DESAIN, ANALISIS, DAN PEMECAHAN KODE MESIN ENIGMA

Dominikus D Putranto - 13506060

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : dominikus.d.putranto@gmail.com

Abstrak

Makalah ini akan mengkaji masalah desain dari Mesin Enigma, bagaimana pihak Jerman membuatnya sedemikian rupa sehingga dapat menjadi mesin kriptografi yang dapat mengenkripsi pesan sedemikian rupa sehingga sangat sulit untuk dipecahkan. Mulai dari membahas desain metode enkripsi yang dilakukan maupun desain perangkat mesin enigma itu sendiri.

Lalu makalah ini juga akan membahas mengenai bagaimana metode enkripsi dari mesin enigma dapat terpecahkan, langkah-langkah yang dilakukan para kriptografer Polandia untuk memecahkan kode enkripsi mesin Enigma ini, juga mengenai metode dekripsi yang berhasil ditemukan tersebut.

Adapun, makalah ini tidak akan membahas mengenai desain perangkat mesin enigma secara mendetail, dan penggunaan Mesin Enigma dalam Perang Dunia II karena fokus bahasan dalam makalah ini adalah mengenai enkripsi dan kriptanalisis sehubungan dengan Mesin Enigma.

***Kata kunci**: Mesin Enigma, Enkripsi, Dekripsi, Perang Dunia II, Marian Rejewski, Jerzy Rozycki, dan Henryk Zygalski*

1. Pendahuluan

Mesin Enigma (berasal dari kata Latin, *aenigma* yang bermakna teka-teki) adalah sebuah mesin rotor elektromekanik yang digunakan untuk mengenkripsi suatu pesan dan mendekripsikan kembali pesan tersebut. Mesin Enigma dipatenkan oleh seorang insinyur asal Jerman yang bernama Arthur Scherbius, yang kemudian digunakan oleh militer dan pemerintah Jerman Nazi sebelum dan selama Perang Dunia II. Dan kemudian yang paling terkenal adalah versi Mesin Enigma yang dipakai oleh Wehrmacht (angkatan bersenjata Jeman Nazi). Nazi sendiri mulai menggunakan mesin ini sejak tahun 1928.

Pada awalnya Nazi menganggap bahwa Enigma adalah mesin kriptografi teraman di dunia. Namun pihak sekutu terus berusaha keras untuk memecahkan kode cipher yang dihasilkan oleh Enigma, sehingga pada akhirnya, pada tahun 1932, metode dekripsi untuk mesin ini ditemukan oleh tim matematikawan muda yang diberi tugas oleh badan intelijen Polandia yang terdiri dari Marian Rejewski, Jerzy Rozycki, dan Henryk Zygalski. Pihak Nazi yang menyadari hal ini pun mendesain ulang Enigma pada tahun 1939, sehingga metode tersebut tidak dapat digunakan kembali. Namun berbekal metode dari Polandia, Britania dan Perancis berhasil membuat mesin pemecah kode untuk mesin Enigma yang baru ini, yang diperkenalkan dengan nama *bombe*.

Keberhasilan pemecahan kode mesin Enigma ini sendiri terbukti menjadi faktor penting kemenangan Sekutu pada Perang Dunia II, dan berhasil memperpendek lamanya Perang Dunia II.

Adapun jauh sebelum itu, bahkan jauh sebelum adanya komputer, kriptografi serupa telah dilakukan, dan biasanya memang dilakukan dalam rangka menyembunyikan pesan yang dikirim dalam perang.

2. Sejarah Awal Mulanya Enigma

Mesin Enigma yang termasuk dalam mesin kriptografi mekanik-elektrik yang berbasis rotor ini ditemukan oleh seorang Jerman bernama Arthur Scherbius di Berlin pada tahun 1918. Di mana di saat itu orang-orang memang sedang

gemar menggunakan *electrical connection* untuk mengotomastisasi pekerjaan mengkonversi huruf menggunakan tabel. Waktu itu, awalnya Arthur Scherbius ingin memproduksi dan memperjualbelikan secara komersil mesin enigma buatannya itu ke khalayak umum, terutama yang bergerak di bidang bisnis, namun ternyata keadaan berkata lain, karena akhirnya mesin ini dibutuhkan oleh angkatan bersenjata Jerman , dan saat itu memang sedang saatnya Perang Dunia II. Dan angkatan laut Jerman berhasil membuat mesin cipher Shcerbius pada tahun 1926 yang merupakan modifikasi dari enigma versi komersial, dan berhasil membuat enigma versi militer pada tahun 1930. Dan pada akhirnya sejak pertengahan 1930, angkatan bersenjata Jerman hampir semua telah memakai enigma.

