Multi ROT-V13 Cipher, Sebuah Algoritma Kriptografi Klasik Multi Enkripsi Baru

Ryan Rheinadi / 13508005
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
if18005@students.if.itb.ac.id
ryanrheinadi@students.itb.ac.id

Abstrak - Kata cryptography berasal dari bahasa Yunani: krupto (hidden atau secret) dan grafh (writing). Artinya "secret writing". Kriptografi adalah ilmu dan seni untuk menjaga kerahasian pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan (message) [Schneier, 1996].

Dalam perkembangan sejarah kriptografi klasik, yaitu kriptografi berbasis karakter, telah tercipta banyak algoritma-algoritma kriptografi yang memiliki keunikan masing-masing, baik cipher-cipher yang bersifat substitusi maupun transposisi. Beberapa diantaranya misalnya Caesar Cipher, Vigenère Cipher, Playfair Cipher, Affine Cipher, Hill Cipher, maupun Enigma Cipher.

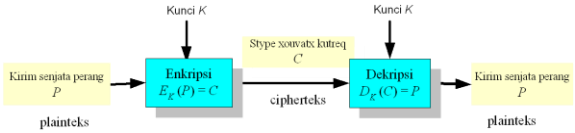
Vigenère Cipher dan ROT-13 adalah algoritma-algoritma kriptografi klasik yang telah obsolete karena telah berhasil dipecahkan, bahkan dengan mudah menggunakan tabel frekuensi kemunculan huruf, bigram dan trigram dalam suatu bahasa sehingga sudah tidak aman lagi untuk digunakan. Oleh karena itu, saya mencoba membuat algoritma kriptografi klasik baru yang merupakan kombinasi dari kedua algoritma tersebut dengan memanfaatkan prinsip multiple encryption sehingga sulit untuk dipecahkan dan memiliki tingkat keamanan yang tinggi, namun mudah diterapkan.

Kata Kunci : Algoritma Kriptografi Klasik, Vigenère Cipher, ROT13, Multi Enkripsi

I. PENDAHULUAN

Kata *cryptography* berasal dari bahasa Yunani: *krupto* (hidden atau secret) dan *grafh* (writing), artinya "secret writing". Definisi lama kriptografi adalah ilmu dan seni untuk menjaga kerahasian pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Dalam perkembangannya, kriptografi berkembang sedemikan rupa sehingga tidak lagi sebatas mengenkripsi pesan, tetapi juga memberikan aspek keamanan yang lain. Oleh karena itu, tercipta definisi baru kriptografi. Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan (message) [Schneier, 1996].

Sistem kriptografi tersusun atas algoritma kriptografi yang akan digunakan untuk penyandian pesan, plainteks yang berperan sebagai teks yang akan disandikan, cipherteks sebagai teks yang telah disandikan, serta kunci yang merupakan parameter dalam proses *enciphering* dan *deciphering*. Penggunaan kunci membuat algoritma kriptografi tidak perlu rahasia atau bersifat publik. Keterkaitan antara plainteks, cipherteks dan kunci dapat dilihat pada gambar berikut ini.



Gambar 1. Gambaran Sistem Kriptografi

Algoritma kriptografi menurut masanya terbagi menjadi dua, yaitu algoritma kriptografi klasik dan algoritma kriptografi modern. Perbedaan mendasar dari kedua jenis algoritma kriptografi ini adalah algoritma kriptografi modern beroperasi dalam mode *bit*, sedangkan algoritma kriptografi klasik masih beroperasi dalam mode karakter. Sehingga jumlah karakter yang dapat digunakan dalam algoritma kriptografi klasik akan lebih sedikit dibandingkan dengan algoritma kriptografi modern.

Secara umum, algoritma kriptografi klasik terbagi atas dua jenis, yaitu algoritma transposisi dan substitusi. Terdapat dua perbedaan mendasar antara kedua jenis algoritma ini. Pada algoritma transposisi, enkripsi dilakukan dengan cara penukaran letak tempat huruf-huruf pada satu kata yang sama, misalnya "KRIPTOGRAFI" menjadi "PRTKIGOFRAI". Pada algoritma substitusi, enkripsi dilakukan dengan cara mengganti masing-masing huruf pada kata dengan huruf lain sesuai algoritma tertentu. Contoh simpelnya adalah *caesar cipher*, dimana setiap huruf akan diubah dengan cara dilakukan substitusi dengan tiga huruf setelahnya, sehingga "A" menjadi "C", "D" menjadi "F" dan sebagainya.

