Laporan Implementasi Kriptografi Enigma

dalam

Pengenkripsian Pesan

Sumber:

https://upload.wikimedia.org/wikipedia/commons/b/bd/Enigma_%28crittografia%29_-_Museo_scienza_e_tecnologia_Milano.jpg

Oleh:

Bill Clinton / 13521064

A. Pengertian Enigma

Enigma merupakan sebuah mesin elektromekanik yang digunakan untuk menyandikan teks tertentu. Mesin ini diciptakan oleh Arthur Scherbius pada tahun 1918. Mesin ini dianggap sebagai mesin penyandi yang sangat aman hingga sering digunakan untuk mengenkripsi pesan-pesan paling rahasia. Pada awalnya, mesin ini digunakan untuk tujuan yang berhubungan dengan bisnis dan pemerintahan. Namun, lama-lama mesin ini mulai banyak digunakan sebelum dan selama Perang Dunia II. Hal ini membuat mesin ini menjadi salah satu simbol yang paling terkenal dalam dunia kriptografi.

Secara umum, mesin ini terdiri dari beberapa komponen, yakni *keyboard*, *plugboard*, *rotor*, dan *reflector*. Huruf yang ditekan pada keyboard akan dipetakan dengan metode penggantian substitusi yang kompleks menjadi huruf lain yang dapat dilihat berdasarkan nyala lampu huruf. Huruf-huruf yang sama dapat dipetakan menjadi huruf-huruf yang berbeda dalam sekali pengetikan. Komponen-komponen, yaitu *plugboard*, *rotor*, dan *reflector*, memegang peranan yang sangat penting dalam pengenkripsian tulisan dan dapat diatur konfigurasinya. Berikut adalah penjelasan dari komponen-komponen mesin enigma.

- *Keyboard* merupakan sebuah komponen yang terdiri dari tombol-tombol berlabel huruf yang ditekan untuk mengenkripsikan teks tertentu.
- *Plugboard* merupakan sebuah komponen yang memiliki kabel-kabel yang menghubungkan sepasang huruf. Dengan adanya plugboard, pengguna dapat menukar huruf sebelum huruf masuk ke proses penggantian pada rotor.
- *Rotor* merupakan roda-roda yang terdiri dari angka-angka yang melambangkan huruf. Angka-angka ini tercetak di sekitar tepi roda. Setiap rotor dapat diubah posisi awalnya dan rodanya akan berubah posisi setiap tombol huruf pada keyboard ditekan. Setiap jenis mesin enigma memiliki jumlah rotor yang berbeda, misalnya mesin Enigma M3 yang menggunakan 3 rotor.
- *Reflector* merupakan sebuah komponen yang memantulkan sinyal kembali ke rotor untuk menghasilkan efek substitusi yang terakhir.

Hal lain yang juga krusial mengenai mesin enigma adalah pada pendekripsinya. Pada proses enkripsi, pengguna dapat dengan bebas menentukan konfigurasi komponen-komponen mesinnya, sedangkan pada proses dekripsi, pengguna perlu untuk mengetahui konfigurasi awal ketika mesin itu digunakan untuk menenkripsi pesan agar dapat mendekripsi pesannya. Kemungkinan konfigurasi komponen-komponen ini

sangat banyak sehingga mesin Enigma pernah dianggap tidak dapat dipecahkan. Namun, seorang matematikawan bernama Alan M. Turing berhasil memecahkannya dengan mengidentifikasi kelemahannya. Salah satu kelemahannya adalah mesin Enigma tidak dapat memetakan suatu huruf ke huruf yang sama. Hal ini tentu akan memperkecil kemungkinan konfigurasi awal komponen-komponen mesin Enigma secara eksponensial.

B. Cara Kerja Enigma

Secara umum, mesin Enigma bekerja dengan urutan *keyboard – plugboard – rotor – reflector – rotor – plugboard – output*. Sebuah huruf yang ditekan pada keyboard akan diganti menjadi huruf lain pada *plugboard* jika huruf yang ditekan dihubungkan dengan huruf lain tersebut dengan kabel. Setelah itu, huruf akan dipetakan menurut konfigurasi *wiring* pada rotor. Beberapa konfigurasi *wiring* yang dikenal, misalnya untuk mesin Enigma M3 yaitu I, II, dan III. Perlu diingat bahwa seiring ditekannya huruf, roda rotor akan berputar. Pada mesin yang memiliki beberapa *rotor*, roda *rotor* yang paling pertama berputar (*fast rotor*) dapat menginisiasi perputaran roda *rotor* disampingnya saat roda mencapai angka tertentu (*turnover notch*). Setelah melalui *rotor*, huruf akan dipetakan melalui *reflector* berdasarkan konfigurasinya. Beberapa konfigurasi untuk *reflector* yang dikenal yaitu UKW-A dan UKW-B. Setelah melalui *reflector*, huruf akan dipetakan kembali oleh *rotor* (dengan cara yang berkebalikan dengan enkripsi *rotor-rotor* sebelum *reflector*), lalu oleh *plugboard*, hingga menghasilkan huruf hasil enkripsi yang ditandai dengan cahaya lampu huruf di atas bagian *keyboard*. Contoh-contoh penggunaan mesin Enigma ini dapat dilihat lebih lanjut pada bagian-bagian di bawah ini.

