Masagus Krisna Ismaliansyah
13503115

STUDI DAN KRIPTANALISIS PADA ENIGMA CIPHER

Abstraksi

Makalah ini membahas tentang studi dan kriptanalisis pada mesin enigma. Mesin enigma merupakan sebuah mesin enkripsi yang digunakan oleh tentara Jerman pada saat perang dunia II. Mesin enigma menggunakan mekanisme rotor yang berputar untuk melakukan enkripsi huruf. Rotor tersebut akan berputar apabila mendapatkan masukan dari papan kunci. Cara kerja mesin enigma berdasarkan ide dari insinyur berkebangsaan Amerika, Edward Hugh Hebern.

Kriptanalisis mesin enigma pertama kali dilakukan oleh pemerintah Polandia, tetapi kriptanalisis ini hanya dapat memecahkan versi awal mesin enigma yang digunakan oleh tentara Jerman. Setelah kemampuan mesin enigma ditingkatkan, kriptanalisis ini tidak dapat memecahkan penyandian tersebut. Selanjutnya, kriptanalisis dilakukan oleh Bletchley Park dan berhasil memecahkan kode enigma tersebut. Tetapi, akibat dari berhasilnya pemecahan kode ini, tentara jerman meningkatkan keamanan mesin enigma dengan menambahkan satu buah rotor lagi sehingga jumlah rotor mesin tersebut menjadi 4. Tetapi sayangnya, walaupun telah ditingkatkan menjadi 4 buah rotor, mesin enigma yang dipakai oleh tentara Jerman tersebut masih dapat dipecahkan oleh Bletchley Park walaupun membutuhkan waktu yang cukup lama.

Pada pembuatan makalah ini, program Enigma Simulator versi 6.0 digunakan untuk melihat cara kerja mesin enigma. Selain itu, program ini juga digunakan untuk melakukan verifikasi terhadap teknik manual yang digunakan untuk menyimulasikan cara kerja mesin enigma.

Kata Kunci : Mesin enigma, Enigma Simulator, Kriptanalisis Mesin Enigma.

I. Pendahuluan

Pada bab ini akan dijelaskan tentang latar belakang, tujuan, lingkup masalah, dan batasan masalah dalam pembuatan makalah ini.

I.1. Latar Belakang

Latar belakang pemilihan mesin enigma sebagai bahan makalah ini adalah sejarah mesin tersebut yang berhubungan dengan tentara Nazi pada Perang Dunia II.

I.2. Tujuan Pembuatan Makalah

Tujuan pembuatan makalah ini adalah untuk memperdalam pengetahuan tentang mesin enigma baik dari segi sejarahnya maupun dari segi teknik kriptografinya.

I.3. Lingkup Bahasan

Makalah ini melingkupi tentang sejarah mesin Enigma, komponen-komponen mesin Enigma, cara kerja mesin enigma, teknik enkripsi dan dekripsi mesin enigma.

I.4. Batasan Masalah

1. Hanya membahas mengenai teknik enkripsi dan deskripsi pada enigma cipher.
2. Hanya membahas teknik manual enkripsi dan dekripsi mesin enigma.

II. Pengenalan Mesin Enigma

Pada bab ini akan dijelaskan tentang sejarah penggunan mesin enigma, komponen penyusun mesin enigma, serta cara kerja mesin enigma.

II.1. Sejarah Penggunaan Mesin Enigma

Sejarah mesin enigma meliputi tentang kemajuan teknologi, militer, dan dunia hitam mata-mata, pemecah kode dan intel kedalam kengerian yang nyata.

Belum pernah dalam sejarah sebuah mesin kriptografi yang melibatkan kehidupan banyak orang di dalamnya, seperti pada Perang Dunia II. Enigma adalah contoh yang paling menarik tentang peperangan antara pembuat kode dan pemecah kode. Enigma menunjukkan pentingnya kriptografi bagi mata-mata kalangan militer dan juga sipil.

II.1.a. Asal Usul Mesin Enigma

Dengan perkembangan komunikasi tanpa kabel pada permulaan abad 19, maka komunikasi yang aman sangat dibutuhkan oleh pihak militer dan juga sipil. Penelitian untuk mengganti pembuatan cipher secara manual dimulai. Hal ini dikarenakan pembuatan secara manual membutuhkan waktu yang lama serta tidak praktis. Pada tahun 1917, seorang berkebangsaan Amerika Edward Hugh Hebern mengembangkan sebuah mesin kriptografi yang menggunakan piringan putar, setiap piringan menampilkan cipher substitusi. Ide Hebern tersebut merupakan dasar untuk membuat mesin yang sama, yang dikembangkan oleh negara lainnya.

Pada tahun 1918, Arthur Scherbius, mempatenkan sebuah mesin cipher yang menggunakan rotor. Mesin tersebut dikenalkan kepada tentara jerman, tetapi mereka tidak tertarik. Pada tahun 1923, paten tersebut jatuh pada Chiggreiermaschinen-AG, sebuah perusahaan yang direkturnya adalah Scherbius, perusahaan inilah yang pertama kali memperdagangkan mesin tersebut. Pada tahun 1925, Scherbius membeli hak paten mesin yang sama dari Dutchman Koch untuk mengamankan patennya sendiri, baru pada tahun 1927 kesepakatan didapatkan.

Mesin enigma pertama, dengan nama kode Enigma A, mulai diperdagangkan di pasaran pada tahun 1923. Saat pertama kali diluncurkan, ukuran mesin tersebut masih sangat besar dan berat. Selain itu mesin ini juga dilengkapi dengan papan ketik dengan berat sekitar 50 kiloan. Enigma B diluncurkan tidak lama setelah Enigma A dikenalkan ke pasar, tetapi berat dan ukurannya tidak berubah sehingga tidak menarik minat untuk penggunaan di bidang militer. Pengembangan bagian pemantul pada mesin Enigma, yang merupakan ide dari kerabat Scherbius, Willi Korn, membuat mesin tersebut dapat dirancang lebih kecil dan ringan sehingga lahirlah Enigma C. Tetapi, pengembangan mesin tersebut tidak berhenti di situ saja, pada tahun 1927, Enigma D dikenalkan dengan penggantian papan ketik dengan panel lampu yang membuat mesin tersebut lebih praktis. Enigma D diperdagangkan dengan berbagai versi, dan diperjualbelikan di Eropa untuk keperluan militer serta diplomatik.

