Wheel Cipher dan Perkembangannya

Marianti Putri Wulandari – 13503093

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl Ganesha No 10, Bandung
Email : if13093@students.if.itb.ac.id

Abstraksi

Wheel Cipher merupakan salah satu alat yang digunakan untuk melakukan enkripsi dan dekripsi suatu pesan. Dasar dari metode ini telah ditemukan pada abad ke-15 oleh Leo Battista Alberti. Kemudian metode ini dikembangkan menjadi alat enkripsi dan dekripsi hingga saat ini.

Metode wheel cipher telah dikembangkan ulang oleh Thomas Jefferson yang kemudian dinamakan Jefferson Wheel Cipher. Kemudian dikembangkan lagi oleh Bazeries yang kemudian dinamakan Bazeries Cylinder. Kemudian dikembangkan menjadi M94, dan versi-versi setelahnya.

Algoritma kriptografi yang digunakan dapat dikatakan aman karena menghasilkan kemungkinan solusi yang banyak. Selain itu, alat ini fleksibel dalam penggunaannya sehingga memungkinkan terjadinya perubahan-perubahan untuk mencegah terjadinya *code breaking*.

Namun metode ini telah berhasil dipecahkan pada tahun 1893 oleh DeViaris. Walaupun sudah terdapat cara pemecahan kode, metode ini tetap dikembangkan dan dianggap masih aman digunakan untuk kasus-kasus tertentu.

Kata Kunci : Wheel Cipher, Jefferson Wheel Cipher, Bazeries Cylinder, M94

I. Pendahuluan

a. Latar Belakang

Di bidang kriptografi, terdapat banyak metode yang digunakan untuk mengenkripsi dan mendekripsi suatu pesan. Untuk mempermudah penggunaan metode untuk enkripsi dan dekripsi, dapat digunakan media khusus. Contohnya adalah media wheel cipher.

Wheel cipher merupakan suatu media khusus untuk melakukan suatu metode enkripsi dan dekripsi. Metode dengan menggunakan media wheel cipher telah ditemukan pada abad ke-15 oleh Leo Battista Alberti. Media ini kemudian dianggap aman hingga dikembangkan dan digunakan hingga saat ini.

b. Perumusan Masalah

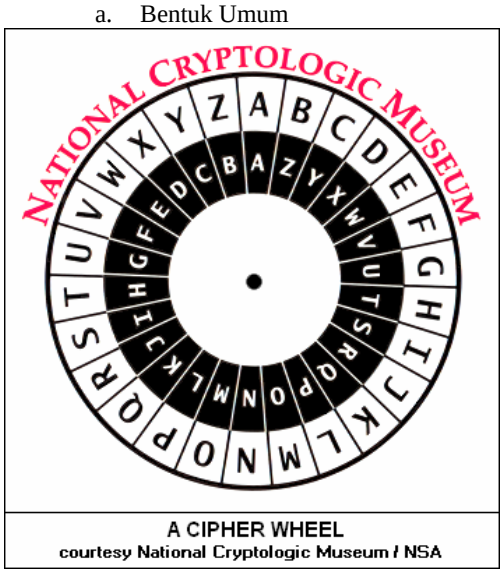
Dalam makalah ini akan dijelaskan mengenai metode wheel cipher pertama kali (cipher disk) dan perkem-bangannya, bagaimana karakteristik dan cara kerjanya, apa kelemahan dan kelebihan dari metode ini. Kemudian akan dijelaskan studi kasus menggunakan wheel cipher ini dan cara kriptanalisisnya. Setelah dilihat cara penggunaan dan cara kriptanalisisnya, akan dijelaskan bagaimana cara pengembangan metode wheel cipher ini agar menjadi lebih baik dan lebih aman untuk digunakan.

c. Batasan Masalah

Batasan dalam makalah ini adalah bahwa perkembangan metode wheel cipher hanya dilihat dari Jefferson Wheel Cipher, Bazeries Cylinder dan M94, karena perkembangan dari wheel cipher yang ada cukup banyak dan perubahan yang terjadi tidak terlalu signifikan.

II. Cipher Disk (Wheel Cipher)

a. Bentuk Umum



Gambar I Cipher Disk

Bentuk dari wheel cipher, yang pada saat itu masih dikenal sebagai cipher disk, saat ditemukan pertama kali oleh Leon Alberti terdiri dari dua buah potongan silinder, yaitu potongan silinder dalam dan potongan silinder luar. Masing-masing potongan silinder memiliki label seluruh alfabet, dengan susunan yang tidak harus terurut dan sama. Potongan silinder luar merupakan alfabet untuk plainteks, dan Potongan silinder dalam merupakan alfabet untuk cipherteks dengan metode monoalphabetic substitution cipher alphabet, yaitu metode enkripsi dengan satu karakter di plainteks diganti dengan satu karakter yang bersesuaian, atau fungsi satu-ke-satu.

b. Cara Kerja

Cipher disk pada saat itu digunakan sebagai media untuk membantu enkripsi dan dekripsi pesan dengan algoritma Vigenere. Sebagai contoh, pihak pengirim ingin mengenkripsi suatu pesan menggunakan Vigenere cipher dengan kunci “WARTHOG”.

Untuk mengenkripsi huruf pertama, pihak pengirim memutar “W” di potongan silindris dalam hingga berdampingan dengan “a” di potongan silindris luar. Kemudian cari huruf cipherteks di potongan silindris dalam yang cocok dengan huruf plainteks yang diinginkan di potongan silindris luar.

Selanjutnya, pihak pengirim mengenkripsi huruf kedua dengan memutar “A” di potongan silindris dalam hingga berdampingan dengan “a” di potongan silindris luar. Kemudian cari huruf cipherteks di potongan silindris dalam yang cocok dengan huruf plainteks yang diinginkan di potongan silindris luar.

Untuk seterusnya, ulang proses untuk huruf “R”, “T”, “H”, “O”, “G”, dan kemudian diulang lagi dari “W” hingga seluruh pesan telah terenkripsi.

