Modifikasi Algoritma Kriptografi Klasik *Vigenère* dengan Sistem Periodik Parsial

Dendy Narendra
Program Studi Teknik Informatika STEI ITB, Bandung, NIM: 13504033

Abstraksi *– Makalah ini membahas modifikasi algoritma kriptografi klasik* Vigenère *dengan menggunakan kunci yang pengulangannya parsial. Yaitu karakter kata kunci berkurang secara teratur di tiap kali pengulangan.*

Dengan menggunakan pola pengulangan parsial yang berkurang ini diharapkan akan makin menyulitkan kriptanalisis penerkaan panjang kunci dengan menggunakan metoda Kasiski. *Terutama dengan menggunakan kata kunci yang relatif panjang*

Kata Kunci*: Algoritma kriptografi klasik,* Vigenère*, modifikasi algoritma, pengulangan parsial, kata kunci yang berkurang, metode* Kasiski.

1. PENDAHULUAN

Algoritma kriptografi (*cipher*) klasik *Vigenère* merupakan salah satu contoh terbaik dari *cipher* abjad-majemuk.

Vigenère Cipher yang dikenal luas sekarang pertama kali disebutkan oleh *Giovan Battista Bellaso* pada tahun 1553 di bukunya *La Cifra del. Sig. Giovan Battista Bellaso.* Baru kemudian pada tahun 1586, *Blaise de Vigenère* menerbitkan algoritma yang mirip tetapi dengan *autokey* yang lebih kuat. Kemudian pada abad 19 *cipher* tersebut disalah persepsikan sebagai penemuan *Vigenère.* Karena itulah hingga kini *cipher* tersebut lebih dikenal dengan nama *Vigenère cipher.*

Vigenère Cipher terkenal karena kesulitannya untuk dipecahkan. Pada abad ke-19 bahkan sempat mendapat predikat *unbreakable cipher* atau *cipher* yang tidak terpecahkan, hingga akhirnya berhasil dipecahkan oleh *Kasiski*, pada abad yang sama.

Vigenère Cipher populer ketika digunakan oleh Tentara Konfiderasi (*Confederate Army*) pada Perang Sipil Amerika (*American Civil War*). Pihak *Union* berhasil memenangkan perang tersebut karena keberhasilannya memecahkan kode-kode rahasia hasil *Vigenère Cipher* dari pihak Konfiderasi.

2. DAFTAR ISTILAH

- *Cipher*:
  algoritma kriptografi
- Cipherteks:
  pesan tersandi
- Dekripsi:
  proses mengembalikan cipherteks menjadi plainteks
- Enkripsi:
  proses menyandikan plainteks menjadi cipherteks
- Plainteks
  pesan jelas/ asli
- Kriptanalis
  pelaku kriptanalisis
- Kriptanalisis
  ilmu memecahkan sipherteks tanpa mengetahui kata kunci yang digunakan
- Sistem periodik:
  pengulangan kata kunci pada *Vigenère Cipher* untuk menyamakan panjang kunci dengan panjang plainteks

3. DASAR TEORI

3.1. *Vigenère Cipher* Klasik

Vigenère Cipher menggunakan bujur sangkar *Vigenère* untuk melakukan enkripsi. Kolom paling kiri dari bujur sangkar menyatakan huruf-huruf kata kunci, sedangkan baris paling atas bujur sangkar menyatakan huruf-huruf plainteks.

Setiap baris di dalam bujur sangkar menyatakan huruf-huruf cipherteks yang diperoleh dengan *Caesar Cipher*, yang mana jauh pergeseran huruf plainteks ditentukan dari nilai desimal huruf kunci yang berkorespondensi dengan baris tersebut. Dimana a=0, b=1, ..., z=25.

Bujursangkar *Vigenère* digunakan untuk memperoleh cipherteks dengan menggunakan kata kunci yang sudah ditentukan. Jika panjang kata kunci lebih pendek daripada panjang plainteks, maka kata kunci diulang penggunaannya (sistem periodik). Bila panjang kata kunci adalah m, maka periodenya dikatakan m.

