Laporan
Tugas Kecil IFXXXX Lab Ilmu Rekayasa Komputasi

Semester Liburan Tahun 2022/2023

Implementasi Kriptografi “Sederhana++” Dalam Pengenkripsian Pesan

oleh

Kenneth Ezekiel Suprantoni 13521089

Sekolah Teknik Elektro dan Informatika

Institut Teknologi Bandung

Bandung

2022

Daftar Isi

Daftar Isi **2**

BAB I
Dasar Teori **1**

1.1. Apa Itu Mesin Enigma 1

1.2 Cara Kerja Mesin Enigma 1

BAB II
Contoh Penggunaan **1**

2.1. Enkripsi 1

2.2. Dekripsi 2

BAB III
Hasil Eksperimen **1**

BAB I

Dasar Teori

1.1. Apa Itu Mesin Enigma

Mesin Enigma adalah sebuah mesin kriptografi elektromekanis yang revolusioner pada zamannya, yang digunakan oleh Jerman Nazi pada Perang Dunia ke-2 untuk mengirim pesan secara rahasia. Pada dasarnya, mesin enigma menggunakan prinsip kriptografi transposisi dan juga substitusi untuk mengubah huruf sebenarnya (*plaintext*) menjadi huruf yang di-enkripsi (*ciphertext*). Mesin enigma itu sendiri memiliki beberapa versi, yang meningkatkan keamanan-nya seiring versinya berubah. Secara keseluruhan, mesin enigma memiliki sebuah *rotor* elektromekanis yang akan berputar setiap ada listrik yang mengalir. Listrik yang mengalir tersebut bersumber dari huruf pada *keyboard* dari mesin yang ditekan.

Mesin Enigma juga adalah sebuah alat kriptografi simetris, yang berarti saat kita memberikan masukan hasil dari enkripsi (*ciphertext*) dengan *setting* mesin yang sama, maka akan muncul teks yang asli atau sebenarnya (*plaintext*).

Singkatnya, sinyal listrik mulai mengalir saat ada sebuah huruf ditekan pada *keyboard*, lalu melewati *plugboard*, setelah itu melalui *rotor*. Setelah sinyal listrik melewati *rotor-rotor*, sinyal akan masuk ke *reflektor*. *Reflektor* merupakan komponen penting dalam Enigma yang menghasilkan substitusi pada huruf sesuai dengan pasangan huruf tersebut. Sinyal yang masuk ke *reflektor* akan dipantulkan kembali melalui *rotor-rotor* dengan arah yang berlawanan.

Setelah melewati reflektor, sinyal listrik kembali melewati *rotor-rotor* dalam urutan terbalik. Masing-masing *rotor* mengubah sinyal lagi, tetapi kali ini dalam arah yang berlawanan dari yang sebelumnya. Akhirnya, sinyal listrik mencapai *lampboard*. Pada *lampboard*, setiap huruf yang mewakili enkripsi masing-masing dinyalakan oleh sinyal listrik yang keluar dari *rotor* terakhir, lalu masuk ke *plugboard*. Akhirnya, Huruf enkripsi ditampilkan sebagai lampu yang menyala.

1.2 Cara Kerja Mesin Enigma

Cara kerja enkripsi dan dekripsi mesin enigma adalah sebagai berikut:

1. Pengguna menekan huruf yang ada pada *keyboard*
2. Listrik akan mengalir dari *keyboard* sesuai dengan huruf yang ditekan ke *plugboard*
3. Di *plugboard*, huruf yang terikat akan disubstitusikan dengan pasangannya
4. Listrik akan mengalir dari *plugboard* ke *rotor* pertama dari 3, kanan, tengah, dan kiri
5. Di *rotor*, Huruf akan ditranslasikan sesuai *mapping* pada *rotor*, dan *rotor* akan berputar. Jika *rotor* sudah mengenai sebuah huruf, maka *rotor* akan memutar rotor sebelah kiri-nya (contoh: saat *rotor* kanan sudah berada pada huruf X (atau bergeser 26 kali), maka *rotor* tengah akan berputar)
6. Lebih lengkap yang terjadi di dalam *rotor* adalah:
    a. Saat *rotor* berputar, huruf asli yang masuk akan berubah maju sesuai *offset* yang diberikan, dimana *offset* merupakan jumlah putaran yang sudah dilakukan sejauh ini
    b. Huruf yang sudah diubah akan di *mapping* sesuai pasangan pada *rotor*
    c. Hasil dari *mapping* tersebut kemudian akan masuk ke *rotor* berikutnya, tetapi akan berubah mundur juga sesuai *offset* yang ada. Hal ini dikarenakan *metal contact* dari *rotor* berikutnya akan menerima huruf yang di belakang huruf yang diberikan dari *rotor* sebelumnya sejauh *offset* karena perputaran *rotor* tersebut
7. Setelah melewati ketiga *rotor* (kanan, tengah, kiri), sinyal listrik yang berkorespondensi dengan huruf akan sampai pada *reflektor*, yang akan “memantulkan” sinyal listrik. Disini, terjadi substitusi huruf kembali, sesuai pasangan atau *mapping* yang terdapat pada reflektor
8. Listrik hasil “pantulan” *reflektor* akan kembali masuk pada *rotor*, dengan urutan kiri-tengah-kanan dan dilakukan *mapping* kembali dari arah yang kebalikan.
9. Setelah melewati *rotor*, listrik akan mengalir kembali melalui *plugboard* yang akan mensubstitusikan huruf yang terikat dengan pasangannya
10. Hasil substitusi kemudian ditampilkan pada *lampboard*

