Aplikasi Kriptografi dalam Mesin Enigma, Pengenkripsi Pesan Tentara Jerman pada Perang Dunia

Adi Purwanto Sujarwadi – NIM : 13506010
Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha No. 10 Bandung
e-mail : if16010@students.if.itb.ac.id

Abstract *– Makalah ini membahas tentang aplikasi dari ilmu kriptografi dalam perang dunia . Kriptografi digunakan untuk mengirimkan pesan rahasia agar tidak dapat dibaca oleh pihak musuh. Dengan mengaplikasikan ilmu kriptografi, maka pesan yang dikirim berupa plaintext dapat diubah menjadi chipertext sehingga meningkatkan tingkat keamananya. Dalam perang dunia II, pasukan Jerman mengirimkan pesan melalui sebuah mesin enkripsi yang diberi nama mesin Enigma.*

Kata Kunci*: Mesin Engima, Kriptografi, enkripsi,, dekripsi*

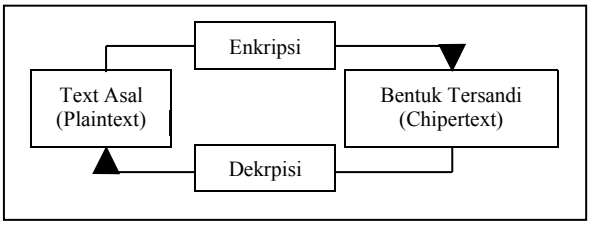
1. PENDAHULUAN

Dalam suatu perang, komunikasi merupakan salah satu factor penting yang dapat menentukan keberlangsungan perang. Seringkali informasi yang dikirimkan bersifat sangat rahasia sehingga akan sangat berbahaya jika diketahui pihak musuh. Untuk itulah diciptakan metode sedemikian rupa untuk mengenkripsi pesan tersebut agar tidak dapat dibaca oleh musuh. Atas dasar alasan tersebut, setiap pihak dalam perang menciptakan teknik enkripsi masing-masing. Dalam perang dunia, teknik enkripsi yang sangat terkenal, digunakan oleh tentara Jerman ialah Mesin Enigma, yang diciptakan oleh Arthur Scherbius pada tahun 1918.

2. ENKRIPSI MESIN ENIGMA

Pada dasarnya, tujuan dari enkripsi ialah untuk menyembunyikan pesan (data atau informasi) dari pihak yang tidak berkepentingan dengan cara menyamarkannya menjadi bentuk tersandi yang tidak mempunyai makna.

Secara garis besar, proses enkripsi dapat digambarkan oleh ambar 2.1 berikut ini :



Gambar 2.1 Proses Enkripsi dan Dekripsi

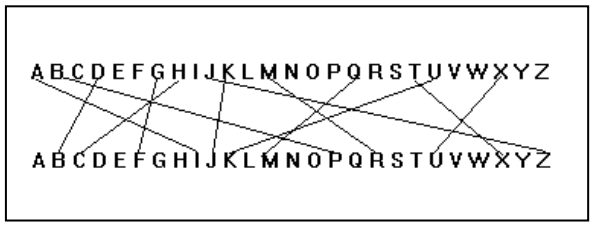
Mesin Enigma yang merupakan mesin pengenkripsi pesan, diciptakan oleh pihak Jerman berdasarkan metode enkripsi tersebut. Konsep dasar dari enkripsi mesin ini, ialah dengan menggunakan metode *Caesar chipper*, yaitu dengan mensubtitusi huruf dengan huruf lainnya.

Contoh dari *Caesar chipper*:
Plaintext : A B C D E F G
Chipertext : E F G H I J K

Pesan tersebut dienkripsi dengan menukarkan tiap huruf alphabet dengan empat huruf berikutnya dalam susunan alphabet. Dengan mengkodekan huruf alphabet dengan integer A=0…Z=25, maka secara matematis dapat dituliskan $(c_i=E(p_i)=(p_i+4) \bmod 26)$.

