ENIGMA BREAKING

Lukman Hakim – NIM : 13503114
Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if13114@students.if.itb.ac.id

Abstrak
Sebelum dan selama Perang Dunia II terdapat publikasi tentang pemecahan Enigma oleh pihak aliansi. Kesimpangsiuran berita ini tidak hanya membingungkan publik tetapi juga para peneliti profesional kriptologi. Sehingga cerita mengenai Enigma jarang dibahas dalam buku teks kriptologi atau sumber bacaan kriptografi dan keamanan jaringan lainnya. Hal ini disebabkan oleh, pertama ketidakjelasan kebenaran pemecahan kode Enigma karena kurangnya sumber yang dapat dipercaya dan dibutuhkan waktu yang panjang untuk menyusun kembali dokumen-dokumen yang terkait dengan aktivitas kriptografer selama Perang Dunia II. Kedua, isu politik antar negara yang memperselisihkan kontribusi dalam pemecahan kode Enigma. Ketiga banyak kriptografer kontemporer yang tidak mendapatkan pelajaran banyak dari analisis kriptosistem Enigma karena berbedanya cipher lama dan modern dengan berkembangnya teori dan praktek dalam kriptografi. Pada makalah ini akan membahas metode dan alat kriptografi yang digunakan untuk memecahkan Enigma dan diperkenalkan pula semua pemain utama yang telah memberikan kontribusi yang besar dalam pemecahan kode Enigma. Akhirnya, penulis menunjukkan bahwa cerita tentang Enigma dapat menjadi input bagi kriptografer kontemporer tentang cara mengorganisasikan dan membangun sistem keamanan dengan skala besar.

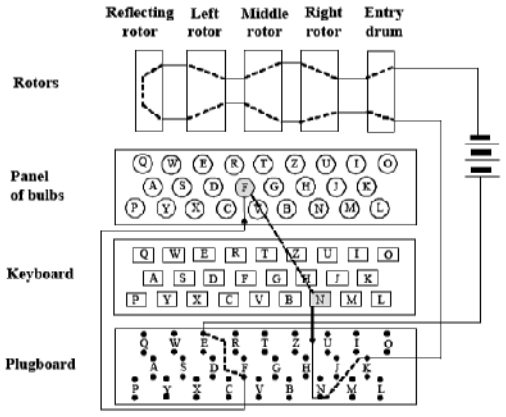
Kata kunci: Enigma, mesin cipher, rotor, kriptalanlisis bombe, codebreaking.

Awal Enigma

Mesin enigma termasuk dalam kelompok mesin kripto yang berbasi rotor. Mesin berbasis rotor pertama kali dibangun dan dipatenkan oleh beberapa penemu dari negara yang berbeda pada tahun 1917 sampai 1921 diantaranya warga Amerika Edward Hug Hebern, warga Jerman Arthur Scherbius, warga Belanda hug Alexander Koch, dan warga Swedia Arvid Gerhard Damm. Arthur Scherbius mengembangkan rancangan milik Koch yang telah dipatenkan, yang diberi nama Enigma, semula ia berharap untuk menjual mesin Enigma tersebut kepada kalangan bisnis dunia tetapi ternyata lebih sukses di pasar yang berbeda yaitu angkatan bersenjata. Tahun 1926, angkatan laut Jerman, memperkenalkan mesin cipher Scherbius , modifikasi sederhana dari Enigma versi komersial. Tahun 1930, Enigma versi militer dibangun. Perbedaan keduanya terletak pada penggunaan komponen baru yaitu plugboard yang dapat meningkatkan kemungkinan aturan mesin dan juga pencarian kunci ciphernya. Sejak pertengahan 1930, Enigma telah menjadi umum digunakan oleh angkatan bersenjata Jerman. Diperkirakan jumlah mesin Enigma yang digunakan pada tahun 1935 sampai 1945 mencapai 100.000 mesin.

Konstruksi Mesin

Enigma merupakan mesin elektromekanik yang cukup kecil yang dilengkapi dengan baterai. Enigma mempunyai dimensi berbentuk balik yang terlihat seperti mesin tik. Komponen utama enigma dan cara koneksi diantara komponen dapat digambarkan pada gambar 1 dibawah ini.

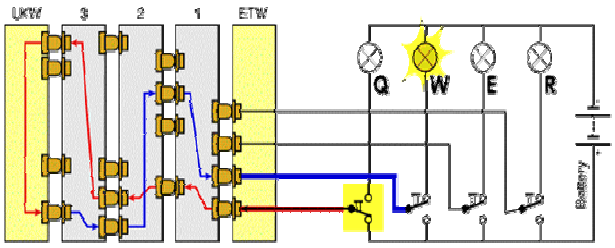


Gambar 1 Diagram fungsional dan aliran data dari Enigma Militer

Sebelum membahas profil mesin Enigma perlu diketahui bahwa banyak varian dari mesin ini.

Hasil pengkodean dari satu model mesin Enigma tidak dapat diterjemahkan dengan menggunakan model mesin Enigma yang lainnya. Pada tulisan ini digunakan mesin Enigma model M3. Mesin Enigma ini terdiri dari keyboard dengan 26 huruf, papan lampu dengan 26 huruf, 3 set roda rotator, sebuah reflektor dan sebuah plugboard.

