Cipher Jefferson

Teguh Pamuji – NIM : 13503054

Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if13054@students.if.itb.ac.id

Abstraksi`

Secara umum algoritma kriptografi klasik dibedakan menjadi dua jenis, yaitu algoritma berbasis substitusi dan algoritma berbasis transposisi. Jenis algoritma pertama menggunakan pergantian karakter atau kumpulan karakter dengan karakter lainnya untuk melakukan enkripsi dan dekripsi, sedangkan algoritma berbasis transposisi menggunakan teknik penukaran karakter dengan karakter lainnya dalam satu kalimat (teks-plain atau teks-cipher). Algoritma kriptografi klasik sudah jarang digunakan karena tergantikan oleh algoritma modern yang terbukti memiliki lebih sedikit kelemahan, namun tetap perlu dipelajari sebagai dasar algoritma kriptografi modern. Salah satu algoritma yang termasuk ke dalam algoritma kriptografi klasik adalah Cipher Jefferson (Jefferson Cipher).

Makalah ini akan membahas teknik enkripsi, teknik dekripsi, dan contoh implementasi sederhana algoritma Cipher Jefferson. Selain itu akan dibahas juga aspek-aspek nonteknis algoritma Cipher Jefferson, semisal sejarah, kelebihan, kelemahan, dan informasi lainnya seputar Cipher Jefferson. Sebagai pelengkap makalah ini juga akan memberikan perbandingan Cipher Jefferson dengan beberapa algoritma cipher klasik lainnya.

Kata kunci: Jefferson Cipher, kriptografi, enkripsi, dekripsi

1. Pendahuluan

Saat ini algoritma kriptografi klasik diyakini sudah tidak cukup ampuh untuk menyembunyikan informasi karena mudah dipecahkan oleh teknik komputasi menggunakan alat tertentu. Akan tetapi algoritma kriptografi klasik masih dirasa penting untuk dipelajari karena merupakan dasar berkembangnya kriptografi modern yang umum dipakai sekarang.

Salah satu algoritma kriptografi klasik yang terbilang ampuh pada masanya adalah Cipher Jefferson yang diciptakan oleh salah satu mantan presiden Amerika Serikat, Thomas Jefferson. Sayangnya Cipher Jefferson kurang memiliki pamor seperti Cipher Caesar atau Cipher Vigenere karena penggunaanya yang terbatas, namun tetap saja dirasa penting untuk membahas Cipher Jefferson sebagai pembanding, bahkan pesaing kedua algoritma cipher lainnya tersebut sebagai cipher klasik terbaik pada masanya masing-masing.

2. Sejarah Cipher Jefferson

Seperti dituliskan di atas, Cipher Jefferson ditemukan oleh salah seorang mantan presiden Amerika Serikat, Thomas Jefferson. Teknik cipher ini digunakan pada masa kerjanya sebagai duta besar Amerika Serikat untuk Perancis [ROL02] sebagai sarana untuk menyampaikan pesan dengan aman ke Amerika Serikat. Di bawah ini adalah gambar Thomas Jefferson, pencipta Cipher Jefferson:

Tidak ada tahun pasti mengenai penciptaan teknik cipher ini, namun diperkirakan pada

sekitar tahun 1795 [WIK06] dan dihentikan penggunaannya pada 1802 [CLA06]. Hal itu disebabkan oleh tidak adanya publikasi Cipher Jefferson. Pada masa pemakaian itu, hanya Thomas Jefferson dan beberapa orang terdekatnya saja yang mengetahui dan menggunakan algoritma cipher tersebut. Namun Thomas Jefferson sempat menulis dan menyimpan dokumentasinya sebelum cipher tersebut ”hilang” pemakaiannya. Dari dokumentasi inilah akhirnya terungkap pemakaian Cipher Jefferson.

Tanpa diketahui bahwa Thomas Jefferson adalah penemu pertamanya, pada tahun 1890 seorang kriptologis Perancis menciptakan teknik dan alat serupa. Orang tersebut adalah Commandant Etienne Bazeries [WIK06] dan alat cipher ciptaannya disebut Silinder Bazeries (*Bazeries Cylinder*).

“Ciptaan kedua” tersebut kemudian dimodernisasi dan selanjutnya digunakan oleh pihak militer Amerika Serikat. Rentang waktu penggunaanya adalah sejak tahun 1922 hingga Perang Dunia II, tepatnya tahun 1942. Sistem cipher yang digunakan militer Amerika Serikat tersebut diberi nama kode M-94.

3. Disk Jefferson

Disk Jefferson (*Jefferson Disks*) atau sering juga disebut *Jefferson Wheel* adalah alat yang diciptakan Thomas Jefferson untuk melakukan enkripsi dan dekripsi dalam teknik cipher ini. Alat ini terkadang juga disebut sebagai Silinder Bazeries karena memang kedua alat tersebut memiliki konsep kerja yang tidak berbeda. Berikut adalah foto salah satu Disk Jefferson yang dimiliki oleh National Cryptologic Museum, Amerika Serikat:

Lebih detail, Disk Jefferson adalah sebuah silinder terbuat dari kayu, berukuran panjang sekitar l5 cm dan tebal 4 cm dengan lubang di tengahnya sebagai tempat poros pemutar (*spindle*), dipotong beriris dengan lebar sekitar 5 mm. Selanjutnya permukaan tiap irisan tersebut dibagi menjadi dua puluh enam bagian, setiap bagiannya diberi satu karakter yang diambil dari alfabet, dan dilakukan secara acak hingga kedua puluh enam bagian permukaan irisan tersebut terisi karakter-karakter alfabet yang berbeda. Kemudian batang panjang sebagai poros pemutar dimasukkan melalui lubang yang dibuat di tengah silinder dan dipasangkan pada penopang. Hal ini menyebabkan tiap irisan disk dapat diputar.

Alat ini bisa dianggap sederhana, namun memiliki kemampuan yang baik dalam mengenkripsi pesan. Pembuatannya tidak terlalu sulit, apalagi untuk membuat replikanya saja dapat menggunakan bahan-bahan yang ada di sekitar sebagai contoh Disk Jefferson sederhana.

4. Teknik Enkripsi dan Dekripsi

4.1. Teori Enkripsi Cipher Jefferson

Cipher Jefferson melakukan enkripsi dengan menggunakan prinsip substitusi abjad tunggal, dimana satu karakter teks-plain digantikan dengan satu karakter lain menggunakan Disk Jefferson yang sudah dijelaskan sebelumnya. Hal ini dilakukan sampai semua karakter pada teks-plain sudah berganti menjadi karakter-karakter yang terlihat acak dan tidak beraturan. Kumpulan karakter acak itu dianggap sebagai teks-cipher. Proses inilah yang selanjutnya disebut sebagai satu tahap enkripsi.