Namun cara enkripsi seperti ini sangatlah tidak aman, enkripsi tersebut mudah dipecahkan, karena hanya ada 26 kemungkinan kunci dari enkripsi tersebut (26C1).
Oleh karena keperluan perang yang membutuhkan teknik enkripsi yang jauh lebih kuat dari *Caesar chipper* tersebut, maka pada tahun 1918, seorang Jerman bernama Arthur Scherbius menemukan metode enkripsi yang lebih efisien, yang menjadi dasar utama dalam enkripsi mesin enigma.

Ide dari Arthur yang pertama ialah dengan menukar suatu huruf menjadi huruf lainnya dengan urutan acak. Urutan ini dibuat dengan cara menghubungkan suatu kabel dengan kabel lainnya dalam suatu system elektronis.

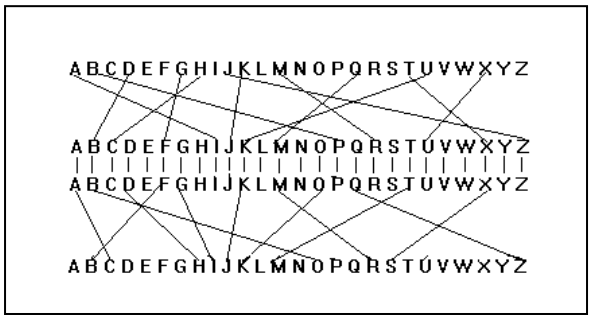


Gambar 2.2 Proses Penukaran Huruf

Gambar 2.2 menunjukkan enkripsi yang dimaksudkan tersebut. Dimana misalkan huruf “B” pada terminal asal, akan dihubungkan dengan huruf “P” pada terminal penerima. Dengan demikian, tercipta suatu metode enkripsi secara acak yang lebih sulit untuk dipecahkan. Namun, metode seperti ini tetaplah belum dapat memenuhi tingkat standar keamanan seperti yang disyaratkan dalam sebuah perang. Enkripsi seperti ini masih terlalu mudah untuk dipecahkan

pihak musuh, karena dengan menganalisis beberapa kata, dapat ditemukan suatu pola yang pada akhirnya akan dapat digunakan untuk mengubah kembali chipertext menjadi plaintext.

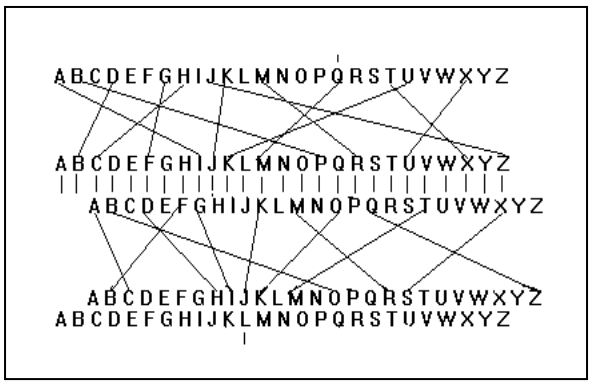
Untuk membuat sandi lebih sulit lagi untuk dipecahkan, Tuan Arthur melakukan enkripsi lagi dari huruf-huruf yang telah terenkripsi. Dengan demikian, akan menjadi lebih sulit lagi bagi para kriptoanalis pihak lawan untuk memecahkannya.



Gambar 2.3 Proses Enkripsi Ganda

Metode enkripsi dengan subtitusi ganda seperti pada gambar 2.3 bekerja dengan cara kembali mengenkripsi chipertext menjadi bentuk chipertext lainnya. Sebagai contoh, huruf "U" yang telah dienkripsi menjadi huruf "K", kembali dienkripsi menjadi "J" dengan teknik subtitusi acak seperti pada gambar 2.2. Enkripsi ini memberikan keamanan yang lebih tinggi dari enkripsi tunggal, namun tetap belum dapat memberikan tingkat keamanan yang diperlukan dalam sebuah perang.

Untuk menciptakan teknik enkripsi yang lebih rumit, Arthur menggabungkan teknik subtitusi ganda tersebut dengan metode *Caesar chipper*, dimana sebelum melakukan enkripsi kedua, terlebih dahulu dilakukan pergeseran huruf dengan menggunakan teknik *Caesar chipper*.

