

LAPORAN TUGAS SELEKSI IRK  
MESIN ENIGMA



Disusun Oleh:

Nama : Sulthan Dzaky Alfaro

NIM : 13521159

## **APA ITU ENIGMA**

Enigma merupakan sebuah mesin kriptografi yang digunakan pada saat perang dunia ke-2 oleh NAZI dalam pengiriman pesan. Kriptografi sendiri berasal dari bahasa Yunani, kriptos dan graphia. Kriptos berarti menyembunyikan dan graphia berarti tulisan. Sehingga kriptografi sendiri merupakan suatu praktik menyembunyikan suatu data dengan cara mengubah bentuk suatu data menjadi berbeda dengan data aslinya. Kriptografi ini bertujuan untuk mengamankan isi data atau menjaga kerahasiaan informasi dari orang yang tidak boleh mengetahui isi dari data tersebut. Oleh karena itu tidak sembarang orang dapat mengetahui suatu data, karena hanya orang-orang tertentu yang dapat mengetahuinya. Enigma dibuat oleh insinyur Jerman bernama Arthur Scherbius pada tahun 1920-an.

Enigma merupakan alat penyandi terenkripsi yang paling kompleks pada masanya. Karena pada mesin ini memiliki komponen yang cukup rumit dan memiliki kemungkinan enkripsi yang sangat banyak. Sehingga untuk memecahkan kode dari hasil enkripsi mesin ini sangatlah sulit dan banyak kemungkinan yang harus dicoba. Pada masanya, ada beberapa orang pada masanya dapat memecahkan kode enigma sehingga dapat menguraikan pesan rahasia yang benar. Orang-orang tersebut adalah Alan Turing dan kriptanalisis di Bletchley Park. Mereka juga berjasa dalam mempersingkat perang di Eropa 2 hingga 4 tahun.

### **Cara Kerja Mesin Enigma**

Enigma merupakan salah satu mesin kriptografi yang sangat kompleks dan memiliki kemungkinan yang sangat banyak. Mesin ini terdiri dari beberapa komponen untuk menenkripsikan dan mendekripsikan sebuah teks. Adapun komponen-komponen pada mesin enigma ini, antara lain:

#### **1. Tombol dan Lampu Indikator**

Enigma memiliki tombol dan lampu indikator yang mewakili abjad, biasanya terdiri dari 26 tombol. Saat sebuah tombol ditekan, lampu pada mesin akan menyala untuk menampilkan hasil enkripsi dari huruf yang ditekan.

#### **2. Rotor**

Mesin ini memiliki 3 hingga 5 jenis rotor yang merupakan piringan/roda dengan huruf-huruf pada tepinya. Setiap rotor memiliki pengaturan awal yang dapat diubah, yang menentukan urutan huruf yang terhubung ke jalur kelistrikan di dalam mesin. Rotor ini akan berputar seiring ditekannya tombol pada mesin. Rotor akan bergerak sesuai dengan notch pada tiap rotor. Notch ini merupakan sebuah acuan untuk menggerakkan rotor, jadi apabila suatu rotor melewati notch tersebut, rotor disebelahnya baru akan bergerak 1 langkah.

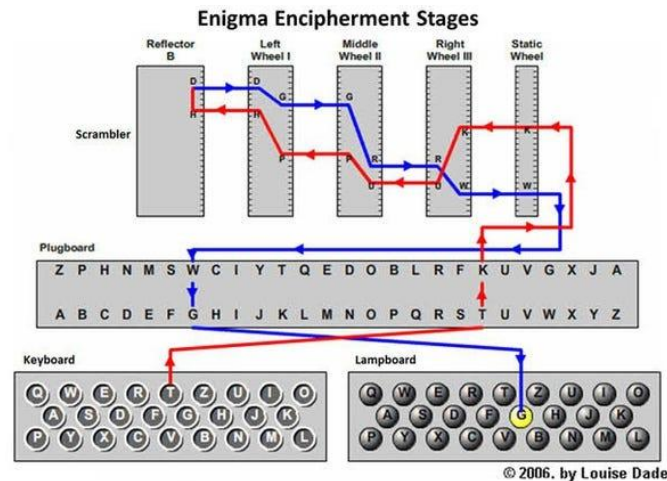
#### **3. Plugboard**

Plugboard merupakan bagian dari mesin enigma yang menggunakan kabel untuk menghubungkan pasangan huruf. Plugboard ini memberikan pengacakan tambahan untuk hasil enkripsi sebuah huruf.