C. Contoh Enkripsi Enigma

Mesin Enigma M3

Konfigurasi

Entry Disc : **ETW** (“ABCDEFGHIJKLMNOPQRSTUVWXYZ”)
Rotor 1 : **I** (“EKMFLGDQVZNTOWYHXUSPAIBRCJ”)
Rotor 2 : **II** (“AJDKSIRUXBLHWTMCQGZNPYFVOE”)
Rotor 3 : **III** (“BDFHJLCPRTXVZNYEIWGAKMUSQO”)
Plugboard : -

Reflector : **UKW-B** (“YRUHQSLDPXNGOKMIEBFZCWVJAT”)
Posisi *Rotor* : **A A A**
Notch : **Q E V**
Pesan : “A”

Proses Enkripsi

Huruf : **A**
Posisi Rotor : **A A B (*Rotor 3* berputar)**
Enkripsi *Plugboard* : **A** (karena tidak ada kabel yang menghubungkan A dengan huruf lain di *plugboard,* tapi misalnya A dihubungkan dengan X, hasil enkripsi dari plugboard menjadi X)

Enkripsi *Rotor 3* :
BCDEFGHIJKLMNOPQRSTUVWXYZA
DFHJLCPRTXVZNYEIWGAKMUSQOB (berubah karena rotor 3 berputar)
A = 1
Pada *wiring*, posisi 1 ditempati oleh huruf D. D sendiri pada posisi 3 pada konfigurasi di atas konfigurasi *wiring*. Kita tahu bahwa huruf ke-3 dari susunan alfabet adalah C. Oleh karena itu, hasil enkripsi rotor 3 yaitu **C**.

Enkripsi *Rotor 2* :
ABCDEFGHIJKLMNOPQRSTUVWXYZ
AJDKSIRUXBLHWTMCQGZNPYFVOE (tetap karena rotor 3 belum berputar hingga *turnover notch*)
C = 3
Pada *wiring*, posisi 3 ditempati oleh huruf D. D sendiri ada pada posisi 4 pada konfigurasi di atas konfigurasi *wiring*. Kita tahu bahwa huruf ke-4 dari susunan alfabet adalah D. Oleh karena itu, hasil enkripsi rotor 2 adalah **D**.

Enkripsi *Rotor 1* :
ABCDEFGHIJKLMNOPQRSTUVWXYZ
EKMFLGDQVZNTOWYHXUSPAIBRCJ (tetap karena rotor 2 belum berputar hingga *turnover notch*)
D = 4

Pada *wiring*, posisi 4 ditempati oleh huruf F. F sendiri ada pada posisi 6 pada konfigurasi di atas konfigurasi *wiring*. Kita tahu bahwa huruf ke-6 dari susunan alfabet adalah F. Oleh karena itu, hasil enkripsi rotor 1 adalah **F**.

Enkripsi *Reflector* :
YRUHQSLDPXNGOKMIEBFZCWVJAT
F = 6
Pada konfigurasi, posisi 6 ditempati oleh huruf S. Oleh karena itu, hasil enkripsi reflektor adalah **S**.

Enkripsi *Rotor 1* :
(Hati-hati, prosesnya berkebalikan dengan enkripsi *rotor-rotor* sebelum *reflector*)
ABCDEFGHIJKLMNOPQRSTUVWXYZ
EKMFLGDQVZNTOWYHXUSPAIBRCJ (tetap karena rotor 2 belum berputar hingga *turnover notch*)
S = 19
Pada konfigurasi di atas konfigurasi *wiring* , posisi 19 ditempati oleh huruf S. S sendiri ada pada posisi 19 pada *wiring*. Kita tahu bahwa huruf ke-19 dari susunan alfabet adalah S. Oleh karena itu, hasil enkripsi rotor 1 adalah **S**.

Enkripsi *Rotor 2* :
ABCDEFGHIJKLMNOPQRSTUVWXYZ
AJDKSIRUXBLHWTMCQGZNPYFVOE (tetap karena rotor 3 belum berputar hingga *turnover notch*)
S = 19
Pada konfigurasi di atas konfigurasi *wiring* , posisi 19 ditempati oleh huruf S. S sendiri ada pada posisi 5 pada *wiring*. Kita tahu bahwa huruf ke-5 dari susunan alfabet adalah E. Oleh karena itu, hasil enkripsi rotor 1 adalah **E**.

Enkripsi *Rotor 3* :
BCDEFGHIJKLMNOPQRSTUVWXYZA
DFHJLCPRTXVZNYEIWGAKMUSQOB

E = 5

Pada konfigurasi di atas konfigurasi *wiring* , posisi 5 ditempati oleh huruf F. F sendiri ada pada posisi 2 pada *wiring*. Kita tahu bahwa huruf ke-2 dari susunan alfabet adalah B. Oleh karena itu, hasil enkripsi rotor 1 adalah **B**.

