Perbandingan *Germany Enigma Machine* dengan *Japanese Purple Machine*

Lio Franklyn Kemit - 13509053
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
lio.f.kemit@gmail.com

***Abstract*—Kriptografi sudah dilakukan sejak zaman dahulu. Kriptografi dilakukan bukan hanya dengan mensubstitusi huruf secara manual. Pada perang dunia II, muncul beberapa mesin enkripsi pesan yang digunakan untuk mengenkripsi suatu pesan sebelum disampaikan kepada tujuan. Mesin-mesin enkripsi yang terkenal antara lain *Enigma Machine* yang dibuat oleh Jerman dan *Purple Machine* yang dibuat oleh Jepang. Namun, kedua mesin mempunyai kelebihan dan kekurangannya masing-masing.**

***Index Terms*—Kriptografi, Mesin Kriptografi, *Enigma Machine, Purple Machine*.**

I. PENDAHULUAN

Pada 1900 sebelum masehi dikenal pertama sekali metode untuk menyembunyikan suatu pesan yang sekarang disebut dengan kriptografi. Kriptografi sendiri berasal dari bahasa Yunani, *kriptos*, yang berarti tersembunyi atau rahasia dan *graphein* yang berarti tulisan. Terkadang disebut juga kriptologi. Kriptografi dikenal sebagai ilmu sekaligus juga seni.

Kriptografi yang dikenal saat ini sangat beragam, mulai dari kriptografi klasik hingga kriptografi modern. Kriptografi klasik adalah kriptografi yang sudah digunakan sebelum tahun masehi hingga zaman berubah menjadi zaman digital. Sejak zaman digital, kriptografi dilakukan pada operasi-operasi bit. Kriptograf-kriptografi tersebut disebut kriptografi modern.

Kriptografi mengalami perkembangan paling pesatnya pada masa peperangan. Pada masa peperangan terdapat tuntutan untuk menyampaikan suatu pesan dari satu markas ke markas lainnya tanpa diketahui oleh musuh. Pesan yang dikirim biasanya disampaikan melalui kurir-kurir yang bergerak dengan transportasi yang ada pada zaman dahulu seperti kuda dan perahu. Namun, kejadian yang memungkinkan kurir tersebut tertangkap sulit untuk dihindari. Oleh karen itu, dilakukan usaha untuk membuat pesan tersebut sulit dibaca walaupun berada di tangan musuh.

Terdapat beberapa cara enkripsi pesan pada zaman peperangan tersebut. Enkripsi yang paling sering adalah enkripsi manual secara langsung yang dilakukan oleh manusia. Namun, ada beberapa negara yang melakukan enkripsi dengan menggunakan peralatan tertentu. Penggunaan alat tersebut dimaksudkan agar usaha untuk enkripsi dapat lebih mudah namun lebih aman. Beberapa negara yang menggunakan mesin untuk melakukan enkripsi pesan antara lain Jerman dan Jepang. Kedua negara tersebut dikenal dengan mesin enkripsinya, khususnya pada zaman perang dunia II. Mesin yang diproduksi oleh Jerman disebut dengan *Engima Machine* sedangkan mesin yang diproduksi oleh Jepand disebut dengan *Purple Machine*.

Pada makalah ini akan dilakukan perbandingan terhadap kedua mesin tersebut. Setiap mesin akan dianalisis mekanisme, kelebihan dan kekurangannya. Lalu setiap aspek akan dibenturkan untuk memperoleh kesimpulan berupa mesin mana yang secara keseluruhan lebih unggul dibandingkan mesin lain.

II. KRIPTOGRAFI

Kriptografi adalah ilmu dan seni untuk mejaga kerahasiaan suatu berita. Kriptografi sering dikaitkan dengan bidang keamanan informasi seperti kerahasiaan data, keabsahan data, dll. Dari hal tersebut dirumuskan empat tujuan mendasar dali ilmu kriptografi, yaitu:

- Kerahasiaan, adalah usaha untuk menjaga isi dan informasi dari siapapun yang tidak berhak untuk mengetahuinya.
- Integritas data, adalah berhubungan dengan pengubahan data yang dilakukan secara ilegal.
- Autentikasi, adalah berhubungan dengan identifikasi dari sesuatu sistem atau informasi itu sendiri.
- Non-repudasi, adalah usaha untuk mencegah adanya penyangkalan terhadap suatu informasi.

