BAB II

TINJAUAN PUSTAKA

II.1. Penelitian Terkait

Telah ada penelitian terdahulu yang terkait dengan penelitian yang penulis buat yang dapat dijadikan referensi bagi penulis, meskipun tidak memiliki kesamaan dalam judul, namun terdapat kesamaan dalam temuan yang ditargetkan. Penelitian tersebut adalah penelitian yang dilakukan oleh Koirul Amri, Anugrah Rizki E., Herman Sah Putra S., Sura Purna A. S., dan Suryadi Sudirja, pada tahun 2015, dalam jurnalnya yang berjudul "Aplikasi Enkripsi Dan Dekripsi Menggunakan Algoritma Vigenere Cipher ASCII Berbasis Java".

Di dalam jurnal ini diterangkan bahwa mereka membuat sebuah aplikasi yang mampu melakukan enkripsi dan dekripsi pada teks yang berisi angka, huruf ataupun tanda baca seperti titik, koma, dan lain-lain menggunakan Algoritma Vigenere Cipher. Perubahan pada rumus algoritmanya tidaklah jauh berbeda dibandingkan dengan rumus algoritma Vigenere Cipher yang aslinya. Perubahan yang dilakukan hanya pada bagian "mod" saja jika dalam rumus algoritma yang sebelumnya menggunakan mod 26 maka agar bisa mengenkripsi karakter yang ada dalam tabel kode ASCII menggunakan mod 256 karena menyesuaikan dengan jumlah karakter dan simbol yang terdapat dalam kode ASCII. Dan dalam penerapannya menggunakan pergeseran (shift) pada bagian kuncinya, yaitu pengurangan sebanyak 97 karakter. Tidak ada alasan yang mereka sebutkan mengapa mereka melakukan pergeseran tersebut, namun menurut penulis mereka

melakukan hal tersebut agar enkripsi dan dekripsinya tidak melampaui karakter yang berada pada nomor 0-127.

Dikarenakan penulis memberikan batasan pada karakter yang akan dienkripsi ataupun didekripsi, dan rumus pergeseran yang mereka gunakan juga masih kurang efektif maka penulis membuat sedikit perubahan hanya pada bagian mod saja dan tidak melakukan pergeseran. Berikut contoh dari rumus enkripsi dan dekripsinya :

a. Rumus enkripsi dan dekripsi berdasarkan jurnal acuan

   Enkripsi : C i = (P i + Ki) mod 256

   Dekripsi : P i = (C i - Ki) mod 256

   Rumus diatas adalah rumus sebelum dilakukan pergeseran, berikut contoh rumus yang sudah diberi pergeseran (shift) :

   Shift = Ki – 97

   Enkripsi : Ci = (Pi + shift) mod 256

b. Rumus enkripsi dan dekripsi berdasarkan yang penulis buat

   Enkripsi : Ci = (Pi + Ki) mod 128

   Dekripsi : P i = (C i - Ki) mod 128

   Untuk dekripsi, jika “Ci – Ki” hasilnya negatif maka “mod 128” diganti menjadi “+ 128”

Keterangan:

C i adalah nilai desimal karakter ciphertext ke-i

P i adalah nilai desimal karakter plaintext ke-i

K i adalah nilai desimal karakter kunci ke-i

shift adalah pergeseran

II.2. Uraian Teori

Adapun uraian teori yang berkaitan dengan penulisan skripsi ini dapat dilihat pada uraian dibawah ini :

II.2.1. Database

Database atau basis data adalah kumpulan data dan informasi yang tersimpan dan tersusun didalam komputer secara sistematik yang dapat diperiksa, diolah atau dimanipulasi dengan menggunakan suatu program komputer untuk mendapatkan informasi dari basis data tersebut. Perangkat lunak yang digunakan untuk mengolah dan memanggil database disebut dengan *Database Management System* (DBMS). Istilah *database* sendiri mengacu pada koleksi data-data yang saling terkait satu sma lain dimana tujuan database adalah untuk mengelola data dengan lebih efektif dan efisien. (Maxmanroe.com, 2019, https://www.maxmanroe.com/vid/teknologi/komputer/pengertian-database.html).