III. Variasi Wheel Cipher

a. Bentuk Umum

Gambar II Jefferson Wheel Cipher

Bentuk dari wheel cipher sejak versi Jefferson Wheel Cipher hingga versi M94 terdiri dari sejumlah potongan silindris yang tersusun di suatu sumbu besi. Setiap potongan silindris memiliki susunan alfabet secara acak di bagian luar. Potongan-potongan silindris dapat diubah susunannya dengan melepas potongan silindris dari sumbunya dan kemudian dipasang kembali sesuai dengan susunan yang diinginkan.

Susunan dari potongan-potongan silindris tersebut akan menjadi kunci dalam mengenkripsi dan mendekripsi pesan dari pihak penerima dan pihak pengirim. Setiap potongan silindris dapat diputar untuk menyusun alfabet-alfabet menjadi cipherteks ataupun menjadi plainteks.

b. Cara Kerja

Untuk mengenkripsi suatu pesan, pihak pengirim harus menyusun potongan silindris sesuai dengan

kunci yang telah disepakati dengan pihak penerima. Kemudian pihak pengirim dapat memutar potongan-potongan silindris untuk menghasilkan plainteks di suatu baris alfabet. Setelah itu, pihak pengirim memilih baris selain baris plainteks sebagai cipherteks.

Untuk mendekripsi suatu pesan, pihak penerima juga harus menyusun potongan silindris sesuai dengna kunci yang telah disepakati dengan pihak pengirim. Kemudian pihak penerima dapat memutar potongan-potongan silindris untuk menghasilkan baris alphabet cipherteks. Setelah itu, pihak penerima dapat mencari baris selain baris cipherteks sebagai plainteks.

c. Analisis Algoritma

Karena memiliki kunci enkripsi yang sama dengan kunci dekripsi, maka metode enkripsi dan dekripsi pesan ini termasuk dalam algoritma kriptografi simetri (symmetric-key cryptography). Yang dimaksud dengan algoritma kriptografi simetri adalah suatu algoritma kriptografi yang memiliki kunci enkripsi yang sama dengan kunci dekripsi.

Jumlah kemungkinan susunan kunci untuk suatu wheel cipher bergantung pada jumlah potongan silindris yang digunakan. Jika jumlah potongan silindris sebesar n, maka jumlah kemungkinan susunan kunci adalah jumlah permutasi dari n, yaitu n!

Jumlah kemungkinan susunan baris juga bergantung pada jumlah potongan silindris yang digunakan. Jika alphabet yang terdapat di setiap potongan silindris sebesar m, maka jumlah kemungkinan susunan baris adalah n^m.

Dalam metode ini dihasilkan selisih baris antara baris plainteks dengan baris cipherteks yang selalu sama untuk setiap potongan silindris. Hal ini merupakan suatu konsep yang dapat digunakan dalam melakukan kriptanalisis (akan dijelaskan lebih lanjut di bab Kriptanalisis)

Dengan metode ini, saat melakukan dekripsi terdapat kemungkinan ada dua baris yang berisi teks bernakna. Jika hal ini terjadi, maka pihak penerima dapat memilih baris yang paling mungkin menjadi plainteks.

d. Kelebihan

Kelebihan yang pertama dari wheel cipher adalah bahwa wheel cipher adalah alat cipher yang cukup aman, mengingat besarnya jumlah kemungkinan susunan kunci, dan jumlah kemungkinan susunan baris. Pada zaman Jefferson dan Bazeries, kemungkinan solusi sebanyak permutasi dari potongan silindris tidak dapat didapatkan dengan cara perhitungan manual. Oleh karena itu, pada zaman tersebut metode ini dianggap aman.

Kelebihan yang kedua adalah wheel cipher tidak membutuhkan banyak teknologi canggih. Wheel cipher dapat dibuat secara sederhana (misalnya dengan menggunakan kaleng dan gulungan kertas) tanpa mengurangi fungsionalitasnya.

e. Kelemahan

Kelemahan yang pertama adalah bahwa seluruh cetakan mesin harus dibuat dan dikirimkan ke pihak-pihak yang mungkin akan menerima pesan rahasia. Pada zaman Thomas Jefferson, hal ini menjadi kendala utama dalam penggunaan wheel cipher, karena pada saat itu transportasi masih sulit, dan keamanan dari pengiriman wheel cipher dan kunci masih kurang.

Kelemahan yang kedua adalah selisih baris antara baris plainteks dengan baris cipherteks selalu sama, sehingga memudahkan proses kriptanalisis dalam memecahkan kunci wheel cipher. Selisih yang sama akan membantu proses perbandingan susunan alphabet untuk mencari susunan kunci.

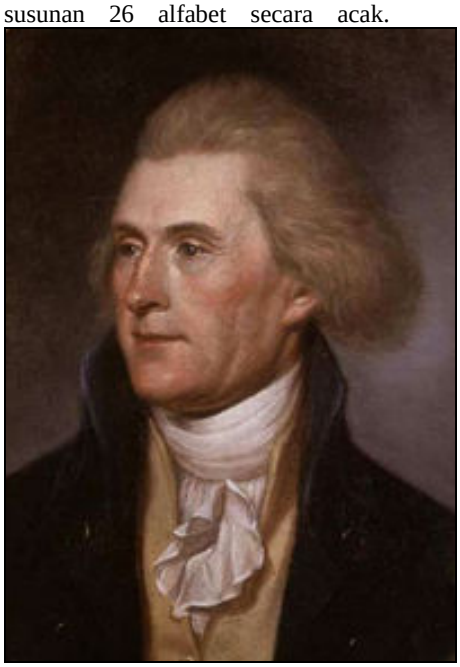
Kelemahan ketiga adalah satu kunci wheel cipher dapat digunakan untuk mengirimkan pesan lebih dari satu kali. Jika seorang kriptanalis berhasil memecahkan kunci wheel cipher, maka kunci tersebut harus

diubah saat mengirimkan pesan selanjutnya untuk mencegah diketahuinya pesan oleh kriptanalis. Pengubahan kunci wheel cipher memerlukan usaha yang besar mengingat perubahan kunci harus diketahui oleh seluruh pihak yang mungkin mengirim atau menerima pesan.

f. Jefferson Wheel Cipher

Thomas Jefferson, lahir pada tanggal 13 April 1743, adalah presiden ketiga Amerika Serikat di masa pemerintahan tahun 1801 hingga tahun 1809. Di samping karir di bidang politik, Jefferson adalah seorang tuan tanah, horticulturist, arsitek, arkeologis, paleontologist, pengarang buku, pemain biola dan penemu. Salah satu penemuan Thomas Jefferson di bidang kriptografi adalah sebuah wheel cipher,yang kemudian dinamakan Jefferson Wheel Cipher. Beliau meninggal pada tanggal 4 Juli 1826.

