STUDI PERBANDINGAN MESIN CIPHER ENIGMA DAN HAGELIN

Ferdian Thung (13507127)

Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika, Institut Teknologi Bandung
Jalan Ganesha No. 10, Bandung 40132
e-mail: if17127@students.if.itb.ac.id

ABSTRAK

Pengiriman informasi memegang peranan penting dalam Perang Dunia II. Pada masa itu, digunakan mesin cipher untuk pengiriman pesan-pesan vital seperti pesan militer kepada anggota pasukan di daerah lain. Informasi ini harus dapat disampaikan dengan aman sehingga pihak musuh tidak dapat mengetahui isi pesan walaupun pesan tersebut berhasil disadap. Mesin cipher yang umumnya dipakai pada masa itu yakni mesin enigma buatan Jerman dan mesin hagelin yang dibuat oleh perusahaan milik Boris Hagelin di negara netral Swedia dan dijual kepada siapa pun yang menginginkannya sehingga mesin ini memiliki banyak variasi, seperti Hagelin, M209, C36, C38, C41, dan lain-lain. Walau memiliki banyak variasi, mesin hagelin pada dasarnya memiliki prinsip kerja yang sama. Pada makalah ini akan dibahas mengenai mesin enigma dan hagelin terutama metode cipher yang digunakan masing-masing mesin. Kemudian akan dilakukan analisis mengenai keunggulan metode cipher masing-masing mesin.

Kata kunci: *mesin cipher enigma, mesin cipher hagelin, vigenere cipher, beaufort cipher*

1. PENDAHULUAN

1.1 Asal Usul Mesin Cipher Enigma

Mesin Enigma adalah salah satu keluarga dari mesin rotor elektro-mekanis yang digunakan untuk enkripsi dan dekripsi pesan rahasia. Enigma pertama kali diciptakan oleh insinyur Jerman Arthur Scherbius pada akhir Perang Dunia I. Model dan varian dari versi original ini digunakan secara komersial dari awal 1920-an, dan diadopsi oleh militer dan jasa pemerintah beberapa negara terutama oleh Nazi Jerman sebelum dan selama Perang Dunia II. Berbagai model Enigma telah banyak diproduksi, tetapi model militer Jerman, Enigma Wehrmacht, adalah versi yang paling sering dibahas.

Mesin ini menjadi terkenal karena, selama Perang Dunia II, pemecah kode dari Inggris dan Amerika, melanjutkan pekerjaan yang dimulai Polandia, berhasil mendekripsi sejumlah besar pesan yang telah dienkripsi menggunakan Enigma. Intelijen yang diperoleh dari sumber ini, yang diberi kode nama ULTRA oleh Inggris, merupakan bantuan substansial untuk usaha perang Sekutu. Pengaruh sebenarnya ULTRA terhadap jalannya perang masih diperdebatkan; sebuah penilaian berulang-ulang mengungkapkan bahwa dekripsi dari cipher Jerman mempercepat akhir perang Eropa dua tahun.

Walaupun mesin cipher Enigma memiliki kelemahan kriptografik, pada prakteknya hal ini merupakan kombinasi dari berbagai faktor (kesalahan prosedural, kesalahan operator, perangkat keras dan tabel kunci yang berhasil didapatkan, dan lain-lain) sehingga kelemahan ini mengizinkan kriptografer Sekutu untuk mengkriptanalisis banyak pesan.

1.2 Asal Usul Mesin Cipher Hagelin

Pada tahun 1925, Staf Umum Swedia dihubungi oleh A.B. Cryptograph untuk merancang sebuah mesin yang diharapkan lebih unggul daripada mesin Enigma milik Jerman. Hagelin mengembangkan sebuah prototipe untuk evaluasi yang disebut dengan B-21. B-21 telah disetujui untuk Staf Umum Swedia dan Hagelin juga menjual mesin ini ke beberapa negara lain. Prinsipnya didasarkan pada rotor Arvid Damm yang telah disederhanakan, disertai dengan desain grid 5x5. Mesin ini memiliki sebuah papan ketik, dua buah rotor yang putarannya dapat dikendalikan oleh dua pasang roda-pin dan sebuah layar display dengan 25 lampu yang akan menyajikan keluaran dari proses enkripsi dan dekripsi. Mesin ini beroperasi pada tegangan 110 atau 220 volt dan lampu panel ditenagai oleh baterai. Pada mesin ini, menekan sebuah tombol akan menutup dua kontak, masing-masing kontak merupakan salah satu dari dua kelompok lima kontak. Sinyal kemudian diteruskan dari dua rotor menuju 25 lampu. Adapun *intechangeable leads*, secara seri dengan rotor, bisa dihubungkan sesuai keinginan.