Untuk melakukan enkripsi, syarat yang harus dipenuhi hanyalah adanya teks-plain dan Disk Jefferson. Kunci tidak diperlukan sebab pengaturan irisan disk dan pengacakan huruf yang khas pada tiap irisan bisa dikategorikan sebagai kunci untuk melakukan enkripsi dan dekripsi, dengan syarat pengirim dan penerima memiliki Disk Jefferson yang sama pengurutan disk dan pengacakan hurufnya.

Mengenai masalah kunci, sebenarnya terdapat satu alternatif kunci untuk melakukan enkripsi dan dekripsi. Setiap irisan disk pada silinder Disk Jefferson dapat diberi nomor urut tertentu. Nomor-nomor inilah yang dapat dimanfaatkan sebagai kunci dengan kesepakatan pihak penerima dan pengirim bahwa proses enkripsi dan dekripsi dilakukan dengan urutan disk yang ditentukan sejak awal.

Langkah pertama adalah menempatkan teks-plain pada Disk Jefferson. Hal ini dilakukan dengan mengeja teks-plain perhuruf pada tiap irisan disk membentuk satu baris yang rapi. Untuk mendapatkan huruf yang diinginkan pengirim memutar tiap irisan disk yang berisi huruf alfabet teracak ke atas atau ke bawah. Hal ini dilakukan sampai teks-plain tertulis dalam satu baris pada silinder Disk Jefferson.

Perlu diketahui bahwa isi teks-plain hanya diperbolehkan berupa karakter-karakter yang terdapat dalam alfabet sehingga variasi karakter yang diizinkan sebanyak dua puluh enam saja. Hal ini berlaku juga pada teks-cipher. Dalam menuliskan pesan tidak diperbolehkan menggunakan spasi, angka, maupun karakter-karakter lain di luar alfabet. Maka langkah pertama juga sekaligus menjadi tahap pengonversian pesan menjadi teks-plain yang dapat diterima oleh Disk Jefferson. Hal ini menjadi salah satu kekurangan Cipher Jefferson, yang akan dibahas kemudian.

Langkah berikutnya adalah mendapatkan teks-cipher dari teks-plain yang sudah ditempatkan pada silinder Disk Jefferson. Untuk melakukannya tidak sulit, sebab pengirim tinggal melihat saja baris lain pada silinder, yang dapat dipastikan berisi barisan karakter acak dari alfabet sejumlah karakter pada teks-plain. Pengirim dapat memilih salah satu dari dua puluh lima baris selain teks-plain. Baris yang dipilih tersebut merupakan teks-cipher yang siap dikirim.

Untuk mempersulit serangan oleh pihak yang tidak berhak, ada satu cara yang bisa ditambahkan. Cara tersebut adalah menyusun karakter-karakter teks-cipher sesuai dengan urutan silinder satu sampai nomor urut silinder terakhir. Dengan bantuan cara ini karakter-karakter pada teks-cipher menjadi tidak berurut, msangat menyulitkan pihak penyadap untuk mendekripsi paksa teks-cipher. Namun dengan cara ini kunci berupa nomor urut irisan silinder menjadi sangat penting untuk dimiliki pihak penerima.

Untuk pesan yang panjangnya melebihi jumlah irisan disk terdapat satu perlakuan khusus. Teks-plain panjang tersebut dipecah-pecah menjadi beberapa fragmen untuk selanjutnya setiap fragmen tersebut dienkripsi secara independen menggunakan teknik enkripsi yang dijelaskan di atas. Hal ini dilakukan sampai seluruh isi pesan sudah terenkripsi.

Langkah terakhir adalah menuliskan teks-cipher dan mengirimkannya ke pihak penerima. Jika proses enkripsi menggunakan kunci nomor urutan disk, maka kunci tersebut juga dapat diikutsertakan untuk dikirim bersamaan teks-cipher.

Kesalahan dalam melakukan proses enkripsi sangat kecil kemungkinannya untuk terjadi sebab Disk Jefferson termasuk mudah dan sederhana digunakan. Jika memang terjadi kesalahan, pihak pengenkripsi dapat dengan mudah menyadari dan membetulkan kesalahannya. Lagipula, kesalahan satu karakter tidak berpengaruh ke proses enkripsi karakter lainnya.

4.2. Teori Dekripsi Cipher Jefferson

Untuk melakukan dekripsi, langkah-langkah yang dilakukan kira-kira sama dengan langkah-langkah yang dibutuhkan untuk melakukan enkripsi. Syarat utamanya adalah pihak penerima memiliki Disk Jefferson berisi irisan-irisan disk yang identik dengan Disk Jefferson yang dipakai pengirim untuk mengenkripsi pesan. Sedikit perbedaan dengan enkripsi adalah pencarian teks-plain yang dirasa cocok sebagai pesan sebenarnya. Selebihnya langkah-langkah melakukan enkripsi dapat diterapkan untuk melakukan dekripsi.

Langkah awal untuk melakukan dekripsi adalah mengurutkan disk sesuai dengan kunci nomor urut yang telah disepakati sebelumnya atau menggunakan nomor urut disk yang dikirimkan. Jika proses enkripsi tidak menggunakan Disk Jefferson dengan nomor urut disk, maka pihak penerima teks-cipher dapat mengabaikan langkah ini.

Langkah berikutnya adalah memasukkan teks-cipher ke dalam Disk Jefferson. Sama seperti proses enkripsi, penerima teks-cipher mengeja setiap karakter dari teks-cipher ke setiap irisan disk, membentuknya ke dalam satu baris pada silinder. Untuk setiap karakter, penerima memutar satu irisan disk ke atas atau ke bawah sampai menemukan karakter yang cocok dengan karakter teks-cipher, dilanjutkan dengan karakter berikutnya. Proses barusan dilanjutkan sampai seluruh karakter terbaca dalam satu baris lurus.

Selanjutnya, langkah yang harus dilakukan penerima teks-cipher adalah mencari di antara baris selain teks-cipher, satu baris yang kira-kira cocok terbaca sebagai teks-plain dari pengirim. Sangat kecil kemungkinan terdapat lebih dari satu baris karakter-karakter yang membentuk pesan berarti. Ini berarti penerima tidak perlu bersusah payah untuk mencari baris teks-plain yang memiliki arti yang sesuai dengan keinginan pengirim.

