LAPORAN TUGAS KECIL

IFXXXX Lab Ilmu Rekayasa Komputasi

Implementasi Kriptografi "Sederhana++" Dalam Pengenkripsian Pesan

Anggota Kelompok :

(13521106) Mohamad Farhan Fahreezy

Sekolah Teknik Elektro dan Informatika

Institut Teknologi Bandung

2023

Daftar Isi

Bab 1:
Deskripsi Tugas

1.1 Latar Belakang

Dalam tugas kecil ini, penulis diminta untuk membuat sebuah simulasi dari sebuah mesin kriptografi sederhana. Simulasi yang akan dibuat menggunakan prinsip kerja mesin enigma yang awalnya merupakan mesin elektromekanik menjadi mesin elektronik dengan cara membuat simulasi dalam komputer.

Enigma M3

German Navy (Kriegsmarine)

The Enigma M1, M2 and M3 machines were used by the German Navy (Kriegsmarine). They are basically compatible with the Enigma I. The wiring of the Enigma M3 is given in the table below. Wheels I thru V are identical to those of the Enigma I. The same is true for UKW B and C. The three additional wheels (VI, VII and VIII) were used exclusively by the *Kriegsmarine*. The machine is also compatible with the Enigma M4 (when the 4th wheel of the M4 is set to position 'A').

Wheel	ABCDEFGHIJKLMNOPQRSTUVWXYZ	Notch	Turnover	#
ETW	ABCDEFGHIJKLMNOPQRSTUVWXYZ			
I	EKMFLGDQVZNTOWYHXUSPAIBRCJ	Y	Q	1
II	AJDKSIRUXBLHWTMCQGZNPYFVOE	M	E	1
III	BDFHJLCPRTXVZNYEIWGAKMUSQO	D	V	1
IV	ESOVPZJAYQUIRHXLNFTGKDCMWB	R	J	1
V	VZBRGITYUPSDNHLXAWMJQOFECK	H	Z	1
VI	JPGVOUMFYQBENHZRDKASXLICTW	HU	ZM	2
VII	NZJHGRCXMYSWBOUFAIVLPEKQDT	HU	ZM	2
VIII	FKQHTLXOCBJSPDZRAMEWNIUYGV	HU	ZM	2
UKW-B	YRUHQSLDPXNGOKMIEBFZCWVJAT			
UKW-C	FVPJIAOYEDRZXWGCTKUQSBNMHL			

Sumber : https://www.cryptomuseum.com/crypto/enigma/wiring.htm#12

Spesifikasi yang diminta adalah sebagai berikut:

1. Buatlah sebuah program yang dapat melakukan kriptografi enigma M3. Pembanding: https://www.101computing.net/enigma-machine-emulator/.
2. Program tidak perlu mengimplementasikan plugboard. (Bonus jika diimplementasikan).
3. Program dapat memilih konfigurasi Rotor dan initial position rotor.

4. Entry disc yang digunakan adalah ETW.
5. Rotor yang dapat dipilih adalah Rotor I,II,III.
6. Reflektor yang digunakan adalah UKW-B.
7. Program dapat melakukan enkripsi teks singkat dengan benar.
8. Program dapat melakukan dekripsi teks singkat dengan benar.
9. Program dapat melakukan enkripsi teks panjang dengan benar.
10. Program dapat melakukan dekripsi teks panjang dengan benar.
11. Program dapat menampilkan step by step enkripsi dan dekripsi dengan benar.

Spesifikasi bonus yang diminta adalah sebagai berikut:

1. Implementasikan Plugboard pada enigma (format dibebaskan).
2. Implementasikan GUI.
3. Implementasi enigma auto decoder yaitu program yang bisa tau konfigurasi rotor, plugboard, dan initial state dari sebuah mesin enigma hanya berdasarkan cypher text yang dipakai..

Bab 2:
Landasan Teori

2.1 Enigma

Mesin Enigma merupakan salah satu mesin kriptografi elektromekanik yang paling terkenal di dunia, salah satunya karena peran penting yang dimainkannya selama Perang Dunia II yang digunakan oleh Jerman Nazi untuk mengenkripsi dan mendekripsi pesan rahasia. Enigma bukanlah sebuah nama sebuah barang, melainkan sebuah *brand* dari serangkaian mesin cipher yang dikembangkan sebelum dan selama Perang Dunia II. Ada banyak jenis mesin enigma. Beberapa di antaranya kompatibel satu sama lain, dan yang lainnya tidak.

