STUDI ENKRIPSI DAN KRIPTANALISIS TERHADAP ENIGMA

Eddo Fajar N – 23505029

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
x60880@lycos.com

Abstrak

Makalah ini membahas tentang mesin enkripsi yang dikenal dengan nama Enigma. Pada masa Perang Dunia II, Jerman menggunakan Enigma untuk mengenkripsi dan mendekripsi pesan-pesan militer. Pada makalah ini akan dibahas bagaimana cara mengenkripsi pesan dengan menggunakan Enigma dan bagaimana cara mendekripsikannya.
Pada masa Perang Dunia II, Jerman begitu yakin pihak Sekutu tidak akan dapat memecahkan sandi yang dihasilkan Enigma. Akan tetapi, sejarah membuktikan bahwa pihak Sekutu akhirnya dapat memecahkannya.. Keberhasilan ini akhirnya menjadi salah satu faktor yang mempercepat usainya Perang Dunia II. Pihak-pihak yang berperan besar dalam memecahkan sandi yang dhasilkan Enigma adalah kelompok ahli matematika asal Polandia.
Pada makalah ini juga akan dibahas bagaimana cara melakukan kriptanalisis terhadap pesan-pesan yang dienkripsi dengan Enigma, seperti yang dilakukan oleh pihak Sekutu.

Kata kunci: Cipher subtitusi, Enigma, Perang Dunia II, enkripsi, dekripsi, kriptografi.

Pendahuluan

Sebelum ada komputer, kriptografi dilakukan dengan berbasis karakter dan dengan peralatan yang sederhana. Kriptografi di masa lampau biasanya digunakan untuk kegiatan spionase atau untuk mengirimkan pesan rahasia pada saat perang. Sejarah mencatat beberapa algoritma kriptografi yang pernah digunakan, yang untuk ukuran masa kini sudah usang karena relatif mudah untuk dipecahkan. Beberapa algoritma kriptografi yang pernah digunakan pada masa lalu antara lain:

1. Scytale
2. Cipher Caesar
3. Cipher Vigénere
4. Cipher Enigma

Scytale

Scytale berasal dari bahasa Yunani yang berarti tongkat. *Scytale* terdiri dari sebatang silinder dan sebuah pita panjang dari daun papirus. Scytale digunakan pada oleh tentara sparta di Yunani untuk mengirimkan pesan rahasia.

Mula-mula, pengirim pesan menuliskan pesannya di atas pita papirus yang digulung pada batang silinder. Setelah itu, pita dilepaskan dan dikirim. Misalkan batang silinder cukup lebar untuk menulis 6 huruf di atas pita dan bisa memuat 3 huruf secara melingkar. Jika pengirim ingin mengirimlan pesan

```
TOLONG SAYA DISERANG
```

Maka ia menulis di atas batang silinder

```
T O L O N G
S A Y A D I
S E R A N G
```

Jika pitanya dilepaskan dari batang silinder, maka tulisan yang muncul di atas pita adalah

```
TSSOAELYROAANDNGIG
```

Untuk membaca pesan yang dikirim, penerima pesan melilitkan kembali pita tersebut pada batang silinder yang berdiamter sama. Yang menjadi kunci dalam penyandian scytale adalah diameter batang atau jumlah huruf yang dapat ditulis secara melingkar (dalam hal ini 3 huruf).

Penyandian dengan *scytale* sangat mudah dipecahkan karena kriptanalis hanya perlu menerka jumlah huruf yang dapat ditulis secara melingkar pada batang silinder yang digunakan, apalagi karena jumlah huruf yang dapat ditulis secara melingkar pada suatu batang silinder relatif sangat sedikit (maksimum adalah setengah dari jumlah huruf yang tertulis pada pita). Tabel 2 memuat hasil dekripsi terhadap pesan di atas dengan kunci $k = 1$ sampai $k = 3$..