Gambar 2 Mesin Enigma M3



Gambar 3 Rangkaian mesin enigma M3

Huruf-huruf diacak oleh 3 set Rotator, dimana tiap Rotator memiliki 26 kontak pada kedua sisi. Tiap kontak pada satu sisi disambungkan ke sebuah kontak pada sisi lain dengan Rotator yang berbeda dan susunan huruf antar Rotator dalam formasi yang acak. Untuk tiap huruf yang ditekan pada keyboard, roda Rotator paling kanan akan diputar satu huruf, menghasilkan pemetaan yang berbeda untuk koneksi yang ada di dalam. Sebuah Rotator memiliki satu atau lebih *Notches* yang berakibat pada Rotator berikutnya akan mengalami pergeseran satu posisi. Hal ini akan menghasilkan pengkodean yang berbeda untuk tiap huruf yang ditekan pada keyboard. Keyboard terdiri dari 26 tombol, diberi nama A hingga Z. Apabila sebuah tombol ditekan, katakanlah huruf Q, Rotator akan berputar pada satu posisi baru dan kontaknya tersambung. Kemudian diikuti mengalirnya arus. Sambungan dari 26 tombol disambungkan ke sebuah roda tetap yang disebut dengan Stator atau *Entrittswalze* (ETW). Urutan tombol yang disambungkan ke 26 kontak pada ETW bervariasi untuk tiap model mesin Enigma. Setelah meninggalkan ETW, arus masuk ke Rotator paling kanan sesuai dengan posisi tangan kanan. Sambungan dalam dari rotator akan men-*translate* ke kontak posisi kiri dari Rotator yang sama, dan dilanjutkan seterusnya ke Rotator yang lain. Posisi paling kiri dari Rotator adalah Reflektor atau *Umkehrwalze* (UKW). Reflektor ini akan mengirimkan arus kembali ke roda rotator, tetapi kali ini arus mengalir dari kiri ke kanan, sampai tiba di ETW kembali. Dari ETW arus menuju papan lampu yang ditunjukkan oleh huruf lampu yang menyala. Ini terlihat bahwa dalam rancangan ini sebuah huruf tidak pernah di kodekan dengan huruf yang sama dengan huruf asal.

Sebelum mulai dioperasikan untuk proses penyandian, kondisi *set up* awal mesin Enigma harus diketahui kedua belah pihak. Ini berarti urutan roda Rotator (*Walzenlage*) perlu diketahui sesuai pengoperasian awal untuk tiap Rotator (*Grundstellung*). Agar lebih rumit, tiap rotator harus memiliki gelang indeks yang dapat diatur yang menggerakkan kontak terlepas dari roda huruf. Ini disebut dengan pengaturan gelang (*Ringstellung*). Supaya lebih rumit lagi, beberapa model Enigma yang lain dilengkapi sebuah *plug board* (*Steckerbrett*) agar huruf-huruf dapat ditukarposisikan. Varian Enigma untuk angkatan laut (M3 dan M4) dilengkapi dengan sebuah plug board (*Steckerbrett*) agar tiap pasangan huruf dapat ditukarposisikan. Jika sepasang kabel diperuntukkan untuk huruf G dan P, kedua huruf ini akan akan ditukarposisikan. Karena terdapat 26 karakter maka secara teoritis maksimum kabel yang dibutuhkan sebanyak 13 pasang. Kebanyakan mesin Enigma menggunakan lebih sedikit kabel (10 atau 11 kabel). Sebagai catatan untuk tiap jumlah kabel yang digunakan, dimulai dari tanpa nomor sampai dengan nomor 13, memberikan peningkatan permutasi yang mungkin dilakukan. Seperti diketahui *Steckerbrett* disambungkan antara keyboard dan ETW, huruf yang dikodekan akan terus melewati stecker yang akan dipetakan dua kali. Hal ini untuk mencegah sebuah huruf dikodekan ke dalam huruf itu sendiri.

Prinsip Kerja Mesin Enigma

Seperti disinggung sebagian pada pembahasan sebelumnya, mesin Enigma adalah mesin yang menghasilkan kode rahasia. Mesin ini memiliki beberapa pengaturan (*setting*) yang berdampak pada pengoperasian mesin. Pemakai harus memilih 3 Rotor dari kumpulan Rotor yang akan digunakan pada mesin ini. Tiga Rotor ini akan menghasilkan kombinasi enkripsi. Elemen lain dari mesin Enigma ini adalah plug board. Plugboard ini memetakan ulang pasangan huruf sebelum proses enkripsi dimulai dan sesudah proses enkripsi.