Gambar 1 Mesin Enigma

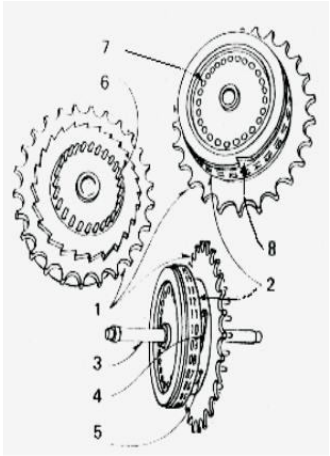
3. Desain dan Mekanisme Enigma

Desain enigma versi militer yang banyak dipakai oleh angkatan bersenjata Nazi terdiri dari bagian-bagian sebagai berikut :

1.Papan ketuk
2. Lampu
3. *Stecker Board*
4. *Scrambler*
5. *Entry Wheel*
6. *Rotor*
7. *Reflector* (*Umkerwalz*)

Gambar 2 Plugboard pada Enigma

Dengan bagian yang paling penting adalah rotor, karena rotorlah mekanisme utama dalam pengenkripsian yang dilakukan :



Gambar 3 Rotor pada Enigma

Adapun bagian-bagian dari rotor tersebut dengan penomoran sesuai dengan gambar di atas adalah :

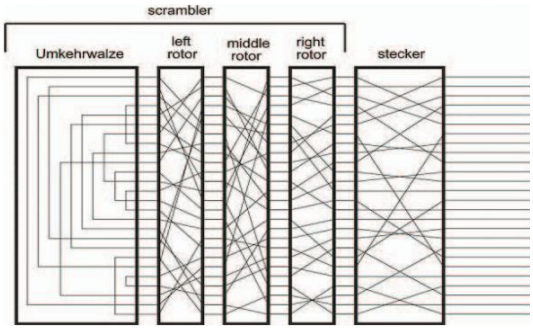
1. nger notches,
2. alphabet ring,
3. shaft,
4. catch,
5. core containing cross-wirings,

6. spring loaded contacts,
7. discs,
8. carry notch.

4. Cara Kerja Enigma

Enkripsi yang dilakukan enigma sebenarnya adalah substitusi, di mana sebuah huruf digantikan dengan tepat sebuah huruf juga, hanya saja substitusi dilakukan beberapa kali. Dan walau hanya dengan substitusi, sebuah pesan akan sulit sekali didekripsi jika tidak dengan alat yang sama, dengan pengaturan posisi yang sama, tipe substitusi yang sama, dan kode kunci yang sama.

Dan semua substitusi tersebut dilakukan dengan *wiring* (sambungan listrik melalui kawat).



Gambar 4 Wiring pada Mesin Enigma

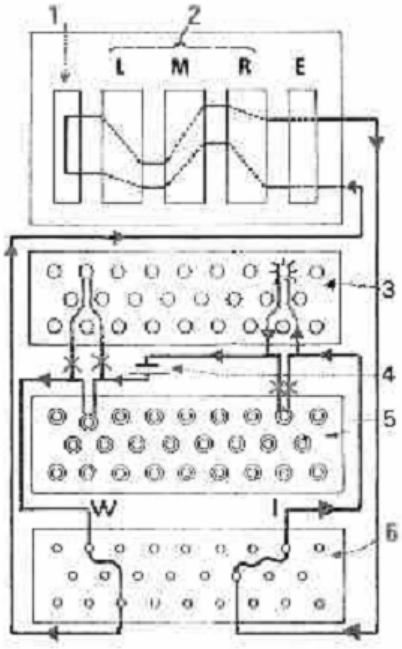
Arti dari wiring tersebut adalah jika misal A pada *left rotor* terhubung dengan D pada *middle rotor*, maka jika A pada *left rotor* teraliri listrik, maka D pada *middle rotor* akan teraliri listrik juga.

Sedangkan secara sederhana cara kerja dari mekanisme wiring tersebut adalah wiring tersebut menunjukkan subsitusi dari tombol yang ditekan, yang dilakukan dengan cara memasang lampu. Jadi misal sesuai contoh di atas jika tombol / saklar A ditekan, maka lampu D akan menyala. Kemudian hal tersebut dilakukan ulang namun dengan mengganti rotor yang sedang digunakan.

