VOL.7, No.2, September 2008 ISSN 1412-6028

DigitalPotpourri

Journal of Computing and Information System

ABFII PERBANAS
Jalan Perbanas, Karet Kuningan
Jakarta 12940 Indonesia
phone (+62.21)525.2533
fax.(+62.21)522.8460
website http://www.perbanasinstitute.ac.id

Seandainya Enigma Tidak Terpecahkan

Nidjo Sandjojo*

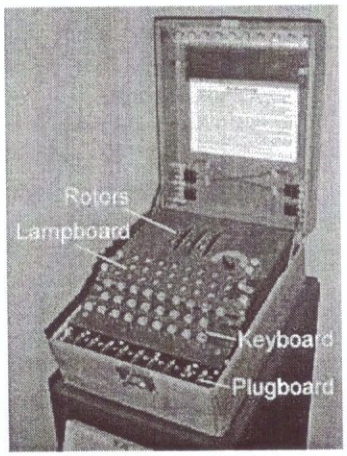
* Penulis adalah Dosen ABFII Perbanas

Seandainya Enigma Tidak Terpecahkan

Nidjo Sandjojo
Email: nsandjoj@hotmail.com

Abstract. *Information secrecy transmitted trough media communication is an important aspect should be taken into consideration. One way to keep information secret is encrypted by cipher. Encrypted information could not be read unless decrypted by the same cipher. During the World War II, enigma was the famous chipper used mostly by the German Forces. If the Allied Forces was not able to decript the information encrypted by Enigma, then the history of the world would be different.*
Key words*: Enigma, enkription, dekription, cryptography.*

Pendahuluan



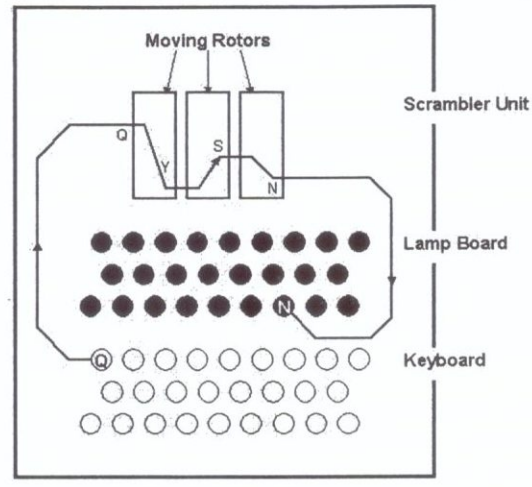
Gambar 1. Mesin Enigma

Sejarah kriptografi telah membuktikan bahwa sandi (*ciphers*) yang katanya tidak terpecahkan, ternyata dapat dipecahkan dalam waktu singkat begitu mesin tersebut digunakan secara luas. Salah satu contoh yang terkenal adalah mesin enkripsi *Enigma* yang kodenya dapat dipecahkan oleh para ahli kriptografi Inggris di *Bletchley Park*. Hal tersebut berakibat terbongkarnya informasi tentang operasi militer Jerman yang kemudian menyebabkan kerugian yang sangat besar tehadap kapal selam Jerman.
Mesin Enigma, seperti nampak pada gambar1[1], merupakan mesin sandi (*cipher*) yang digunakan untuk mengenkrip (*encrypt*) dan mendekrip (*decrypt*) berita-berita rahasia. Lebih tepatnya, mesin Enigma adalah satu keluarga dari mesin rotor yang berhubungan dengan elektro-mekanik yang terdiri dari berbagai model berbeda.

Enigma tersebut digunakan secara komersial sejak tahun 1920-an, yang diadopsi oleh militer dan pemerintah dari sejumlah negara. Sedangkan yang paling terkenal adalah yang digunakan oleh Angkatan Laut Jerman sebelum dan selama Perang Dunia ke II.
Model yang digunakan oleh militer Jerman, disebut *Wehrmacht Enigma* merupakan versi yang paling banyak dibicarakan. Mesin jenis tersebut menjadi terkenal karena para ahli kriptologi dari Pasukan Sekutu mampu men-dekrip sejumlah besar berita yang telah disandi dengan mesin tersebut. Pembongkaran sandi mesin Enigma versi non-militer awalnya dilakukan di tahun 1932 oleh ahli kriptografi Polandia, yaitu: Marian Rejewski, Jerzy Różycki dan Henryk Zygalski dari Biro Sandi (*Cipher Bureau*). Pada pertengahan tahun 1939 rekonstruksi dan model dekripsi oleh Polandia disampaikan kepada Inggris dan Pernacis. Unit intelijen yang bertugas menangani *cryptosystem*, yang diberi kode sandi "ULTRA", memperoleh keuntungan dari sumber ini dan merupakan bantuan yang sangat penting kepada Pasukan Sekutu dalam upayanya untuk memenangkan perang.
Mesin Enigma adalah salah satu dari mesin sandi (*cipher*) yang sangat populer dan banyak digunakan selama Perang Dunia II, khususnya oleh Jerman. Seperti nampak pada gambar 1, salah satu contoh mesin Enigma terdiri dari *Rotors, Lampboard,*

