Venigmarè Cipher dan *Vigenère Cipher*

Unggul Satrio Respationo – NIM : 13506062

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if16062@students.if.itb.ac.id

Abstrak

Vigenère Cipher adalah enkripsi yang mampu mengurangi korelasi antara frekuensi huruf pada *plaintext* dan *Ciphertext*. Tetapi sayangnya metode ini masih menyisakan pola yang berulang, apalagi jika *plaintext* yang di enkripsi cukup panjang. Hal ini dikarenakan tabel yang relatif sama dan penggunaan kunci yang lebih pendek dari *plaintext*. Dan juga metode ini hanya bisa digunakan untuk mengenkripsi karakter. Perlu metoda tambahan untuk mengenkripsi selain karakter. Akan tetapi metode ini yang sering digunakan karena mudah untuk diimplementasikan.

Terinspirasi dari mesin *Enigma* yang melakukan rotasi roda gigi huruf setiap selesai melakukan enkripsi 1 huruf, maka penulis mencoba untuk melakukan modifikasi terhadap *Vigenère Cipher* menggunakan metoda yang sama. Metoda ini nantinya akan menggeser tabel alfabetis setiap selesai melakukan enkripsi terhadap 1 huruf. Metoda ini penulis beri nama sebagai "*Venigmarè Cipher*".

Masalah yang akan dibahas dalam makalah ini adalah bagaimana keamanan dari metoda hasil penelitian ini. Pengecekan dengan cara meneliti korelasi antara jumlah frekuensi pada *plaintext* dan *ciphertext*, serta pemunculan pola pada *ciphertext* atau yang biasa dikenal sebagai *Kasiski Examination*.

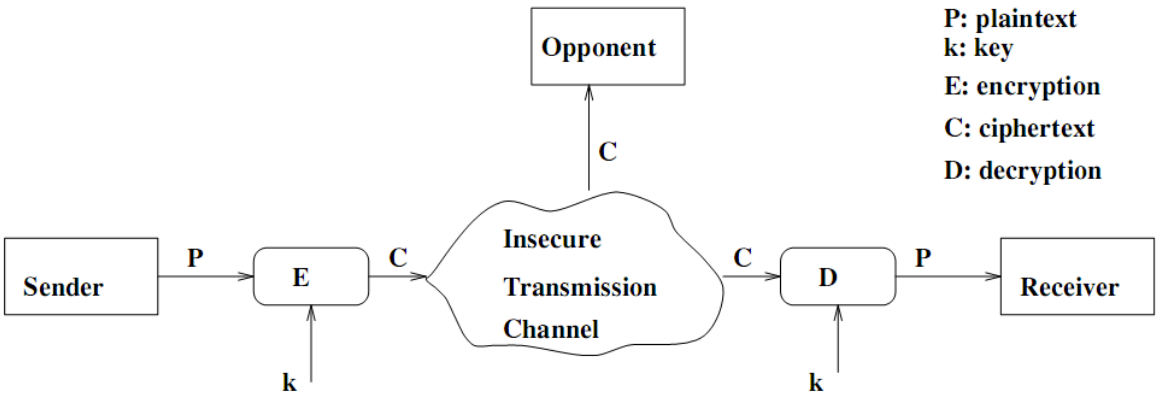
***Kata kunci**: Vigenère Cipher, Enigma, Wrapping*, Enkripsi, Dekripsi, Kasiski.

1. PENDAHULUAN

Kriptografi adalah bidang yang mempunyai pengaruh besar dalam bidang informatika, terutama pada bagian *security* (keamanan). Tentunya tidak hanya digunakan dalam bidang informatika saja, tetapi juga dalam hal komunikasi, transfer data, bahkan dalam dunia militer juga diperlukan teknik enkripsi yang baik agar data dapat dengan aman dikirimkan tanpa gangguan dari luar. Enkripsi dan dekripsi adalah proses utama dalam melakukan pengamanan terhadap data. Kriptosistem[1] oleh C.E. Shannon dapat diformulasikan sebagai pasangan 5-tuple[2] yaitu (*P;K; C; E;D*) dimana *P* adalah himpunan plainteks, *K* adalalah himpunan kunci, *C* adalah himpunan cipherteks, untuk setiap $k \in K$, terdapat aturan enkripsi $E_k \in E$ dan inversnya (dekripsi) $D_k \in D$.