Enkripsi *Plugboard* : **B** (karena tidak ada kabel yang menghubungkan B dengan huruf lain di *plugboard*)

Output : **B**

Jadi, hasil enkripsi dari "**A**" menurut konfigurasi sebelumnya adalah "**B**".

D. Contoh Dekripsi Enigma

Seperti yang saya sebutkan dalam bagian sebelumnya, kunci dari dekripsi adalah mengetahui konfigurasi awal komponen-komponen mesin. Selebihnya, prosesnya berlaku simetris. Oleh karena itu, pada kasus kali ini, diasumsikan pengguna sudah mengetahui konfigurasi awal tersebut.

Mesin Enigma M3

Konfigurasi

Entry Disc : **ETW** ("ABCDEFGHIJKLMNOPQRSTUVWXYZ")
Rotor 1 : **I** ("EKMFLGDQVZNTOWYHXUSPAIBRCJ")
Rotor 2 : **II** ("AJDKSIRUXBLHWTMCQGZNPYFVOE")
Rotor 3 : **III** ("BDFHJLCPRTXVZNYEIWGAKMUSQO")
Plugboard : -
Reflector : **UKW-B** ("YRUHQSLDPXNGOKMIEBFZCWVJAT")
Posisi *Rotor* : **A A A**
Notch : **Q E V**
Pesan : "B"

Proses Dekripsi

Huruf : **B**
Posisi Rotor : **A A B (Rotor 3 Berputar)**
Dekripsi *Plugboard* : **B** (karena tidak ada kabel yang menghubungkan B dengan huruf lain di *plugboard,* tapi misalnya B dihubungkan dengan X, hasil dekripsi dari plugboard menjadi X)

Dekripsi *Rotor 3* :

BCDEFGHIJKLMNOPQRSTUVWXYZA

DFHJLCPRTXVZNYEIWGAKMUSQOB (berubah karena rotor 3 berputar)

B = 2

Pada *wiring*, posisi 2 ditempati oleh huruf F. F sendiri pada posisi 5 pada konfigurasi di atas konfigurasi *wiring*. Kita tahu bahwa huruf ke-5 dari susunan alfabet adalah E. Oleh karena itu, hasil dekripsi rotor 3 yaitu **E**.

Dekripsi *Rotor 2* :

ABCDEFGHIJKLMNOPQRSTUVWXYZ

AJDKSIRUXBLHWTMCQGZNPYFVOE (tetap karena rotor 3 belum berputar hingga *turnover notch*)

E = 5

Pada *wiring*, posisi 5 ditempati oleh huruf S. S sendiri ada pada posisi 19 pada konfigurasi di atas konfigurasi *wiring*. Kita tahu bahwa huruf ke-19 dari susunan alfabet adalah S. Oleh karena itu, hasil dekripsi rotor 2 adalah **S**.

Dekripsi *Rotor 1* :

ABCDEFGHIJKLMNOPQRSTUVWXYZ

EKMFLGDQVZNTOWYHXUSPAIBRCJ (tetap karena rotor 2 belum berputar hingga *turnover notch*)

S = 19

Pada *wiring*, posisi 19 ditempati oleh huruf S. S sendiri ada pada posisi 19 pada konfigurasi di atas konfigurasi *wiring*. Kita tahu bahwa huruf ke-19 dari susunan alfabet adalah S. Oleh karena itu, hasil dekripsi rotor 1 adalah **S**.

Dekripsi *Reflector* :

YRUHQSLDPXNGOKMIEBFZCWVJAT

S = 19

Pada konfigurasi, posisi 19 ditempati oleh huruf F. Oleh karena itu, hasil dekripsi reflektor adalah **F**.

Dekripsi *Rotor 1* :

(Hati-hati, prosesnya berkebalikan dengan enkripsi *rotor-rotor* sebelum *reflector*)
ABCDEFGHIJKLMNOPQRSTUVWXYZ
EKMFLGDQVZNTOWYHXUSPAIBRCJ (tetap karena rotor 2 belum berputar hingga *turnover notch*)
F = 6
Pada konfigurasi di atas konfigurasi *wiring* , posisi 6 ditempati oleh huruf F. F sendiri ada pada posisi 4 pada *wiring*. Kita tahu bahwa huruf ke-4 dari susunan alfabet adalah D. Oleh karena itu, hasil dekripsi rotor 1 adalah **D**.

Dekripsi *Rotor 2* :
ABCDEFGHIJKLMNOPQRSTUVWXYZ
AJDKSIRUXBLHWTMCQGZNPYFVOE (tetap karena rotor 3 belum berputar hingga *turnover notch*)
D = 4
Pada konfigurasi di atas konfigurasi *wiring* , posisi 4 ditempati oleh huruf D. D sendiri ada pada posisi 3 pada *wiring*. Kita tahu bahwa huruf ke-3 dari susunan alfabet adalah C. Oleh karena itu, hasil dekripsi rotor 1 adalah **C**.