Jika sudah mendapatkan satu baris karakter-karakter yang berarti, maka itulah yang disebut teks-plain. Ini menandakan selesainya tahap enkripsi, pengiriman, dan dekripsi pesan. Untuk membalas pesan, penerima tinggal menggunakan tahap yang sama seperti tahapan di atas, dan seterusnya.

Sama seperti enkripsi, kesalahan dalam proses dekripsi sangat kecil kemungkinannya untuk terjadi. Penerima pasti menyadari jika da penyimpangan satu karakter pada teks-plain yang dihasilkan dari proses dekripsi. Penyimpangan karakter tersebut dapat segera diperbaiki dengan menggunakan asumsi. Selain itu kesalahan dekripsi pada satu karakter tidak berpengaruh pada proses dekripsi pada karakter-karakter lainnya.

4.3. Contoh Enkripsi dan Dekripsi

Berikut ini akan diberikan sebuah contoh implementasi sederhana melakukan enkripsi dan dekripsi pada Cipher Jefferson. Contoh ini juga sekaligus akan menjelaskan cara singkat menggunakan alat Disk Jefferson.

Misalnya pihak pengirim ingin memberikan pesan singkat rahasia yaitu ”perang dimulai 11 Maret”. Pesan ini belum dapat diterima oleh Disk Jefferson sebab pesan tersebut mengandung karakter ilegal spasi dan angka. Karena Disk Jefferson hanya akan menerima karakter-karakter dalam alfabet, maka pekerjaan awal pengirim pesan adalah mengonversikan pesan tersebut agar bisa ditempatkan pada Disk Jefferson. Misalnya saja konversi pesan yang dilakukan mengubah pesan menjadi ”perangdimulaisebelasmaret”. Inilah yang disebut teks-plain yang dapat diterapkan pada Disk Jefferson.

Langkah berikutnya adalah pengirim menyusun dan mengurutkan irisan-irisan disk sesuai keinginannya atau sesuai kesepakatan pihak pengirim dan penerima. Nomor urut inilah yang akan menjadi kunci enkripsi dan dekripsi pesan yang dikirimkan. Misalnya saja nomor urut irisan-irisan disknya adalah sebagai berikut:

8	13	5	25	20	11	9	3	17	19	6	21	1
10	12	24	7	15	18	4	22	16	23	2	14	

Selanjutnya pengirim memasukkan teks-plain ”perangdimulaisebelasmaret” tersebut ke dalam satu baris pada permukaan silinder Disk Jefferson. Karakter pertama ”p” didapat dengan memutar irisan silinder sampai menemukan karakter tersebut, karakter kedua juga demikian, dan seterusnya hingga selesai. Setiap karakter dimasukkan ke satu irisan hingga membentuk seperti ini:

8	13	5	25	20	11	9	3	17	19	6	21	1
p	e	r	a	n	g	d	i	m	u	l	a	i
10	12	24	7	15	18	4	22	16	23	2	14	
s	e	b	e	l	a	s	m	a	r	e	t	

Bagian atas adalah nomor urut irisan disk, sedangkan di bagian bawahnya merupakan teks-plain. Karena ruang yang terbatas, maka contoh penulisan teks-plain pada Disk Jefferson dibagi menjadi dua bagian, yaitu tiga belas karakter di bagian atas dan dua belas karakter sisanya di bagian bawah.

Langkah berikutnya yaitu memilih satu baris selain baris teks-plain untuk dijadikan teks-cipher pada Disk Jefferson. Seperti sudah disebutkan sebelumnya, pengirim memilih saja secara bebas salah satu dari dua puluh lima baris sisa pada silinder sebagai teks-cipher yang ingin dikirimkan.

Sebagai contoh, pengirim akan mengambil satu baris di atas baris teks-plain sebagai baris teks-cipher pilihannya. Hal tersebut akan digambarkan sebagai berikut, dimana baris teks-plain berada diantara dua baris berisi karakter-karakter acak:

8	13	5	25	20	11	9	3	17	19	6	21	1
a	g	y	m	s	q	b	x	u	e	h	p	f
p	e	r	a	n	g	d	i	m	u	l	a	i
d	b	t	i	a	w	m	d	w	q	v	z	x

10	12	24	7	15	18	4	22	16	23	2	14
y	h	n	d	j	l	x	w	m	s	u	q
s	e	b	e	l	a	s	m	a	r	e	t
a	r	t	c	i	q	m	d	h	f	r	o

Terlihat dari contoh gambar bahwa baris karakter yang diambil pengirim sebagai teks-cipher adalah:

8	13	5	25	20	11	9	3	17	19	6	21	1
a	g	y	m	s	q	b	x	u	e	h	p	f
10	12	24	7	15	18	4	22	16	23	2	14	
y	h	n	d	j	l	x	w	m	s	u	q	

Maka teks-cipher yang siap dikirimkan ke tujuan adalah “agymsqbxuehpfyhndjlxwmsuq”. Barisan karakter ini benar-benar teracak, tidak beraturan, dan juga tidak memiliki arti secara bahasa. Pihak yang berhasil menyadap pesan tidak akan mengerti maksud dari pesan tersebut jika tidak memiliki alat yang sama.

Selanjutnya teks-cipher dapat dikirimkan ke tujuan melalui jalur apapun yang menjamin bahwa teks-cipher sampai sesuai bentuk awal dikirimkannya. Jika belum ada kesepakatan antara pihak pengirim dan penerima sebelumnya, maka nomor urut irisan-irisan disk juga dikirimkan sebagai kunci yang digunakan untuk mendekripsi pesan.

Setelah teks-cipher sampai di tujuan dan diterima oleh pihak yang diinginkan, pihak tersebut dapat langsung mendekripsikan teks-cipher dengan syarat menggunakan Disk Jefferson yang serupa dengan yang dimiliki pengirim. Penerima tinggal melakukan langkah-langkah dekripsi yang sudah diberikan sebelumnya.