II.2.2. MySQL

MySQL adalah salah satu jenis *database server* yang terkenal, disebabkan MySQL menggunakan SQL sebagai bahasa dasar untuk mengakses database. MySQL termasuk RDBMS (*Relational Database Management System*) yang lebih populer lewat kalangan pemrograman web, terutama dilingkungan Linux. (Nugraha Saputra, 2017).

II.2.3. ASCII

Kode Standar Amerika untuk Pertukaran Informasi atau *American Standard Code for Information Interchange* (ASCII) merupakan suatu standar internasional dalam kode huruf dan simbol seperti *Unicode* dan *Hex* tetapi ASCII lebih bersifat universal, contohnya 124 adalah untuk karakter "|". Ia selalu digunakan oleh komputer dan alat komunikasi lain untuk menunjukkan teks.

Kode ASCII sebenarnya memiliki komposisi bilangan biner sebanyak 7 bit. Namun, ASCII disimpan sebagai sandi 8 bit dengan menambakan satu angka 0 sebagai bit significant paling tinggi. Bit tambahan ini sering digunakan untuk uji paritas. Karakter control pada ASCII dibedakan menjadi 5 kelompok sesuai dengan penggunaan yaitu berturut-turut meliputi l*ogical communication, Device control, Information separator, Code extention,* dan *physical communication.* Code ASCII ini banyak dijumpai pada papan ketik (keyboard) computer atau instrument-instrument digital.

Jumlah kode ASCII adalah 255 kode. Kode ASCII 0..127 merupakan kode ASCII untuk manipulasi teks; sedangkan kode ASCII 128..255 merupakan kode ASCII untuk manipulasi grafik. Kode ASCII sendiri dapat dikelompokkan lagi kedalam beberapa bagian:

- Kode yang tidak terlihat simbolnya seperti Kode 8 (Backspace), 10 (pergantian baris/Line Feed), 13 (pergantian baris/Carriage Return), 32(Space).
- Kode yang terlihat simbolnya seperti numerik (0..9), abjad (A..Z), karakter khusus (~!@#$%^&*()_+?:”{}).

- Kode yang tidak ada di keyboard namun dapat ditampilkan. Kode ini umumnya untuk kode-kode grafik.

(MateriDosen, 2016, http://www.materidosen.com/2016/10/pengertian-dan-funsi-kode-ascii-lengkap.html?m=1).

Tabel II.1. Code ASCII

Nilai ANSI ASCII (Desimal)	Nilai Unicode (Heksa Desimal)	Karakter	Keterangan
0	0000	NUL	Null (tidak terlihat)
1	0001	SOH	Start of heading (tidak terlihat)
2	0002	STX	Start of text (tidak terlihat)
3	0003	ETX	End of text (tidak terlihat)
4	0004	EOT	End of transmission (tidak terlihat)
5	0005	ENQ	Enquiry (tidak terlihat)
6	0006	ACK	Acknowledge (tidak terlihat)
7	0007	BEL	Bell (tidak terlihat)
8	0008	BS	Backspace
9	0009	HT	Horizontal tabulation
10	000A	LF	Pergantian baris (Line feed)
11	000B	VT	Tabulasi vertikal
12	000C	FF	Pergantian baris (Form feed)
13	000D	CR	Pergantian baris (carriage return)
14	000E	SO	Shift out (tidak terlihat)
15	000F	SI	Shift in (tidak terlihat)
16	0010	DLE	Data link escape (tidak terlihat)
17	0011	DC1	Device control 1 (tidak terlihat)
18	0012	DC2	Device control 2 (tidak terlihat)
19	0013	DC3	Device control 3