Kriptografi biasanya dilakukan pada suatu pesan berupa teks. Kemudian pesan tersebut akan diolah dengan mekanisme atau algoritma tertentu untuk mengubah pesan tersebut. Dengan mengubah pesan tersebut, orang lain akan sulit untuk mengenali dan mengerti pesan tersebut. Beberapa elemen yang berperan dalam suatu kriptografi antara lain:

- *Plaintext* : teks pesan yang akan dikriptografi
- *Key* : kunci yang biasanya dipakai untuk

mengenkripsi pesan

- *Ciphertext* : pesan yang sudah dienkripsi

Kriptografi sendiri sudah dimulai dari zaman dahulu kala. Terdapat banyak metode-metode kriptografi yang ditemukan sudah digunakan sejak dahulu. Kemudian seiring perkembangan zaman, muncul berbagai metode kriptografi baru yang bersifat digital. Oleh karena itu, menurut perkembangan zaman kriptografi dibagi menjadi dua, yaitu:

- Kriptografi klasik
- Kriptografi modern

Pada kriptografi klasik terdapat algoritma yang sangat populer digunakan bahkan hingga saat ini. Algoritma tersebut adalah algoritma *cipher* substitusi, selain algoritma *cipher* transposisi. Ide utama dari algoritma ini adalah dengan menggantikan satu huruf pada pesan dan dengan mekanisme atau aturan tertentu huruf tersebut digantikan dengan huruf lainnya.

Salah satu contoh kriptografi klasik dengan algoritma *cipher* substitusi yang sudah ada dari dahulu adalah *Caesar Cipher*. *Caesar Cipher* adalah sebuah algoritma *cipher* substitusi yang dibuat oleh Caesar pada saat peperangan. Cara yang digunakan untuk mengenkripsi pesan pada algoritma ini adalah dengan menggeser huruf yang digunakan sebanyak tiga huruf.

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

Berikut adalah contohnya:

Plainteks: AWASI ASTERIX DAN TEMANNYA OBELIX
Cipherteks: **DZDVL DVWHULA GDQ WHPDQQBA REHOLA**

Berdasarkan metode substitusinya, algoritma *cipher* substitusi dibagi menjadi empat jenis, antara lain:

- *Cipher* abjad tunggal (*monoalphabetic cipher*)
- *Cipher* substitusi hmofonik (*homophonic substitution cipher*)
- *Cipher* abjad majemuk (*polyalphabetic substitution cipher*)
- *Cipher* substitusi poligram (*polygram substitution cipher*)

Keempat jenis algoritma kriptografi substitusi tersebut memiliki keunikan masing-masing. Setiap jenis mempunyai cara untuk enkripsi yang masing-masing. Dan cara yang digunakan untuk mendekripsinya juga berbeda-beda.

Selain dengan menggunakan algoritma yang dibuat atau ditulis secara manual, terdapat juga usaha-usaha lain untuk mengenkripsi pesan. Beberapa negara mengembangan mesin yang digunakan untuk mengenkripsi pesan. Contohnya adalah German dan Jepang.

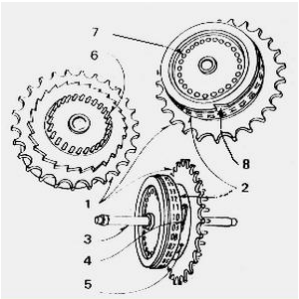
III. ENIGMA MACHINE

A. Sejarah

Enigma adalah sebuah mesin enkripsi pesan yang dikembangakan oleh Jerman. Orang yang pertama sekali membuat Engima adalah seorang perekayasa teknik yang berkebangsaan Jerman pada akhir Perang Dunia I. Model awalnya digunakan secara komersil pada tahun 1920-an. Lalu Enigma diadopsi oleh militer dan servis pemerintahan Jerman pada awal dan selama Perang Dunia II. Lalu beberapa model Enigma diproduksi, namun yang paling sering dibahas adalah Engima yang digunakan oleh militer.