Keyboard, dan *Plugboard.* Mesin tersebut menyediakan substitusi menggunakan alphabet yang berobah-robah secara terus-menerus. Mesin Enigma digunakan secara komersial sejak awal tahun 1920-an, dan diadopsi oleh militer dan pemerintahan dari berbagai negara, dan yang paling terkenal adalah oleh Nazi Jerman.

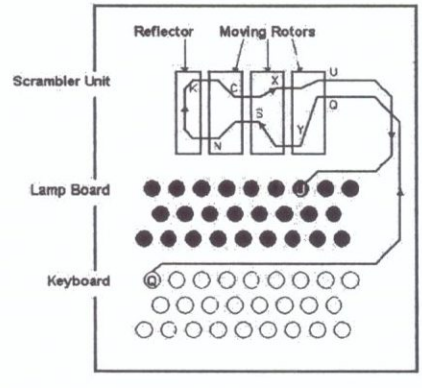
Enigma dirancang untuk mengungguli teknik pembacaan atau pemecahan sandi dengan secara terus-menerus melakukan penggantian alfabet atau abjad. Seperti halnya mesin rotor yang lain, Enigma menerapkan penggantian sandi multi-abjad (*polyalphabetic substitution cipher*) dengan periode yang lama. Dengan menggunakan rotor bertakik tunggal (*single-notched*), periode dari mesin tersebut adalah 16.900 atau (26 x 25 x 26). Periode yang panjang ini sangat membantu dalam melindungi alphabet yang tumpang tindih (*overlapping*).



Gambar 2: Bagian-bagian Mesin Enigma

Mesin Enigma

Mesin Enigma pertama kali diporduksi sebagai produk komersial pada tahun 1923 oleh orang Jerman bernama Arthur Scherbius. Tujuan dibuatnya mesin Enigma adalah untuk keperluan bisnis dengan menyediakan sarana yang dapat digunakan untuk keamanan komunikasi. Seperti pada Gambar 2^2, secara garis besar skema mesin Enigma versi komersial, terdiri dari tiga bagian utama, yaitu: (i) *Scrambler Unit*, (ii) *Lamp Board,* dan (iii) *Keyboard.* Konsepsi mesin ini sebenarnya cukup sederhana. Setiap kali operator atau pengguna menekan huruf di *keyboard* maka ada satu huruf di papan-berlampu (*lamp-board*) yang menyala yang berkaitan dengan *ciphertext*-nya. Kemudian operator mencatat *ciphertext* tersebut, dan dapat meneruskan mengetik huruf lain.



Gambar 3. Scrambler Unit dengan Reflector

Pengguna mengetik pesan dengan menggunakan keyboard dan tiap kali keyboard ditekan, akan menimbulkan tenaga satu dari 26 arus listrik huruf di dalam mesin. Tenaga disalurkan dari *keyboard* ke salah satu dari 26 hubungan ujung di dalam unit acak (*scrambler*). Tenaga tersebut kemudian diteruskan melalui tiga rotor, masing-masing rotor saling dikaitkan sehingga rotor tersebut merubah dari satu huruf ke huruf lain. Mesin tersebut sekarang telah menerapkan operasi acak terhadap

huruf aslinya. Pengkabelan (*wiring*) dari mesin tersebut dirobah setelah setiap huruf disandi dengan cara memutar rotor pertama satu posisi putaran, dan seterusnya sampai dengan 26 huruf, sehingga walaupun menekan huruf yang sama dua kali akan menghasilkan sandi (*ciphertext*) yang berbeda.