Sehingga jika dirangkum, mesin enigma bekerja menggunakan prinsip enkripsi substitusi dan transposisi, dimana representasi huruf akan diwakili oleh aliran listrik

pada kabel yang berkoresponden dengan huruf tersebut. Aliran listrik dimulai pada keyboard, lalu substitusi pertama dilakukan pada plugboard, yang akan dilanjutkan dengan substitusi berturut-turut dengan rotor, dan juga transposisi rotor, lalu dilanjutkan dengan substitusi huruf dengan reflektor, diteruskan ke rotor pada sisi kebalikannya, dan terakhir substitusi oleh plugboard sebelum akhirnya muncul hasilnya pada lampboard.

BAB II

Contoh Penggunaan

2.1. Enkripsi

Contoh enkripsi *step-by-step*:

Enkripsi teks AB, dengan initial position rotor pada P dan ring setting rotor pada A

1. Listrik akan keluar dari kabel yang berkoresponden dengan huruf A
2. Listrik akan masuk ke plugboard dan mensubstitusi A dengan A
3. Listrik akan keluar dari plugboard
4. Rotor I akan berputar satu kali
5. Listrik akan masuk pada rotor I, yang akan mensubstitusi A dengan H (A masuk sebagai Q, Q disubstitusi sebagai X, X kemudian keluar sebagai H), belum ada perputaran rotor II dan III
6. Listrik akan masuk pada rotor II yang akan mensubstitusi H dengan U
7. Listrik akan masuk pada rotor III yang akan mensubstitusi U dengan K
8. Listrik akan masuk ke reflektor dan akan merubah K menjadi N
9. Listrik akan masuk kembali pada sisi kebalikan rotor III dan mensubstitusi N menjadi N
10. Listrik akan masuk kembali pada sisi kebalikan rotor II dan mensubstitusi N menjadi T
11. Listrik akan masuk kembali pada sisi kebalikan rotor I dan mensubstitusi T menjadi J (T masuk sebagai J, J disubstitusi sebagai Z, Z keluar sebagai J)
12. Listrik akan masuk kembali pada plugboard dan mensubstitusi J menjadi J
13. Listrik akan masuk ke *lampboard* dan menyalakan lampu yang berkoresponden dengan huruf J

1. Listrik akan keluar dari kabel yang berkoresponden dengan huruf B
2. Listrik akan masuk ke plugboard dan mensubstitusi B dengan B
3. Listrik akan keluar dari plugboard
4. Rotor I akan berputar satu kali
5. Listrik akan masuk pada rotor I, yang akan mensubstitusi B dengan B (B masuk sebagai S, S disubstitusi sebagai S, S kemudian keluar sebagai B), rotor II berputar satu kali

6. Listrik akan masuk pada rotor II yang akan mensubstitusi B dengan C (B masuk sebagai C, C disubstitusi sebagai D, D kemudian keluar sebagai C)
7. Listrik akan masuk pada rotor III yang akan mensubstitusi C dengan F
8. Listrik akan masuk ke reflektor dan akan merubah F menjadi S
9. Listrik akan masuk kembali pada sisi kebalikan rotor III dan mensubstitusi S menjadi X
10. Listrik akan masuk kembali pada sisi kebalikan rotor II dan mensubstitusi X menjadi U (X masuk sebagai Y, Y disubstitusi sebagai V, V keluar sebagai U)
11. Listrik akan masuk kembali pada sisi kebalikan rotor I dan mensubstitusi U menjadi N (U masuk sebagai L, L disubstitusi sebagai E, E keluar sebagai N)
12. Listrik akan masuk kembali pada plugboard dan mensubstitusi N menjadi N
13. Listrik akan masuk ke *lampboard* dan menyalakan lampu yang berkoresponden dengan huruf N

