Kriptanalisis pada Vigenere Cipher Menggunakan Aplikasi Maple untuk Menerapkan Teknik Signature dan Scrawls

Christabella Chiquita B. – NIM 13509050[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]*christabella.c.b.@students.itb.ac.id*

***Abstract*—Vigenere cipher merupakan salah satu teknik enkripsi yang sudah umum dilakukan. Untuk memecahkan suatu kode hasil enkripsi ini harus dilakukan pencarian panjang kata kunci, barulah kata kunci itu sendiri. Pengujian Friedman dan Kasiski hanya digunakan untuk menentukan panjang kata kunci. Teknik yang dibahas di sini adalah teknik yang tidak hanya membantu mengestimasi panjang kunci saja, melainkan juga mengestimasi kata kuncinya sendiri. Teknik signature digunakan untuk menentukan panjang kunci berdasarkan perbandingan grafik panjang kunci dengan English Frequency Signature. Sedangkan teknik scrawls digunakan untuk menemukan kata kunci berdasarkan pemillihan grafik yang paling mendekati grafik frekuensi huruf pada teks bahasa Inggris. Maple merupakan suatu aplikasi algebra matematika yang sudah digunakan secara luas untuk melakukan analisa probabilitas, plotting grafik, permodelan, dan berbagai fungsi matematika lainnya.**

***Index Terms*—scrawls, frequency, kunci, maple, signature, vigenere.**

I. PENDAHULUAN

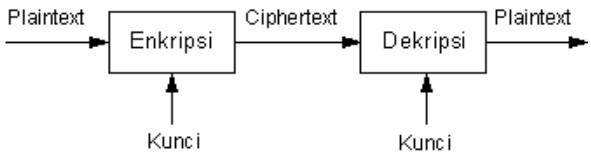
Saat ini kriptografi sudah semakin meluas perannya, terutama di bidang teknologi informasi. Karena semakin meluasnya penggunaan komputer dan internet, keamanan data / pesan pun menjadi hal yang semakin penting. Di sinilah kriptografi banyak diterapkan, yaitu untuk menyembunyikan pesan asli yang sering disebut *plaintext* menjadi pesan tersembunyi atau kode yang sering disebut *ciphertext*. Saat ini sudah banyak teknik kriptografi yang memanfaatkan berbagai algoritma berbeda. Salah satunya adalah Vigenere Cipher. Vigenere cipher merupakan salah satu teknik yang sudah banyak digunakan karena implementasinya yang cukup mudah, dan memiliki kekuatan yang cukup baik dikarenakan teknik ini menggunakan kata kunci untuk mengenkripsi *plaintext*.

Seiring meluasnya penggunaan kriptografi, begitu pula dengan teknik pemecahannya, yaitu kriptanalisis. Kriptanalisis merupakan suatu studi dan teknik untuk mendapatkan kembali *plaintext* (pesan asli) dari *ciphertext* yang ada tanpa perlu mengetahui teknik dan algoritma yang digunakan untuk mengenkripsi. Kriptanalisis pada Vigenere Cipher yang sering dilakukan saat ini adalah dengan menggunakan metode Friedman dan Kasiski. Metode Friedman dan Kasiski ini lebih menekankan pada pencarian panjang kunci yang ditemukan dengan mencari dua atau lebih kriptogram berulang. Namun hal ini terkadang belum tentu berhasil, terutama apabila *ciphertext* tidak terlalu panjang sehingga sulit ditemukan kriptogram yang berulang.

Pada tugas makalah ini dilakukan eksperimen untuk memecahkan sebuah *ciphertext* dengan menerapkan dua teknik, yaitu teknik signature dan teknik scrawls. Teknik signature digunakan untuk mengeetahui estimasi panjang kata kunci, dan teknik scrawls digunakan untuk menemukan kata kunci itu sendiri. Dengan kedua teknik ini, dilakukan analisa dari perbandingan grafik yang dihasilkan dari fekuensi setiap huruf, baik pada *ciphertext* maupun standard English Text.

II. PENGERTIAN DASAR

Suatu pesan yang tidak disandikan disebut sebagai *plaintext* / *cleartext*. Proses yang dilakukan untuk mengubah plaintext ke dalam ciphertext disebut enkripsi. Sedangkan proses untuk mengubah ciphertext kembali ke plaintext disebut dekripsi. Secara sederhana istilah-istilah di atas dapat digambarkan seperti gambar 2.1.



Gambar 2.1 Bagan proses enkripsi dan dekripsi

Kriptanalisis (cryptanalysis) adalah ilmu dan seni untuk memecahkan cipherteks menjadi plainteks tanpa mengetahui kunci yang digunakan. Pelakunya disebut kriptanalis. Kriptologi adalah studi mengenai kriptografi dan kriptanalisis.

