Cryptanalysis Menggunakan *Methode Vigenere Cipher*

Akik hidayat[1], Asep Sholahuddin[2], Rudi Rosadi[3]
[1,2,3]Teknik Informatika , Universitas Padjadjaran, Bandung
akik@unpad.ac.id[1], ashol@unpad.ac.id[2], r_rosadi@unpad.ac.id[3]

Abstrak – *Kriptanalisis (cryptanalysis) adalah ilmu dan seni untuk memecahkan cipherteks menjadi plainteks tanpa mengetahui kunci yang digunakan. Pelakunya disebut kriptanalis. Vigenere Cipher merupakan metoda kriptografi klasik yang memanfaatkan subsitusi polialpabetik. Vigenere cipher hanya dapat mengenkripsi huruf alfabetik dan tidak membedakan antara huruf hapital dan huruf kecil. Metode yang digunakan Kriptanalisis pada Vigenere Cipher adalah dengan menggunakan metode Friedman dan Kasiski.*

Kata kunci *: kriptanalisis, polialpabetik, Friedman, Kasiski*

1. Pendahuluan

Cryptography ”suatu studi teknik matematik yang berkaitan dengan aspek-aspek keamanan informasi seperti kerahasiaan, integritas data, autentikasi entiti, dan autentikasi keaslian data”. *Cryptography* menyediakan cara untuk mengamankan informasi dan mencegah aktifitas-aktifitas yang tidak sah, sedangkan Kriptanalisis (cryptanalysis) adalah ilmu dan seni untuk memecahkan cipherteks menjadi plainteks tanpa mengetahui kunci yang digunakan. *Cryptography* bertujuan untuk menjaga kerahasiaan *plaintext* dari pihak lain yang tidak berkepentingan. Dua proses dalam *cryptography* yaitu proses enkripsi dan dekripsi. Enkripsi mengubah *plaintext* menjadi *ciphertext* dengan melibatkan *cipher* dan sebuah *key*. Dekripsi mengembalikan *ciphertext* menjadi *plaintext* juga menggunakan *cipher* dan *key* (Brown, 1996). Ada dua tipe algoritma yang menggunakan *key* yaitu *symmetric algorithms* dan *public-key algorithm*s. Pada s*ymmetric algorithms*, proses enkripsi dan dekripsi menggunakan *key* yang sama sedangkan p*ublic-key algorithm* menggunakan *key* berbeda. *Substitution cipher* termasuk *symmetric algorithms. Substitution cipher* melakukan substitusi terhadap setiap karakter dari *plaintext* menjadi karakter lain pada *ciphertext*. Untuk memperoleh kembali *plaintext*, penerima pesan membalikkan proses substitusi tersebut. Ada empat tipe dari *substitution cipher* yaitu *Simple substitution cipher* atau *monoalphabetic cipher, homophonic substitution cipher, polygram substitution cipher,* dan *polyalphabetic substitution cipher* (Schneier, 1996).*Cryptanalysis* adalah ilmu untuk mengubah kembali suatu *ciphertext* menjadi *plaintext* tanpa mengetahui *key*-nya. *Cryptanalysis* dikatakan sukses jika dapat mengembalikan *plaintext* atau menemukan *key*-nya. Usaha untuk melakukan *cryptanalysis* disebut *attack*. *Cryptanalyst* adalah orang yang melakukan *cryptanalysis*. Menurut Dutchman A. Kerckhoffs, kerahasiaan sebuah *ciphertext* semuanya terletak pada *key* dengan asumsi bahwa seorang *cryptanalyst* memiliki detail lengkap algoritma *cryptography* dan implementasinya (Schneier, 1996).

2. Metode penelitian

Metode yang digunakan adalah Metode Friedman dan Kasiski yaitu memanfaatkan keuntungan bahwa bahasa Inggris tidak hanya mengandung perulangan huruf, tetapi juga perulangan pasangan huruf atau tripel huruf, seperti TH, THE, dsb. Perulangan kelompok huruf ini ada kemungkinan menghasilkan kriptogram yang berulang.

Algoritma metode Friedman dan Kasiski adalah :

1. Temukan semua kriptogram yang berulang di dalam cipherteks (pesan yang panjang biasanya mengandung kriptogram yang berulang).
2. Hitung jarak antara kriptogram yang berulang
3. Hitung semua faktor (pembagi) dari jarak tersebut (faktor pembagi menyatakan panjang kunci yang mungkin).
4. Tentukan irisan dari himpunan faktor pembagi tersebut. Nilai yang muncul di dalam irisan menyatakan angka yang muncul pada semua faktor pembagi dari jarak-jarak tersebut . Nilai tersebut mungkin adalah panjang kunci.
5. Misalkan panjang kunci yang sudah berhasil dideduksi adalah *n*. Setiap huruf kelipatan ke-*n* pasti dienkripsi dengan huruf kunci yang sama. Kelompokkan setiap huruf ke-*n* bersama-sama sehingga kriptanalis memiliki *n* buah "pesan", masing-masing dienkripsi dengan substitusi alfabet-tunggal (dalam hal ini *Caesar cipher*).
6. Tiap-tiap pesan dari hasil langkah 1 dapat dipecahkan dengan teknik analisis trigram yang paling sering muncul dalam bahasa inggris.
7. Kriptanalis dapat menerka kata yang membantu untuk memecahkan cipherteks.

3. Hasil dan Analisis

Kita akan mencari kunci dari cipherteks dari Plainteks dibawah ini.

LJVBQ STNEZ LQMED **LJV**MA MPKAU FAVAT **LJV**DA YYVNF JQLNP **LJV**HK VTRNF **LJV**CM LKETA **LJV**HU YJVSF KRFTT WEFUX VHZNP

Kriptogram yang berulang adalah **LJV**.