Pembuatan algoritma ini menggunakan algoritma ROT13, *Vigenère cipher* serta konsep multi enkripsi, sehingga penting untuk mengetahui terlebih dahulu konsep tentang hal-hal tersebut. ROT-13 Cipher adalah bentuk khusus dari *Caesar Cipher*, yaitu *Caesar Cipher* dengan k=13. Keunikan dari ROT-13 Cipher ini adalah baik untuk mengenkripsi maupun mendekripsi pesan,

cukup melakukan *Caesar Cipher* dengan k=13. *Vigenere Cipher* adalah modifikasi dari *Caesar Cipher*, yaitu *Caesar Cipher* dengan kunci yang berbeda-beda dalam setiap karakternya. Kunci yang berbeda diperoleh dari masukan user yang diterjemahkan menjadi angka per-alfabetnya. Dalam perkembangannya, terdapat banyak varian *Vigenere Cipher*. *Multiple Encryption* adalah metode mengenkripsi kembali pesan yang telah terenkripsi oleh satu algoritma, baik dengan algoritma yang sama maupun berbeda, baik hanya sekali maupun berulang-ulang.

II. KONSEP ALGORITMA MULTI ROT V-13

Setelah mengenali konsep-konsep kriptografi dasar yang digunakan dalam pembuatan algoritma ini, akan dilakukan pembahasan mengenai konsep algoritma multi rot V-13 ini. Perbedaan mendasar antara multi rot V-13 dengan algoritma kriptografi klasik lainnya terletak pada penggunaan multi enkripsi menggunakan dua algoritma klasik lain, yaitu ROT13 dan *Vigenère*. Penggunaan konsep multi enkripsi dengan multi algoritma ini akan mempersulit usaha-usaha kriptanalis untuk memecahkan algoritma ini. Hal ini akan mengakibatkan untuk memperoleh informasi, perlu dilakukan usaha kriptanalisis yang tidak sebanding dengan nilai informasi yang didapat.

Secara umum, langkah-langkah enkripsi algoritma multi rot V-13 ini adalah sebagai berikut.

1. Tentukan kunci yang akan digunakan untuk mengenkripsi pesan. Kunci harus terdiri atas alfabet-alfabet A-Z atau angka 0-9, karena algoritma kriptografi masih berbasis karakter, bukan bit.
2. Lakukan proses enkripsi *Vigenère* standar pada plainteks berdasarkan kunci.. Proses enkripsi adalah sebagai berikut.
   - Berikan enumerasi masing-masing karakter pada plainteks sesuai dengan urutan alfabet, dengan enumerasi 0 dilakukan setelah enumerasi alfabet Z.
   - Lakukan pula enumerasi pada masing-masing karakter kunci dengan cara yang sama dengan enumerasi plainteks.
   - Apabila panjang kunci lebih sedikit daripada panjang plainteks, lakukan pengulangan kunci secara periodik hingga panjang kunci sama dengan panjang plainteks.
   - Apabila panjang kunci lebih panjang daripada panjang plainteks, cukup gunakan n karakter pertama dari kunci, dimana n adalah panjang plainteks.
   - Jumlahkan nilai enumerasi karakter plainteks dengan nilai enumerasi kunci yang bersesuaian.
   - Lakukan operasi modulo 26 pada hasil penjumlahan enumerasi sehingga diperoleh hasil yang merepresentasikan enumerasi dari cipherteks.
   - Terjemahkan enumerasi tersebut sehingga terdapat cipherteks yang dihasilkan.

   Secara matematis, proses enkripsi dan dekripsi dapat ditulis sebagai berikut.
   - Enkripsi
     $Ci = Ek(Mi) = (Mi + Ki) \bmod 26$
   - Dekripsi
     $Mi = Dk(Ci) = (Ci – Ki) \bmod 26$

   Dengan pendefinisian :
   M = M0 . . . Mn adalah plain textnya,
   C = C0 . . . Cn adalah ciphertextnya, dan
   K = K0 . . . Km adalah kunci yang digunakan
3. Lakukan proses enkripsi ROT13 pada cipherteks hasil enkripsi dengan *Vigenère* dan kunci. Proses enkripsi yang dilakukan adalah sebagai berikut.
   - Lakukan enumerasi masing-masing karakter teks.
   - Jumlahkan hasil enumerasi masing-masing karakter kunci dengan 13.
   - Lakukan operasi modulo 26 pada hasil penjumlahan enumerasi karakter teks dengan 13.
4. Lakukan enkripsi *Vigenère* pada cipherteks saat ini dengan menggunakan kunci yang telah di ROT13.
5. Ulangi langkah dua hingga langkah empat selama tiga belas kali, sehingga jumlah ROT13 yang dilakukan pada kunci akan memiliki total sebanyak 13 kali