Kunci	Hasil dekripsi
1	TSSOAELYROAANDNGIG
2	TSALRANNISOEYOADGG
3	TOLONGSAYADISERANG

Tabel 1. Contoh Dekripsi Terhadap *Scytale*

Karena dekripsi dengan k = 3 menghasilkan pesan yang bermakna, maka bisa disimpulkan bahwa pesan yang dikirim adalah TOLONG SAYA DISERANG

Cipher Caesar

Algoritma kriptografi ini pertama kali digunakan oleh Julius Caesar. Idenya adalah mengganti setiap huruf dengan huruf ke-n sesudah huruf tersebut dalam susunan abjad.
Misalnya, tiap huruf disubstitusi dengan huruf kelima berikutnya, maka akan diperoleh tabel substitusi seperti di bawah ini:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
FGHIJKLMNOPQRSTUVWXYZABCDE
```

Untuk mengenkripsi pesan, huruf di barisan bawah ditulis sebagai pengganti huruf pada kolom yang sama di barisan atas. Untuk mendekripsi pesan, tiap huruf pada cipherteks diacu ke barisan bawah dan diganti dengan huruf pada kolom yang sama di barisan atas. Sebagai contoh, dengan menggunakan tabel substitusi di atas, pesan

```
SERANG KAMPUNG GALIA
```

dienkripsi menjadi

```
XJWFSL PFRUZSL LFQNF
```

Pada algoritma kriptografi ini, kunci enkripsi yang perlu diketahui oleh penerima pesan adalah jumlah pergeseran huruf. Pada contoh di atas, kuncinya adalah 5 (jumlah pergesernan huruf).

Secara matematis, fungsi enkripsi untuk cipher Caesar adalah

$E(x_i) = (x_i+k) \bmod 26$

dengan x_i adalah huruf ke-i dalam susunan abjad dan k adalah kunci enkripsi. Fungsi dekripsi untuk cipher Caesar dapat dinyatakan sebagai

$D(x_i) = (x – k) \bmod 26$

Kelemahan utama cipher Caesar adalah sangat sedikitnya jumlah kunci, yaitu sejumlah huruf pada sistem abjad yang digunakan (dalam hal ini ada 26). Karena hanya ada 26 kunci, maka seorang kriptanalis dapat memecahkan cipher Caesar dengan cara *brute force* dalam waktu singkat.

Misalkan kriptanalis menemukan potongan cipherteks FDHVDU dan ia tahu bahwa algoritma kriptografi yang digunakan adalah cipher Caesar. Maka ia hanya perlu mencoba mendekripsikan cipherteks tersebut dari kunci terkecil (0) sampai kunci terbesar (25) lalu memeriksa apakah ada di antara hasil dekripsi yang memiliki makna. Tabel 2 memuat hasil dekripsi terhadap cipherteks FDHVDU dengan menggunakan semua kunci yang mungkin.

Kunci	Hasil dekripsi
0	FDHVDU
1	GEIWEV
2	HFJXFW
3	IGKYGX
4	JHLZHY
5	KIMAIZ
6	LJNBJA
7	MKOCKB
8	NLPDLC
9	OMQEMD
10	PNRFNE
11	QOSGOF
12	RPTHPG
13	SQUIQH
14	TRVJRI
15	USWKSJ
16	VTXLTK
17	WUYKUL
18	XVZLVM
19	YWAMWN
20	ZXBNXO
21	AYCOYP
22	BZDPZQ
23	CAESAR
24	DBFTBS
25	ECGUCT

Tabel 2. Contoh Dekripsi Terhadap Cipher Caesar Secara Brute Force

Dari hasil dekripsi pada Tabel 1, terlihat bahwa plainteks yang paling mungkin adalah CAESAR dengan menggunakan k = 21.

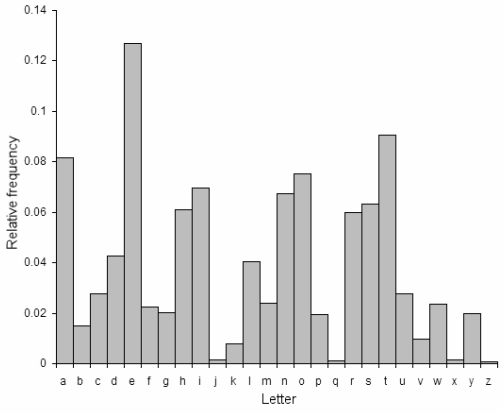
Cipher Substisuti Huruf Tunggal

Dalam perkembangan selanjutnya, barisan bawah pada tabel substitusi dibangkitkan secara acak. Contohnya:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
RHMNITBUDGXASLZQOCYJWFPEVK
```

Dengan cipher substitusi seperti ini, penerima pesan harus mengetahui urutan huruf pada barisan bawah yang merpakan kuncinya. Jika plainteks hanya terdiri dari huruf abjad, maka jumlah kunci yang mungkin untuk cipher substitusi ini adalah 26! = 403.291.461.126.605.635.584.000.000.

