STUDI DAN PERBANDINGAN ALGORITMA SIMETRI NIHILIST DAN VIGENERE CHIPER

Aldo Juwito Yahya – NIM : 13503085

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if13085@students.if.itb.ac.id

Abstrak

Algoritma kriptografi klasik merupakan metode kriptografi yang berbasis karakter, bukan bit seperti pada algoritma kriptografi modern. Salah satu jenis kriptografi klasik yang lazim dikenal adalah substitusi abjad-majemuk *chiper* (*Polyalpabetic substitution cipher*). *Chiper* jenis ini menggunakan kunci yang berbeda untuk mengenkripsi tiap huruf. Salah satu contoh *chiper* jenis ini adalah *nihilist chiper* dan *Vigenere chiper.*

Nihilist chiper ditemukan sekitar abad ke-19 tepatnya tahun 1880an dan digunakan di Rusia oleh *Russian nihilist* untuk mengorganisir teroris-teroris dalam melawan rezim *czarist.* Beberapa tahun kemudian, algoritma ini mengalami perkembangan dan digunakan sebagai alat komunikasi mata-mata Soviet. *Vigenere Chiper* sendiri merupakan chiper abjad-majemuk yang paling dikenal karena menghasilkan banyak varian atau cipher turunan seperti Beaufort, Gronsfeld, Porta, dsb. Chiper ini dipublikasikan oleh seorang diplomat yang juga kriptologis andal dari Prancis, Blaise de Vigenere pada tahun 1586.

Makalah ini membahas dan membandingkan kedua chiper tersebut. Kelebihan dan kelemahan masing-masing chiper akan dipaparkan disamping persamaan dan perbedaan di antara keduanya. Selain itu, pengujian kriptanalisis terhadap kedua chiper juga dilakukan untuk melihat seberapa andal dan kuat algoritma dari chiper tersebut.

Dari hasil pengujian dan perbandingan didapatkan bahwa Percobaan penyerangan pada kedua *chiper* berhasil memecahkan chiperteks dengan sempurna. Namun, dari hasil ini tidak dapat dikatakan bahwa kedua chiper ini lemah karena chiperteks yang dijadikan objek penyerangan hanya mengimplementasikan panjang kunci yang relatif pendek yaitu 4 karakter. *Nihilist Chiper* unggul dalam penggunaan bujursangkar *Polybius* yang bisa berubah tergantung kunci. *Vigenere chiper* unggul lebih karena faktor sejarah di mana chiper ini sudah sangat dikenal sehingga mudah dipahami dan masih cukup aman untuk digunakan.

Kata kunci: kriptografi, kriptanalis, *nihilist chilper, vigenere chiper,* algoritma kriptografi klasik, *polyalphabetic substitution chiper*

1. Pendahuluan

Jauh sebelum ditemukannya media komputer, orang menggunakan kertas untuk saling bertukar pesan. Pesan yang akan disampaikan ditulis dalam suatu kertas, kemudian dikirimkan kepada pihak yang dituju. Proses pengiriman ini ada kalanya dibantu oleh pihak lain. Pihak lain yang dimaksud disini bisa saja orang yang dipercaya, melalui pos, merpati, atau media-media perantara lainnya. Kebutuhan keamanan akan pesan tersebut timbul ketika ternyata ada pihak lain yang tidak berwenang ingin mengetahui isi dari pesan tersebut.

Berdasarkan permasalahan ini lahirlah metode untuk menjaga kerahasiaan pesan yang disebut kriptografi. Kriptografi merupakan salah satu metode dalam menuliskan pesan di mana tidak ada seorang pun yang dapat membaca isi pesan tersebut selain dari pihak yang dituju. Kriptografi berasal dari bahasa Yunani “krypte” yang berarti tersembunyi, dan “grafik” yang berarti tulisan. Pesan asli yang akan disembunyikan atau dilindungi disebut dengan

plainteks, sedangkan hasil dari proses penyamaran pesan disebut chiperteks. Proses untuk menyamarkan atau menyembunyikan pesan itu sendiri disebut enkripsi, sedangkan proses untuk mengembalikan ke pesan semula disebut dekripsi. Adapun orang yang melakukan proses enkripsi disebut dengan kriptografer, sedangkan orang yang berusaha untuk memecahkan chiperteks disebut kriptanalis.

Proses penyandian plainteks membutuhkan algoritma-algoritma tertentu. Algoritma-algoritma tersebut merupakan jenis algoritma kriptografi klasik karena dibuat hanya menggunakan pena dan kertas dan berbasis karakter, tidak seperti sekarang di mana algoritma dibuat dengan bantuan komputer dan berbasiskan bit. Kriptografi klasik terdiri dari dua kelas yaitu chiper substitusi dan chiper transposisi. Pembagian ini didasarkan pada metode penyandian plainteks. Chiper substitusi menggunakan metode penggantian karakter dalam plainteks dengan karakter lain, sedangkan chiper transposisi mengacak susunan karakter dari pesan untuk membentuk chiperteks.

Dalam sejarah, terdapat berbagai macam algoritma kriptografi yang telah diciptakan. Algoritma-algoritma tersebut bervariasi mulai dari yang sederhana sampai yang sangat kompleks yang sulit untuk dipecahkan. Dari berbagai macam jenis tersebut, terdapat beberapa algoritma yang merupakan pionir dan terkenal di kalangan pecinta kriptografi di seluruh dunia. Salah satu di antaranya adalah *Vigenere Chiper*. Chiper ini termasuk dalam algoritma substitusi abjad-majemuk di mana setiap karakter pada plainteks disandikan dengan karakter kunci yang berbeda-beda.

Chiper ini mempunyai banyak varian dan pengembangan. Salah satu pengembangan yang menarik adalah *Nihilist Chiper* di mana hasil penyandian pesannya bukan dalam bentuk alfabet, melainkan bilangan. Chiper ini ditemukan di Uni Soviet, salah satu negara yang terkenal menghasilkan banyak macam algoritma kriptografi.