Tentara Swiss menggunakan mesin Enigma versi K, angkatan laut Italia menggunakan jenis Enigma D yang komersil seperti negara Spanyol pada saat Perang Sipil. Beberapa mata-mata berhasil memecahkan kode mesin Enigma versi sipil dan militer. Contohnya pemecah kode dari Inggris memecahkan Enigma yang digunakan oleh Spanyol yang dioperasikan tanpa papan panel. Jepang menggunakan Enigma versi T, dikenal juga dengan Enigma Tirpiz, yang merupakan adaptasi dari versi Enigma K. Jepang juga mengembangkan versi Enigma mereka sendiri, dengan peletakan mesin rotor secara horizontal. Tetapi pesan

cipher dari kedua model tersebut, model T dan K masih dapat dipecahkan.

II.1.b. Mesin Enigma Versi Militer

Pada tahun 1926, mesin enigma dibeli oleh angkatan laut Jerman dan diadaptasikan untuk keperluan militer. Mereka menyebut mesin tersebut Funkschlüssel C. Pada tahun 1928, Jerman Abwehr (jasa rahasia), Wehrmacht dan Luftwaffe membeli versi mereka sendiri, Enigma G, dikenal juga dengan Enigma Zahlwerk. Model ini memiliki kotak gigi untuk memajukan rotor-rotor, sebuah pemantul (reflektor) berputar, tetapi mesin ini tidak dilengkapi oleh papan steker. Wehrmacht memperbarui mesin ini dengan menambahkan papan steker ke dalamnya dan mekanisme pemajuan rotor yang berbeda. Mesin yang telah diperbarui ini diberi nama Enigma I, dan lebih dikenal sebagai Enigma Wehrmacht dan diperkenal dalam skala yang luas untuk kewenangan militer dan publik. Mesin Enigma Wehrmacht pada awalnya terdiri dari tiga rotor dan baru pada tahun 1939 mereka melengkapi mesin tersebut dengan lima rotor.

Pada tahun 1934, angkatan laut Jerman mengadaptasi model Wehrmacht, dengan papan steker yang aman, dan memperbanyak komponen rotor menjadi delapan buah. Mesin ini dinamakan Funkschlüssel M atau M3. Pada tahun 1941, walaupun Abwehr menyatakan bahwa mesin M3 tidak dapat dipecahkan, Admiral Karl Dönitz tetap meminta peningkatan dari Enigma Kriegsmarine. Pada permulaan tahun 1942, model empat rotor yang terkenal, M4, diperkenalkan di Kriegsmarine. Dan mesin tersebut diperkirakan diproduksi sebanyak 100.000.

Gambar 1 Mesin Enigma

Gambar 2 Mesin Enigma Yang Dibuka

II.1.c. Sejarah Pemecahan Kode di Polandia

Pada tahun 1932, Biro Polandia, Szyfrow, memulai mencoba menganalisi dan memecahkan pesan dari Enigma. Walaupun pemimpin biro tersebut mendapatkan salinan buku kode yang dijual oleh mata-mata Jerman, Hans-Thilo Schmidt, dia tidak memberikan buku tersebut kepada pada pemecah kodenya. Dia beranggapan bahwa menyimpan informasi ini akan merangsang usaha mereka dalam memecahkan pesan Enigma tersebut. Marian Rejewski, Henryk Zygalski dan Jerzy Rozicki berhasil memecahkan kode Enigma dan mengembangkan

mesin elektronis yang dinamakan Bombe untuk mempercepat proses pemecahan kode. Dua cela keamanan pada prosedur Enigma Jerman adalah pengaturan awal yang sama dan penyandian dua kali kunci pesan, ini untuk menghilangkan kesalahan. Tetapi, ketentuan tersebut merupakan cela yang dapat digunakan untuk melakukan kriptanalisis. Pada tahun 1939, biro tersebut tidak dapat lagi memecahkan kode mesin Enigma tersebut dikarenakan peningkatan kesempurnaan pada perancangan mesin, prosedur-prosedur baru dan kekurangan dana untuk membayar para pemecah kode. Ketika Jerman menginvasi Polandia, hasil riset dari Polandia tersebut dan beberapa replika mesin Enigma berhasil dikirimkan ke mata-mata Prancis dan juga Inggris.

II.1.d. Bletchley Park

Pemerintah dan sekolah penyandian di Bletchley Park pada awalnya memecahkan kode Enigma dengan hanya menggunakan tangan (manual). Pada bulan Agustus 1940, mereka mulai menggunakan mesin Bombe mereka sendiri, yang dirancang oleh Alan Turing dan Gordon Welchman. Mesin tersebut merupakan alat mekanik elektronis tetapi mesin tersebut dapat bekerja pada semua prinsip enigma yang ada. Semua informasi didapatkan dari kriptanalisis, yang memiliki nama kode "ULTRA" dan memainkan peran yang sangat penting pada saat perang, terutama pada saat Perang Atlantik. Semua informasi yang didapatkan dari ULTRA digunakan dengan sangat hati-hati, antara lain untuk menghindari kecurigaan oleh tentara Jerman.

Petugas penghubung ULTRA, ditempatkan di markas besar dan tempat strategis lainnya. Tetapi, ULTRA tidak pernah menggunakan mereka sampai hasil mata-mata mereka disahkan oleh sumber lainnya untuk menghindari kecurigaan para tentara Jerman bahwa komunikasi mereka telah disadap.

II.1.e. Kriegsmarine

Para Kriegsmarine Jerma sangat berhasil dalam menerapkan taktik Rudel mereka atau "Wolfpack Tactics" dengan kapal U. Mereka berburu secara individual untuk mendapatkan konvoi kapal musuh. Jika sebuah konvoi ditemukan, kapal U tersebut membuntuti konvoi tersebut dan memanggil kapal U lainnya. Ketika semua kapal U berada pada tempat yang telah ditentukan, mereka menghancurkan konvoi tersebut dengan serangan jarak dekat. Teknik ini menghancurkan persediaan sekutu yang berdampak pada hasil peperangan.