Aturan enkripsi adalah fungsi satu-satu yang mengambil pesan plainteks apapun, $p \in P$, dan mentranformasikannya kedalam bentuk yang tidak dapat dibaca yang disebut cipherteks yang ditujukan untuk menyembunyikan pesan. Aturan dekripsi mengembalikan plainteks original dari cipherteks yang diberikan. Sebuah model kriptosistem yang sederhana ditunjukkan oleh gambar 1.

Kriptosistem dapat dibedakan menjadi 2 macam



Gambar 1 Model sederhana dari metode kriptosistem umum

yaitu *symmetric cryptosystem* dan *public key cryptosystem*[3]. Kriptosistem simetri adalah dimana pada saat enkripsi dan dekripsi menggunakan kunci yang sama yang hanya diketahui pengirim dan penerima. Sedangkan pada kriptosistem kunci publik, terdapat kunci enkripsi yang diberikan kepada publik sehingga semua orang bisa menggunakannya. Tetapi kunci untuk dekripsi hanya diketahui oleh penerima pesan. Termasuk di dalam kriptosistem simetri adalah Vigenère cipher yang sudah sangat terkenal dan luas penggunaannya.

Vigenère cipher cukup lama digunakan sebelum berhasil dipecahkan oleh seorang kriptanalis yang bernama Kasiski. Akan tetapi karena algoritma ini cukup *simple* dan mudah diimplementasikan masih banyak yang menggunakannya dalam berbagai aplikasi. Untuk itu telah banyak yang mencoba untuk memvariasikan algoritma ini.

Untuk itu diperlukan berbagai algoritma tambahan yang dapat diterapkan ke dalam Vigenère cipher ini agar menambah tingkat kekebalannya terhadap serangan. Tentunya hal ini merupakan suatu tantangan yang cukup menarik untuk dikembangkan.

2. VIGENÈRE CIPHER

2.1. Enkripsi dan dekripsi

Vigenère cipher diberikan nama sesuai dengan *Blaise de Vigenère*. Akan tetapi sebenarnya metode ini pertama kali dikenalkan oleh *Giovan Batista Bellaso*. Pada masanya (abad ke-16) metode ini termasuk yang paling kuat. Tetapi pada abad ke-19 seorang ilmuwan bernama *Kasiski* berhasil memecahkan algoritma ini. Bahkan pada abad ke-16 seorang kriptanalis telah mampu memecahkannya. Untuk itu banyak yang telah mengembangkan metode ini agar tidak bisa diserang dengan mudah menggunakan metode kasiski.

Vigenère cipher termasuk ke dalam metode enkripsi dengan substitusi sama halnya dengan *Caesar Cipher*. Pada caesar cipher tiap huruf disubstitusikan dengan huruf yang sama. Jika tiap huruf A…Z dapat direpresentasikan dengan huruf 1…26 maka caesar cipher dapat dituliskan dengan formula :

$$\boldsymbol{Enkripsi}: \boldsymbol{c_i = E(p_i) = (p_i + k) mod\ 26}$$

$$\boldsymbol{Dekripsi}: \boldsymbol{p_i = E(c_i) = (c_i - k) mod\ 26}$$

Dimana *k* adalah banyaknya pergeseran huruf pada tabel kunci. Maka yang perlu dirahasiakan dalam metode enkripsi ini hanyalah *k.* Jika ingin diimplementasikan dalam ASCII maka cukup mengganti *mod 26* dengan *mod 256.* Jika diberikan sebuah plainteks ATTACKATDAWN, dan dienkripsikan dengan caesar cipher dengan *k* sebesar 3 maka akan menghasilkan cipherteks DWWDFNDWGDZQ.