Akan tetapi cipher substitusi seperti ini masih mudah untuk dipecahkan. Dengan menggunakan teknik analisis frekuensi, misalnya, kita bisa mengetahui bahwa huruf E adalah huruf yang paling sering digunakan dalam teks bahasa Inggris, dan kata THE adalah kata yang paling sering digunakan. Histogram yang memperlihatkan frekuensi kemunculan huruf dalam teks bahasa Inggris dapat dilihat pada Gambar 1.



Gambar 1. Histogram Frekuensi Kemunculuan Huruf Dalam Teks Bahasa Inggris

Misalkan ada potongan cipherteks yang dienkripsi dengan substitusi huruf tunggal

```
C XZ X XZQ
```

Kriptanalis tidak memerlukan waktu lama untuk meyimpulkan bahwa pesan aslinya adalah

```
I AM A MAN
```

Cipher Substisusi Abjad Majemuk

Cipher abjad majemuk dibuat dari sejumlah cipher abjad tunggal, masing-masng dengan kunci yang berbeda.Cipher abjad majemuk pertama kali ditemukan oleh Leon Battista pada tahun 1467.

Contoh cipher stbstitusi abjad majemuk yang paling dikenal adalah cipher Vigénere yang diperkenalkan oleh Blaise de Vigénere pada tahun 1586. Ide dasarnya adalah dengan menggunakan cipher Caesar, tapi jumlah pergeseran hurufnya berbeda-beda untuk setiap periode beberapa huruf tertentu.

Untuk mengenkripsikan pesan dengan cipher Vigénere, digunakan *tabula recta* (disebut juga bujursangkar Vigénere) seperti pada Gambar 2.

	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

Gambar 2. Tabula Recta

Tabula recta digunakan untuk memperoleh cipherteks dengan menggunakan kunci yang sudah ditentukan. Jika panjang kunci lebih pendek daripada panjang plainteks, maka penggunaan kunci diulang.

Secara matematis, enkripsi dengan cipher Vigénere bisa dinyatakan sebagai

$$E(p_i) = V(p_i , k_{(i \bmod m)})$$

dengan:

p_i = huruf ke-i dalam plainteks
k_n = huruf ke –n dalam kunci
m = panjang kunci, dan

$V(x,y)$ = huruf yang tersimpan pada baris x dan kolom y pada *tabula recta*.

Misalkan palintext adalah `AKU ANAK SEHAT` dan kunci adalah `DOMBA`. Cipher Vigénere dilakukan sebagai berikut:

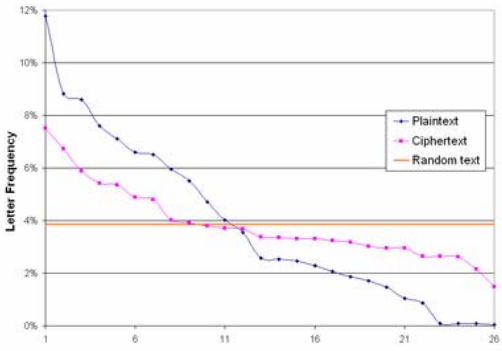
Plainteks : `AKU ANAK SEHAT`
Kunci : `DOM BADO MBADO`

Hasil enkripsinya adalah sebagai berikut:

`DYG BNDY EFHDH`

Untuk mendekripsi pesan, penerima pesan harus mengetahui kunci yang digunakan, lalu mencari baris huruf manakah yang menghasilkan huruf pada cipherteks jika kolomnya adalah huruf yang bersesuaian pada kunci. Misalnya, pada huruf pertama cipherteks (`D`), huruf yang bersesuaian pada kunci yang digunakan adalah `D`. Dengan melihat *tabula recta*, kita dapatkan bahwa huruf `D` pada tabel untuk baris huruf `D` ada pada kolom huruf `A`. Karena itu, huruf pertama plainteks adalah `A`.

Salah satu kelebihan cipher Vigénere adalah sulitnya melakukan kriptanalisis dengan metode analisis frekuensi. Pada cipher Vigénere, sulit untuk melakukan kriptanalisis dengan analisi frekuensi karena dua huruf yang sama dalam cipherteks belum tentu bisa didekripsikan menjadi dua huruf yang sama dalam plainteks. Pada contoh di atas, huruf H pada cipherteks berasal dari huruf H dan T pada plainteks. Gambar 3 memperlihatkan perbandinggan frekuensi kemunculan huruf pada suatu plainteks dan huruf pada cipherteks dengan menggunakan cipher Vigénere.



