Meningkatkan Keamanan pada Vigènere Cipher dengan Melakukan Pergeseran Tambahan

Aulia Hakim - 13504135
Program Studi Teknik Informatika Institut Teknologi Bandung, Bandung 40132,
e-mail : if14135@students.if.itb.ac.id

Abstrak
Makalah ini membahas modifikasi pada algoritma Vigènere Cipher yang dapat meningkatkan keamanan terhadap serangan dengan metode Kasiski, namun proses enkripsi dan dekripsi masih cukup sederhana untuk dilakukan tanpa alat bantu komputasi. Modifikasi yang dilakukan diterapkan adalah dengan melakukan pergeseran tambahan pada proses enkripsi dan dekripsi. Nilai pergeseran tambahan ini dibangkitkan dari kunci.

Kata kunci: *Vigènere cipher, metode Kasiski*

1. PENDAHULUAN

Vigènere Cipher adalah salah satu algoritma kriptografi klasik yang cukup populer. Kelebihan dari algoritma ini adalah kesederhanaannya. Proses enkripsi dan dekripsi cukup mudah untuk dilakukan tanpa alat bantu komputasi (hanya mengunakan alat tulis dan kertas).

Di sisi lain, *Vigènere Cipher* memiliki kelemahan yaitu panjang kunci dapat ditentukan dengan metode Kasiski. Metode Kasiski didasari adanya susunan huruf yang sering muncul dalam bahasi Inggris seperti 'TH', 'THE'. Perulangan susunan huruf ini mungkin menghasilkan perulangan pada kriptogram/cipherteks [1]. Kemunculan berulang ini akan banyak jika panjang kunci terlalu pendek (relatif terhadap panjang pesan plainteks). Metode Kasiski memanfaatkan sifat ini untuk menentukan panjang kunci.

Solusi paling sederhana terhadap serangan metode Kasiski adalah memperpanjang kunci. Namun solusi ini menjadi tidak praktis jika kita harus berhadapan dengan pesan yang sangat panjang, karena untuk menghilangkan perulangan tadi dibutuhkan kunci yang juga sangat panjang. Oleh karena itu, penulis merasa perlu untuk mengajukan modifikasi yang memenuhi kriteria sebagai berikut:

1. Mempersulit serangan dengan metode Kasiski
2. Mempertahankan kesederhanaan *Vigènere Cipher*. Enkripsi dan dekripsi harus cukup sederhana untuk dilakukan tanpa alat bantu.

2. USULAN MODIFIKASI PADA VIGÈNERE CIPHER

Pada *Vigènere Cipher*, jika panjang kunci lebih pendek dari pada panjang pesan plainteks, maka kunci digunakan secara periodik/berulang [1]. Jika kunci terlalu pendek, maka pengulangan kunci menjadi banyak. Hal ini meningkatkan kemungkinan terjadinya suatu susunan huruf pada plainteks dienkripsi dengan suatu susunan huruf kunci tertentu berkali-kali yang berakibat banyaknya perulangan susunan huruf pada cipherteks. Untuk mempersulit serangan dengan metode Kasiski kita harus mengurangi atau menghilangkan pengulangan kunci. Salah satu cara untuk mencapai ini ialah dengan melakukan pergeseran tambahan (*adjustment*) sejauh nilai tertentu yang dibangkitkan dari kunci.

```
Plainteks    : PLAINTEKSMESSAGE
Kunci        : keykeykeykeykeyk
Adjustment+  : xyz............
Cipherteks   : ...............
```

Dengan melakukan pergeseran ini maka kita seakan-akan memiliki kunci yang lebih panjang. Misal panjang kunci m karakter dan panjang *stream* pergeseran yang dihasilkan memiliki panjang n karakter, maka kunci baru akan benar-benar berulang setelah m*n karakter. Semakin panjang dan acak *stream* pergeseran ini maka akan semakin sulit untuk melakukan serangan dengan metode Kasiski. Namun untuk memenuhi kriteria kedua harus dilakukan kompromi keamaan dan kesederhanaan.

Untuk mempertahankan kesederhanaan proses enkripsi dan dekripsi, maka algoritma pembangkit *stream* pergeseran tidak boleh terlalu rumit, misalnya menggunakan kunci dengan tiap karakternya digandakan.

```
Plainteks    : PLAINTEKSMESSAGE
Kunci        : keykeykeykeykeyk
Adjustment+  : kkeeyykkeeyy....
Cipherteks   : ...............
```

Jika panjang kunci m karakter, maka kunci akan benar-benar berulang setelah setiap m*2 karakter. Hal ini mungkin belum cukup untuk menghalangi serangan metode Kasiski. Untuk mengatasinya tiap karakter dikalikan dengan panjang kunci sehingga perulangan kunci baru terjadi setelah m^2 karakter.

```
Plainteks    : PLAINTEKSMESSAGE
Kunci        : keykeykeykeykeyk
```

Adjustment+ : kkkeeeyyykkk....
Cipherteks : ....