			(tidak terlihat)
20	0014	DC4	Device control 4 (tidak terlihat)
21	0015	NAK	Negative acknowledge (tidak terlihat)
22	0016	SYN	Synchronous idle (tidak terlihat)
23	0017	ETB	End of transmission block (tidak terlihat)
24	0018	CAN	Cancel (tidak terlihat)
25	0019	EM	End of medium (tidak terlihat)
26	001A	SUB	Substitute (tidak terlihat)
27	001B	ESC	Escape (tidak terlihat)
28	001C	FS	File separator
29	001D	GS	Group separator
30	001E	RS	Record separator
31	001F	US	Unit separator
32	0020	Spasi	Spasi
33	0021	!	Tanda seru (exclamation)
34	0022	“	Tanda kuti dua
35	0023	#	Tanda pagar (kres)
36	0024	$	Tanda mata uang dolar
37	0025	%	Tanda persen
38	0026	&	Karakter ampersand (&)
39	0027	‘	Karakter Apostrof
40	0028	(	Tanda kurung buka
41	0029	)	Tanda kurung tutup
42	002A	*	Karakter asterisk (bintang)
43	002B	+	Tanda tambah (plus)
44	002C	,	Karakter koma
45	002D	-	Karakter hyphen (strip)
46	002E	.	Tanda titik
47	002F	/	Garis miring (slash)
48	0030	0	Angka nol
49	0031	1	Angka satu

50	0032	2	Angka dua
51	0033	3	Angka tiga
52	0034	4	Angka empat
53	0035	5	Angka lima
54	0036	6	Angka enam
55	0037	7	Angka tujuh
56	0038	8	Angka delapan
57	0039	9	Angka sembilan
58	003A	:	Tanda titik dua
59	003B	;	Tanda titik koma
60	003C	<	Tanda lebih kecil
61	003D	=	Tanda sama dengan
62	003E	>	Tanda lebih besar
63	003F	?	Tanda tanya
64	0040	@	A keong (@)
65	0041	A	Huruf latin A kapital
66	0042	B	Huruf latin B kapital
67	0043	C	Huruf latin C kapital
68	0044	D	Huruf latin D kapital
69	0045	E	Huruf latin E kapital
70	0046	F	Huruf latin F kapital
71	0047	G	Huruf latin G kapital
72	0048	H	Huruf latin H kapital
73	0049	I	Huruf latin I kapital
74	004A	J	Huruf latin J kapital
75	004B	K	Huruf latin K kapital
76	004C	L	Huruf latin L kapital
77	004D	M	Huruf latin M kapital
78	004E	N	Huruf latin N kapital
79	004F	O	Huruf latin O kapital
80	0050	P	Huruf latin P kapital
81	0051	Q	Huruf latin Q kapital
82	0052	R	Huruf latin R kapital
83	0053	S	Huruf latin S kapital

84	0054	T	Huruf latin T kapital
85	0055	U	Huruf latin U kapital
86	0056	V	Huruf latin V kapital
87	0057	W	Huruf latin W kapital
88	0058	X	Huruf latin X kapital
89	0059	Y	Huruf latin Y kapital
90	005A	Z	Huruf latin Z kapital
91	005B	[	Kurung siku kiri
92	005C	/	Garis miring terbalik (*backslash*)
93	005D	]	Kurung sikur kanan
94	005E	^	Tanda pangkat
95	005F	_	Garis bawah (underscore)
96	0060	`	Tanda petik satu
97	0061	A	Huruf latin a kecil
98	0062	B	Huruf latin b kecil
99	0063	C	Huruf latin c kecil
100	0064	D	Huruf latin d kecil
101	0065	E	Huruf latin e kecil
102	0066	F	Huruf latin f kecil
103	0067	G	Huruf latin g kecil
104	0068	H	Huruf latin h kecil
105	0069	I	Huruf latin i kecil
106	006A	J	Huruf latin j kecil
107	006B	K	Huruf latin k kecil
108	006C	L	Huruf latin l kecil
109	006D	M	Huruf latin m kecil
110	006E	N	Huruf latin n kecil
111	006F	O	Huruf latin o kecil
112	0070	P	Huruf latin p kecil
113	0071	Q	Huruf latin q kecil
114	0072	R	Huruf latin r kecil
115	0073	S	Huruf latin s kecil
116	0074	T	Huruf latin t kecil