Kapal U menggunakan Enigma untuk mengiring pesan kepada kapal lainnya ketika penyerangan. Setelah waktu yang lama, Bletchley Park memecahkan kode tersebut. Penurunan pada efektifitas kapal U-nya, Admiral Donitz curiga dengan keamanan pada Enigma. Dia memerintahkan untuk mengembangkan keamanan Enigma. Pada awal tahun 1942, mesin empat rotor yang dikenal dengan “SHARK” diperkenalkan di Kriegmarine dan mempersulit Bletchley Park dalam memecahkan kodenya. Pada musim semi tahun 1942, tentara sekutu tidak dapat memecahkan kode tersebut dan kapal U kembali dapat menenggelamkan kapal-kapal tanpa adanya gangguan.

II.1.f. Pembalikan Keadaan

Para pemecah kode di Blechtley Park menyadari bahwa mesin empat rotor tersebut telah masuk ke dalam medan peperangan kode-kode. Setelah 10 bulan kekalahan yang sangat menyakitkan, Bletchley Park berhasil memecahkan kode "Shark". Satu alasan keberhasilan mereka adalah mengambil alih buku kode oleh angkatan laut Inggris dari kapal cuaca Jerman, dan

juga kapal U yang dinahkodai oleh Kapitanleutenant Heidtmann oleh HMS Petard. Tujuan dari misi kapal cuaca ini adalah untuk memutuskan lalu lintas pesan Shark, bukan untuk mencuri mesin Enigma. Bahkan, mesin Bombe yang baru telah berhasil dikembangkan untuk memecahkan kode yang dibuat oleh mesin Enigma empat rotor. Dan pada akhir tahun 1943, 50 mesin Bombe lainnya dioperasikan pada angkatan laut Amerika.

Setelah mesin Bombe dioperasikan, hasil perang mulai berubah. Seluruh sistem komunikasi Jerman telah disadap oleh banyak stasiun pendengan yang diberi nama stasiun Y, dan kode mereka telah berhasil dipecahkan oleh Bletchley Park, dimana lebih dari 7000 pekerja dipekerjakan untuk keberhasilan misi tersebut. Dengan diketahuinya posisi kapal U, sekarang kapal tentara sekutu dapat menghindari musuh dan perburuan kapal U dimulai. Senjata elit dari Kriegsmarine dapat dihancurkan, yang menyebabkan kekalahan yang sangat besar pada kru kapal U. Diperkirakan sebanyak 700 kapal U dan 30.000 kru meninggal di laut. Pemerintah Jerman tidak menyangka bahwan kekalahan ini disebabkan oleh berhasil dipecahkannya kode Enigma, dan tetap menggunakannya selama waktu perang. Karena itulah, dikatakan bahwa keberhasilan memecahkan kode Enigma mempersingkat waktu perang dunia II.

II.2. Komponen Mesin Enigma

Mesin Enigma terdiri dari 5 bagian utama, yaitu rotor, penggerak rotor, reflector, papan steker, dan juga kotak enigma.

II.2.a. Rotor

Rotor merupakan bagian terpenting dari Enigma. Dengan kisaran diameter 10 cm, sebuah rotor merupakan sebuah piringan yang terbuat dari karet yang keras atau bakelit dengan deretan kuningan yang berisi pin-pin yang menonjol yang berbentuk bundar. Di sisi satunya bersesuaian dengan deretan angka yang juga berbentuk bundar.

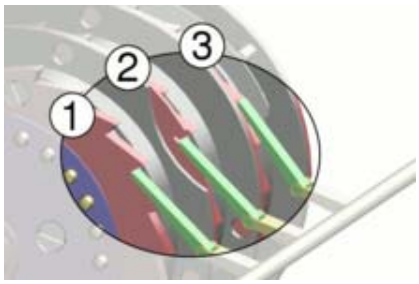
Gambar 3 Rotor Enigma

Gambar 4 Detail Rotor Enigma

Sebuah rotor menunjukkan sebuah enkripsi yang sangat sederhana. sebuah huruf dienkripsikan menjadi satu huruf lainnya. Tetapi, hasil enkripsinya akan menjadi lebih rumit apabila digunakan lebih dari satu rotor.

II.2.b. Penggerak Rotor

Untuk menghindari cipher substitusi sederhana, beberapa rotor harus diputar berdasarkan penekanan sebuah kunci. Ini untuk memastikan bahwa kriptogram yang dibuat itu merupakan sebuah transformasi perputaran rotor yang menghasilkan substitusi poliponik cipher. Alat yang paling banyak digunakan untuk mengimplementasikan pergerakan rotor tersebut adalah mekanisme roda bergigi dan sebuah penggerak roda tersebut. Penggerak roda tersebut memutar rotor sebanyak satu karakater ketika sebuah huruf diketikkan pada papan kunci.



Gambar 5 Penggerak Rotor

II.2.c. Reflektor

Reflektor pada mesin Enigma baru digunakan pada versi diatas C. Komponen ini, selain digunakan untuk memastikan bahwa sebuah huruf tidak dikodekan terhadap dirinya sendiri, juga berguna untuk menjadikan mesin ini bersifat reversible, maksudnya apabila sebuah huruf dienkripsikan kembali, maka hasil enkripsi huruf tersebut adalah huruf semula. Berbeda dengan rotor, reflector hanya terdiri dari 13 pasangan huruf, yang susunannya acak.

Gambar 6 Reflektor Tipe B

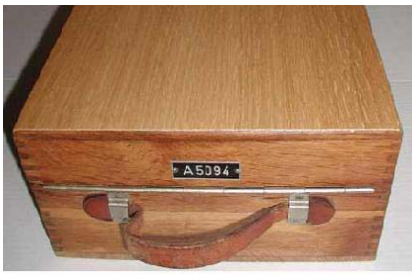
II.2.d. Papan Steker

Papan steker digunakan untuk menukar 2 buah huruf. Papan ini berguna untuk meningkatkan keamanan dari pesan rahasia mesin enigma. Apabila papan ini digunakan pada saat penyandian pesan, sebelum masuk ke proses penyandian, huruf yang telah ditentukan pertukarannya akan diubah di papan ini. Setelah ini, baru huruf tersebut masuk ke dalam proses penyandian.