2. Definisi

2.1 Algoritma Kriptografi Klasik

Kriptografi klasik pada dasarnya berbasis karakter. Kriptografi klasik juga sering disebut dengan *pen-and-paper chiper* karena pengoperasiannya yang hanya menggunakan pena dan kertas saja.
Algoritma kriptografi klasik dapat dibedakan menjadi dua kelas yaitu:

1. Chiper substitusi, yaitu teknik kriptografi yang mengganti satu atau beberapa karakter dari plainteks dengan karakter lain berdasarkan sistem atau kunci yang ditetapkan. Salah satu contoh yang terkenal adalah *Caesar Chiper*, di mana setiap huruf pada plainteks diganti dengan huruf ke-3 dari huruf yang bersangkutan pada urutan abjad.
2. Chiper transposisi, yaitu teknik kriptografi yang mengubah susunan karakter dari plainteks berdasarkan sistem tertentu.

Pada umumnya, algoritma kriptografi modern yang banyak digunakan sekarang menerapkan kedua jenis chiper tersebut untuk menghasilkan pesan rahasia.

2.2 Chiper Abjad-Majemuk (*Polyalphabetic Substitution Chiper*)

Chiper abjad-majemuk merupakan salah satu jenis chiper substitusi yang dibuat dari sejumlah chiper abjad-tunggal, masing-masing dengan kunci yang berbeda.
Ada dua macam tipe chiper abjad-majemuk yaitu:

1. Periodik. Pada tipe ini, pesan dapat dibagi ke dalam grup-grup dengan setiap grup dienkripsi dengan kunci yang sama. Hal ini disebabkan pesan dienkripsi dengan menggunakan kunci yang diulang secara periodik. Kebanyakan chiper abjad-majemuk mempunyai tipe seperti ini. Tipe periodik digolongkan lagi menjadi dua jenis yaitu:
   a. *Multiple Alphabet Chiper*, di mana setiap karakter enkripsi dibuat berdasarkan kunci yang telah ditentukan sebelumnya.
   b. *Progressive Alphabet Chiper,* di mana terdapat sebuah karakter enkripsi utama dengan 25 karakter lainnya yang digunakan untuk melakukan penjumlahan, melakukan penggeseran satu karakter, atau sebaliknya

berdasarkan penggeseran karakter sebelumnya.

2. Non periodik. Pada tipe ini, tidak ada pengulangan secara periodik dari kunci yang digunakan.

2.3 *Nihilist Chiper*

2.3.1 Sejarah

Nihilist chiper merupakan salah satu *chiper* dengan algoritma simetri. *Chiper* ini ditemukan oleh penganut paham nihilisme di belahan Uni Soviet sekitar tahun 1880. *Chiper* ini digunakan untuk berkomunikasi dengan teroris-teroris yang sedang mengalami konflik dengan kekaisaran Uni Soviet.

2.3.2 Deskripsi *Chiper*

Seperti yang telah disebutkan di atas bahwa *Nihilist Chiper* merupakan salah satu contoh dari algoritma simetri, dan juga merupakan chiper substitusi abjad-majemuk (*polyalphabetic substitution chiper*).

Langkah awal yang dilakukan untuk menggunakan *chiper* ini adalah membentuk sebuah bujursangkar *Polybius* (*Polybius square*) dengan elemennya adalah alfabet secara acak. Kotak ini nantinya akan digunakan untuk mengenkripsi plainteks dan kunci menjadi bentuk rangkaian dua digit bilangan. Bilangan-bilangan tersebut kemudian dijumlahkan, dan apabila panjang kunci lebih pendek dari plainteks, maka kunci diulang secara periodik.

Contoh:

1. Bentuk *polybius square*. Dengan menggunakan kunci ZEBRAS diperoleh:

	1	2	3	4	5
1	Z	E	B	R	A
2	S	C	D	F	G
3	H	I/J	K	L	M
4	N	O	P	Q	T
5	U	V	W	X	Y

2. Untuk mengenkripsi, setiap huruf pada plainteks dan kunci disandikan dengan nomor dari baris dan kolom pertama pada *polybius square.* Contoh: huruf Z disandikan dengan 00, huruf M dengan 24, dst.
3. Misalkan plainteks adalah "*DYNAMITE WINTER PALACE*" dan kunci NARODNIK (kunci bisa sama dengan kunci yang digunakan untuk membentuk *polybius square*). Kunci diulang secara periodik sepanjang plainteks. Representasi plainteks dan kunci adalah sebagai berikut:

   PT : 23 55 41 15 35 32 45 12 53 32 41 45 12 14 43 15 34 15 22 12

   KEY : 41 15 14 42 23 41 32 33 41 15 14 42 23 41 32 33 41 15 14 42
4. Chiperteks diperoleh dengan menjumlahkan nilai plainteks dengan kunci. Hasilnya adalah sebagai berikut:

   CT : 64 70 55 57 58 73 77 45 94 47 55 87 35 55 75 48 75 30 36 54

Sebagai informasi tambahan, *polybius square* dapat dibentuk dengan berbagai macam cara. Cara yang di atas adalah menggunakan kunci sepanjang enam karakter dan diikuti oleh karakter sisanya. Cara lain adalah menggabungkan dengan sedikit metode transposisi. Contoh:

Gunakan kunci BLACKSMITH, diikuti dengan karakter sisa secara terurut menjadi:

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

Dengan membaca dari atas ke bawah, didapatkan urutan karakter sebagai berikut: B D V L E W A F X C G Y K N Z S O M P I Q T R H U

Maka, kotak *polybius* menjadi:

	1	2	3	4	5
1	B	D	V	L	E
2	W	A	X	F	C
3	G	Y	K	N	Z
4	S	O	M	P	I/J
5	Q	T	R	H	U

2.3.3 Deskripsi *Chiper*

Nilai bilangan yang paling kecil yang mungkin untuk enkripsi adalah 11, sehingga nilai bilangan untuk chiperteks yang paling kecil yaitu 22. Bilangan ini didapat apabila huruf kunci dan huruf plainteks adalah huruf dengan nilai 11. Hal sama juga berlaku untuk nilai bilangan chiperteks yang paling besar yaitu 110 yang diperoleh dengan menjumlahkan representasi nilai huruf kunci dan huruf plainteks terbesar yaitu 55.