Gambar 3. Perbandingan Frekuensi Kemunculan Huruf Pada Cipher Vigénere

Kelemahan utama cipher Vigénere adalah kuncinya yang pendek dan penggunaannya yang berulang-ulang. Jika kriptanalis dapat menentukan panjang kuncinya, maka cipherteks dapat diperlakukan seperti rangkaian beberapa cipher Caesar.

Pada abad ke-19, dikembangkanlah algoritma-algoritma lain untuk cipher abjad majemuk. Algoritma-algoritma tersebut biasanya menggunakan tabel-tabel yang lebih rumit daripada *tabula recta* dan untuk mengenkripsikan satu pesan saja butuh waktu lama.

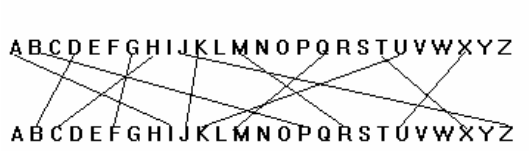
Enigma

Memasuki abad ke-20, orang mulai menggunakan sambungan listrik (*electrical conntection*) untuk mengotomasi pekerjaan mengonversi huruf dengan bantuan tabel. Salah satu mesin enkripsi yang paling terkeal pada awal abad ke-20 adalah Enigma.

Enigma pertama kali diciptakan oleh Arthur Scherbius di Berlin pada tahun 1918. Enigma adalah mesin yang digunakan Jerman selama Perang Dunia II untuk mengenkripsi dan mendekripsi pesan-pesan militer. Mesin ini juga mampu mengirim dan menerima pesan.

Prinsip Kerja Enigma

Enigma melakukan enkripsi dengan cara melakukan beberapa kali substitusi huruf. Scherbius mengimplementasikan substitusi huruf ini dengan menggunakan sambungan listrik melalui kawat (*wiring*). Gambar 4 memperlihatkan beberapa contoh *wiring* pada Enigma.

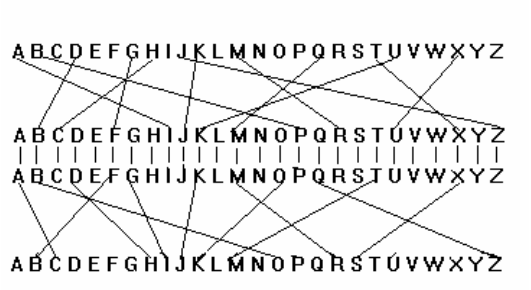


Gambar 4. Contoh *Wiring* pada Enigma

Gambar 4 di atas hanya memperlihatkan 12 dari 26 sambungan yang ada. Pada gambar di atas terlihat bahwa huruf Q tersambung dengan hurf M. Ini berarti jika terminal Q di barisan atas dialiri listrik, maka terminal M di barisan bawah akan ikut teraliri listrik.

Ide dasarnya adalah memasang tombol saklar pada barisan di atas dan lampu pada barisan di bawah. Jika saklar pada huruf Q ditekan, maka lampu pada terminal M di barisan bawah akan menyala. Ini menunjukkan bahwa huruf M merupakan substitusi untuk huruf Q.

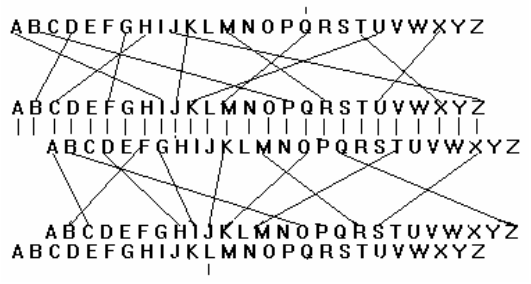
Ide berikutnya adalah untuk menyambungkan terminal output di barisan bawah ke terminal input barisan lain dan memindahkan semua lampu ke terminal ouput barisan yang baru, seperti terlihat pada Gambar 5.



Gambar 5. Contoh *Wiring* Dua Tingkat pada Enigma

Pada Gambar 5, arus yang dialirkan ke terninal M di barisan kedua dikirimkan ke terminal R pada barisan ketiga. Jika saklar pada huruf Q ditekan, maka lampu pada terminal R akan menyala.