B. Mekanisme

Mesin Enigma ini terdiri atas tiga buah komponen utama yang dibutuhkan untuk menjalankan mesin ini. Komponen pertama adalah papan ketik yang digunakan untuk menerima masukan pesan. Komponen kedua adalah seperangkat cakram berputar yang disebut rotor yang diatur agar saling berjejeran satu dengan yang lain. Komponen ketiga adalah sebuah komponen *stepping* yang beragam untuk memutar satu atau lebih rotor ketika sebuah huruf ditekan pada papan ketik.



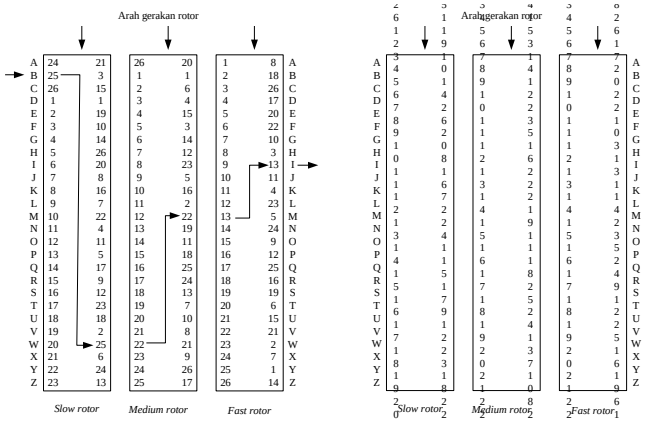
Pada gambar di kanan, terdapat gambaran sederhana tentang rotor yang terdapat pada mesin Enigma. Rotor-rotor tersebut ter diri dari delapan buah elemen penting. Elemen tersebut antara lain :

1. *Finger notch* untuk memutar rotor ke posisi mulai.
2. Cincin huruf yang mengelilingi rotor.
3. Poros dari rotor untuk berputar.
4. Pengunci antara cincin dan rotor.
5. Inti yang terdiri dari simpul antara kontak(6) dan cakram (7). Bagian ini adalah inti untuk pergantian huruf.
6. Per yang berhubungan dengan rotor berikutnya.
7. Sebuah cakram yang bergabung ke inti untuk berhubungan dengan per dan rotor berikutnya.
8. *Notch* Carry yang menyatu dengan cincin huruf.

Pada tahun 1930-an, Enigma hanya mempunyai tiga buah rotor yang berbeda jenis dan diberi nama rotor I, rotor II, dan rotor III. Penyusunan ketiga rotor tersebut memungkinkan enam buah kombinasi urutan yang berbeda pada penyusunan rotor. Namun pada tahun 1938,

German menambahkan rotor IV dan rotor V untuk Enigma. Hal ini menyebabkan terdapat kemungkinan sebanyak 60 kemungkinan untuk menempatkan tiga dari lima buah pilihan rotor ke Enigma. Penempatan rotasi dari ketiga motor pada Enigma juga menjadi salah satu sara konfigurasi untuk mengenkripsi pesan. Biasanya terdapat aturan-aturan tertentu dalam penyusunan rotornya. Berikut adalah salah satu contoh aturan *walzenlage* yang sering digunakan.

Ketiga rotor tersebut akan mengalami perputaran. Perputaran tersebut bertujuan agar setiap kali suatu hruf dienkripsi maka konfigurasi dari Enigma akan berubah. Ketiga rotor tersebut memiliki kecepatan putaran yang berbeda-beda. Rotor kanan adalah rotor yang putarannya paling cepat, rotor tengah adalah rotor yang perputarannya sedang, sedangkan rotor kiri adalah rotor paling lambat. Ketika suatu huruf dimasukkan melalui papan ketik, maka rotor paling kanan akan mengalami rotasi sebesar 1/26 putaran. Ketika rotor kanan sudah mencapai satu putaran penuh, maka rotor tengah akan mengalami putaran juga sebesar 1/26 ketika suatu huruf dimasukkan. Penggambaran putaran pada mesin Enigma dapat dilihat pada gambar berikut.