Bilangan pada karakter plainteks hanya terdiri dari 1, 2, 3, 4, atau 5. Bilangan 6, 7, 8, atau 9 hanya terdapat pada chiperteks.
Apabila terdapat angka 0 pada chiperteks, maka dapat diketahui bahwa itu merupakan penjumlahan dari dua buah angka 5.

2.4 *Vigenere Chiper*

2.4.1 Sejarah

Vigenere Chiper merupakan chiper abjad-majemuk yang paling dikenal karena menghasilkan banyak varian atau cipher turunan seperti Beaufort, Gronsfeld, Porta, dsb. Chiper ini dipublikasikan oleh seorang diplomat yang juga kriptologis andal dari Prancis, Blaise de Vigenere pada tahun 1586. Vigenere menuliskan hasil penemuannya dalam buku/traktat yang berjudul "Traicte des Chiffres". Sebenarnya, Giovan Batista Belaso telah menggambarkannya pertama kali pada tahun 1553 pada bukunya "La Cifra del Sig. Giovan Batista Belaso", namun kurang mendalam. Baru sekitar 200 tahun kemudian, chiper ini dikenal luas dan oleh penemunya diberi nama *Vigenere Chiper*.

Gambar 2.1 Potret wajah Blaise de Vigenere

Chiper ini kemudian dipecahkan oleh Babbage dan Kasiski pada pertengahan abad 19. Kasiski berhasil menemukan metode untuk mengetahui panjang kunci yang digunakan yang kemudian disebut metode Kasiski. Chiper ini juga digunakan oleh tentara konfederasi pada saat Perang Sipil Amerika.

2.4.2 Deskripsi Chiper

Vigenere Cipher menggunakan Bujursangkar Vigenere untuk melakukan enkripsi dan dekripsi. Gambar bujursangkarnya ditunjukkan oleh gambar 2.1

	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 2.2 Bujursangkar Vigenere

Alfabet yang terurut pada baris pertama di bujursangkar mengacu pada plainteks, sedangkan kolom pertama untuk karakter kunci. Perpotongan dari karakter plainteks dan kunci yang terletak dalam badan bujursangkar menyatakan huruf-huruf cipherteks.
Sebagai contoh, plainteks "COME AT ONCE" dengan kunci "TENT". Karena panjang kunci lebih pendek dari plainteks, maka kunci diulang secara periodik. Jadi diperoleh:

```
PT  : COME AT ONCE
KEY : tent te ntte
CT  : VSZX TX BGVI
```

Untuk melakukan dekripsi, maka proses yang dilakukan merupakan kebalikan dari proses enkripsi. Dengan menggunakan contoh di atas, diketahui bahwa chiperteks adalah VSZX TX BGVI dengan kunci tent. Karakter plainteks dapat dengan mudah diperoleh dengan cara mencari huruf chiperteks pada baris huruf kunci yang bersesuaian pada badan bujursangkar

vigenere, maka diperoleh huruf plainteks yang merupakan perpotongan dari kolom plainteks.

Bila dicermati, setiap huruf hasil enkripsi pada *Vigenere Chiper* merupakan *Caesar Chiper* dengan kunci yang berbeda-beda. Contoh:
C('C') = ('C' + 't') mod 26 = V
C('T') = ('T' + 'e') mod 26 = X
Huruf yang sama tidak selalu dienkripsi menjadi huruf chiperteks yang juga sama. Seperti yang terlihat pada contoh di atas, huruf plainteks E dapat dienkripsi menjadi X atau I, tergantung kunci. Inilah yang menjadi karakteristik utama dari chiper abjad-majemuk di mana setiap huruf plainteks dapat memiliki kemungkinan banyak huruf chiperteks.

2.5 Metode Kasiski (Dasar Pemfaktoran)

Metode kasiski ditemukan pada tahun 1863 oleh Mayor Friedrich W. Kasiski yang merupakan seorang pegawai pada Resimen Tentara 33 di Prussia Timur. Beliau hidup pada tahun 1805 sampai 1881. Dia berhasil melihat pengulangan sistem kunci pada chiper substitusi abjad-majemuk khususnya *Vigenere Chiper.* Pengulangan yang terjadi oleh karena kunci yang sama diterapkan pada karakter plainteks yang sama menghasilkan pengulangan pada hasil chiperteks. Interval munculnya pengulangan pada chiperteks kemudian dapat difaktorkan dan dapat mengindikasikan kunci beserta panjangnya yang digunakan dalam proses enkripsi.
Apabila terdapat beberapa pengulangan yang relatif panjang pada chiperteks, maka intervalnya dihitung mulai dari karakter pertama dari pengulangan sampai ketemu dengan karakter pengulangan yang sama berikutnya. Faktor terbesar dari nilai interval ini merepresentasikan panjang karakter kunci yang digunakan untuk mengenkripsi pesan.
Berikut adalah contoh singkat:
`CT : IZGSV PFLBW RXGBP WLBWR XRUNZ DPGLJ LUOPR NOUOD LJ`

Pemfaktoran:

Pengulangan	Interval	Faktor	Faktor terbesar
LBWRX	9	3, 3	3
LJ	12	2, 2, 3	3
UO	6	2, 3	3

Periode dari faktor terbesar adalah 3, maka dapat disimpulkan bahwa 3 merupakan panjang dari kunci yang digunakan.