Langkah pertama dekripsi adalah menyusun irisan-irisan disk pada Disk Jefferson sesuai nomor urut yang dikirimkan. Penerima akan menyusun nomor urut tersebut serupa dengan saat pengirim melakukan enkripsi pada teks-plain, yaitu:

8	13	5	25	20	11	9	3	17	19	6	21	1
10	12	24	7	15	18	4	22	16	23	2	14	

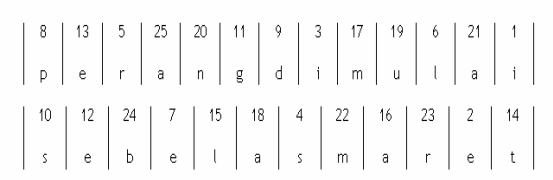
Langkah selanjutnya dalam proses dekripsi adalah menempatkan teks-cipher ke permukaan Disk Jefferson. Penempatan dilakukan karakter perkarakter hingga semua karakter teks-cipher “agymsqbxuehpfyhndjlxwmsuq” berada dalam satu baris lurus pada silinder. Hasil akhir proses tersebut dicontohkan pada gambar sebagai berikut:

8	13	5	25	20	11	9	3	17	19	6	21	1
a	g	y	m	s	q	b	x	u	e	h	p	f
10	12	24	7	15	18	4	22	16	23	2	14	
y	h	n	d	j	l	x	w	m	s	u	q	

Setelah penerima selesai menempatkan seluruh karakter teks-cipher pada Disk Jefferson, secara otomatis baris-baris lain pada permukaan silinder tersusun rapi. Hal ini dapat digambarkan sebagai berikut, dimisalkan bahwa teks-cipher yang telah dimasukkan pada silinder berada di posisi tengah:

8	13	5	25	20	11	9	3	17	19	6	21	1
q	t	u	j	a	c	y	q	n	c	d	u	p
a	g	y	m	s	q	b	x	u	e	h	p	f
p	e	r	a	n	g	d	i	m	u	l	a	i
10	12	24	7	15	18	4	22	16	23	2	14	
e	t	g	g	k	n	z	q	y	u	f	j	
y	h	n	d	j	l	x	w	m	s	u	q	
s	e	b	e	l	a	s	m	a	r	e	t	

Secara kebetulan teks-plain berada pada posisi satu baris di bawah teks-cipher karena sebelumnya pihak pengirim mengambil teks-cipher satu baris di atas teks-plain. Oleh karena itu, untuk mendapatkan teks-plain pihak penerima tidak perlu bersusah payah mencari satu persatu baris yang kira-kira cocok sebagai teks-plain. Dengan melihat sekilas saja pihak penerima menyadari bahwa karakter-karakter pada posisi satu baris di bawah teks-cipher “agymsqbxuehpfyhndjlxwmsuq” memiliki arti, yaitu sebuah baris berisikan karakter-karakter ”perangdimulaisebelasmaret”, yaitu digambarkan sebagai berikut:



Untuk sekedar memastikan, pihak penerima dapat memeriksa baris-baris lain untuk benar-benar yakin bahwa pesan tersebut merupakan pesan yang dimaksud pihak pengirim. Pada kondisi tertentu bisa saja terdapat lebih dari satu baris karakter-karakter yang memiliki arti secara bahasa, namun kondisi ini bisa dianggap sangat sulit dan jarang sekali terjadi. Jika memang terjadi kondisi seperti itu, maka tergantung pihak penerima yang memilih salah satu kandidat pesan yang dianggap kompatibel dengan pesan yang diharapkan sesuai dengan maksud pesan dari pihak pengirim teks-cipher.

Setelah benar-benar menerima dan mengerti isi pesan yang diterima, maka selesailah satu proses enkripsi dan dekripsi Cipher Jefferson.

4.4. Kesimpulan Enkripsi dan Dekripsi

Enkripsi dan dekripsi dilakukan dengan relatif mudah. Tidak perlu ada kesulitan penghitungan matematis ataupun menyubstitusikan karakter pada tabel yang rumit. Syarat utamanya adalah memiliki Disk Jefferson, barulah pihak pengirim dapat melakukan enkripsi teks-plain dan pihak penerim dapat melakukan dekripsi teks-cipher. Selain itu tidak diperlukan keahlian khusus untuk mempelajari teknik Cipher Jefferson ini, karena teknik kriptografi ini bergantung pada pemakaian alat.

5. Analisis Keamanan

Pada beberapa literatur, tingkat keamanan Cipher Jefferson kira-kira dapat disamakan dengan Cipher Vigenere karena dianggap merupakan salah satu hasil variasi dari Cipher Vigenere [THI99]. Selain itu karena Cipher Jefferson sedikit beririsan sifat dengan One-Time Pad atas kesamaannya menggunakan alat yang identik antara pengirim dan penerima, maka tingkat keamanannya dapat dianggap lebih baik dari Cipher Vigenere yang berusia lebih tua. Apalagi pada masa itu belum ada teknik komputasi otomatis seperti sekarang.

Secara umum tingkat keamanan pada penggunaan Cipher Jefferson terbilang baik. Pihak penyadap yang berhasil mendapatkan pesan berupa teks-cipher, tetapi tidak memiliki Disk Jefferson, atau memiliki Disk Jefferson yang berbeda dengan pengirim, akan mendapat kesulitan besar untuk mencari teks-plain yang dimaksud pihak pengirim. Meskipun demikian, tetap ada kesempatan, walaupun kecil, bagi pihak penyadap untuk menemukan teks-plain. Teknik-teknik yang dapat digunakan untuk mengetahui teks-plain adalah *Exhaustive Search* (*Brute Force*) dan Analisis Frekuensi.

5.1. *Exhaustive Search*

Menggunakan Exhaustive Search, pihak penyadap harus mencari kemungkinan teks-plain dengan mencoba mengombinasikan satu persatu karakter hingga membentuk teks-plain yang utuh dan sempurna. Syarat utamanya adalah pihak penyadap mengetahiu gamabaran Disk Jefferson yang dipakai mengenkripsi pesan. Meskipun terbilang tidak efektif dilakukan, teknik ini adalah salah satu teknik yang memungkinkan penyadap mengetahui kandungan pesan dari teks-cipher yang diterimanya.

Dengan *Exhaustive Search*, pihak penyadap harus menghitung kemungkinan karakter alfabet, sebanyak dua puluh enam kemungkinan untuk satu huruf. Hal ini dilakukan sejumlah semua karakter yang ada pada teks-cipher. Perhitungan pencarian kemungkinan tersebut adalah sebagai berikut:

$$26 \times 26 \times 26 \times \ldots \text{ sebanyak n jumlah perkalian}$$

Dalam proses matematis di atas, setiap jumlah kemungkinan dikalikan dengan jumlah kemungkinan berikutnya sejumlah n kali, dimana n merupakan jumlah total karakter yang terdapat pada teks-cipher. Hal ini dilakukan untuk mencari kombinasi karakter yang mungkin saja membentuk teks-plain. Penggambaran matematis di atas dapat juga dituliskan seperti pada di bawah ini:

$$f(\text{exhaustive search}) = 26^n$$

Pada fungsi di atas, n tetap merupakan jumlah total karakter yang terdapat pada teks-cipher, yang tentu saja sama jumlahnya dengan jumlah total karakter pada teks-plain.