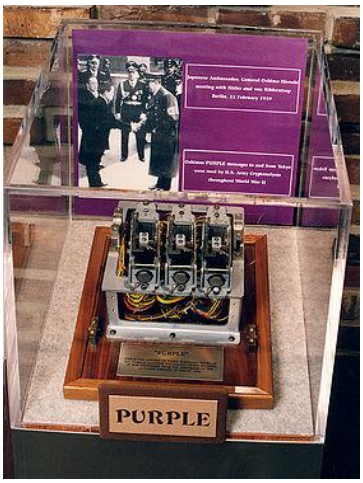
C. Pemecahan

Pada Desember 1932, *Polish Cripto Bureau*, sebuah agensi yang bertugas untuk menangani kriptografi dan kriptanalis, berhasil memecahkan misteri dari mesin Enigma. Kemudian lima hari sebelum pecahnya Perang Dunia II pada 25 Juli 1939, *Polish Cripto Bureau* mempresentasikan teknik dekripsi Enigma yang mereka temukan kepada intelegensi militer Prancis dan Inggris. Berkat hal ini, banyak pesan-pesan rahasia yang berhasil dipecahkan menggunakan Engima.

IV. PURPLE MACHINE

A. Sejarah

Purple machine adalah mesin enkripsi pesan yang dikembangkan oleh Jepang pada awal tahun 1930-an. Di Jepang, mesin ini diberi nama 97-shiki O-bun In-ji-ki, yang berarti mesin ketik huruf'97. Pada saat itu, Jepang membeli Mesin Enigma versi komersil yang diproduksi oleh Jerman. Lalu mesin yang dibeli itu dimodifikasi oleh Jepang dan diberikan nama Red oleh Jepang. Namun karena Signal Intelligence Service pasukan amerika berhasil memecahkannya, Red tidak digunakan lagi oleh Jepang. Kemudian pada tahun 1939, pemerintahan Jepang memperkenalkan sebuah mesin cipher pesan baru yang diberi nama Purple.



B. Mekanisme

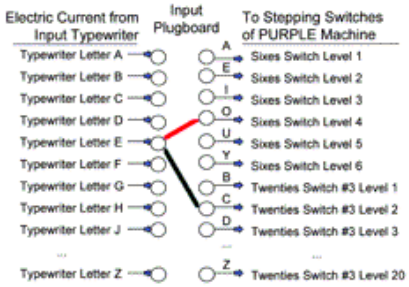
Pruple Machine terdiri atas tiga buah komponen utama. Komponen pertama adalah papan ketik elektronik yang digunakan untuk menerima masukan pesan. Komponen kedua adalah bagian kriptografi yang terdiri dari *plugboard*, empat cincin pengode elektrik, dan beberapa kabel dan saklar yang digabung menjadi satu komponen. Komponen terakhir adalah mesin pencetak yang mencetak pesan yang sudah dienkripsi. Namun Purple Machine tidak menggunakan rotor layaknya Enigma Machine melainkan menggunakan "*stepping-switch* mekanikal elektrik". *Stepping switch* tersebut menghubungkan satu huruf masukan dan 25 keluaran huruf. Sebuah *elektromagnet* tersambung ke *switch* tersebut dan akan mengubah *switch* ke posisi berikutnya ketika sinyal dinyalakan.

Papan ketik untuk menerima *plaintext* dibuat agar dapat menerima tiga jenis huruf, bahasa Inggris, Romanji, dan Roman. Inti dari mesin ini adalah kombinasi dari empat buah *stepping switch* diantara papan ketik dan *plugboard*. *Stepping switch* tersebut akan berubah-ubah secara konstan satu dengan lainnya untuk menciptakan jalur kompleks antara *plaintext* dan *ciphertext*.*Plugboard* adalah bagian yang bekerja sama dengan *stepping switch*

untuk mendiversi huruf dari masukan menjadi keluaran yang dicetak mesin. Bagian ini yang membuat mesin mempunyai tingkat kompleksitas yang besar dan menjadi bagian pusat mekanisme dari mesin.