2.2. Dekripsi

Contoh dekripsi *step-by-step*:

Dekripsi teks JN, dengan initial position rotor pada P dan ring setting rotor pada A:

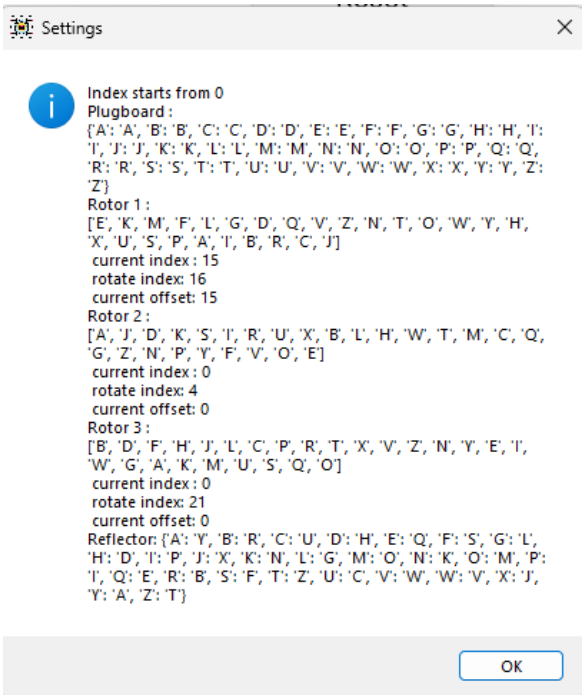
1. Listrik akan keluar dari kabel yang berkoresponden dengan huruf J
2. Listrik akan masuk ke plugboard dan mensubstitusi J dengan J
3. Listrik akan keluar dari plugboard
4. Rotor I akan berputar satu kali
5. Listrik akan masuk pada rotor I, yang akan mensubstitusi J dengan T (J masuk sebagai Z, Z disubstitusi sebagai J, J kemudian keluar sebagai T), belum ada perputaran rotor II dan III
6. Listrik akan masuk pada rotor II yang akan mensubstitusi T dengan N
7. Listrik akan masuk pada rotor III yang akan mensubstitusi N dengan N
8. Listrik akan masuk ke reflektor dan akan merubah N menjadi K
9. Listrik akan masuk kembali pada sisi kebalikan rotor III dan mensubstitusi K menjadi U
10. Listrik akan masuk kembali pada sisi kebalikan rotor II dan mensubstitusi U menjadi H
11. Listrik akan masuk kembali pada sisi kebalikan rotor I dan mensubstitusi H menjadi A (H masuk sebagai X, X disubstitusi sebagai Q, Q keluar sebagai A)

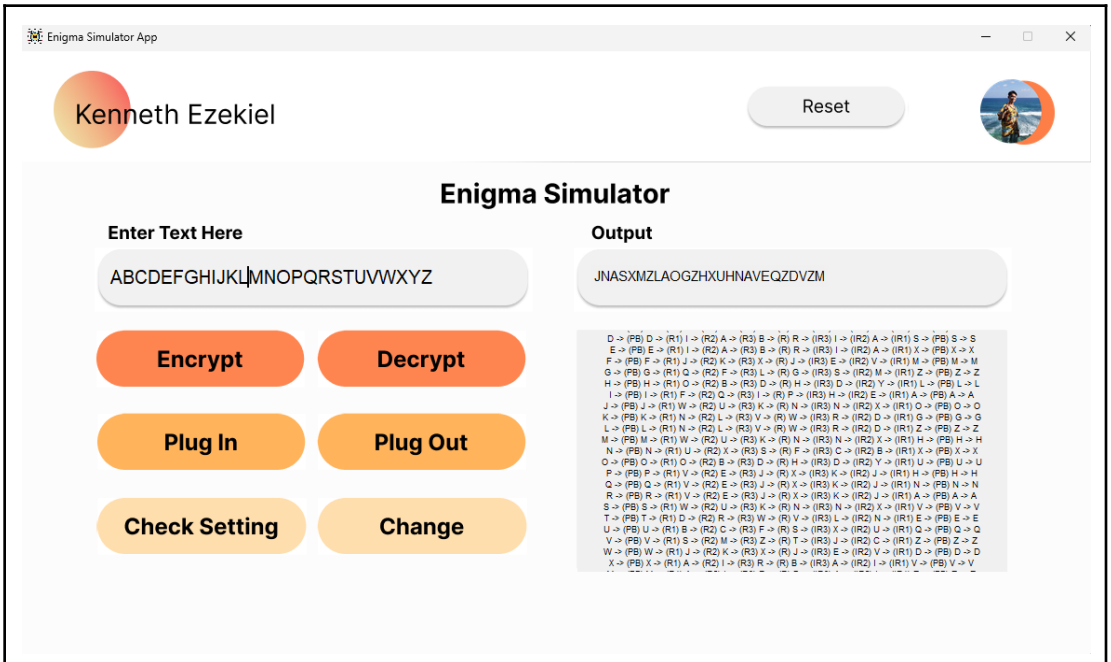
12. Listrik akan masuk kembali pada plugboard dan mensubstitusi A menjadi A
13. Listrik akan masuk ke *lampboard* dan menyalakan lampu yang berkoresponden dengan huruf A