A. Vigenere Cipher

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. Oleh karena itu, plainteks dari vigenere cipher tidak boleh terdapat spasi ataupun tanda baca lainnya, karena tidak dapat dienkripsi, jika ada, maka algoritma vigenere cipher

harus dimodifikasi sedemikian sehingga dapat menghiraukan spasi atau tanda baca lainnya. Kunci yang digunakan dalam algoritma vigenere cipher biasanya adalah satu kata atau satu kalimat agar mudah diingat. Apabila kunci lebih pendek dari panjang plainteks maka kunci akan diulang hingga kunci memiliki panjang yang lebih besar atau sama dengan panjang plainteks. Pada zaman dahulu, digunakan tabel substitusi alfabet yang sering disebut sebagai Vigenere square seperti pada gambar 2.2

	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 Vigenere square / tabel substitusi alfabet
(Sumber : http://commons.wikimedia.org/wiki/File:Vigenere-square.png)

B. Deskripsi Matematika Vigenere Cipher

Ketika melakukan enkripsi pada suatu *plaintext* menggunakan persegi Vigenere, untuk setiap huruf dari *plaintext* tersebut dilakukan penjumlahan dari hasil mod huruf pada *plaintext* dengan hasil mod huruf dari kata kunci. Hasil penjumlahan ini apabila di-mod dengan 26 akan merepresentasikan huruf *ciphertext*.

Misalnya :

Misalkan kita mengenkripsi kata "GOD" dengan kata kunci "TEN" dengan menggunakan Vigenere cipher square,

Tabel 2.1 Tabel hasil enkripsi menggunakan Vigenere square

Plaintext	G	O	D
Keyword	T	E	N
Ciphertext	Z	S	Q

Ciphertext "ZSQ" tersebut dapat diperoleh dari penggunaan tabel alfabet mod 26, yaitu sebagai berikut

Huruf ke-1 :
G → 6
T → 19 +
25 mod 26 = 25 ('Z')

Huruf ke-2 :
O → 14
E → 4 +
18 mod 26 = 18 ('S')

Huruf ke-3 :
D → 3
N → 13 +
16 mod 26 = 16 ('Q')

Teknik ini dapat diterapkan pada Vigenere Cipher, yaitu untuk menentukan panjang kata kunci yang digunakan. Karena untuk memecahkan sebuah ciphertext hasil enkripsi Vigenere, hal yang paling penting dan perlu diketahui pertama kali adalah panjang kata kunci itu sendiri.

Tabel 2.2 Hasil enkripsi menggunakan Vigenere square

Plain	I	L	0	V	E	D	0	G	A	N	D	C	A	T
Key	P	E	T	P	E	T	P	E	P	E	T	P	E	T
Cipher	X	P	H	K	I	W	D	K	P	R	W	R	E	M

Melihat tabel 2..2 huruf 'E' pada keyword menghasilkan shift cipher '4' terhadap *plaintext* dan menghasilkan coset yaitu [P,I,K,W,M]. Begitu juga dengan hurut 'P' dan 'T' pada keyword masing – masing menghasilkan sebuah coset. Jumlah coset yang terbentuk menunjukkan panjang kata kunci. Apabila sudah diketahui jumlah coset yang berarti panjang kunci diketahui, selanjutnya dapat dilakukan analisis frekuensi menggunakan Maple untuk setiap coset shift cipher dan mencobakan berbagai keyword secara *rand*om untuk melihat grafik mana yang paling sesuai.

C. Signature dan Scrawls

Signature dapat dibagi menjadi dua, yaitu English signature dan sample signature. English signature memberikan plot probabilitas / frekuensi kemunculan huruf pada teks bahasa Inggris standar dan diplot secara terurut menaik (*increasing order*). Frekuensi ini didasarkan pada tabel frekuensi English standar, yaitu gambar 2.3. Sedangkan sample signature memberikan plot probabilitas / frekuensi kemunculan huruf pada teks sampel dan diplot secara terurut menaik (*increasing order*).

Sedangkan untuk sample signature, karena teks sampel pastinya mencakup huruf yang lebih sedikit daripada keseluruhan bahasa inggris, makan ada kemungkinan beberapa huruf tidak muncul sama sekali sehingga frekuensinya 0. Karena frekuensi masing – masing huruf pada teks sample itu apabila dijumlahkan harus bernilai 1, maka akan dihasilkan beberapa huruf frekuensinya akan lebih tinggi daripada pada English signature. Hal ini akan mengakibatkan grafik bagian kiri (lower frequency) pada teks sampel akan lebih rendah daripada grafik bagian kiri pada teks English standar, dan grafik bagian kanan pada teks sampel akan lebih tinggi daripada teks English standar.