Ide berikutnya adalah untuk menggeser sambungan antara barisan kedua dan barisan ketiga sebanyak satu huruf setiap kali ada saklar di barisan pertamayang dtekan. Gambar 6 memperlihatkan pergerseran sambungan setelah saklar di barisan pertama ditekan dua kali.



Gambar 6. Keadaan *Wiring* Setelah Dua Kali Pergeseran

Pada Gambar 6 terlihat ada dua operasi cipher Caesar yang dilakukan, yaitu pada barisan kedua dan ketiga. Jika saklar pada terminal Q ditekan, maka arus listrik akan diteruskan ke terminal input M pada barisan kedua lalu ke terminal output K pada barisan kedua. Setelah itu, arus listrik akan mengalir ke terminal input J pada barisan ketiga lalu ke terminal L sehingga lampu pada terminal L akan menyala. Setelah itu, sambungan antara baris kedua dan ketiga akan bergeser lagi.

Barisan-barisan pada Gambar 4, 5 dan 6 dapat diimplementasikan dengan mengunakkan *rotor* (mesin berbentuk roda yang berputar). Inilah prinsip kerja Enigma.

Penggunaan *Reflector*

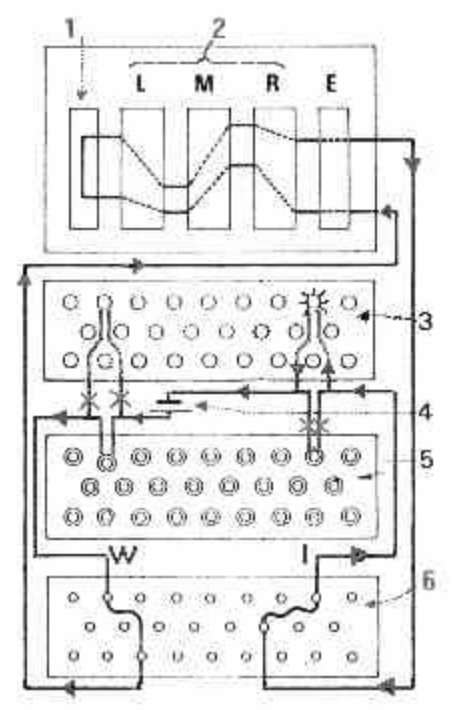
Untuk menambah kerumitan, penemu Willi Korn menambahkan sebuah *reflector* yang berfungsi membalikkan jalannya arus dari *rotor* paling bawah kembali *rotor* paling atas. Dengan adanya *reflector*, ada *2r + 1* (*r* = jumlah *rotor*) kali operasi substitusi huruf dalam Enigma: *r* kali oleh masing-masing *rotor*, satu kali oleh *reflector* dan *r* kali lagi oleh masing-masing *rotor* pada arah yang berlawanan.

Salah satu efek dari penggunaan *reflector* adalah bertambanya jumlah kemungkinan substitusi huruf menjadi 26 kali jumlah kemungkinan semula.

Tapi penggunaan *refelctor* bukannya tanpa kelemahan. Adanya *refelctor* membuat Enigma bersifat resiprok. Jika pada suatu posisi *rotor* huruf A dienkripsikan menjadi Q, maka pada posisi *rotor* yang sama, huruf Q akan dienkripsikan menjadi A. Selain itu, adanya *reflector* membuat suatu huruf tidak bisa dienkripsi menjadi huruf itu sendiri. Pengetahuan tentang kelemahan inilah yang menjadi dasar para ilmuwan Polandia untuk memecahkan sandi yang dikirim dengan Enigma.

Sebenarnya ada satu keuntungan lain yang diperoleh dengan adanya *reflector* pada Enigma. *State* pada Enigma tidak perlu diubah-ubah dari mode enkripsi ke mode dekripsi, dan sebaliknya. Hal ini dapat mengurangi banyaknya kesalahan oleh para operator yang lupa mengubah-ubah *state* pada Enigma. Akan tetapi pada akhirnya Jerman harus membayar mahal untuk penggunaan *reflector* ini.

Gambar 7 menunjukkan mekaisme kerja Enigma dengan menggunakan *reflector*.