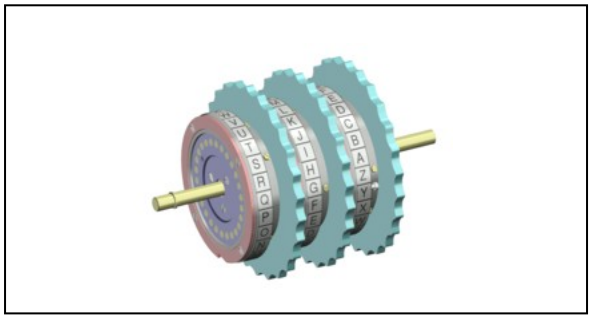


Gambar 2.4 Proses Enkripsi Kombinasi

Dengan menerapkan proses enkripsi ganda yang dikombinasikan dengan metode *Caesar chipper* tersebut, didapatkan sebuah teknik enkripsi dengan keamanan yang sangat tinggi. Hal ini disebabkan oleh setiap pergeseran pada *Caesar chipper*, akan mengakibatkan kombinasi huruf yang sangat berbeda, sehingga akan sulit dipecahkan oleh kriptoanalis dari pihak lawan.

3. CARA KERJA

Untuk dapat merealisasikan teknik enkripsi seperti yang telah dibahas dalam bab 2, Mesin Enigma menggunakan beberapa buah roda yang dihbungkan dengan benda semacam cincin bertuliskan huruf yang digunakan untuk menciptakan hasil yang berbeda dari tiap huruf yang digunakan.. Pengacakan huruf diperoleh dari pergeseran gigi roda antara roda yang satu dengan roda lainnya. Dengan menggunakan kombinasi n buah roda, mesin enigma memiliki 26^n buah kombinasi pengacakan huruf yang diperoleh dari tiap roda memiliki n buah huruf alphabet.



Gambar 3.1 Roda pada mesin Enigma

Dalam penembangannya, seorang matematikawan Jerman bernama Will Korn, menambahkan sebuah komponen yang dinamakan reflector pada mesin enigma. Komponen ini bekerja secara sederhana, dengan cara menukarkan suatu huruf yang merupakan hasil enkripsi kombinasi, dengan huruf lainnya (misalkan menukar huruf "A" dengan "E"), yang kemudian akan dikirimkan kembali melalui tiga roda tersebut dengan teknik berlawanan dengan yang telah digunakan sebelumnya, pengirimian pesan kembali secara kebalikan ini juga berfungsi agar pengirim pesan dapat memeriksa kembali pesan yang telah ia kirimkan. Penggunaan reflector ini memberi beberapa keuntungan, di antaranya ialah tidak ada huruf yang akan terdekripsi menjadi dirinya sendiri, dan mesin enigma dapat melakukan enkripsi dan dekripsi tanpa perlu melakukan pengaturan ulang.

Pada awalnya, penambahan kekuatan enkripsi mesin enigma hanya dilakukan dengan penambahan roda. Namun, penambahan roda tersebut tidak terlalu memberikan dampak yang signifikan pada kekuatan enkripsi enigma. Hingga akhirnya, pada tahun 1930, angkatan darat Jerman menemukan suatu metode tambahan yang pada akhirnya menjadi kekuatan utama enkripsi mesin enigma. Metode tambahan ini bekerja dengan cara mengubah hasil dari penekanan tombol pada papan kunci enigma. Metode ini

diimplementasikan dengan menambahkan sebuah alat yang dinamakan *plugboard* pada enigma. Alat tersebut merubah hasil dari penekanan huruf pada papan kunci sebelum huruf tersebut dienkripsi oleh roda-roda.

Gambar 3.1 Plugboard pada mesin enigma

Sebagai contoh, apabila pada plugboard, soket huruf "A" dihubungkan dengan huruf "J", maka pada saat operator menekan huruf "A" pada papan kunci, sinyal yang diterima oleh roda pengenkripsi adalah huruf "J". Dengan plugboard ini, metode enkripsi yang digunakan oleh enigma menjadi sangat aman. Bahkan jauh lebih aman dibandingkan dengan menambahkan roda-roda tambahan.