Dekripsi *Rotor 3* :
BCDEFGHIJKLMNOPQRSTUVWXYZA
DFHJLCPRTXVZNYEIWGAKMUSQOB
C = 3
Pada konfigurasi di atas konfigurasi *wiring* , posisi 3 ditempati oleh huruf D. D sendiri ada pada posisi 1 pada *wiring*. Kita tahu bahwa huruf ke-1 dari susunan alfabet adalah A. Oleh karena itu, hasil dekripsi rotor 1 adalah **A**.

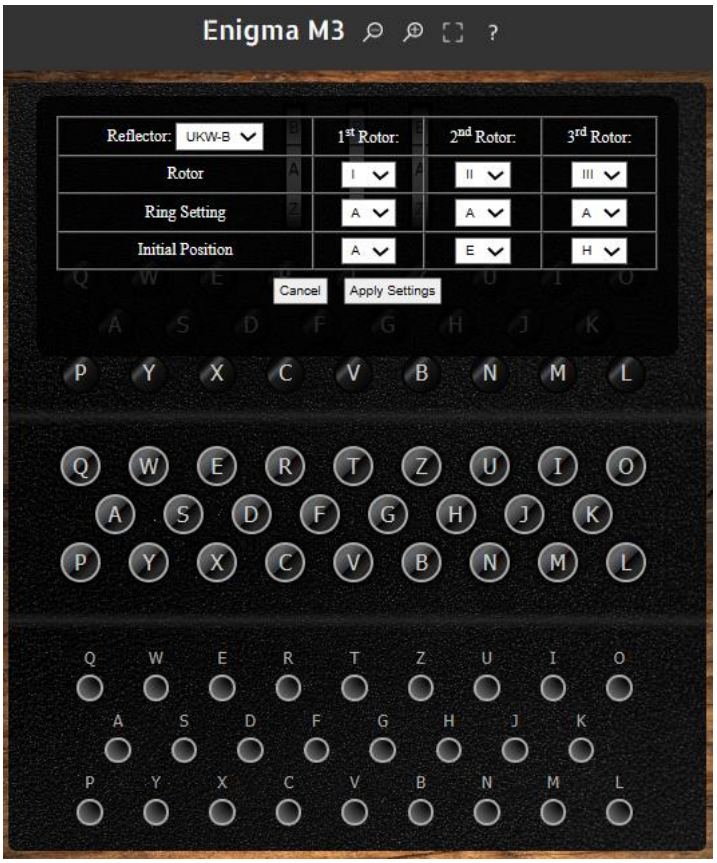
Dekripsi *Plugboard* : **A** (karena tidak ada kabel yang menghubungkan A dengan huruf lain di *plugboard*)

Output : **A**
Jadi, hasil dekripsi dari "**B**" menurut konfigurasi awal yang diketahui adalah "**A**" (hasilnya berkebalikan dengan enkripsi yang dilakukan sebelumnya yang menandakan bahwa pesan berhasil didekripsi).

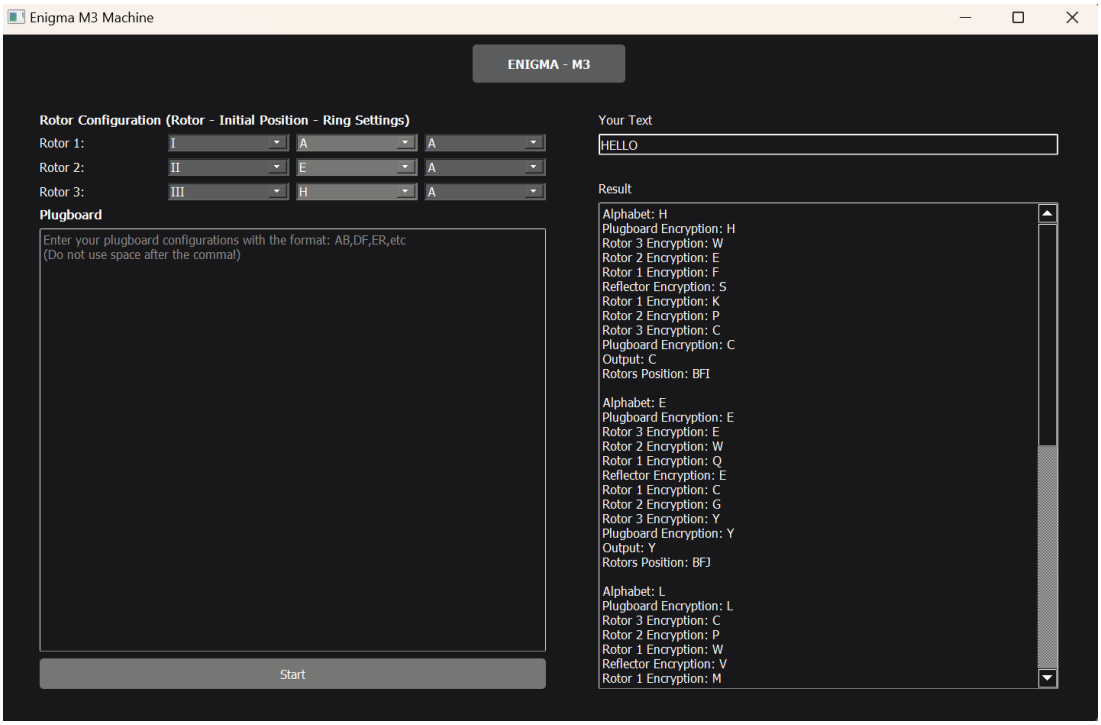
E. Perbandingan Program dengan Enigma di Internet