Salah satu faktor penting pada rancangan Enigma adalah mudahnya untuk menggunakan mesin tersebut. Penerapan operasi acak satu arah yang sederhana seperti yang dijelaskan, mengandung kerugian; untuk mendekrip pesan tersebut perlu membentuk ulang mesin tersebut sehingga untuk memasukkan tenaga dari keyboard ke ujung yang berlawanan dari rotor tersebut. Hal tersebut membuat teknis mesin menjadi lebih sulit dan yang lebih penting mempersulit penggunaannya dan hal tersebut lebih membuat kecenderungan adanya kesalahan.

Enigma memecahkan permasalahan tersebut dengan menambahkan satu rotor pembalik rangkaian (*circuit*) tersebut melewati rotor. Hal tersebut menghubungkan setiap ujung kontak dengan kontak yang lain, sehingga mengarahkan sirkit/rangkaian (*circuit*) kembali melalui tiga rotor tersebut ke salah satu dari 26 kontak input. Hasilnya seperti pada Gambar 3^3 diatas.

Jerman menggunakan Enigma pada Perang Dunia ke II

Enigma versi komersial dipamerkan pada saat pameran perdagangan pada tahun 1923, tetapi kemudian menarik perhatian militer Jerman. Hasilnya adalah penarikan dari pemasaran mesin Enigma yang kemudian diproduksi dan diperbaiki khusus untuk keperluan militer.

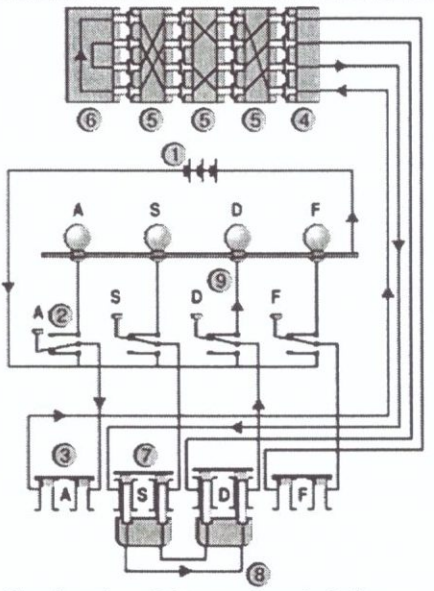
Pada saat pecah Perang Dunia ke II, mesin Enigma digunakan secara luas disebagian besar militer Jerman. Dengan ukuran yang kecil, mudah dibawa dan mudah digunakan membuatnya menjadi sarana sangat ideal untuk digunakan sebagai bagian dari strategi Serangan Kilat (*Blitzkrieg*) Jerman dimana mobilitas dan kerja sama yang erat antara pasukan darat dan pasukan udara yang merupakan kuci kesuksesan pasukan Jerman.
Salah satu prinisip perang elektronika (*Electronic Battlefields*) dimana mesin Enigma memerankan sebagai sarana pokok selama Perang Dunia ke II adalah pertempuran Atlantik (*Battle of the Atlantic*). Kapal Selam Jerman (*Undersea = U Boats*) dilengkapi dengan mesin Enigma yang digunakan untuk mengirimkan laporan secara periodik dan juga mengamati konvoi Pasukan Sekutu. Penyebaran informasi tentang posisi konvoi tersebut merupakan berita penting bagi *U Boats* sehingga dapat memusatkan sejumlah besar kapal untuk menyerangnya sehingga dapat menenggelamkan sebanyak mungkin kapal musuh. Demikian juga, bagi Pasukan Sekutu informasi tentang posisi *U Boats* adalah penting sehingga dapat menghindarkan konvoi pasukannya dari serangan *U Boats*. Keamanan atau kemudahan membaca Enigma yang dimiliki oleh pasukan Angkatan Laut Jerman semasa pertempuran Atlantik merupakan faktor kunci kelangsungan hidup Inggris Raya semasa periode ini.

Terdapat banyak variasi dan peningkatan dalam pembangunan mesin Enigma dan dalam prosedur penggunaannya semasa Perang Dunia ke II. Pada awal peningkatannya dikenalkan dua tambahan rotor sehingga tiga dari lima rotor tersebut dapat dipasang dengan sembarang urutan. Angkatan Laut Jerman juga mengenalkan empat variasi rotor yang lebih kuat di tahun 1942.