Sebagai contoh jika plainteks adalah `MODIFIKASI CIPHER VIGENÈRE` dan kata kunci adalah `KUNCI`, maka penggunaan kunci secara periodik adalah sebagai berikut:

Plainteks:
`MODIFIKASI CIPHER VIGENÈRE`
Kunci:
`KUNCIKUNCI KUNCIK UNCIKUNC`

Contoh 1.1-Vigenère Cipher klasik

Setiap huruf plainteks akan dienkripsi dengan setiap kunci di bawahnya.

Untuk melakukan enkripsi dengan *Vigenère Cipher* dapat dilakukan dengan menggunakan bujursangkar *Vigenère*. Tarik garis vertikal dari huruf plainteks ke bawah, lalu terik garis mendatar dari huruf kunci ke kanan. Perpotongan kedua garis tersebut menyatakan huruf cipherteksnya.

Sebagai contoh untuk plainteks diatas, tarik garis vertikal dari huruf M di baris teratas dan tarik garis mendatar dari huruf K di kolom terkiri, perpotongannya adalah pada kotak yang berisi huruf W.

Untuk huruf cipherteks kedua, tarik garis vertikal dari huruf O di baris teratas dan tarik garis mendatar dari huruf U di kolom terkiri, perpotongannya adalah pada kotak yang berisi huruf I.

Demikian juga dengan huruf-huruf berikutnya hingga diperoleh cipherteks sebagai berikut:

Plainteks:
`MODIFIKASI CIPHER VIGENÈRE`
Kunci:
`KUNCIKUNCI KUNCIK UNCIKUNC`
Cipherteks:
`WIQKNSENUQ MCCJMB PVIMXYEG`

Contoh 1.2-Vigenère Cipher klasik dengan cipherteks hasil enkripsi

Selain dengan menggunakan bujursangkar *Vigenère*, enkripsi *Vigenère Cipher* juga bisa ditulis secara aljabar yaitu dengan menggunakan rumus:

$$C_i \equiv (P_i + K_i) \bmod 26$$

Dimana:

- C_i = nilai desimal karakter cipherteks ke-i
- P_i = nilai desimal karakter plainteks ke-i
- K_i = nilai desimal karakter kunci ke-i

3.2. Metode *Kasiski*

Pada tahun 1863, *Friedrich Kasiski* menemukan cara memecahkan *Vigenère Cipher*. Metodenya membantu menemukan panjang kunci yang digunakan pada cipherteks yang menggunakan *Vigenère Cipher* pada proses enkripsinya.

Metode *Kasiski* memanfaatkan keuntungan bahwa bahasa Inggris tidak hanya mengandung perulangan huruf tetapi juga perulangan pasangan huruf atau tripel huruf, seperti TH, THE, dan sebagainya. Perulangan kelompok huruf ini memungkinkan menghasilkan kriptogram yang berulang.

Secara intuitif dapat dibuat argumentasi bahwa jika jarak antara dua buah *string* yang berulang di dalam plainteks merupakan kelipatan dari panjang kunci, maka *string* yang sama tersebut akan muncul menjadi kriptogram yang sama pula di dalam cipherteks.

Menurut metode *Kasiski*, untuk menentukan panjang kunci, langkah-langkahnya sebagai berikut:

1. Kriptanalis menghitung semua kriptogram yang berulang di dalam cipherteks (pesan yang panjang biasanya mengandung kriptogram yang berulang). Kemudian jarak antara kriptogram yang berulang dihitung.
2. Kriptanalis menghitung semua faktor pembagi dari jarak tersebut. Faktor pembagi menyatakan panjang kunci yang mungkin. Irisan dari himpunan faktor tersebut mungkin merupakan panjang kunci. Hal ini karena *string* yang berulang dapat muncul bertindihan, tetapi sangat mungkin terjadi huruf yang sama dienkripsi dengan huruf kunci yang sama. Huruf-huruf kunci diulang pada kelipatan panjang kunci, sehingga jarak yang ditemukan pada langkah satu sangat mungkin merupakan kelipatan panjang kunci.