Karakteristik dari Jefferson Wheel Cipher terdiri dari 26 potongan roda kayu silindris kecil, masing-masing tersusun dalam sebuah sumbu besi. Setiap potongan kayu memiliki susunan 26 alfabet secara acak.



Gambar III Thomas Jefferson

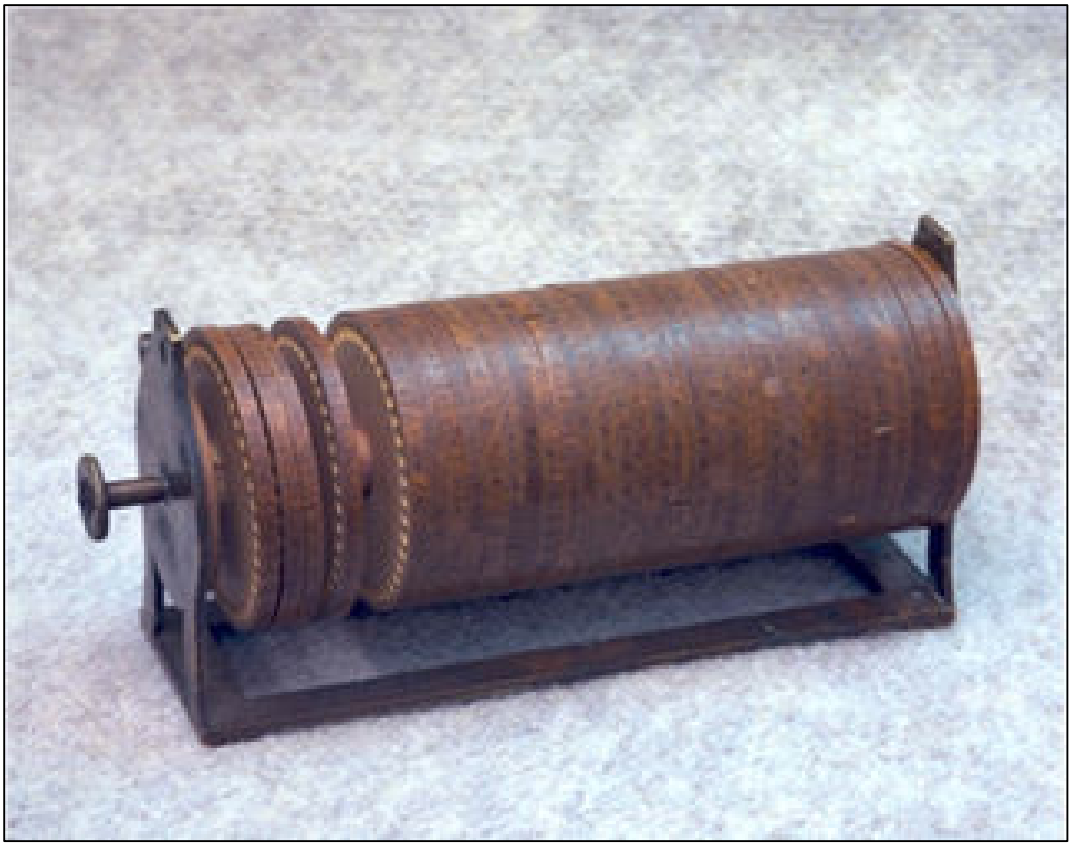
Saat Revolusi Amerika, Jefferson menggunakan jasa kurir untuk menyampaikan surat atau pesan penting. Pada saat beliau menjadi menteri Amerika dan berada dalam upaya membina hubungan dengan Perancis, pengkodean suatu pesan menjadi hal penting karena timbulnya kekhawatiran akan dibacanya pesan tersebut oleh orang yang tidak berkepentingan. Lalu saat Jefferson menjadi sekretaris George Washington pada kurun waktu tahun 1790 hingga 1793, Jefferson mengembangkan suatu metode penyembunyian pesan yang aman dengan menggunakan alat wheel cipher untuk sistem enkripsi dan dekripsi pesan.

Metode ini relatif tidak terlalu terkenal dan digunakan secara luas. Thomas Jefferson menggunakan metode ini sejak tahun 1790 hingga tahun 1802. Setelah periode tersebut, Jefferson mulai tertarik untuk mengganti wheel cipher dalam menyembunyikan pesan. Beliau menemukan bahwa metode Vigenere Cipher lebih mudah digunakan daripada Thomas Jefferson Aplication.

g. Bazeries Cylinder

Gambar IV Eitenne Bazeries

Gambar V Jefferson Wheel Cipher



Gambar VI Bazeries Cylinder

Etienne Bazeries, lahir pada tanggal 21 Agustus 1846 di Port-Vendres di Perancis, adalah seorang kriptanalis di bidang militer dari Negara Perancis. Beliau aktif sejak tahun 1890 hingga saat Perang Dunia pertama.

Ketertarikan Bazeries di bidang kriptografi diawali dari penyelesaian kriptogram di koran. Kemampuan kriptanalisisnya kemudian diterapkan dalam konteks militer, yaitu pada tahun 1890 saat beliau memecahkan cipherteks dengan sistem transposisi kemiliteran resmi Perancis, yang menyebabkan kementerian perang mengubah strateginya. Karirnya di bidang kriptanalisis berkembang dan beliau kemudian bekerja di kementerian, dan di masa Perang Dunia pertama beliau membantu dalam memecahkan cipherteks militer Jerman.