#### 4. Reflektor

Komponen ini berfungsi untuk mengarahkan sinyal listrik kembali ke rotor-rotor tetapi dalam arah yang berlawanan setelah melewati rotor-rotor

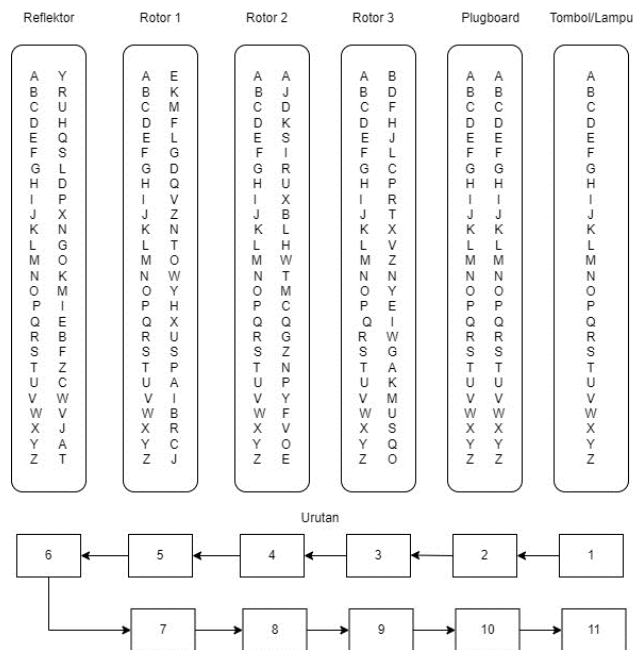
Setelah mengetahui bagian bagian dari enigma ini, berikut tahapan/alur dari cara kerja mesin enigma:



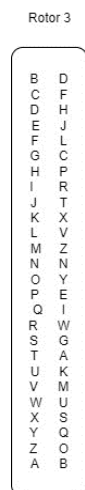
1. Pada saat tombol ditekan, sinyal listrik akan melewati tombol yang ditekan dan masuk ke plugboard.
2. Setelah melewati plugboard, sinyal akan masuk ke rotor-rotor. Setiap menekan sebuah tombol pada mesin, rotor rotor ini akan bergerak berputar.
3. Setelah melewati rotor rotor tersebut, sinyal listrik akan masuk ke dalam reflektor. Lalu reflektor ini akan memantulkan sinyal kembali ke rotor-rotor lagi tetapi dengan arah yang berlawanan.
4. Setelah melalui reflektor, sinyal listrik akan melewati rotor-rotor lagi.
5. Akhirnya, sinyal meninggalkan rotor-rotor terakhir dan masuk ke dalam plugboard. Jika ada plugboard yang terpasang, maka sinyal akan melalui huruf yang tersambung dari hasil terakhir rotor. Setelah itu, sinyal akan menuju lampu indikator yang sesuai dengan hasil akhir enkripsi.

### Enkripsi dan Dekripsi Enigma

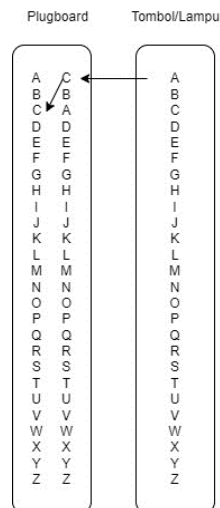
Untuk urutan enkripsi dari sebuah mesin enkripsi dan komponen pada mesin dapat dilihat dari gambar dibawah ini. Untuk huruf yang ada dibagian kiri rotor merepresentasikan huruf pada tampilan rotor (lebih tepatnya kiri paling atas yang sebagai tampilan pada mesin), dan yang kanan adalah yang sejajar dengan tampilan rotor. Kedua huruf yang sejajar tersebut tidak saling berhubungan. Yang saling berhubungan (sebagai jalur sinyal nanti) adalah huruf yang sama, antara huruf yang kiri dengan huruf yang kanan. Jadi misal huruf “A” pada bagian kiri terhubung dengan huruf “A” pada bagian kanan.



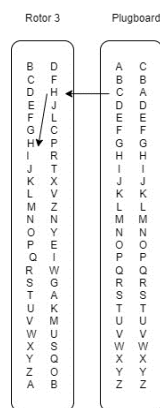
Sebagai contoh, kita misalkan untuk huruf pertama yang ditekan adalah “A”. Maka setelah “A” ditekan, rotor 3 akan bergerak keatas 1 kali.