Metode ini membutuhkan frekuensi pengulangan yang cukup banyak agar memudahkan proses identifikasi faktor. Hal ini tentu saja menyulitkan apabila pesan ternyata sangat singkat sehingga jarang atau bahkan tidak ditemukan pengulangan sama sekali. Namun, terkadang pesan yang panjang pun gagal untuk diidentifikasi dengan metode ini. Hal tersebut kemungkinan besar disebabkan oleh penggunakan kunci yang sangat panjang atau tidak periodik.

3. Pengujian Kriptanalis

3.1 Kriptanalisis pada *Nihilist Chiper*

Percobaan untuk melakukan kriptanalisis
Periode dapat ditemukan melalui pengulangan yang terjadi, atau dari ketidakhadiran, melalui sebuah karakter yang berulang, menghasilkan frekuensi individual yang dihitung pada beberapa alfabet dari periode yang bersangkutan. Apabila susunan dari chiperteks mengikuti bujursangkar Polybius, maka hasil perhitungan frekuensi akan mengikuti grafik dari ke-26 alfabet dikurangi satu alfabet karena jumlah karakter pada bujursangkar Polybius hanya 25 buah.

Alfabet utama dari chiper ini hanya terdiri dari digit 1-2-3-4-5. Selisih maksimum yang mungkin hanya 4. Begitu pula dengan selisih maksimum dari penjumlahan dari bilangan yang dibentuk oleh digit tersebut tetap bernilai 4. Bilangan yang dijumlahkan ketika proses enkripsi dilakukan adalah tidak lain juga terdiri dari 1-2-3-4-5. Hal ini mengakibatkan setiap angka yang terdapat pada chiperteks dapat dianggap sebagai penjumlahan dua digit bilangan, atau dengan kata lain penjumlahan antara puluhan dan satuan.

Untuk penjumlahan dua buah bilangan 5, didapatkan hasil nilai 0 dan nilai puluhan 1 (biasa disebut *carry number*). *Carry number* ini dapat dikeluarkan dari perhitungan terlebih dahulu dengan cara mengurangi nilai puluhan dari bilangan yang diikuti oleh angka 0. Misalnya, terdapat bilangan 40, maka bilangan ini dianggap sebagai tiga puluhan dengan sepuluh satuan.

Apabila pada chiperteks terdapat bilangan 29 dan 87, maka dapat disimpulkan bahwa keduanya dienkripsi dengan karakter kunci yang berbeda. Hal ini karena selisihnya lebih besar dari 4 dengan anggapan bahwa sepuluh satuan ada dan

tidak terdapat bilangan manapun yang bila dijumlahkan dengan sembarang dua digit dari bujursangkar *Polybius* dapat menghasilkan selisih yang besar dari 4. Misalnya, terdapat bilangan 30 dan 77, maka munculnya angka 0 perlu untuk dianalisis. Bilangan 30 mengandung dua puluhan dan 10 satuan. Akibatnya, selisih nilai puluhannya yaitu 7-2 > 4, sehingga dugaan bahwa kedua bilangan tersebut dienkripsi dengan karakter kunci yang sama ditolak.

Berikut adalah tabel bantuan dalam melakukan kriptanalis yang didasarkan pada bujursangkar *Polybius* standar. Baris paling atas menyatakan bilangan kunci, baris paling kiri menyatakan karakter plainteks, dan hasil chiperteks merupakan perpotongan antara keduanya.

	11	12	13	14	15	21	22	23	24	25	31	32
	A	B	C	D	E	F	G	H	I/J	K	L	M
A	11	22	23	24	25	26	32	33	34	35	36	42	43
B	12	23	24	25	26	27	33	34	35	36	37	43	44
C	13	24	25	26	27	28	34	35	36	37	38	44	45
D	14	25	26	27	28	29	35	36	37	38	39	45	46
E	15	26	27	28	29	30	36	37	38	39	40	46	47
F	21	32	33	34	35	36	42	43	44	45	46	52	53
G	22	33	34	35	36	37	43	44	45	46	47	53	54
H	23	34	35	36	37	38	44	45	46	47	48	54	55
I	24	35	36	37	38	39	45	46	47	48	49	55	56
K	25	36	37	38	39	40	46	47	48	49	50	56	57
L	31	42	43	44	45	46	52	53	54	55	56	62	63
M	32	43	44	45	46	47	53	54	55	56	57	63	64
N	33	44	45	46	47	48	54	55	56	57	58	64	65
O	34	45	46	47	48	49	55	56	57	58	59	65	66
P	35	46	47	48	49	50	56	57	58	59	60	66	67
Q	41	52	53	54	55	56	62	63	64	65	66	72	73
R	42	53	54	55	56	57	63	64	65	66	67	73	74
S	43	54	55	56	57	58	64	65	66	67	68	74	75
T	44	55	56	57	58	59	65	66	67	68	69	75	76
U	45	56	57	58	59	60	66	67	68	69	70	76	77
V	51	62	63	64	65	66	72	73	74	75	76	82	83
W	52	63	64	65	66	67	73	74	75	76	77	83	84
X	53	64	65	66	67	68	74	75	76	77	78	84	85
Y	54	65	66	67	68	69	75	76	77	78	79	85	86
Z	55	66	67	68	69	70	76	77	78	79	80	86	87

Sambungan tabel

	33	34	35	41	42	43	44	45	51	52	53	54	55
	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	11	44	45	46	52	53	54	55	56	62	63	64	65	66
B	12	45	46	47	53	54	55	56	57	63	64	65	66	67
C	13	46	47	48	54	55	56	57	58	64	65	66	67	68
D	14	47	48	49	55	56	57	58	59	65	66	67	68	69
E	15	48	49	50	56	57	58	59	60	66	67	68	69	70
F	21	54	55	56	62	63	64	65	66	72	73	74	75	76
G	22	55	56	57	63	64	65	66	67	73	74	75	76	77
H	23	56	57	58	64	65	66	67	68	74	75	76	77	78