Mesin ini adalah mesin pertama yang menerapkan roda-pin, sebuah fitur yang digunakan dalam banyak penerusnya. Sebuah roda-pin adalah sebuah disk dengan jumlah aksial lubang di mana pin tersebut berada. Pin ini dapat dipindahkan ke sisi kiri maupun kanan disk. Pada satu sisi, pin ini tidak aktif sedangkan di sisi lainnya pin ini aktif. Pada setiap langkah, roda-roda pin bergerak satu posisi. Beberapa roda-pin dengan jumlah pin yang berbeda dan tanpa faktor yang umum akan digunakan untuk memperoleh kunci dengan periode panjang.

Pada tahun 1932, Angkatan Darat Perancis tertarik dengan B-21 tapi meminta untuk dua modifikasi penting. Mesin harus portabel dan harus mampu mencetak teks. Hagelin mengembangkan B-211 yang bisa dioperasikan baik dengan tenaga listrik atau dengan tangan menggunakan tenaga mekanik. Dia menggantikan lampu panel dengan roda untuk mekanisme percetakan dan sirkuit ciphering yang ditenagai oleh baterai. Sekitar 500 mesin B-211 kemudian dibangun. Pada tahun 1940, Hagelin membangun sebuah workshop di Swedia dengan menggunakan keuntungan yang diperoleh atas sukses B-211 dan kemudian A.B. Cryptograph diubah namanya menjadi A.B. Ingenieursfirman Cryptoteknik.

2. MESIN CIPHER ENIGMA

2.1 Struktur Mesin Enigma

Enigma yang dikonstruksikan dan ditampilkan Scherbius pada Universal Postal Union Congress di Vienna tahun 1923 didasarkan pada komponen-komponen berikut:

(1) Sebuah papan ketik dengan 26 huruf untuk memasukkan pesan plainteks.
(2) 26 buah lampu yang akan menyala untuk menunjukkan huruf cipher.
(3) Sebuah sumber tegangan (baterai 3.5 volt atau ekivalensinya).
(4) Tiga *removable wired wheels* yang dapat berputar pada sumbu tertentu.
(5) Sebuah reflektor.
(6) Sebuah *entry wheel*.

Papan ketik yang digunakan serupa dengan papan ketik pada mesik bahasa Inggris dengan pengecualian, yakni huruf Y dan Z dipertukarkan serta huruf P berada di bawah baris, tidak di atas. Hanya huruf kapital yang digunakan, tidak ada nomor ataupun *umlauts*, seperti Ü. Pola yang sama juga diaplikasikan pada huruf di lampu. Kemudian, baterai hanya digunakan untuk mengirimkan arus ke roda dan reflektor, serta untuk menyalakan lampu. Ia tidak menyediakan tenaga untuk menggerakkan roda, di mana hal ini dilakukan secara mekanik.