Gambar 7. Cara Kerja enigma

Pada Gambar 7 di atas, operator menekan saklar W pada papan ketik (5). Arus dari baterai (4) akan mengalir ke soket W *plugboard* (6). Karena soket W disambung ke soket X, maka arus masuk ke *entry disc* (E) pada terminal X. Arus lalu mengalir melalui *rotor* R, M dan L (2) sampai ke *reflector* (1). Dari *reflector*, arusnya dibalikkan lagi ke *rotor* L, M dan R sampai ke *entry disc* pada terminal H. Dari *entry disc,* arus ditersukan ke *plugboard*. Karena soket H pada *plugboard* tersambung ke soket I, maka arus akan mengalir ke soket I yang mengakibatkan lampu I menyala. Kesimpulannya, huruf W dienkripsi menjadi huruf I.

Layout papan ketik pada Enigma dapat dilihat pada Gambar 8

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

Gambar 8. *Layout* Papan Ketik Enigma

***Rotor* Enigma**

Ketika diciptakan, Enigma hanya memiliki 3 buah *rotor* yang masing-masing diberi nama I, II dan III Ketiga *rotor* ini bisa dipasang dengan urutan apapun dari kiri ke kanan. Posisi *rotor* di sebelah kiri disebut posisi L, posisi tengah M dan posisi kanan R. Pada tahun 1938, pihak Jerman menambahkan rotor IV dan V. Ada juga beberapa *rotor* lain yang dibuat, tapi jumlah *rotor* yang dapat digunakan pada satu waktu di mesin Enigma tetap 3.

Tabel 3 memuat beberapa jenis *rotor* yang digunakan oleh Enigma beserta subsitusi huruf yang dihasilkan oleh masing-masing *rotor*.

Rotor	ABCDEFGHIJKLMNOPQRSTUVWXYZ
I	EKMFLGDQVZNTOWYHXUSPAIBRCJ
II	AJDKSIRUXBLHWTMCQGZNPYFVOE
III	BDFHJLCPRTXVZNYEIWGAKMUSQO
IV	ESOVPZJAYQUIRHXLNFTGKDCMWB
V	VZBRGITYUPSDNHLXAWMJQOFECK
VI	JPGVOUMFYQBENHZRDKASXLICTW
VII	NZJHGRCXMYSWBOUFAIVLPEKQDT
VIII	FKQHTLXOCBJSPDZRAMEWNIUYGV

Tabel 3. Beberapa Jenis *Rotor* pada Enigma

Reflector yang digunakan pada Enigma pun ada beberapa jenis. Setidaknya ada empat jenis *reflector* yang pernah digunakan pada Enigma. Tabel 4 memuat beberapa jenis *reflector* yang digunakan dan pertukaran huruf yang dihasilkannya (contoh: pada *reflector* B, huruf A dienkripsi menjadi huruf Y dan sebaiknya).

Reflector	
B	AY BR CU DH EQ FS GL IP JX KN MO TZ VW
C	AF BV CP DJ EI GO HY KR LZ MX NW TQ SU
B Dünn	AE BN CK DQ FU GY HW IJ LO MP RX SZ TV
C Dünn	AR BD CO EJ FN GT HK IV LM PW QZ SX UY

Tabel 4. Beberapa Jenis *Reflector* pada Enigma

Setiap kali ada saklar yang ditekan, rotor R akan berputar sejauh 1/26 putaran (1 huruf). Ketika *rotor* R mencapai posisi tertentu (disebut posisi *turnover*), ia akan ikut menggeser *rotor* M sejauh 1 huruf. Dan ketika *rotor* M mencapai posisi *turnover*, ia akan ikut menggeser *rotor* L sejauh 1 huruf. Tabel 5 menunjukkan posisi *turnover* masing-masing *rotor*.

Rotor	**Posisi *Turnover***
I	R
II	F

III	W
IV	K
V	A
VI, VII dan VIII	A dan N

Tabel 5. Posisi Turnover pada Beberapa *Rotor*

Penyetelan Enigma

Pihak Jerman membuat spesifikasi yang mendetil mengenai penggunaan Enigma. Hampir semua hal tentang penyetellan Enigma dispesifikasikan, kecuali posisi mulai tiap *rotor*. Spesifikasi setelan enigma ditulis pada lembar penyetelan (*setting sheet*) untuk periode satu bulan dan selalu berubah setiap hari. Spesifikasi ini kemudian disebarkan ke semua operator melalui kurir.