p	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
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	C

Gambar 2 Tabel *Caesar Cipher* dengan pergeseran sebesar 3

Vigenère cipher menggunakan prinsip caesar cipher dalam implementasiannya. Yaitu tiap huruf dalam plainteks akan dikenakan fungsi substitusi tapi dengan *k* yang berbeda tergantung kunci. Untuk melakukan enkripsi digunakan suatu tabel huruf yang disebut *tabula recta*, *Vigenère square*, atau *Vigenère table.* Tabel initerdiri dari matriks huruf sejumlah 26 x 26. Nantinya tabel ini digunakan untuk mencari huruf yang bersesuaian dengan plainteksnya berdasarkan huruf pada kunci. Jika panjang kunci kurang dari plainteks, maka panjang kunci akan diulang.

	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

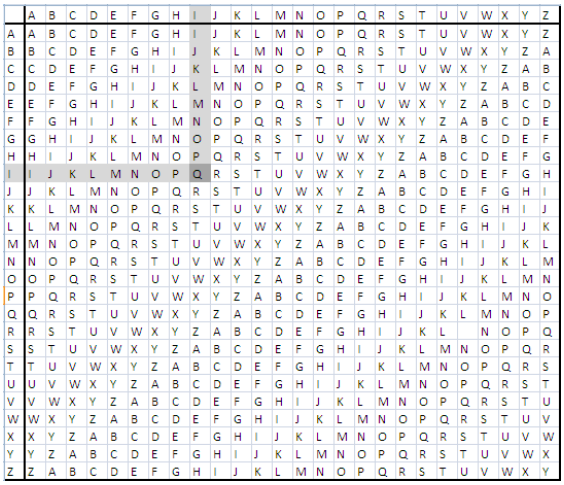
Gambar 3 Tabula Recta

Jika menggunakan persamaan maka secara umum algoritma enkripsi dan dekripsi dapat dituliskan sebagai berikut :

$$Enkripsi: C_i \equiv (P_i + K_i) mod\ 26$$

$$Dekripsi: P_i \equiv (C_i - K_i) mod\ 26$$

Maka jika kita mengenkripsikan plainteks ATTACKATDAWN dengan kunci LEMON yang akan diperpanjang dengan pengulangan kata sehingga menjadi sama panjang dengan plainteks akan menghasilkan cipherteks LXFOPVEFRNHR. Jika dibandingkan dengan metode caesar cipher yang menghasilkan DWWDFNDWGDZQ, metode Vigenère telah mengurangi pngulangan huruf yang bersesuaian dengan plainteks semula.



	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 4 Penggunaan Tabula Recta

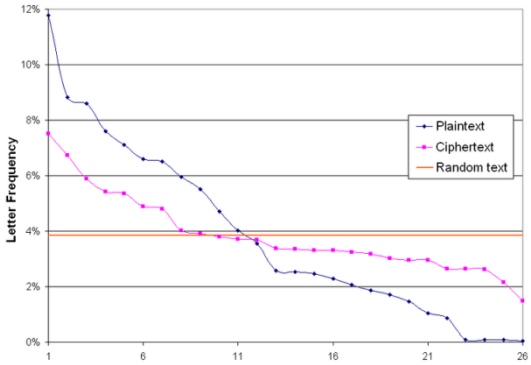
2.2. Serangan pada Vigenère cipher

Tujuan utama dari Vigenère cipher adalah menghilangkan frekuensi huruf cipherteks yang bersesuaian dengan plainteks. Jika dengan analisis frekuensi pada caesar cipher ditemukan bahwa P adalah huruf terbanyak dalam cipherteks, dan kriptanalis tahu plainteks dalam bahasa inggris maka kriptanalis dapat menerka bahwa P adalah E. Dengan Vigenère cipher hal ini dapat dikurangi. Grafik di bawah menunjukkan berkurangnya korelasi huruf antara plaintekx dan cipherteks.