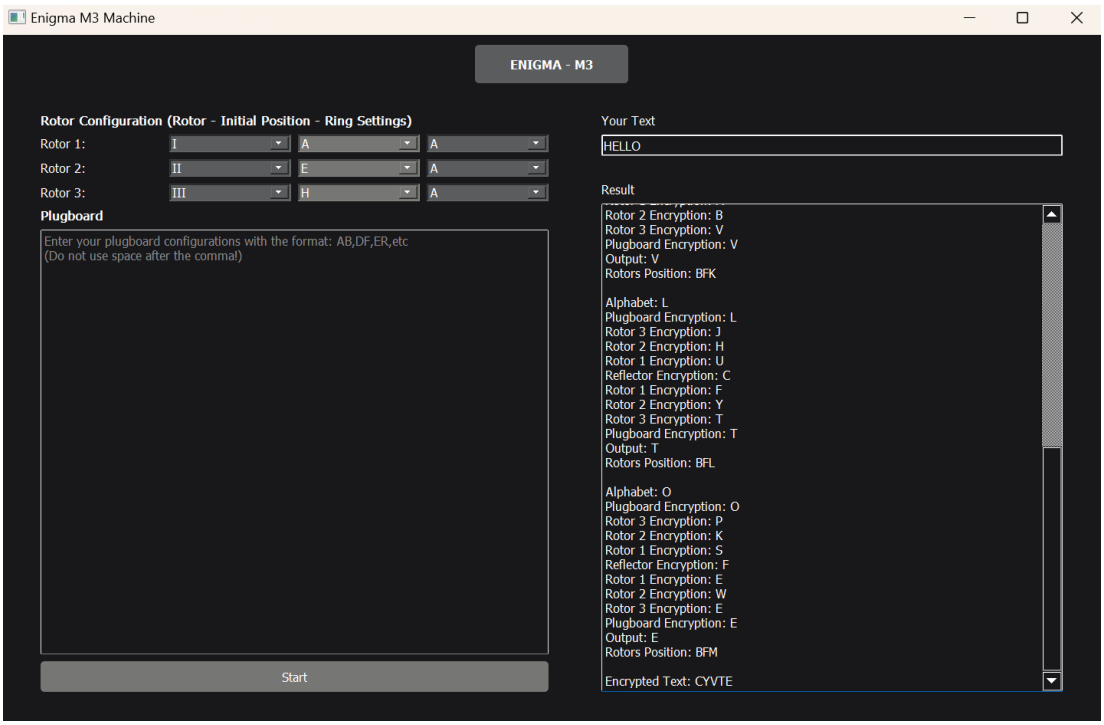
Contoh 1

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



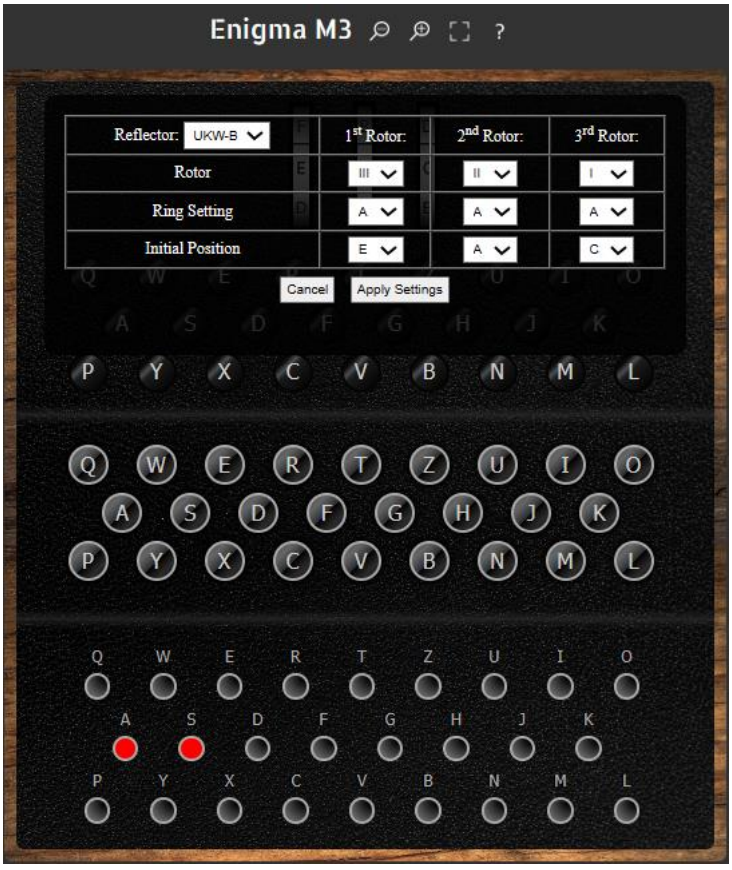
Program Penulis