Cara Kerja. Nampak pada Gambar 4^4, seperti halnya dengan mesin-mesin rotor lain, Enigma adalah kombinasi dari sistem mekanik dan elektrik. Mekanisme mekaniknya terdiri dari satu keyboard, satu set disk berputar (*rotating disks*) disebut rotor yang

diatur saling berdampingan sepanjang sebuah kumparan, dan satu mekanisme melangkah untuk memutar satu atau beberapa rotor dengan setiap kali menekan kunci. Meknisme yang persis bervariasi, tetapi bentuk yang paling umum adalah rotor yang disebelah kanan bergerak sekali setiap ada kunci yang ditekan, dan kadang-kadang menggerakkan rotor-rotor sebelahnya. Pergerakan dari rotor secara terus menerus menghasilkan satu transformasi kriptografi yang berbeda setelah setiap kali kunci ditekan.

Gambar 4: diagram pengkabelan Enigma menggambarkan aliran arus listrik. Kunci 'A' di sandi ke kunci 'D'. D menghasilkan 'A' tetapi 'A' tidak pernah menghasilkan 'A'.
Bagian-bagian mekanik tersebut bertindak sedemikian rupa untuk membentuk arus listrik (*circuit*) yang bervariasi, sedangkan penyandian huruf yang sebenarnya dilakukan secara elektrik. Ketika satu kunci ditekan, sirkit tersebut diselesaikan, arus listrik mengalir melalui berbagai componen dan akhirnya menyalakan salah satu dari lampu-lampunya yang mengindikasikan huruf output. Misalnya, ketika akan menyandi berita yang dimulai dengan huruf ANX, operator pertama kali menekan huruf A, dan lampu Z mungkin menyala, yang menandakan bahwa Z tersebut yang menjadi huruf pertama sandi (*ciphertext*). Kemudian operator menekan huruf N, dan seterusnya.



Gambar 4. Diagram Pengkabelan Enigma

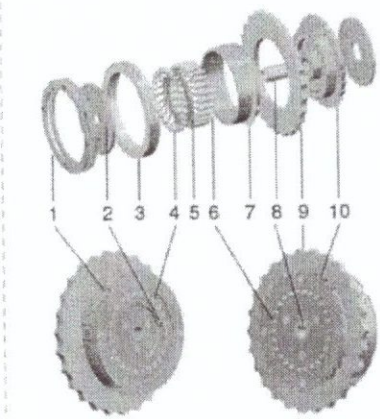
Untuk menjelaskan cara kerja Enigma, digunakan diagram pengkabelan seperti pada Gambar 4. Untuk menyederhanakan contoh, hanya empat komponen yang ditunjukkan, sedangkan yang sebenarnya ada 26 lampu, kunci (*keyboard*), steker (*plugs*), dan pengkabelan di dalam rotor. Arus listrik mengalir dari batery (1) melalui tombol huruf dua arah (*bi-directional letter-switch*) yang ditekan (2) ke *plugboard* (3). *Plugboard* tersebut mengijinkan pengkabelan ulang koneksi antara *keyboard* (2) dan *fixed entry wheel* (4). Berikutnya, arus berlanjut melalui plug yang tidak digunakan yang disebut *closed plug* (3) via *entry wheel* (4) melalui tiga rotor pada *Wehrmacht Enigma* atau empat rotor pada *Kriegsmarine M4 or Abwehr variant* (5) dan memasuki pemantul atau *reflector* (6). Reflektor mengembalikan arus, via alur yang berbeda, kembali ke rotor (5) dan *entry wheel* (4), dan berlanjut melalui plug "S" yang dihubungkan dengan kabel (8) ke plug "D" dan tombol dua-arah atau *bi-directional* lain (9) ke lampu *light-up*.
Perubahan alur elektrik secara terus menerus melalui unit tersebut karena perputaran rotor (yang menyebabkan pin kontak untuk merobah setiap kali kunci ditekan) yang mengimplementasikan enkripsi polyalphabetic yang menyediakan keamanan tinggi Enigma.

Gambar 5. Tiga Rotor Berurutan

Rotor. Rotor-rotor, seperti nampak pada Gambar 5[5], yang juga disebut *wheels* atau *drums*, yang dalam bahasa Jerman disebut *Walzen,* merupakan jantung dari mesin Enigma. Rotor tersebut kira-kira berdiameter 10 cm, yang melakukan enkripsi sederhana, yang disebut substitusi cipher sederhana. Sedangkan yang membuat menjadi kompleks adalah dengan digunakannya beberapa seri rotor, biasanya tiga atau empat, serta pergerakan dari rotor-rotor tersebut secara regular yang menyediakan tipe enkripsi yang lebih kuat.