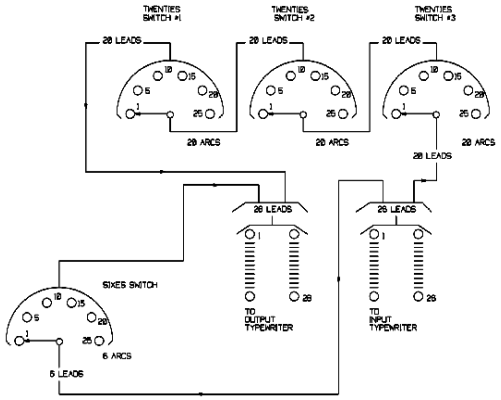
Purple machine membagi 26 huruf menjadi dua bagian, kelompok pertama terdiri dari enam huruf yaitu "AEIOUY" dan kelompok kedua terdiri dari 20 huruf yaitu huruf lainnya(konsonan). Dan pada kedua kelompok huruf tersebut akan diberlakukan algoritma yang berbeda juga.

Pada Purple, *plugboard* masukan dan keluaran akan mengacak huruf yang akan dienkripsi. Masukan apapun dari papan ketik dapat dipasangkan dengan masukan manapun di Purple. Misalnya, jika huruf 'E' diketikkan pada papan ketik dan dipasangkan dengan huruf 'O', maka 'E' akan dienkripsi dengan salah satu dari huruf pada kelompok enam huruf. Sedangkan jika huruf 'E' diketikkan pada papan ketik dan dipasangkan dengan huruf 'C', maka 'E' akan dienkripsi menjadi salah satu dari huruf pada kelompok dua puluh huruf.

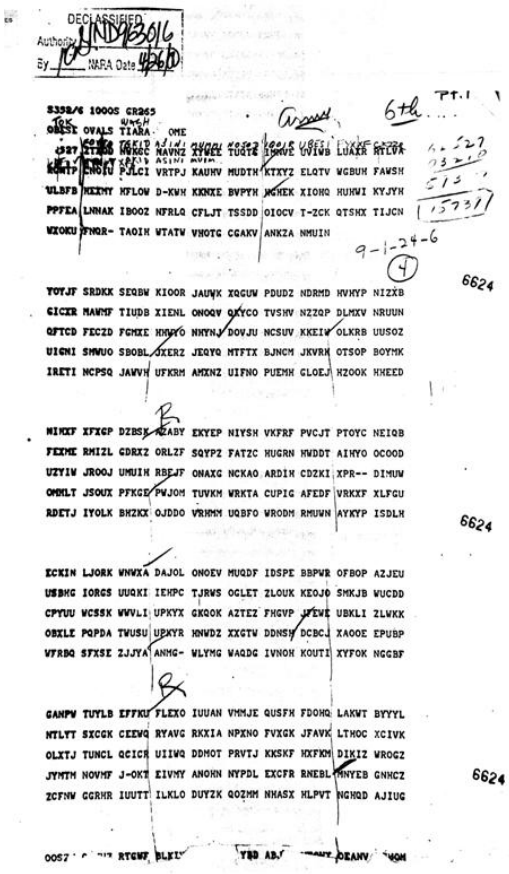


Pada gambar berikut dapat dilihat sebuah diagram skema sederhana dari cara kerja sebuah Purple. Pda gambar tersebut dapat dilihat bahwa dari huruf yang diterima oleh papan ketik masukan dibagi menjadi dua buah bagian, yaitu kelompok enam huruf dan kelompok dua puluh huruf. Keenam huruf tesebut akan dienkripsi oleh 25-posisi *switch* untuk kelompok enam huruf hanya sekali. Setiap posisi dari keenam *swith* tersebut akan menghasilkan satu buah huruf acak. Keenam huruf tersebut akan berlanjut setiap satu buah huruf dienkripsi. Namun, keenam huruf tersebut akan berulang setiap 25 huruf.