Pada saat sebuah tombol huruf ditekan, arus listrik akan mengalir pada mesin ini yang diawali melewati plug board, kemudian terus melewati 3 Rotor dan setelah tiba di Reflektor arus listrik dibalikkan kembali melewati 3 Rotator selanjutnya diteruskan ke plug board dan kemudian di huruf dienkripsi yang ditampilkan pada lampu yang menyala. Setelah tampilan huruf yang telah dienkripsi menyala, Rotator berputar. Perputaran Rotor sama halnya dengan sebuah Odometer yaitu jika Rotor yang paling kanan telah menyelesaikan satu putaran penuh sebelum Rotor yang ditengah berubah satu posisi dan begitu seterusnya untuk Rotor yang berikutnya. Ketika arus melewati tiap komponen yang ada di dalam mesin Enigma , huruf mengalami pemetaan ke dalam huruf yang lain. Plug board melakukan pemetaan yang pertama. Jika terdapat sambungan antara dua huruf, huruf-huruf ini akan dipertukarkan satu sama lain. Misalnya jika sambungan A dan F, maka F akan dipetakan menjadi A, dan A akan dipetakan menjadi F. Jika tidak ada sambungan huruf yang bersangkutan maka huruf tersebut tidak akan mengalami pemetaan. Setelah melewati Plug board, huruf akan dipetakan melalui 3 Rotor. Tiap Rotor mengandung satu pemetaan huruf tetapi berhubung rotator berputar untuk tiap penekanan tombol huruf sehingga pemetaan Rotator berubah untuk tiap penekanan tombol. Setelah melewati 3 Rotator selanjutnya diteruskan ke Reflektor. Reflektor sangat mirip dengan Rotor hanya saja Reflektor tidak berputar sehingga pemetaan selalu sama. Keseluruhan proses enkripsi untuk satu huruf minimum mengandung 7 pemetaan (arus listrik mengalir melalui 3 Rotator sebanyak 2 kali) dan maksimum sebanyak 9 pemetaan (jika huruf tersambung ke plug board).

Untuk menterjemah sandi rahasia dari mesin Enigma, penerima harus mengetahui Rotor-Rotor apa yang digunakan, sambungan pada plug board dan *setting* awal dari Rotor. Untuk memecahkan sandi rahasia, pihak penerima harus men-*settting* mesinnya sesuai dengan *setting* mesin yang mengirimkan sandi rahasia tersebut. Sandi rahasia akan sangat sulit dipecahkan apabila tidak mengetahui *setting* mesin yang mengirimkan pesan rahasia tersebut.

Tiga rahasia Enigma

1. Koneksi internal mesin

Mayoritas sistem militer merahasiakan algoritma enkripsi mesin enigma. Jumlah koneksi internal diperkirakan mencapai 3×10^{114} , oleh karena itu jelas bahwa koneksi internal Enigma sulit untuk diterka, dan hanya dapat ditemukan melalui analisis matematika atau dengan membuat salinan mesinnya.

Kunci harian

Setting mesin ditentukan oleh tabel kunci harian yang didistribusikan oleh seorang kurir kepada semua unit militer dengan menggunakan Enigma. Sebelumnya, semua unit militer menggunakan mesin dan kunci harian yang sama. Pada tahun 1939, digunakan kunci harian berbeda untuk enam jaringan militer.

Pada periode 1930 sampai 1938, kunci harian Enigma digunakan angkatan bersenjata Jerman yang terdiri dari setting berikut:

a. Urutan ketiga rotor – 6 kombinasi.
b. Koneksi plugboard – sekitar 0.5×10^{15} kombinasi.
c. Posisi awal rotor - $26^3 = 17.576$ kombinasi.
d. Posisi cincin yang ditentukan oleh posisi kedua rotor – $26^2 = 676$ kombinasi.

Jadi, jumlah kemungkinan kombinasi kunci harian sekitar 3.6×10^{22} atau 2^{75}. Hal ini terlihat mengesankan, kontribusi terbesar berasal dari koneksi plugboard.

2. Kunci pesan

Jika semua pesan telah dienkripsi menggunakan setting awal yang sama yang ditentukan oleh kunci harian, kriptanalisis dapat menerapkan analisis frekuensi sederhana pada semua huruf pertama dari cipherteks setiap harinya, kemudian semua huruf kedua, dan selanjutnya. Untuk mencegah serangan ini, dibutuhkan kunci pesan yang identik dengan *initialization vetor* (IV) pada cipher modern.

Pada periode 1930 sampai 1938, kunci pesan disusun oleh tiga huruf pada ketiga rotor ketika pesan akan dimulai untuk dienrkipsi.

Kriptografer Jerman, berusaha keras untuk menyempurnakan sistem mesin Enigma yang lebih aman dengan cara mengenkripsi kunci pesan menggunakan mesin Enigma pula dengan kunci harian. Untuk membuat lebih buruk, agar dapat dideteksi kemungkinan kesalahan saat transmisi, maka setiap kunci pesan dienkripsi dua kali sehingga menghasilkan enam huruf, hasilnya akan ditempatkan pada header pesan. Lebih buruk kunci pesan ditentukan oleh individu operator yang cenderung memilih pola yang sederhana, dapat diprediksikan, seperti tiga huruf yang identik atau huruf yang berkorespodensi dengan huruf lain yang bertetanggan pada keyboard.

Hasilnya, prosedur distribusi kunci pesan menjadi kelemahan dari sistem Enigma sehingga banyak serangan termasuk serangan koneksi internal mesin itu sendiri.

Prosedur untuk mentransfer kunci pesan diubah oleh Jerman pada tahun 1938, dan diubah kembali pada tahun 1940, tetapi kemudian, koneksi internal mesin telah direkontruksi dan terdapat metode alternatif untuk mengembalikan kunci harian yang telah dibangktikan. Hal ini dilakukan oleh ahli kriptologi Inggris.