III. PEMBAHASAN ALGORITMA MULTI ROT V-13

Metode algoritma multi rot V-13 ini menggabungkan beberapa jenis metode algoritma kriptografi klasik terdahulu, dalam hal ini ROT13 dan *Vigenère*, serta prinsip multi enkripsi. Dalam satu kali siklus, akan dilakukan satu kali operasi ROT13 pada kunci dan teks, dua kali operasi *Vigenère* pada teks. Proses multi enkripsi dan penggunaan dua algoritma ini akan mempersulit proses penyerangan yang dilakukan oleh kriptanalis. Berikut ini adalah beberapa kelebihan yang diharapkan dapat diperoleh dari algoritma multi rot V-13.

- Mudah diimplementasikan. Algoritma ini cukup mudah untuk diimplementasikan karena hanya menggunakan dua buah algoritma substitusi.
- Penyerangan menggunakan *known-plainteks attack* sulit untuk dilakukan. Sekalipun panjang kunci diketahui, tidak akan terbentuk pola huruf karena dilakukan tiga belas kali perulangan proses enkripsi. Proses multi enkripsi ini mengakibatkan sekalipun panjang kunci diketahui, hasil cipherteks akan tetap tidak berpola sehingga sulit dilakukan analisis. Tentu

saja untuk mengetahui panjang kunci itu cukup sulit karena tidak akan terbentuk pola huruf.

- Kata kunci dapat memiliki panjang yang sama dengan panjang teks. Keistimewaan dari hal ini adalah apabila kata kunci yang dimasukkan memiliki panjang yang sama dengan panjang teks, algoritma ini secara praktis akan menjadi sebuah *one-time pad*.
- Tidak dapat dipecahkan menggunakan metode analisis frekuensi. Hal ini disebabkan oleh penggunaan ROT13 pada kunci maupun teks mengakibatkan *Vigenère* yang dilakukan menjadi sangat tidak berpola. Terlebih baik ROT13 maupun *Vigenère* dilakukan dengan perulangan sebanyak 13 kali.

Tentunya setiap algoritma memiliki kelebihan dan kekurangan masing-masing. Hal ini berlaku pula pada algoritma kriptografi multi rot V-13 ini. Berikut ini beberapa kekurangan dari algoritma kriptografi multi rot V-13.

- Huruf "N" dan "A" pada kunci akan mengakibatkan algoritma multi rot V-13 tidak akan melakukan substitusi pada teks yang bersesuaian dengan letak huruf "N" dan "A" pada kunci.
- Angka 0-9 yang tidak dienkripsi akan mengakibatkan angka-angka terlihat dengan jelas pada cipherteks. Hal ini berakibat fatal pada teks-teks yang memiliki informasi dalam angka-angka yang penting.

IV. PROSES DAN IMPLEMENTASI

Pada bab ini akan dijelaskan contoh dari penerapan algoritma multi rot V-13 untuk mengenkripsi maupun mendekripsi suatu teks.

Misalkan plain teks adalah :

ku terbiasa tersenyum tenang.
walau, aaaa, hatiku menangis
kaulah cerita tertulis dengan pasti
selamanya dalam pikiranku

Kunci yang digunakan adalah "peterpan". Berikut ini adalah langkah-langkah penenkripsian dan pendekripsian teks. Proses vigenere dan ROT13 dilakukan menggunakan aplikasi "*cryptohelper.jar*"

1.Perulangan Pertama

- Vigenere pertama

  Cipherteks sementara

  ZYMII QINHE MIIHE ANYFX VCAAV
  ATPRJ ANPEA EKXKH BIGEE VIFZE
  NPRWC RGMME KTRGJ PBWUT
  NTPRI EJIIF TPTQR CYNSE EEDEI
  XXVTR BJ

  Kunci : peterpan
- ROT13

  Cipherteks sementara

  MLZVV DVAUR ZVVUR NALSK
  IPNNI NGCEW NACRN RXKXU
  OVTRR IVSMR ACEJP ETZZR
  XGETW COJHG AGCEV RWVVS
  GCGDE PLAFR RRQRV KKIGE OW