Sebelum dan selama Perang Dunia II, Enigma menjadi inspirasi bagi banyak desain mesin cipher rotor lainnya, seperti British Typex dan American SIGABA. Dan bahkan setelah perang, beberapa mesin cipher dibuat berdasarkan pada prinsip yang sama, seperti KL-7 Amerika, Fialka Rusia, dan Nema Swiss.

2.2 Cara Kerja Enigma

Mesin Enigma bekerja dengan melakukan substitusi huruf yang dimasukkan oleh pengguna dengan huruf yang diacak menggunakan arus listrik dan putaran rotor. Mesin enigma dapat memberikan hasil enkripsi dan dekripsi yang sama dengan syarat seluruh konfigurasi dekripsi harus sama dengan konfigurasi enkripsi.

Cara kerja mesin Enigma dapat dijelaskan dengan langkah-langkah berikut:

1. Pengaturan awal: user mengatur posisi awal rotor pada mesin Enigma dengan memilih urutan rotor dan mengatur posisi huruf di rotor. Setiap rotor memiliki pengaturan awal yang berbeda.
2. Pengetikan pesan: user memasukkan pesan yang akan dienkripsi dengan menekan tombol pada keyboard mesin Enigma.
3. Memutar rotor: pada tiap ketikan yang diberikan oleh user, sebuah rangka mekanik yang terhubung dengan keyboard mesin Enigma akan mendorong rotor paling kanan untuk berubah posisi sebanyak satu karakter.

4. Listrik melintasi kabel: saat user menekan tombol, arus listrik mengalir melintasi kabel-kabel yang terhubung dengan tombol tersebut. Arus ini akan melewati serangkaian komponen elektromekanik pada mesin Enigma.
5. Plugboard: arus listrik kemudian masuk ke plugboard, sebuah papan dengan konektor yang dapat diatur. User dapat mengatur konektor-konektor ini untuk memetakan satu huruf ke huruf lainnya sebelum masuk ke rotor.
6. Rotor: arus listrik yang keluar dari plugboard masuk ke rotor-rotor. Setiap rotor memiliki pengaturan internal yang memetakan huruf-huruf secara kompleks, sehingga mengubah huruf masukan menjadi huruf yang berbeda saat melewati rotor. Rotor-rotor juga memiliki kontak yang berhubungan dengan rotor lainnya dan akan mempengaruhi perubahan arus listrik saat melintasinya.
7. Reflektor: setelah melewati rotor-rotor, arus listrik memasuki reflektor. Reflektor mengubah arus listrik kembali ke rotor-rotor dengan lintasan yang berbeda. Tujuannya adalah agar setiap huruf yang masuk akan memiliki keluaran yang berbeda.
8. Rotor: setelah keluar dari reflektor, arus listrik melewati rotor-rotor lagi dalam urutan yang berlawanan dengan sebelumnya. Namun, kali ini perjalanan arus listrik berbeda karena kontak rotor bekerja dalam arah yang berlawanan.
9. Plugboard: arus listrik yang sudah keluar dari rotor akan masuk ke dalam plugboard sekali lagi sebelum menuju output yang menyalakan lampu indikator.
10. Output: setelah keluar dari plugboard, arus listrik akan bergerak menuju ke lampu indikator yang terhubung dengan sebuah baterai. Hal ini menyebabkan terjadinya sebuah loop tertutup pada rangkaian mesin enigma yang membuat lampu indikator menyala dan memberi tahu user hasil enkripsi.

2.3 Rotor

Mesin enigma memiliki berbagai varian mesin dan rotor. Pada tugas ini, penulis menggunakan mesin Enigma M3 dengan konfigurasi rotor I, II, III, IV dan V. Tiap rotor yang digunakan pada mesin Enigma M3 memiliki fungsi pemetaan yang berbeda.

Setiap rotor memiliki konfigurasi *turnover* yang berbeda. *Turnover* merupakan batas satu kali putaran dari sebuah rotor yang dapat membuat rotor di sebelah kiri rotor tersebut berputar satu karakter.