Rekonstruksi koneksi internal Enigma oleh Ahli matematika Marian Rejewski

Polandia merupakan negara pertama yang memperkenalkan adopsi mesin enigma versi militer yang dibeli dari Jerman. Apabila enigma versi militer dibandingkan dengan enigma versi komersial didapatkan pengetahuan tentang mesin sebenarnya yang digunakan oleh angkatan bersenjata Jerman. Pada tahun 1929, ahli cipher mengumpulkan 20 mahasiswa Universitas Poznan. Tiga diantaranya merupakan mahasiswa terbaik yang nantinya akan bekerja untuk memecahkan Enigma. Mahasiswa yang paling jenius adalah Marian Rejewski, ditugaskan untuk menginvestigasi kekuatan cipher Jerman yang baru. Rejewski memulai kerjanya dengan menganalisa pesan cipher Jerman yang didapatkan dari penangkapan sinyal radio. Pada tahun 1932, Rejewski mendapatkan pembentukan pesan yang terdiri dari enam huruf yang dihasilkan dari dua enkripsi dari tiga huruf kunci pesan. Kunci yang berbeda pada setiap pesan tetapi dienkripsi dengan setting sama (kunci harian). Penelitian ini memberikan kesimpulan dan membentuknya dalam persamaan permutasi sebagai berikut:

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

Kesimpulan ini terdiri dari enam persamaan dan empat permutasi yang tidak diketahui: S, H, R', T'. Empat permuasi tersebut direpresentasikan:

S – permutasi yang ditentukan oleh koneksi plugboard,

H – permutasi tetap yang ditentukan oleh koneksi antara soket plugboard dan koneksi rotor *entry drum*.

R – permutasi yang ditentukan oleh koneksi internal rotor kanan.

T' – kombinasi permutasi yang ditentukan oleh koneksi internal rotor tengah, kiri dan *fixed refrelcting*.

Q merupakan permutasi sederhana yang merubah setiap huruf kedalam huruf berikutnya, contohnya 'a' menjadi 'b', 'b' menjadi 'c', …., 'z' menjadi 'a'.
A-E merupakan permutasi yang ditentukan oleh Rejewski berdasarkan hasil analisis kunci pesan, dikombinasikan dengan pemilihan kunci pesan yang signifikan menjadi tiga huruf alfabet yang identik.

Berikutnya, tidak diketahui apakah persamaan tersebut dapat diselesaikan semuanya. Rejewski mencoba menyelesaikan permasalah tersebut dengan bantuan yang tidak terduga. Kapten Gustave Bertrand – pimpinan intelejensi radio dari French Intelligence Service membantu ahli cipher mendapatkan informasi dari agen bayaran, Hans-Thilo Schmidit, nama samaran Asche, yang bekerja pada di depertemen kriptografi angkatan bersenjata Jerman.

Informasi tersebut berisi tabel kunci harian utuk dua bulan berturut-turut, pada bulan September dan Oktober 1932 tetapi tidak berisi informasi tentang internal rotor Enigma. Namun Rejewski tidak berputus asa karena ternyata kunci harian tersebut membuka permutasi ketiga yaitu S, yang mempresentasikan koneksi plugboard mesin. Permuasi kedua, H, masih bersifat rahasia, tetapi Rejewski berhasil menemukannya dengan terkaan imanjitifnya.

Terlihat kontras antara enigma versi militer yang mentranformasikan ‘a’ menjadi ‘a’, ‘b’ menjadi ‘b’, dan lainnya. Persamaan yang masih belum diketahui adalah R’ dan T’. Menurut Rejewski hal ini mudah untuk diselesaikan dengan cara menempatkan rotor koneksi pada hari yang diberikan. Dua tabel kunci harian memungkinkan untuk menemukan hubungan dua rotor. Sisa permutasi tersebut mudah ditentukan dan direkonstruksi setelah mendapatkan bantuan tambahan dari Jerman untuk menggunakan Enigma yang dikirim oleh Asche. Pesan tersebut berisi pasangan plainteks dan cipherteks yang autentik dengan kunci harian dan pesan yang sederhana.

Dalam manuskrip yang tidak dipublikasikan Rejewski, akhirnya Rejewski berhasil untuk merekonstruksi kembali koneksi internal rotor, berdasarkan pada kunci harian dengan tanpa menerka permutasi H. Meskipun begitu cara ini membutuhkan akses penangkapan sinyal radio dan hal ini menghabiskan banyak waktu (sekitar setahun) dan waktu komputasi yang panjang, akhirnya didapatkan kesulitan untuk merekonstruksi koneksi internal.

Metode pemulihan kunci kriptografi
Pada tahun 1932 sampai 1939, ditemukan metode mempersingkat waktu komputasi untuk pencarian kunci harian oleh tiga ahli kriptologi, Marian Rejewski, Jerzy Rozycki, dan Herryk Zygalski. Banyak metode yang dihasilkan dari perubahan dalam prosedur distribusi kunci dan mesin oleh Jerman.

Metode berikut ini dapat memulihkan kunci menjadi lebih efektif:

- Metode ‘grill’, yang digunakan bersama dengan metode ‘distinct letters’, ‘Rozycki’s clock’ dan disebut ‘ANX’.
- Katalog karakteristik, dibangun dengan bantuan alat khusus disebut ‘cyclometer’
- Lembar berlubang Zygalski.
- ‘Bomby’

Metode Grill
Metode grill digunakan pada tahun 1933 – 1936 terdiri dari rangkaian kertas dan pensil yang bertujuan merekonstruksi semua komponen kunci harian, satu per satu.