Dari perhitungan matematis di atas terlihat bahwa banyak sekali kemungkinan yang harus dicoba satu persatu menggunakan teknik

Exhaustive Search ini. Teknik ini akan sangat melelahkan dan menghabiskan waktu, sehingga tidak disarankan untuk melakukannya secara manual, terlebih lagi untuk teks-cipher yang panjang.

Akan tetapi, jika teknik penggunaan Cipher Jefferson sudah diketahui oleh pihak penyadap, maka teknik Exhaustive Search dapat digunakan sedikit lebih singkat. Dikatakan sedikit lebih singkat sebab karakter yang ada pada teks-cipher tidak digunakan pada teks-plain. Hal ini terjadi berdasarkan konsep bahwa dalam satu irisan silinder hanya terdapat dua puluh enam karakter, sehingga kemungkinan pencarian karakter tinggal dua puluh enam karakter dikurangi satu karakter yang sudah terpakai pada teks-cipher, menyisakan kemungkinan dua puluh lima karakter dari karakter-karakter yang terdapat pada satu irisan silinder di Disk Jefferson. Kondisi ini dapat diperhitungkan sebagai:

$25 \times 25 \times 25 \times \ldots$ sebanyak n jumlah perkalian

Atau dengan menggunakan gambaran matematis lain yaitu:

$$f(\text{exhaustive search}) = 25^n$$

Sayang sekali teknik Exhaustive Search ini tidak dapat diterapkan untuk mencari kemunculan satu persatu karakter, karena akan ada banyak sekali kemungkinan kalimat yang mungkin. Jadi teknik ini digunakan untuk mencari tahu urutan irisan silinder yang digunakan, apabila irisan-irisan tersebut dipakai secara acak untuk melakukan enkripsi. Untuk mencari tahu urutan ini dapat dilakukan dengan menggunakan *Exhaustive Search* permutasi matematis berikut ini:.

$$\frac{P(\text{jumlah karakter total})}{n_1!n_2!\ldots n_i!}$$

Dimana n adaah jumlah kemunculan satu karakter berulang.

Dengan kecanggihan teknologi komputasi saat ini, proses *Exhaustive Search* tersebut dapat dilakukan relatif cepat dengan bantuan komputer yang berkemampuan tinggi. Kecepatan pencarian dengan menggunakan *Exhaustive Search* masih dapat ditingkatkan lagi apabila proses tersebut dilakukan secara paralel dengan banyak komputer bersamaan. Dengan kata lain tingkat keamanan Cipher Jefferson untuk pemakaian saat ini tidak bagus dan Cipher Jefferson sebaiknya tidak diterapkan di masa ini.

Sayangnya teknik *Exhaustive Search* dengan teknologi tinggi seperti dijelaskan di atas tidak dapat diterapkan pada masa pemakaian yang sebenarnya, yaitu sekitar abad kedelapan belas. Pada saat itu belum ada teknik komputasi sehebat ini, sehingga pencarian dengan teknik *Exhaustive Search* saat itu belum memungkinkan diterapkan secara memuaskan untuk mencari teks-plain dari teks-cipher yang disadap. *Exhaustive Search* dianggap tidak *feasible* untuk dipakai mendeskripsikan pesan dari teks-cipher. Jadi pada masa itu Cipher Jefferson dapat dianggap memiliki tingkat keamanan tinggi untuk dipakai dalam melakukan enkripsi sebelum pengiriman pesan.

5.2. Analisis Frekuensi

Teknik analisis frekuensi juga dapat diterapkan untuk membongkar teks-plain dari teks-cipher menggunakan Cipher Jefferson. Tetapi meskipun menggunakan teknik ini, tetap saja sulit bagi penyadap untuk melakukan dekripsi paksa terhadap teks-cipher yang sudah didapat.

Teknik analisis frekuensi adalah teknik yang menggunakan konsep keseringan atau kekerapan penggunaan huruf dalam satu bahasa. Teknik analisis frekuensi ini harus didukung dengan data hasil analisis kemunculan huruf, biasanya merupakan hasil riset terhadap seringnya kemunculan huruf-huruf tertentu dari media.

Ada syarat tertentu untuk memungkinkan penyadap menggunakan teknik analisis frekuensi pada teks-cipher dengan Cipher Jefferson. Syarat tersebut adalah bahwa teks-cipher harus sangat panjang, yang mengakibatkan proses enkripsi membutuhkan pesan yang harus dipecah menjadi fragmen-fragmen yang banyak jumlahnya. Jika teks-plain yang panjang dienkripsi melalui proses pemecahan fragmen-fragmen, maka kemungkinan kemunculan huruf yang sama dari Disk Jefferson menjadi tinggi. Semakin panjang teks-plain, maka semakin banyak fragmen yang dihasilkan, mengakibatkan semakin tinggi kemungkinan kemunculan huruf berulang pada teks-cipher. Kondisi inilah yang dapat dimanfaatkan dengan menggunakan teknik analisis frekuensi.

Teknik analisis frekuensi yang dilakukan adalah teknik analisis frekuensi biasa, yang secara umum menghitung kemunculan setiap karakter pada teks-cipher, kemudian membandingkannya dengan hasil analisis kemunculan karakter pada suatu bahasa tertentu. Selanjutnya penyadap mencoba menyubstitusikan karakter-karakter tersebut diikuti dengan menebak-nebak kalimat yang cocok sampai akhirnya menemukan teks-plain yang dirasa sesuai.

Lebih detail, Langakah pertama dekripsi teks-cipher dengan Cipher Jefferson dengan teknik analisis frekuensi adalah menghitung satu persatu jumlah kemunculan setiap karakter yang ada pada teks-cipher. Jumlah kemunculan setiap karakter kemudian dicatat sampai kedua puluh enam karakter selesai dihitung. Untuk saat ini proses tersebut dapat dilakukan memanfaatkan teknik komputasi menggunakan aplikasi tertentu dengan waktu relatif singkat. Akan tetapi pada masa pemakaian Cipher Jefferson dulu, proses ini memakan waktu lama karena dilakukan secara manual, terlebih lagi apabila teks-cipher yang dihitung kemunculan karakternya merupakan teks panjang. Apalagi saat itu ilmu statistika belum berkembang seperti kondisi saat ini.