1. Listrik akan keluar dari kabel yang berkoresponden dengan huruf N
2. Listrik akan masuk ke plugboard dan mensubstitusi N dengan N
3. Listrik akan keluar dari plugboard
4. Rotor I akan berputar satu kali
5. Listrik akan masuk pada rotor I, yang akan mensubstitusi N dengan U (N masuk sebagai E, E disubstitusi sebagai L, L kemudian keluar sebagai U), rotor II berputar satu kali
6. Listrik akan masuk pada rotor II yang akan mensubstitusi U dengan X (U masuk sebagai V, V disubstitusi sebagai Y, Y kemudian keluar sebagai X)
7. Listrik akan masuk pada rotor III yang akan mensubstitusi X dengan S
8. Listrik akan masuk ke reflektor dan akan merubah S menjadi F
9. Listrik akan masuk kembali pada sisi kebalikan rotor III dan mensubstitusi F menjadi C
10. Listrik akan masuk kembali pada sisi kebalikan rotor II dan mensubstitusi C menjadi B (C masuk sebagai D, D disubstitusi sebagai C, C keluar sebagai B)
11. Listrik akan masuk kembali pada sisi kebalikan rotor I dan mensubstitusi B menjadi B (B masuk sebagai S, S disubstitusi sebagai S, S keluar sebagai B)
12. Listrik akan masuk kembali pada plugboard dan mensubstitusi B menjadi B
13. Listrik akan masuk ke *lampboard* dan menyalakan lampu yang berkoresponden dengan huruf B

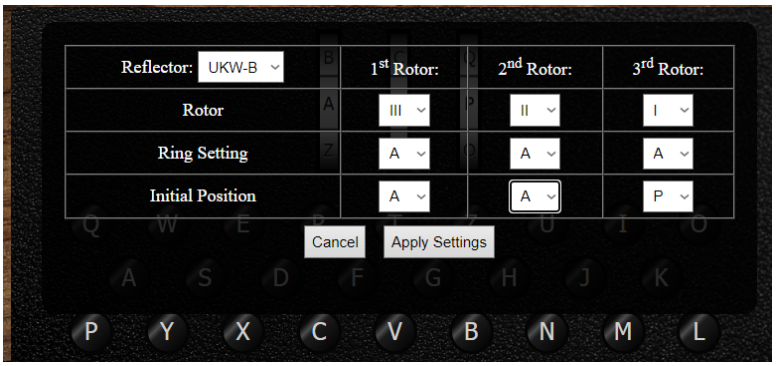
BAB III

Hasil Eksperimen

Program



Enigma Simulator App
Kenneth Ezekiel
Reset
Enigma Simulator
Enter Text Here
ABCDEFGHIJKLMNOPQRSTUVWXYZ
Output
JNASXMZLAOGZHXUHNAVEQZDVZM
Encrypt
Decrypt
Plug In
Plug Out
Check Setting
Change

