DFHJLCPRTXVZNYEIWGAKMUSQO

Diperoleh hasil rotor III = Z + 1 = A (Catatan, B diperoleh dari C - 1, kemudian hasil ditambahkan kembali dengan 1 dan modulo untuk melakukan invers).

- k. Selanjutnya sinyal kembali tiba di *plugboard*, gunakan untuk melakukan substitusi terakhir. Karakter “A” dapat disubstitusi dengan “H”.
- l. Proses karakter selesai dilaksanakan, tambahkan ke dalam *string* solusi.

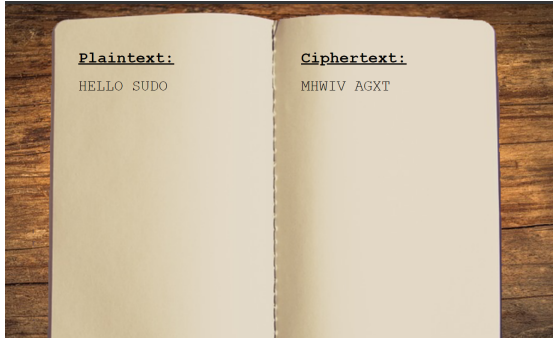
Dengan menjalankan prosedur diatas, maka karakter “B” akan dikodekan menjadi “H”. Jika proses enkripsi dilanjutkan untuk setiap karakter, maka akan dihasilkan sebuah *string* dengan hasil “HELLO WORLD”.

E. Pengujian dan Perbandingan Hasil

Proses pengujian dilakukan dengan berbagai mekanisme, mulai dari konfigurasi rotor, *plugboard* hingga panjang kalimat yang dienkripsi. Adapun proses perbandingan akan dilakukan dengan hasil yang diperoleh dari laman [berikut](#).

1. Pengujian konfigurasi rotor

Akan digunakan rotor I, II, dan III secara berurutan dengan posisi awal rotor adalah K-D-U sebagai pengujian pula terhadap *edge case* perputaran rotor yang saling berurutan. Dengan menggunakan kalimat “HELLO SUDO” diperoleh hasil sebagai berikut.

Hasil Program yang dibuat	Hasil Laman Pemandang
<div><p>Encryption</p><p>Please input the text to be encrypted</p><p>Plain Text</p><div>HELLO SUDO</div><div>Encrypt</div><p>Result <div>Save the process</div></p><div>MHWIV AGXT</div></div>	

Diperoleh bahwa keduanya mendapatkan hasil yang sama.

2. Pengujian *plugboard*

Akan digunakan rotor I, II, dan III secara berurutan dengan posisi awal rotor adalah B-X-Y dan *plugboard* dengan pasangan “AH EL OP US DB”.

Dengan menggunakan kalimat “HELLO SUDO” diperoleh hasil sebagai berikut.

Hasil Program yang dibuat	Hasil Laman Pembanding
<div>Encryption Please input the text to be encrypted Plain Text HELLO SUDO Encrypt Result Save the process MOAZQ NSBR</div>	 <p>The image shows an open notebook with two pages. The left page is labeled 'Plaintext:' and contains the text 'HELLO SUDO'. The right page is labeled 'Ciphertext:' and contains the text 'MOAZQ NSBR'.</p>

Diperoleh bahwa keduanya mendapatkan hasil yang sama.

3. Pengujian panjang kalimat

Akan digunakan rotor I, II, dan III secara berurutan dengan posisi awal rotor adalah A-F-T dan *plugboard* dengan pasangan “AB CD EF GH IJ”.

Dengan menggunakan kalimat “TUGAS INI BAGIAN DARI SELEKSI LAB IRK” diperoleh hasil sebagai berikut.

Hasil Program yang dibuat	Hasil Laman Pembanding
<div>Encryption Please input the text to be encrypted Plain Text TUGAS INI BAGIAN DARI SELEKSI LAB IRK Encrypt Result Save the process JBJPC TET XHRYBD TVLT MUSBLCK THH YHU</div>	 <p>The image shows an open notebook with two pages. The left page is labeled 'Plaintext:' and contains the text 'TUGAS INI BAGIAN DARI SELEKSI LAB IRK'. The right page is labeled 'Ciphertext:' and contains the text 'JBJPC TET XHRYBD TVLT MUSBLCK THH YHU'.</p>

Diperoleh bahwa keduanya mendapatkan hasil yang sama.

F. Daftar Pustaka dan Sumber Belajar

<https://www.cryptomuseum.com/crypto/enigma/index.htm>

<http://practicalcryptography.com/ciphers/mechanical-era/enigma/#javascript-example>

<https://www.codesandciphers.org.uk/enigma/>

<https://www.codesandciphers.org.uk/enigma/example1.htm>

<https://www.une.edu.au/info-for/visitors/museums/museum-of-antiquities/exhibitions-and-programs/codebreaker-challenge/enigma>

<https://www.101computing.net/enigma-machine-emulator/>