Bazeries Cylinder memiliki bentuk yang hampir sama dengan Jefferson Wheel Cipher. Perbedaannya terletak di komponen-komponennya secara teknis. Jumlah potongan silindris tidak terbatas hanya 26 buah. Jumlahnya dapat ditambah ataupun dikurangi.

Jefferson Wheel Cipher tidak terlalu terkenal dan tidak digunakan secara luas. Lalu Commandant Etienne Bazeries mengembangkan kembali seabad kemudian menjadi Bazeries Cylinder.

h. M-94

M94 merupakan perkembangan dari Bazeries Cylinder yang ditujukan oleh Amerika Serikat sebagai media komunikasi kemiliteran pada tahun 1923 hingga 1942. Selain itu, M94 juga digunakan oleh Coast Guard dan Radio Intelligence Division of the Federal Communications Commission hingga awal Perang Dunia kedua. Setelah itu, M94 dikembangkan lagi menjadi M-138-A.

M94 juga memiliki bentuk yang hampir sama dengan Jefferson Wheel Cipher. Perbedaannya adalah M94 terbuat dari alumunium. Untuk potongan ke 17, susunan alfabetnya berupa ARMYOFTHEUSZJXDPCWGQIBKLNV. Susunan ARMYOFTHEUS menunjukkan “Army Origin of the M94”.

Gambar M94

M94 memiliki 100 pilihan potongan silindris, walaupun yang akan dipilih untuk digunakan dalam suatu kunci hanya sebanyak 25 buah saja. Hal ini dapat memperbanyak kemungkinan solusi dari kunci wheel cipher.

IV. Studi Kasus

Di bab ini akan dijelaskan tentang contoh kasus penggunaan Wheel Cipher dalam mengenkripsi dan mendekripsi suatu pesan. Untuk kasus ini, potongan silindris yang digunakan berjumlah sepuluh buah. Setiap potongan silindris memiliki indeks dan susunan alfabet yang digambarkan dengan tabel di bawah ini.

1:	< ZWAXJGDLUBVIQHKYPNTCRMOSFE <
2:	< KPBELNACZDTRXMJQOYHGVSFUWI <
3:	< BDMAIZVRNSJUWFHTEQGYXPLOCK <
4:	< RPLNDVHGFCUKTEBSXQYIZMJWAO <
5:	< IHFRLABEUOTSGJVDKCPMNZQWXY
6:	< AMKGHIWPNYCJBFZDRUSLOQXVET <
7:	< GWTHSPYBXIZULVKMRAFDCEONJQ <
8:	< NOZUTWDCVRJLXKISEFAPMYGHBQ <
9:	< XPLTDSRFHENYVUBMCQWAOIKZGJ <
10:	< UDNAJFBOWTGVRSCZQKELMXYIHP <

Tabel I Alfabet Wheel Cipher

1. Anggap kunci dari enkripsi di kasus ini adalah urutan dari potongan silindris dengan indeks :

   7,9,5,10,1,6,3,8,2,4

2. Pihak pengirim ingin mengirimkan sebuah pesan (plainteks) yang berisi “retreat now” ke pihak penerima.

3. Pihak pengirim kemudian menyusun potongan-potongan silindris sesuai dengan urutan indeks kunci.

4. Lalu Pihak pengirim menyusun suatu baris yang membentuk susunan alfabet “retreat now”. Berikut ini adalah gambaran dari susunan alfabet di wheel cipher. Plainteks yang ingin disampaikan digambarkan di kolom paling kiri. Spasi diberikan untuk memudahkan penggambaran.

7:	< R AFDCE O NJQGWTHSPYBXIZULVKM <
9:	< E NYVUB M CQWAOIKZGJXPLTDSRFH <
5:	< T SGJVD K CPMNZQWXYIHFRLABEUO <
10:	< R SCZQK E LMXYIHPUDNAJFBOWTGV <
1:	< E ZWAXJ G DLUBVIQHKYPNTCRMOSF <
6:	< A MKGHI W PNYCJBFZDRUSLOQXVET <
3:	< T EQGYX P LOCKBDMAIZVRNSJUWFH <
8:	< N OZUTW D CVRJLXKISEFAPMYGHBQ <
2:	< O YHGVS F UWIKPBELNACZDTRXMJQ <

4:	 W AORPL N DVHGFCUKTEBSXQYIZMJ <

Tabel II Alfabet Wheel Cipher Setelah Diacak

5. Kemudian pihak pengirim memilih baris ke enam dari plainteks sebagai cipherteks. Pada gambar di atas diberikan spasi untuk memudahkan penggambaran.

6. Isi dari cipherteks adalah :
   OMKEGWPDFN

7. Saat pihak penerima menerima cipherteks, pihak penerima menyusun potongan-potongan silindris sesuai dengan urutan indeks kunci

8. Kemudian pihak penerima memutar potongan silindris untuk mendapatkan baris dengan susunan alfabet sesuai dengan cipherteks, yaitu "OMKEGWPDFN"

9. Lalu pihak penerima mencari baris lain yang masuk akal untuk menjadi plainteks. Baris yang masuk akal adalah baris ke enam dari baris cipherteks yang berisi "retreat now"

Contoh di atas merupakan contoh yang normal karena panjang dari teks sama dengan panjang wheel cipher. Berikut ini adalah contoh alternatif ketika panjang dari teks lebih kecil dari panjang wheel cipher.

1. Anggap kunci dari enkripsi di kasus ini sama dengan kasus sebelumnya, yaitu :
   7,9,5,10,1,6,3,8,2,4

2. Pihak pengirim ingin mengirimkan sebuah pesan (plainteks) yang berisi "hello" ke pihak penerima. Karena panjang teks lebih kecil dari panjang wheel cipher, maka sisa dari potongan silinder diberi alfabet "z", sehingga plainteks yang akan dikirimkan adalah "hellozzzzz"

3. Pihak pengirim kemudian menyusun potongan-potongan silindris sesuai dengan urutan indeks kunci.

4. Lalu pihak pengirim menyusun suatu baris yang membentuk susunan alfabet "hellozzzzz". Berikut ini adalah gambaran dari susunan alfabet di wheel cipher. Plainteks yang ingin disampaikan digambarkan di kolom paling kiri. Spasi diberikan untuk memudahkan penggambaran.