Dengan ditambahkannya plugboard tersebut, maka enigma memiliki kemampuan untuk mengenkripsi pesan sebagai berikut :

1. Enkripsi dengan menggunakan roda
2. Enkripsi menggunakan reflector
3. Enkripsi menggunakan plugboard

Dalam penggunaan mesin enigma, agar suatu pesan dapat dienkripsi dan kembali didekripsi dengan benar, ada beberapa hal yang perlu saling diketahui anatara pihak pengirim dan penerima pesan :

1. Urutan Roda (pemilihan jenis roda yang akan digunakan, dan tatacara urutan pemasangan roda tersebut) - 3 x 2 x 1 = 6 kombinasi
2. Posisi awal dari Roda (ditentukan oleh pengirim pesan, dapat berbeda tiap pengiriman) – 26^3 = 17576 kombinasi
3. Posisi huruf pada cincin roda (dapat berbeda tiap pengiriman pesan) 26^2= 676 kombinasi
4. Plugboard (aturan penggunaan plugboard, mengenai soket mana saja yang dihubungkan) 0.5 x 10^{15} kombinasi

Agar dapat mengirim dan menerima pesan dengan baik, keempat hal tersebut haruslah sama antara mesin pengirm pesan dan mesin penerima pesan. Keempat hal inilah yang menjadi kunci dalam enkripsi pesan yang dilakukan oleh mesin enigma. Agar pihak penerima dan pengirim pesan dapat melakukan komunikasi dengan baik,. Pihak Jerman menciptakan suatu standar operasi dalam menggunakan enigma. Standar operasi tersebut berupa tabel yang memuat informasi mengenai aturan mengenai keempat kombinasi yang harus diseragamkan tersebut. Aturan ini dicetak di atas kertas yang mudah hancur, untuk menghindari jatuhnya kertas tersebut ke pihak lawan.

Geheim! Sonder - Maschinenschlüssel BGT

Datum	Walzenlage	Ringstellung	Steckerverbindungen	Grundstellung
31.	IV II I	F T R	HR AT IW SN UY DF GV LJ BO KA	vyj
30.	III V II	Y V P	OR KI JV GT ZW MU BF YC DS GP	eqr
29.	V IV I	Q H R	UX JC FB LN TA ED ST DS LU FI	vhf

Gambar 3.2 Standar operasi enigma Jerman

Dalam gambar 3.2 dapat terlihat bahwa kolom paling kiri menunjukkan tanggal, yang menandakan bahwa setiap hari kombinasi enigma akan dirubah, kolom kedua berisi nomor roda dan urutan roda yang digunakan, misalkan IV II I, kolom berikutnya berisikan huruf awal pada cincin, misalkan angka 06 menunjukkan cincin harus diset pada huruf keenam yaitu "F", sedangkan kolom berikutnya, berisikan kombinasi dari plugboard yang digunakan pada saat itu. Namun, dari kertas tersebut, belum diperoleh informasi mengenai posisi awal dari roda. Posisi awal dari roda akan dikirimkan pada awal pesan, dengan cara menyamarkannya dengan mengetikkan dua kali huruf yang menjadi awal pesan setelah dua huruf lainnya.misalkan, apabila posisi awal adalah huruf "A", maka di awal pesan tersebut, pengirim akan mengetikkan ABC A, hal inilah yang di kemudian hari akan menjadi kelemahan terbesar dari mesin enigma ini.