Gambar 7 Papan Steker

II.2.e. Kotak Enigma

Kotak enigma digunakan untuk menyimpan semua perlengkapan dari mesin ini. Biasanya kotak ini dapat menampung sampai 10 buah rotor, papan steker, dan juga papan ketik.



Gambar 8 Kotak Enigma

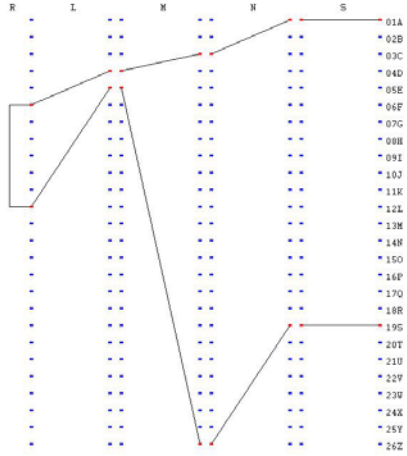
II.3. Cara Kerja Mesin Enigma

Mesin Enigma bekerja berdasarkan perputaran rotor-rotor yang ada pada mesin tersebut. Ketika sebuah huruf diketikkan ke papan panel, urutan kerja dari mesin enigma adalah sebagai berikut :

3. Majukan rotor kanan sebanyak satu huruf. Huruf yang diketikkan masuk ke rotor paling kanan. Pada rotor ini dicari padanan pada rotor kedua. Setelah itu, masuk ke rotor ke dua.
4. Pada rotor kedua, huruf hasil padanan dari rotor pertama dicari padanannya untuk rotor ke tiga. Setelah itu, masuk rotor ke tiga.
5. Pada rotor ketiga, dicari padanan untuk reflector.

6. Setelah masuk ke reflector, dicari pasangan huruf tersebut pada reflector, dan hasil pada reflector dikembalikan kepada rotor ketiga, kedua, ke satu, dan akhirnya menghasilkan huruf enkripsi.

Cara kerja mesin enigma diilustrasikan oleh gambar berikut ini :



Gambar 9 Ilustrasi Cara Kerja Rotor

Apabila mesin Enigma tersebut dilengkapi dengan penggantian huruf pada papan steker, maka sebelum diproses, huruf tersebut diubah dahulu dengan huruf penggantinya. Misalkan huruf A -> Q, B -> K, dan U -> V, maka ketika huruf A dimasukkan ke dalam mesin Enigma, maka huruf akan diterjemahkan dahulu menjadi huruf Q, selanjutnya huruf Q inilah yang akan diproses ke dalam mesin Enigma.

II.4. Deskripsi Matematis Mesin Enigma

Misalkan :

P = transformasi papan steker
L,M,R = ketiga Rotor
U = Reflektor

Maka :

E = PRMLUL-1M-1R-1P-1

Dengan Fakta sebagai berikut:

E[x] != x, huruf x tidak pernah dienkripsikan dengan dirinya sendiri
E[E[x]] = x, pengenkripsian hasil enkripsi pertama, menghasilkan plainteks.

Dengan fakta itulah, proses dekripsi pada Enigma Cipher sama dengan proses enkripsinya.

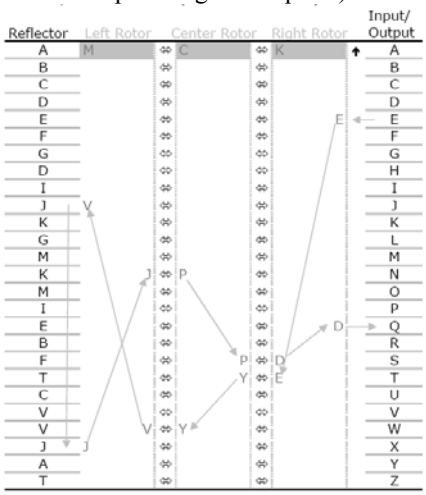
II.5. Kekuatan Enigma Cipher

Dengan hanya menggunakan tiga buah rotor, perputaran yang dapat dihasilkan oleh mesin enigma adalah 26*25*26 = 16.900. Angka 25 pada rotor tengah dikarenakan adanya "double step" dikarenakan adanya saat dimana waktunya rotor kedua melakukan putaran.

III. Enkripsi dan Dekripsi Pada Enigma Cipher Dengan Teknik Manual

Mesin enigma mengenkripsi pesan plainteks dengan cara melakukan substitusi huruf sesuai dengan perputaran rotor yang ada pada mesin tersebut. Cara kerja enkripsi mesin enigma diilustrasikan oleh teknik manual berikut ini.

1. Sediakan kertas dengan isi sebagai berikut (citra lebih jelas dapat dilihat pada bagian lampiran):



Gambar 10 Ilustrasi Mesin Enigma

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

Gambar 11 Ilustrasi Rotor

2. Pilih rotor pada gambar 11 untuk ditempatkan sebagai rotor kiri, tengah dan kanan.
3. Tentukan kunci dengan memposisikan huruf-huruf pada rotor-rotor tersebut terhadap baris pertama pada gambar 10.
4. Jika tanda panah atas (↑) berada pada baris pertama, naikkan rotor tersebut satu huruf dan naikkan juga rotor di sebelah kirinya sebanyak satu huruf.
5. Pilih huruf yang akan di enkripsi/dekripsi.
6. Baca huruf yang bersebelahan, misalkan huruf pada bagian kanan rotor tersebut adalah X, maka pilih huruf X pada bagian kiri rotor tersebut.
7. Ulangi untuk rotor tengah.
8. Ulangi untuk rotor kiri.
9. Baca huruf yang bersebelahan, misalkan R, pilih huruf R lain yang ada pada reflector.
10. Ulangi untuk rotor tengah.
11. Ulangi untuk rotor kanan.
12. Tuliskan huruf yang bersebelahan pada kolom keluaran.

Ulangi untuk tiap huruf pada pesan.