  Kunci : CRGRECNA
- Vigenere kedua

  OCFMZ FIAWI FMZWE NCCYB
  MRANK EMTIY AAEIT IBMKU
  QMZIV KISOI GTILC EVQFI BIRTY
  TUALI NGEVB IAXIS ITMUI RYAHI
  XIUTI KMZMV SY

  Kunci : CRGRECNA

2. Perulangan Kedua

- Vigenere pertama

  QTLDD HVAYZ LDDYR NETES
  QTNNM VSKMA NAGZZ ZFOXU
  SDFZZ MVSQZ MKMNP EXHLZ
  FKETA KARPK AGGMH ZEZVS
  KKSLM TLAJZ DZYVV KOQSM WA

  Kunci : CRGRECNA
- ROT13

  DGYQQ UINLM YQQLE ARGRF
  DGAAZ IFXZN ANTMM MSBKH
  FQSMM ZIFDM ZXZAC RKUYM
  SXRGN XNECX NTTZU MRMIF
  XXFYZ GYNWM QMLII XBDFZ JN

  Kunci : PETERPAN
- Vigenere kedua

  SKRUH JIAAQ RUHAE NGKKJ
  UVANO MYBQC AAIQF QJQKU
  UULQD OISSQ SBQPC EZYRQ
  JMRTC BGITM NGIDN QIBIS MBYCQ
  VYALQ JQCXI KQHYD AC

  Kunci : PETERPAN

3.Perulangan Ketiga

- Vigenere pertama

  HOKYY YINPU KYYPE AVODN
  LKAAD QRFHR ANXUY UAFKH
  JYEUU DIFHU LFHEC ROCKU
  ABRGR FZMKB NTXHG UZQIF
  BFRGH KYNAU CUTMI XFLRH RR

  Kunci : PETERPAN
- ROT13

  UBXLL LVACH XLLCR NIBQA
  YXNNQ DESUE NAKHL HNSXU
  WLRHH QVSUH YSURP EBPXH
  NOETE SMZXO AGKUT HMDVS
  OSETU XLANH PHGZV KSYEU EE

  Kunci : CRGRECNA
- Vigenere kedua

  WSDCP NIAEY DCPEE NKSWR
  CZANS UKJYG AAMYR YRUKU
  YCXYL SISWY EJYTC EDGDY
  RQRTG JSQBQ NGMLZ YQFIS
  QJKKY ZYAPY VYKBI KUPKL IG

  Kunci : CRGRECNA

4.Perulangan Keempat

- Vigenere pertama

YJJTT PVAGP JTTGR NMJCI GBNNU LQACI NAOPX PVWXU ATDPP UVSYP KACVP EFXJP VSETI AYHFS AGOCF PUHVS SAQBC BLARP BPODV KWGQC MI

Kunci : CRGRECNA

- ROT13

LWWGG CINTC WGGTE AZWPV TOAAH YDNPV ANBCK CIJKH NGQCC HIFLC XNPIC RSKWC IFRGV NLUSF NTBPS CHUIF FNDOP OYNEC OCBQI XJTDP ZV

Kunci : PETERPAN

- Vigenere kedua

AAPKX RIAIG PKXIE NOAIZ KDANW CWRGK AAQGD GZYKU CKJGT WISAG QRGXC EHOPG ZURTK REYJU NGQTL GYJIS URWSG DYATG HGSFI KYXWT QK

Kunci : PETERPAN

5.Perulangan Kelima

- Vigenere pertama

PEIOO GINXK IOOXE ADEBD BSAAL GPVXZ ANFKW KQNKH ROCKK LIFPK JVXMC RWSIK QJRGZ VXCAJ NTFXE KPYIF JVPWX SYNIK AKJUI XNBPX HZ

Kunci : PETERPAN

- ROT13

CRVBB TVAKX VBBKR NQROQ OFNNY TCIKM NASXJ XDAXU EBPXX YVSCX WIKZP EJFVX DWETM IKPNW AGSKR XCLVS WICJK FLAVX NXWHV KAOCK UM

Kunci : CRGRECNA

- Vigenere kedua

EIBSF VIAMO BSFME NSIUH SHANA KIZOO AAUOP OHCKU GSVOB AISEO CZOBC ELWBO HYRTO ZQGRY NGUBX OGNIS YZIAO HYAXO TOAJI KCFIB YO