117	0075	U	Huruf latin u kecil
118	0076	V	Huruf latin v kecil
119	0077	W	Huruf latin w kecil
120	0078	X	Huruf latin x kecil
121	0079	Y	Huruf latin y kecil
122	007A	Z	Huruf latin z kecil
123	007B	{	Kurung kurawal buka
124	007C	|	Garis vertikal (pipa)
125	007D	}	Kurung kurawal tutup
126	007E	~	Karakter gelombang (tilde)
127	007F	DEL	Delete
128	0080	€	Euro sign
129	0081		
130	0082	‚	Single low-9 quotation mark
131	0083	Ƒ	Latin small letter f with hook
132	0084	„	Double low-9 quotation mark
133	0085	…	Horizontal ellipsis
134	0086	†	Dagger
135	0087	‡	Double dagger
136	0088	ˆ	Modifier letter circumflex accent
137	0089	‰	Per mille sign
138	008A	Š	Latin capital letter S with caron
139	008B	‹	Single left-pointing angle quotation
140	008C	Œ	Latin capital ligature OE
141	008D		
142	008E	Ž	Latin captial letter Z with caron
143	008F		
144	0090		
145	0091	‘	Left single quotation mark
146	0092	’	Right single quotation mark
147	0093	“	Left double quotation mark

148	0094	”	Right double quotation mark
149	0095	•	Bullet
150	0096	–	En dash
151	0097	—	Em dash
152	0098	˜	Small tilde
153	0099	™	Trade mark sign
154	009A	Š	Latin small letter S with caron
155	009B	›	Single right-pointing angle quotation mark
156	009C	Œ	Latin small ligature oe
157	009D		
158	009E	Ž	Latin small letter z with caron
159	009F	Ÿ	Latin capital letter Y with diaeresis
160	00A0		Spasi yang bukan pemisah kata
161	00A1	¡	Tanda seru terbalik
162	00A2	¢	Tanda sen (Cent)
163	00A3	£	Tanda Poundsterling
164	00A4	¤	Tanda mata uang (Currency)
165	00A5	¥	Tanda Yen
166	00A6	¦	Garis tegak putus-putus
167	00A7	§	Section sign
168	00A8	¨	Spacing diaeresis - umlaut
169	00A9	©	Tanda hak cipta (Copyright)
170	00AA	ª	Feminine ordinal indicator
171	00AB	«	Left double angle quotes
172	00AC	¬	Not sign
173	00AD		Tanda strip (hyphen)
174	00AE	®	Tanda merk terdaftar
175	00AF	¯	Spacing Macron (Macron)
176	00B0	°	Tanda derajat
177	00B1	±	Tanda kurang lebih (plus-minus)
178	00B2	²	Tanda kuadrat (pangkat dua)

179	00B3	³	Tanda kubik (pangkat tiga)
180	00B4	´	Acute accent
181	00B5	µ	Micro sign
182	00B6	¶	Pilcrow sign
183	00B7	·	Middle dot
184	00B8	¸	Spacing cedilla
185	00B9	¹	Superscript one
186	00BA	º	Masculine ordinal indicator
187	00BB	»	Right double angle quotes
188	00BC	¼	Fraction one quarter
189	00BD	½	Fraction one half
190	00BE	¾	Fraction three quarters
191	00BF	¿	Inverted question mark
192	00C0	À	Latin capital letter A with grave
193	00C1	Á	Latin capital letter A with acute
194	00C2	Â	Latin capital letter A with circumflex
195	00C3	Ã	Latin capital letter A with tilde
196	00C4	Ä	Latin capital letter A with diaeresis
197	00C5	Å	Latin capital letter A with ring above
198	00C6	Æ	Latin capital letter AE
199	00C7	Ç	Latin capital letter C with cedilla
200	00C8	È	Latin capital letter E with grave
201	00C9	É	Latin capital letter E with acute
202	00CA	Ê	Latin capital letter E with circumflex
203	00CB	Ë	Latin capital letter E with diaeresis
204	00CC	Ì	Latin capital letter I with grave