Langkah pertama adalah menemukan kunci pesan yang tidak terenkripsi sebaik permutasi A-F menggunakan perrsamaan (1)-(6). Analisis kunci pesan, membutuhkan 70 – 80 cipherteks Enigma yang hanya mempunyai nilai produk AD, BE, CF. Untuk mendapatkan nilai permuasi A-F, kriptologis menggunakan pengetahuan tentang kebiasaan operator Enigma dalam pemilihan kunci pesan yang disusun oleh tiga huruf identik. Ketika pilihan ini dilarang oleh prosedur Jerman, operator cenderung memilih tiga huruf yang saling berdekatan pada keyboard Enigma. Ketika hal itu dilarang kembali, kriptologis mendapatkan metode baru ‘distinct letters’. Metode ini didasarkan pada fakta bahwa operator dilarang menggunakan tiga huruf identik, mereka juga menghindari kunci pesan apapun dengan dua huruf yang berulang. Ini merupakan bias statistik kecil, dikombinasikan dengan pengetahuan teori permutasi, ddapatkan sedikit waktu untuk rekonstruksi permutasi A-F, sebaik kunci pesan individu pada hari yang diberikan.

Langkah berikutnya untuk menentukan tiga rotor mana yang ditempatkan pada hari yang diberikan pada posisi paling kanan. Rozycki ‘clock method’ menyandarkan properti enigma pada posisi rotor paling kanan dan rotor tengah bergerak berbeda untuk setiap tiga rotor yang digunakan oleh Angkatan Bersenjata Jerman. Dengan analisis statistik dari dua cipherteks terenkripsi menggunakan kunci pesan yang sama (dan juga setting mesin yang sama), memungkinkan menentukan posisi mana dari rotor paling kanan, rotor tengah bergerak, dan menentukan pilihan rotor kanan.

Bagian utama metode grill dicurahkan untuk rekonstruksi koneksi plugboard. Metode ini berbasis pada fakta bahwa plugboard tidak merubah semua huruf. Prosedur tersebut otomatis menggeser sheet kertas dengan permutasi A-F, lembar dengan transformasi form Q-x x R xQx, untuk x=0,25 (dimana R merepresentasikan tranformasi rotor kanan) dan pencarian nilai x yang berkorelasi antara permutasi terkait mendapatkan enam baris berlanjut. Prosedur ini menyatakan antara koneksi plugboard, dan posisi rotor kanan.

Kemudian urutan dan posisi rotor tengah dan kiri ditemukan menggunakan pencarian exhaustive terdiri 2x26x26 = 1532 percobaan bergantung pada enkripsi dan un-enkripsi kunci pesan. Akhirnya lokasi cincin rotor ditentukan dengan menggunakan pencarian lain berdasarkan faktor bahwa mayoritas pesan jerman dimulai dari huruf ‘an’ diikuti oleh ‘x’ (menggunakan spasi).

Katalog karateristik
Metode kalatog karakteristik, digunakan pada periode 1939-1938, didasarkan pada fakta bahwa format hasil permutasi AD, BE, dan CF tergantung pada urutan dan setting sesungguhnya rotor, tidak tergantung apda koneksi plugboard. Dengan format sebuah permutasi, berarti panjang putaran dalam representasi permutasi dalam bentuk hasil putaran disjuntif. Contohnya, permutasi 26 huruf dapat mempunyai bentuk apapun antara lain:

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

Dimana a_1 ditransformasi ke a_2,a_2 menjadi a_3, …. Dan a_{13} kembali ke a_1, begitu pula, b_1 ditransformasikan menjadi b_2,b_2 ke b_3, …. Dan b_{13} ke b_1.
Sampai

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

Dimana setiap huruf ditransformasikan menjadi dirinya sendiri.

Pola ini panjang putaran merupakan karakteristik dari setiap kunci harian, dan oleh karena itu oleh Rejewski dinamakan dengan ‘Karakteristik hari”. Berdasarkan properti individu permutasi A-F, hasil AD, BE, dan CF dapat memiliki 101 perbedaan panjang pola putaran atau 101^3 = 1.030.301 pola putaran yang berbeda (‘karakteristik’). Sedangkan, terdapat 3! x 26^3 kemungkinan penyusunan (urutan dan setting) tiga rotor. Hal ini berarti seperti pemberian karakteristik sesuai dengan penyusunan unik rotor atau minimal sejumlah kecil penyusunan yang dapat mudah untuk diuji.

Untuk membuat metode praktis, dibutuhkan pembuatan katalog karakteristik sebesar 6 x 26^3 = 105.456 urutan dan setting rotor. Pemberian pola putaran untuk permutasi AD, BE, dan CF, katalog ini mengembalikan kesesuaian urutan dan setting rotor. Dengan mengetahui posisi rotor, koneksi plugboard dapat ditentukan relatif lebih mudah, dan metode ANX *known-plainteks* masih tetap dapat digunakan untuk menentukan setting cincin. Untuk membuat sebuah katalog karakteristik, Rejewski merancangnya, dan teknisi pemerintah mengimplementasikannya menjadi alat elektromekanik yang disebut cyclometer, pendahulu dari Bomba dan Bombe.