Jika algoritma enkripsi dan dekripsi bersifat terbuka (tidak dirahasiakan), maka algoritma ini akan sangat mudah diserang dengan metode *chosen-text attack*, karena huruf pertama dienkripsi dengak dua huruf yang sama (dalam contoh k+k). Setelah huruf tersebut ditemukan, sisa kunci dapat dicari karena enkripsi huruf kedua sampai dengan panjang kunci dienkripsi dengan huruf _+k. Untuk mengatasi ini *stream* pergeseran dibalik.

Plainteks : PLAINTEKSMESSAGE
Kunci : keykeykeykeykeyk
Adjustment+ : yyyeeekkkyyy....
Cipherteks : ....

3. HASIL DAN PEMBAHASAN

3.1 Implementasi

Algoritma yang dirancang diimplementasikan dalam sebuah program kecil dalam bahasa C. Program menerima parameter file masukan, file keluaran, dan kunci. Program membaca file masukan melakukan enkripsi/dekripsi dengan kunci yang diberikan dan menuliskannya ke file keluaran.

Proses enkripsi yang diimplementasikan seperti yang dicantumkan pada potongan kode berikut.

```
unsigned char enkrip (unsigned char cin,
unsigned char key, unsigned char key2)
{
  unsigned char cc;
  unsigned char c = 'A';

  cin -= c;
  key -= c;
  key2 -= c;

  cc = cin + key + key2;
  cc = cc % 26;
  cc += c;

  return cc;
}
```

cin : karaker yang di enkripsi;
key : karakter pada kunci;
key2 : karakter pada *stream* pergeseran tambahan

Cara lain melakukan enkripsi adalah dengan melakukan enkripsi menggunakan *Vigènere Cipher* sebanyak 2 kali. Pertama dengan kunci dan kedua dengan stream pergeseran yang dibangkitkan dari kunci.

Dekripsi dilakukan sebaliknya.

```
unsigned char dekrip (unsigned char cin,
unsigned char key, unsigned char key2)
{
  unsigned char cc;
  unsigned char c = 'A';

  cin -= c;
  key -= c;
  key2 -= c;

  cin += 52;
  cc = cin - key - key2;
  cc = cc % 26;
  cc += c;

  return cc;
}
```

Sebagai pembanding juga dilakukan implementasi *Vigènere Cipher* yang belum dimodifikasi.

3.2 Pengujian

Untuk pengujian, dilakukan enkripsi terhadap sebuah pesan teks dengan *Vigènere Cipher*, dan *Vigènere Cipher* yang sudah dimodifikasi. Pesan teks yang dipilih adalah sebuah artikel berbahasa Inggris mengenai gerhana matahari menggunakan kunci berupa kata 'LANGIT'. Pemilihan artikel tersebut dikarenakan artikel tersebut sudah berhasil dipecahkan dengan metode Kasiski dan analisis frekuensi pada Tugas 1 IF5054 Kriptanalisis Sederhana. Artikel tersebut dikoversi menjadi upper-case tanpa spasi, sesuai format yang diterima oleh program kecil yang dibuat.

```
HUNDREDSOFBANDUNGR...
```

Artikel selengkapnya dapat dilihat pada lampiran A.

3.2.1 Hasil Enkripsi

Enkripsi dengan *Vigènere Cipher*:

Plainteks : HUNDREDSOFBANDUNGR...
Kunci : LANGITLANGITLANGIT...
Cipherteks : SUAJZXOSBLJTYDHTOK...

Enkripsi dengan *Vigènere Cipher* yang telah dimodifikasi:

Plainteks : HUNDREDSOFBANDUNGR...
Kunci : LANGITLANGITLANGIT...
Adjustment+ : TTTTTTIIIIIIGGGGGG...
Cipherteks : LNTCSQWAJTRBEJNZUQ...

Hasil enkripsi selengkapnya dapat dilihat pada lampiran A.

3.2.2 Pengujian terhadap Serangan Metode Kasiski

Kita lakukan pencarian kriptogram yang berulang pada cipherteks. Pencarian dilakukan dengan menggunakan sebuah applet java ciptaan Tom Linton (http://pages.central.edu/emp/LintonT/classes/spring01/cryptography/java/kasiski.html). Pada *Vigènere Cipher* yang belum dimodifikasi terdapat banyak kriptogram yang berulang. Kriptogram yang berulang bahkan ada yang mencapai 10 huruf yaitu 'SEBHAXCVNZ' pada posisi 258-267 dan posisi 426-435.