Langkah berikutnya adalah mengurutkan tingkat jumlah kemunculan karakter pada teks-cipher hasil perhitungan. Sebaiknya pengurutan dimulai dari karakter yang memiliki jumlah kemunculan terbanyak, kemunculan kedua terbanyak, dan seterusnya sampai pada karakter yang memiliki tingkat jumlah kemunculan terkecil pada teks-cipher. Langkah ini sebenarnya tidak wajib dilakukan, namun bila dilakukan akan lebih mempermudah langkah berikutnya yang akan dijalani.

Ketiga, penyadap harus membandingkan jumlah penghitungan kemunculan karakter dari teks-cipher dengan data statistik kemunculan karakter berasal dari hasil riset. Penyadap mencocokkan karakter yang paling sering muncul pada teks-cipher dengan karaker dengan tingkat kemunculan tertinggi hasil riset, diikuti dengan mencocokkan karakter dengan jumlah kemunculan kedua tertinggi di teks-cipher dengan karakter hasil riset dengan tingkat kemunculan tertinggi kedua, dan seterusnya sampai karakter dengan tingkat kemunculan terendah. Dengan kata lain, jika langkah kedua sudah dijalankan tinggal mencocokkan saja karakter-karakternya sesuai urutan teratas hingga yang paling bawah dari hasil penghitungan dan hasil riset.

Langkah selanjutnya, keempat, yaitu mencoba menyubstitusikan satu persatu karakter-karakternya dimulai dari yang paling sering muncul. Semakin sering muncul, semakin besar kemungkinan bahwa karakter tersebut merupakan karakter yang tepat untuk disubstitusikan. Sebaiknya langkah ini dilakukan bertahap sambil menganalisis apakah proses substitusi karakter tersebut sudah tepat. Seringkali substitusi yang dilakukan tidak sesuai dan tidak menghasilkan karakter teks-plain yang sesuai. Jika terjadi seperti itu maka yang dapat dilakukan adalah mengulangi proses substitusi ke titik dimana substitusi karakter tidak tepat. Biasanya proses ini dilengkapi dengan menebak-nebak kalimat teks-plain yang cocok dari beberapa substitusi karakternya. Maka dari itu, sebenarnya langkah ini merupakan langkah yang paling sulit dan menghabiskan banyak tenaga dan waktu untuk dikerjakan.

Dengan langkah sebelumnya seharusnya pihak penyadap sudah dapat menemukan teks-plain yang sesuai. Langkah terakhir ialah tinggal merapikan teks-plain agar pesan yang disampaikan dapat terbaca dengan baik. Maka dengan itu selesailah langkah dekripsi paksa dengan menggunakan teknik analisis frekuensi kemunculan karakter.

Ada kondisi khusus pada Cipher Jefferson, yaitu jika urutan penyusunan karakter tidak diketahui. Apabila kondisi tersebut benar-benar terjadi, maka teknik analisis frekuensi tidak dapat digunakan sempurna, sebab proses menebak-nebak kalimat yang sesuai dari karakter-karakter yang sudah terbuka akan menjadi sangat sulit dilakukan.

5.3. Perbandingan Teknik Dekripsi Cipher Jefferson

Teknik analisis frekuensi jika dilakukan manual seharusnya akan memberikan waktu pencapaian hasil yang lebih singkat jika dibandingkan dengan penggunaan *Exhaustive Search* secara manual. Analisis frekuensi dianggap lebih mangkus dan sangkil dalam mencari hasil dekripsi Cipher Jefferson dibandingkan metode *Exhaustive Search*.

Akan tetapi dengan kondisi karakter-karakter teks-cipher tidak berurut, kedua teknik ini akan

sangat berbeda jauh ketika dibandingkan. Teknik analisis frekuensi menjadi sangat tidak mangkus dan sangkil sebagai teknik dekripsi, sementara teknik *Exhaustive Search* memang digunakan pada kondisi ini.

5.4. Kesimpulan Analisis Keamanan

Kedua teknik yang dibahas di atas membuktikan bahwa teknik Cipher Jefferson dapat dibongkar juga, sama seperti hampir semua teknik kriptografi lainnya. Namun karena kedua teknik ini belum berkembang pesat pada masa pemakaian Cipher Jefferson, ditambah juga belum adanya sistem komputasi modern seperti saat ini, mengakibatkan Cipher Jefferson diakui kuat dan aman dipakai pada masanya. Belum ada catatan sejarah sampai saat ini bahwa Cipher Jefferson pernah diserang dan berhasil dibongkar oleh pihak yang tidak seharusnya pada masa pemakaiannya itu.

Untuk pesan yang berukuran pendek, Cipher Jefferson sangat aman untuk diterapkan. Namun jika pesan yang dikirimkan berukuran panjang tetapi dengan posisi karakter berurutan rapi, pengirim harus berhati-hati dengan penyadap yang menggunakan teknik analisis frekuensi. Kekhawatiran penggunaan *Exhaustive Search* ada jika penyadap memiliki Disk Jefferson yang sama tetapi tidak memiliki kunci urutan posisi irisan silinder.

Untuk saat ini, pembongkaran Cipher Jefferson dapat dilakukan dengan relatif cepat dan mudah dengan bantuan teknik komputasi modern menggunakan komputer dan dilakukan secara paralel, banyak mesin bersamaan.

6. Kelebihan dan Kekurangan Cipher Jefferson

6.1. Kelebihan Cipher Jefferson

Kelebihan utama Cipher Jefferson adalah pemakaian alat enkripsi dan dekripsi yang khas dinamai Disk Jefferson. Meskipun sederhana, alat ini terbukti ampuh dan aman dalam mengenkripsi pesan dalam teks-plain menjadi teks-cipher. Mirip dengan One-Time Pad, alat ini juga hanya boleh dimiliki pihak pengirim dan penerima, dan kedua belah pihak memiliki alat yang identik. Selain kedua pihak tersebut tidak ada orang lain yang bisa memiliki Disk Jefferson serupa. Hal ini mengakibatkan tingkat kerahasiaan pesan tinggi karena hanya dapat didekripsi menggunakan Disk Jefferson yang sama.

Jika sampai Disk Jefferson jatuh ke tangan orang yang tidak seharusnya, maka salah satu cara yang dapat dilakukan untuk menjaga keamanannya adalah tidak menggunakan Disk Jefferson yang sama untuk mengenkripsi pesan dengan tujuan menghindari kemungkinan pesan jatuh ke tangan pihak yang tidak berhak dan berhasil mengambil informasi penting menggunakan alat yang sama.

Kelebihan lainnya adalah kemudahan untuk mengimplementasikan Cipher Jefferson. Dengan menggunakan Disk Jefferson hampir semua orang langsung bisa membentuk teks-ciphernya masing-masing. Tidak perlu waktu lama untuk dapat menggunakan Disk Jefferson dan mempelajari teknik ciphernya.