Akan tetapi jika kita dapat mengetahui panjang kunci, maka dengan mudah kita dapat menerapkan teknik analisi frekuensi untuk setiap huruf sepanjang kunci. Hal inilah yang mendasari metode kasiski untuk memecahkan metode Vigenère cipher ini.

Pada metode kasiski (*Kasiski Examination)* dilakukan pencarian kata yang berulang pada cipherteksnya. Kemudian kata yang berulang itu kita asumsikan sebagai kata yang sama, sehingga jarak antara kedua kata tersebut faktor-faktornya adalah panjang kunci.

```
Key:        ABCDAB CD ABCDA BCD ABCDABCDABCD
Plaintext:  CRYPTO IS SHORT FOR CRYPTOGRAPHY
Ciphertext: CSASTP KV SIQUT GQU CSASTPIUAQJB
```



Gambar 5 Korelasi frekuensi huruf

Pada contoh di atas dapat dilihat bahwa kata CRYPTO terenkripsi dengan susunan kunci yang sama sehingga menghasilkan cipherteks yang sama yaitu CSASTP. Jarak antara kedua kata adalah 16, sehingga kriptanalis dapat menerka bahwa panjang kunci adalah 2, 4, 8, atau 16. Dan benar bahwa panjang kunci sebenarnya adalah 4 yaitu ABCD. Setelah menerka panjang kunci maka kriptanalis dapat melanjutkan dengan analisis frekuensi yang akan memecahkan cipherteks yang ada. Semakin panjang pesan akan mengakibatkan semakin mudah metode ini digunakan karena semakin banyak kemungkinan plainteks yang sama akan dienkripsi dengan cipherteks yang sama.

2.3. Perbaikan dan variasi

Perbaikan pada metode Vigenère ditujukan untuk menghilangkan pengulangan cipherteks yang sama untuk plainteks yang sama agar tidak bisa dikenakan teknik kasiski untuk melakukan kriptanalisis. Telah banyak yang mengembangkan variasi dari Vigenère cipher, yaitu :

2.3.1. Running-key

Running-key varian dari Vigenère cipher sempat dikatakan sebagai enkripsi yang tidak terpecahkan. Variasi ini menggunakan plainteks untuk menambahkan panjang kunci jika panjang kunci kurang dari plainteks. Maka jika plainteks adalah ATTACKATDAWAN dan kunci adalah LEMON akan dihasilkan

```
Plaintext:  ATTACKATDAWN
Key:        LEMONATTACKA
Ciphertext: LXFOPKTMDCGN
```

Karena panjang kunci menjadi sama panjang dengan plainteks, akibatnya metode kasiski tidak dapat digunakan lagi untuk variasi ini. Akan tetapi pada tahun 1920, *Friedman* menemukan kelemahan dari variasi ini. Jika kriptanalis mengetahui informasi statistik dari kunci yang digunakan, maka informasi plainteks dapat terlihat dari cipheteks yang dihasilkan.

2.3.2. One-time pad

Idenya adalah menggunakan kunci yang benar-benar acak dan unik sepanjang plainteks dan kunci hanya digunakan sekali. Secara teori maka variasi ini tidak dapat dipecahkan. Akan tetapi metode ini mempunyai kendala yaitu pembangkitan kunci yang benar-benar acak. Juga untuk komputasi knci sepanjang plainteks akan membutuhkan waktu yang lama, terutama jika plainteks yang akan dienkripsikan sangat panjang. Juga dengan panjangnya kunci akan menyulitkan dalam pengiriman kunci pada penerima pesan.