Untuk kelompok dua puluh huruf, huruf tersebut akan dienkripsi oleh tiga buah 25-posisi *stepping switch* yang bekerja secara berlanjut seperti layaknya air terjun. Sama seperti *swith* untuk kelompok enam huruf, *switch* ini juga akan berlanjut setiap suatu huruf dienkripsi. Namun, *switch switch switch* yang berputar tidak ketiga-tiganya, namun hanya satu. Ketiga *switch* berputar dengan kecepatan yang berbeda, lambat, sedang, dan cepat. Ketika *swich* yang cepat berputar sebanyal satu periode penuh, maka *switch* yang sedang akan berputar satu kali. Dan begitu juga untuk *swith* cepat bergerak sesuai dengan *switch* sedang. Dengan mekanisme ini, huruf pada kelompok dua puluh huruf tidak akan mengalami pengulangan hingga 25x25x25 kali yaitu sebanyak 15.625 huruf telah dienkripsi dengan alat ini.



Berikutnya, akan dibahas salah satu contoh pesan yang telah didekripsi. Pesan ini merupakan bagian satu dari suatu pesan yang dikirim oleh oemerintahan Jepang ke Sekretaris US pada 7 Desember 1941.



Pada pesan tersebut dapat dilihat beberapa petunjuk untuk mendekripsi pesan tersebut, antara lain:

- "6th" adalah tanggal pengiriman pesan
- "ARMY" penanda bahwa pesan dituju ke tentara amerika
- "Pt.1 " berarti pesan tersebut adalah bagian pertama dari pesan
- "15739" adalah indikator dari pergerakan, yang memberitahu tujuan dimana mengatur *switch* sebelum melakukan decipher pada pesan.
- "9-1-24-6" merepresentasikan posisi mulai untuk *switch* kelompok enam huruf dan ketiga *switch* kelompok dua puluh huruf.

- "4" berarti *motion switch.*

Dengan catatan-catatan berikut dapat didekripsi pesan dengan menggunakan mesin Purple yang sebelumnya sudah dikonfigurasi sesuai dengan petunjuk yang ada.

Berikut adalah hasil dekripsi dari pesan di atas:

> *NARA. RG457 NSA Historical Cryptographic Collection*. Copies of Messages 901, 902, 907 and 910 from Tokyo to Wash On 6 and 7 Dec 41. *NR. 1815, Box 738.*

C. Pemecahan

Pada tahun 1929, pasukan Amerika menyewa William F. Friedman, seorang figur pemimpin pada bidang kriptanalisis untuk memecahkan Purple. Mereka harus memecahkan Purple dengan lima buah pesan yang berhasil direbut. Setelah 18 bulan bekerja memecahkan Purple, Friedman mengalami keterpurukan mental dan harus istirahat sementara dari tugas tersebut. Namun, dia tetap membantu timnya untuk memecahkan Purple. Dan akhirnya pada Agustus 1940, SIS berhasil membuat delapan buah replika Purple. Namun mereka masih punya kendala untuk memperoleh kunci dalam memecahkan pesan tersebut.

V. PERBANDINGAN

Dalam membandingkan mesin Enigma dan Purple, akan dilakukan analisis pada beberapa aspek, antara lain:

1. Mekanisme kerja mesin

   Pada mesin Enigma, mekanisme kerja mesin yang digunakan dalam mengenkripsi pesan dapat digolongkan tidak terlalu kompleks. Pada Enigma digunakan tiga buah motor yang berputar dengan aturan tertentu. Selain itu, adanya kemungkinan untuk mengubah urutan rotor menyebabkan mekanisme akan lebih sulit, namun Enigma berhasil mewarakan solusi untuk kemudahan permasalahan tersebut.