IV. Laporan Teknis Studi Dan Kriptanalisis Enigma Cipher

Setelah melakukan studi mengenai mesin enigma, baik dari segi cara kerja (enkripsi dan dekripsi) ataupun dari segi kriptanalisis, dilakukan pengujian terhadap hasil studi tersebut. Pengujian tersebut menggunakan simulator mesin enigma yang diprogram oleh Dirk Rijmenants, simulator yang diprogram oleh Geoff Sullivan, teknik manual enkripsi dan dekripsi, serta kriptanalisis yang sumber pesan rahasianya adalah cipher dari pengujian ini sendiri.

Simulator yang diprogram oleh Dirk Rijmenants digunakan untuk menguji simulator yang dibuat oleh Geoff Sullivan, apakah simulator tersebut bekerja sesuai dengan mesin enigma yang asli. Selain itu, simulator yang dibuat oleh Geoff Sullivan digunakan untuk menguji kebenaran hasil teknik manual yang telah dijelaskan pada bab sebelumya. Kemudian, cipher hasil enkripsi tersebut dijadikan sebagai bahan yang akan dianalisis pada teknik kriptanalisis.

Adapun langkah-langkah pengujian dari hasil studi ini adalah sebagai berikut :

1. Melakukan pengujian simulator terhadap simulator Dirk Rijmenants dan Geoff Sullivan.
2. Melakukan pengujian terhadap teknik manual enkripsi dan dekripsi.
3. Melakukan kriptanalisis terhadap hasil enkripsi pada point 2.

IV.1. Hasil Pengujian Kedua Simulator

Sebelum melakukan pengujian, pertama-tama kedua simulator tersebut

diatur supaya memiliki settingan mesin enigma yang sama. Selain itu, sedapat mungkin pengaturan ini juga merupakan pengaturan standar untuk melakukan teknik manual enkripsi/dekripsi, sehingga pengaturan awal yang dilakukan adalah sebagai berikut :

1. Rotor kiri menggunakan rotor I, rotor tengah menggunakan rotor II, rotor kanan menggunakan rotor III.
2. Reflektor yang digunakan adalah reflector jenis B.
3. Cincin pada semua rotor menunjukkan nilai A.
4. Tidak menggunakan papan steker.
5. Kunci yang digunakan adalah MKI.

Setelah pengaturan awal selesai, dimasukkan teks "STUDI DAN KRIPTANALISIS PADA ENIGMA CIPHER" pada kedua simulator mesin tersebut.

Simulator pertama menghasilkan cipher sebagai berikut :
EMKQK BFFSF FSUJG KAPGD LEBAX NDAPP XUPWL BB

Simulator kedua menghasilkan cipher sebagai berikut :
EMKQK BFFSF FSUJG KAPGD LEBAX NDAPP XUPWL BB

Setelah melakukan enkripsi, dilakukan proses dekripsi untuk memastikan apakah hasil enkripsi tersebut dapat dikembalikan menjadi teks asal. Proses dekripsi dilakukan dengan melakukan pengaturan kembali simulator menjadi kondisi semula dan memasukkan teks hasil enkripsi.

Simulator pertama menghasilkan plainteks sebagai berikut :
STUDIDANKRIPTANALISISPADAE NIGMACIPHER

Simulator kedua menghasilkan plainteks sebagai berikut :
STUDIDANKRIPTANALISISPADAE NIGMACIPHER

Hasil dari kedua plainteks tersebut apabila dipisahkan kata per kata akan menghasilkan teks "STUDI DAN KRIPTANALISIS PADA ENIGMA CIPHER"

Dari kedua hasil enkripsi/dekripsi diatas, dapat disimpulkan bahwa algoritma kedua program diatas sesuai dengan aturan yang berlaku pada mesin enigma.

IV.2. Hasil Pengujian Terhadap Teknik Manual Enkripsi Dan Dekripsi

Hasil enkripsi dengan kunci MKI untuk teks "STUDI DAN KRIPTANALISIS PADA ENIGMA CIPHER" pada teknik manual ini menghasilkan cipher "EMKQK BFFSF FSUJG KAPGD LEBAX NDAPP XUPWL BB".

Dan pada proses dekripsinya, cipher tersebut dapat dikembalikan ke teks semula, yaitu "STUDI DAN KRIPTANALISIS PADA ENIGMA CIPHER".

Sedangkan langkah-langkah enkripsi dan dekripsinya dapat dilihat pada bagian lampiran.

Dari kedua hasil diatas, dapat disimpulkan bahwa teknik manual ini sesuai dengan aturan yang berlaku pada mesin enigma.

V. Kesimpulan

Berdasarkan pembahasan di atas dapat disimpulkan bahwa :

1. Keamanan mesin Enigma tergantung pada rotor, dan papan steker.
2. Enkripsi dan dekripsi pada mesin Enigma dapat dilakukan secara manual, tetapi dengan kerumitan yang cukup tinggi.

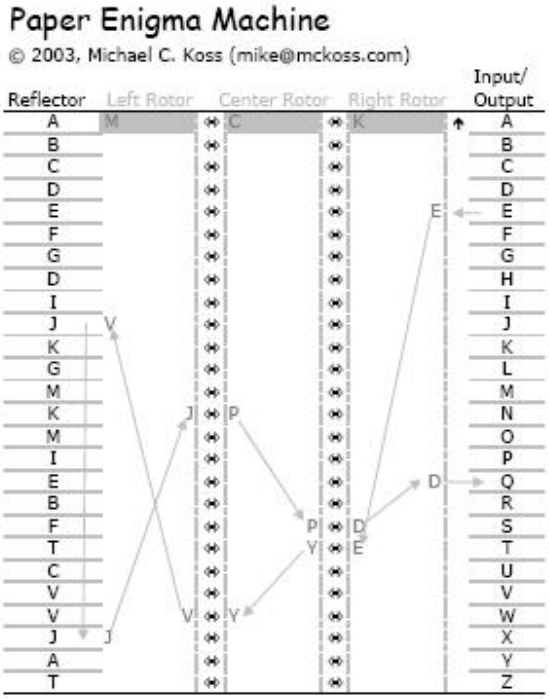
3. Mesin enigma juga dapat di-kriptanalisis dengan menggunakan teknik statistik frekuensi.