I	24	57	58	59	65	66	67	68	69	75	76	77	78	79
K	25	58	59	60	66	67	68	69	70	76	77	78	79	80
L	31	64	65	66	72	73	74	75	76	82	83	84	85	86
M	32	65	66	67	73	74	75	76	77	83	84	85	86	87
N	33	66	67	68	74	75	76	77	78	84	85	86	87	88
O	34	67	68	69	75	76	77	78	79	85	86	87	88	89
P	35	68	69	70	76	77	78	79	80	86	87	88	89	90
Q	41	74	75	76	82	83	84	85	86	92	93	94	95	96
R	42	75	76	77	83	84	85	86	87	93	94	95	96	97
S	43	76	77	78	84	85	86	87	88	94	95	96	97	98
T	44	77	78	79	85	86	87	88	89	95	96	97	98	99
U	45	78	79	80	86	87	88	89	90	96	97	98	99	00
V	51	84	85	86	92	93	94	95	96	02	03	04	05	06
W	52	85	86	87	93	94	95	96	97	03	04	05	06	07
X	53	86	87	88	94	95	96	97	98	04	05	06	07	08
Y	54	87	88	89	95	96	97	98	99	05	06	07	08	09
Z	55	88	89	90	96	97	98	99	00	06	07	08	09	10

Tabel 3.1 Tabel Bantuan untuk Kriptanalisis *Nihilist Chiper*

Contoh kasus:

Berikut adalah chiperteks hasil dari *Nihilist Chiper*.

```
24 66 35 77 37 77 55 59 55 45 55
88 28 66 46
88 37 67 33 59 58 65 45 66 67 58
44 55 34 79
44 59 55 45 42 87 28 76 43 78 46
86 26 67 24
85 26 67 28 76 26 78 46 65 65 88
36 49 54 67
28 65 42 88 36 49 44 89 57 58 54
66 47 67 26
```

Sebagai langkah awal, dimisalkan periode = 2. Proses pencarian dimulai dari bilangan 24 dan terus ke bawah sampai ditemukan perbedaan yang lebih besar dari 4, dengan 2 sebagai nilai selisih konstan. Hasil dari pencarian adalah 33 dan 38 dan kemudian berhenti karena gagal.

Berikutnya, untuk periode = 3, pencarian gagal pada bilangan 24 dan 77.

Untuk periode = 4, ternyata pencarian dapat berlangsung hingga bilangan terakhir chiperteks. Dengan membandingkan setiap bilangan pada interval = 4, pencarian tidak menemukan bilangan puluhan atau satuan yang lebih besar dari 4. Oleh karena itu, tahap berikutnya adalah membuat kolom yang terdiri dari karakter chiperteks dengan interval atau periode = 4.

```
24  66  35  77
37  77  55  59
55  45  55  88
28  66  46  88
37  67  33  59
58  65  45  66
67  58  44  55
34  79  44  59
55  45  42  87
28  76  43  78

46  86  26  67
28  76  26  78
46  65  65  88
36  49  54  67
28  65  42  88
36  49  44  89
57  58  54  65
47  67  26  -
```

Analisis kolom 1: Bilangan puluhan pada kolom pertama mengandung angka 2. Karena angka 2 hanya dapat diperoleh dari penjumlahan 1 dan 1, maka angka kunci yang mungkin adalah 1. Kemudian, bilangan satuan pada kolom pertama mengandung angka yang berkisar dari 4-5-6-7-8. Angka terkecil yang dapat menghasilkan 8 adalah 3, begitu pula dengan angka terbesar yang dapat menghasilkan 4 adalah 3. 3 merupakan satu-satunya angka yang dapat menghasilkan semua kemungkinan angka 4-5-6-7-8, sehingga

dapat disimpulkan bahwa karakter kunci untuk kolom ini bernilai 13.

Analisis kolom 2: Semua puluhan pada bilangan di kolom 2 bernilai antara 4-5-6-7-8 yang dengan menggunakan metode pada analisis di kolom 1, dapat diketahui angka kunci adalah 3. Selain itu, nilai satuannya ternyata berkisar dari 5-6-7-8-9, yang dengan metode yang sama didapat angka kunci adalah 4. Ini membawa pada kesimpulan bahwa bilangan kunci adalah 34.

Analisis kolom 3: nilai puluhan pada kolom ketiga mengandung angka 2 yang berarti angka kunci adalah 1. Hal yang sama juga ditemui pada nilai satuan yaitu angka 2. Sehingga bilangan kunci adalah 11.

Analisis kolom 4: Nilai puluhan dari kolom keempat berkisar antara 5-6-7-8. Hal ini menyulitkan karena kesulitan dalam menentukan angka yang hilang apakah 4 atau 9. Untuk itu, angka kunci yang mungkin adalah 3 atau 4. Sedangkan untuk nilai satuan, bilangan-bilangan pada kolom keempat berkisar antara 5-6-7-8-9, sehingga angka kunci adalah 4. Jadi, dugaan sementara adalah bilangan kunci bernilai 34 atau 44. Dari tabel bantuan diketahui bahwa karakter 34 dan 44 adalah O dan T. Besar kemungkinan, karakter kunci adalah T, mengingat hasil dari analisis ketiga kolom sebelumnya adalah COA, sehingga kata kunci yang dimaksud adalah COAT.

Dengan menggunakan kunci COAT, diperoleh pesan sebagai berikut:

C'	'O'	'A'	'T'
A	M	I	N
I	S	T	E
R	A	T	T
E	M	P	T
I	N	G	E
U	L	O	G
Y	I	N	A
F	U	N	E
R	A	L	S
E	R	M	O
N	W	E	H
A	V	E	H
E	R	E	O
N	L	Y	T
H	E	S	H
E	L	L	T
H	E	N	U
T	I	S	G

O N E

Yang jika dituliskan kembali akan berbunyi: “A minister attempting eulogy in a funeral sermon: We have here only the shell, the nut has gone.”