2.3.3. Gronsfeld cipher

Variasi ini diciptakan oleh *Count Gronsfeld.* Algoritma ini telah menyebar luas sampai seluruh Eropa. Idenya adalah dengan mengganti huruf dengan bilangan desimal maka akan mengakibatkan plainteks tidak akan beupa huruf melainkan hanya berupa susunan angka. Kemudian enkripsi menggunakan prinsip yang sama dengan Vigenère yaitu menggunkan tabel yang hanya berukuran 10x10. Maka jika ada kata ATTACK akan diubah menjadi susunan angka 012020010311. Dan jika kunci LEMON akan menjadi 1205131514. Sehingga akan dihasilkan :

```
Plaintext:  012020010311 - ATTACK
Key:        120513151412 - LEMONL
Ciphertext: 132533161723
```

Metode ini memiliki kekuatan lebih dibandingkan dengan Vigenère cipher pada kata yang dienkripsikan yang berupa angka bukan huruf, sehingga kriptanalis tidak bisa menerka kata yang digunakan untuk kunci atau kata yang ada di dalam plainteks. Akan tetapi hal ini justru menimbulkan kelemahan yaitu hanya terdapat 10 huruf / angka di dalam cipherteksnya.

	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

Gambar 6 *Gronsfeld Table*

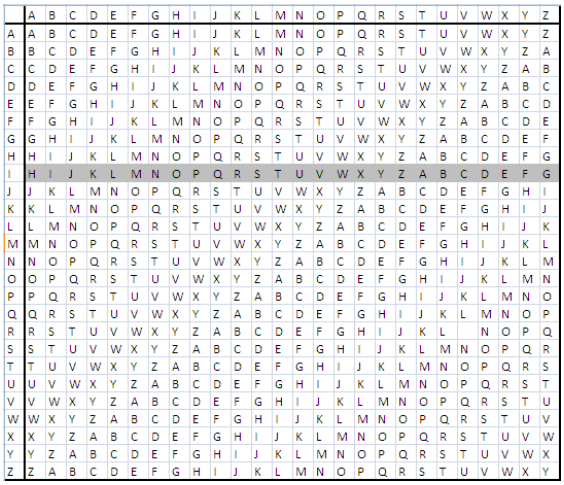
2.3.4. ASCII Table

Variasi ini sebetulnya hanyalah memperbanyak jumlah karakter yang dienkripsi mejadi 256 karakter sesuai dengan tabel ASCII. Dengan variasi ini, tidak hanya karakter alfabet saja yang akan dienkripsi, melainkan juga karakter lain seperti numerik dan operator-operator serta tanda baca. Juga huruf kapital dan tidak akan dienkripsikan dengan huruf yang berbeda. Akan tetapi variasi ini tentunya masih dapat dikenakan terhadap metode kasiski dan analisis frekuensi. Memang analisis akan membutuhkan waktu lebih lama karena ukuran jumlah karakter yang perlu di analisis akan bertambah.

3. *VENIGMARÈ CIPHER*

Pada Vigenère biasa, enkripsi satu huruf plainteks pada satu huruf kunci yang sama akan mengakibatkan satu huruf cipherteks yang sama. Hal ini lah yang mengakibatkan teknik analisis frekuensi masih dapat dilakukan pada Vigenère cipher cukup dengan mengetahui panjang kunci. Untuk itu dibutuhkan variasi yang mengakibatkan satu huruf palinteks jika di enkripsikan dengan satu huruf kunci yang sama akan menghasilkan hasil yang berbeda.

Berdasarkan dalam cara kerja mesin enigma, yaitu ada rotor yang akan menyebabkan susunan substitusi huruf akan berubah setiap selesai melakukan enkripsi satu huruf. Maka pada algoritma Venigmarè yang dirancang ini sistem kerja ini digunakan. Ketika satu huruf selesai dienkripsi dengan sebuah kunci maka baris dimana cipherteks didapatkan akan digeser (*wrapping)* ke kanan. Jadi, pada kondisi awal jika kita melakukan enkripsi huruf I dengan kunci I, sehingga menghasilkan cipherteks Q, posisi baris pada tabel tersebut akan berubah seperti yang digambarkan pada gambar 7.