Daftar Pustaka

1. Munir, Rinaldi. (2004). Bahan Kuliah IF5054 Kriptografi. Departemen Teknik Informatika. Institut Teknologi Bandung.
2. Sullivan, Geoff and Frode Weierud. (2005). Cryptologia. http://www.tandf.co.uk/journals/pdf/papers/ucry_06.pdf
3. James J. Gillogly. (1995). Cryptologia. http://members.fortunecity.com/jpeschel/gillog1.htm
4. Bantuan pada Enigma Simulator Version 6.0.
5. http://en.wikipedia.org/wiki/Cryptanalysis_of_the_Enigma
6. http://en.wikipedia.org/wiki/Enigma_machine

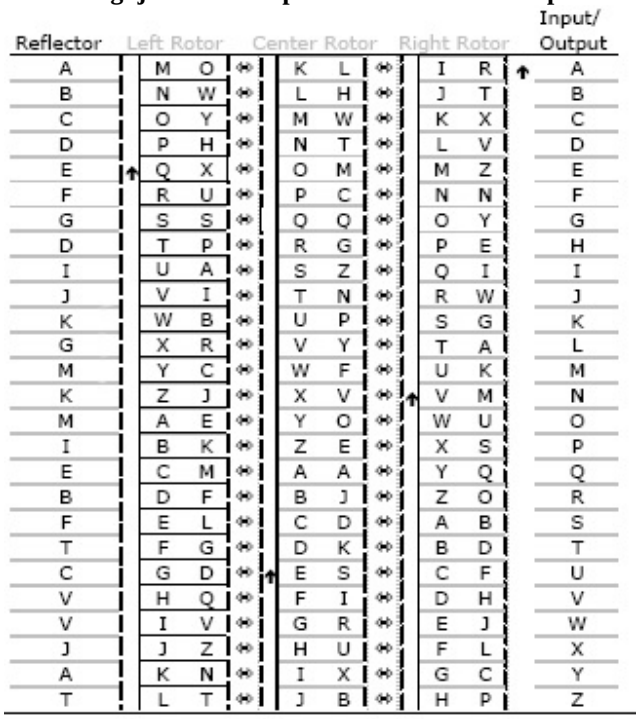
Lampiran

A. Detail Gambar 10 dan Gambar 11

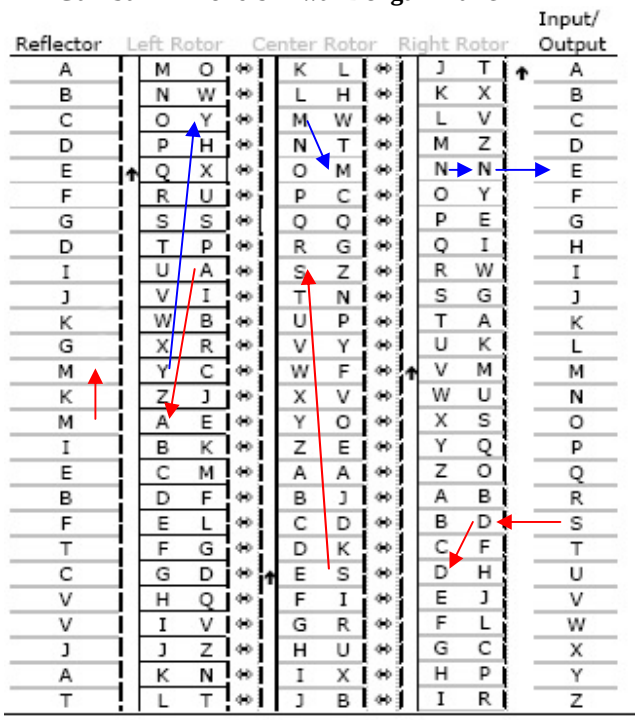


Rev: 2003-03-11-1047

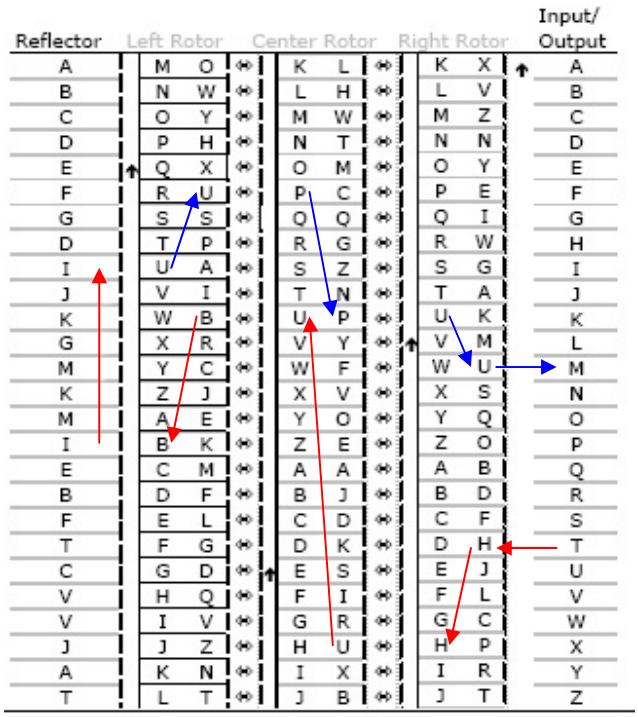
B. Hasil Pengujian Terhadap Teknik Manual Enkripsi Dan Dekripsi