Polish “Bomba”
Hasil perubahan utama yang dikenalkan dalam prosedur distribusi kunci Enigma pada 15 September 1938, sebelumnya semua membangun metode pemulihan kunci harian. Mulai dari tanggal ini, setiap operator Enigma memilih oleh dirinya sendiri setting awal rotor yang digunakan untuk mengenkripsi kunci pesan. Posisi ini kemudian ditransmisikan sebagai header cipherteks, dan hal ini tidak identik bagi setiap operator.

Polish ‘Bomba’, dibangun pada bulan November 1938 oleh Perusahaan Manufaktur Radio AVA, didasarkan pada rancangan Marian Rejewski, yang merespon pada perubahan ini. Bomba terdiri dari kumpulan enam mesin Enigma, beroperasi bersama, mulai dari setting awal ditentukan berdasarkan analisis enkripsi kunci pesan. Dengan input yang benar, Bomba dapat menentukan posisi benar rotor dalam waktu 2 jam. Koneksi plugboard, dan setting ring ditentukan sama sebagaimana sebelumnya.

Lembar Berlubang Zygalski
Metode Zygalski, dibangun pada akhir tahun 1938, dibutuhkan aplikasi khusus berupa kertas. Banyak komputasi dan percobaan manual dibutuhkan untuk menghasilkan lembaran, dengan kerumitan dan memakan waktu.

Metode pemulihan kunci didasarkan pada fakta bahwa 26^3 kemungkinan setting rotor, hanya 40% pasti permutasi AD termasuk minimal satu pasang satu putaran kertas $(a_1)(a_2)$. Sebagian lembar dibuat untuk setiap posisi rotor kiri. Setiap lembar berisi matrik persegi berkorespodensi pada semua posisi rotor kanan dan tengah. Isian matriks berkorespodensi dengan posisi rotor dengan putaran kertas tunggal yang telah dilubangi.

Pada setiap hari, beberapa kunci pesan terenkripsi menjadi permutasi AD dengan satu putaran kertas. Berdasarkan setting rotor yang digunakan untuk mengenkripsi kunci pesan, yang dikirim sebagai header cipherteks, criptanalisis dapat menentukan posisi relatif rotor sesuai pada putaran kertas tunggal.

Selama analisis, lembar Zygalski dilapisi, ditempatkan pada tempat yang baik. Jumlah lubang yang bersinar melalui penurunan

berangsur-angsur, dan akhirnya hanya satu atau paling banyak sedikit isian dengan lubang yang bersinar melalui semua lembar. Posisi korespodensi rotor merupakan sebuah potensi kecurigaan untuk pengujian ke depan.

Dengan tiga rotor untuk memilih bentuk, terdapat 3! = 6 kemungkinan kombinasi rotor. Kumpulan lembar 26 yang berlubang dibuat untuk setiap kombinasinya. Sayangnya, karena keterbatasan sumber dari Polish Cipher Bureau, dari akhir 1938 sampai 1 September 1939, hanya dua set lembar berlubang yang dapat dibuat. Hal ini bertambah buruk, pada desember 1938, Jerman memperkenalkan dua tambahan rotor. Meskipun mesin itu tidak mengalami perubahan, dan hanya tiga rotor yang digunakan pada waktunya, tiga rotor ini sekarang dipilih dari kumpulan lima rotor yang tersedia pada setiap mesin Enigma. Perubahan ini meningkatkan jumlah kemungkinan kombinasi rotor sampai menjadi 60. hasilnya, kemampuan Polish untuk memulihkan kunci Enigma secara substansial mengalami penurunan dalam waktu sebulan sesaat sebelum Perangan Dunia II.

Jalan salinan rekonstruksi mesin Enigma

Pada 24-26 Juli 1939, di Pyry, Kabackie Woods di luar Warsaw, sebuah sejarah dimulai. Sisi Polish direpresentasikan oleh tiga kriptologi (Rejewski, Rozycki, Zygalski) dan dua officer Polish Cipher Bureau (Langer, Ciezki). Dari sisi Perancis direpresentasikan oleh Gustave Bertrand dan Henri Braquenie, dan dari sisi Inggris oleh Alastair Denniston, Alfred D. Knox, dan satu atau lebih offices (Humprey Sandwith). Selama pertemuan ini, Polish membawa dua salinan hasil konstruksi mesin Enigma kepada Perancis dan Inggris. Serupa, dokumentasi lengkap lembar Zygalski dan Bombyh Polish dan metode Polish lainnya didiskusikan untuk representatif antar negara. Pertemuan tersebut datang sebagai kejutan besar bagi mata-mata Perancis dan Inggris, karena pada waktu itu tidak dibenarkan Polish mengembangkan pemecahan Enigma dan tidak membuat kemajuan substasial dalam pemecahan cipher Enigma.

Operasi Bletcleh Park

Pada musim panas tahun 1939, Britain's Government Code and Cypher School (GC&CS) berpindah dari London menuju Viktoria di Bletchley, barat daya London, disebut Bletchley Park. Awalnya, pusat tersebut berisi tidak lebih dari 30 orang, tetapi terus berkembang, sampai mencapai 10.000 pekerja.