4. PERMASALAHAN

4.1. *Vigenère* Dengan Sistem Periodik Parsial

Pada makalah ini diajukan modifikasi terhadap *Vigenère Cipher* untuk menambah kerumitan pemecahan pada kriptanalisis dengan menggunakan metode *Kasiski*. Modifikasi yang dilakukan disini adalah penggunaan sistem periodik parsial, dimana pengulangan kata kunci untuk menyamakan panjang kata kunci dengan plainteks tidak langsung dilakukan secara utuh, tetapi berubah secara teratur. Selanjutnya dalam makalah ini, *cipher* modifikasi ini akan disebut *Vigenère Cipher* modifikasi saja.

Pengulangan yang berubah secara teratur disini bisa bermacam-macam. Untuk makalah ini digunakan pengulangan secara parsial berkurang. Yaitu jumlah karakter kata kunci dikurangi tiap pengulangannnya dengan pengurangan pada karakter terakhir.

Sebagai contoh untuk kasus yang sama dengan kasus sebelumnya:

Plainteks:
`MODIFIKASI CIPHER VIGENÈRE`
Kunci:
`KUNCIKUNCK UNKUKK UNCIKUNC`

Contoh 2.1-Vigenère Cipher modifikasi dengan pemenggalan berdasarkan plainteks

Plainteks:
`MODIF IKAS ICI PH E RVIGE NERE`
Kunci:
`KUNCI KUNC KUN KU K KUNCI KUNC`

Contoh 2.2-Vigenère Cipher modifikasi dengan pemenggalan berdasarkan kata kunci

4. PENGUJIAN

4.1. Metode Pengujian

Untuk melakukan pengujian telah dikembangkan suatu aplikasi yang memuat algoritma *Vigenère Cipher* modifikasi. Dengan bantuan aplikasi, suatu plainteks diubah ke dalam bentuk cipherteks dengan kata kunci yang telah ditentukan. Meskipun demikian, metode pengujian adalah dengan melakukan serangan kriptanalisis yang bersifat *ciphertext only attack*. Seolah-olah, cipherteks didapatkan dari plainteks yang tidak diketahui yang kemudian dienkripsi dengan kunci yang juga tidak diketahui baik nilai maupun panjangnya.

4.2. Pengujian

Diketahui plainteks sebagai berikut:

> Cryptanalysis (from the Greek kryptos, "hidden", and analyein, "to loosen" or "to untie") is the study of methods for obtaining the meaning of encrypted information, without access to the secret information which is normally required to do so. Typically, this involves finding the secret key. In non-technical language, this is the practice of codebreaking or cracking the code, although these phrases also have a specialised technical meaning (see code).
>
> "Cryptanalysis" is also used to refer to any attempt to circumvent the security of other types of cryptographic algorithms and protocols in general, and not just encryption. However, cryptanalysis usually excludes attacks that do not primarily target weaknesses in the actual cryptography; methods such as bribery, physical coercion, burglary, keystroke logging, and so forth, although these latter types of attack are an important concern in computer security, and are often more effective than traditional cryptanalysis.
>
> Even though the goal has been the same, the methods and techniques of cryptanalysis have changed drastically through the history of cryptography, adapting to increasing cryptographic complexity, ranging from the pen-and-paper methods of the past, through machines like Enigma in World War II, to the computer-based schemes of the present. The results of cryptanalysis have also changed — it is no longer possible to have unlimited success in codebreaking, and there is a hierarchical classification of what constitutes a rare practical attack. In the mid-1970s, a new class of cryptography was introduced: asymmetric cryptography. Methods for breaking these cryptosystems are typically radically different from before, and usually involve solving carefully-constructed problems in pure mathematics, the best-known being integer factorization.
>
> Cryptanalysis has coevolved together with cryptography, and the contest can be traced through the history of cryptography—new ciphers being designed to replace old broken designs, and new cryptanalytic techniques invented to crack the improved schemes. In practice, they are viewed as two sides of the same coin: in order to create secure cryptography, you have to design against possible cryptanalysis.
> Although the actual word "cryptanalysis" is relatively recent (it was coined by William Friedman in 1920), methods for breaking codes and ciphers are much older. The first known recorded explanation of cryptanalysis was given by 9th century Arabian polymath Abu Yusuf Yaqub ibn Ishaq al-Sabbah Al-Kindi in A Manuscript on Deciphering Cryptographic Messages. This treatise includes a description of the method of frequency analysis (Ibrahim Al-Kadi, 1992- ref-3).