Berikut daftar beberapa trigram yang paling banyak muncul beserta posisinya :
MSE 6 kali : 35, 257, 275, 353, 425, 467
MGE 3 kali : 22, 538, 694
PRI 3 kali : 48, 126, 631
TOA 3 kali : 167, 216, 504

MPR 3 kali : 173, 197, 401
NTL 3 kali : 176, 572, 608
ZPX 3 kali : 219, 525, 645
PUV 3 kali : 248, 512, 650
UVW 3 kali : 249, 513, 651
BTW 3 kali : 358, 662, 764
WFP 3 kali : 389, 664, 760
TUK 3 kali : 409, 679, 733

Jumlah trigram yang muncul berulang adalah 100 trigram.

Daftar selengkapnya dapat dilihat pada lampiran B.

Pada Vigènere Cipher yang dimodifikasi, kemunculan kriptogram yang berulang jauh lebih sedikit yaitu 37 trigram. Berikut adalah beberapa trigram yang paling banyak muncul pada vigènere yang telah dimodifikasi beserta posisinya :
YEW 3 kali : 176, 572, 608
XMH 3 kali : 215, 315, 503

Setelah diperiksa, ternyata perulangan kriptogram pada cipherteks yang benar-benar disebabkan oleh perulangan pada plainteks hanya ada 1 yaitu "IYFEOB" pada posisi 682-687 dan posisi 826-831. Kriptogram ini bersesuaian dengan kata plainteks "PUBLIC". Jarak perulangan ini adalah 144 karakter.

Berhubung perulangan trigram yang benar-benar disebabkan oleh perulangan pada plainteks hanya satu, sulit untuk mencari panjang kunci. Tidak ada pasangan angka untuk dicari faktor persekutuannya. Adanya 36 trigram berulang yang bukan disebabkan perulangan plainteks juga bersifat mengecoh dan mempersulit penentuan panjang kunci.

3.2.3 Analisis Frekuensi

Dilakukan analisis frekuensi huruf pada kedua cipherteks. Dari hasil yang diperoleh terlihat bahwa sebaran huruf pada *Vigènere Cipher* yang telah dimodifikasi lebih seragam.

Pada *Vigènere Cipher*, frekuensi kemunculan huruf pada cipherteks yang digunakan berkisar antara 13 dan 56. Pada *Vigènere Cipher* yang dimodifikasi, frekuensi kemunculan huruf pada cipherteks berkisar antara 19 dan 52.

Hasil selengkapnya dapat dilihat pada lampiran B.

3.3 Analisis terhadap Serangan Kriptanalisis Umum Lain.

Sebagaimana algoritma kriptografi klasik pada umumnya, keamanan Vigènere Cipher tidak hanya bergantung pada kerahasiaan kunci. Kerahasian algoritma juga berpengaruh terhadap keamanan data.

Jika algoritma tidak dirahasiakan, maka dalam kasus serangan secara *brute-force*, Vigènere Cipher yang telah dimodifikasi hanya sedikit lebih aman daripada Vigènere Cipher yang biasa. Hal ini karena *stream* pergeseran (*adjustment*) diturunkan secara sederhana dari kunci. Perpanjangan semu kunci hanya memperlambat pencarian secara *brute-force*.

Dalam serangan dengan *chosen-text attack* pada *Vigènere Cipher*, enkripsi plainteks 'AAAAA....' akan menghasilkan cipherteks berupa kunci. Pada *Vigènere Cipher* yang telah dimodifikasi, enkripsi plainteks 'AAAAA...' akan menghasilkan cipherteks berupa kunci+*stream* pergeseran%26. Jika kunci pendek, maka tidak terlalu sulit untuk mencari kunci yang digunakan. Untungnya penggunanan *Vigènere Cipher* yang memungkinkan serangan secara *chosen-text attack* sangat langka.

Perlu diingat bahwa *Vigènere Cipher* bukanlah algoritma yang sesuai untuk mengenkripsi data secara serius. *Vigènere Cipher* hanya cocok untuk digunakan dalam pembelajaran atau kegiatan iseng/hiburan.

4. KESIMPULAN

Modifikasi sederhana yang dilakukan pada algoritma Vigènere Cipher mampu menghalangi serangan sengan metode Kasiski. Di sisi lain, proses enkripsi dan dekripsi masih sangat sederhana dan dapat dengan mudah dilakukan hanya dengan pensil dan kertas tanpa alat bantu komputasi.