Britain, seperti Polandia, memulai mempekerjakan pakar matematika untuk bekerja dalam *codebreaking*, dan dua diantaranya, Alan Turing dan Gordon Welchman, menjadi instrumental dalam membawa keberhasilan memecahkan Enigma. keduanya datang berasal dari Universitas Cambridge.

Awalnya, Inggris mengadaptasi metode Polish. Contohnya, pada akhir tahun 1939 mereka mengelola pembuatan 60 set lembar Zygalski dan menggunkaan metode ini dengan nama "Jeffrey's apparantus" sampai bulan Mei 1940. Pada tanggal 10 Mei 1940, hari penyerangan di Perancis, Jerman kembali mengubah prosedur distribusi kunci mereka. Perubahan untuk mengenkripsi setiap kunci pesan hanya sekali, sampai dua. Hal ini terlihat perubahan kecil yang membuat semua metode rekonstruksi kunci sebelumnya menjadi tidak terpakai.

Sayangnya, kriptologis Inggris mengelola mendatangkan beberapa metode dadakan. Pertama dari mereka dikeluarkan, serupa dengan metode Polish, yang memanfaatkan kebiasaan buruk dari beberapa operator Enigma, dan disebut dengan tips Herivel dan 'sillies'. Contohnya, banyak operator, setelah memasukkan rotor ke dalam mesin, tidak mengubah lokasinya sebelum memulai kembali bekerja pada pesan pertama. Sejak rotor dimasukkan kedalam mesin menggunakan orientasi spesifik, analisis beberapa header cipherteks untuk pesan pertama sering menampakkan posisi signifikan dari kunci harian. Kesalahan umum lainnya adalah penggunaan tiga kertas yang sama untuk keduanya: posisi awal rotor dan untuk kunci pesan (dikirim dalam bentuk terenkripsi).

Meskipun begitu, terobosan utama adalah penemuan dan pengembangan Bombe Inggris. Tidak seperti Bomba Polis, Bombe Inggris didasarkan tidak hanya pada prosedur distribusi kunci, tetapi pada serangan tanpa mengetahui plainteks.

Bombe Inggris memanfaatkan bentuk sterotip dari banyak pesan terenkrpisi menggunakan Enigma yang ditransmisikan dalam jaringan angkatan bersenjata Jerman selama Perang Dunia II. Stereotip susunan kata ini bertanggung jawab sehingga disebut "cribs" – fragmen dari plainteks yang kriptoanalisis dapat menerkanya.

Di Bletchley Park, divisi khusus, disebut Crib Room, bertanggung jawab untuk menemukan crib baru pada dasar regular. Sumber crib ini banyak. Contohnya, pesan Jerman berisi penuh data tentang pengirim dan peneriman, termasuk judul penuh dan keanggotaan, sebagaimana surat ucapan selamat. Data ini mudah untuk menerkannya tergantung pada pengetahuan stasiun intersepsi pesan terenkripsi sebagaimana informasi kontrol header cipherteks yang tidak terenkripsi. Sumber lainnya seperti contoh laporan, mudah memperkirakan perkiraan cuaca, atau pesan yang ditransmisikan kembali antara jaringan menggunakan kunci harian berbeda.

Ide Bombe Inggris datang dari Alan Turing, yang merupakan pengembangan signikan dari 'diagonal board' milik Gordon Welhman. Realisasi teknik tersebut diserahkan kepada Harold "doc' Keen, teknisi dari British Tabulating Machines(BTM).

Dari titik kriptologi Bombes Inggris sangat berbeda dengan Bomby Polish, meskipun begitu tujuan dari operasinya sama: menemukan posisi rotor yang tidak dapat dikeluarkan kemungkinan digunakan pada awal enkripsi. Keuntungan terbesar Bombes Inggris adalah mereka tidak bergantung pada prosedur distribusi kunci, yang konstan membuat metode sebelumnya menjadi tidak terpakai. Kelemahannya adalah ketergantungan pada crib, yang mudah ditebak dengan tidak benar.

Dari titik teknik, alat Inggris menyerupai Bomby Polish. Setiap Bombe memiliki 12 set tiap rotor, dan bekerja secara sinkron melalui semua kemungkinan posisi rotor. Setiap Bombe mempunyai beban satu ton dan panjang 7 feet, lebar 2 feet dan tinggi 6.5 feet. Bombes dioperasikan oleh anggota dari Women's Royal Naval Service, "Wrens", yang bertanggung jawab untuk mengelola mesin, menuliskan kombinasi rotor yang ditemukan mesin, dan memulai mesin setelah setiap potensial kombinasi yang benar ditemukan. Proses tunggal untuk kombinasi yang diberikan rotor memakan waktu 15 menit. Untuk menguji semua 60 kemungkinan kombinasi rotor, 15 jam dibutuhkan.

Bombes pertama diambil dan digunakan pada bulan Oktober 1941. Mereka dinamakan dengan nama seperti Agnew, Warspite, Victorious, atau Tiger. Sekitar 210 Bombes dibangun dan digunakan Inggris selama perang.