3.2 Kriptanalisis pada *Vigenere Chiper*

Langkah awal yang dilakukan dalam memecahkan *vigenere chiper* adalah menentukan panjang kunci, yang disimbolkan dengan *m*.
Ada dua jenis teknik yang dapat digunakan yaitu:

1. Metode Kasiski yang menggunakan pemfaktoran seperti yang dijelaskan pada landasan teori.
2. *Index of coincidence*.

Untuk metode kasiski, langkah awal yang dilakukan adalah mencari bigram atau trigram atau kumpulan karakter yang berulang. Simpan jarak antara kedua kedua elemen yang berulang atau biasa interval. Jika diperoleh nilai interval d1, d2, d3, ..., maka nilai *m* merupakan FPB (faktor persekutuan terbesar) dari seluruh nilai interval yang diperoleh.

Metode *index of coincidence* sendiri merupakan metode yang lebih mendalam karena menggunakan perhitungan matematik yang cukup rumit. Metode ini ditemukan oleh Wolfe Friedman pada tahun 1920. Metode ini didefinisikan sebagai berikut:
Misalkan $\mathbf{x} = x_1x_2...x_n$ adalah sebuah string dari n karakter alfabet. *Index of coincidence* dari **x**, disimbolkan dengan $I_c(\mathbf{x})$, didefinisikan sebagai nilai probabilitas di mana dua elemen acak dari **x** adalah identik. Misalkan frekuensi dari A, B, C, ..., Z pada **x** disimbolkan dengan f_0, f_1, ..., f_{25}. Kita dapat memilih dua elemen untuk **x** dalam $\binom{n}{k}$ cara. Untuk setiap i, $0 \le i \le 25$, terdapat $\binom{fi}{2}$ cara untuk memilih kedua elemen pada i. Sedemikian sehingga kita mendapatkan persamaan :

$$I_c(x) = \frac{\sum_{i=0}^{25} f_i(f_i - 1)}{n(n-1)}$$

Sekarang, misalkan **x** adalah *string* untuk kalimat bahasa Inggris. Misalkan frekuensi

kemunculan huruf dalam teks bahasa Inggris dari A, B, ..., Z pada tabel 4.1 disimbolkan dengan p_0, ..., p_{25}, maka kita harapkan hasilnya adalah:

$$I_c(x) \approx \sum_{i=0}^{25} p_i^{\,2} = 0{,}065$$

Karena probabilitas bahwa kedua elemen acak itu A adalah p_0^2, maka probabilitas bahwa keduanya B adalah p_i^2, dst. Alasan yang sama dapat diterapkan jika **x** adalah ciphertext yang diperoleh dari chiper substitusi abjad-tunggal. Pada kasus ini, probabilitas tunggal tersebut akan dipermutasikan, namun nilai

$$\sum_{i-0}^{25} p_i^{\,2}$$

Tidak akan berubah.

Huruf	%	Huruf	%
A	8.2	N	6.7
B	1.5	O	7.5
C	2.8	P	1.9
D	4.2	Q	0.1
E	12.7	R	6.0
F	2.2	S	6.3
G	2.0	T	9.0
H	6.1	U	2.8
I	7.0	V	1.0
J	0.1	W	2.4
K	0.8	X	2.0
L	4.0	Y	0.1
M	2.4	Z	0.1

Tabel 3.2 Tabel Frekuensi Kemunculan Huruf pada Teks Bahasa Inggris

Misalkan suatu chiperteks yang dihasilkan dengan *Vigenere Chiper* $y = y_1y_2...y_n$, dengan *m* adalah substring y_1, y_2, ..., y_m dari y dengan menuliskan chiperteks dalam bentuk kolom, dalam array dengan dimensi *m* x (*n/m*). Baris dari matriks ini adalah substring y_i, $1 \le i \le m$. Jika telah selesai, maka *m* adalah panjang kunci yang dimaksud, dan untuk setiap $I_c(y_i)$ harus bernilai sekitar 0,065. Dengan kata lain, jika *m* bukan panjang kunci, maka substring y_i akan terlihat acak dengan distribusi yang tidak merata. Hal ini disebabkan substring-substring tersebut didapatkan dari metode penggeseran terhadap kunci-kunci yang berbeda. Hasil observasi terhadap string yang benar-benar acak akan menghasilkan:

$$I_c \approx 26(1/26)^2 = 1/26 = 0{,}038$$

Dua nilai yang diperoleh yaitu 0,065 dan 0,038 sudah cukup jauh terpisah sehingga kita kemungkinan besar dapat menebak panjang kunci yang sebenarnya.

Contoh kasus:
Chiperteks berikut merupakan hasil dari *Vigenere Chiper*.

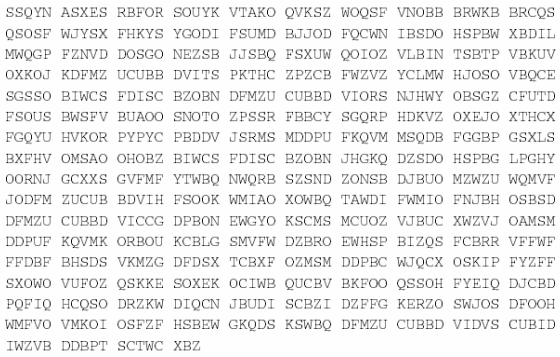
```
CHREEVOAHMAERATBIAXXWTNXBEEOPHBS
BQMQEQERBWRVXUOAKXAOSXXWEAHBWGJM
MQMNKGRFVGXWTRZXWIAKLXFPSKAUTEMN
DCMGTSXMXBTUIADNGMGPSRELXNJELXVR
VPRTULHDNQWTWDTYGBPHXTFALJHASVBF
XNGLLCHRZBWELEKMSJIKNBHWRJGNMGJS
GLXFEYPHAGNRBIEQJTAMRVLCRREMNDGL
XRRIMGNSNRWCHRQHAEYEVTAQEBBIPEEW
EVKAKOEWADREMXMTBHHCHRTKDNVRZCHR
CLQOHPWQAIIWXNRMGWOIIFKEE
```

Cara pertama digunakan metode Kasiski. String CHR pada chiperteks muncul pada lima kali yaitu pada posisi 1, 166, 236, 276, dan 286. Selisih jarak antara string-string tersebut adalah 165, 235, 275, dan 285. Faktor persekutuan terbesar dari keempat interval tersebut adalah 5. Jadi, kemungkinan besar panjang kunci adalah lima karakter.