Gambar 1 Mesin Enigma

Di dalam setiap *removable wheel* terdapat 26 kabel yang secara ‘acak’ terhubung dengan 26 titik kontak pada salah satu sisi roda dengan 26 kontak pada sisi lain roda. Titik kontak pada salah satu sisi roda (sisi kiri bila dilihat dari depan mesin) akan di-*flush* dengan muka roda, tetapi kontak pada sisi yang lain (sisi ‘kanan’) menonjol keluar dari muka di atas pegas kecil. Hal ini ditujukan untuk menyediakan kontak yang baik antara sebuah roda dengan roda yang berada di sebelahnya. Serupa dengan hal itu, kontak yang baik dijamin antara *rightmost wheel* dan *entry wheel* serta antara *leftmost wheel* dan reflektor. Sebuah alfabet *tyre* berada pada lingkaran setiap roda dan pada sisi kiri dari setiap *removable wheel* terdapat sebuah cincin metal (*notch ring*) yang diikatkan di mana cincin ini memiliki sebuah *notch* berbentuk V pada sisi berlawanan dari huruf-huruf dalam *tyre*. Pada sisi kanan dari roda ini terdapat cincin bergerigi dengan 26 gerigi (*setting ring*) yang mengizinkan operator cipher untuk memutar roda ke posisi yang diinginkannya.

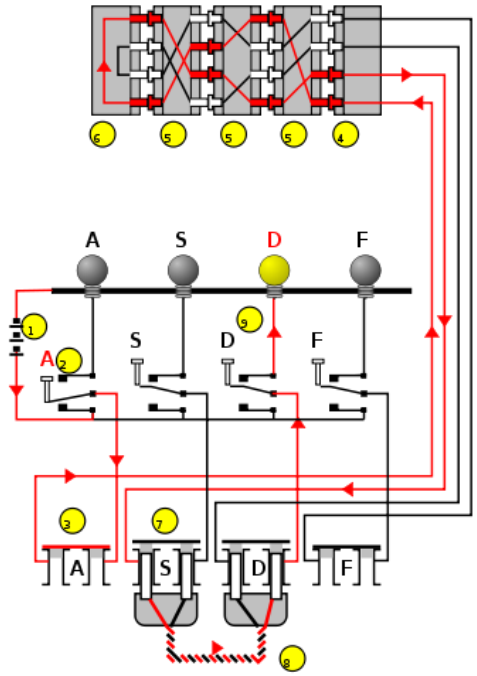
Reflektor berada pada posisi tetap dan memiliki sebanyak 26 kontak pada satu sisi. Di dalam reflector terdapat 13 kabel yang menghubugkan 26 kontak dalam pasangan sehingga arus yang memasuki sebuah titik kontak dari reflektor akan keluar pada titik kontak yang lain. Pengkabelan internal pada reflektor juga dilakukan secara ‘acak’. Tidak seperti *three wired wheels*, reflektor secara permanen tetap dan hanya diganti sekali pada tahun 1937.

Entry wheel menyediakan koneksi antara *rightmost wheel* dan papan ketik serta antara *rightmost wheel* dan lampu. Hal yang mengejutkan, *entry wheel* dihubungkan dengan huruf pada papan ketik berdasarkan urutan alfabet normal, dibandingkan urutan pada papan ketik. Hal ini tidak memberikan keuntungan kriptografik apapun dan melibatkan pengkabelan internal yang berantakan.

2.2 Operasi pada Mesin Enigma

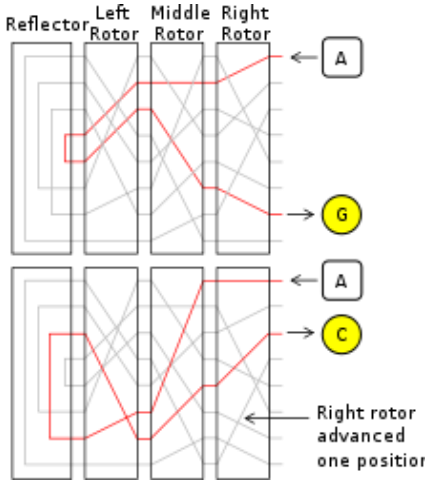
Untuk mengilustrasikan operasi dari mesin Enigma, perhatikan diagram pengkabelan pada gambar (2). Untuk