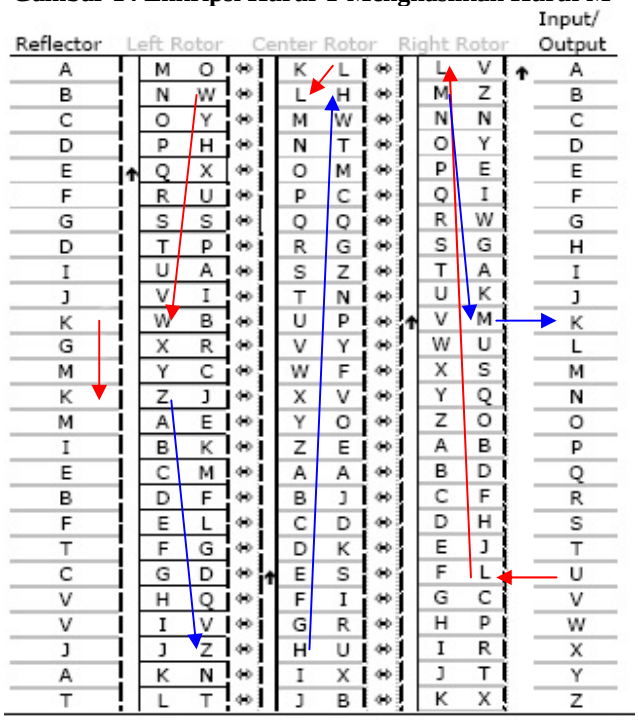
Gambar 12 Kondisi Awal Dengan Kunci MKI



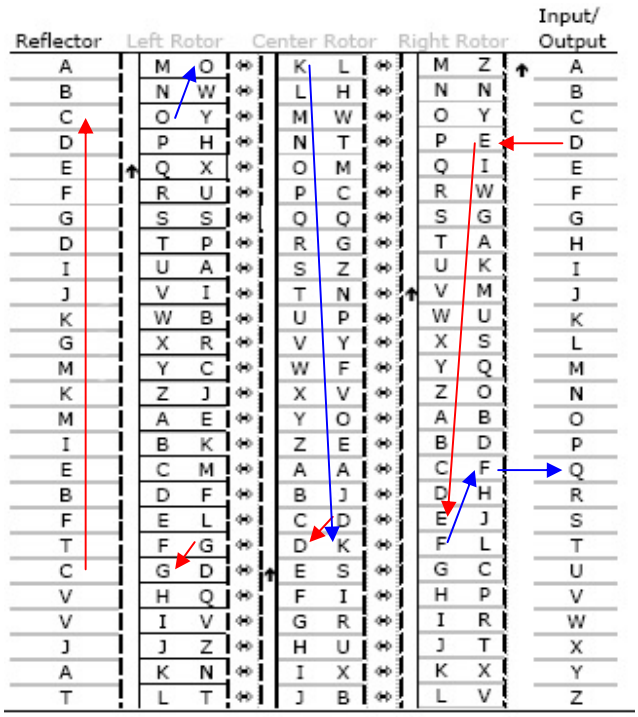
Gambar 13 Enkripsi Huruf S Menghasilkan Huruf E



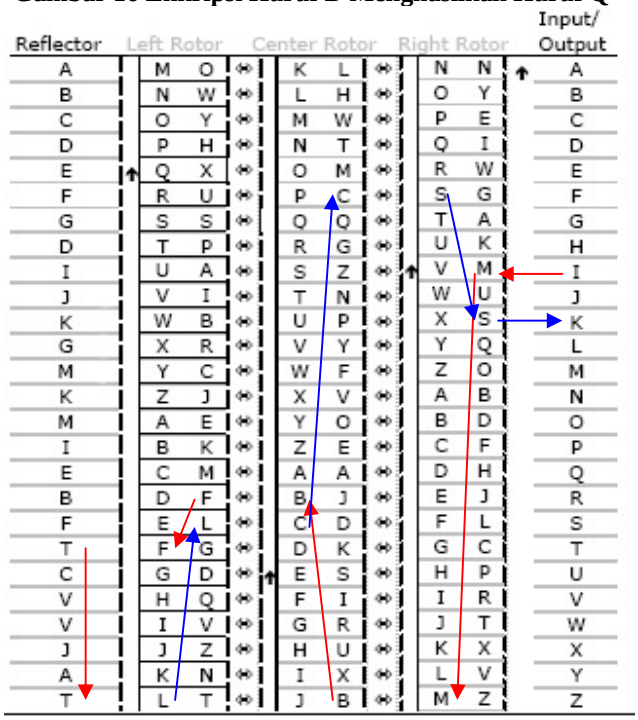
Gambar 14 Enkripsi Huruf T Menghasilkan Huruf M



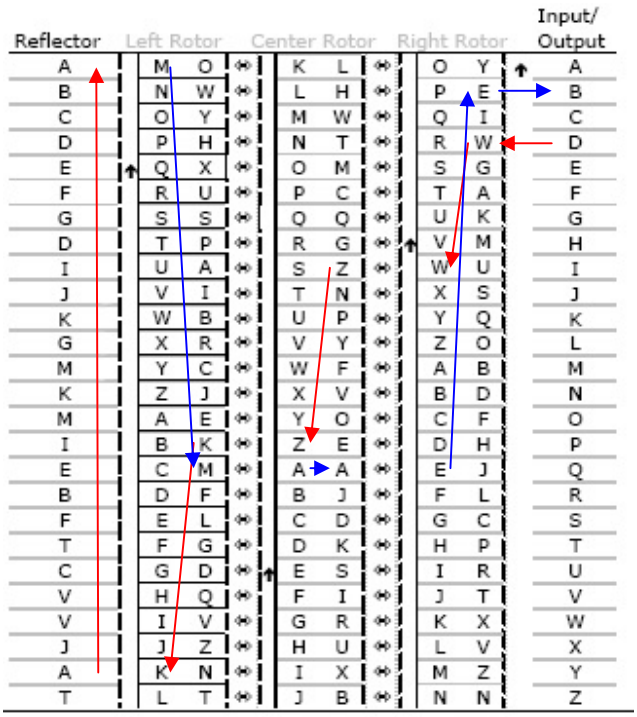
Gambar 15 Enkripsi Huruf U Menghasilkan Huruf K