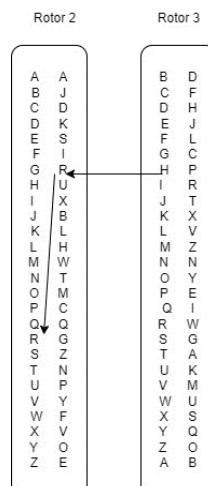
Lalu, apabila tombol ditekan, sinyal akan masuk ke dalam plugboard. Apabila ada yang terhubung dengan huruf lain, maka plugboard akan mengubah huruf yang ditekan menjadi huruf yang terhubung tersebut. Sebagai contoh “A” terhubung dengan “C” sehingga apabila kita menekan “A” akan menjadi “C” saat melewati plugboard.



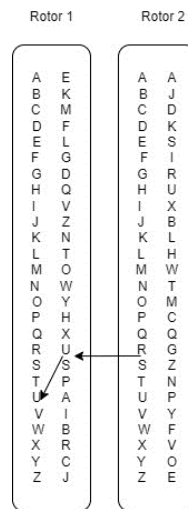
Lalu, kita lihat huruf disebelah huruf plugboard pada rotor disebelahnya, yaitu rotor 3. Huruf yang ada di plugboard sekarang adalah “C”. Kita lihat huruf apa disebelah huruf “C” plugboard pada rotor 3. Lalu kita jadikan huruf tersebut untuk rotor 3.



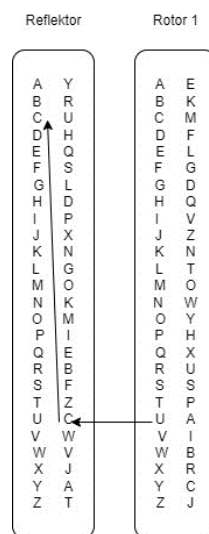
Lalu, kita lihat huruf disebelah rotor 3 (yaitu rotor 2) yang sejajar dengan huruf pada rotor 3. Pada rotor 3, huruf pada rotor 3 pada saat ini adalah “H”. Lalu kita lihat huruf yang sejajar pada rotor 2 dengan huruf “H” rotor 3. Huruf itu menjadi huruf rotor 2 saat ini.



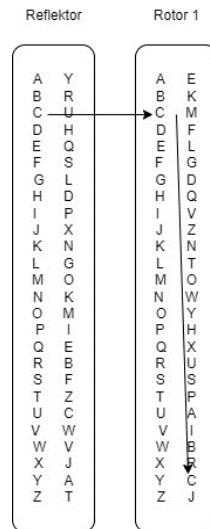
Lanjut, sama seperti sebelumnya, lihat huruf yang sejajar pada rotor 1 dengan huruf rotor 2. Pada rotor 2, huruf pada rotor 2 pada saat ini adalah “R”. Lalu kita lihat yang sejajar dengan huruf “R” rotor 2 pada rotor 1. Huruf itu menjadi huruf rotor 1 untuk saat ini.



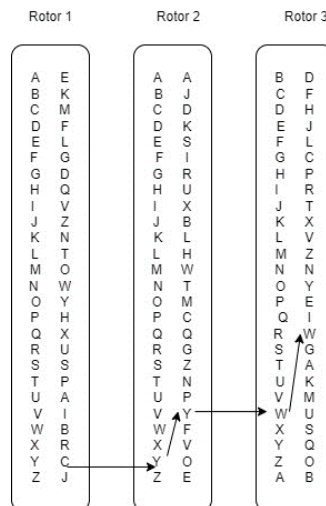
Lalu, sama seperti sebelumnya, lihat huruf yang sejajar pada reflector dengan huruf rotor 1. Pada rotor 1, huruf pada rotor 1 pada saat ini adalah “U”. Lalu kita lihat yang sejajar dengan huruf “U” rotor 1 pada reflector. Huruf itu menjadi huruf pada reflector.