7:	 H SP Y BXIZULVKMRAFDCEONJQGWT <
9:	 E NY V UBMCQWAOIKZGJXPLTDSRFH <
5:	 L AB E UOTSGJVDKCPMNZQWXYIHFR <
10:	 L MX Y IHPUDNAJFBOWTGVRSCZQKE <
1:	 O SF E ZWAXJGDLUBVIQHKYPNTCRM <
6:	 Z DR U SLOQXVETAMKGHIWPNYCJBF <
3:	 Z VR N SJUWFHTEQGYXPLOCKBDMAI <
8:	 Z UT W DCVRJLXKISEFAPMYGHBQNO <
2:	 Z DT R XMJQOYHGVSFUWIKPBELNAC <
4:	 Z MJ W AORPLNDVHGFCUKTEBSXQYI <

Tabel III Alfabet Wheel Cipher Setelah Diacak

5. Kemudian pihak pengirim memilih baris ke tiga dari plainteks sebagai cipherteks. Pada gambar di atas diberikan spasi untuk memudahkan penggambaran.

6. Isi dari cipherteks adalah :
   VEYEUNWRW

7. Saat pihak penerima menerima cipherteks, pihak penerima menyusun potongan-potongan silindris sesuai dengan urutan indeks kunci

8. Kemudian pihak penerima memutar potongan silindris untuk mendapatkan baris dengan susunan alfabet sesuai dengan cipherteks, yaitu “VEYEUNWRW”

9. Lalu pihak penerima mencari baris lain yang masuk akal untuk menjadi plainteks. Baris yang masuk akal adalah baris ke tiga dari baris cipherteks yang berisi “hellozzzzz”. Pihak penerima dapat mengambil asumsi bahwa “zzzzz” hanyalah sebagai karakter tambahan untuk mengisi kekosongan potongan silindris

Berikut ini adalah contoh-contoh lain dalam penggunaan wheel cipher.

1. Anggap kunci dari enkripsi di kasus ini sama dengan kasus sebelumnya, yaitu :
   7,9,5,10,1,6,3,8,2,4

2. Pihak pengirim ingin mengirimkan sebuah pesan (plainteks) yang berisi “kriptograf” ke pihak penerima.

3. Pihak pengirim kemudian menyusun potongan-potongan silindris sesuai dengan urutan indeks kunci.

4. Lalu pihak pengirim menyusun suatu baris yang membentuk susunan alfabet “kriptograf”. Berikut ini adalah gambaran dari susunan alfabet di wheel cipher. Plainteks yang ingin disampaikan digambarkan di kolom paling kiri. Spasi diberikan untuk memudahkan penggambaran.

7:	 K MRAFDCEONJQGWTHSPYBXIZUL V
9:	 R FHENYVUBMCQWAOIKZGJXPLTD S
5:	<
	I HFRLABEUOTSGJVDKCPMNZQWX Y
10:	 P UDNAJFBOWTGVRSCZQKELMXYI H
1:	 T CRMOSFEZWAXJGDLUBVIQHKYP N
6:	 O QXVETAMKGHIWPNYCJBFZDRUS L
3:	 G YXPLOCKBDMAIZVRNSJUWFHTE Q
8:	 R JLXKISEFAPMYGHBQNOZUTWDC V
2:	 Z DTRXMJQOYHGVSFUWIKPBELNA C
4:	 F CUKTEBSXQYIZMJWAORPLNDVH G

Tabel III Alfabet Wheel Cipher Setelah Diacak

5. Kemudian pihak pengirim memilih baris ke satu dari plainteks sebagai cipherteks. Pada gambar di atas diberikan spasi untuk memudahkan penggambaran.

6. Isi dari cipherteks adalah :
   VSYHNLQVCG

7. Saat pihak penerima menerima cipherteks, pihak penerima menyusun potongan-potongan silindris sesuai dengan urutan indeks kunci

8. Kemudian pihak penerima memutar potongan silindris untuk mendapatkan baris dengan susunan alfabet sesuai dengan cipherteks, yaitu “VSYHNLQVCG”

9. Lalu pihak penerima mencari baris lain yang masuk akal untuk menjadi plainteks. Baris yang masuk akal adalah baris ke satu dari baris cipherteks yang berisi “kriptograf”.

Berikut ini adalah contoh lain dalam penggunaan wheel cipher.

1. Anggap kunci dari enkripsi di kasus ini sama dengan kasus sebelumnya, yaitu :
   7,9,5,10,1,6,3,8,2,4

2. Pihak pengirim ingin mengirimkan sebuah pesan (plainteks) yang berisi “cipherteks” ke pihak penerima.

3. Pihak pengirim kemudian menyusun potongan-potongan silindris sesuai dengan urutan indeks kunci.

4. Lalu pihak pengirim menyusun suatu baris yang membentuk susunan alfabet “cipherteks”. Berikut ini adalah gambaran dari susunan alfabet di wheel cipher. Plainteks yang ingin disampaikan digambarkan di kolom paling kiri. Spasi diberikan untuk memudahkan penggambaran.

7:	< C EONJQGWTHSPYBXIZULVKM R AFD <
9:	< I KZGJXPLTDSRFHENYVUBMC Q WAO <
5:	< P MNZQWXYIHFRLABEUOTSGJ V DKC <
10:	< H PUDNAJFBOWTGVRSCZQKEL M XYI <
1:	< E ZWAXJGDLUBVIQHKYPNTCR M OSF <
6:	< R USLOQXVETAMKGHIWPNYCJ B FZD <
3:	< T EQGYXPLOCKBDMAIZVRNSJ U WFH <
8:	< E FAPMYGHBQNOZUTWDCVRJL X KIS <
2:	< K PBELNACZDTRXMJQOYHGVS F UWI <
4:	< S XQYIZMJWAORPLNDVHGFCU K TEB <

Tabel III Alfabet Wheel Cipher Setelah Diacak

5. Kemudian pihak pengirim memilih baris ke satu dari plainteks sebagai cipherteks. Pada gambar di atas diberikan spasi untuk memudahkan penggambaran.