Kasus Uji-Plainteks asli

Pemilihan plainteks untuk kasus uji sengaja menggunakan plainteks yang relatif panjang. Kemudian dihilangkan spasi, tanda bacanya, dan penggunaan huruf kapitalnya sebelum dimasukkan ke dalam aplikasi menjadi sebagai berikut:

> cryptanalysisfromthegreekkryptoshi
> ddenandanalyeintoloosenortountieis
> thestudyofmethodsforobtainingtheme
> aningofencryptedinformationwithout
> accesstothesecretinformationwhichi
> snormallyrequiredtodosotypicallyth
> isinvolvesfindingthesecretkeyinnon
> technicallanguagethisisthepractice

```
ofcodebreakingorcrackingthecodealt
houghthesephrasesalsohaveaspeciali
sedtechnicalmeaningseecodecryptana
lysisisalsousedtorefertoanyattempt
tocircumventthesecurityofothertype
sofcryptographicalgorithmsandproto
colsingeneralandnotjustencryptionh
owevercryptanalysisusuallyexcludes
attacksthatdonotprimarilytargetwea
knessesintheactualcryptographymeth
odssuchasbriberyphysicalcoercionbu
rglarykeystrokeloggingandsoforthal
thoughtheselattertypesofattackarea
nimportantconcernincomputersecurit
yandareoftenmoreeffectivethantradi
tionalcryptanalysiseventhoughthego
alhasbeenthesamethemethodsandtechn
iquesofcryptanalysishavechangeddra
sticallythroughthehistoryofcryptog
raphyadaptingtoincreasingcryptogra
phiccomplexityrangingfromthepenand
papermethodsofthepastthroughmachin
eslikeenigmainworldwariitothecompu
terbasedschemesofthepresenttheresu
ltsofcryptanalysishavealsochangedi
tisnolongerpossibletohaveunlimited
successincodebreakingandthereisahi
erarchicalclassificationofwhatcons
titutesararepracticalattackinthemi
d1970sanewclassofcryptographywasin
troducedasymmetriccryptographymeth
odsforbreakingthesecryptosystemsar
etypicallyradicallydifferentfrombe
foreandusuallyinvolvesolvingcarefu
llyconstructedproblemsinpuremathem
aticsthebestknownbeingintegerfacto
rizationcryptanalysishascoevolvedt
ogetherwithcryptographyandtheconte
stcanbetracedthroughthehistoryofcr
yptographynewciphersbeingdesignedt
oreplaceoldbrokendesignsandnewcryp
tanalytictechniquesinventedtocrack
theimprovedschemesinpracticetheyar
eviewedastwosidesofthesamecoininor
dertocreatesecurecryptographyyouha
vetodesignagainstpossiblecryptanal
ysisalthoughtheactualwordcryptanal
ysisisrelativelyrecentitwascoinedb
ywilliamfriedmanin1920methodsforbr
eakingcodesandciphersaremucholdert
hefirstknownrecordedexplanationofc
ryptanalysiswasgivenby9thcenturyar
abianpolymathabuyusufyaqubibnishaq
alsabbahalkindiinamanuscriptondeci
pheringcryptographicmessagesthistr
eatiseincludesadescriptionofthemet
hodoffrequencyanalysisibrahimalkad
i1992ref3
```