Teknik scrawls adalah teknik yang memanfaatkan grafik yang menggambarkan distribusi probabilitas setiap huruf

pada teks sampel dan dibuat terurut sesuai alfabet (A-Z). Seperti signature, scrawls pun dibagi dua, yaitu English scrawls (English text) dan sample scrawls (sample text). Teknik ini diawali dengan pembentukan seluruh coset (panjang kunci sudah diketahui). Dari masing – masing coset tersebut dibuat plot grafiknya menggunakan Maple dengan nilai shift berubah dari 0 sampai 25. Di antara 26 grafik yang dibentuk, diambil sebuah grafik yang paling mendekati grafik English scrawl. Nilai shift grafik tersebut d-mod dengan 26 dan dihasilkan sebuah huruf penyusun kata kunci. Langkah ini diulangi terus sampai semua coset menghasilkan sebuah huruf penyusun kata kunci. Dan kata kunci pun berhasil ditemukan.

TABLE II
LETTERS FREQUENCY

Letter	Frequency	Letter	Frequency
A	8.167%	N	6.749%
B	1.492%	O	7.507%
C	2.782%	P	1.929%
D	4.253%	Q	0.095%
E	12.702%	R	5.987%
F	2.228%	S	6.327%
G	2.015%	T	9.056%
H	6.094%	U	2.758%
I	6.966%	V	0.978%
J	0.153%	W	2.360%
K	0.772%	X	0.150%
L	4.025%	Y	1.974%
M	2.406%	Z	0.074%

Gambar 2.3 Tabel English letters frequency
(sumber : techpiece.wordpress.com/category/information-security/)

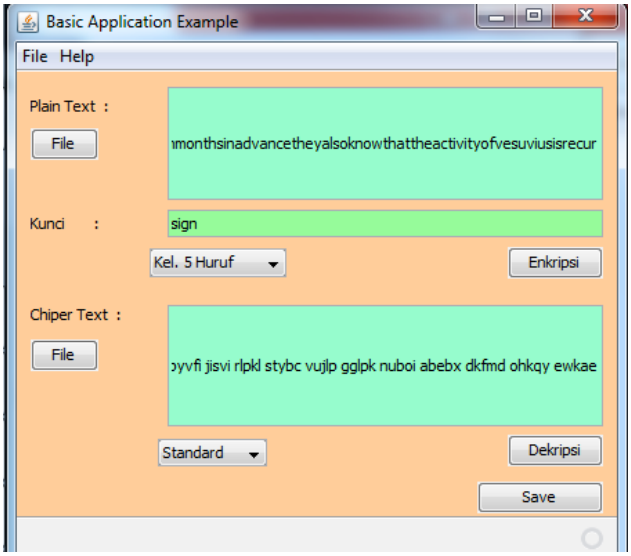
D. Maple

Maple adalah program komputer yang dikembangkan pertama kali pada tahun 1980 oleh Grup Symbolic Computation di University of Waterloo Ontario, Kanada untuk keperluan bidang matematika, statistika dan komputasi aljabar. Program ini biasa digunakan untuk melakukan berbagai operasi matematika yang bisa menampilkan notasi matematis pada proses-proses perhitungan yang dijalankan serta melakukan plotting grafik 2D dan 3D beserta animasinya, membuat tabel, dll. Ciri-ciri maple antara lain:

- Menggunakan simbol-simbol operasi dan notasi matematika yang umum digunakan
- Digunakan untuk perhitungan-perhitungan kalkulus dengan penerapan prinsip-prinsip matematika yang tidak terlalu rumit sehingga mudah untuk digunakan
- Eksekusi setiap perintah selalu menggunakan tanda titik koma (;)
- Bersifat kontinyu untuk setiap prosesnya. Artinya operasi-operasi yang telah dibuat dapat digunakan untuk referensi operasi berikutnya tanpa harus merumuskan ulang.

III. EKSPERIMEN

Pada tugas ini, penulis melakukan eksperimen untuk memecahkan sebuah kode yang dihasilkan dari enkripsi menggunakan vigenere cipher. Penulis membuat sebuah program sederhana (*Vigenere Cipher Application)* yang menerima input berupa *ciphertext* dan kunci, dan mengeluarkan hasil berupa *plaintext* hasil dekripsi. Hasil *screenshot* dari program tersebut dapat dilihat pada gambar 3.1.



Gambar 3.1 Tampilan program pertama (program Vigenere Cipher)

Plaintext yang digunakan adalah

It is certain that when the eruption of Vesuvius started on the morning of 24 August, AD 79, it caught the local population utterly unprepared. Although at the same time, as we now know in retrospect, all the tell-tale signs were there to warn them. It is mainly thanks to the vivid eye-witness account of the younger Pliny (a Roman administrator and poet, whose many vivid letters have been preserved), that we have some understanding of what happened. And it is through him that we can gain insight into the reactions and feelings of the people caught up in the drama of this natural catastrophe.