Berikut ini adalah contoh spesifikasi harian.

```
31
I V III
F T X
UA PF RQ SO NI EY BG HL TX ZJ
```

Pada baris paling atas, 31 menunjukkan tanggal pada bulan yang sedang berjalan. Baris kedua menunjukkan *rotor* yang digunakan dari kiri ke kanan (dalam hal ini I, V dan III). Baris ketiga menunjukkan posisi awal masing-masing *rotor*. Posisi awal *rotor* L (I) adalah F, *rotor* M (V) adalah T dan rotor R (III) adalah X. Baris terakhir memuat spesifikasi sambungan antar soket pada *plugboard*, misalnya huruf U disambungkan dengan huruf A dan seterusnya.

Baik pengirim maupun penerima pesan selalu mendapat lembar penyetelan ini sehingga mereka bisa menyetel mesinnya dengan setelan yang sama persis setiap harnya.

Ketika mengirimkan pesan, pengirim pesan menentukan posisi awal masing-masing *rotor* dan mengirimkannya kepada penerima sebagai *preamble* dari pesan yang dikirm. Berikut ini langkah-langkah mengirimkan pesan dengan Enigma:

1. Setel mesin Enigma dengan konfigurasi dasar seperti tertulis pada lembar penyetelan.
2. Pilih tiga huruf (indikator) sebagai awal untuk mengenkripsi kunci pesan yang terdiri dari tiga huruf.
3. Putar masing-masing *rotor* ke posisi indikator. Masukkan kunci pesan dua kali dan catat lampu apa saja yang menyala.
4. Putar masing-masing *rotor* ke poisi kunci pesan lalu ketikkan pesan yang akan dikirim. Catat lampu apa saja yang menyala.
5. Serahkan pesan yang telah dienkripsi beserta *preamble*-nya kepada operator radio untuk dikirimkan dengan kode Morse.

Untuk mendekripsikan pesan dengan Enigma, langkah-langkah berikut haurs dilakukan:

1. Setel mesin Enigma dengan konfigurasi dasar seperti tertulis pada lembar penyetelan.
2. Putar masing-masing *rotor* ke posisi indikator yang tertera pada *preamble* pesan yang dikirim.
3. Masukkan enam huruf berikutnya untuk mendapatkan kunci pesan yang diulang.
4. Putar masing-masing *rotor* ke posisi kunci pesan, lalu ketikkan pesan yang dikirim untuk mendekripsikannya.

Kunci dari pesan yang dikirm harus dikirim dua kali untuk memastikan bahwa kunci yang dikirim tidak salah. Namun ini adalah kesalahan besar yang dilakukan oleh pihak Jerman karena data yang dikirim menjadi redundan. Kesalahan ini membuat para analis dari Polandia berhasil memecahkan sebagian besar dari sandi yang dikirim oleh Enigma.

Kompleksitas Enigma

Pada mesin Enigma dengan 3 buah *rotor*, ada 26 x 26 x 26 = 17.576 *state rotor* yang mungkin. Karena posisi ketiga *rotor* yang digunakan dapat diubah-ubah, maka ada 6 x 17.576 = 105.456 *state* yang mungkin. Untuk 10 pasang huruf yang tersambung pada *plugboard*, ada 26! / (6! 10! 210) = 150.738.274.937.250 *state* yang mungkin terjadi pada *plugboard*. Jadi secara keseluruhan, ada sekitar 15.000.000.000.000.000.000 kombinasi yang mungkin terjadi. Iapapun yang mencoba melakukan kriptanalisis terhadap pesan yang disandikan dengan Enigma harus mencari tahu *state* manakah di antara 15.000.000.000.000.000.000 *state* yang digunakan. Pihak Jerman menganggap itu sebagai sesuatu yang mustahil dan komputer yang paling canggih pun mungkin membutuhkan

waktu lebih dari satu tahun untuk mencoba melakukan dekripsi secara *brute force*.

Kriptanalisis Terhadap Enigma

Seperti telah dibahas sebelumnya, penyandian dengan Enigma memiliki beberapa kelemahan, antara lain:

1. Penyandian bersifat resiprok. Jika pada suatu *state* huruf A dienkripsi menjadi huruf Q, maka huruf Q akan dienkripsi menjadi huruf A.
2. Suatu huruf tidak dapat dienkripsi menjadi huruf itu sendiri.
3. Posisi *turnover* pada *rotor-rotor* awal berbeda-beda. Ini adalah suatu kesalahan karena bisa mengungkap *rotor* manakah yang digunakan pada posisi R. Seharusnya semua *rotor* memiliki posisi *turnover* yang sama. Para kriptanalis membuat ungkapan yang merupakan kepanjangan dari posisi awal *rotor* I sapai V: Royal Flags Wave Kings Above.
4. Kunci pesan dikirimkan dua kali.