6.2. Kekurangan Cipher Jefferson

Kekurangan pertama penggunaan Cipher Jefferson adalah bahwa setiap calon penerima pesan harus memiliki Disk Jefferson yang identik dengan Disk Jefferson yang dimiliki oleh pengirimnya. Bisa terbayang repotnya mendistribusikan Disk Jefferson kepada semua calon penerima pesan, terlebih lagi bila calon penerima pesan berjumlah banyak. Hal ini masih bisa diperparah apabila setiap penerima pesan harus memiliki Disk Jefferson yang berbeda-beda, sehingga pesan yang tepat hanya bisa dibuka oleh orang yang sesuai. Kondisi ini menyebabkan pihak pengirim akan memiliki banayk Disk Jefferson yang berbeda-beda untuk mengirim pesan dengan tujuan yang berbeda-beda. Ini akan sangat merepotkan pengirim dan penerima pesan.

Pada masa pemakaian Cipher Jefferson, fasilitas transportasi dan komunikasi masih buruk, sehingga kekurangan di atas sangat terasa. Hal inilah yang menyebabkan masa pemakaian Cipher Jefferson terbilang singkat, sebab Thomas Jefferson sendiri merasa kerepotan untuk mendistribusikan alat ciptaannya itu. Thomas Jefferson akhirnya lebih memilih menggunakan teknik kriptografi tertulis untuk mengirimkan pesan karena dianggap lebih sederhana.

Kekurangan lain adalah kemajuan teknologi komputasi saat ini mengakibatkan tenik enkripsi menggunakan Cipher Jefferson ini mudah dan

dapat dengan cepat dibongkar oleh pihak yang tidak seharusnya.

6.3. Kesimpulan Kelebihan dan Kekurangan Cipher Jefferson

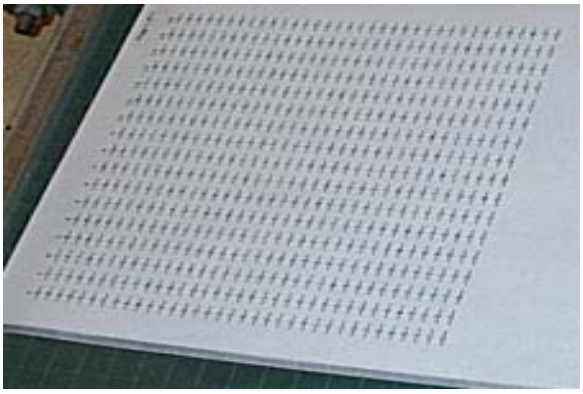
Dari pembahasan kelebihan dan kekurangan di atas, terlihat bahwa untuk penggunaan kalangan terbatas, Cipher Jefferson sangat layak dipakai sebagai teknik enkripsi dan dekripsi dalam pengiriman pesan. Tingkat keamanan tinggi didukung dengan kemudahan implementasi merupakan nilai lebih penggunaan Cipher Jefferson dibandingkan teknik kriptografi lainnya.

Untuk penggunaan secara luas, sebaiknya Cipher Jefferson tidak dipakai sebab kebutuhan dan kebergantungan terhadap Disk Jefferson akan merepotkan dan membingungkan pengirim dan penerima pesan. Selain itu pengaruh kemajuan teknologi komputasi menjadi keuntungan untuk penyadap dan penyerang untuk membongkar pesan terenkripsi.

7. Membuat Replika Disk Jefferson Sederhana

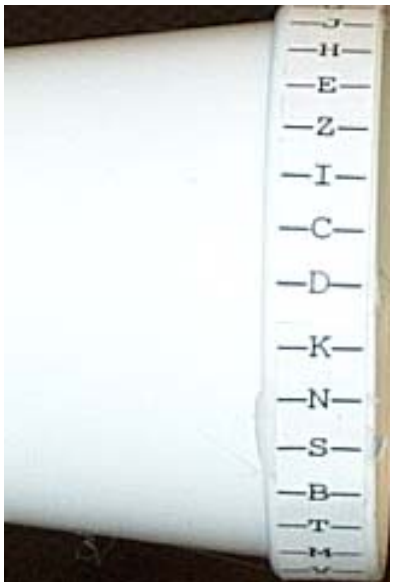
Topik terakhir yang akan dibahas adalah langkah-langkah membuat replika Disk Jefferson secara sederhana. Pembuatan replika yang akan dilakukan tidak sulit dan hanya membutuhkan waktu singkat. Alat dan bahan yang diperlukan pun tidak sulit didapat, yaitu sejumlah gelas plastik, kertas kosong, alat tulis, lem kertas, dan gunting. Untuk lebih lengkapnya langkah-langkah ini dapat dilihat pada situs http://www3.brinkster.com/Redline/jefferson.asp

Langkah pertama adalah menulisi kertas dengan karakter-karakter alfabet secara acak dalam bentuk kolom-kolom. Penulisan tersebut dibuat sejumlah yang diinginkan, semakin banyak maka semakin panjang teks-plain yang dapat dipetakan ke dalam teks-cipher dalam satu waktu, sehingga menurunkan kemungkinan terjadinya pemecahan pesan menjadi fragmen-fragmen. Penulisan ini bertujuan untuk membuat satu permukaan irisan disk pada replika Disk Jefferson. Contoh penulisan pada irisan-irisan silider, dipetakan pada kertas kosong dapat dilihat pada gambar sebagai berikut:

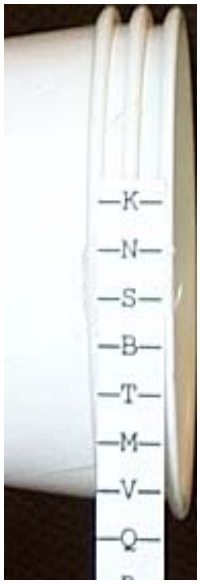


Berikutnya kertas berisi kolom-kolom karakter acak tadi digunting menurut kolom-kolomnya. Selanjutnya setiap hasil guntingan tadi ditempelkan pada gelas plastik secara melingkar di permukaan sisinya. Satu penempelan ini dianggap sebagai satu buah irisan silinder pada Disk Jefferson. Gambar berikut adalah gambar guntingan kertas memanjang sesuai kolom-kolom berisi karakter-karakter alfabet teracak. Yang perlu diperhatikan adalah posisi penempelan kertas pada gelas plastik. Proses ini dikerjakan sebanyak yang diinginkan.