Kunci : CRGRECNA

6.Perulangan Keenam

- Vigenere pertama

GZHJJ XVAOF HJJOR NUZAY WJNNC BOQSQ NAWFV FLEXU IJBFF CVSGF IQSDP ENNHF LAETQ QWXVA AGWSD FKPVS AQORS JLAZF ZFELV KEWOS CQ

Kunci : CRGRECNA

- ROT13

TMUWW KINBS UWWBE AHMNL JWAAP OBDFD ANJSI SYRKH VWOSS PIFTS VDFQC RAAUS YNRGD DJKIN NTJFQ SXCIF NDBEF WYNMS MSRYI XRJBF PD

Kunci : PETERPAN

- Vigenere kedua

IQNAN ZIAQW NANQE NWQGP ALANE SUHWS AAYWB WPGKU KAHWJ EISIW OHWFC EPENW PCRTS HCOZC NGYJJ WORIS CHUIW LYABW FWINI KGNUJ GS

Kunci : PETERPAN

7.Perulangan Ketujuh

- Vigenere Pertama

XUGEE OINFA GEEFE ALUZT RAAAT WNLNH ANNAU AGVKH ZEAAA TIFXA HLNUC REIGA GRRGH LVSQR NTNNC AFGIF RLNMN AYNQA YAZCI XVRNN XH

Kunci : PETERPAN

- ROT13

KHTRR BVASN TRRSR NYHMG ENNNG JAYAU NAANH NTIXU MRNNN GVSKN UYAHP ERVTN TEETU YIFDE AGAAP NSTVS EYAZA NLADN LNMPV KIEAA KU

Kunci : CRGRECNA

- Vigenere Kedua

MYZIV DIAUE ZIVUE NAYSX IPANI AGPEW AACEN EXKKU OITER IISME APEJC ETMZE XGRTW POWHG NGCRV EWVIS GPGQE PYAFE REQRI KKVGR OW

Kunci : CGRGRECNA

8.Perulangan Kedelapan

- Vigenere Pertama

OPFZZ FVAWV FZZWR NCPYO MRNNK RMGIY NAEVT VBMXU QZZVV KVSOV GGILP EVDFV BIETY GUNLI AGEIB VAXVS IGMHI RLAHV XVUTV KMMMI SY

Kunci : CGRGRECNA

- ROT13

BCSMM SINJI SMMJE APCLB ZEAAX EZTVL ANRIG IOZKH DMMII XIFBI TTVYC RIQSI OVRGL THAYV NTRVO INKIF VTZUV EYNUI KIHGI XZZZV FL

Kunci : PETERPAN

- Vigenere Kedua

QGLQD HIAYM LQDYE NEGEF QTANM ISXMA AAGMZ MFOKU SQFMZ MISQM MXMNC EXULM FKRTA XAEPK NGGZH MEZIS KXSYM TYAJM DMYVI KODSZ WA

Kunci : PETERPAN

9.Perulangan Kesembilan

- Vigenere Pertama

FKEUU WINNQ EUUNE ATKXJ
HIAAB MLBDP ANVQS QWDKH
HUYQQ BIFFQ FBDCC RMYEQ
WZRGP BTIGZ NTVDA QVOIF
ZBLCD IYNYQ WQPKI XDHLD NP

Kunci : PETERPAN

- ROT13

SXRHH JVAAD RHHAR NGXKW
UVNNO ZYOQC NAIDF DJQXU
UHLDD OVSSD SOQPP EZLRD
JMETC OGVTM AGIQN DIBVS
MOYPQ VLALD JDCXV KQUYQ AC

Kunci : CRGRECNA

- Vigenere Kedua

UOXYL LIACU XYLCE NIOQN
YXANQ QEFUE AAKUL UNSKU
WYRUH QISUU YFURC EBCXU
NORTE FMMXO NGKHT UMDIS
OFEGU XYANU PUGZI KSLEH EE

Kunci : CRGRECNA

10. Perulangan Kesepuluh
    - Vigenere Pertama

WFDPP NVAEL DPPER NKFWE
CZNNS HKWYG NAMLR LRUXU
YPXLL SVSWL EWYTP EDTDL
RQETG WSDBQ AGMYZ LQFVS
QWKXY ZLAPL VLKBV KUCKY IG