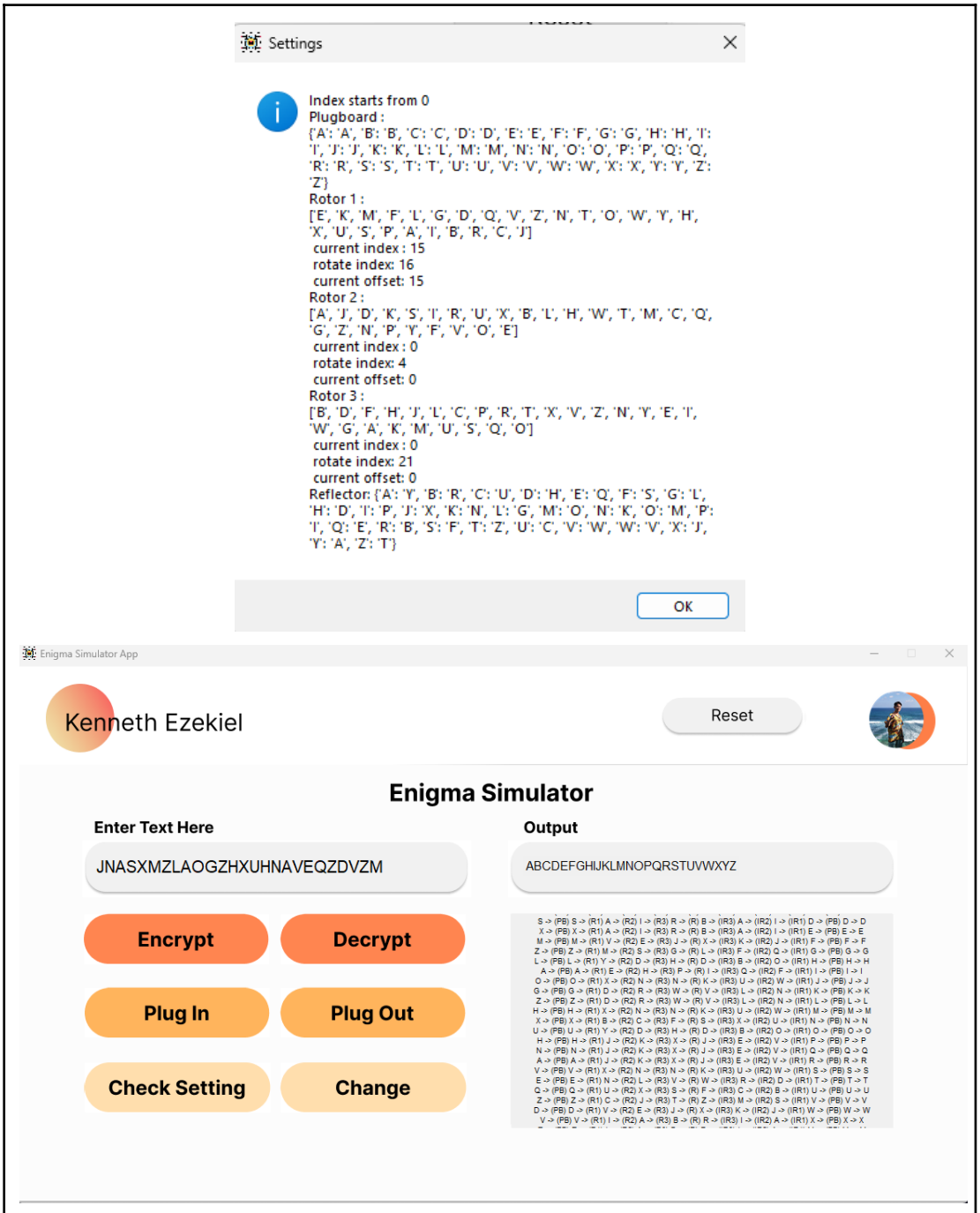
Web


Reflector: UKW-B
1st Rotor:
2nd Rotor:
3rd Rotor:
Rotor
III
II
I
Ring Setting
A
A
A
Initial Position
A
A
P
Cancel
Apply Settings