Pliny's account leaves no doubt that everyone was caught unprepared. His uncle, known as Pliny the Elder, was stationed in command of the imperial naval base at Misenum, on the north-west extremity of the Bay of Naples. He was not only the senior military officer in the district, but possibly the most well informed living Roman on matters of natural science. His 37-volume Natural History is the longest work on science in Latin that has survived from antiquity.

But for all his science and his seniority, his nephew tells us that the elder Pliny was relaxing, after a bath and lunch, when Vesuvius started to erupt. And the sighting of a column of smoke 'like an umbrella pine' on the far side of the Bay triggered a response more of curiosity than of alarm in him. He and his companions were evidently not anticipating such an event.

The same account reveals, however, that the signs were there. Pliny's casual reference to earth tremors 'which were not particularly alarming because they are frequent in Campania' reveals the Roman's comprehensive ignorance of the link between seismic activity (earth tremors) and volcanic activity.

The volcanologists of today constantly monitor any changes

in levels of seismic activity from the observatory on Vesuvius, because they know that the same increase of activity in the deep reservoir of magma (molten or partially molten rock beneath the Earth's surface) causes both earth tremors and volcanic eruptions. Through measuring seismic activity, these scientists expect to predict an approaching eruption months in advance.

They also know that the activity of Vesuvius is recur

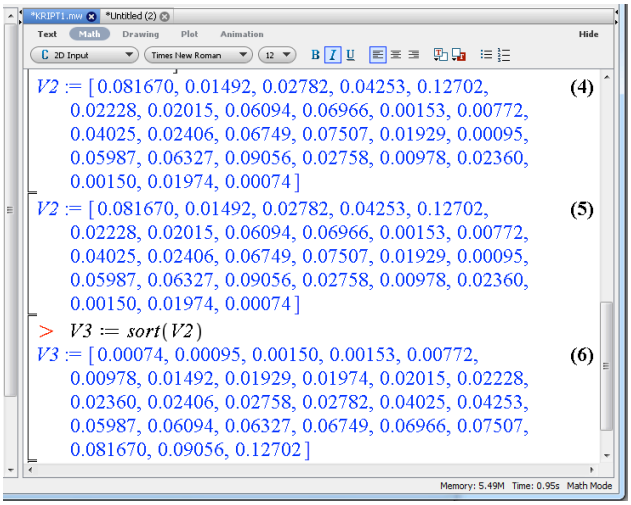
Kunci yang digunakan adalah "SIGN". Dengan program ini, dihasilkan ciphertext yaitu

abofu mxgsq tgziz jzmtg zmkem xzvgv usnmy hnqaf kbgel mjbfb nrewx aavmb xiatm aznvq zpscm ulbnr dwind xucmt ggawt hlbke dgaah zkcsz kqstz ugcmu sbzuw agzwb ozwiy jwvuj cvuja vxrlz ufhmi gstrg zmzrd tzndm yvyvy jwzkg zmxrl wcnjv zuwuo gaasn avrll pgaca zblpk iadoq wgkja btrka gpuwa alwlg zmebm vmrjx rvfgg eguga slsvf qygji zbjit qhwkg opufw ugaqd oialr rlbke kpgiw jkrfx xrkmx iwlzu sbcrz ibrkw srmvj rjazn floay wljzi zusxv rfmjn floga azujw atzpo zlpgg ominf ogvfq tfaon gavzb lpkew iigaw tfsvj swmrv foybx bnrhm ucdmi nmong mxoal pkqji sngnz uaatn lcxnd kggsa zegxn rhtoa qagpu waalt knnmy agluh tbzus bkiwz ebfmc nkkgh ypzhf xxrhi xrvpo fmviy wstbo vgfht oaqbn rwtjr jegfk bggaw trvqt pgusn flusl pkvex keair asdgy tiyrs bsvkm thewt gzmtb jbnjw azrpb xreqz lgnzu wjglg ntnht kfzmc nkvug gvrll pkfwv objuo yabge qwlsa kkeav zuwlo flzop ljagh wyfaj rllpk zgazj wtrvf nueem jyado ayzuz svuae izgwz ybxvg gmzgy kkorf kkuaa bbdcs rfizh jirua azbjg oflpk ygvmr kbcbj suakk orfkk vftgg avzus bnnka aenqb rvnxb eitga yavlg hhlnu estru aaypa mtpwi tqzqy fwvob jqzlz qyawx nrobk ydaaf lpggl pkrdl kehto aqegf jmrnp qttsn zrjih nlpga vtaau pcuwv brkcb vmayg szzrv burjc vgsvj gzmyv ypzvf oussk uymut bxasb cmrvc mgamu hewtr nhqtr gvzuw ngekq jrgnz uwjgl lzoty mxrvi xrkxu akmsb jmusu cxvga ogqbn nfwln dixza vnvep knfln vkkuz hitvg vyjwz krnqj rfbrl fwznf bopax ggavm fmknn fmbrf bzuwa gzwii pgctg jmbrs tyuge kiwzz usbzu waotf acrjm zuwzk cdqtl kkgfm irewn kewvi rlwkn jbngj msbja cuakn jwzka gbvnj bopmt gedgg yszsv fohru iafwb nrqix rxzkd mmtga vinex gaaix rnmgy kbnrj wsnfa ibexx rzmtf adkvy vuesv irgnz uwtoa cjkgo mkakm ofeqi nuboi abers zzulz kzgzy nflbb dkgaa kgplq bvlgz uwduy uitbd wmvkb ybxbu qsgib faznf brlew tvlwx nfgiu svmrk qtywd kykwl fwqyz akgpl qbvlg leguz uwwhf wzbnl wxlgv brkcb vmahr uiafw bnrqs tbobn nlbnr kisra viewi yrgng plqbv lgoal pkqwm vewak enwoe gnsny ugzgt zrfwx cszzv strle wrgwv xbush rfmgg zbnrw ixgza yhjng pwkgh kmyog bnrsz zulzk zgzyn flbbd kgaak kemxz vgvyg zzuhy psrsa aeavm fwqyz akgpl qbvlg zuwak fuqka lqygk mdcwk zggxx rvqig svgch zunup oaymx hhbob fuual pyvfi jisvi rlpkl stybc vujlp gglpk nuboi abebx dkfmd ohkqy ewkae