4. PEMECAHAN ENKRIPSI ENIGMA

4.1 Metode Permutasi Marian Rejewski

Marian Rejewski meripakan seorang matematikawan Polandia yang pertama kali dapat memecahkan enkripsi dari enigma. Ia mendapatkan 6 buah pesan tersandi dari 6 hari yang berbeda, sehingga dari pesan-pesan tersebut ia menyusun persamaan :

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

Persamaan tersebut terdiri atas enam persamaan dengan empat buah permutasi yang tidak diketahui :
S = Permutasi yang berasal dari hubungan plugboard
H = Permutasi yang berasal dari hubungan antara soket pada plugboard dengan penghubung pada mesin
R'= Permutasi yang berasal dari roda kanan
T' = Permutasi kombinasi yang berasal dari roda

tengah, kiri dan reflector.
Q = Permutasi seederhana yang merubah huruf menjadi huruf berikutnya dalam alphabet(misalkan "a" menjadi "b", "b" menjadi "c" dan seterusnya.)
A-E = permutasi yang ditentukan oleh Rejewski berdasarkan analisis dari kunci pesan yang telah didapatkan.

Hingga hari ini, belum dapat diketahui apakah 6 buah persamaan tersebut dapat diselesaikan. Dalam menyelesaikan teka-teki mesin Enigma ini, Rejewski mendapat bantuan dari seorang Perancis bernama Gustave Bertrand. Bantuan yang ia dapatkan berupa kertas yang berisikan kunci harian enigma selama dua bulan.

Dengan mendapatkan informasi tersebut, Rejewski berhasil memecahkan permutasi S (koneksi plugboard). Permutasi H masihlah merupakan misteri, namun Rejewski berhasil memecahkannya dengan menebak, ternyata permutasi tersebut hanyalah permutasi identitas, yaitu mengubah suatu huruf kembali menjadi dirinya sendiri. Setelah permutasi S berhasil terpecahkan, dengan mudah Rajewski memecahkan permutasi R' dan T'.

Rajewski pada akhirnya berhasil membuat tabel berisikan kunci harian mesin Enigma, dengan menyelesaikan persamaan tersebut, ia dapat mengetahui pola pengacakan pesan yang dilakukan oleh Jerman. Namun hal ini tidak berlangsung lama, tentara Jerman, yang sebelumnya mengganti kunci berdasarkan standar operasi setiap 24 jam, merubah cara menentukan kunci, sehingga tabel Rajewski tidak dapat digunakan lagi.

4.2 Metode Grill

Metode ini digunakan pada periode 1933-1936, terdiri dari serangkaian prosedur "pensil dan kertas" yang bertujuan memperoleh komponen dari kunci harian enigma satu demi satu.

Langkah pertama dari metode ini ialah melakukan dekripsi pesan dengan cara menganalisis pesan tersandi yang telah didaptkan seperti pada enam persamaan metode Rajewski. Namun, pesan tersandi tersebut hanya dapat memberikan hasil AD, BE, dan CF. Untuk mendapatkan hasil dari permutasi A-F, Kriptoanalis menganalisa kebiasaan operator Enigma mengenai pengiriman 3 huruf di awal pesan, Karena pihak Jerman telah melarang penggunaan tiga huruf secara berurutan, pastilah huruf yang digunakan berjauhan. Dengan cara seperti ini, berhasil didapatkan informasi yang cukup untuk memecahkan permutasi A-F.

Langkah berikutnya ialah menentukan roda yang mana yang ditempatkan paling kanan di hari tersebut. Melalui analisa statistik dari dua pesan yang dikirimkan dengan kunci pesan yang sama, dapat ditentukan pilihan roda yang tepat.

Langkah selanjutnya, yang merupakan langkah utama dalam metode grill ialah untuk menentukan kombinasi dari plugboard. Metode ini didasari dari fakta bahwa plugboard tidak merubah seluruh huruf. Prosedur ini dapat dilaksanakan dengan menyelesaikan permutasi A-F dan prmutasi $Q^{x}RQ^{x}$ dengan x =0,25. Prosedur ini berhasil menemukan tidak hanya koneksi plugboard, tetapi juga informasi dari roda paling kanan.