6. Isi dari cipherteks adalah :
   RQVMMBUXFK

7. Saat pihak penerima menerima cipherteks, pihak penerima menyusun potongan-potongan silindris sesuai dengan urutan indeks kunci.

8. Kemudian pihak penerima memutar potongan silindris untuk mendapatkan baris dengan susunan alfabet sesuai dengan cipherteks, yaitu “RQVMMBUXFK”

9. Lalu pihak penerima mencari baris lain yang masuk akal untuk menjadi plainteks. Baris yang masuk akal adalah baris ke satu dari baris cipherteks yang berisi “cipherteks”.

Berikut ini adalah contoh lain dalam penggunaan wheel cipher.

1. Anggap kunci dari enkripsi di kasus ini sama dengan kasus sebelumnya, yaitu :
   7,9,5,10,1,6,3,8,2,4

2. Pihak pengirim ingin mengirimkan sebuah pesan (plainteks) yang berisi “cipheraaaa” ke pihak penerima.

3. Pihak pengirim kemudian menyusun potongan-potongan silindris sesuai dengan urutan indeks kunci.

4. Lalu pihak pengirim menyusun suatu baris yang membentuk susunan alfabet “cipheraaaa”. Berikut ini adalah gambaran dari susunan alfabet di wheel cipher. Plainteks yang ingin disampaikan digambarkan di kolom paling

kiri. Spasi diberikan untuk memudahkan penggambaran.

7:	 C EONJQGWTHSPYBXIZULVKMRAF D
9:	 I KZGJXPLTDSRFHENYVUBMCQWA O
5:	 P MNZQWXYIHFRLABEUOTSGJVDK C
10:	 H PUDNAJFBOWTGVRSCZQKELMXY I
1:	 E ZWAXJGDLUBVIQHKYPNTCRMOS F
6:	 R USLOQXVETAMKGHIWPNYCJBFZ D
3:	 A IZVRNSJUWFHTEQGYXPLOCKBD M
8:	 A PMYGHBQNOZUTWDCVRJLXKISE F
2:	 A CZDTRXMJQOYHGVSFUWIKPBEL N
4:	 A ORPLNDVHGFCUKTEBSXQYIZMJ W

Tabel III Alfabet Wheel Cipher Setelah Diacak

5. Kemudian pihak pengirim memilih baris ke satu dari plainteks sebagai cipherteks. Pada gambar di atas diberikan spasi untuk memudahkan penggambaran.

6. Isi dari cipherteks adalah :
   DOCIFDMFNW

7. Saat pihak penerima menerima cipherteks, pihak penerima menyusun potongan-potongan silindris sesuai dengan urutan indeks kunci.

8. Kemudian pihak penerima memutar potongan silindris untuk mendapatkan baris dengan susunan alfabet sesuai dengan cipherteks, yaitu “DOCIFDMFNW”

9. Lalu pihak penerima mencari baris lain yang masuk akal untuk menjadi plainteks. Baris yang masuk akal adalah baris ke satu dari baris cipherteks yang berisi “cipheraaaa”.

V. Kriptanalisis

Untuk memecahkan kunci wheel cipher, tidak cukup dengan hanya mengetahui salah satu kasus plainteks dan cipherteks. Harus ada analisis yang lebih lanjut karena jumlah kemungkinan susunan kunci adalah sejumlah permutasi dari n dimana n adalah jumlah potongan silindris. Cara untuk mempermudah pemecahan kunci dapat menggunakan kelemahan dari wheel cipher dalam hal kesamaan selisih baris antara baris cipherteks dengan baris plainteks

Contoh kriptanalisis wheel cipher di makalah ini menggunakan contoh wheel cipher di bab studi kasus, dengan hanya menggunakan sepuluh potongan silindris. Dengan hanya menggunakan sepuluh potongan silindris, jumlah kemungkinan susunan kunci adalah sebesar

10! = 3.628.800

Pada zaman Jefferson dan Bazeries, solusi dari kemungkinan susunan kunci sebanyak 3,6 juta tersebut tidak mungkin dapat dicari karena relatif masih menggunakan metode trial and error secara manual, walaupun saat ini komputer modern tidak akan memerlukan waktu yang lama untuk mencari solusinya.

Pembahasan kriptanalisis kali ini lebih ditujukan ke pencarian kunci wheel cipher, dengan asumsi bahwa kriptanalis telah mengetahui satu contoh kasus plainteks dan cipherteks. Isi dari plainteks yang telah diketahui adalah heilhitler, sedangkan isi dari cipherteks untuk plainteks tersebut adalah AZNCZEAPBH. Berikut ini adalah proses kriptanalisis untuk contoh kasus tersebut.

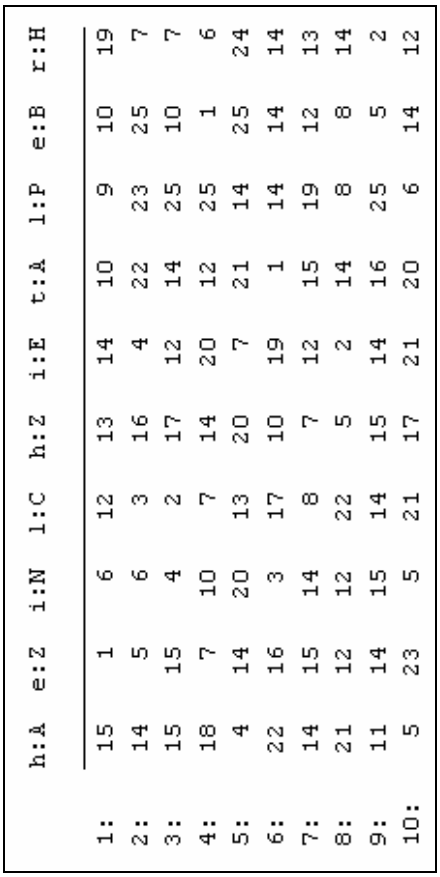
1. Anggap saat ini kriptanalis masih belum mengetahui potongan silindris tertentu untuk mengenkripsi suatu alphabet. Namun kriptanalis memegang teori bahwa selisih antara alphabet plainteks dengan alphabet cipherteks adalah sama untuk seluruh karakter.