Langkah selanjutnya adalah menyusun gelas platik untuk dapat ditempeli dengan potongan-potongan kertas seperti pada gambar di atas. Penyusunan gelas plastik tidak memerlukan aturan khusus, cukup dilakukan sesuai selera masing-masing.



Berikutnya adalah menempelkan satu persatu potongan kertas pada gelas plastik secara melingkar. Terlihat pada gambar adalah satu potongan kertas bertuliskan karakter acak ditempelkan pada tiga buah gelas plastik yang dirapatkan satu sama lain menggunakan lem. Hal tersebut dimaksudkan agar permukaan kertas dapat menempel dengan sempurna pada ujung tiga buah gelas plastik tersebut.



Selanjutnya langkah terakhir ialah menyatukan semua gelas plastik yang sudah ditempeli dengan potongan kertas sebanyak yang dikehendaki. Caranya dengan menumpukkan saja gelas-gelas bertempelkan kertas tersebut tanpa menggunakan lem. Hasil dari penggabungan semua gelas plastik dapat dilihat pada gambar sebagai berikut:

Perlu diingat juga bahwa tidak perlu memberikan lem saat menyatukan gelas plastik. Hal ini dimaksudkan agar gelas plastik dapat dirotasi sebagai proses enkripsi dan dekripsi.

Dengan berakhirnya langkah di atas, maka berakhir juga proses pembuatan replika Disk Jefferson. Seperti sudah dijelaskan di awal bahwa pembuatan replika ini mudah dan cepat, namun bisa mewakili penggunaan Disk Jefferson sebenarnya untuk melakukan proses enkripsi dan dekripsi sederhana.

5. Kesimpulan

Dari pembahasan terhadap Cipher Jefferson di atas, dapat diambil beberapa kesimpulan singkat, yaitu:

1. Cipher Jefferson merupakan salah satu teknik kriptologi klasik terbaik. Cipher Jefferson memiliki beberapa kelebihan unik dibandingkan jenis cipher klasik lain.

2. Cipher Jefferson memiliki konsep enkripsi dan dekripsi yang relatif mudah dimplementasikan sebagai sarana pengiriman pesan yang aman.

3. Cipher Jefferson sangat bergantung kepada Disk Jefferson untuk melakukan enkripsi dan dekripsinya. Tanpa Disk Jefferson, proses enkripsi dan dekripsi pesan tidak dapat dilakukan.

4. Cipher Jefferson pada masa pemakaiannya memiliki tingkat keamanan yang tinggi untuk dipakai mengirim pesan-pesan terenkripsi.

5. Tidak ada teknik yang benar-benar mangkus untuk dapat membongkar teks-cipher yang dihasilkan Cipher Jefferson. Teknik yang mungkin digunakan adalah *Exhaustive Search* dan Analisis Frekuensi, namun terbatas pada kondisi-kondisi enkripsi tertentu.

6. Perbandingan kelebihan dan kekurangan Cipher Jefferson seimbang bergantung luasnya pemakaian teknik Cipher Jefferson. Pada tingkat luas pemakaian tertentu, Cipher Jefferson masih layak dipakai sebagai salah satu teknik mengenkripsi dan mendekripsi pesan.

7. Kesalahan pada proses enkripsi dan dekripsi sangat kecil kemungkinannya untuk terjadi, namun seandainya kejadian tersebut muncul tidak akan berpengaruh banyak pada Cipher Jefferson.

8. Dengan kemajuan teknologi komputasi saat ini , tidak disarankan untuk memakai teknik Cipher Jefferson sebagai teknik kriptografi dalam pengiriman pesan.

9. Disk Jefferson dapat dibuat replikanya secara sederhana. Replika ini layak mewakili fungsionalitas kerja Disk Jefferson sebenarnya.

DAFTAR PUSTAKA

Buku Acuan

Munir, Rinaldi. 2004. *Bahan Kuliah IF5054 Kriptografi*. Departemen Teknik Informatika, Institut Teknologi Bandung.

Situs Acuan

http://en.wikipedia.org/wiki/Bazeries_cylinder
Tanggal akses: 11 September 2006 pukul 13.00.

http://en.wikipedia.org/wiki/Thomas_Jefferson
Tanggal akses: 11 September 2006 pukul 13.00.

http://en.wikipedia.org/wiki/Etienne_Bazeries
Tanggal akses: 11 September 2006 pukul 13.00.

http://www.vectorsite.net/ttcode.html
Tanggal akses: 11 September 2006 pukul 13.00.

http://commons.wikimedia.org/wiki/Jefferson_Disk
Tanggal akses: 11 September 2006 pukul 13.00.

http://en.wikipedia.org/wiki/M-94
Tanggal akses: 11 September 2006 pukul 13.00.

http://en.wikipedia.org/wiki/Codebreaking
Tanggal akses: 11 September 2006 pukul 13.00.

http://www.monticello.org/reports/interests/wheel_cipher.html
Tanggal akses: 11 September 2006 pukul 13.00.

http://en.wikipedia.org/wiki/History_of_cryptography
Tanggal akses: 11 September 2006 pukul 13.00.

http://library.thinkquest.org/04oct/00451/president.htm
Tanggal akses: 11 September 2006 pukul 13.00.

http://www.lewis-clark.org/content/content-article.asp?ArticleID=2224
Tanggal akses: 11 September 2006 pukul 13.00.

http://www.lewis-clark.org/content/content-article.asp?ArticleID=2222
Tanggal akses: 11 September 2006 pukul 13.00.

http://library.thinkquest.org/28005/flashed/timemachine/courseofhistory/jefferson.shtml
Tanggal akses: 11 September 2006 pukul 13.00.

http://www3.brinkster.com/Redline/crypt.asp
Tanggal akses: 15 September 2006 pukul 10.00.

http://www3.brinkster.com/Redline/jefferson.asp
Tanggal akses: 15 September 2006 pukul 10.00.

http://www.nsa.gov/museum/museu00013.cfm
Tanggal akses: 15 September 2006 pukul 10.00.

http://library.thinkquest.org/27158/concept1_14.html
Tanggal akses: 15 September 2006 pukul 10.00.

http://library.thinkquest.org/27158/concept1_5.html
Tanggal akses: 15 September 2006 pukul 10.00.

Gambar Acuan

http://library.thinkquest.org/04oct/00451/president.htm
Tanggal akses: 11 September 2006 pukul 13.00.

http://www3.brinkster.com/Redline/jefferson.asp
Tanggal akses: 15 September 2006 pukul 10.00.

http://www.nsa.gov/museum/museu00013.cfm
Tanggal akses: 15 September 2006 pukul 10.00.