Rotor	ABCDEFGHIJKLMNOPQRSTUVWXYZ	Turnover
I	EKMFLGDQVZNTOWYHXUSPAIBRCJ	Q
II	AJDKSIRUXBLHWTMCQGZNPYFVOE	E
III	BDFHJLCPRTXVZNYEIWGAKMUSQO	V
IV	ESOVPZJAYQUIRHXLNFTGKDCMWB	J
V	VZBRGITYUPSDNHLXAWMJQOFECK	Z

Sumber : https://www.cryptomuseum.com/crypto/enigma/wiring.htm#12

2.4 Reflektor

Mesin enigma memiliki berbagai varian mesin dan reflektor. Pada tugas ini, penulis menggunakan mesin Enigma M3 dengan konfigurasi reflektor UKW-B. Tiap reflektor yang digunakan pada mesin Enigma M3 memiliki fungsi pemetaan yang berbeda.

Reflektor	ABCDEFGHIJKLMNOPQRSTUVWXYZ
UKW-B	YRUHQSLDPXNGOKMIEBFZCWVJAT
UKW-C	FVPJIAOYEDRZXWGCTKUQSBNMHL

Sumber : https://www.cryptomuseum.com/crypto/enigma/wiring.htm#12

2.4 Mesin Bombe

Mesin Bombe adalah sebuah mesin kriptanalisis yang digunakan selama Perang Dunia II oleh Britania Raya untuk membantu dalam dekripsi kode yang dihasilkan oleh mesin Enigma. Mesin Bombe dirancang oleh sekelompok ilmuwan, termasuk Alan Turing, di Pusat Kode Bletchley Park di Britania Raya. Mesin ini dirancang untuk mengotomatiskan proses dekripsi kode Enigma dengan mencoba semua kemungkinan pengaturan kunci.

Bombe bekerja dengan menganalisis pola-pola yang muncul dalam teks terenkripsi. Dalam operasinya, mesin ini menggunakan informasi tentang struktur internal Enigma dan kemungkinan kata-kata yang terdapat dalam pesan yang sedang dipecahkan. Mesin Bombe mencoba memetakan kombinasi kabel penghubung dan pengaturan rotor yang digunakan dalam mesin Enigma pada suatu waktu tertentu. Jika suatu konfigurasi menghasilkan pola yang masuk akal dalam dekripsi pesan, maka ini menjadi kunci yang mungkin digunakan.

Bab 3:
Implementasi dan Pengujian

3.1 Implementasi Enkripsi Teoritis

Mesin enigma melakukan enkripsi dengan menggunakan berbagai konfigurasi agar pesan sulit untuk dipecahkan. Sedikit catatan, hasil dari setiap input dan output dari rotor mengalami shifting karena *initial position* tidak selalu berada di posisi A. Setiap akan masuk ke sebuah rotor, input yang diterima akan digeser sebanyak jumlah putaran rotor (atau sebanding dengan jarak posisi sekarang ke A) dan setiap keluar dari sebuah rotor, output yang diberikan juga digeser berlawanan arah sebanyak jumlah putaran rotor.

Berikut merupakan hasil enkripsi secara teoritis.

<table>
<tr><td colspan="5">Contoh 1</td></tr>
<tr><td colspan="4">Konfigurasi</td><td rowspan="5">Input : U
Rotor Position : XTD
Plugboard In : U
Right Wheel 1 : P
Middle Wheel 1 : F
Left Wheel 1 : E
Reflection : Q
Left Wheel 2 : P
Middle Wheel 2 : S
Right Wheel 2 : I
Plugboard Out: I
Output: I</td><td rowspan="5">Input : U
Output : I</td></tr>
<tr><td>Rotor</td><td>V</td><td>IV</td><td>III</td></tr>
<tr><td>Initial Rotor Position</td><td>X</td><td>T</td><td>C</td></tr>
<tr><td>Plugboard</td><td colspan="3">-</td></tr>
<tr><td colspan="5">Contoh 2</td></tr>
<tr><td colspan="4">Konfigurasi</td><td rowspan="5">Input : C
Rotor Position : UKN
Plugboard In : A
Right Wheel 1 : U
Middle Wheel 1 : Z
Left Wheel 1 : V
Reflection : W
Left Wheel 2 : N
Middle Wheel 2 : A
Right Wheel 2 : Z</td><td rowspan="5">Input : C
Output : Z</td></tr>
<tr><td>Rotor</td><td>I</td><td>III</td><td>V</td></tr>
<tr><td>Initial Rotor Position</td><td>U</td><td>K</td><td>M</td></tr>
<tr><td>Plugboard</td><td colspan="3">(A,C)</td></tr>
</table>