205	00CD	Í	Latin capital letter I with acute
206	00CE	Î	Latin capital letter I with circumflex
207	00CF	Ï	Latin capital letter I with diaeresis
208	00D0	Ð	Latin capital letter ETH
209	00D1	Ñ	Latin capital letter N with tilde
210	00D2	Ò	Latin capital letter O with grave
211	00D3	Ó	Latin capital letter O with acute
212	00D4	Ô	Latin capital letter O with circumflex
213	00D5	Õ	Latin capital letter O with tilde
214	00D6	Ö	Latin capital letter O with diaeresis
215	00D7	×	Multiplication sign
216	00D8	Ø	Latin capital letter O with slash
217	00D9	Ù	Latin capital letter U with grave
218	00DA	Ú	Latin capital letter U with acute
219	00DB	Û	Latin capital letter U with circumflex
220	00DC	Ü	Latin capital letter U with diaeresis
221	00DD	Ý	Latin capital letter Y with acute
222	00DE	Þ	Latin capital letter THORN
223	00DF	ß	Latin small letter sharp s - ess-zed
224	00E0	à	Latin small letter a with grave
225	00E1	á	Latin small letter a with acute
226	00E2	â	Latin small letter a with circumflex
227	00E3	ã	Latin small letter a with tilde

228	00E4	Ä	Latin small letter a with diaeresis
229	00E5	Å	Latin small letter a with ring above
230	00E6	Æ	Latin small letter ae
231	00E7	Ç	Latin small letter c with cedilla
232	00E8	È	Latin small letter e with grave
233	00E9	É	Latin small letter e with acute
234	00EA	Ê	Latin small letter e with circumflex
235	00EB	Ë	Latin small letter e with diaeresis
236	00EC	Ì	Latin small letter i with grave
237	00ED	Í	Latin small letter i with acute
238	00EE	Î	Latin small letter i with circumflex
239	00EF	Ï	Latin small letter i with diaeresis
240	00F0	Đ	Latin small letter eth
241	00F0	Ñ	Latin small letter n with tilde
242	00F0	Ò	Latin small letter o with grave
243	00F0	Ó	Latin small letter o with acute
244	00F0	Ô	Latin small letter o with circumflex
245	00F0	Õ	Latin small letter o with tilde
246	00F0	Ö	Latin small letter o with diaeresis
247	00F0	÷	Division sign
248	00F0	Ø	Latin small letter o with slash
249	00F0	Ù	Latin small letter u with grave
250	00F0	Ú	Latin small letter u with acute
251	00F0	Û	Latin small letter u with circumflex
252	00F0	Ü	Latin small letter u with diaeresis

253	00F0	Ý	Latin small letter y with acute
254	00F0	Þ	Latin small letter thorn
255	00F0	Ÿ	Latin small letter y with diaeresis

(Sumber : MateriDosen, 2016)

II.2.4. Vigenere Cipher

Pada bagian ini penulis akan menjelaskan apa itu Vigenere Cipher, dan penulis akan membedakan Vigenere Cipher yang masih original dengan yang menggunkan Code ASCII. Berikut penjelasannya.

II.2.4.1. Vigenere Cipher Original

Vigenere Cipher merupakan pengembangan dari *Caesar Cipher* dimana dasar dari algoritma ini adalah beberapa huruf dari kata kunci yang diambil dari pergeseran yang dilakukan oleh *Caesar Cipher*. Pada dasarnya *Vigenere Cipher* serupa dengan *Caesar Cipher*, perbedaannya adalah pada *Vigenere Cipher* setiap huruf pesan aslinya digeser sebanyak satu huruf pada kuncinya sedangkan *Caesar Cipher* setiap huruf pesannya digeser sebanyak 1 huruf yang sama. Metode ini menggunakan kode abjad majemuk (*polyalphabetic substitution cipher*) yang melibatkan penggunaan 2 atau lebih *cipher alphabet*, hal ini untuk membuat *cipher* lebih aman. Ini adalah bentuk sederhana dari abjad-majemuk dimana setiap *alphabet* dapat diganti dengan beberapa huruf *cipher alphabet*. *Vigenere Cipher* pertama kali diusulkan oleh *Blaise de Vigenere* dari pengadilan Henry III di Perancis pada abad 16. Nama vigenere diambil sebagai nama algoritma ini karena beliau menemukan kunci yang lebih kuat lagi untuk algoritma dengan metode

autokey cipher meskipun algoritma dasarnya telah ditemukan lebih dulu oleh Giovan Battista Bellaso. Algoritma enkripsi jenis ini sangat dikenal karena mudah dipahami dan diimplementasikan. Teknik untuk menghasilkan *ciphertext* bisa dilakukan menggunakan substitusi angka maupun bujur sangkar *vigenere*. Teknik substitusi *vigenere* dengan menggunakan angka dilakukan dengan menukarkan huruf dengan angka, hampir sama dengan kode geser. Setiap baris di dalam bujur sangkar menyatakan huruf-huruf ciphertext yang diperoleh dengan *Caesar Cipher*.