Langkah selanjutnya ialah menentukan posisi dari roda tengah dan kiri. Hal ini berhasil didapatkan melalui percobaan sebanyak 1352 kali berdasarkan pesan yang telah tersandi. Posisi dari roda ini berhasil didapatkan dari fakta bahwa pesan Jerman biasanya diawali dengan kata "an"(yang artinya adalah untuk), diikuti huruf "x" (digunakan sebagai pengganti spasi)

4.3 Metode Kertas Berlubang Zygalski

Metode ini dikembangkan pada akhir tahun 1938, metode ini membutuhkan banyak perhitungan dan percobaan secara manual sehingga merupakan metode yang cukup rumit dan memakan waktu.

Metode ini didasarkan pada fakta bahwa dari 17576 kombinasi roda, hanya 40% yang merupakan permutasi AD. Kertas terpisah dibuat untuk setiap posisi dari roda sebelah kiri. Setiap kertas berisikan matriks segiempat yang berhubungan dengan posisi dari roda tengah dan kanan.

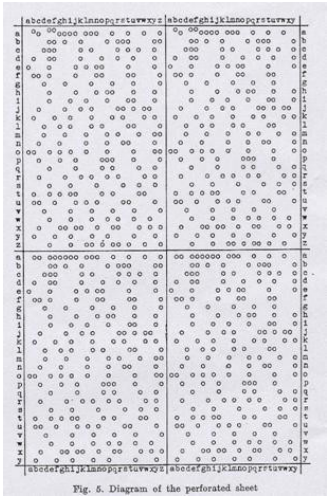


Fig. 5. Diagram of the perforated sheet

Gambar 4.1 Kertas Berlubang Zygalski

Setiap harinya, pesan terenkripsi yang didapatkan mengarah kepada permutasi AD siklus satu huruf. Dengan berdasarkan pada aturan rode untuk mengenkripsi pesan, para kriptoanalis berhasil

menentukan posisi roda relative siklus satu huruf.
Dengan adanya tiga buah roda yang dapat digunakan(yang menghasilkan 3!= 6 buah kombinasi), harus dibuat 26 buah kertas berlubang untuk tiap kombinasi. Namun, karena terbatasnya dana, hanya 2 buah kertas berlubang yang berhasil dibuat. Hal yang memperburuk keadaan ialah Jerman memperkenalkan dua roda tambahan. Meskipun mesin tidak berubah, kini ada 5 buah roda yang dapat dipilih, yang menghasilkan 5P3=60 kombinasi, sehingga metode kertas berlubang ini semakin sulit untuk diaplikasikan.

4.4 Katalog Karakteristik

Metode Katalog Karakteristik didasarkan pada fakta bahwa permutasi AD, BE, dan CF bergantung pada posisi roda dan tidak bergantung pada koneksi plugboard yang digunakan.
Sesuai dengan format dari permutasi, kita dapat memodelkan panjang dari siklus dalam bentuk pemutasi disjungtif. Misalkan, pemrutasi dari 26 huruf dapat memiliki bentuk seperti :

$(a_1\ a_2\ a_3\ a_4\ a_5\ a_6\ a_7\ a_8\ a_9\ a_{10}\ a_{11}\ a_{12}\ a_{13})$
$(b_1\ b_2\ b_3\ b_4\ b_5\ b_6\ b_7\ b_8\ b_9\ b_{10}\ b_{11}\ b_{12}\ b_{13})$

Dimana setiap huruf ditransformasikan menjadi huruf berikutnya. (misalnya a_1 ke a_2, a_2 ke a_3, dan seterusnya hingga a_{13} kembali ke a_1)

Pola ini merupakan karakterisitik dari kunci pesan tiap harinya. Berdasarkan permutasi A-F, hasil yang berupa AD, BE, dan CF dapat memiliki 101^3=1.030.301 pola yang berbeda. Sedangkan, hanya ada 6 kombinasi yang dimungkinkan dari ketiga roda. Hal ini menunjukkan bahwa karakteristik tersebut berhubungan dengan susunan roda yang dapat dengan mudah diujikan.