Peran Polandia dalam Melakukan Kriptanalisis Terhadap Enigma

Ketika kekuatan militer Jerman mulai meningkat pada 1920-an, orang-orang Polandia merasa terancam karena berada di antara dua negara adidaya: Jerman di barat dan Rusia di Timur. Untuk mengetahui apa yang direncanakan oleh musuh-musuh potensial mereka, mereka mencoba menyadap transmisi radio Jerman. Pada tahun 1928, pihak Polandia mulai menyadari bahwa Jerman mengirimkan pesan yang dienkripsikan degan suatu alat, yang kemudian diketahui bernama Enigma.

Pada awalnya intelijen Polandia tidak dapat memecahkan sandi yang dienkripsikan dengan Enigma. Mereka lalu mencoba melakukan pendekatan secara matematis. Pada tahn 1932 dibentuklah suatu kelompok ahli matematika yang terdiri dari Jerzy Rozycki, Henryk Zygalski dan Marian Rejewski.

Rejewski menunjukkan bahwa metode-metode matematis dapat digunakan untuk mencari kunci pesan yang selalu dikirim dua kali pada awal transmisi.

Masalah yang masih harus dipecahkan adalah *wiring* pada masing-masing *rotor*. Untuk masalah ini, mereka dibantu oleh pihak Prancis yang juga merasa kuatir dengan menguatnya pasukan militer Jerman.

Pada tahun 1931 dan 1932, Gustave Bertrand, kriptografer asal Prancis, mendapatkan informasi mengenai mesin Enigma Jerman dari seorang mata-mata Hans-Tilo Schmidt. Informasi tersebut berkaitan dengan cara pengopersian Enigma oleh pihak Jerman dan lembar-lembar penyetelan yang selalu diedarkan setiap bulan. Pihak Prancis tidak dapat menggunakan informasi ini untuk memecahkan sandi Enigma. Mereka lalu menyebarkan informasi ini kepada pihak Inggris, namun Inggris pun tidak mampu memecahkan sandi Enigma. Akhirnya Bertrand menyebarkan informasi ini kepada pihak Polandia yang pada waktu itu belum memberi tahu siapa-siapa tentang perkembangan mereka dalam memecahkan sandi Enigma. Informasi ini memungkinkan Rejewski untuk memecahkan *wiring* pada setiap *rotor*. Tapi masih ada satu masalah yang tersisa, yaitu bagaimana urutan huruf pada masing-masing *rotor*.

Pada mesin Enigma di Polandia, urutan huruf pada setiap *rotor* sama dengan urutan huruf pada papan ketiknya, yaitu

```
QWERTZUIOASDFGHJKPYXCVBNML
```

Rejewski menyadari bahwa urutan huruf pada mesin Enigma Jerman pasti berbeda. Ia lalu berandai-andai, mungkin Jerman menggunakan urutan huruf seperti pada urutan huruf abjad:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

Rejewski mencoba melakukan kriptasalisis dengan urutan ini dan ternyata berhasil. Pemecahan *wiring* oleh Rejewski ini memngkinkan para kriptografer di olandia untuk membuat mesin Enigma yang sama persis dengan mesin Enigma yang digunakan oleh pihak Jerman untuk mendekripsikan pesan-pesan yang disadap dari transmisi radio Jerman. Hasilnya, 75% pesan yang dienkripsi dengan Enigma dapat dipecahkan.

DAFTAR PUSTAKA

[1] Munir, Rinaldi. (2004). Bahan Kuliah IF5054 Kriptografi. Departemen Teknik Informatika, Institut Teknologi Bandung.

[2] Wikipedia (2006), http://*www.wikipedia.org*. Tanggal akses: 10 Oktober 2006

[3] The Enigma Cipher Machine, *http://www.codesandciphers.org.uk/enigma* . Tanggal akses: 10 Oktober 2006.

[4] On Enigma and a Method for its Decryption (2006), **http://www.cs.miami.edu/~harald**. Tanggal akses : 10 Oktober 2006