Kasus Uji-Plainteks tanpa spasi, tanda baca, dan kapital

Lalu dimasukkan ke dalam aplikasi dengan kata kunci:

```
Kriptografi
```

Kasus Uji-Kata kunci

Menghasilkan cipherteks sebagai berikut:

```
migemotrldasjnghazyelbvmzdfegtyjpx
wrkekelpgorivqcmcvfwhxxfziylvdzosj
bwxgzlddwpdmiacjjftbfjitwtznqkptfs
geseodystmigemsnzvuhbdiisfvgzdrfci
tqivsxbykptlsiieysendkagkiyeewbqnz
cewgforvpztjisimsmyuwhykgzzmkctnmv
ojisdycdtltoednxxbwxgktrokstrwteye
btvvtstiaeoxxcpzokpxczadyoziirmwiv
okkyumqksgbisqfzrkoibixxbwxquuorti
acaqybwxgogpgtcvapvjwrrforaexqorln
aoubtvvtzcfvdmpgwtxsovkdwsiiigbpgo
rijqhbgkcadncvliyimpvbdficrozkerxd
kwrbfilmaoebiasyvceiqirclfdymgmmvo
jwuvfigbdzbrxwstivxybzbwfggeduzykw
rhzyznloemgtzgedxfbyngzvxtznihoyep
dpsfvzrkigbpxrtijsclajtzrpeckvlltl
ozkahujbwthjfnykxgbagiscgitfmokett
yxvahxczvirvimkekckgrdzfgwizygbxhn
fdxclkwtghiilvznivejstiavckbtqdgpe
ioatbpstijbbfuocwvzwtxaslcfndkhnrl
yrfcvahnvsociimsxkigmhhtgdkirdobvi
cbwgwgdrvdtyxtmggwttorxekmglsilrnd
picwoxvopkmcfcxvowntvhofvbwtbdiisb
dzwckckbpzdrvpemyzsjdoebwhimytmoxw
pevgjbovviasyrwvbwxakdywsloxubtvre
qfevaywmbpxitbgcyxqcyikxqnrnloulgt
gzzckctnmvxfexpiasnsjbdkmywkgrzkwv
brxrpknrxibbmkonvmimplwtxcwigbdzfg
ghstkdfdrvhzbnkotqzvvyfydbwxzvvpxu
xkgobdmiacjjokbrvxplhzyrtexpbtqnzn
ojtxdskesxupbbcyitspobzqihdymrydxe
kobsihxrythjuojwumvkgrjcvvimvkiecl
tilcltbpxitbgvpaxlvkmmpecfkwkeoous
dzachzuegjzzfahbprvttrrdtnbrzmskms
liitojaxgqunvjgxouzvvtxubwoimsjkrz
mgtfiyihivttplgowihkkqdgclnhkkkdgg
zzdlbtloxkimekomkqrtvrbiktssedrvux
w1970ggeebkvrahhtiiyudfogtdnpwkjqc
mfuuetmstgewdmikwmtznidfogkgpidody
wsltuibwmkbqczhnvsjmigemcypsdvuhtf
kkigqrtzriiisbqkctnwswntbvvdwbydjt
ycxvaslejcpezeznaycdtlcrmixxkpksll
vcgrhbydicrmsngzduvvuhsexeiowrbwxa
gkihadymqxgzbntgejtbbmzndvotktgtdf
zxsozsfvrkmzkictvpaxcyictyomwaosjk
olmdymgpwzycwigbdzfgghirvsmvktyebt
lhikejtmfktmsmriwjqybrvrsjbdkmuwcw
gzkwvkovyysonkxivkislvqczrkjsxvtwh
ubvxatqoftsubfstxumczqxjicwbkncwgz
kictzekihdvkwgwwleczvkxbzvnkwrkoiu
kptbaziwkxnjkwodmczxziirmwivtmmirz
towkneikjblhgouecfniasyrwvkdbboxfz
sxfdfkgxkkmhotcbvmbpxihuxrpmgifcwt
jkkoiojqvgomrixjbehgyzlcmrkmvdrvpe
mczapedywjqybrvkmkcpekuidhzigbpgor
```

```
psnczagxzgkifvtnksivxkqipoymfqcxrl
pexevzibpiqouwkeqc1920fszyoiapfzqk
sgbisqtwsxggedmzxwxfyrbvujvvuvumgm
vowqgldbvdgezotybumsxlvcasidzwchti
iyudrvpemyzsgravbjkelp9bwvstdlzntf
ksqpgzftnwrbrrlepchnterqzjssvxlvgh
aqcrjqtvgckselxbbgdkechvfozkwcwsmz
xwxbzvvmigzkyqiieawidexakxmhmvojtw
orbxlsoecvlltlojvctzxihoyewumvodmi
ayuwupimaloxtgpgorpsnasszpawsrlpku
q1992gxt3
```