Jarak **LJV** ke-1 dengan **LJV** ke-2 = 15
Jarak **LJV** ke-2 dengan **LJV** ke-3 = 15
Jarak **LJV** ke-3 dengan **LJV** ke-4 = 15
Jarak **LJV** ke-4 dengan **LJV** ke-5 = 10
Jarak **LJV** ke-5 dengan **LJV** ke-6 = 10

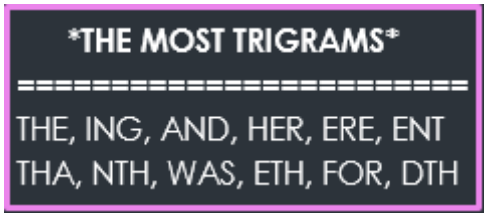
Faktor pembagi 15 = {3, 5, 15}
Faktor pembagi 10 = {2, 5, 10}
Irisan kedua himpunan ini = 5. Jadi, panjang kunci diperkirakan = 5

Tabel Frekuensi Kemunculan Huruf Dalam Bahasa Inggris

Karakter	Peluang	Karakter	Peluang
A	0.082	N	.067
B	.015	O	.075
C	.028	P	.019
D	.043	Q	.001
E	.127	R	.060
F	.022	S	.063
G	.020	T	.091
H	.061	U	.028
I	.070	V	.010
J	.002	W	.023
K	.008	X	.001
L	.040	Y	.020
M	.024	Z	.001

Dalam Bahasa Inggris, 10 huruf yang yang paling sering muncul adalah E, T, A, O, I, N, S, H, R, dan D,

ISBN : 978-602-512-810-3



Triplet yang paling sering muncul adalah THE.
Karena **LJV** paling sering muncul di dalam cipherteks, maka dari 10 huruf tsb semua kemungkinan kata 3-huruf dibentuk dan kata yang yang cocok untuk **LJV** adalah THE. Jadi, kita dapat menerka bahwa **LJV** mungkin adalah THE.
Dari sini kita buat tabel yang memetakan huruf plainteks dengan cipherteks dan huruf-huruf kuncinya (ingatlah bahwa setiap nilai numerik dari huruf kunci menyatakan jumlah pergeseran huruf pada *Caesar cipher*):

No	Huruf Plainteks	Huruf Cipherteks	Huruf kunci
1	T = 19	L = 11	S (=18)
2	H = 7	J = 9	C (=2)
3	E = 4	V = 21	R(=17)
4	-	-	-
5	-	-	-

$K = Ci - Pi ; Ci > Pi$

$K = (Ci + 26) - Pi ; Ci < Pi$

	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	D
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	C
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	B
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

ISBN : 978-602-512-810-3

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Dengan menggunakan kunci SCRAA cipherteks berhasil didekripsi menjadi :

LJVBQ STNEZ LQMED **LJV**MA MPKAU FAVAT **LJV**DA YYVNF JQLNP **LJV**HK VTRNF **LJV**CM LKETA **LJV**HU YJVSF KRFTT WEFUX VHZNP
THEBQ ARWEZ TOVED THEMA UNTAU NYEAT THEDA GWENF ROUNP THEHK DRANF THECM TINTA THEHU GHESF SPOTT ECOUX DFINP

No	Huruf Plainteks	Huruf Cipherteks	Huruf kunci
1	U = 20	M = 12	S (=18)
2	N = 13	P = 15	C (=2)
3	T = 19	K = 10	R(=17)
4	A = 0	A = 0	A(=0)
5	I = 8	U = 20	M(=12)

Dengan menggunakan kunci SCRAM cipherteks berhasil didekripsi menjadi :
THEBE ARWEN TOVER THEMO UNTAI NYEAH THEDO GWENT ROUND THEHY DRANT THECA TINTO THEHI GHEST SPOTH ECOUL DFIND
atau dalam kalimat yang lebih jelas :
THE BEAR WENT OVER THE MOUNTAIN YEAH
THE DOG WENT ROUND THE HYDRANT THE CAT INTO THE HIGHEST SPOT HE COULD FIND

4. Kesimpulan

Cryptanalisis Vigenere cipher menggunakan metode Friedman dan Kasiski untuk penyelesaiannya menitik beratkan pada perulangan pasangan huruf atau tripel huruf, seperti TH, THE, dsb. Perulangan kelompok huruf ini ada kemungkinan menghasilkan kriptogram yang berulang juga harus melihat huruf apa yang paling banyak muncul serta susunan huruf dari paragraf yang akan di dekripsi. Paragraf yang harus di dekripsi harus dalam bahasa inggris.

Daftar Pustaka

[1]. D. E. R. Denning. *Cryptography and Data Security*. Addison-Wesley, 1982.
[2]. D. Kahn. *The Codebreakers. The Story of Secret Writing*. Macmillan, 1967.
[3]. H. Anton. *Elementary Linear Algebra* (Sixth Edition). John Wiley and Sons, 1991.
[4]. H. Beker and F. Piper. *Cipher Systems, The Protection of Communications*. John Wiley and Sons, 1982.
[5]. K. H. Rosen. *Elementary Number Theory and its Applications* (Third Edition). Addison Wesley, 1993.
[6]. L. S. Hill. Cryptogaphy in an algebraic alphabet. *American Mathematical Monthly*, 36 (1929), 306-312.
[7]. R. A. Rueppel. *Analysis and Design of Stream Ciphers*. Springer-Verlag, 1986.
[8]. Stinson, D. (1995). *Cryptography: Theory and Practice.* CRC Press.

ISBN : 978-602-512-810-3