Meskipun demikian, dalam menghadapi serangan secara *brute-force*, modifikasi yang dilakukan tidak banyak membantu. Akan tetapi, kriptanalisis secara *brute-force* masih membutuhkan manusia untuk memeriksa hasil dekripsi yang mana yang memiliki makna. Sangat sedikit mungkin orang yang mau malakukan hal tersebut mengingat Vigènere Cipher tidak digunakan untuk mengenkripsi data yang benar-benar serius.

Berikut adalah beberapa kelebihan yang dimiliki modifikasi Vigènere Cipher ini :

- Sulit menemukan perulangan susunan huruf pada cipherteks
- Jika ditemukan perulangan susunan huruf pada cipherteks, kemungkinan hal ini disebabkan oleh perulangan susunan huruf pada plainteks kecil.
- Sebaran huruf lebih seragam.
- *Stream* pergeseran dibangkitkan dari kunci sehingga walaupun mengetahui panjang kunci, kriptanalisis masih sulit dilakukan

Adapun kekurangan modifikasi ini adalah:

- Tidak banyak berpengaruh terhadap serangan *brute-force*.
- Proses enkripsi dan dekripsi menjadi lebih rumit.

DAFTAR REFERENSI

[1] Munir, Rinaldi, *Diktat Kuliah IF5054 Kriptografi*, Institut Teknologi Bandung, 2006, hal 52-56.

Lampiran A Dokumen Plainteks dan Cipherteks

Pesan plainteks:

```
HUNDREDSOFBANDUNGRESIDENTSFLOCKEDTOTHEBOSSCHAOBSERVATORYINLEMBANGNORTHBANDUNGTOCATC
HAGLIMPSEOFTHETOTALLUNARECLIPSEONTUESDAYOBSERVATIONACTIVITIESWEREFOCUSSEDATTHEVANAL
BADACENTERANDAIREDLIVEBYTVRISTATERUNTELEVISIONSTATIONTHEEIGHTBOSSCHAASTRONOMERSWHOC
ONDUCTEDTHEOBSERVATIONSAIDTHEYWERESATISFIEDALTHOUGHTHETELESCOPESWEREONLYEFFECTIVETE
NMINUTESINTOTHEPEAKOFTHETOTALLUNARECLIPSEWITHTRAFFICBACKEDUPONEKILOMETERALONGTHEROA
DLEADINGTOTHEOBSERVATORYASTRONOMERSWEREFORCEDTOSHARETHEVIXENTELESCOPEWITHVISITORSOB
SERVATIONSWERECONDUCTEDATOPTHEVANALBADACENTERBYUSINGTWOCELESTRONTELESCOPESANDONEWIL
LIAMOPTICSMEASURINGTWENTYCMANDSEVENCMINDIAMETERRESPECTIVELYITWASTHESECONDTIMEASTRON
OMERSHADINVITEDTHEPUBLICTOANEVENTANDALLOWEDITTOBROADCASTLIVEONTVAFTERTHEPREVIOUSMAR
SFULLMOONPHENOMENONONAUGUSTAGEGERKALONGRESIDENTRINDACAMEWITHSIXOFHERROOMMATESBYPUBL
ICBUSTOWITNESSTHESPECTACLE
```

Cipherteks dengan Vigènere Cipher biasa menggunakan kunci “LANGIT”:

```
SUAJZXOSBLJTYDHTOKPSVJMGESSRWVVEQZWMSEOUALNHNUJLPRIGBHCYVTTXXBNTOGZRGNJTYDHTOMZCNZK
ALGYOUIDEBLBAPTBZIEWUAGZXNLVVAXZNGAMLOALUJLPRIGBBZNNIBBGIGOMLHEEKNHNUFYMWLTGNMOLNNR
JTOAPKVMPRNTLTTRRJTBGEOEBOCIFZIMPRHTBXWEIOABZNFZIMTOAZPXPITNBUZSFIPTLSGXWGZMRXAPSOP
UVWFCGKLMSEBHAXCVNZQHYSNOLMSELCMKPSNZQLQIRJIEEHBAOAEHRZMEPSPUXXDWRXMHYLLKNYPCGODXEE
ASQGFTRYQGEOGNMIPAXUNMSEGUBTWLHTIKPCYOXLPWVZPMCASLQVMAPQMWFPBTMDTLBSMMPRNRWGRTUKZHL
DYKIWTNTZWMSEBHAXCVNZWKJAFZZHYOZKZLHEEKNHCCRJBHDHNXMMSEIOFXYTRRMLNOCKEBEHIOABEOEYWU
DEEBIMTOAYEXCEPUVWFCGKLTEOCZPXGAAGTULDNIMGEEEHGNDIAMBPZCRRMLERBTBXWEFIWIPSNTLHYEJOT
ETAZUXMTCFSMTDUEOVZEWRTBRNMNTLLPVRTKFTNQOIFPTRXZXDPRIBBGEYEQMHAFZPXDEPUVWEIZKILERBT
WFPRFNIWTNIOBXOTUKXNMLVIBHLNRBMGEAAJIEWOJKLBETBHZHLDPGAMWIIKWGEVNLBXCTUKXKPVVUCLXAE
YNNWLZUWGAHRTWFPNBTWGLUTAAMLGRMMKVAYUVZCEFOLXYTEOVWLCNSMPTTUYQQZFUKZKZOZSIMPSOEXNML
VIJNDTBCQMYEFYBAPSCKKMLCYK
```