menyederhanakan contoh, hanya empat komponen dari mesin Enigma utuh yang ditampilkan. Pada kenyataannya, terdapat 26 lampu dan kunci, beberapa plug (bervariasi berdasarkan model) dan pengkabelan rotor dalam setiap rotor (setidaknya ada tiga). Prinsip kerjanya yakni arus mengalir dari baterai(1) melalui *depressed bi-directional letter-switch* (2) menuju *plugboard* (3). *Plugboard* mengizinkan pengkabelan ulang beberapa koneksi huruf antara papan ketik (2) dan *entry wheel* (4). Kemudian, arus mengalir menuju (tidak digunakan pada contoh ini sehingga ditunjukkan tertutup) *plug* (3) melalui *entry wheel* (4) melewati pengkabelan tiga (Wehrmacht Enigma) atau empat four (varian *Kriegsmarine* M4 dan *Abwehr*) rotor yang terinstalasi (5), dan memasuki reflektor (6). Reflektor mengembalikan arus melalui jalur yang berbeda melewati rotor dan *entry wheel*(4), melanjutkan melalui plug 'S' yang terhubung dengan sebuah kabel(8) menuju plug 'D', dan *bi-directional switch* (9) untuk menyalakan lampu yang sesuai.



Gambar 2 Cara Kerja Mesin Enigma

Perubahan yang berulang pada jalur elektrikal melalui sebuah *Enigma scrambler*, mengimplementasikan sebuah enkripsi *polyalphabetic substitution* yang menyediakan tingkat keamanan tinggi Enigma pada zamannya. Diagram pada gambar (3) menunjukkan bagaimana jalur elektrikal berubah dengan setiap *key depression*, yang mengakibatkan rotasi pada setidaknya rotor pada sisi kanan. Arus akan mengalir menuju sekelompok rotor, masuk dan keluar dari reflektor, dan keluar melalui rotor lagi.



Gambar 3 Aksi *Scrambling* pada Enigma untuk Penekanan Tombol A Berurutan

Garis yang berwarna abu-abu merupakan beberapa jalur lain yang mungkin untuk setiap rotor; jalur ini diimplementasikan pada mesin secara langsung dari satu sisi pada setiap rotor ke rotor lainnya. Huruf A dienkripsi secara berbeda pada penekanan tombol yang berurutan, pertama ke *G*, kemudian ke *C*. Hal ini dikarenakan rotor pada sisi kanan telah naik dan mengirimkan sinyal pada rute yang berbeda; rotor lain juga akan mengalami hal yang sama saat penekanan sebuah tombol.

2.3 Algoritma Cipher pada Mesin Enigma

Algoritma cipher yang digunakan pada mesin enigma pada dasarnya merupakan vigenere cipher. Algoritma ini dipublikasikan oleh diplomat (sekaligus seorang kriptologis) Perancis, Blaise de Vigènere pada abad 16 (tahun 1586). Cipher ini termasuk *polyalphabetic substitution cipher*. Vigenere cipher menggunakan rumus berikut untuk proses enkripsi huruf:

$$c = (k+p) \bmod 26 \quad (1)$$

dan dekripsi:

$$p = (c-k) \bmod 26 \quad (2)$$

di mana:

c = cipherteks
p = plainteks
k = kunci

Enkripsi dengan menggunakan vigenere cipher dapat diilustrasikan sebagai berikut.

PLAINTEKS : VIGENERE
KUNCI : KUNCIKUN
CIPHERTEKS : ????????

Ubah ke dalam angka untuk melakukan perhitungan.

PLAINTEKS	V	I	G	E	N	E	R	E
	21	8	6	4	13	4	17	4
KUNCI	K	U	N	C	I	K	U	N
	10	20	13	2	8	10	20	13
CIPHERTEKS	F	C	T	G	V	O	L	R
	5	2	19	6	21	14	11	17

Dengan menggunakan rumus (1) diperoleh cipherteks FCTGVOLR dari plainteks VIGENERE dan kunci KUNCI. Plainteks dapat diperoleh kembali dari cipherteks dengan menggunakan rumus (2).

Tabel 1 Tabel Enkripsi/Dekripsi Vigenere

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

Enkripsi dan dekripsi vigenere cipher akan lebih mudah apabila menggunakan tabel (2). Untuk enkripsi sebuah pesan plainteks, temukan indeks baris yang bernilai sama dengan huruf yang akan dienkripsi dan indeks kolom yang bernilai sama dengan huruf kunci. Huruf cipherteks terletak pada perpotongan baris dan kolom ini. Untuk dekripsi, ambil indeks kolom yang bernilai sama dengan huruf kunci dan telusuri isi tabel pada kolom tersebut hingga menemukan huruf cipherteks. Lihat indeks baris yang memuat huruf cipherteks tersebut, itulah huruf plainteks yang dicari.