Kasus Uji-Cipherteks

Selanjutnya metode pengujian akan dimulai dengan melakukan serangan kriptanalisis terhadap cipherteks dengan menggunakan metode *Kasiski*.

Langkah-langkah dekripsi:

1. Mencari kumpulan huruf yang berulang.
   Didapatkan:
   - `migem` dengan jarak 111 dan 1234
   - `pgori` dengan jarak 330
   - `dmiacjj` dengan jarak 913
   - `agki` dengan jarak 1303
   - `btvvt` dengan jarak 105
   - `stia` dengan jarak 389
   - `qksgbisq` dengan jarak 1658
   - `rkoi` dengan jarak 1407
   - `gged` dengan jarak 1481
   - `iasy` dengan jarak 1333
   - `vlltlo` dengan jarak 1612
   - `hnvs` dengan jarak 654
   - `cwigbdzfggh` dengan jarak 598
   - `vpax` dengan jarak 411
   - `zkict` dengan jarak 158
   - `pgorpsn` dengan jarak 324
   - `igbpgor` dengan jarak 1495
   - `xxbwx` dengan jarak 75

   Menentukan faktor pembagi dari nilai jarak yang telah didapatkan:
   - 111 : (1, 3, 37, 111)
   - 1234: (1, 2, 617, 1234)
   - 330 : (1, 2, 3, 5, 6, 10, 11, 15, 22, 30, 33, 55, 66, 110, 165, 330)
   - 913 : (1, 11, 83, 913)
   - 1303: (1, 1303)
   - 105 : (1, 3, 5, 7, 15, 21, 35, 105)
   - 389 : (1, 389)
   - 389 : (1, 2, 829, 1658)
   - 1407: (1, 3, 469, 1407)
   - 1481: (1, 1481)
   - 1333: (1, 31, 43, 1333)
   - 1612: (1, 2, 4, 13, 26, 31, 52, 62, 124, 403, 806, 1612)
   - 654 : (1, 2, 3, 109, 327, 654)
   - 598 : (1, 2, 13, 23, 26, 46, 299, 598)
   - 411 : (1, 411)
   - 158 : (1, 2, 79, 158)
   - 324 : (1, 2, 4, 41, 162, 324)
   - 1495: (1, 5, 13, 23, 65, 115, 299, 1495)
   - 75 : (1, 3, 5, 15, 25, 75)

2. Menerka panjang kunci dari irisan dari himpunan faktor-pembagi nilai jarak yang telah ditemukan. Mencari irisan ini bisa disebut mencari *great common divisor* (*GCD*) atau faktor persekutuan terbesar (FPB) dari nilai jarak yang ditemukan.

3. Bila mengambil semua nilai jarak yang ditemukan didapatkan panjang kunci yaitu irisan faktor-faktor pembaginya adalah 1. Hal ini tidak mungkin, karena kita sudah mengetahui di awal bahwa kunci yang digunakan adalah kata `kriptografi` dengan panjang kata 11 karakter. Karena itu kemunculan ulang beberapa kata bisa dianggap sebuah kebetulan, dalam artian nilai jaraknya diabaikan.