Cipherteks dengan Vigènere Cipher yang sudah dimodifikasi menggunakan kunci “LANGIT”:

```
LNTCSQWAJTRBEJNZUQCFIWZTESSRWVGPBKHXLXHNTEVPVCRTVXOMHNPLIGGKXBNTOGKCRYUERWAMHFHKVHS
IRMEUAOQROYONPTBZIEHFLRKIGEOOTQHVOIUTUGRAPRCEVTOOZNNIBBRTRZXWAXXDGAVCNGUERZMTSUYAAE
WGOAPKVMACYEWEMKKCMUOMWMJWIOLFOSCEUGOKWEIOABKYQKTXMHTSIQXQBVJCFYLOVZYFTKJTZMRXAPDZA
FGHYVZDEFAMJPIFIBTFWNLFABYZSELCMKADYKBWJBKCBXMPJIWIKNXFSKCFCHKKDWRXMHJWWVYJIVZHWQMM
IAYOLZXEWMRBTAZVPAXUNMDPRFMEPEAMBDXKGWFTVCBFVSPNFYDIMAPQMWQAMEXOMEULFFXZVZEOXZAQFNY
QLXVJTNTZWMDPMSLIVOGSPDRINHHPEUFQFRURRXAUCCRJBHOSYIXXLXBHYQGBZZUTTUIQKHRUVBNOEOEYWU
OPPMTXMHTRXQKMXCDELIMQRZRBPMCKGAAGTUWOYTXRXXXAZGLQIUJXFIXXSRREOGOKWEFIWIADYEWSRXCHM
XBIHCFUZILYSZQHRBIMEWRTBRYXYEWWIOKMDYBVYWQNVZXDFDQCEVOOGEYEQMSLQKAIWXINOPMQHSQTKXHZ
CLCESAVJTNIOBXZEFVIYFEOBUATVZJUOKGGPOKJBWXYOETBHZHWOARLXPBBDPZMDVTJFIZAQDQCIIHPYXAE
YNNHWKFHRTAKMPYXVJBEORAZGGSYTEZZXVAYUVZNPQZWIRMXHOPTKVAUXZZAEWWMSHXMXZOZSIMADZPIYFE
OBCGLBJKYUEKLEHGCFPXXZLCYK
```

Lampiran B Hasil Analisis Frekuensi dan Pencarian Perulangan Susunan Tripel.