Kemudian dilakukan pergeseran pada rotor setiap kali ada tombol yang ditekan. Begitu seterusnya selama pesan diketik.

Dan dengan adanya *reflector* jalannya arus dapat dibalikkan dari *right rotor* ke *left rotor*, yang efeknya adalah kemungkinan yang meningkat 26 kali dari substitusi huruf. Relector ini menyebabkan Enigma tidak perlu mengubah state jika sedang ingin mengenkripsi sebuah pesan ataukah ingin mendekripsikannya.

Namun *Reflector* ini menyebabkan kelemahan pada mesin Enigma ini, di mana terjadi resiprok, di mana jika misal huruf M dienkripsikan menjadi T, maka huruf T akan dienkripsikan menjadi huruf M pada rotor yang sama, dan sebuah huruf tidak akan mungkin bisa dienkripsi menjadi dirinya sendiri.



Gambar 5 Skema Cara kerja Enigma

Sedangkan rotor untuk enigma ada beberapa, walaupun yang dapat dipakai dalah satu waktu pada satu enigma adalah 3 buarh saja, yang diberi nama L (left), M (middle), dan R (right). Sedangkan jenis-jenis rotor yang ada diberi nama rotor I, rotor II, rotor III, dan seterusnya.

Di bawah ini adalah beberapa jenis rotor yang pernah digunakan oleh enigma

Rotor	ABCDEFGHIJKLMNOPQRSTUVWXYZ
I	EKMFLGDQVZNTOWYHXUSPAIBRCJ
II	AJDKSIRUXBLHWTMCQGZNPYFVOE
III	BDFHJLCPRTXVZNYEIWGAKMUSQO

```
IV     ESOVPZJAYQUIRHXLNFTGKDCMWB
V      VZBRGITYUPSDNHLXAWMJQOFECK
VI     JPGVOUMFYQBENHZRDKASXLICTW
VII    NZJHGRCXMYSWBOUFAIVLPEKQDT
VIII   FKQHTLXOCBJSPDZRAMEWNIUYGV
```

Pada setiap rotor tersebut dikenal adanya istilah *Turnover*, yaitu posisi di mana sebuah rotor mulai bergerak menggeser rotor di sampingnya. Rotor R akan selalu bergerak 1 huruf setiap kali tombol ditekan., dan jika *turnover* dari rotor R tersebut adalah S, maka rotor R tersebut akan menggeser rotor M sejauh 1 huruf jika sudah mencapai posisi *turnover*nya (posisi di huruf S). Setiap jenis rotor mempunyai *turnover* masing-masing.

Adapun peran besar juga disumbangkan oleh plugboard. Plugboard sendiri adalah sebuah papan yang mengganti arus dari huruf awal ke huruf yang diinginkan dengan cara meneruskan arus tersebut dengan kabel. Seperti yang terlihat di Gambar 2, di situ terlihat bahwa huruf A dihubungkan dengan huruf J, dan huruf S dihubungkan dengan huruf Q, jadi semua A, akan menjadi J, dan sebaliknya demikian juga, semua huruf J akan berubah menjadi huruf A. Hal tersebut juga terjadi antara huruf S dan huruf Q.

5. Enkripsi Pada Enigma

Sebenarnya yang terjadi pada enigma pada sebuah enkripsi yang dia lakukan adalah sebuah permutasi panjang :

$$E = P\,R\,M\,L\,U\,L^{-1}M^{-1}R^{-1}P^{-1}$$

Dengan R adalah *right rotor*, M adalah *middle rotor*, L adalah *left rotor*, P adalah *plugboard*, dan U adalah *reflector*. Dan E adalah hasil enkripsinya.

Dan semuanya itu ditentukan oleh ketetapan yang ditentukan Jerman berbeda-beda untuk setiap jaringan yang ada dan untuk setiap harinya. Dan kesemuanya itu ditentukan Jerman dengan cara memberikan sebuah buku sebagai standar untuk masing-masing operator. Adapun hal-hal yang diatur adalah : pilihan rotor dan peletakan posisi dari rotor-rotor tersebut, pemilihan huruf awal dari setiap rotornya, posisi plug pada plugboard, dan tipe reflector yang digunakan.