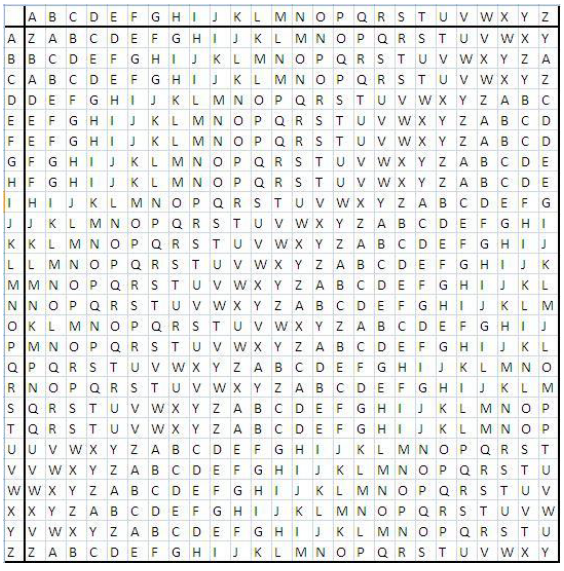


Gambar 7 Simulasi Venigmarè Cipher

Maka jika menggunakan kasus sebelumnya akan didapatkan sebagai berikut :

```
Key:        ABCDAB CD ABCDA BCD ABCDABCDABCD
Plaintext:  CRYPTO IS SHORT FOR CRYPTOGRAPHY
Ciphertext: CSASTP KV RIPUS GOT BQZRRMIRAOIZ
```

Jika dibandingkan dengan hasil pada Vigenère cipher, dapat dilihat bahwa kata CRYPTO yang di enkripsi dengan kunci yang sama akan menghasilkan cipherteks yang berbeda yaitu CSASTP dan BQZRRM. Sehingga metode kasiski tidak berlaku lagi pada kasus seperti ini. Akan tetapi karena tabel substitusi yang ada sudah berubah, maka dalam dekripsi juga dibutuhkan informasi tabel substitusi akhir hasil enkripsi. Untuk itu hasl ini menjadi masalah tersendiri untuk mengirimkan informasi akhir tabel substitusi.



Gambar 8 Tabel Akhir Enkripsi

Teknik yang mungkin bisa digunakan untuk melakukan pengiriman informasi adalah menyisipkan nya kedalam berkas hasil enkripsi itu sendiri. Tentunya tidak dengan begitu saja di tuliskan ke dalam berkas, melainkan dengan teknik steganografi dengan cover objek adalah berkas cipherteks dan data yang disembunyikan adalah informasi ukuran tabel. Dan informasi tabel yang perlu dikirimkan relatif kecil untuk ukuran teks yang besar > 1kB. Karena informasi yang perlu dikirimkan hanyalah jumlah pergeseran akhir dari setiap baris huruf, yang hanya membutuhkan 26 karakter / byte saja. Tentunya metode steganografi yang digunakan serta cara ekstraksi kembali informasi itu menjadi masalah tersendiri.

Untuk melakukan dekripsi, jika penerima pesan telah menerima pesan dan informasi tabel hasil akhir enkripsi tidak begitu sulit. Dengan mencari kolom kunci huruf yang terdapat pada cipherteks, kemudian menggeser baris tersebut ke kiri, maka akan didapatkan plainteks yang bersesuaian pada posisi kolomnya. Akan tetapi karena proses enkripsi mirip dengan metode enkripsi *block cipher* yaitu CBC (*Cipher Block Chaining)* maka kesalahan 1 data pada berkas cipherteks akan mengakibatkan kesalahan yang merambat. Dan juga untuk melakukan dekripsi kita harus melakukannya dari huruf paling belakang, berbeda dengan ketika enkripsi yang dilakukan dari paling depan.