2. Buat perbandingan antara dua kelompok alphabet, yaitu alphabet dari plainteks, dan alphabet dari cipherteks. Berikut ini adalah tabel perbandingannya.

Alfabet	
Plainteks	Cipherteks
h	A
e	Z
i	N
l	C
h	Z
i	E
t	A
l	P
e	B
r	H

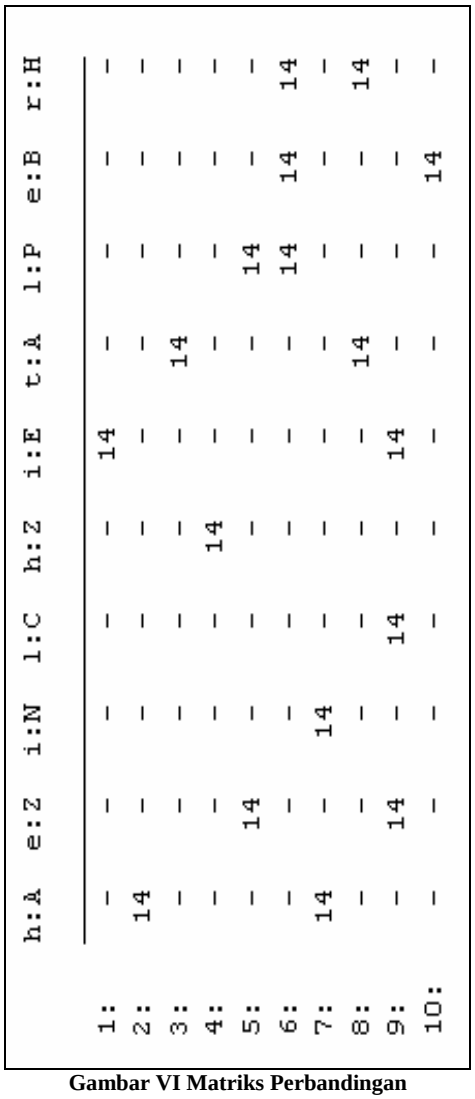
Tabel III Perbandingan Alfabet Plainteks-Cipherteks

3. Berdasarkan perbandingan alfabet antara plainteks dengan cipherteks, buat sebuah matriks yang menggambarkan selisih antara alfabet di setiap potongan silindris. Berikut ini adalah matriks perbandingannya.



Gambar V Matriks Perbandingan

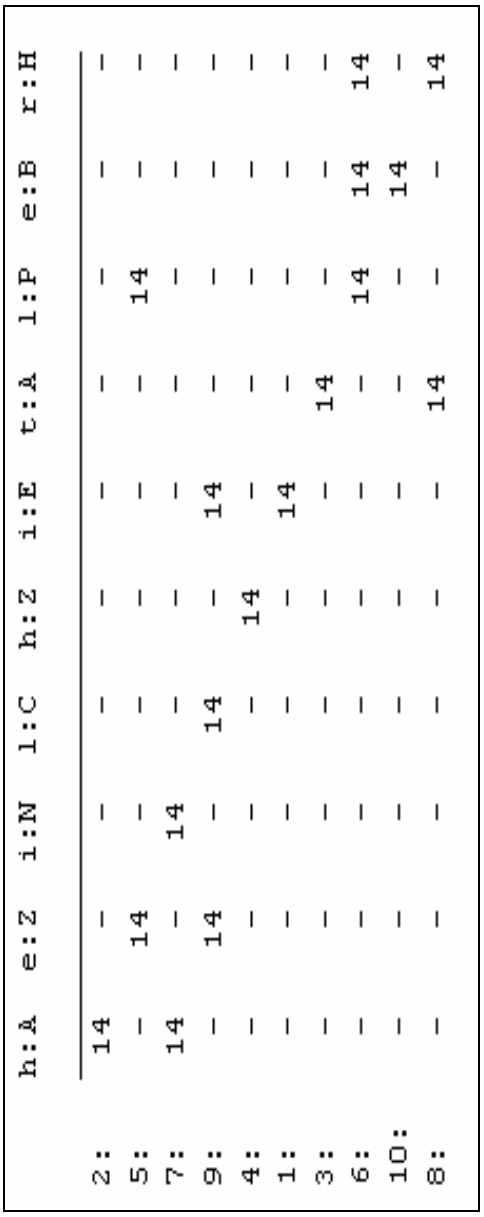
4. Analisis matriks perbandingannya. Cari sebuah angka yang muncul di setiap baris (potongan silindris) dan kolom (perbandingan alphabet). Angka tersebut akan menjadi kemungkinan solusi dari selisih antara plainteks dengan cipherteks. Setelah dianalisis, angka yang muncul di matriks tersebut adalah 14. Berikut ini adalah matriks yang menggambarkan kemunculan angka 14 di kasus ini.



	h:A	e:Z	i:N	l:C	h:Z	i:E	t:A	l:P	e:B	r:H
1:	–	–	–	–	–	14	–	–	–	–
2:	14	–	–	–	–	–	–	–	–	–
3:	–	–	–	–	–	–	14	–	–	–
4:	–	–	–	–	14	–	–	–	–	–
5:	–	14	–	–	–	–	–	14	–	–
6:	–	–	–	–	–	–	–	14	14	14
7:	14	–	14	–	–	–	–	–	–	–
8:	–	–	–	–	–	–	14	–	–	14
9:	–	14	–	14	–	14	–	–	–	–
10:	–	–	–	–	–	–	–	–	14	–

Gambar VI Matriks Perbandingan

5. Cari susunan potongan silindris yang tepat di wheel cipher dengan mencoba menempatkan angka-angka 14 dalam susunan diagonal utama dari matriks. Proses ini dilakukan dengan mencoba seluruh kemungkinan susunan diagonal utama dari matriks. Berikut ini adalah solusi yang didapat.



