

LAPORAN TUGAS SELEKSI LAB IRK



Disusun Oleh:

Fahrian Afdholi

13521031

**SEKOLAH TEKNIK ELEKTRO DAN INFORMATIKA
INSTITUT TEKNOLOGI BANDUNG**

1. Apa itu enigma?

enigma adalah alat perang dari nazi yang berfungsi untuk menenkripsi maupun mendekripsi kode morse yang diberikan antar sesama tentara nazi dengan tujuan agar musuh tidak mengetahui kode yang dikirimkan jika mereka menyadap jaringan dari nazi. Biasanya enigma digunakan untuk mengkomunikasikan strategi perang yang sangat vital sehingga antar sesama tentara harus berkomunikasi tanpa ada yang mengetahui apa yang dikomunikasikan sehingga rencana yang dijalankan menjadi lancar.

2. Bagaimana cara enigma bekerja?

enigma sendiri memiliki beberapa bagian yang penting dalam menenkripsi ataupun mendekripsi kode yang diberikan di antaranya:

- a. Keyboard
- b. Plugboard
- c. Rotor
- d. Reflector

Cara kerja dari enigma itu sendiri adalah dengan menginput huruf pada keyboard enigma akan mengirimkan sinyal dari keyboard menuju plugboard, pada plugboard akan dicek dari plugboard bagian kanan ke bagian kiri yang dimana plugboard tersebut bisa di kustom sesuai hati dengan tujuan untuk menukar huruf seperti contoh pada 26 huruf saya ingin menukar huruf A dengan Z, jika sinyal memberikan huruf A maka akan mengeluarkan output huruf Z. Setelah melewati plugboard sinyal akan melewati 3 rotor yang dimana per-rotor memiliki kode yang berbeda beda untuk mengacak acak sinyal. Setelah melewati rotor sinyal keluaran akan melewati reflector yang dimana berfungsi untuk memantulkan sinyal dan mengeluarkannya. Setelah reflektor selesai maka sinyal akan kembali ke 3 rotor lalu ke plugboard dan akhirnya akan menampilkan output yang sudah dienkripsi.

Pada rotor enigma setiap kita memasukkan satu huruf, rotor ketiga akan terus berputar agar kode enkripsi akan semakin acak. Rotor ke 2 akan berputar ketika rotor 3 sudah mencapai notch begitupun dengan rotor ke 1.

3. Cara kerja enkripsi enigma step by step

- a. Yang pertama enigma akan meminta input dari keyboard
- b. Setelah menerima input dari keyboard, keyboard akan mengirimkan sinyal ke plugboard, plugboard akan mengecek apakah pengguna telah mengubah

susunan huruf atau tidak , jika iya akan mengeluarkan output sesuai dengan huruf yang ditukar

- c. Dengan menerima sinyal dari plugboard. Rotor akan mengacak lagi sinyal tersebut dengan cara, anggaplah sinyal adalah sebuah index semisal sinyal memiliki index ke 4 maka rotor bagian kanan akan menunjuk huruf pada index ke 4 semisal huruf G, huruf G pada rotor bagian kanan akan dicari huruf yang sama ke bagian sebelah kiri dan akan mengeluarkan input dengan index yang ada pada rotor bagian kiri. Proses ini akan diulang sebanyak 3 kali pada input pertama sebelum kerefrlektor, setiap rotor memiliki kode acak yang berbeda beda di bagian kanannya sehingga output yang diberikan juga acak.
- d. Setelah melewati ketiga rotor maka akan dilanjutkan dengan reflector. Hampir mirip dengan cara kerja rotor tetapi reflector hanya memantulkan sinyalnya saja, semisal output pada rotor adalah 3 dimana misalkan bagian kanan reflektor pada index 3 adalah K maka akan dicek pada bagian sebelah kiri index ke berapa yang memiliki huruf K lalu akan mengambil output index K sebelah kiri ke sebelah kanan.
- e. Setelah melewati reflector sinyal akan dikirimkan melalui ketiga rotor lalu ke plugboard dan akhirnya akan mendapatkan huruf yang sudah dienkripsi.

4. Cara kerja dekripsi step by step

Pada dasarnya sama saja seperti enkripsi tetapi rotor harus dikembalikan pada posisi awal yaitu AAA dan plugboard harus sama dengan enigma yang menkripsi kode. Jika sudah melakukan kedua hal tersebut maka kita hanya tinggal menginput kode enkripsi yang diberikan dan akan otomatis di dekripsi.

5. Screenshot

hasil akan berbeda pada huruf ke 4 karena saya menggunakan notch D pada rotor ke 1

enkripsi:

Enigma

?

×

Clear All

Encrypt

Decrypt

plain text

AAAA

chipper text

BDZX

Q

W

E

R

T

Y

U

I

O

P

A

S

D

F

G

H

J

K

L

Z

X

C

V

B

N

M

Plugboard:

Example: A

to

Example: B

Post

plugboard list:

<u>Plaintext:</u>	<u>Ciphertext:</u>
AAAA	BDZG
<u>Show Encryption Steps</u>	<u>Clear</u> <u>Encrypt</u> <u>Decrypt</u>

dekripsi:

Enigma

?

×

Clear All

Encrypt

Decrypt

plain text

BDZX

chipper text

AAAA

Q

W

E

R

T

Y

U

I

O

P

A

S

D

F

G

H

J

K

L

Z

X

C

V

B

N

M

Plugboard:

Example: A

to

Example: B

Post

plugboard list:

Plaintext:

BDZG

Ciphertext:

AAAA

Show Encryption Steps

Clear

Encrypt

Decrypt