Contoh, misalkan *plaintext* dengan huruf P disandikan dengan kunci K, maka hasil *ciphertext* yang dihasilkan adalah huruf Z. Proses enkripsi dilakukan hingga setiap karakter pada pesan memiliki pasangan sebuah karakter dari kunci. pengaturan karakter yang lebih besar memungkinkan lebih banyak jenis pesan yang dienkripsi seperti kata sandi. Hal tersebut, juga meningkatkan domain kunci dan memberikan keamanan yang lebih pada kata. apabila metode *Vigenere Chiper* ini ditranslasikan ke dalam suatu algoritma pemograman, secara sederhana, notasi algoritmik yang digunakan untuk mengenkripsi suatu karakter *alphabet plaintext* (P) menjadi *chipertext* (C) dengan kunci K adalah sebagai berikut :

$$C_i = EK\,(P_i) = (P_i + K_i)\ mod\ 26$$

C_i merupakan ciphertext dari pergeseran karakter yang terdapat pada plaintext. P_i merupakan pergeseran karakter pada plaintext. K_i merupakan kunci berupa hasil konversi tabel berbentuk bilangan desimal dari pergeseran karakter yang terdapat pada kunci yang digunakan. Proses dekripsi menggunakan Vigenere Cipher membutuhkan satu buah kunci untuk dapat menghasilkan plaintext. Kunci

yang digunakan merupakan kunci yang sama dengan kunci yang digunakan pada proses enkripsi. Selain mengkonversi kunci yang digunakan, Vigenere Cipher juga harus mengkonversi ciphertext menggunakan tabel konversi yang juga menghasilkan bilangan desimal, kemudian plaintext akan diperoleh dengan mendekripsi plaintext dengan persamaan.

$$P_i = DK\,(C_i) = (C_i + K_i)\ mod\ 26$$

P_i merupakan plaintext dari pergeseran karakter yang terdapat pada ciphertext. C_i merupakan pergeseran karakter pada ciphertext. K_i merupakan kunci berupa hasil konversi tabel berupa bilangan desimal dari pergeseran karakter yang terdapat pada kunci yang digunakan. P_i dapat dilakukan dengan terlebih dahulu mengurangi nilai C_i dengan nilai K_i. Hasil dari pengurangan akan dijumlahkan dengan angka 26 untuk kemudian hasil penjumlahan akan dimodulo 26.

Jika panjang kunci lebih pendek daripada plaintext, maka kunci diulang secara periodik. Bila panjang kunci adalah m, maka periodenya dikatakan m. Sebagai contoh proses enkripsi dekripsi, misalkan plaintext yang akan dienkripsi adalah MAKALAH KRIPTOGRAFI dengan kunci yang telah ditetapkan bersama, yaitu VIGENERE. Kunci akan diulang secara periodik sesuai dengan plaintext terlebih dahulu sebagai berikut.

Plainteks : MAKALAHKRIPTOGRAFI

Kunci : V I GENEREVIGENEREVI

Untuk huruf pertama M, tarik garis vertikal dari huruf M dan tarik garis horizontal dari huruf V, perpotongannya adalah pada kotak yang berisi huruf H (Tabel 1). Dengan cara yang sama, tarik garis vertikal A dan tarik garis horizontal I,

perpotongannya adalah pada kotak yang juga berisi huruf I. Berlaku juga untuk huruf selanjutnya. Hasil enkripsi seluruhnya adalah sebagai berikut :

Plainteks : MAKALAHKRIPTOGRAFI

Kunci : VIGENEREVIGENEREVI

Ciphertext : HIQEYEOMQVXBKIEAQ

Tabel II.2. Enkripsi Huruf M Dengan Kunci V Dan A Dengan Kunci I

	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
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