Vigènere Cipher biasa

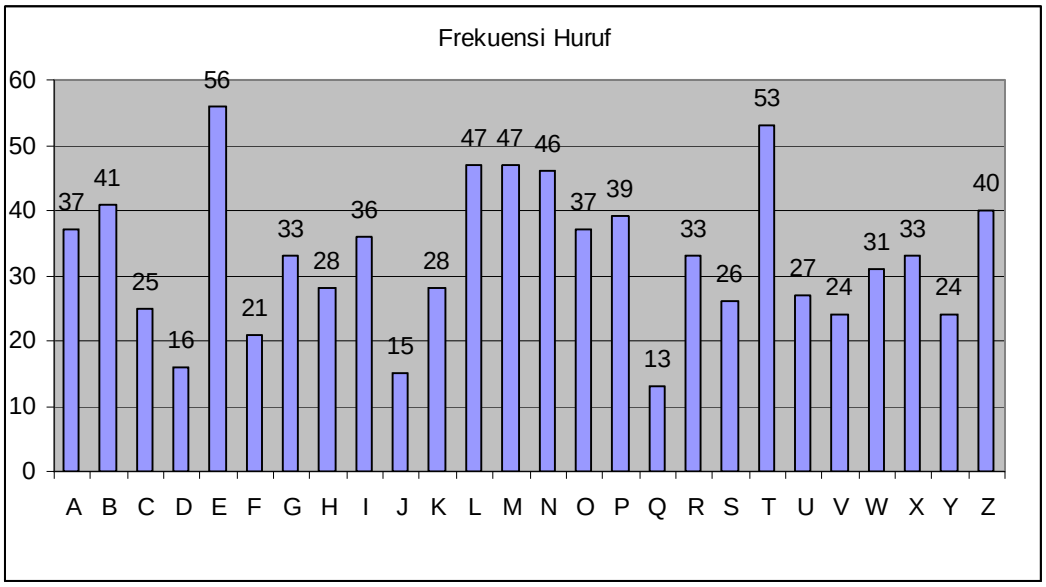
Kemunculan kriptogram berulang (keluaran dari appet buatan Tom Linton):

```
JTY: occurs 2 times, at pos 10, 70
     distance(s): 60
TYD: occurs 2 times, at pos 11, 71
     distance(s): 60
YDH: occurs 2 times, at pos 12, 72
     distance(s): 60
DHT: occurs 2 times, at pos 13, 73
     distance(s): 60
HTO: occurs 2 times, at pos 14, 74
     distance(s): 60
KPS: occurs 2 times, at pos 17, 281
     distance(s): 264
MGE: occurs 3 times, at pos 22, 538, 694
     distance(s): 516, 672, 156
ZWM: occurs 2 times, at pos 33, 423
     distance(s): 390
WMS: occurs 2 times, at pos 34, 424
     distance(s): 390
MSE: occurs 6 times, at pos 35, 257, 275, 353, 425, 467
     distance(s): 222, 240, 318, 390, 432, 18, 96, 168,
210, 78, 150, 192, 72, 114, 42
NHN: occurs 2 times, at pos 42, 148
     distance(s): 106
HNU: occurs 2 times, at pos 43, 149
     distance(s): 106
UJL: occurs 2 times, at pos 45, 123
     distance(s): 78
JLP: occurs 2 times, at pos 46, 124
     distance(s): 78
LPR: occurs 2 times, at pos 47, 125
     distance(s): 78
PRI: occurs 3 times, at pos 48, 126, 631
     distance(s): 78, 583, 505
RIG: occurs 2 times, at pos 49, 127
     distance(s): 78
IGB: occurs 2 times, at pos 50, 128
     distance(s): 78
BAP: occurs 2 times, at pos 94, 844
     distance(s): 750
IEW: occurs 2 times, at pos 100, 700
     distance(s): 600
GAM: occurs 2 times, at pos 116, 717
     distance(s): 601
AML: occurs 2 times, at pos 117, 772
     distance(s): 655
BZN: occurs 2 times, at pos 131, 209
     distance(s): 78
IBB: occurs 2 times, at pos 135, 633
     distance(s): 498
BBG: occurs 2 times, at pos 136, 634
     distance(s): 498
LHE: occurs 2 times, at pos 143, 449
     distance(s): 306
HEE: occurs 2 times, at pos 144, 450
     distance(s): 306
EEK: occurs 2 times, at pos 145, 451
     distance(s): 306
EKN: occurs 2 times, at pos 146, 452
     distance(s): 306
KNH: occurs 2 times, at pos 147, 453
     distance(s): 306
GNM: occurs 2 times, at pos 158, 344
     distance(s): 186
RJT: occurs 2 times, at pos 165, 182
     distance(s): 17
TOA: occurs 3 times, at pos 167, 216, 504
     distance(s): 49, 337, 288
MPR: occurs 3 times, at pos 173, 197, 401
     distance(s): 24, 228, 204
PRN: occurs 2 times, at pos 174, 402
     distance(s): 228
NTL: occurs 3 times, at pos 176, 572, 608
     distance(s): 396, 432, 36
TRR: occurs 2 times, at pos 180, 475
     distance(s): 295
BGE: occurs 2 times, at pos 185, 635
     distance(s): 450
GEO: occurs 2 times, at pos 186, 341
     distance(s): 155
EOE: occurs 2 times, at pos 187, 492
     distance(s): 305
FZI: occurs 2 times, at pos 194, 212
     distance(s): 18
ZIM: occurs 2 times, at pos 195, 213
     distance(s): 18
IMP: occurs 2 times, at pos 196, 820
     distance(s): 624
TBX: occurs 2 times, at pos 201, 561
     distance(s): 360
BXW: occurs 2 times, at pos 202, 562
     distance(s): 360
XWE: occurs 2 times, at pos 203, 563
     distance(s): 360
WEI: occurs 2 times, at pos 204, 653
     distance(s): 449
EIO: occurs 2 times, at pos 205, 469
     distance(s): 264
IOA: occurs 2 times, at pos 206, 488