   Pada mesin Purple, mekanisme kerja mesin dapat digolongkan lebih kompleks. Hal ini dikarenakan selain terdapat tiga buah rotor layaknya Enigma, terdapat juga satu buah rotor untuk fungsi tertentu. Selain itu, terdapat pengelompokan huruf menjadi kelompok enam huruf dan kelompok dua puluh huruf membutuhkan mekanisme yang lebih. Dan terakhir, pada Purple tidak ada kemungkinan untuk mengubah urutan rotor, sehingga pada bagian ini mekanismenya lebih mudah.

   Dari hasil analisis diatas, dapat disimpulkan mekanisme kerja mesin Enigma lebih baik daripada mekanisme kerja mesin Purple.

2. Kompleksitas

   Pada mesin Enigma, kemungkinan pengaturan dari sebuah Enigma dapat dihitung dengan menggabungkan kombinasi dari kemungkinan pemosisian tiga buah rotor, kemungkinan pemosisian awal dari rotor, pemosisian cincin, dan kombinasi 10 pasang dari 26 huruf pada *plugboard*. Jika seluruh kemungkinan diatas digabungkan maka, kemungkinan kombinasi pengaturan Enigma adalah sejumlah:

   60 x 17,576 x 676 x 150,738,274,937,250

   Yaitu sejumlah 107,458,687,327,250,619,360,000.

   Pada mesin Purple rotor yang digunakan berjumlah empat namun tidak ada kemungkinan untuk mengubah posisi rotor, oleh karena itu mesin Purple mempunyai kombinasi pengaturan sejumlah:

   6x15625x676x150,738,274,937,250

   Yaitu sejumlah 9,553,038,174,148,218,750,000.

   Dari hasil perhitungan di atas, dapat disimpulkan bahwa dari aspek kompleksitas, mesin Enigma mempunyai angka yang lebih tinggi daripada mesin Purple.

3. Usaha pemecahan

   Jika dilihat dari sejarahnya, mesin Engima pertama sekali dibuat pada tahun 1920. Kemudian untuk pertama kalinya berhasil dipecahkan pada tahun 1932. Dari hal tersebut dapat dilihat bahwa usaha pemecahan Enigma membutuhkan waktu sekitar 12 tahun.

   Pada mesin Purple, mesin ini diciptakan pertama sekali pada tahun 1930 dan berhasil dipecahkan pada tahun 1940 untuk pertama kalinya. Dari hal tersebut dapat dilihat bahwa usaha untuk memecahkan Purple membutuhkan waktu sekitar 10 tahun.

   Dari kedua fakta di atas, dapat disimpulkan dari aspek usaha pemecahan, mesin Enigma lebih sulit untuk dipecahkan daripada mesin Purple.

4. Tambahan
   a. Mesin Purple lebih berat daripada Mesin Enigma sehingga pada saat perang sulit untuk dibawa.
   b. Mesin Enigma memiliki nilai originalitas yang lebih karena mesin Purple dikembangkan dengan mesin Enigma sebagai dasarnya.

Dari analisis yang ada di atas, dapat disimpulkan bahwa secara umum mesin Enigma yang dibuat oleh Jerman lebih baik dari mesin Purple yang dibuat oleh Jepang baik dari segi mekanisme, performansi, kompleksitas, dan beberapa aspek lainnya.

VI. UCAPAN TERIMA KASIH

Pertama sekali penulis mengucapakan terima kasih kepada Tuhan, karena hanya berkat pertolongannyalah penulisan makalh ini dapat diselesaikan. Penulis juga mengucapakan terima kasih kepada Bapak Rinaldi Munir sebagai dosen kriptografi yang sudah mengajar kriptografi kepada penulis. Terakhir penulis mengucapkan terima kasih atas berbagai dukungan kepada penulis atas segala bantuan yang diperolehnya.

REFERENSI

[1] Balciunas, Marijus(2004). *Japan's Purple Machine*.
[2] O'Hara, Jonathan(2010). *The Purple Machine.*
[3] http://ciphermachines.com
[4] http://en.wikipedia.org/wiki/Purple_(cipher_machine)
[5] http://en.wikipedia.org/wiki/Enigma_machine
[6] http://www.hut-six.co.uk

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 19 Maret 2012

Lio Franklyn Kemit/13509053