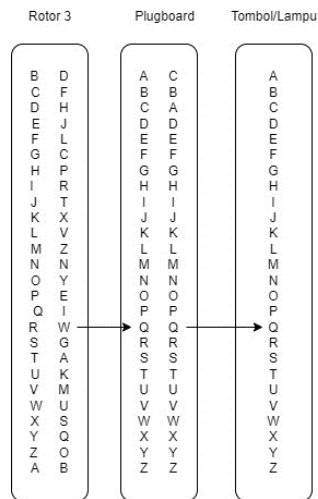
Lalu, sinyal yang masuk ke dalam reflector, akan membalikkan arah sinyal sehingga sinyal akan balik lagi ke rotor 1. Sama seperti sebelumnya, kita lihat huruf pada reflector saat ini yang sejajar dengan huruf pada rotor 1. Pada reflector, huruf pada reflector adalah “C”. Maka kita lihat huruf yang sejajar “C” reflector pada rotor 1. Huruf itu akan menjadi huruf rotor 1 saat ini.



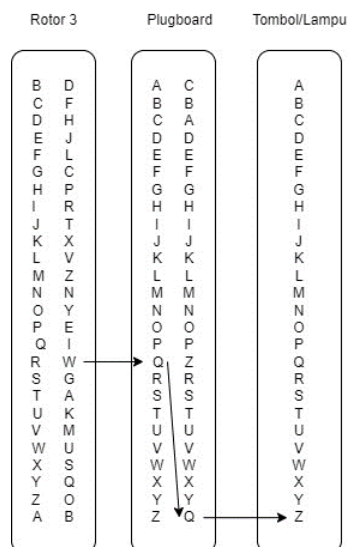
Begitu seterusnya sampai rotor 3.



Setelah mendapatkan huruf terakhir, yaitu huruf pada rotor 3, kita lihat huruf disamping rotor 3 (yaitu pada plugboard) yang sejajar dengan huruf pada rotor 3. Huruf tersebut dijadikan hasil enkripsi apabila tidak ada yang terhubung pada plugboard. Pada kasus ini huruf pada rotor 3 adalah “W”. Huruf yang sejajar dengan huruf “W” (pada rotor 3) pada plugboard adalah “Q”, sehingga hasil enkripsi adalah “Q”.

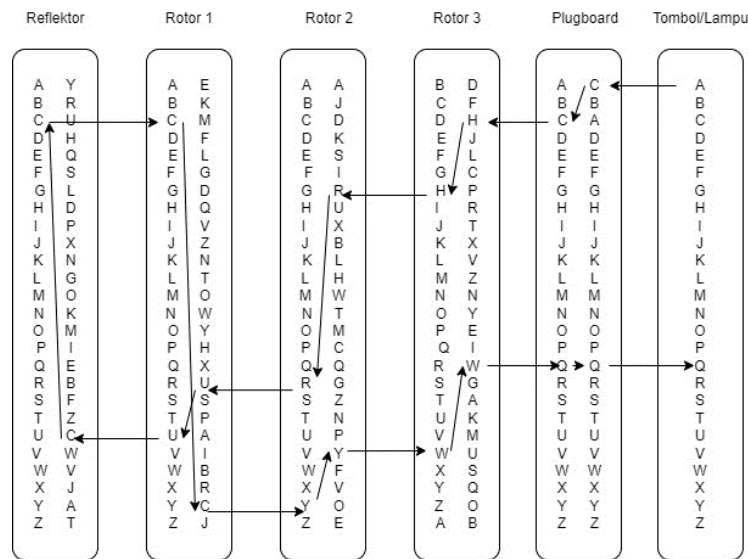


Apabila huruf yang sejajar tersebut terhubung dengan huruf lain pada plugboard, maka huruf yang sejajar tersebut akan menjadi huruf yang terhubung pada plugboard sebagai hasil enkripsi. Misal (hanya contoh) “Q” terhubung dengan “Z”, maka hasil enkripsi menjadi “Z”.



Sehingga didapat apabila input “A” dengan plugboard adalah “A” dan “C” adalah “Q”. Berikut adalah gabungan dari tahapan enkripsi dari mesin enigma.





Begitu seterusnya untuk huruf berikutnya. Untuk rotor 2 dan rotor 1, bergerak apabila ada notch yang telah melewati batasan pada rotor disebelahnya. Misal notch rotor 3 adalah “V”. Maka apabila “V” ini sudah melewati batas (batas ini merupakan baris paling atas pada gambar/tampilan pada mesin) maka rotor 2 baru bergerak 1 langkah. Begitu juga dengan rotor 1, apabila notch rotor 2 telah melewati batas, maka rotor 1 akan bergerak 1 langkah

Untuk dekripsi, cara kerja sama seperti enkripsi. Karena hasil dari enkripsi suatu teks, apabila ditekan kembali sesuai konfigurasi rotor enkripsinya, maka akan dihasilkan kembali teks seperti awal(dekripsi).