     distance(s): 282
OAB: occurs 2 times, at pos 207, 489
     distance(s): 282
IMT: occurs 2 times, at pos 214, 502
     distance(s): 288
MTO: occurs 2 times, at pos 215, 503
     distance(s): 288
ZPX: occurs 3 times, at pos 219, 525, 645
     distance(s): 306, 426, 120
APS: occurs 2 times, at pos 244, 845
     distance(s): 601
PSO: occurs 2 times, at pos 245, 822
     distance(s): 577
PUV: occurs 3 times, at pos 248, 512, 650
     distance(s): 264, 402, 138
UVW: occurs 3 times, at pos 249, 513, 651
     distance(s): 264, 402, 138
VWF: occurs 2 times, at pos 250, 514
     distance(s): 264
WFC: occurs 2 times, at pos 251, 515
     distance(s): 264
FCG: occurs 2 times, at pos 252, 516
     distance(s): 264
CGK: occurs 2 times, at pos 253, 517
     distance(s): 264
GKL: occurs 2 times, at pos 254, 518
     distance(s): 264
LMS: occurs 2 times, at pos 256, 274
     distance(s): 18
SEB: occurs 2 times, at pos 258, 426
     distance(s): 168
EBH: occurs 2 times, at pos 259, 427
     distance(s): 168
BHA: occurs 2 times, at pos 260, 428
     distance(s): 168
HAX: occurs 2 times, at pos 261, 429
     distance(s): 168
AXC: occurs 2 times, at pos 262, 430
     distance(s): 168
XCV: occurs 2 times, at pos 263, 431
     distance(s): 168
CVN: occurs 2 times, at pos 264, 432
     distance(s): 168
VNZ: occurs 2 times, at pos 265, 433
     distance(s): 168
NZQ: occurs 2 times, at pos 266, 284
     distance(s): 18
PSN: occurs 2 times, at pos 282, 570
     distance(s): 288
JIE: occurs 2 times, at pos 291, 699
     distance(s): 408
EEH: occurs 2 times, at pos 293, 541
     distance(s): 248
BTW: occurs 3 times, at pos 358, 662, 764
     distance(s): 304, 406, 102
WFP: occurs 3 times, at pos 389, 664, 760
     distance(s): 275, 371, 96
TUK: occurs 3 times, at pos 409, 679, 733
     distance(s): 270, 324, 54
UKZ: occurs 2 times, at pos 410, 812
     distance(s): 402
ZHL: occurs 2 times, at pos 412, 712
     distance(s): 300
HLD: occurs 2 times, at pos 413, 713
     distance(s): 300
IWT: occurs 2 times, at pos 418, 670
     distance(s): 252
WTN: occurs 2 times, at pos 419, 671
     distance(s): 252
AFZ: occurs 2 times, at pos 439, 643
     distance(s): 204
ZKZ: occurs 2 times, at pos 446, 814
     distance(s): 368
XYT: occurs 2 times, at pos 473, 791
     distance(s): 318
RRM: occurs 2 times, at pos 476, 554
     distance(s): 78
RML: occurs 2 times, at pos 477, 555
     distance(s): 78
EPU: occurs 2 times, at pos 511, 649
     distance(s): 138
TEO: occurs 2 times, at pos 521, 793
     distance(s): 272
LER: occurs 2 times, at pos 557, 659
     distance(s): 102
ERB: occurs 2 times, at pos 558, 660
     distance(s): 102
RBT: occurs 2 times, at pos 559, 661
     distance(s): 102
EOV: occurs 2 times, at pos 596, 794
     distance(s): 198
TWF: occurs 2 times, at pos 663, 759
     distance(s): 96
UKX: occurs 2 times, at pos 680, 734
     distance(s): 54
XNM: occurs 2 times, at pos 682, 826
     distance(s): 144
NML: occurs 2 times, at pos 683, 827
```

```
     distance(s): 144
MLV: occurs 2 times, at pos 684, 828
     distance(s): 144
```

```
LVI: occurs 2 times, at pos 685, 829
     distance(s): 144
```