<table>
<tr><td></td><td colspan="3"></td><td>Plugboard Out: Z
Output: Z</td><td></td></tr>
<tr><td colspan="6">Contoh 3</td></tr>
<tr><td colspan="4">Konfigurasi</td><td rowspan="5">Input : G
Rotor Position : PTL
Plugboard In : U
Right Wheel 1 : X
Middle Wheel 1 : X
Left Wheel 1 : Z
Reflection : T
Left Wheel 2 : G
Middle Wheel 2 : Z
Right Wheel 2 : S
Plugboard Out : S
Output: S</td><td rowspan="5">Input : G
Output : S</td></tr>
<tr><td>Rotor</td><td>I</td><td>II</td><td>II</td></tr>
<tr><td>Initial Rotor Position</td><td>P</td><td>T</td><td>K</td></tr>
<tr><td>Plugboard</td><td colspan="3">(U,G),(N,T)</td></tr>
</table>

3.2 Implementasi Dekripsi Teoritis

Enigma dapat melakukan dekripsi hasil enkripsi dengan menggunakan konfigurasi yang sama saat melakukan enkripsi. Berikut implementasi dekripsi menggunakan input yang sama dengan output enkripsi bagian 3.1

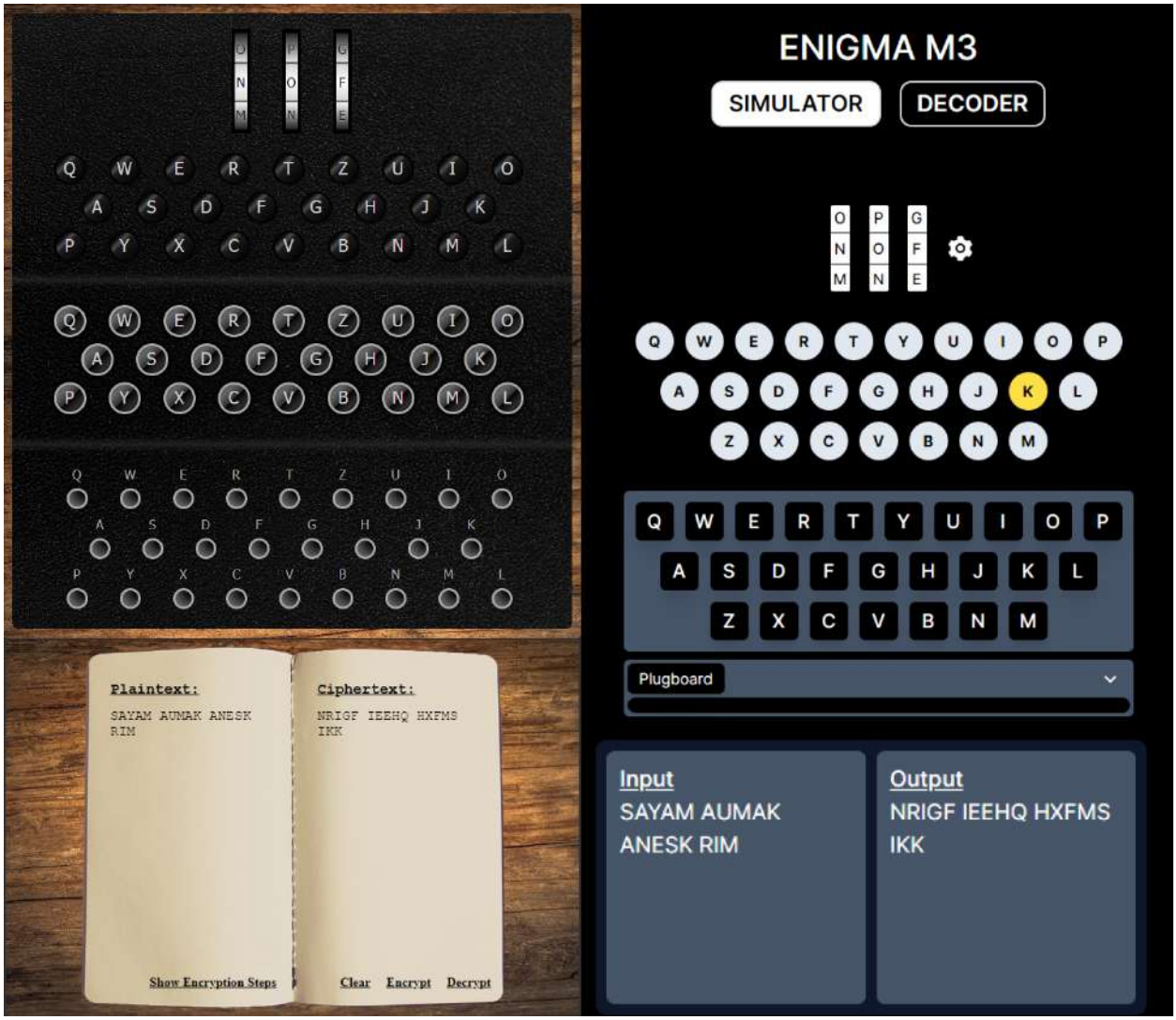
<table>
<tr><td colspan="6">Contoh 1</td></tr>
<tr><td colspan="4">Konfigurasi</td><td rowspan="5">Input : I
Rotor Position : XTD
Plugboard In : I
Right Wheel 1 : S
Middle Wheel 1 : P
Left Wheel 1 : Q
Reflection : E
Left Wheel 2 : F
Middle Wheel 2 : P
Right Wheel 2 : U
Plugboard In : U
Output: U</td><td rowspan="5">Input : I
Output : U</td></tr>
<tr><td>Rotor</td><td>V</td><td>IV</td><td>III</td></tr>
<tr><td>Initial Rotor Position</td><td>X</td><td>T</td><td>C</td></tr>
<tr><td>Plugboard</td><td colspan="3">-</td></tr>
<tr><td colspan="6">Contoh 2</td></tr>
<tr><td colspan="4">Konfigurasi</td><td rowspan="2">Input : Z
Rotor Position : UKN</td><td rowspan="2">Input : Z
Output : C</td></tr>
<tr><td>Rotor</td><td>I</td><td>III</td><td>V</td></tr>
</table>