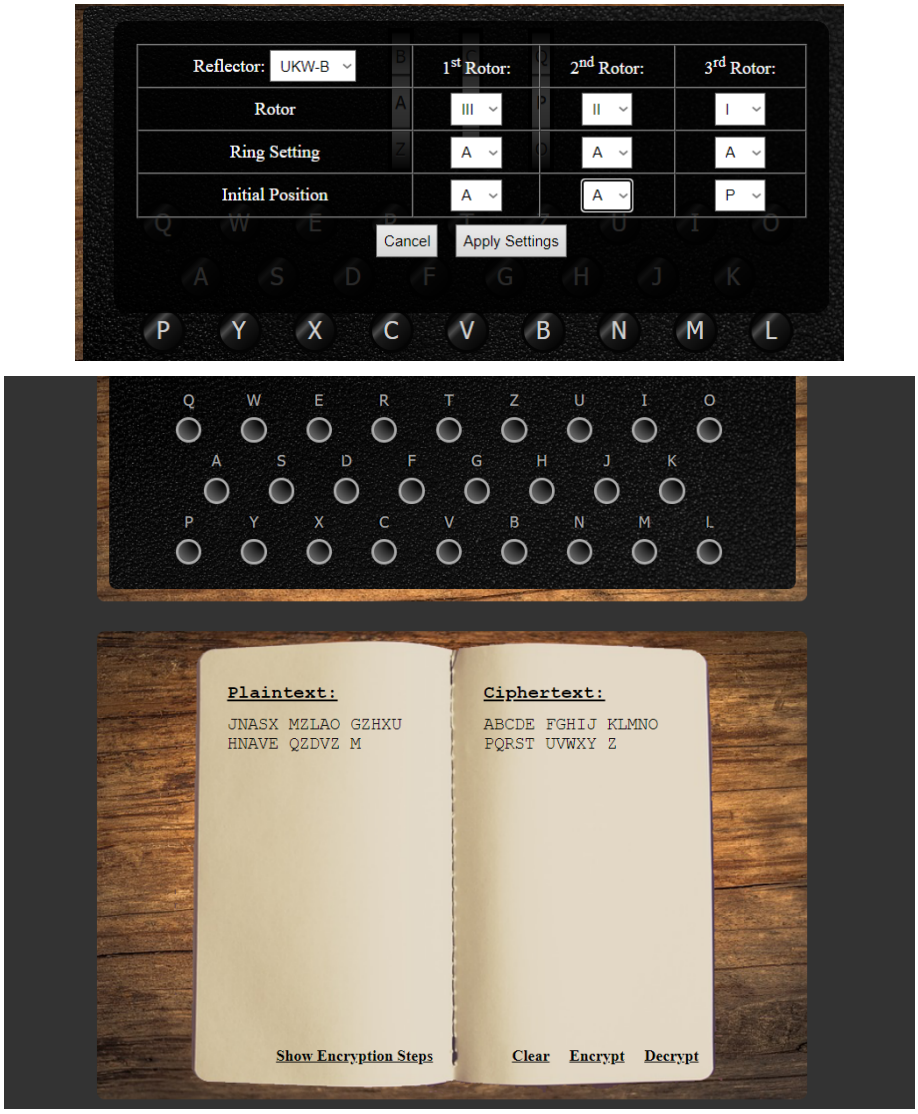
Deskripsi

Hasil yang didapatkan dari aplikasi dan web sama, dengan initial position rotor I di P dan ring setting ketiga rotor di A

Program


Settings
Index starts from 0
Plugboard :
{'A': 'A', 'B': 'B', 'C': 'C', 'D': 'D', 'E': 'E', 'F': 'F', 'G': 'G', 'H': 'H', 'I': 'I', 'J': 'J', 'K': 'K', 'L': 'L', 'M': 'M', 'N': 'N', 'O': 'O', 'P': 'P', 'Q': 'Q', 'R': 'R', 'S': 'S', 'T': 'T', 'U': 'U', 'V': 'V', 'W': 'W', 'X': 'X', 'Y': 'Y', 'Z': 'Z'}
Rotor 1 :
['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']
current index : 15
rotate index: 16
current offset: 15
Rotor 2 :
['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']
current index : 0
rotate index: 4
current offset: 0
Rotor 3 :
['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']
current index : 0
rotate index: 21
current offset: 0
Reflector: {'A': 'Y', 'B': 'R', 'C': 'U', 'D': 'H', 'E': 'Q', 'F': 'S', 'G': 'L', 'H': 'D', 'I': 'P', 'J': 'X', 'K': 'N', 'L': 'G', 'M': 'O', 'N': 'K', 'O': 'M', 'P': 'I', 'Q': 'E', 'R': 'B', 'S': 'F', 'T': 'Z', 'U': 'C', 'V': 'W', 'W': 'V', 'X': 'J', 'Y': 'A', 'Z': 'T'}
OK
Enigma Simulator App
Kenneth Ezekiel
Reset
Enigma Simulator
Enter Text Here
JNASXMZLAOGZHXUHNAVEQZDVZM
Output
ABCDEFGHIJKLMNOPQRSTUVWXYZ
Encrypt
Decrypt
Plug In
Plug Out
Check Setting
Change

Web



Deskripsi

Hasil dekripsi yang dilakukan pada hasil enkripsi teks sebelumnya konsisten dalam teori, aplikasi, dan juga web