Partisipasi Amerika dalam Produksi Kriptologi Bombe

Representatif dari kedua angkatan bersenjatan U.S dan angkatan lautnya mengunjungi Bletchley Park pada tahun 1941, dan mereka menjadi sadar tentang kesuksesan Inggris dengan Enigma. Perubahan situasi pada musim panas 1942, ketika menjadi nyata bahwa keterbatasan sumber Inggris untuk menunda rencananya membangun Bombe dengan empat rotor dengan kecepatan tinggi yang mampu memecahkan Enigma dengan cepat. Angkatan Laut Amerika memberikan rancangan tersebut kepada Joseph Desch, direktur penelitian dari National Cash Register Company (NCR) yang berada di Dayton, Ohio. Rancangan amerika didasarkan pada prinsip kriptologi yang sama seperti Bombe Inggris, tetapi diperbaiki dari tekniknya. Dalam keterangan, sedikit intervensi manusia dibutuhkan dan mesin mempunyai kemampuan mencetak semua setting rotor yang tidak dapat dieliminasi berdasarkan pada crib yang digunakan untuk inisialisasi mesin. Seperti versi Inggris, Bombes Amerika biasanya menemukan dua atau tiga kemungkinan solusi yang benar. Proses pertama untuk satu kombinasi rotor memakan waktu sekitar 20 menit. Pada bulan Mei 1943, dua Bombe Amerika, Adam dan Eve, berhasil diuji. Pada musim panas tahun 1943, Bombes dimulai ditransfer dari Daton, Ohio ke Washington, D.C. Mereka dioperasikan oleh wanita di angkatan Laut Amerika, sehingga disebut "Waves" (Women Accepted for Volunteer Emergency Service). Sekitar 120 Bombe dibangun dan dioperasikan sebelum berakhirnya Perang Dunia II.

Kesimpulan

Dengan adanya pemecahan kode Enigma didapatkan pelajaran berharga bagi para perancang algoritma, protokol dan sistem. Pertama tidak membantu dalam keamanan jika hanya menjagakan kehebatan mesin atau cipher. Enigma versi Angkatan Bersenjata Jerman direkonstruksi kembali oleh ahli kriptologi Marian Rejewski, dengan analisis matematikanya dalam pengujian kunci harian yang didapatkan dari mata-mata Perancis. Suatu ketika Enigma tersebut telah didapatkan oleh angkatan laut Inggris melalui kapal boat milik Jerman yang tenggelam di laut. Besarnya jumlah kunci dibandingkan dengan cipher modern tidak membantu dalam pemecahannya, oleh karena itu ahli kriptologi Inggris menggunakan metode terbaik pencarian kunci dengan exhaustic search.

Metode ini merekonstruksi berbagai kunci harian satu per satu. Kriptanalisis menambahkan bantuan dengan adanya mesin elektromekanik baru yang dapat mempercepat waktu komputasi dan fase berulang dalam analisis kriptologi. Mesin tersebut diantaranya 'Bomby' dari Inggris dan 'Bombes' dari Amerika yang nantinya menjadi dasar dalam hardware modern.
Serangan dengan mengetahui plainteks dapat memudahkan penyusunan stuktur pesan dan pengiriman kembali pesan melalui jaringan dengan kunci harian berbeda. Serangan yang pertama dan terkenal melawan Enigma menggunakan metode ANX dengan *Crib Room* dan *Bombe* yang berasal dari Inggris.

Pengelolaan kunci dengan perubahan enkripsi kunci pesan merupakan kelemahan dari protokol Enigma, tidak hanya membuat metode rekontruksi harian saja tetapi juga mengancam kerahasian mesin cipher itu sendiri. Pengelolaan kunci menjadi subjek menarik dalam perancangan kunci dalam sistem dan protokol modern.

Pelajaran berharga lainnya adalah dalam pemecahan kode Enigma diperlukan uang, waktu, orang, perhatian, dan resiko yang tidak sedikit. Operasi pemecahan pesan Jerman oleh ahli kriptologi Inggris di Bletchley Park membutuhkan ratusan orang, organisasi, perhatian lebih, dan visi yang jelas. Setiap negara telah berusaha untuk memecahkan Enigma, tetapi ahli kriptologi Jerman tidak pernah percaya bahwa sebeluma atau selama Perang Dunia II, Enigma telah dipecahkan.

DAFTAR PUSTAKA

[1] Rejewski, Marian. (1980). An Application of the Theory of Permutations in Breaking the Enigma Cipher. *http://frode.home.cern.ch/frode/crypto/rew80.pdf*. Tanggal akses : 28 September 2006 pukul 04:48 PM.

[2] Gaj, Kris. And Arkaiusz Orlowski. (2003). Facts and myts of Enigma : breaking stereotypes. *http://ece.gmu.edu/courses/ECE543/viewgraphs_F03/EUROCRYPT_2003.pdf*. Tanggal akses : 28 September pukul 04:48 PM.

[3] Sullivan, Geoff. And Frode Weierud. (2006). Breaking German Army Ciphers. *http://www.tandf.co.uk/journals/pdf/papers/ucry_06.pdf*. Tanggal akses : 28 September pukul 04:48 PM.

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

[5] Kruh Louis. And Cipher Deavours.(2002). The Commercial Enigma: Beginnings Of Machine Cryptography. Departemen of Mathematics, Kean University of New Jersey.