Misal pada suatu hari standar yang disebarkan oleh kurir-kurir Jerman ke setiap operator enigma mereka adalah sebagai berikut

25

I III V

B M X

DM OA MR IS NE IL KI UN

Maka kode tersebut dikeluarkan pada tanggal 30 pada bulan itu, kemudian rotor yang digunakan untuk *left rotor* adalah I, untuk *middle rotor* adalah III, dan kemudian untuk *right rotor* adalah V. Dan baris berikutnya adalah posisi awal untuk masing-masing rotor, jadi B adalah posisi awal dari rotor I, M adalah posisi awal dari rotor kemudian baris terakhir menentukan huruf-huruf apa saja yang perlu disambungkan pada plugboard. Jadi untuk contoh ini huruf D dihubungkan dengan M, huruf O disambungkan dengan A, dan seterusnya.

6. Pemecahan Kode Mesin Enigma

Kode hasil enkripsi mesin enigma yang telah serumit itu dan bahkan diklaim oleh Jerman tidak mungkin dipecahkan tersebut ternyata tetap saja mempunyai kelemahan-kelemahan yang pada akhirnya berakhir pada terpecahkannya kode enkripsi tersebut oleh pihak musuh.

Kelemahan tersebut antara lain :

1. Fakta bahwa sebuah huruf tidak dapat dipetakan ke huruf itu sendiri, contohnya misal huruf ‘A’ sebagai input tidak mungkin menghasilkan huruf ‘A’ juga; sebagai output.

2. Operator harus melakukan setting untuk mendapatkan *initial value*. Di mana di kasus-kasus tertentu, hal tersebut dapat terprediksi, dan kesalahan yang umum dilakukan oleh operator-operator tersebut adalah dalam memilih nilai yang dapat dengan mudah diprediksi sebagai *initial value*.

3. Penyandian bersifat resiprok, jadi bila huruf ‘A’ disandikan menjadi huruf ‘Z’, maka huruf ‘Z’ akan disandikan menjadi huruf ‘A’.

4. Kunci pesan dikirimkan 2 kali.

5. Posisi turnover pada setiap rotor unik, sehingga memungkinkan untuk ditebak rotor mana saya yang digunakan.

6.1. Metode Permutasi Marian Rejewski

Marian Rejewksi adalah seorang matematikawan asal Polandia yang memang ditugaskan untuk memecahkan kode enigma. Saat itu Rejewski bisa mendapatkan pesan-pesan terenkripsi Jerman dengan menyadap sinyal komunikasi radio tentara Jerman. Sampai akhirnya dia berhasil mendapatkan 6 buah pesan terenkripsi pada hari yang berbeda. Dan dapat disusun dalam persamaan permutasi sebagai berikut :

$$\mathbf{A = S\,H\,R'\,T'\,R'^{-1}\,H^{-1}\,S^{-1}}$$
$$\mathbf{B = S\,H\,Q\,R'\,Q^{-1}\,T'\,Q\,R'^{-1}\,Q^{-1}\,H^{-1}\,S^{-1}}$$
$$\mathbf{C = S\,H\,Q^{2}\,R'\,Q^{-2}\,T'\,Q^{2}\,R'^{-1}\,Q^{-2}\,H^{-1}\,S^{-1}}$$
$$\mathbf{D = S\,H\,Q^{3}\,R'\,Q^{-3}\,T'\,Q^{3}\,R'^{-1}\,Q^{-3}\,H^{-1}\,S^{-1}}$$
$$\mathbf{E = S\,H\,Q^{4}\,R'\,Q^{-4}\,T'\,Q^{4}\,R'^{-1}\,Q^{-4}\,H^{-1}\,S^{-1}}$$
$$\mathbf{F = S\,H\,Q^{5}\,R'\,Q^{-5}\,T'\,Q^{5}\,R'^{-1}\,Q^{-5}\,H^{-1}\,S^{-1}}$$

Dengan S adalah permutasi yang berasal dari plugboard, H adalah permutasi yang berasal dari hubungan antara socket pada plugboard dengan mesin, T adalah permutasi rotor, dan kemudian yang terakhir, Q adalah permutasi sederhana yang memetakan sebuah huruf menjadi huruf berikutnya.