## Screenshot Hasil Program

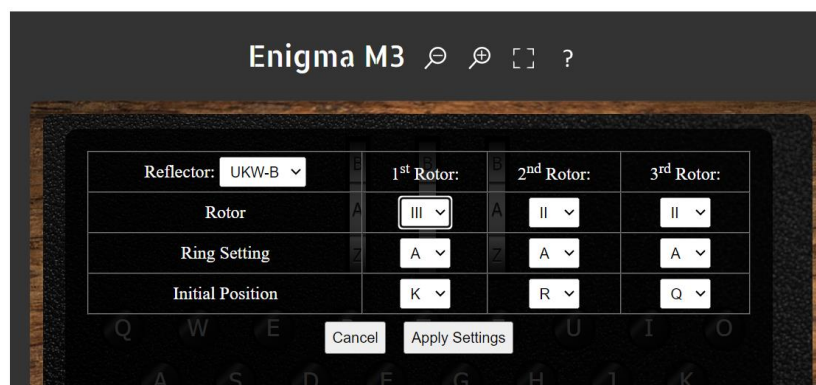
### 1. Test 1

Rotor 1 = III

Rotor 2 = II

Rotor 3 = II

Initial Position = KRQ



<u>Plaintext:</u>	<u>Ciphertext:</u>
MANTA PJIWA CUUUY	FPEXP OKQLB ICESX
UDAHB ISAAA	LFGJ VMHVB

[Show Encryption Steps](#)
[Clear](#)
[Encrypt](#)
[Decrypt](#)

## Internet

Input:

Plugin:

Alan Turing Plugin

Enkripsi/Dekripsi

Alan Turing

Input:

FPEXP OKQLB ICESX LFGJ VMHVB

Output:

MANTA PJIWA CUUUY UDAHB ISAAA

Left

III

K

Middle

II

S

Right

II

P

Rincian

Huruf input: F  
Current Rotor Position: KRR  
Rotor 3: O  
Rotor 2: R  
Rotor 1: T  
Reflector: Z  
Rotor 1: U  
Rotor 2: T  
Rotor 3: M  
Huruf output: M

Huruf input: P  
Current Rotor Position: KRS  
Rotor 3: C  
Rotor 2: W  
Rotor 1: S  
Reflector: F  
Rotor 1: X  
Rotor 2: H  
Rotor 3: A  
Huruf output: A

Huruf input: F  
Current Rotor Position: KRT  
Rotor 3: V  
Rotor 2: F  
Rotor 1: U  
Reflector: C  
Rotor 1: L  
Rotor 2: Y

## Hasil Program

### 2. Test 2

Rotor 1 = I

Rotor 2 = III

Rotor 3 = II

Initial Position = STZ

Reflector: UKW-B ▾	1 <sup>st</sup> Rotor: A ▾	2 <sup>nd</sup> Rotor: Z ▾	3 <sup>rd</sup> Rotor: I ▾
Rotor	I ▾	III ▾	II ▾
Ring Setting	A ▾	A ▾	A ▾
Initial Position	S ▾	T ▾	Z ▾
Cancel		Apply Settings	

<b><u>Plaintext:</u></b>	<b><u>Ciphertext:</u></b>
LETSG OOOOO MUANT	SZVLY UYCEV IHMPX
APJIW AMEEN	HILOD HHIUF
<a href="#">Show Encryption Steps</a>	<a href="#">Clear</a> <a href="#">Encrypt</a> <a href="#">Decrypt</a>

Internet

Input: SZVLY UYCEV IHMPX HILOD HHIUF	<b>Rincian:</b> Huruf input: S Current Rotor Position: STA Rotor 3: Z Rotor 2: N Rotor 1: O Reflector: M Rotor 1: I Rotor 2: H Rotor 3: L Huruf output: L  Huruf input: Z Current Rotor Position: STB Rotor 3: Z Rotor 2: N Rotor 1: O Reflector: M Rotor 1: I Rotor 2: H Rotor 3: E Huruf output: E  Huruf input: V Current Rotor Position: STC Rotor 3: T Rotor 2: G Rotor 1: K Reflector: N Rotor 1: L Rotor 2: W	
Plugin: Alan Turing Plugin Enkripsi/Dekripsi Alan Turing		
Input: SZVLY UYCEV IHMPX HILOD HHIUF		
Output: LETSG OOOOO MUANT APJIW AMEEN		
Left: I ▾ S ▾	Middle: III ▾ U ▾	Right: II ▾ Y ▾