Cara kedua digunakan metode *index of coincidence*. Dengan *m* = 1, maka diperoleh *index of coincidence* adalah 0,045. Dengan *m* = 2, maka diperoleh *index of coincidence* adalah 0,046 dan 0,041. Dengan *m* = 3, diperoleh 0,043, 0,050, dan 0,047. Dengan *m* = 4, diperoleh nilai 0,042, 0,039, 0,046, dan 0,040. Kemudian dengan *m* = 5, diperoleh nilai 0,063, 0,068, 0,069, 0,061, dan 0,072. Data ini semakin memperkuat hasil dari metode kasiski bahwa panjang kunci adalah lima karakter.

Contoh kasus2:
Kasus berikut memaparkan cara mengetahui kunci, tidak hanya sampai pada panjang kunci saja. Kasus ini diambil dari tugas kriptanalis mata kuliah Kriptografi Sem. I Tahun 2006/2007 Pada Program Studi Teknik Informatika, Institut Teknologi Bandung.

Diberikan berkas chiperteks sebagai berikut:



Gambar 3.1 Berkas chiperteks *Vigenere Chiper*

Mula – mula, panjang kunci dihitung dari chiperteks dengan metode kasiski. Berikut adalah hasil pencarian kata yang berulang (kata yang berwarna sama selain hitam merupakan kata yang mengalami perulangan)

```
SSQYN ASXES RBFOR SOUYK VTAKO QVKSZ WOQSF
VNOBB BRWKB BRCQS
QSOSF WJYSX FHKYS YGODI FSMUD BJJOD FQCWN
IBSDO HSPBW XBDIL
MWQGP FZNVD DOSGO NEZSB JJSBQ FSXUW QOIOZ
VLBIN TSBTP VBKUV
OXKOJ KDFMZ UCUBB DVITS PKTHC ZPZCB FWZVZ
YCLMW HJOSO VBQCE
SGSSO BIWCS FDISC BZOBN DFMZU CUBBD VIORS
NJHWY OBSGZ CFUTD
FSOUS BWSFV BUAOO SNOTO ZPSSR FBBCY SGQRP
HDKVZ OXEJO XTHCK
FGQYU HVKOR PYPYC PBDDV JSRMS MDDPU FKQVM
MSQDB FGGBP GSXLS
BXFHV OMSAO OHOBZ BIWCS FDISC BZOBN JHGKQ
DZSDO HSPBG LPGHY
OORNJ GCXXS GVFMF YTWBQ NWQRB SZSND ZONSB
DJBUO MZWZU WQMVF
JODFM ZUCUB BDVIH PSOOK WMIAO XOWBQ TAWDI
FWMIO FNJBH OSBSD
DFMZU CUBBD VICCG DPBON EWGYO KSCMS MCUOZ
VJBUC XWZVJ OAMSM
DDPUF KQVMK ORBOU KCBLG SMVFW DZBRO EWHSP
BIZQS FCBRR VFFWF
FFDBF BHSDS VKMZG DFDSX TCBXF OZMSM DDPBC
WJQCX OSKIP FYZFF
SXOWO VUFOZ QSKKE SOXEK OCIWB QUCBV BKFOO
QSSOH FYEIQ DJCBD
PQFIQ HCQSO DRZKW DIQCN JBUDI SCBZI DZFFG
KERZO SWJOS DFOOH
WMFVO VMKOI OSFZF HSBEW GKQDS KSWBQ DFMZU
CUBBD VIDVS CUBID
IWZVB DDBPT SCTWC XBZ
```

Kata yang berulang	Jarak antar kata (karakter)
BIWCSFDISCBZOBN	160
SMDDPUFKQVM	224
DFMZUCUBBDI	64, 232, 48, 280

Dari jarak-jarak antar karakter tersebut, didapatkan bahwa faktor persekutuan terbesarnya adalah 8, sehingga panjang kunci yang mungkin adalah faktor dari 8, yaitu 2, 4, dan 8.

Diasumsikan bahwa kunci dengan panjang 2 karakter bukan panjang kunci yang sebenarnya karena perulangan yang terjadi terlalu sedikit untuk chiperteks sepanjang 818 karakter. Jadi, kemungkinan panjang kunci adalah 4 karakter atau 8 karakter.

Berikutnya, digunakan metode analisis frekuensi dengan asumsi panjang kunci adalah 4 karakter. Setelah itu chiperteks dikelompokkan setiap kelipatan atau periode 4, dimulai dari huruf chiperteks pertama, kedua, dan seterusnya.