<table>
<tr><td>Initial Rotor Position</td><td>U</td><td>K</td><td>M</td><td rowspan="2">Plugboard In : Z
Right Wheel 1 : A
Middle Wheel 1 : N
Left Wheel 1 : W
Reflection : V
Left Wheel 2 : Z
Middle Wheel 2 : U
Right Wheel 2 : A
Plugboard In : C
Output: C</td><td rowspan="2"></td></tr>
<tr><td>Plugboard</td><td colspan="3">(A,C)</td></tr>
<tr><td colspan="6">Contoh 3</td></tr>
<tr><td colspan="4">Konfigurasi</td><td rowspan="5">Input : S
Rotor Position : PTL
Plugboard In : S
Right Wheel 1 : Z
Middle Wheel 1 : G
Left Wheel 1 : T
Reflection : Z
Left Wheel 2 : X
Middle Wheel 2 : X
Right Wheel 2 : U
Plugboard In : G
Output: G</td><td rowspan="5">Input : S
Output : G</td></tr>
<tr><td>Rotor</td><td>I</td><td>II</td><td>II</td></tr>
<tr><td>Initial Rotor Position</td><td>P</td><td>T</td><td>K</td></tr>
<tr><td>Plugboard</td><td colspan="3">(U,G),(N,T)</td></tr>
</table>