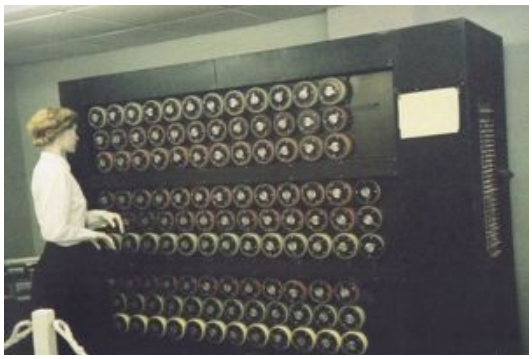
4.5 Bombe

Dengan menggunakan teknik-teknik yang telah ditemukan oleh para matematikawan Polandia, kriptoanalis dari Inggris berhasil membaca pesan terenkripsi Jerman, namun mereka khawatir sewaktu-waktu Jerman akan merubah standar operasi penggunaan Enigma yang akan membuat teknik-teknik tersebut tidak dapat diaplikasikan kembali.

Untuk mencegah hal ini, Alan Turring, seorang matematikawan Inggris dari universitas Cambridge merancang sebuah alat untuk melawan Enigma, alat tersebut diberi nama Bombe.

Bombe bekerja berdasarkan pada sifat reflektif mesin enigma. Seperti yang telah dibahas sebelumnya, enigma bersifat reflektif, misalkan jika ia merubah "C" menjadi "R", maka secara otomatis "R" juga akan berubah menjadi "C". Alan Turring mentimpulkan, bahwa seringkali terjadi pasangan huruf berulang di tempat yang berbeda dalam sebuah pesan. Ia juga menyadari bahwa posisi roda dan awal roda dapat ditemukan dengan mencoba kombinasi dari pasangan huruf tersebut. Namun, untuk mencoba seluruh kombinasi tersebut diperlukan waktu yang sangat lama.

Untuk memecahkan kombinasi tersebut dalam waktu yang lebih singkat, dibutuhkan suatu alat mekanis. Alat mekanis tersebut dibuat dengan cara membongkar mesin enigma yang telah berhasil didapatkan, dan menganalisa isinya.



Gambar 4.2 Bombe

Setiap Bombe memiliki 12 set roda dan bekerja secara bersamaan melalui segala kemungkinan yang ada. Dengan menggunakan Bombe, pihak Inggris dapat menguji keseluruh 60 buah kombinasi dengan waktu hanya 15 jam.

5. KESIMPULAN

Kriptografi telah digunakan sejak zaman dahulu kala untuk mengirimkan pesan rahasia. Setiap suatu metode enkripsi ditemukan, pasti para kriptanalis akan berlomba-lomba memecahkan metode tersebut.

Kriptanalis menggunakan berbagai macam cara untukdapat memecahkan sebuah teknik enkripsi pesan. Dari makalah yang telah dibuat, dapat ditarik kesimpulan bahwa metode untuk memecahkan enkripsi pada umumnya ialah dengan menggunakan prinsip permutasi dan kombinasi,

Enigma merupakan salah satu aplikasi ilmu matematika diskrit yang luar biasa, meskipun dengan aplikasi matematika diskrit lainnya pada akhrinya enkripsi enigma berhasil dipecahkan.

Pada akhirnya, ilmu pengetahuan memegang peranan penting dalam sejarah dunia. Tanpa para kemampuan kriptanalis, mungkin sejarah akan sangat berbeda.

DAFTAR REFERENSI

I. Gaj, Kris, dan Arkadiusz, Orlowski (2003), *Facts and Myth of Enigma : Breaking Stereotypes*.

II. Sales, Tony, *Codes and Chipers in World War II* http:// www.codesandciphers.org.uk
Tanggal Akses : 18 Desember 2007 pukul 12.15 WIB

III. http://www.avoca.ndirect.co.uk/enigma/enigma4.htm
Tanggal Akses : 29 Desember 2007 pukul 18.30 WIB

IV. Sullivan, Geoff, dan Weierud, Frode(2005), *Breaking German Army Chiper*.

V. Shaylor, Neill (1997), *Enigma and Turing Bombe*.

VI. Rejewski, Marian (1980), *An Application of the Theory of Permutations in Breaking the Enigma Cipher*.
http://frode.home.cern.ch/frode/crypto
Tanggal Akses : 30 Desember 2007 pukul 21.15