Persamaan yang terdiri dari 6 persamaan dan 4 buah permutasi yang tidak diketahui tersebut tidak dapat terpecahkan, sampai pada saatnya Rejewksi berhasil mendapat bantuan berupa tabel kunci harian untuk bulan September dan Oktober 1932. Yang kemudian memberi petunjuk pada Rejewksi dalam memecahkan kode enigma.

6.2. Metode Grill

Metode ini adalah metode yang merupakan kelangsungan dari penemuan Rejewski. Yang mendekripsi pesan berdasarkan persamaan permutasi yang telah ditemukan oleh oleh Rejewski, dan akhirnya dengan mengetahui kebiasaan bahwa 3 huruf pertama kunci biasanya diset berjauhan oleh operator, akhirnya keenam persamaan permutasi tersebut dapat terpecahkan.

Adapun urutan dari hal-hal yang dapat dipecahkan oleh Metode ini adalah pilihan roda kanan, kombinasi dari plugboard, baru kemudian posisi dari roda tengah dan kiri. Yang kesemuanya ini didapatkan dari percobaan ribuan kalo yang dilakukan untuk memecahkan kode enigma ini.

6.3. Metode Lembar Berlubang Zygalski

Metode ini berdasar fakta bahwa dari semua kemungkinan posisi rotor, 40% pasti permutasi AD. Yang kemudian berkahir dengan ditemukannya posisi roda pada setiap siklus. Namun pada akhirnya metode ini tidak berhasil untuk digunakan, karena banyaknya waktu dan biaya yang dibutuhkan untuk membuat kertas berlubang untuk setiap kombinasi roda.

6.4 Metode Katalog Karakteristik

Metode ini didasarkan pada fakta bahwa permutasi AD, BE, dan CF tidak ditentukan oleh kombinasi plugboard, dan hanya ditentukan oleh posisi-posisi roda rotor yang digunakan. Yang kemudian dapat dimodelkan dalah bentuk permutasi disjungtif :

$(a_1a_2a_3a_4a_5a_6a_7a_8a_9a_{10}a_{11}a_{12}a_{13})$
$(b_1b_2b_3b_4b_5b_6b_7b_8b_9b_{10}b_{11}b_{12}b_{13})$

Dan setiap huruf dipetakan ke hurud berikutnya, dengan a_{13} dipetakan kembali ke a_1.

6.4 Bombe

Alat yang dibuat oleh Alan Turing dari Inggris ini dirancang supaya walau Jerman mengubah standar operasi mereka, dengan teknik-teknik yang sudah ditemukan, tetap dapat memecahkan kode dari mesin enigma.

Hal yang mendasari kerja bombe adalah sifat yang disebabkan oleh reflector pada mesin enigma, di mana terjadi enkripsi yang resiprok, yang kemudian berhasil diturunkan sehingga posisi dari roda-roda tersebut dapat ditebak dengan memperhitungkan hal tersebut, hanya saja waktu yang diperlukan cukup lama jika dilakukan secara manual seperto sebelum-sebelumnya.

Maka dibuatlah bombe sebagai alat mekanik untuk mengotomatisasi pekerjaan tersebut.

7. Kesimpulan

Enigma adalah sebuah mesin enkripsi yang hanya menggunakan substitusi, namun karena dilakukan dalam sebuah rangkaian dan dengan bermacam-macam cara setiap substitusi dilakukan, maka enkripsi yang dihasilkan sangatlah bagus, bahkan sampe pihak Jerman waktu itu meyakini bahwa kode tersebut tidak mungkin dipecahkan oleh siapapun.

Dan akhirnya kode tersebut dapat dipecahkan, walaupun dengan memakan waktu yang sangat lama dan usaha yang luar biasa. Jadi dapat disimpulkan bahwa semua teknik enkripsi dapat dikuak, dan kode hasil enkripsi tentu saja dapat dipecahkan. Tidak ada kode enkripsi yang tidak dapat dipecahkan.

8. Daftar Pustaka

[1] Gaj, Kris, and Arkaiusz Orlowski. (2003). Facts and Myths of Enigma : Breaking Stereotypes.

[2] Munir, Rinaldi. (2004). Bahan Kuliah IF1504 Kriptografi. Departemen Teknik Informatika, Institut Teknologi Bandung.

[3] Rejewski, Marian. (1980). An Application of the Theory of Permutations in Breaking the Enigma Cipher.

[4] Shingleton, Tyler. Enigma Machine:Design and Analysis

[5] Tuma, Jiri. (2003). Permutation Groups and the Solution of German Enigma Cipher