(Sumber : Rahmanita Syahdan dan Erni Anitasari, 2017)

Tabel ini terdiri dari karakter alphabet yang ditulis 26 kali dalam baris yang berbeda, setiap alphabet secara siklis bergeser ke kiri, menghasilkan 26 kombinasi *Caesar Cipher*. Kolom paling kiri menyatakan huruf-huruf kunci, sedangkan baris paling pertama menyatakan huruf-huruf *plaintext*. Bujursangkar *vigenere* digunakan untuk memperoleh ciphertext dengan menggunakan kunci yang sudah

ditentukan. Karakter huruf yang digunakan pada *Vigenere Cipher* yaitu A, B, C, ..., Z dan disamakan dengan 0, 1, 2, ..., 25. Pada *cipher* substitusi sederhana, setiap huruf *ciphertext* selalu menggantikan huruf *plaintext* tertentu, sedangkan pada *cipher* alphabet-majemuk setiap huruf *ciphertext* dapat memiliki kemungkinan banyak huruf *plaintext*. *Vigenere Cipher* dapat mencegah frekuensi huruf-huruf di dalam *ciphertext* yang mempunyai pola tertentu yang sama seperti pada *cipher* abjad-tunggal. Untuk contoh di atas maka pendeskripsiannya adalah sebagai berikut:

Kunci : VIGENEREVIGENEREVI

Ciphertext : HIQEYEOMQVXBKIEAQ

Untuk karakter yang pertama, huruf V maka akan dicari seluruh isi karakter yang berada pada kolom huruf V ke bawah, dimana terdapat karakter ciphertext huruf H, maka dilihat pada kolom kunci yang menunjukkan bahwa huruf H tersebut berada pada baris huruf M. Berlaku juga pada karakter selanjutnya dalam kunci tersebut. Demikian cara kerja proses deskripsi mencari plaintext seperti yang ditunjukkan dalam Tabel 2 berikut. (Rahmanita Syahdan dan Erni Anitasari, 2017)

Tabel II.3/ Deskripsi Huruf M Dengan Kunci V Dan A Dengan Kunci I

	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
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

(Sumber : Rahmanita Syahdan dan Erni Anitasari, 2017)

II.2.4.1. Vigenere Cipher Dengan Code ASCII

Dalam penerapannya tidak terlalu banyak perubahan yang dipakai untuk mengubah rumus enkripsi dan dekripsi dari rumus vigenere cipher tersebut. Bagian yang diubah disini hanya pada bagian mod saja. Jika di vigenere cipher yang biasa menggunakan mod 26, maka disini mod yang digunakan adalah 256.

Berikut rumus enkripsi dan dekripsi vigenere cipher:

Enkripsi

$C\ i = (P\ i + K) \bmod 256$

Dekripsi

$P\ i = (C\ i - K) \bmod 256$

Keterangan:

C i adalah nilai desimal karakter ciphertext ke-i

P i adalah nilai desimal karakter plaintext ke-i

K adalah nilai desimal karakter kunci ke-i

mod 256 adalah karena berdasarkan ASCII

Misal Pada Vigenere Cipher kunci K adalah urutan huruf-huruf K = k.....kd dimana ki didapat dari banyak penggeseran pada karakter ACII ke-i. Berikut adalah formula vigenere cipher :

Misalnya m menentukan beberapa nilai integer positif diberikan P = C = K = (Z 97) m . untuk sebuah kunci K=(k1,k2,.....,km), didefinisikan :

Enkripsi :

ek (p1, p2 ... pm) = (p1 + k1, p2 + k2 ... pm + km) (mod 26)

Dekripsi :

dk (c1, c2 ... cm) = (c1-k1, c2-k2 ... cm-km) (mod 26)

Contoh :

Plaintext : HANTAM MEREKA

KEY : BOMBOMBOMBOMB

Ciphertext :)/:5/9 ;1337"

Berdasarkan contoh yang mereka buat, dari segi rumusnya mereka hanya melakukan perubahan pada modnya saja tetapi untuk programnya mereka melakukan shift (pergeseran) dengan cara pengurangan sebanyak 97 digit, tidak ada alasan pasti disebutkan oleh para penyusunnya, untuk lebih jelasnya bisa dilihat pada penjelasan dibawah ini.