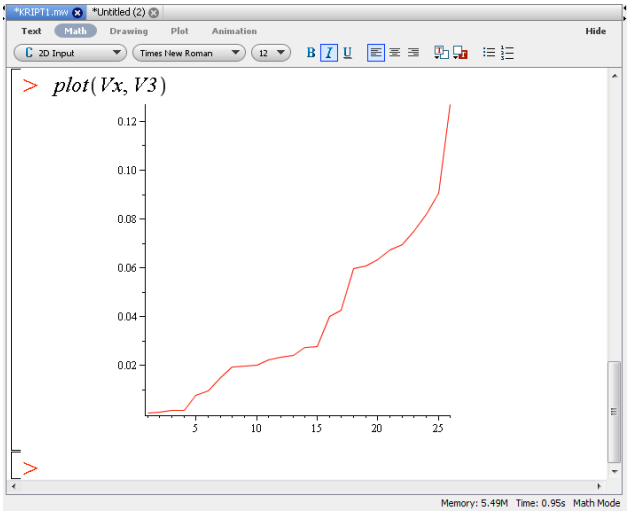
A. Teknik Signature untuk Menentukan Panjang Kunci

Karena teknik *signature* dan *crawling menggunakan* frekuensi kemunculan huruf dibandingkan dengan frekuensu kemunculan huruf pada teks bahasa Inggris, maka digunakan aplikasi Maple 12.0 untuk melakukan plotting grafik. Mula – mula, dibuat sebuah list V2 yang berisi frekuensi kemunculan tiap huruf pada teks bahasa Inggris (*English Signature*) yang kemudian diurutkan dari frekuensi terkecil sampai terbesar dan disimpan pada list V3 seperti pada gambar 3.2.

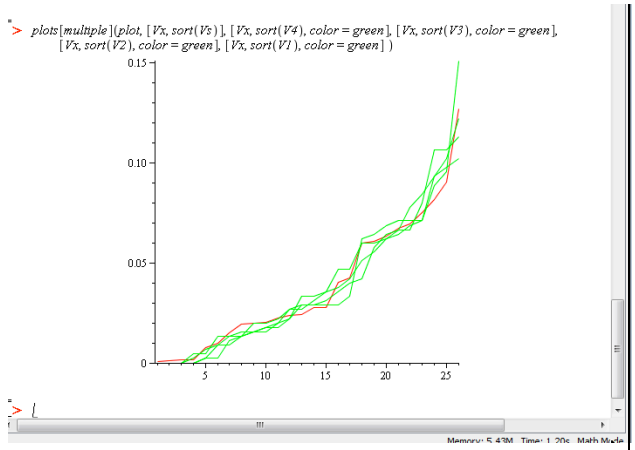
Kemudian dibuat plot grafik dari list V3 tersebut dan dihasilkan grafik seperti pada gambar 3.3. Untuk menemukan panjang kunci, maka dibuat suatu program sederhana yang menerima input berupa *chipertext* sebagai teks sampel. Program ini dapat menghasilkan *output* berupa perhitungan frekuensi setiap huruf yang ada pada teks sampel dan dapat melakukan filter untuk mendapatkan coset. Dengan program ini, dapat dilakukan penghitungan frekuensi untuk setiap coset dan dibuat plot grafiknya. Dari semua plot grafik yang dihasilkan, dilihat mana grafik yang memenuhi prinsip seperti yang sudah dijelaskan pada bab sebelumnya, yaitu semakin ke kiri, grafik akan menunjukkan frekuensi yang lebih rendah daripada English Signature sedangkan bagian kanan grafik akan menunjukkan frekuensi yang lebih tinggi daripada Engish Signature. Menggunakan aplikasi Maple, dapat dilakukan plot grafik frekuensi huruf untuk setiap huruf sepanjang kunci yang diperkirakan (misalnya jika panjang kunci 3 huruf, maka grafik yang dibentuk adalah untuk setiap huruf pertama, kedua, dan ketiga). Grafik yang paling memenuhi syarat adalah grafik untuk panjang kunci 4 huruf yang ditampilkan pada gambar 3.4