3. MESIN CIPHER HAGELIN

3.1 Struktur Mesin Hagelin

Mesin Hagelin membuat *key stream* menggunakan enam roda-pin dan sebuah *lug cage*. Enam roda-pin disusun parallel pada sumbu tertentu dan dapat digerakkan secara independen, di mana hal ini diperlukan ketika mesin sedang dikonfigurasi, atau bersamaan, di mana hal ini terjadi setiap saat sebuah huruf dienkripsi atau didekripsi. Setiap roda memiliki nomor pin pada sekitar lingkarannya dan setiap nomor pin ini dapat digerakkan sehingga ia berada pada sisi kiri atau kanan roda. Nomor pin ini berbeda untuk setiap roda; dilihat dari depan mesin nomor pin pada enam roda dari kiri ke kanan adalah 26, 25, 23, 21, 19 and 17. Setiap saat sebuah huruf dienkripsi setiap roda bergerak sebanyak satu posisi. Karena panjang enam roda tidak memiliki faktor umum, mereka tidak akan kembali ke posisi awal hingga 101405850 (26x25x23x21x19x17) huruf telah dienkripsi. Huruf pada alfabet diukir di sekitar pinggiran setiap roda untuk memungkinkan operator untuk mengatur roda pada posisi awalnya. Pada roda dengan panjang 26, semua alfabet diukir tetapi roda lain tentunya membutuhkan huruf yang lebih sedikit. Jadi, pada roda dengan panjang 17 huruf A sampai Q akan memenuhi.

Gambar 4 Mesin Hagelin

Lug cage terdiri dari 27 batang mendatar yang diatur sebagai sebuah silinder dengan akhir setiap batang berada pada dua disk sirkuler tertentu. *Cage* dapat berotasi pada sebuah sumbu tertentu yang paralel dengan sumbu pada roda-pin. *Cage* diposisikan tepat di belakang roda-pin. Pada setiap batang *cage* terdapat dua '*lugs'*, yakni bagian kecil metal yang dapat bergeser sepanjang batang dan dapat menempati delapan posisi. Enam dari delapan posisi secara langsung berlawanan dengan enam roda; dua yang lainnya, posisi '*netral*', tidak berlawanan dengan roda mana pun tetapi berada di antara roda 1 dan 2 dan antara roda 5 dan 6. Jika tidak ada lebih dari satu *lug* pada bar mana pun yang berlawanan dengan sebuah roda, mesin dikatakan berada pada kondisi *unoverlapped*; jika pada bar mana pun terdapat dua *lug* yang berlawanan dengan roda, mesin dikatakan berada pada kondisi *overlapped*.

Pada sebuah *unoverlapped cage*, sebuah *lug* pada setiap batang mungkin diletakkan berlawanan dengan roda. Merupakan hal yang tidak esensial untuk semua *lugs*

untuk berada pada posisi tersebut, tetapi tidak ada keuntungan kriptografik dalam menggunakan jumlah lebih sedikit. Jadi, sebagai contoh, 27 *lugs* mungkin didistribusikan kepada enam roda sebagai berikut.

Tabel 2 Contoh Distribusi *Lug* pada Roda Mesin Cipher Hagelin

Roda	26	25	23	21	19	17
Jumlah *Lug*	4	1	9	6	5	2

Jumlah *lugs* yang berlawanan dengan sebuah roda kadang-kadang disebut sebagi '*kick*' dari roda tersebut. Jadi, roda dengan panjang 26 di atas memiliki '*kick of 4*'. Urutan merupakan hal yang penting; *cage* di atas (4, 1, 9, 6, 5, 2) tidak akan menghasilkan key stream yang sama seperti (9, 1, 4, 2, 6, 5) walaupun akan terdapat beberapa kesamaan statistik.