3.2 Implementasi Mesin Enigma

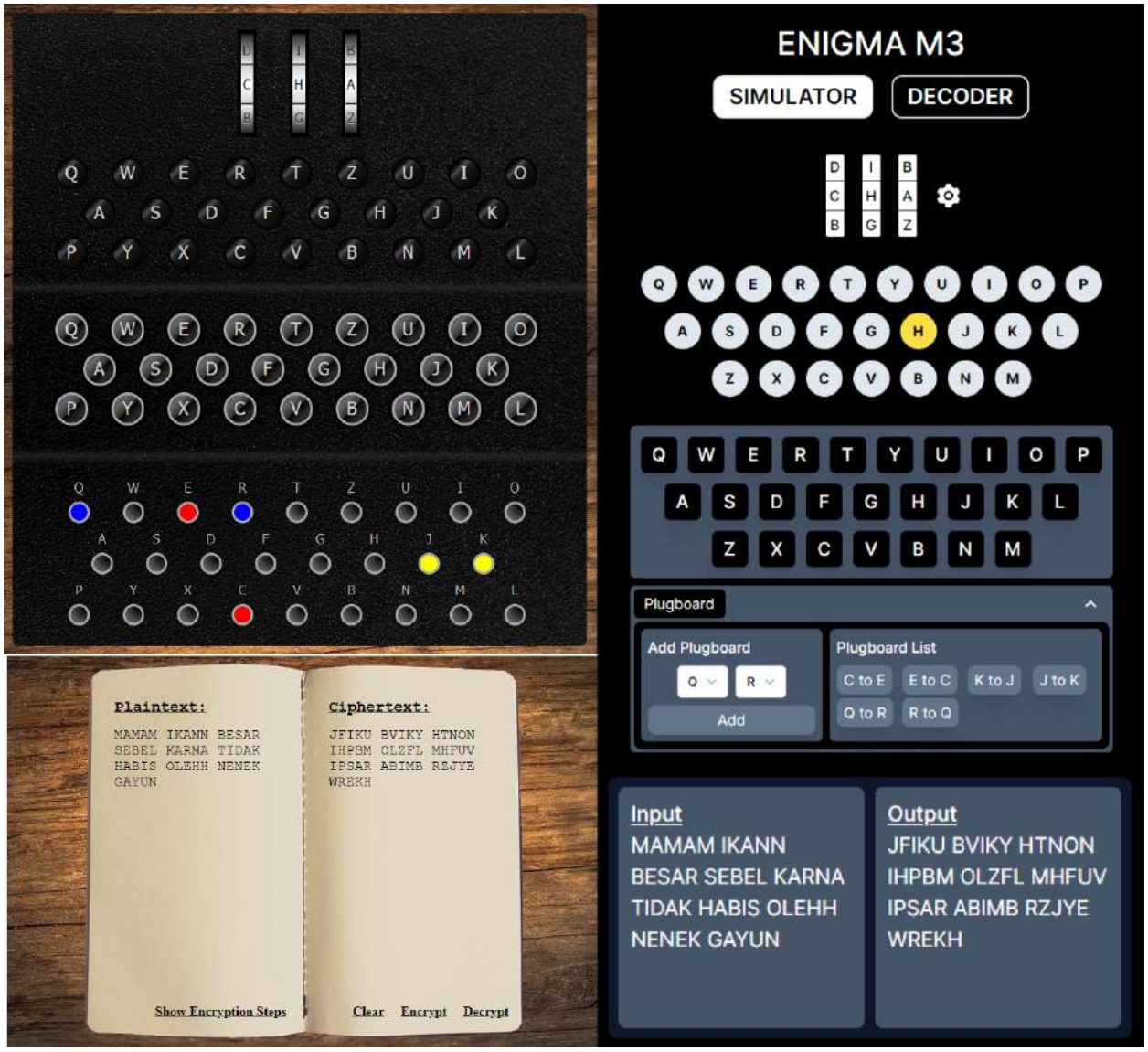
Simulasi mesin Enigma dibuat menggunakan prinsip yang sama dengan mesin aslinya, yaitu dengan menggunakan 3 rotor yang bisa diatur jenis dan posisi awalnya. Program dibuat menggunakan framework React Js. Hasil program dapat langsung diakses di https://enigma-m3.vercel.app/ atau dapat mengakses *source code* di https://github.com/farhanfahreezy/Enigma-M3.

Untuk menguji kebenaran dari simulasi mesin Enigma yang penulis buat, akan dilakukan perbandingan menggunakan simulasi yang disediakan di https://www.101computing.net/enigma-machine-emulator/. Berikut merupakan perbandingan hasil enkripsi mesin Enigma versi penulis dan mesin Enigma versi internet.