Gambar 3.2 List V2 dan V3 yang berisi frekuensi kemunculan setiap huruf pada teks bahasa Inggris (English Signature



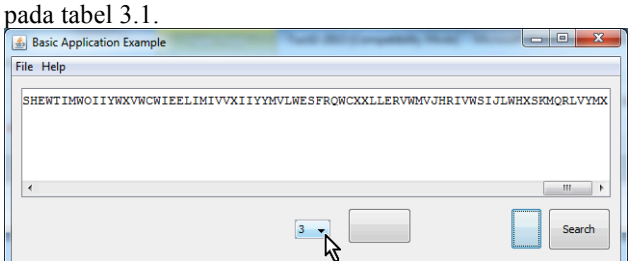
Gambar 3.3 Hasil plot grafik list V3



Gambar 3.4 Plot grafik Sample Signature untuk panjang kunci 4 huruf (merah menyatakan English Signature, hijau menyatakan Sample Signature)

B. Teknik Scrawls untuk Menentukan Kunci

Seperti pada penentuan panjang kunci, digunakan dua program yang dibuat oleh penulis. Program kedua digunakan untuk memfilter agar diperoleh seluruh coset yang dapat dilihat pada gambar 4.5 yang merupakan hasil *screenshot* program. Hasil dari filter tersebut dapat dilihat pada tabel 3.1.



Gambar 3.5 Screenshot Program kedua ketika melakukan filter untuk memperoleh coset ke-3

Tabel 3.1 Tabel Coset hasil Filter Program kedua

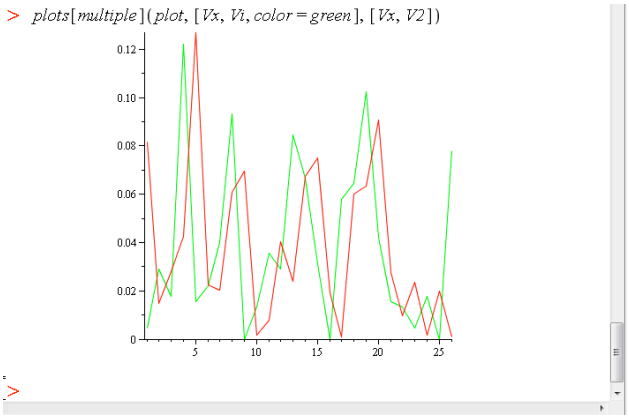
Coset 1 :
[auszzzmgnnklfeaxmvslddmaldhssgswwwwcalhszddywzljwaalc lawakulzmjfgsfjjhowqalkwfkwszkmjfyzsffajzloffaalwaswfxhdm mljgaldsghqulngtswfkyfhvmwohqwjkavgfleastskezjwpegwghzk glwjaqaawllhalgwfeaysewxmkfadfjajlgkjkffasknveallsaawzwjz wodlldhqjpsjlvuwkmsvjszyfsmxccmwhgwkgwlyvkkjugqfdaefkh gwnfffaamffwwgjsgwswfjwdkmwwljjjawgjmdsfuwqxmaeankjf ezaysgwcokeuaslgfdallwudkxsffelfskwkwallgwwlgkmuwqolka wglllwwngygfssewufzwzjwkgslgfdamgzysawallwulkwgvshuyhf lfslsclluaxmkw]

Coset 2 :
[bmqimmxvmqbmbwviaqcbwxtwbgzztcbabivvvzmtmtmvzmwv uavpapdgbawwmvxgulqiiwpudlbpjxmlbiwvalwixmlawppmoqov piwvmobmmoxpinackaxtawtmlbbzmkpxipvsvtbtebwqulpxidibm wmbabqnjntmvvpvubwkvlzjwjpatnmdzvizvzkkaciiagpvbskktvb aqniygntamiqvqqxbappltemqniptpvcazbcvmpokuammutqvnqnjz mixmmcabwivplkivzqbwbxvkmbaicmtezbaamzqkinvwbmakzbb tgzoibizmvximbwaxmdvvntjmmqbbzzzlkkqgdiwbbgabwwgvqd wqkqguwzwvcaibsbbivinqgpmawnutwztwvsmbiankmbzzzlkkxv zpavqkqgaqqmkxqvzpmbupivptvppbbddqk]