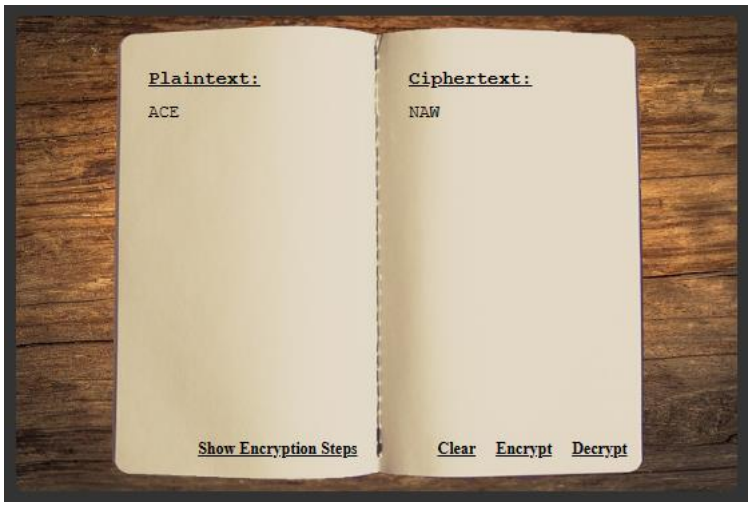




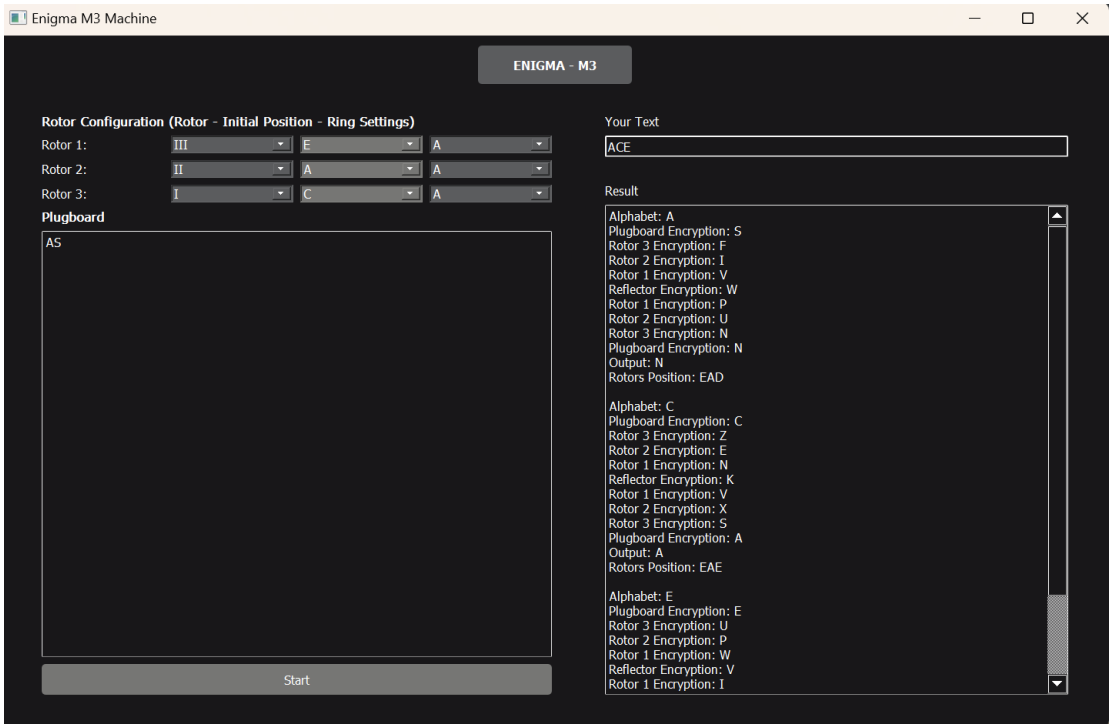
Contoh 2

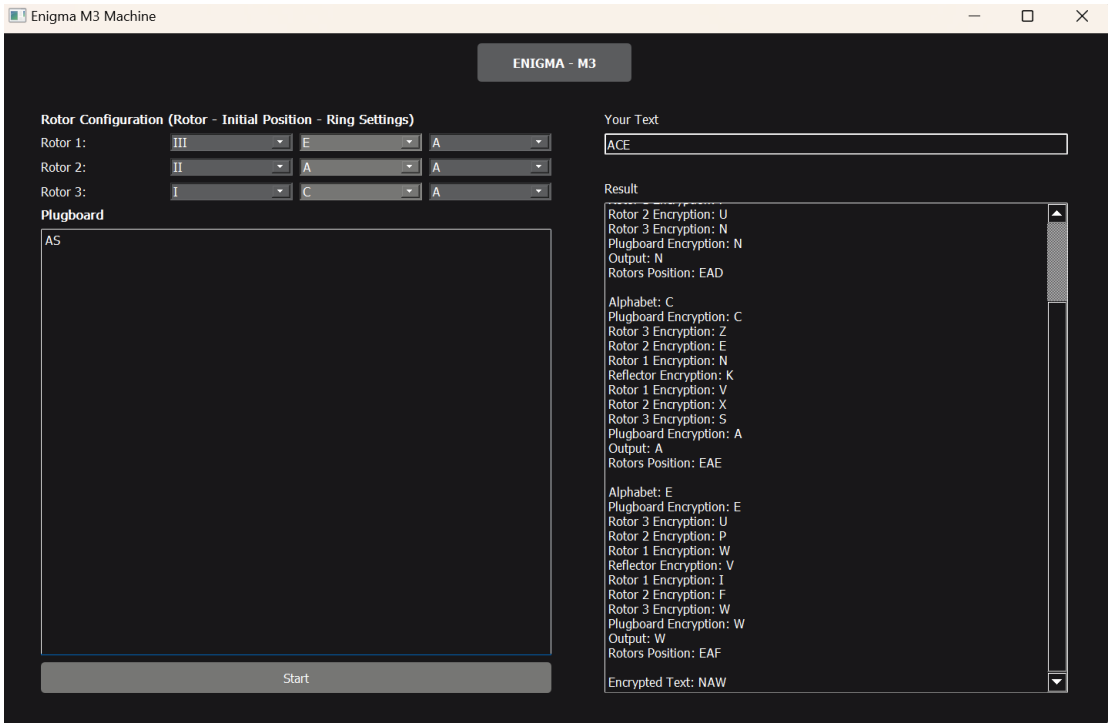
Website: https://www.101computing.net/enigma-machine-emulator/