Daftar frekeunsi kemunculan huruf:

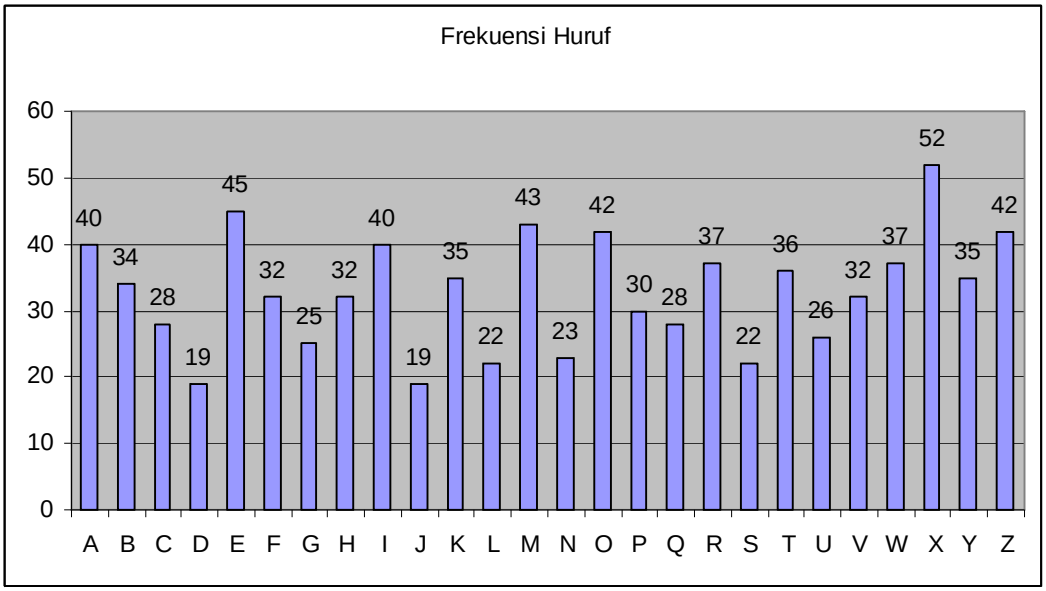


Vigènere Cipher yang sudah dimodifikasi

Kemunculan kriptogram berulang (keluaran dari appet buatan Tom Linton):

```
FIW: occurs 2 times, at pos 19, 566
     distance(s): 547
XLX: occurs 2 times, at pos 35, 467
     distance(s): 432
XOM: occurs 2 times, at pos 49, 394
     distance(s): 345
YUE: occurs 2 times, at pos 69, 838
     distance(s): 769
UER: occurs 2 times, at pos 70, 154
     distance(s): 84
IRM: occurs 2 times, at pos 83, 791
     distance(s): 708
MEU: occurs 2 times, at pos 85, 396
     distance(s): 311
CEV: occurs 2 times, at pos 126, 631
     distance(s): 505
AEW: occurs 2 times, at pos 164, 806
     distance(s): 642
YEW: occurs 3 times, at pos 176, 572, 608
     distance(s): 396, 432, 36
WIO: occurs 2 times, at pos 191, 611
     distance(s): 420
GOK: occurs 2 times, at pos 201, 561
     distance(s): 360
OKW: occurs 2 times, at pos 202, 562
     distance(s): 360
KWE: occurs 2 times, at pos 203, 563
     distance(s): 360
TXM: occurs 2 times, at pos 214, 502
     distance(s): 288
XMH: occurs 3 times, at pos 215, 315, 503
     distance(s): 100, 288, 188
MHT: occurs 2 times, at pos 216, 504
     distance(s): 288
RXA: occurs 2 times, at pos 242, 452
     distance(s): 210
ADY: occurs 2 times, at pos 282, 570
     distance(s): 288
IWI: occurs 2 times, at pos 297, 567
     distance(s): 270
ZHW: occurs 2 times, at pos 326, 712
     distance(s): 386
MDP: occurs 2 times, at pos 353, 425
     distance(s): 72
IMA: occurs 2 times, at pos 383, 820
     distance(s): 437
ZAQ: occurs 2 times, at pos 409, 733
     distance(s): 324
XVJ: occurs 2 times, at pos 417, 762
     distance(s): 345
VJT: occurs 2 times, at pos 418, 670
     distance(s): 252
JTN: occurs 2 times, at pos 419, 671
     distance(s): 252
MSL: occurs 2 times, at pos 428, 641
     distance(s): 213
IXX: occurs 2 times, at pos 465, 553
     distance(s): 88
AZG: occurs 2 times, at pos 543, 769
     distance(s): 226
EWW: occurs 2 times, at pos 609, 807
     distance(s): 198
DQC: occurs 2 times, at pos 629, 736
     distance(s): 107
IYF: occurs 2 times, at pos 682, 826
     distance(s): 144
YFE: occurs 2 times, at pos 683, 827
     distance(s): 144
FEO: occurs 2 times, at pos 684, 828
     distance(s): 144
EOB: occurs 2 times, at pos 685, 829
     distance(s): 144
PYX: occurs 2 times, at pos 742, 760
     distance(s): 18
```

Daftar frekuensi kemunculan tiap huruf:


Frekuensi Huruf
60
50
40
30
20
10
0
40
34
28
19
45
32
25
32
40
19
35
22
43
23
42
30
28
37
22
36
26
32
37
52
35
42
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