Setiap rotor memiliki berbagai variasi posisi awal, selain hanya urutan ABC, tetapi dapat juga ACB. Pada model-model Enigma berikutnya, ada tambahan sebuah ring abjad variabel di setiap rotor. Pada sebagian besar versi Enigma yang digunakan militer Jerman memiliki sebuah *plugboard* yang dalam bahasa Jerman disebut *Steckerbrett* yang fungsinya untuk pertukaran abjad. Meskipun demikian, kunci kombinasi yang kompleks tersebut masih dapat dengan mudah berkomunikasi dengan pengguna lain, seperti halnya versi yang sebelumnya yang belum rumit, yang terdiri dari: rotor-rotor yang digunakan, urutan rotor, posisi ring, posisi awal, dan koneksi *plugboard*. Hal inilah yang membuat mesin Enigma merupakan satu sistem enkripsi yang istimewa.

Ketika ditempatkan di mesin Enigma, sebuah rotor dapat di set pada salah satu dari 26 kemungkinan posisi. Tiap rotor berisi satu atau kadang-kadang banyak *notch*, digunakan untuk mengendalikan perpindahan rotor. Contoh rotor yang terurai dengan nama-nama bagiannya nampak pada Gambar 6[6] yang terdiri dari:



Gambar 6. Rotor Diurai

1. *notched ring*
2. *marking dot for "A" contact*
3. *alphabet ring*
4. *plate contacts*
5. *wire connections*
6. *pin contacts*
7. *spring-loaded ring adjusting lever*
8. *hub*
9. *finger wheel*
10. *ratchet wheel*

Awal Diskripsi. Jerman menganggap bahwa Enigma adalah mesin enkripsi yang tidak terpecahkan. Ternyata anggapan Jerman tersebut salah.

Biro Sandi Polandia merupakan negara pertama yang berusaha membongkar mesin sandi Enigma. Biro Sandi Rolandia, pada tahun 1928 secara tidak sengaja menerima Enigma yang seharusnya dikirim ke Kedutaan Jerman di Warsawa dengan menggunakan angkutan umum.

Intel Polandia telah membaca *cryptogram* yang dihasilkan Enigma sejak Desember 1932. Akibat modifikasi, baik mesin maupun prosedur operasinya, mengakibatkan

gangguan yang memerlukan cara baru untuk dapat memecahkan kode Enigma. Pada bulan April dan Mei 1939, Polandia mengikat perjanjian dengan Inggris dan Perancis. Polandia menyadari terjadinya perobahan arah dan langkah situasi politik di Eropa, pada pertengahan tahun 1939 memutuskan untuk berbagi hasil kerjanya dengan Inggris dan Perancis. Sehinga pada saat konferensi di Warsawa tanggal 26 juli 1939, berjandji untuk memberikan mesin Enigma yang dibuat oleh Polandia sekaligus dengan rincian teknik memecahkan kode yang telah dikembangkan, yaitu: lembaran yang berlobang (*perforated sheets*) dan *cryptologic bomb* yang dalam bahasa Polandia disebut *bomba kryptologiczna*.

Kemajuan pertama dalam memecahkan sandi Enigma dilakukan oleh Polandia pada tahun 1930-an. Pada saat itu, mesin yuang digunakan oleh Jerman hanya memiliki tiga rotor pada enam kemungkinan kombinasi (3 nPr 3). Walaupun pemecahan sandi pada tahun 1930-an merupakan satu prestai yang besar, namun Polandia tidak dapat lagi memecahkan sandi Enigma setelah Jerman meningkatkan jumlah kmobinasi rotor dengan menambahkan dua rotor lagi. Pada bulan September 1938, Jerman merobah sistem indikator yang sudah diketahui oleh Polandia. Sistem tersebut lebih komplek dari pada sistem yang sebelumnya, tetapi masih tetap menggunakan pengulangan satu kelompok tiga huruf.

Inggris kemudian meneruskan pekerjaan memecahkan sandi dengan memulai dari yang ditinggalkan oleh Rolandia. Oleh Alan Turing, seorang ahli matematika muda, membuat sebuah mesin untuk memecahkan Enigma sambil bekerja pada kantor pemerinkat Inggris. Mesin hasil karya Alan Turing ini disebut Turing Bombe, merupakan cikal bakal komputasi modern.