	h:A	e:Z	i:N	l:C	h:Z	i:E	t:A	l:P	e:B	r:H
2:	14	–	–	–	–	–	–	–	–	–
5:	–	14	–	–	–	–	–	14	–	–
7:	14	–	14	–	–	–	–	–	–	–
9:	–	14	–	14	–	14	–	–	–	–
4:	–	–	–	–	14	–	–	–	–	–
1:	–	–	–	–	–	14	–	–	–	–
3:	–	–	–	–	–	–	14	–	–	–
6:	–	–	–	–	–	–	–	14	14	14
10:	–	–	–	–	–	–	–	–	14	–
8:	–	–	–	–	–	–	14	–	–	14

Gambar VII Matriks Perbandingan

6. Dengan ditemukannya susunan potongan silindris yang tepat, maka dapat disimpulkan bahwa kunci wheel cipher untuk kasus plainteks dan cipherteks di atas adalah :

   2,5,7,9,4,1,3,6,10,8

Proses kriptanalisis di atas memiliki kemungkinan solusi di bagian besar selisih baris antara baris plainteks dengan baris cipherteks; dan kemungkinan solusi di bagian susunan diagonal utama matirks yang

menggambarkan susunan dari potongan silindris. Jumlah kemungkinan solusi yang muncul selama proses kriptanalisis berbanding lurus dengan jumlah potongan silindris. Semakin banyak potongan silindris dalam suatu wheel cipher, maka semakin banyak kemungkinan solusi yang muncul. Hal ini berarti semakin sulit kunci wheel cipher untuk dipecahkan.

Dalam kasus nyata dengan jumlah potongan silindris sebanyak 25-30 buah di suatu wheel cipher, maka jumlah kemungkinan solusi dari kunci wheel cipher juga berkali lipat lebih banyak. Proses kriptanalisis dapat dipermudah jika kriptanalis mengetahui lebih dari satu kasus plainteks-cipherteks untuk satu kunci wheel cipher yang sama.

Terdapat cara kriptanalisis yang lain yang dapat digunakan untuk memecahkan kunci wheel cipher. Yaitu jika selisih baris plainteks dengan baris cipherteks telah diketahui, maka dapat dilakukan metode seperti multiple anagram untuk menyusun potongan silindris.

VI. Arah Pengembangan

Berdasarkan analisis algoritma, studi kasus dan kriptanalisis yang dilakukan di bab sebelumnya, didapatkan beberapa cara untuk meningkatkan faktor keamanan dari penggunaan wheel cipher sebagai metode untuk mengenkripsikan dan mendekripsikan data.

Cara yang pertama adalah dengan meningkatkan jumlah potongan silindris yang digunakan atau yang dapat dipilih. Dengan meningkatnya jumlah potongan silindris yang digunakan, maka akan memperbanyak kemungkinan solusi kunci sehingga semakin mempersulit kriptanalis dalam mendapatkan solusi. Dengan meningkatnya jumlah potongan silindris, seperti pada M94, maka kemungkinan solusi akan semakin banyak karena kriptanalis tidak mengetahui potongan silindris apa saja yang sedang digunakan untuk setiap kasus.

Cara yang kedua adalah dengan membuat pola tertentu untuk kunci wheel cipher. Dengan begitu, untuk setiap kasus yang berurutan tidak menggunakan kunci yang sama sehingga kriptanalis semakin sulit mendapatkan kunci. Pola kunci wheel cipher diketahui oleh pihak penerima dan pihak pengirim dan menjadi suatu rahasia.

Cara yang ketiga adalah dengan menggunakan jumlah potongan silindris yang berbeda-beda untuk setiap kasus. Hal ini dapat mengecoh kriptanalis dalam memecahkan kunci. Cara ini dapat dipermudah dengan penggunaan cara kedua untuk menggenerate kunci yang digunakan untuk suatu kasus.

VII. Kesimpulan

Dari penjelasan di atas, dapat disimpulkan bahwa metode wheel cipher merupakan sebuah metode kriptografi yang cukup aman. Walaupun sudah ada metode untuk memecahkan kunci wheel cipher, metode wheel cipher tetap dapat digunakan secara aman jika dikembangkan dengan cara penambahan potongan silindris atau perubahan kunci.

Selain itu dapat disimpulkan juga bahwa metode ini sangat fleksibel dengan perkembangan-perkembangan baru yang aka menjadikan wheel cipher aman untuk digunakan sebagai metode kriptografi.

VIII. Daftar Pustaka

http://ejefferson.org/gallery/innovations/wheelcipher.htm

http://ejefferson.org/reports/interests/wheel_cipher.htm

http://en.wikipedia.org/wiki/bazeries.htm

http://en.wikipedia.org/wiki/bazeries_cylinder.htm

http://en.wikipedia.org/wiki/Thomas_Jefferson.htm

http://library.thinkquest.org/04oct/00451/president.htm

http://monticello.org/jefferson/lewisandclark/cipher.html

http://monticello.org/jefferson/wheelcipher/cipher_decode.html

http://monticello.org/reports/interests/wheel_cipher.html
http://www.bankersonline.com/vendor_guru/diebold/diebold-pin.html
http://www.bellaonline.com/articles/art28440.htm
http://www.economicexpert.com/a-bazeries-cylinder.htm
http://www.jeffersonlibrary.org/reports/interests/wheel_cipher.htm
http://www.jproc.ca/crypto/m94.htm
http://www.lewis-clark.org/content/content-article.asp
http://www.maritime.org/csp488.htm
http://www.nsa.gov/museum/museu00013.cfm
http://www.pacificsites.com/~brooke/m94.htm
http://www.quadibloc.com/crypto/ro020101.htm
http://www.quadibloc.com/crypto/ro0207.htm
http://www.vectorsite.net/ttcode_05.htm
http://www.whitehouse.gov/history/presidents/tj3.htm
http://www3.brinkster.com/redline/crypt/jefferson.asp

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