Hasil Program

- Test 3
  - Rotor 1 = III
  - Rotor 2 = II
  - Rotor 3 = I

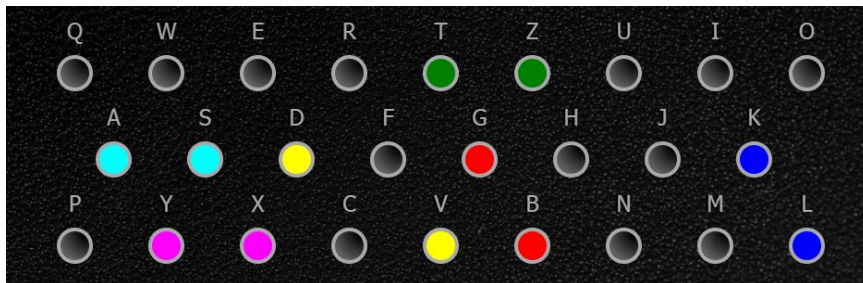
Initial Position = ZZZ

Plugboard = B-G V-D L-K Z-T Y-X S-A

**Enigma M3** ☹ ☺ ☐ ?

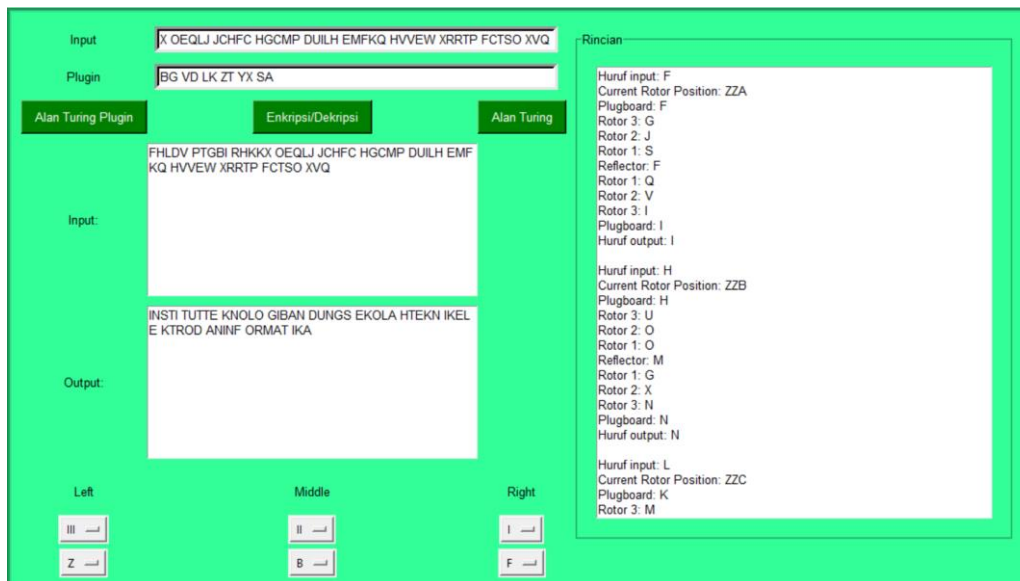
Reflector:	1 <sup>st</sup> Rotor:	2 <sup>nd</sup> Rotor:	3 <sup>rd</sup> Rotor:
UKW-B ▾	III ▾	II ▾	I ▾
Rotor	S	Y	
Ring Setting	A ▾	A ▾	A ▾
Initial Position	Z ▾	Z ▾	Z ▾

Cancel   Apply Settings



<u>Plaintext:</u>	<u>Ciphertext:</u>
INSTI TUTTE KNOLO	FHLDV PTGBI RHKKX
GIBAN DUNGS EKOLA	OEQLJ JCHFC HGCMP
HTEKN IKELE KTROD	DUILH EMFKQ HVVEW
ANINF ORMAT IKA	XR RTP FCTSO XVQ