Jika dituliskan dalam program, maka metode ini selain menggunakan formula umum (*P;K; C; E;D*) perlu adanya tambahan untuk menyimpan informasi tabel hasil enkripsi. Akibatnya kita perlu menambahkan satu struktur data baru berupa `array of char` sebanyak 26 huruf, yang tiap index menyatakan jumlah pergeseran pada tiap baris. Jika diformulasikan maka algoritma untuk enkripsi akan didapatkan :

$$\boldsymbol{Enkripsi: C_i \equiv (P_i + K_i + B_k)\ mod\ 26}$$

Dimana *C* adalah cipherteks, *P* adalah plainteks, *K* adalah kunci, dan *B* adalah informasi pergeseran baris pada kunci yang bersesuaian. Dan setelah selesai enkripsi satu huruf, informasi tabel perlu di-*increment.* Sehingga $\boldsymbol{B_k = B_k + 1}$.

Dan untuk proses dekripsi akan didapatkan formula yang merupaka balikan dari formula enkripsi yaitu :

$$\boldsymbol{Dekripsi: P_i = (C_i - K_i + B_k)\ mod\ 26}$$

Untuk setiap selesai melakukan dekripsi maka nilai dari *B* akan di-*decrement*. Sehingga $\boldsymbol{B_k = B_k - 1}$.

Tentunya algoritma ini masih dapat divariasikan juga dengan variasi yang digunakan pada Vigenère cipher sebelumnya seperti running-key, one-time pad, dan gronsfeld cipher serta ekspansi dari alfabet menjadi ASCII table.

4. KESIMPULAN

Kesimpulan yang didapat dari studi pengembangan metode enkripsi baru yang didasarkan pada Vigenère cipher adalah :

1. Vigenère cipher adalah salah satu teknik enkripsi yang murah dan mudah digunakan dan diimplemenasikan.
2. Untuk mengatasi kelemahan pada metode enkripsi substitusi, yaitu adanya korelasi antar frekuensi huruf pada plainteks dan cipherteks, perlu dikembangkan metode-metode baru.
3. Masalah utama dalam menghilangkan kelemahan dalam Vigenère cipher adalah bagaimana agar plainteks yang sama jika di enkripsikan dengan kunci yang sama akan menghasilkan cipherteks yang berbeda.
4. Venigmarè cipher membuat kelemahan itu hilang, tetapi menimbulkan masalah adanya data tambahan yang perlu dikirimkan kepada penerima pesan agar ia mampu mendekripsi pesan yaitu informasi tabel akhir hasil enkripsi.
5. Proses pengiriman informasi tabel akhir hasil enkripsi menjadi masalah tersendiri yang sementara ini bisa diterapkan dengan menerapkan teknik steganografi.
6. Karena proses enkripsi berantai untuk tiap huruf, maka pada saat dekripsi juga perlu untuk dilakukan secara berantai dengan urutan kebalikannya.
7. Proses enkripsi dan dekripsi yang berantai menyebabkan kesalahan satu byte / karakter huruf akan menyebabkan huruf berikutnya juga mengalami kesalahan.
8. Tingkat keamanan algoritma ini terhadap metode kasiski dan analisis frekuensi sangat kuat karena telah hilangnya korelasi antara huruf pada plainteks dan cipherteks.
9. Algoritma ini masih bisa dikembangkan dan divariasikan dengan teknik lainnya untuk menciptakan teknik enkripsi yang kuat sehingga tidak mudah dienkripsi tetapi tetap memegang konsep mudah untuk diimplementasikan.

DAFTAR REFERENSI

[1] Dalkilic, Mehmet E. dan Gungor, Cengiz. 2000. *An Interactive Cryptanalysis Algorithm*. Ege University, International Computer Institute Bornova, Izmir, Turkey.

[2] D. R. Stinson. 1995. *Cryptography: Theory and Practice*. CRC Press.

[3] Talbot, John and Dominic Welsh. 2006. *Complexity and Cryptography*. Cambridge University Press.

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