Kelompok	Huruf yg sering muncul diurut berdasarkan abjad
1	B, E, F, I, J, O, P, S, T, U
2	B, C, D, F, G, H, O, Q, S, W
3	B, C, D, F, G, O, Q, V, W, Z
4	B, D, K, N, O, S, V, Y, X, Z

Seperti yang diketahui bahwa dalam teks berbahasa Inggris, 10 karakter yang yang paling sering muncul adalah E, T, A, O, I, N, S, H, R, dan D. Kesepuluh karakter ini jika diurutkan berdasarkan abjad akan menjadi A, D, E, H, I, N, O, R, S, dan T. Dengan mengingat bahwa setiap kelompok karakter dienkripsi dengan metode *caesar Chiper,* maka dengan mengenkripsi A, D, E, H, I, N, O, R, S, T menggunakan Caesar Chiper dihasilkan seperti tabel dibawah ini :

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

Kemudian, keterurutan abjad tiap kelompok dengan tabel pembanding diatas dibandingkan untuk mendapatkan kunci yang cocok. Untuk kelompok pertama didapatkan hasilnya sesuai dengan kunci **B**. Untuk kelompok kedua yang paling mendekati hasil pada tabel pembanding adalah kunci **O**, sama halnya dengan kelompok ketiga. Sedangkan kelompok keempat yang paling mendekati hasil pada tabel pembanding adalah kunci **K.**

Dengan mendekripsi chiperteks dengan kunci BOOK diperoleh plainteks yang memiliki makna. Sehingga dapat disimpulkan bahwa kata kunci yang dipakai adalah BOOK.

4. Perbandingan *Nihilist Chiper* dan *Vigenere Chiper*

4.1 Persamaan dan Perbedaan

Dari beberapa literatur, penulis mendapatkan banyak pengetahuan dan wawasan akan kedua chiper tersebut. Beberapa persamaan dan perbedaan yang penulis dapatkan antara lain adalah:

1. Sama-sama merupakan chiper substitusi abjad-majemuk. Lebih jauh lagi, keduanya merupakan tipe periodik.
2. Sama-sama menggunakan tabel/ bujursangkar (biasa disebut *checkerboard chiper*) dalam melakukan proses enkripsi dan dekripsi. Perbedaannya adalah pada *Nihilist Chiper,* bujursangkar yang digunakan dapat berubah-ubah tergantung dari kunci bujursangkar ataupun keinginan dari kriptografer, sedangkan pada *Vigenere Chiper* telah didefinisikan dan tidak berubah.
3. Sama-sama digunakan pada saat kondisi perang. *Nihilist chiper* digunakan ketika perang terhadap rezim kaisar yang saat itu berkuasa, sedangkan *Vigenere Chiper* digunakan ketika perang sipil di Amerika Serikat.
4. Hasil enkripsi dari *Nihilist Chiper* berupa sepasang bilangan, sedangkan *Vigenere Chiper* berupa sebuah karakter/alfabet.
5. *Nihilist chiper* ditemukan di Rusia, sedangkan *Vigenere chiper* di Prancis.

4.1 Kelebihan dan Kekurangan

4.1.1 *Nihilist Chiper*

1. Menggunakan substitusi sepasang bilangan, bukan abjad. Hal ini mengakibatkan proses kriptanalisis menjadi sulit karena representasi chiperteks yang berupa bilangan.
2. Bujursangkar *Polybius* sulit untuk ditebak karena bentuknya dapat berubah tergantung dari cara kriptografer membuatnya ataupun kunci bujursangkar yang digunakan. Namun, ini juga mengakibatkan si kriptografer harus memberi tahu kepada pihak yang dituju mengenai bentuk bujursangkar *Polybius*. Hal ini tentu saja tidak efektif.

4.1.2 *Vigenere Chiper*

1. Mudah untuk dipahami dan dapat dikembangkan lebih jauh untuk mendapatkan algoritma yang lebih baik.
2. algoritmanya termasuk masih cukup aman untuk digunakan karena tergantung dari panjang kunci.
3. Termasuk mudah untuk diserang dengan metode Kasiski dengan catatan kunci tidak terlalu panjang.

5. Kesimpulan

Kesimpulan yang dapat dimbil dari studi dan perbandingan antara *Nihilist Chiper* dan *Vigenere Chiper* ini adalah:

1. Algoritma klasik masih layak untuk dipelajari karena melalui itu kita dapat memahami konsep dasar kriptografi sekaligus mengetahui kelemahan sistem *cipher* yang ada.
2. *Nihilist Chiper* dan *Vigenere Chiper* merupakan jenis kriptografi klasik dengan chiper substitusi abjad-majemuk.
3. Percobaan penyerangan pada kedua *chiper* berhasil memecahkan chiperteks dengan sempurna. Namun, dari hasil ini tidak dapat dikatakan bahwa kedua chiper ini lemah karena chiperteks yang dijadikan objek penyerangan hanya mengimplementasikan panjang kunci yang relatif pendek yaitu 4 karakter.

4. Dari hasil perbandingan antara keduanya, *Nihilist Chiper* unggul dalam penggunaan bujursangkar *Polybius* yang bisa berubah tergantung kunci, namun sekaligus menjadi kelemahan karena tidak efektif di mana kriptografer harus memberitahukan bentuk bujursangkar tersebut kepada penerima pesan.
5. *Vigenere chiper* unggul lebih karena faktor sejarah di mana chiper ini sudah sangat dikenal sehingga mudah dipahami dan masih cukup aman untuk digunakan. Namun, chiper ini mudah diserang dengan metode Kasiski.

DAFTAR PUSTAKA

[1] Gaines, Helen Fouche. (1956). Cryptanalysis, Dover, New York.

[2] Munir, Rinaldi. (2006). *Diktat Kuliah IF5054 Kriptografi.* Program Studi Teknik Informatika, Institut Teknologi Bandung

[3] Piper, Fred and Sean Murphy. (2002). *Cryptography: A Very Short Introduction.* Oxford University Press.

[4] Scheneier, Bruce. (1996). *Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C.* John Wiley & Sons, Inc. New York.

[5] Http://en.wikipedia.org

[6] Http://answers.com

[7] Http://evercrack.cjb.cc/crypto/pmulti.html

[8] Http://math.utoledo.edu

[9] Http://www.nic.funet.fi/pub/crypt/

[10] Http://www.quadibloc.com/crypto/