Internet



Hasil Program

#### 4. Test 4

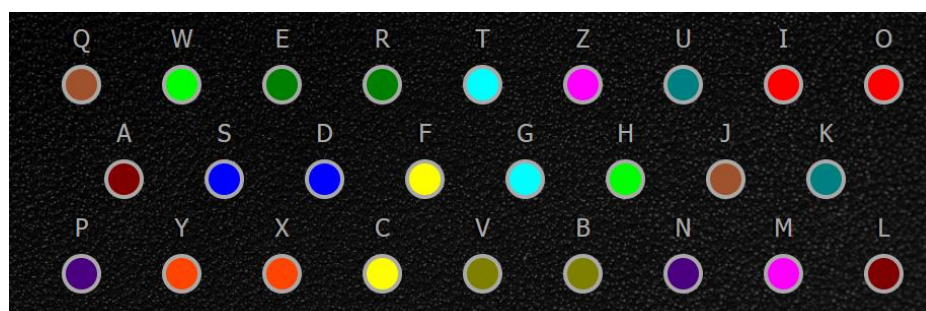
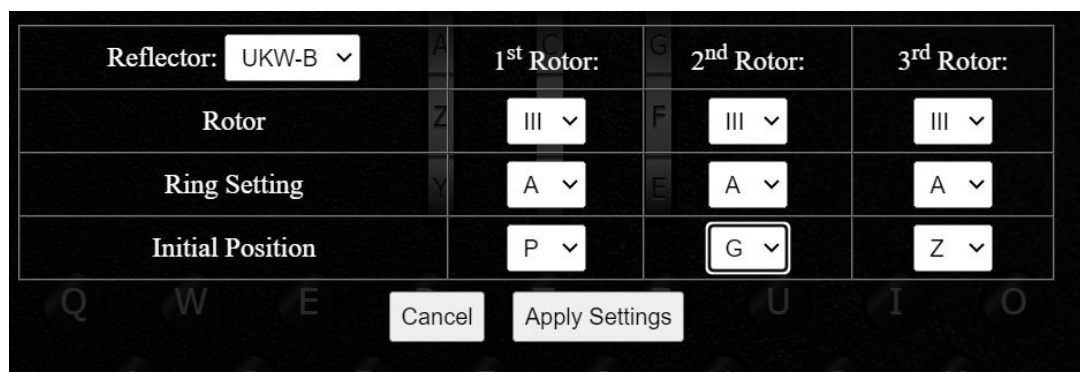
Rotor 1 = III

Rotor 2 = III

Rotor 3 = III

Initial Position = PGZ

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



<p><b><u>Plaintext:</u></b></p> <p>BANDU NGIBU KOTAJ          AWABA RATDE NGANB          AHASA DAERA HSUND          ADANS UHUNY ADING          INBAN GET</p>	<p><b><u>Ciphertext:</u></b></p> <p>HCYFK LVT VH VDFTQ          NPEML UIICT ZUUEG          HWUYP KQGGP GEVGB          DPTTA KGGXB GKZMX          TORQE EAD</p>
<p><b><u>Show Encryption Steps</u></b></p>	<p><b><u>Clear</u></b>   <b><u>Encrypt</u></b>   <b><u>Decrypt</u></b></p>

Internet

Input:

Plugin:

Input:

HCYFK LVT VH VDFTQ NPEML UIICT ZUUEG HWUYP KQ  
 GGP GEVGB DPTTA KGGXB GKZMX TORQE EAD

Output:

BANDU NGIBU KOTAJ AWABA RATDE NGANB AHASA D  
 AERA HSUND ADANS UHUNY ADING INBAN GET

Rincian

Huruf input: H  
 Current Rotor Position: PGA  
 Plugboard: W  
 Rotor 3: U  
 Rotor 2: V  
 Rotor 1: I  
 Reflector: P  
 Rotor 1: A  
 Rotor 2: M  
 Rotor 3: V  
 Plugboard: B  
 Huruf output: B

Huruf input: C  
 Current Rotor Position: PGB  
 Plugboard: F  
 Rotor 3: B  
 Rotor 2: J  
 Rotor 1: B  
 Reflector: R  
 Rotor 1: D  
 Rotor 2: Y  
 Rotor 3: L  
 Plugboard: A  
 Huruf output: A

Huruf input: Y  
 Current Rotor Position: PGC  
 Plugboard: X  
 Rotor 3: M

Left

III

P

Middle

III

I

Right

III

P

Hasil Program