Gambar 3.3.1 Perbandingan mesin Enigma internet (kiri) dan penulis (kanan) konfigurasi 531 NNN

Sumber : Dokumentasi pribadi



Gambar 3.3.1 Perbandingan mesin Enigma internet (kiri) dan penulis (kanan) konfigurasi 531 NNN (C,E), (K,J), (Q,R)

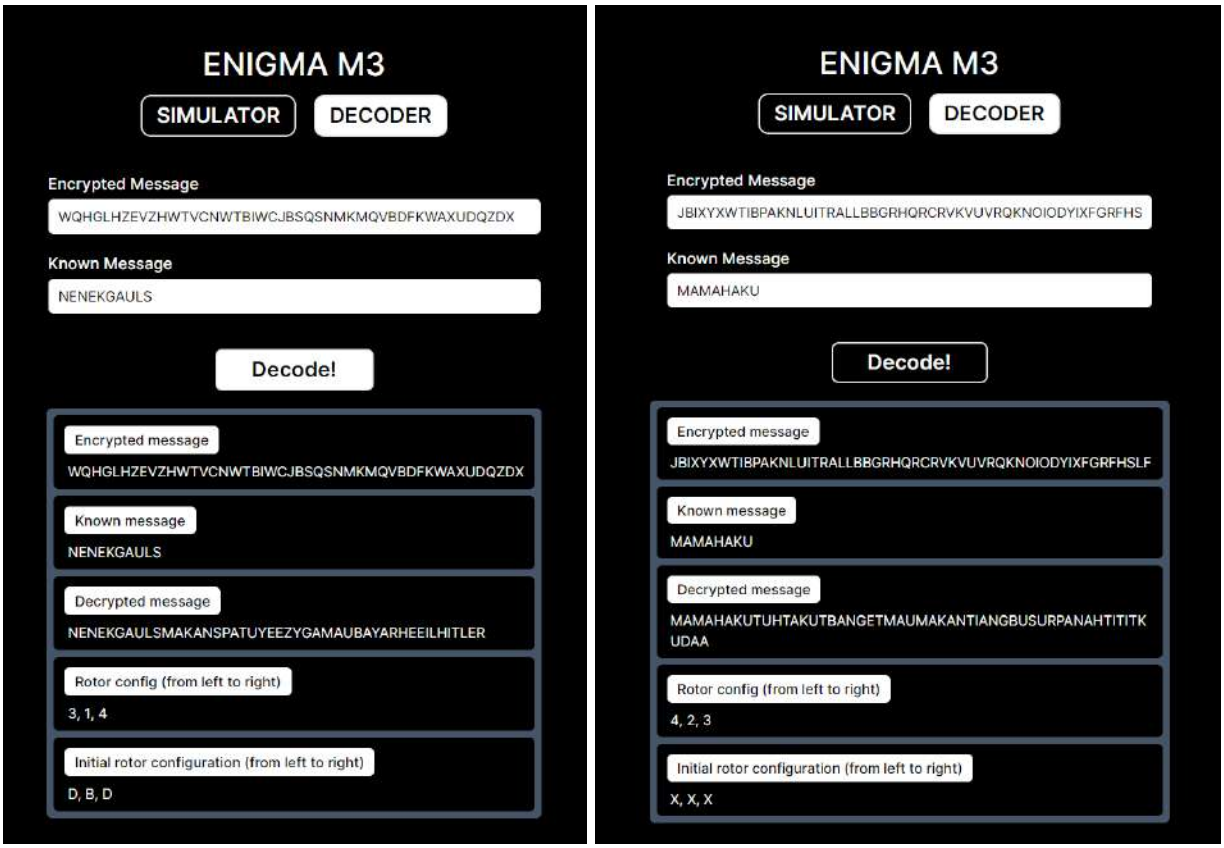
Sumber : Dokumentasi pribadi

3.4 Implementasi Mesin Bombe

Simulasi mesin Bombe dibuat menggunakan prinsip yang sama dengan mesin aslinya, yaitu dengan melakukan pengecekan terhadap seluruh kemungkinan kombinasi dari rotor dan posisi awal rotor. Pada program yang penulis buat, pesan yang dienkripsi dapat dipecahkan dengan menggunakan kata yang dikenali pada awal pesan. Dari kata yang dikenali tersebut, program

akan mencari semua kemungkinan dari rotor dan posisi awal rotor untuk mencocokkan hasil enkripsi dengan kata yang dikenali tersebut.

Berikut merupakan contoh penggunaan simulasi mesin Bombe.



Sumber : https://www.cryptomuseum.com/crypto/enigma/wiring.htm#12

Lampiran

Link Repository GitHub: https://github.com/farhanfahreezy/Enigma-M3

Link Deployment: https://enigma-m3.vercel.app/