Pada sisi kiri mesin terdapat roda kecil yang diukir dengan alfabet; ini digunakan untuk masukan huruf plainteks. Terdapat pula roda print yang mencetak huruf cipher pada sebuah sepotong pita kertas. Pita ini memiliki lem pada sisi berlawannya, tujuannya yakni untuk memungkinkan operator untuk menempelkan cipherteks atau plainteks pada lembaran kertas. Sebuah penggulung dari kertas berlem ini berada pada belakang mesin dan di sana juga terdapat obeng untuk memungkinkan operator mengeset pin dan *lug*.

Pada sisi kanan mesin terdapat pegangan yang ketika dirotasikan akan memutar *cage* sehingga mengenkripsi atau mendekripsi teks; pegangan ini juga menyebabkan setiap roda untuk bergerak maju satu posisi.

3.2 Cara Kerja Mesin Hagelin

Operasi dasar mesin hagelin relatif sederhana. Enam roda yang dapat diatur di atas mesin menampilkan sebuah huruf dalam alfabet. Enam roda ini terdiri dari kunci eksternal untuk mesin yang menyediakan kondisi awal (serupa dengan sebuah *initialization vector*) untuk proses enkripsi atau dekripsi.

Gambar 5 *Key Wheels*

Untuk mengenkripsi sebuah pesan, operator mengatur roda kunci ke sebuah urutan acak huruf. *Enciphering-deciphering knob* pada sisi kiri mesin diset pada "encipher". Sebuah *dial* yang dikenal sebagai *indicator disk*, juga pada sisi kiri, digeser ke huruf pertama pada pesan. Huruf ini dienkripsi dengan menggerakkan *hand crank* atau *power handle* pada sisi kanan mesin. Pada akhir siklus, huruf cipherteks dicetak pada pita kertas, roda kunci kemudian maju sebanyak satu huruf, dan mesin siap untuk memasukkan karakter selanjutnya dari pesan. Untuk mengindikasikan spasi antarkata dalam pesan, huruf "Z" dienkripsi. Mengulang proses ini untuk sisa pesan akan memberikan cipherteks lengkap, yang dapat ditransmisikan dengan metode apa pun. Karena pengaturan awal roda kunci adalah acak, perlu untuk mengirim pengaturan tersebut ke penerima pesan yang disampaikan. Pengiriman ini dapat dienkripsikan dengan menggunakan kunci harian atau ditransmisikan menth-mentah.

Cipherteks yang dicetak dapat secara otomatis dikelompokkan dalam suatu kelompok huruf. Berkaitan dengan ini, bergantung dengan variasi mesin hagelin yang digunakan. M-209, contohnya, mengelompokkan ke dalam kelompok lima huruf. Sebuah penghitung huruf di posisi atas mesin mengindikasikan jumlah huruf terenkripsi dan dapat digunakan sebagai penanda jika kesalahan dibuat pada proses enkripsi atau dekripsi.

Prosedur dekripsi mirip dengan prosedur enkripsi. Operator mengeset *enciphering-deciphering knob* pada posisi "decipher", dan mengatur roda kunci dengan urutan yang digunakan pada proses enkripsi. Huruf pertama cipherteks dimasukkan melalui *indicator disk*, dan *power handle* dioperasikan sehingga memajukan roda kunci dan mencetak huruf hasil dekripsi. Ketika huruf "Z" ditemui, sebuah spasi tampak pada pesan, sehingga merekonstruksi pesan asli dengan spasi. "Z" yang hilang dapat diinterpretasikan dengan mudah oleh operator berdasarkan konteks kalimat.

3.3 Algoritma Cipher pada Mesin Hagelin

Algoritma cipher yang digunakan pada mesin hagelin pada dasarnya merupakan beaufort cipher. Algoritma ini mirip dengan vigenere cipher, hanya saja ia menggunakan rumus yang sedikit berbeda untuk enkripsi huruf:

$$c = (k-p) \bmod 26 \qquad (3)$$

dan dekripsi:

$$p = (k-c) \bmod 26 \qquad (4)$$

di mana:

c = cipherteks
p = plainteks
k = kunci

Enkripsi dengan menggunakan beaufort cipher dapat diilustrasikan sebagai berikut.