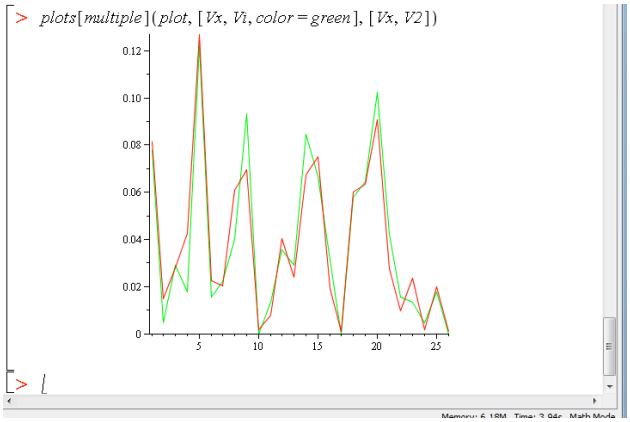
Coset 3:
[oxtztkzuyagjnxmazzmniugtkakkzmzgoyuuxuirzzyykxczosrgzk oktgalemrggsyztkugorkgkxxzcbsjzolzvjozaogigtnzkitjrynuinoks ztxgznogakyuzkecgzxxoitgonjggttsukkrgystttnzxzzgtkcurkooglk zooayrkzrujouuzyggokbszrzokmcuokgznabxtahuryttyozynkagkk ogrtzhgacbbyzuvjyzuutsrghrtzgjzgoxxusuxonlxnknutykjrzogmn bzgitbykzzoczktgrkiknscnkvoggshanxktigxgnsixtkuizokkoioezk ybggbzutmyuizrtximtklygblzhbxbbhantnnsiygbokvkosgzxzrrxh gnxyggynzkybgkzyusamygbzkkydzxiguoxouyjikyugkoekoya]

Coset 4 :
[fggjgevshfebrabtnpurncgheacquuuzzjjjrfggrnvjgrnugnlabiqjrpa gbrveavgbqgfaireirriurrrrrnajurngutzgnvfgbegfsvbrcngaqnunnger apanahuibnhhrrfybfarrfgrpnsveayrvhgbjrrlulnfnglfbyeseufpgflzj veyazagbgyrubrhubfyrbarvgunerbgvheuppqfblaryfgreafntrnaaur vgrrggvvsybbvaenruerultrrabsvgnnzvnvzvjrrlnpgfnruzpgruiuutr uclfeerngbujanpeyvrfrrdgnaryrnbrfveruagafniruznbapvuybvbqb nlvnuryyfzpveufnlrvrfrbnrrerpvaqeeenzrcvlgbrgrghphoruznbaev ghrefzpvufagcgrgcnahbavirlbjgnibfhee]

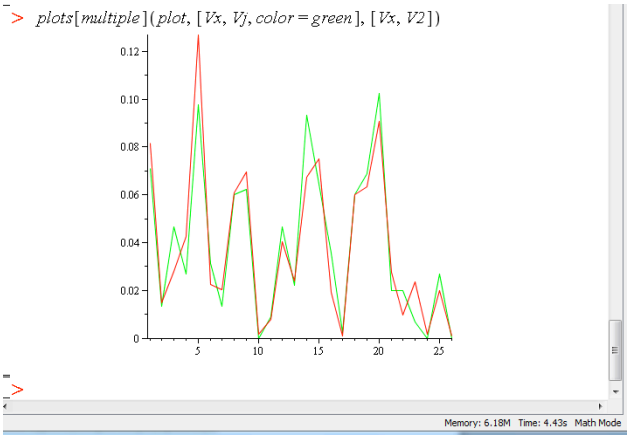
Menggunakan program pertama, dari setiap coset tersebut dilakukan analisa distribusi probabilitas untuk setiap nilai shift dari 0-25 dengan membuat plot grafiknya menggunakan Maple. Hasil tersebut tidak dapat ditampilkan seluruhnya pada makalah ini karena terlalu banyak (4x26=104 grafik), melainkan hanya yang paling mendekati untuk setiap hurufnya, dapat dilihat pada gambar 3.6 sampai 3.10 berikut ini. (warna merah menyatakan English Frequency Distribution, hijau menyatakan Sample Frequency Distribution)



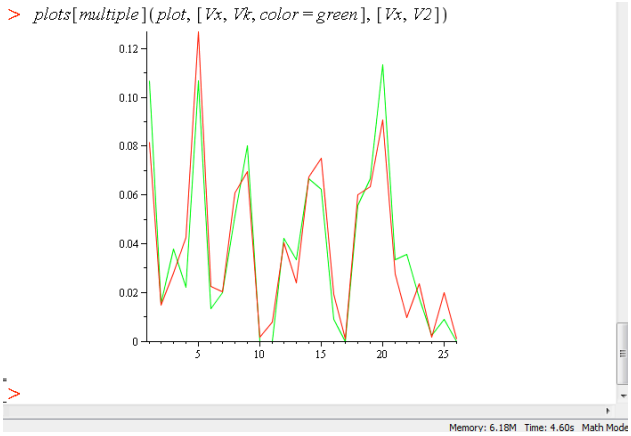
Gambar 3.6 Plot grafik hasil scrawls List 1 dengan left shift '19' yang agak mendekati