Kunci :CRGRECNA

    - ROT13

JSQCC AINRY QCCRE AXSJR PMAAF
UXJLT ANZYE YEHKH LCKYY FIFJY
RJLGC RQGQY EDRGT JFQOD
NTZLM YDSIF DJXKL MYNCY
IYXOI XHPXL VT

Kunci : PETERPAN

    - Vigenere Kedua

YWJGT PIAGC JGTGE NMWCV
GBANU YQNCI AAOCX CVWKU
AGDCP UISYC KNCVC EFKJC VSRTI
NYUFS NGOPF CUHIS SNQOC
BYARC BCODI KWTQP MI

Kunci : PETERPAN

11. Perulangan Kesebelas
    - Vigenere Pertama

NACKK EINVG CKKVE ABAVZ
XQAAJ CJRTX ANDGQ GMLKH
PKWGG JIFNG DRTKC RUOCG
MHRGX RRYWH NTDTY GLWIF
HRJST QYNGG UGFSI XLXJT DX

Kunci : PETERPAN

    - ROT13

ANPXX RVAIT PXXIR NONIM
KDNNW PWEGK NAQTD TZYXU
CXJTT WVSAT QEGXP EHBPT
ZUETK EELJU AGQGL TYJVS
UEWFG DLATT HTSFV KYKWG QK

Kunci : CRGRECNA

    - Vigenere Kedua

CEVOB TIAKK VOBKE NQEOD
OFANY GCVKM AASKJ KDAKU
EOPKX YISCK WVKZC EJSVK
DWRTM VKCNW NGSXR KCLIS
WVCWK FYAVK NKWHI KABCX UM

Kunci : CRGRECNA

Dari proses enkripsi di atas, diperoleh cipherteks

CEVOB TIAKK VOBKE NQEOD OFANY GCVKM AASKJ KDAKU EOPKX YISCK WVKZC EJSVK DWRTM VKCNW NGSXR KCLIS WVCWK FYAVK NKWHI KABCX UM

Bandingkan dengan plainteks semula, yaitu

ku terbiasa tersenyum tenang.
walau, aaaa, hatiku menangis
kaulah cerita tertulis dengan pasti
selamanya dalam pikiranku

Kunci dari enkripsi adalah "PETERPAN". Pada kata "PETERPAN", terdapat huruf "A" dan "N" pada huruf ke-7 dan ke-8. Dapat dilihat pada huruf ke-7 dan ke-8 pada plain teks dan kelipatannya ("I" dan "A" pada "terbiasa") tidak terdapat antara perbedaan antara plainteks dan cipherteks. Huruf-huruf yang tidak bersesuaian dengan "A" dan "N" pada kunci dapat dilihat disubstitusikan tanpa pola.

Sedangkan dari hasil perhitungan frekuensi kemunculan huruf, bigram dan trigram diperoleh data seperti berikut.

- Frekuensi kemunculan huruf
  - A = 7 = IIIIIII
  - B = 3 = III
  - C = 8 = IIIIIIII
  - D = 3 = III
  - E = 5 = IIIII
  - F = 2 = II
  - G = 2 = II
  - H = 1 = I
  - I = 4 = IIII
  - J = 2 = II
  - K = 17 = IIIIIIIIIIIIIIIII
  - L = 1 = I
  - M = 3 = III
  - N = 5 = IIIII
  - O = 5 = IIIII
  - P = 1 = I
  - Q = 1 = I
  - R = 2 = II
  - S = 5 = IIIII
  - T = 2 = II
  - U = 2 = II
  - V = 8 = IIIIIIII
  - W = 6 = IIIIII
  - X = 3 = III
  - Y = 3 = III
  - Z = 1 = I
- Frekuensi bigram