Dekripsi (*Decryption*) di Bletchley Park. Pada bulan Jaruari 1939, pertemuan diadakan di Paris antara perwakilan-perwakilan dari intel Inggris, Polandia, dan Pernacis yang telah memperoleh informasi tentang Enigma melalui seorang informan (*clandestine*). Setelah pertemuan tersebut, pemerintah Sekolah Kode dan Sandi Pemerintah Inggris (GC&CS) membahas untuk memecahkan sandi Enigma. Inggris memulainya dengan menyediakan cukup sumber daya untuk publikasi yang dibutuhkan. Inggris juga mempekerjakan seorang ahli matematik, Alan Turing, untuk merancang versi yang lebih baru dari versi Bombe yang dibuat oleh Polandia. Bombe Inggris lebih maju dibandingkan dengan versi yang dimiliki oleh Polandia dalam hal kecepatan operasi dan ketergantungan pada sistem indikator khusus.

Bagaimana jika mesin Enigma tidak terpecahkan?

Keunggulan Sekutu pada komunikasi rahasia musuh dipandang sebagai satu kontribusi yang penting dalam kemenangan Perang Dunia ke II (PD II). Di Eropa, keberhasilan Sekutu, khususnya Unit *Cryptosystems*, membaca sandi yang dibuat oleh Jerman sangat membatu dalam memperoleh kemenangan demi kemenangan pada PD II. Informasi yang dimiliki tentang lokasi kapal selam Jerman, menyebabkan Sekutu terhindar dari kerugian yang bakal terjadi, sehingga personnel dan meterial dapat sampai ke Inggris. Unit *Cryptosystems* yang dibentuk oleh Sekutu, diberi kata sandi "ULTRA".

Tetapi bagaimana jika Sekutu tidak dapat memecahkan sandi musuh yang dibuat dengan mesin Enigma? Pertanyaan ini tidak dapat dijawab dengan satu jawaban saja. Hal tersebut karena jaringan komunikasi semua pasukan Jerman yang menggunakan sandi yang dihasilkan oleh mesin Enigma memiliki kunci Enigma masing-masing. Misalnya Angkatan Darat memiliki kunci sendiri, demikian juga halnya dengan Angkatan Lautnya baik yang dibawah air (*submarines*) serta yang diatas air (*surface*

vessels). Sehingga salah satu jawaban adalah ketergantungan pada sistem persandian yang digunakan yang menjadi bahan pertimbangan. Solusinya dihasilkan oleh Marian Rejewski di Rolandia pada tahun 1931 dan Alan Turing serta Gordon Welchman di Inggris pada tahun 1939, tanpa mereka mungkin mesin sandi Enigma Belem terpecahkan.

Pengetahuan yang diperoleh tentang keberadaan papal selam Jerman, mengakibatkan berkurangnya papal cargo Sekutu ditenggelamkan olehnya, sehingga meningkatkan persediaan logistik yang dipasok dari Amerika ke Inggris melalui Atlantik. Hal tersebut berarti menigkatkan persediaan amunisi, persenjataan, bahan bakar, makanan, dan material penting lainnya untuk keperluan perang. Peningkatan ini terjadi karena keberhasilan ULTRA dalam menyadap dan menterjemahkan sandi yang dihasilkan Enigma. Sebagai akibat, maka invasi ke Afrika Utara, dan Italy, serta Eropa, tidak tertunda dan lebih sukses dari pada bila seandainya ULTRA tidak berhasil mendekrip sandi yang dibuat dengan Enigma.