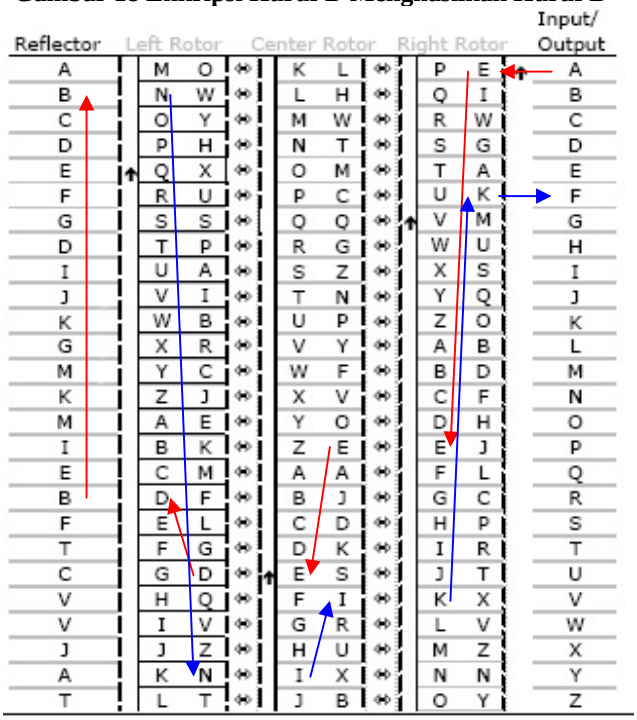
Gambar 16 Enkripsi Huruf D Menghasilkan Huruf Q



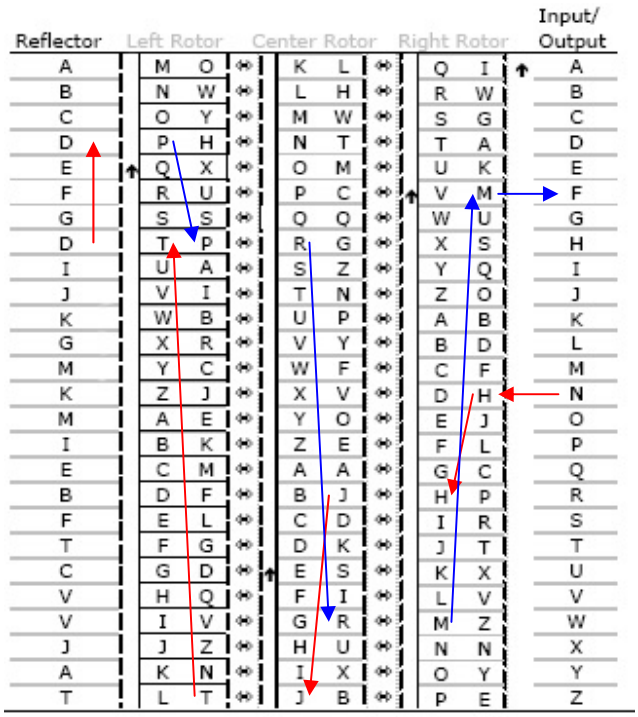
Gambar 17 Enkripsi Huruf I Menghasilkan Huruf K



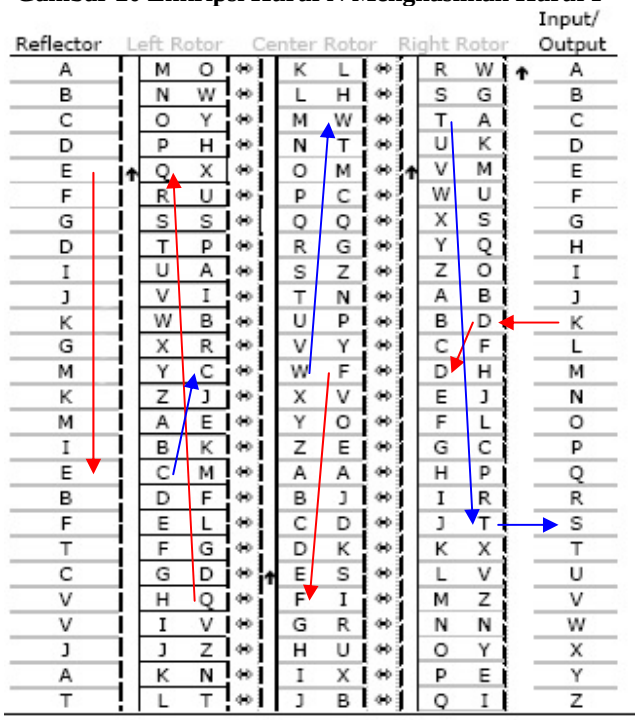
Gambar 18 Enkripsi Huruf D Menghasilkan Huruf B



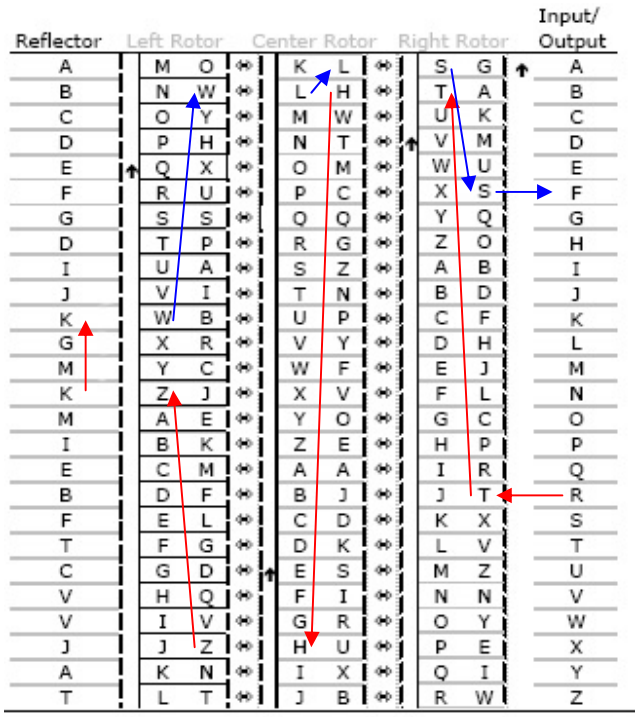
Gambar 19 Enkripsi Huruf A Menghasilkan Huruf F



Gambar 20 Enkripsi Huruf N Menghasilkan Huruf F



Gambar 21 Enkripsi Huruf K Menghasilkan Huruf S



Gambar 22 Enkripsi Huruf R Menghasilkan Huruf F

Ulangi langkah tersebut sampai dengan huruf terakhir. Maka akan didapatkan hasil cipherteksnya "EMKQK BFFSF FSUJG KAPGD LEBAX NDAPP XUPWL BB".

Sedangkan untuk mendekripsi cipherteks tersebut, atur ulang kunci menjadi MKI, dan lakukan proses enkripsi terhadap cipherteks tersebut.