   Akan tetapi untuk menentukan yang mana kemunculan kata yang bersifat kebetulan akan membutuhkan proses *trial and error* yang cukup rumit.

5. PEMBAHASAN

Tanpa perlu melanjutkan kriptanalisis kita sudah bisa mengetahui bahwa kriptanalis yang melakukan serangan akan menemui kesulitan dalam memecahkan panjang kunci. Karena dari data yang diperoleh, hanya kata `pgori` dan `dmiacjj` yang muncul berulang dengan jarak merupakan kelipatan 11, yang metupakan panjang kunci.

Bila ditelaah lebih lanjut, sebenarnya modifikasi algoritma seperti ini tidak terlalu rumit dalam implementasinya. Pengulangan parsial hanya menambah panjang kata kunci dari semestinya.

Seperti yang dapat dilihat pada contoh 2.2, Kata kunci `KUNCI` tidak langsung berulang setelah lima karakter sesuai panjangnya, melainkan ditambah 4, 3, 2, dan 1 karakter lagi menjadi 15 karakter.

```
KUNCI+KUNC+KUN+KU+K= KUNCIKUNCKUNKUK
  (5)    (4)   (3)  (2) (1)        (15)
```

Setelah karakter ke 15 kata kunci akan berulang lagi. Dengan kata lain, *Vigenère Cipher* modifikasi dengan kata kunci `KUNCI` akan menghasilkan hasil yang sama dengan *Vigenère Cipher* klasik dengan kata kunci `KUNCIKUNCKUNKUK`.

Begitu juga dengan contoh kasus uji yang diujikan pada tahap pengujian. Yaitu plainteks yang dienkripsikan dengan *Vigenère Cipher* modifikasi dengan kata kunci:

```
kriptografi
```

dengan panjang kata kunci 11, bisa dikatakan juga plainteks sebenarnya dienkripsikan dengan *Vigenère*

Cipher klasik dengan kata kunci:

```
kriptografikriptografkriptograkripto
grkriptogkriptokriptkripkrikrk
```

dengan panjang kata kunci: 66 karakter.

Yang menarik adalah, penggunaan kata yang berulang sebagian (parsial) dalam satu kata kunci ternyata dapat membingungkan kriptanalis yang melakukan serangan terhadap cipherteks dengan menggunakan metode *Kasiski* biasa.

Karena pada metode *Kasiski* biasa, huruf-huruf kunci dianggap berulang bila telah memasuki pengulangan kata kunci secara keseluruhan. Sedangkan pada kata kunci yang terdapat pengulangan kata secara parsial, enkripsi pada *Vigenère Cipher* dapat memberikan kesan seolah-olah plainteks dienkripsi dengan kata kunci pendek yang telah diulang, padahal itu adalah kata kunci panjang yang belum selesai diulang satu putaran.

Hal tersebut menjelaskan kenapa pada kasus uji sebelumnya, tidak didapatkan nilai irisan yang memuaskan (mengacu pada panjang kunci sebenarnya), malah memberikan data yang membingungkan kriptanalis.

6. KESIMPULAN

Kesimpulan yang diperoleh dari pengujian dan pembahasan masalah pada makalah ini, yaitu *Vigenère Cipher* modifikasi antara lain:

1. Algoritma kriptografi *Vigenère* modifikasi dengan kata kunci K, memiliki algoritma yang sama dengan algoritma kriptografi *Vigenère* klasik dengan kata kunci K+(K-1)+(K-2)+...+(K-(K-1))
2. Algoritma kriptografi *Vigenère* modifikasi sulit dipecahkan dengan menggunakan metode Kasiski biasa.

7. DAFTAR REFERENSI

[1] Rinaldi Munir, M.T., "Diktat Kuliah IF5054", *Program Studi Teknik Informatika STEI ITB*, 2006, hal.1-5, 15, 52-56.

[2] Vigenère Cipher - Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher

[3] Cryptanalysis - Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Cryptanalysis