Salah kasus yang penting adalah, bagaimana jira pesan sandi Enigma yang menjelaskan dimana dan kapan kapal-kapal Jerman yang membawa bahan bakar yang akan digunakan oleh pasukan Rommel di Afrika tidak dapat dipecahkan? Lembaga pemecahan kode (*code-breaking*) Inggris di Bletchley Park, yang lokasinya kurang lebih 60 mil ke arah barat laut London, berhasil memecahkan pesan yang melaporkan bahwa bahan bakar yang dikonsumsi oleh pasukan dibawah pimpinan Rommel telah melampaui persediaan bahan bakar yang dimiliki, dan bahan bakar yang ada hanya untuk sampai 26 Agustus 1946. Berdasarkan informasi tersebut Kepala Staf Pasukan Inggris menginstruksikan kepada pasukan yang ada di Mediterranean untuk mencegat papal-kapal Jerman yang membawa supply bahan bakar. Kemudian papal-kapal yang membawa bahan bakar tersebut ditenggelamkan satu persatu baik oleh pesawat pembom maupun kapal selam yang bermarkas di Malta. Bahan bakar yang dimiliki oleh Rommel menjadi semakin menipis dan sangat membatasi pergerakan pasukan tank yang memerlukan banyak bahan bakar. Pada akhirnya, ketika Jenderal Bernard Law Montgomery merebut dan mengalahkan Rommel di El Alamein, yang dapat dilakukan oleh Rommel hádala mundur. Tetapi bagaimana jika Inggris tidak dapat memecahkan pesan yang ditujukan kepada Rommel tentang rencana pengiriman bahan bakar. Tentu Rommel tidak mengalami krisis bahan bakar sehingga pergerakan pasukannya tidak terhambat dan dapat bebas bergerak sampai ke Afrika Utara.

Kesimpulan

Kasus keberhasilan Sekutu dalam memecahkan pesan yang disandi dengan mesin Enigma, merupakan bukti bahwa mesin cipher yang dikatakan tidak terpecahkan, ternyata dapat dipecahkan setelah melalui berbagai upaya.

Keberhasilan Pasukan Sekutu dalam memecahkan kode-kode yang dihasilkan mesin Enigma merupakan rahasia terbesar PD II. Awal keberhasilan tersebut dimulai di Polandia pada tahun 1930-an. Namun awal keberhasilan yangn dibuat oleh Polandia tidak cukup untuk mendekrip kode yang dibuat oleh mesin Enigma versi militer yang sudah dimodifikasi. Alan Turing dari Inggris kemudian yang melanjtukan pekerjaan yang telah dirintis oleh Polandia sehingga berhasil men-dekrip kode Enigma. Dari keberhasilan men-dekrip kode sandi Enigma tersebut menyebabkan Sekutu dapat menghindari kerugian baik personnel maupun material perang, yang pada akhirnya menyebabkan kemenangan Sekutu di PD II.

Daftar Pustaka

Crowley, Robert (editor), 2001. *The Collected What If?: Enigma Uncracked: The Allies fail to break the German cipher machine by David Khan*, American Historical Publications, Inc., New York

Howland, John E., 2002. *Introduction to Internet Security*, http://www.cs.trinity.edu/~jhowland/security/security/security.html, http://www.cs.trinity.edu/jhowland, Akses terakhir: 12 Oktober 07

Pfleeger, Charles P., 1997. *Security in Computing, Second Edition*, Prentice-Hall, Upper Saddle River, New Jersey.

Stallings, William, 2003. *Cryptography and Network Security: Principles and Practices, 3rd Edition*, Pearson Education, Inc., Upper Saddle River, New Jersey.

-----, *About Enigma and Its Decryption,* http://homepages.tesco.net/~andycarlson/enigma/about_enigma.html, Akses terakhir: 21 Oktober 2007

-----, *Cracking Enigma*, http://library.thinkquest.org/28005/flashed/timemachine/courseofhistory/bombe.s html, Akses terakhir: 9 Maret 2007

-----, *Cryptanalysis of the Enigma*, http://en.wikipedia.org/wiki/Cryptanalysis_of_the_Enigma, Akses terakhir: 9 Maret 2007

-----, *Enigma machine*, http://en.wikipedia.org/wiki/Enigma_machine, Akses terakhir: 12 Oktober 07

-----, *Marian Rejewski*, http://en.wikipedia.org/wiki/Marian_Rejewski, Akses terakhir: 12 Oktober 07

---

[1] *Marian Rejewski*, http://en.wikipedia.org/wiki/Marian_Rejewski

[2] *About Enigma and Its Decryption,* http://homepages.tesco.net/~andycarlson/enigma/about_enigma.html

[3] *About Enigma and Its Decryption,* http://homepages.tesco.net/~andycarlson/enigma/about_enigma.html

[4] *Enigma machine*, http://en.wikipedia.org/wiki/Enigma_machine

[5] *Enigma machine*, http://en.wikipedia.org/wiki/Enigma_machine

[6] *Enigma machine*, http://en.wikipedia.org/wiki/Enigma_machine