- CE = 2 at positions 0,54
- EV = 1 at positions 1
- VO = 2 at positions 2,10
- OB = 2 at positions 3,11
- BT = 1 at positions 4
- TI = 1 at positions 5
- IA = 1 at positions 6
- AK = 2 at positions 7,37
- KK = 1 at positions 8
- KV = 1 at positions 9
- BK = 1 at positions 12
- KE = 1 at positions 13
- EN = 1 at positions 14
- NQ = 1 at positions 15
- QE = 1 at positions 16
- EO = 2 at positions 17,40
- OD = 1 at positions 18
- DO = 1 at positions 19
- OF = 1 at positions 20
- FA = 1 at positions 21
- AN = 1 at positions 22
- NY = 1 at positions 23
- YG = 1 at positions 24
- GC = 1 at positions 25
- CV = 1 at positions 26
- VK = 5 at positions 27,51,58,65,88
- KM = 1 at positions 28
- MA = 1 at positions 29
- AA = 1 at positions 30
- AS = 1 at positions 31
- SK = 1 at positions 32
- KJ = 1 at positions 33
- JK = 1 at positions 34
- KD = 2 at positions 35,59
- DA = 1 at positions 36
- KU = 1 at positions 38
- UE = 1 at positions 39
- OP = 1 at positions 41
- PK = 1 at positions 42
- KX = 1 at positions 43
- XY = 1 at positions 44
- YI = 1 at positions 45
- IS = 2 at positions 46,78
- SC = 1 at positions 47
- CK = 1 at positions 48
- KW = 2 at positions 49,91
- WV = 2 at positions 50,80
- KZ = 1 at positions 52
- ZC = 1 at positions 53
- EJ = 1 at positions 55
- JS = 1 at positions 56
- SV = 1 at positions 57
- DW = 1 at positions 60
- WR = 1 at positions 61
- RT = 1 at positions 62
- TM = 1 at positions 63
- MV = 1 at positions 64
- KC = 2 at positions 66,75
- CN = 1 at positions 67
- NW = 1 at positions 68
- WN = 1 at positions 69
- NG = 1 at positions 70
- GS = 1 at positions 71
- SX = 1 at positions 72
- XR = 1 at positions 73
- RK = 1 at positions 74
- CL = 1 at positions 76
- LI = 1 at positions 77
- SW = 1 at positions 79
- VC = 1 at positions 81
- CW = 1 at positions 82
- WK = 1 at positions 83
- KF = 1 at positions 84
- FY = 1 at positions 85
- YA = 1 at positions 86
- AV = 1 at positions 87
- KN = 1 at positions 89
- NK = 1 at positions 90
- WH = 1 at positions 92
- HI = 1 at positions 93
- IK = 1 at positions 94
- KA = 1 at positions 95
- AB = 1 at positions 96
- BC = 1 at positions 97
- CX = 1 at positions 98
- XU = 1 at positions 99
- UM = 1 at positions 100

- Frekuensi Trigram

- CEV = 1 at positions 0
- EVO = 1 at positions 1
- VOB = 2 at positions 2,10
- OBT = 1 at positions 3
- BTI = 1 at positions 4
- TIA = 1 at positions 5
- IAK = 1 at positions 6
- AKK = 1 at positions 7
- KKV = 1 at positions 8
- KVO = 1 at positions 9
- OBK = 1 at positions 11
- BKE = 1 at positions 12
- KEN = 1 at positions 13
- ENQ = 1 at positions 14
- NQE = 1 at positions 15
- QEO = 1 at positions 16
- EOD = 1 at positions 17
- ODO = 1 at positions 18
- DOF = 1 at positions 19
- OFA = 1 at positions 20
- FAN = 1 at positions 21
- ANY = 1 at positions 22
- NYG = 1 at positions 23
- YGC = 1 at positions 24
- GCV = 1 at positions 25
- CVK = 1 at positions 26