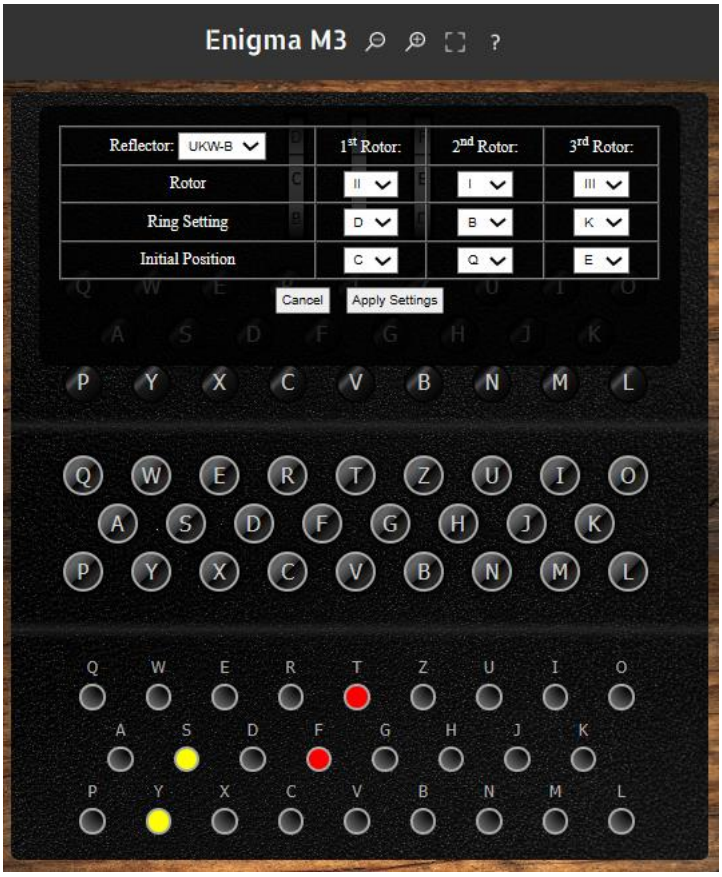
Program Penulis



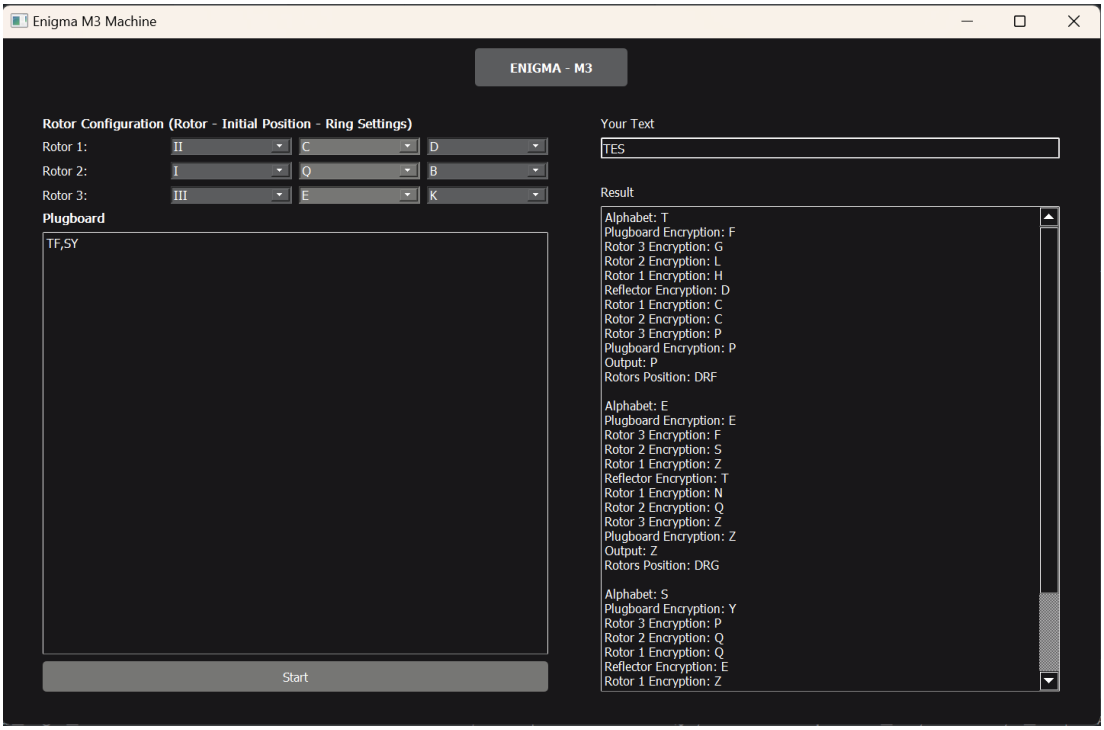


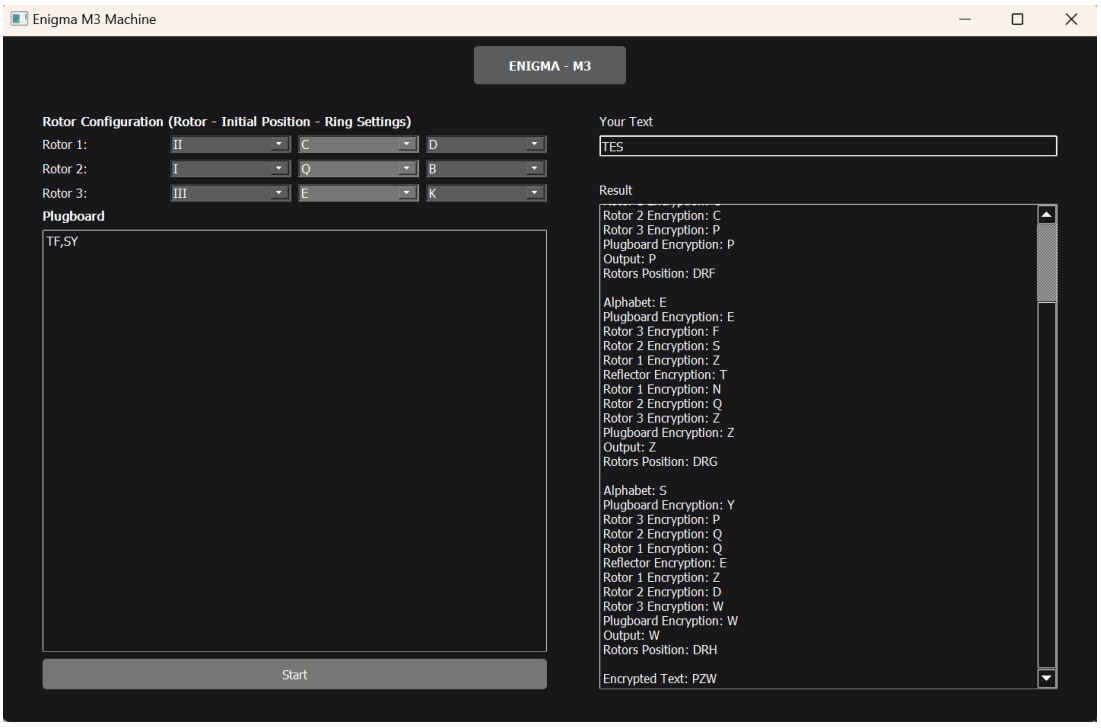
Contoh 3

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



Program Penulis





F. Referensi

Berikut adalah beberapa referensi yang membantu penulis dalam penulisan laporan ini.

- https://history-computer.com/the-complete-history-of-the-enigma-machine/

- https://www.scienceabc.com/innovation/cracking-the-uncrackable-how-did-alan-turing-and-his-team-crack-the-enigma-code.html
- https://www.101computing.net/enigma-machine-emulator/