Plaintext : HANTAM MEREKA

Key : BOMBOMBOMBOMB

Ciphertext :)/:5/9ı;1337" (angka 1 kecil tersebut adalah ASCII ke 1 “SOH”)

Rumus enkripsi : Ci = (Pi + Ki) mod 256

- H = 72
  - shift = nilai desimal kunci (B) – 97
    = 66 - 97
    = -31
  - Ci = (72 + shift) mod 256
    = (72 - 31) mod 256
    = 41
  - Nilai desimal 41 di tabel ASCII mempunyai karakter “) “
- A = 65
  - shift = nilai desimal kunci (O) – 97
    = 79 - 97
    = -18
  - Ci = (65 + shift) mod 256
    = (65 - 18) mod 256
    = 47
  - nilai desimal 47 di tabel ASCII mempunyai karakter “ / “
- N = 78
  - shift = nilai desimal kunci (M) – 97
    = 77 - 97

= -20

- Ci = (78 + shift) mod 256

  = (78 - 20) mod 256

  = 58

- nilai desimal 58 di tabel ASCII mempunyai karakter “ : “

- T = 84
  - shift = nilai desimal kunci (B) – 97

    = 66 - 97

    = -31

  - Ci = (84 + shift) mod 256

    = (84 - 31) mod 256

    = 53

  - nilai desimal 53 di tabel ASCII mempunyai karakter “ 5 “
- A = 65
  - shift = nilai desimal kunci (O) – 97

    = 79 - 97

    = -18

  - Ci = (65 + shift) mod 256

    = (65 - 18) mod 256

    = 47

  - nilai desimal 47 di tabel ASCII mempunyai karakter “ / “
- M = 77
  - shift = nilai desimal kunci (M) – 97

= 77 - 97

= -20

- Ci = (77 + shift) mod 256

= (77 - 20) mod 256

= 57

- nilai desimal 57 di tabel ASCII mempunyai karakter “ 9 “

- Spasi = 32
  - shift = nilai desimal kunci (B) – 97

    = 66 - 97

    = -31
  - Ci = (32 + shift) mod 256

    = (32 - 31) mod 256

    = 1
  - nilai desimal 1 di tabel ASCII mempunyai karakter “ SOH “
- M = 77
  - shift = nilai desimal kunci (O) – 97

    = 79 - 97 = -18
  - Ci = (77 + shift) mod 256

    = (77 - 18) mod 256

    = 59
  - nilai desimal 59 di tabel ASCII mempunyai karakter “ ; “
- E = 69
  - shift = nilai desimal kunci (M) – 97

= 77 - 97

= -20

- Ci = (69 + shift) mod 256

= (69 - 20) mod 256

= 49

- nilai desimal 49 di tabel ASCII mempunyai karakter “ 1 “

- R = 82
  - shift = nilai desimal kunci (B) – 97

= 66 - 97

= -31

  - Ci = (82 + shift) mod 256

= (82 - 31) mod 256

= 51

  - nilai desimal 51 di tabel ASCII mempunyai karakter “ 3 “
- E = 69
  - shift = nilai desimal kunci (O) – 97

= 79 - 97

= -18

  - Ci = (69 + shift) mod 256

= (69 - 18) mod 256

= 51

  - nilai desimal 51 di tabel ASCII mempunyai karakter “ 3 “
- K = 75

- shift = nilai desimal kunci (M) – 97

  = 77 - 97

  = -20

- Ci = (75 + shift) mod 256

  = (75 - 20) mod 256

  = 55

- nilai desimal 49 di tabel ASCII mempunyai karakter “ 7 “

- A = 65
  - shift = nilai desimal kunci (B) – 97

    = 66 - 97

    = -31

  - Ci = (65 + shift) mod 256

    = (65 - 31) mod 256

    = 34

  - nilai desimal 34 di tabel ASCII mempunyai karakter “ " “

Jadi, Plaintext “HANTAM MEREKA” dengan kunci “BOM” mempunyai ciphertext)/:5/9ı;1337".