PLAINTEKS : BEAUFORT
KUNCI : KUNCIKUN
CIPHERTEKS : ????????

Ubah ke dalam angka untuk melakukan perhitungan.

PLAINTEKS	B	E	A	U	F	O	R	T
	1	4	0	20	5	14	17	19
KUNCI	K	U	N	C	I	K	U	N
	10	20	13	2	8	10	20	13
CIPHERTEKS	J	Q	N	I	D	W	D	U
	9	16	13	8	3	22	3	20

Dengan menggunakan rumus (3) diperoleh cipherteks JQNIDWDU dari plainteks BEAUFORT dan kunci KUNCI. Plainteks dapat diperoleh kembali dari cipherteks dengan menggunakan rumus (4).

Beaufort cipher menggunakan tabel yang sama dengan Vigenere cipher, tetapi dengan algoritma yang berbeda. Untuk mengenkripsi sebuah huruf, cari indeks baris yang bernilai sama dengan huruf yang ingin dienkripsi. Kemudian cek isi tabel pada baris tersebut hingga menemukan huruf kunci. Lalu lihat indeks kolom yang bersangkutan untuk mendapatkan huruf cipherteks. Untuk mendekripsi sebuah huruf, temukan indeks kolom yang bernilai sama dengan huruf yang ingin didekripsi lalu cari isi tabel pada kolom tersebut yang sesuai dengan huruf kunci kemudian lihat indeks baris yang bersangkutan untuk mendapatkan huruf plainteks.

4. PEMBAHASAN DAN ANALISIS

Dalam penjelasan sebelumnya, telah diketahui bahwa mesin cipher enigma menggunakan algoritma vigenere cipher sedangkan mesin cipher hagelin menggunakan algoritma beaufort cipher. Pada dasarnya, kedua algoritma ini memiliki karakteristik yang mirip, yakni melakukan pergeseran huruf sesuai kunci dengan penerapan rumus tertentu. Fakta bahwa kedua algoritma ini dapat menggunakan tabel yang sama untuk melakukan enkripsi/dekripsi pesan secara implisit memberitahukan bahwa kedua algoritma tersebut memiliki suatu kemiripan. Menurut hipotesis saya, untuk setiap pesan yang dienkripsi dengan huruf kunci tertentu dengan vigenere cipher akan memiliki pemetaan bersifat korespondensi satu-satu dengan suatu huruf kunci pada beaufort cipher di mana jika pesan dienkripsi menggunakan huruf kunci tersebut maka akan dihasilkan cipherteks yang sama.

Untuk membuktikannya, saya melakukan pemetaan huruf kunci pada vigenere cipher dengan huruf kunci pada beaufort cipher yang akan memberikan cipherteks yang sama. Pertama, saya mengambil huruf ‘a-z’ yang akan dienkripsi selain huruf ‘a’, kemudian saya melakukan proses enkripsi dengan menggunakan tabel enkripsi/dekripsi dengan algoritma vigenere cipher untuk megenkripsi suatu huruf yang sama dengan kunci ‘a-z’. Kemudian, untuk mencari kunci pada beaufort cipher yang akan memberikan cipherteks yang sama untuk plainteks yang sama, dicari perpotongan indeks baris yang bernilai sama dengan plainteks dan indeks kolom yang bernilai sama dengan cipherteks untuk menemukan kunci tersebut.

Contohnya, saya ambil huruf plainteks ‘b’ dan huruf kunci ‘a’, maka dengan menggunakan tabel enkripsi/dekripsi, hasil enkripsi vigenere cipher memberikan huruf cipherteks ‘b’. Untuk memperoleh huruf kunci pada beaufort cipher yang memberikan cipherteks sama untuk plainteks yang sama, ambil perpotongan indeks baris dan kolom yang masing-masing bernilai sama ‘b’ dan ‘b’, maka kita peroleh huruf kunci ‘c’. Lanjutkan dengan huruf kunci ‘b’, maka enkripsi vigenere cipher memberikan huruf cipherteks ‘c’. Cari kunci pada beaufort cipher dengan cara yang sama dengan sebelumnya, maka diperoleh huruf kunci ‘d’. Hal ini dilakukan untuk semua kemungkinan domain huruf plainteks ‘b-z’ dengan domain kunci ‘a-z’.