- VKM = 1 at positions 27
- KMA = 1 at positions 28
- MAA = 1 at positions 29
- AAS = 1 at positions 30
- ASK = 1 at positions 31
- SKJ = 1 at positions 32
- KJK = 1 at positions 33
- JKD = 1 at positions 34
- KDA = 1 at positions 35
- DAK = 1 at positions 36
- AKU = 1 at positions 37
- KUE = 1 at positions 38
- UEO = 1 at positions 39
- EOP = 1 at positions 40
- OPK = 1 at positions 41
- PKX = 1 at positions 42
- KXY = 1 at positions 43
- XYI = 1 at positions 44
- YIS = 1 at positions 45
- ISC = 1 at positions 46
- SCK = 1 at positions 47
- CKW = 1 at positions 48
- KWV = 1 at positions 49
- WVK = 1 at positions 50
- VKZ = 1 at positions 51
- KZC = 1 at positions 52
- ZCE = 1 at positions 53
- CEJ = 1 at positions 54
- EJS = 1 at positions 55
- JSV = 1 at positions 56
- SVK = 1 at positions 57
- VKD = 1 at positions 58
- KDW = 1 at positions 59
- DWR = 1 at positions 60
- WRT = 1 at positions 61
- RTM = 1 at positions 62
- TMV = 1 at positions 63
- MVK = 1 at positions 64
- VKC = 1 at positions 65
- KCN = 1 at positions 66
- CNW = 1 at positions 67
- NWN = 1 at positions 68
- WNG = 1 at positions 69
- NGS = 1 at positions 70
- GSX = 1 at positions 71
- SXR = 1 at positions 72
- XRK = 1 at positions 73
- RKC = 1 at positions 74
- KCL = 1 at positions 75
- CLI = 1 at positions 76
- LIS = 1 at positions 77
- ISW = 1 at positions 78
- SWV = 1 at positions 79
- WVC = 1 at positions 80
- VCW = 1 at positions 81
- CWK = 1 at positions 82
- WKF = 1 at positions 83
- KFY = 1 at positions 84
- FYA = 1 at positions 85
- YAV = 1 at positions 86
- AVK = 1 at positions 87
- VKN = 1 at positions 88
- KNK = 1 at positions 89
- NKW = 1 at positions 90
- KWH = 1 at positions 91
- WHI = 1 at positions 92
- HIK = 1 at positions 93
- IKA = 1 at positions 94
- KAB = 1 at positions 95
- ABC = 1 at positions 96
- BCX = 1 at positions 97
- CXU = 1 at positions 98
- XUM = 1 at positions 99

Pada tabel frekuensi kemunculan alfabet, dapatdilihat kemunculan huruf “K” pada cipherteks ada sebanyak 17 kali. Oleh karena panjang teks yang sedikit, dapat kita analisis kemunculan huruf “K” tersebut, mengikuti sebuah pola atau tidak.

Huruf K dapat kita lihat berkorespondensi dengan plainteks sebagai berikut.

```
kuter biasa terse nyumt enang walau aaaah atiku
CEVOB TIAKK VOBKE NQEOD OFANY GCVKM AASKJ KDAKU
PETER PANPE TERPA NPETE RPANP ETERP ANPET ERPAN
```

Gambar 2. Plainteks, Cipherteks dan Kunci

Ternyata dapat kita lihat huruf “K” pada cipherteks yang berkorespondensi dengan kunci “P” akan selalu berasal dari plainteks “S”. Demikian pula dengan cipherteks “V” yang apabila berkorespondensi dengan kunci “T” selalu berasal dari plainteks “T”. Dengan kata lain, masih terdapat pola-pola yang jelas dan dapat teramati.

Hal ini juga dapat dilihat dari trigram “VOB” yang berulang, yang merupakan cipherteks dari plainteks “TER”. Hal ini semakin menegaskan bahwa metode kasiski masih dapat digunakan untuk memecahkan algoritma ini.

V. SIMPULAN

Algoritma Multi ROT V-13 Cipher tidak memiliki tingkat keamanan yang mencukupi untuk menjadi solusi algoritma klasik yang dapat mengatasi metode kasiski sebagai metode pemecah algoritma substitusi.

Untuk memperoleh algoritma yang dapat mengatasi serangan terhadap algoritma substitusi, dibutuhkan kombinasi dengan algoritma transposisi. Penggabungan beberapa algoritma substitusi tidak akan mampu mengatasi serangan-serangan kriptanalis yang secara spesifik mampu memecahkan algoritma substitusi.

Penggunaan multi enkripsi tidak akan menghasilkan hasil yang efektif apabila algoritma-algoritma yang digunakan adalah algoritma yang sejenis. Dalam kasus ini, kedua buah algoritma adalah algoritma substitusi.

Akan diperoleh hasil yang lebih baik apabila digunakan kombinasi antara algoritma ROT 13 dengan algoritma transposis 13 karakter.

REFERENSI

[1] http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2010-2011/Pengantar%20Kriptografi.ppt Tanggal akses 19 Maret 2012

[2] http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2010-2011/Algoritma%20Kriptografi%20Klasik_bag1%20(baru).ppt Tanggal akses 19 Maret 2012

[3] http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2010-2011/Algoritma%20Kriptografi%20Klasik_bag2%20(baru).ppt Tanggal akses 19 Maret 2012

[4] http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2010-2011/Algoritma%20Kriptografi%20Modern_bag1%20(baru).ppt Tanggal akses 19 Maret 2012

[5] Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, "Handbook of Applied Cryptography", 1997, CRC Press

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, 19 Maret 2012

Ryan Rheinadi / 13508005