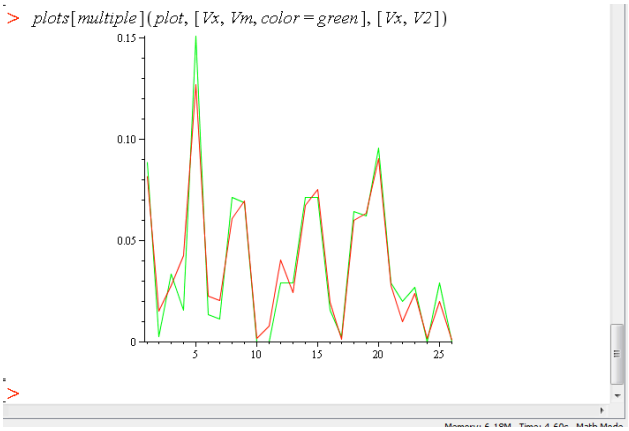
Gambar 3.7 Plot grafik hasil scrawls List 1 dengan left shift '18'



Gambar 3.8 Plot grafik hasil scrawls List 2 dengan left shift '8'



Gambar 3.9 Plot grafik hasil scrawls List 3 dengan left shift '6'



Gambar 3.10 Plot grafik hasil scrawls List 4 dengan left shift '13'

Dari hasil scrawls tersebut, diperoleh bahwa nilai shift yang menghasilkan grafik paling mendekati grafik frekuensi huruf dalam teks Bahasa Inggris adalah 18, 8, 6, dan 13. Apabila masing – masing di-mod dengan 26, maka dihasilkan kata kunci yaitu SIGN yang memang benar merupakan kata kunci yang digunakan untuk mengenkripsi plaintext.

IV. KESIMPULAN

Untuk memecahkan ciphertext hasil enkripsi menggunakan teknik Vigenere, hal yang perlu diketahui Pertama kali adalah panjang huruf kata kunci.

Teknik signature merupakan teknik yang dapat membantu untuk mengestimasi panjang kata kunci dengan lebih mudah. Sedangkan teknik scrawls merupakan teknik yang dapat membantu estimasi kata kunci itu sebenarnya. Untuk menggunakan kedua teknik ini, aplikasi Maple merupakan aplikasi yang cocok untuk menciptakan grafik yang digunakan sebagai analisa.

VI. KRITIK DAN SARAN

Pada pengujian ini hanya dilakukan kriptanalisis pada ciphertext yang dihasilkan oleh kata kunci dengan panjang 4 huruf. Sedangkan apabila kata kunci lebih panjang (jumlah huruf lebih banyak) akan cukup sulit karena coset yang dibentuk banyak.

Saran dari penulis adalah agar penelitian berikutnya dapat melakukan analisis dan memberikan solusi cara yang dapat mendukung kriptanalisis pada Vigenere cipher ini apabila kata kunci panjang.

VII. UCAPAN TERIMA KASIH

Saya mengucapkan terima kasih kepada Tuhan Yang Maha Esa karena atas berkat dan rahmat-Nya saya dapat menyelesaikan makalah ini tepat waktu. Saya juga mengucapkan terima kasih kepada Pak Rinaldi Munir sebagai dosen mata kuliah kriptografi yang telah memberi kesempatan sehingga saya dapat menyelesaikan makalah ini sebagai pengganti UTS.

REFERENCES

[1] Munir, Rinaldi, Algoritma Kriptografi Modern, dibaca tanggal : 20 Maret 2013

[2] Munir, Rinaldi, Kriptanalisis (2013), dibaca tanggal : 20 Maret 2013

[3] Introduction to Cryptography, http://www.ssh.com/support/cryptography/introduction/cryptanalysis.html. Diakses tanggal 24 Maret 2013

[4] Encryption, http://cs110.wellesley.edu/lectures/L18-encryption/handout.html. Diakses tanggal 25 Maret 2013

[5] Basic Cryptanalysis Techniques, SANS Institute InfoSec Reading Room. Diakses pada tanggal 25 Maret 2013

[6] Cryptanalysis of The Vigenere Cipher Using Signature and Scrawls, Prectice, From Barr Text. Dibaca tanggal 19 Maret 2013

[7] Online Help, Maple, Maplesoft, http://www.maplesoft.com/support/help/Maple. Diakses tanggal 24 Maret 2013

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 25 Maret 2013

Christabella C.B. - 13509050