Untuk kasus plainteks dengan huruf ‘a’ hasil enkripsi pada vigenere cipher dan beaufort cipher dengan kunci yang sama akan menghasilkan cipherteks yang sama. Hal ini dapat dibuktikan dengan mudah dengan menggunakan rumus (1) dan (3), yakni:

- Vigenere cipher
  c = (p+k) mod 26
  = (0+k) mod 26
  = k
- Beaufort cipher
  c = (k-p) mod 26
  = (k-0) mod 26
  = k

Dengan melakukan semua langkah di atas, diperoleh pemetaan dari kunci pada vigenere cipher dengan kunci pada beaufort cipher di mana jika plainteks yang sama dienkripsi dengan kunci tersebut menggunaka beaufort cipher maka akan diperolah cipherteks yang sama. Untuk pemetaan kunci tersebut, dapat dibuat tabel seperti tabel (3). Dengan menggunakan tabel ini, untuk mencari kunci beaufort yang akan menghasilkan cipherteks yang sama, dicari perpotongan antara indeks baris yang bernilai sama dengan huruf plainteks yang ingin dienkripsi dan indeks kolom yang bernilai sama dengan kunci vigenere yang akan dipetakan ke kunci beaufort. Isi tabel pada perpotongan tersebut merupakan kunci beaufort yang dicari.

Tabel 3 Pemetaan Kunci Vigenere ke Kunci Beaufort

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

Karena untuk setiap kasus dapat diperoleh pemetaan bersifat korespondensi satu-satu antara kunci pada vigenere cipher dan kunci pada beaufort cipher di mana kunci ini menghasilkan cipherteks yang sama untuk kedua algoritma, maka pada dasarnya kedua algoritma cipher ini memiliki kesamaan karakteristik. Setiap sifat yang dimiliki vigenere cipher akan dimiliki pula oleh beaufort cipher, begitupula sebaliknya. Misalnya, karena vigenere cipher dapat dipecahkan dengan metode kasiski, maka beaufort cipher juga dapat dipecahkan dengan metode kasiski.

Tampak bahwa untuk kedua mesin cipher, tidak ada yang lebih unggul dalam hal algoritma enkripsi karena pada dasarnya kedua algoritma memiliki karakteristik yang sama. Keunggulan mesin akan lebih bergantung pada periode pengulangan kunci. Hal ini akan berbeda-beda pada setiap varian dan model mesin enigma dan hagelin yang telah ada.

5. KESIMPULAN

Berdasarkan pembahasan dan analisis yang dilakukan, dapat ditarik kesimpulan berikut:

4.1 Mesin cipher enigma menggunakan algoritma vigenere cipher sedangkan mesin cipher hagelin menggunakan algoritma beaufort cipher.

4.2 Secara teori, antara enigma dan hagelin, tidak ada mesin cipher yang lebih unggul dalam hal metode enkripsi. Keunggulan mesin tergantung periode pengulangan kuncinya, yang berbeda-beda pada setiap varian dan modelnya.

REFERENSI

[1] Munir, Rinaldi. 2005. *Diktat Kuliah IF 5054 Kriptografi.* Departemen Teknik Informatika Institut Teknologi Bandung : Bandung.

[2] Churchouse, Robert. 2004. *Codes and Ciphers, Julius Caesar, the Enigma and the Internet.* Cambridge University Press : Cambridge.

[3] http://users.telenet.be/d.rijmenants/en/enigmatech.htm diakses tanggal 23 Maret 2010 pukul 21.00.

[4] http://practicalcryptography.com/ciphers/beaufort-cipher/ diakses tanggal 23 Maret 2010 pukul 19.00.

[5] http://users.telenet.be/d.rijmenants/en/b21.htm diakses tanggal 23 Maret 2010 pukul 19.00.