Military Cryptanalysis

Sonny Theo Tumbur Manurung
NIM : 13510027

Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
Jalan Ganesha 10 Bandung 40132, Indonesia

I. PENDAHULUAN

Definisi Kriptanalisis

Kriptografi menyebabkan timbulnya kriptanalisis, yaitu ilmu pengetahuan dan seni untuk membongkar data acak. Praktisi kriptanalisis disebut juga kriptanalis. Setiap kali ada algoritma kriptografi baru yang dibuat oleh kriptografer, akan langsung diikuti oleh adanya upaya percobaan kriptanalisis. Percobaan kriptanalisis ini sering disebut juga serangan (*attack*). Okeey

Kriptanalisis mencoba mengembalikan data jelas tanpa akses ke kunci kriptografi. Ukuran keberhasilan suatu upaya kriptanalisis adalah sampai sejauh mana keberhasilan diketahuinya data jelas atau kunci kriptografi. Asumsi dasar dari suatu kriptosistem adalah bahwa seorang kriptanalis mengetahui keseluruhan mekanisme enkripsi kecuali kuncinya. Berdasarkan itu, maka serangan terhadap suatu kriptografi dapat beragam.

Sejarah Kriptanalisis

Teknik kriptanalisis sudah ada sejak abad ke-9. Adalah seorang ilmuwan Arab pada Abad IX bernama Abu Yusuf Yaqub Ibnu Ishaq Ibnu As-Sabbah Ibnu 'Omran Ibnu Ismail AlKindi, atau yang lebih dikenal sebagai Al-Kindi yang menulis buku tentang seni memecahkan kode. Dalam buku yang berjudul ‘Risalah fi Istikhraj al-Mu'amma (*Manuscript for the Deciphering Cryptographic Messages*), ia menuliskan naskah untuk menguraikan kode-kode rahasia. Di dalam buku tersebut Al-Kindi memperkenalkan teknik penguraian kode atau atau sandi yang sulit dipecahkan. Ia juga mengklasifikasikan sandi rahasia itu serta menjelaskan ilmu fonetik Arab dan sintaksisnya. Yang paling penting lagi, dalam bukunya ini ia mengenalkan penggunaan beberapa teknik statistika untuk memecahkan kode-kode rahasia (dikutip dari Republika online, 16 Juni 2006).

Apa yang dilakukan oleh Al-Kindi didalam kriptanalisis dikenal dengan nama teknik analisis frekuensi, yaitu teknik untuk memecahkan cipherteks berdasarkan frekuensi kemunculan karakter di dalam pesan dan kaitannya dengan frekuensi kemunculan karakter di dalam alfabet. Analisis frekuensi dilatarbelakangi oleh fakta bahwa cipher gagal menyembunyikan statistik kemunculan karakter di dalam cipherteksnya. Misalnya, di dalam Bahasa Inggris huruf “E” adalah huruf paling sering muncul di dalam kalimatkalimat berbahas Inggris. Jika di dalam cipherteks terdapat huruf yang paling sering muncul, maka kemungkinan besar huruf tersebut di dalam plainteksnya adalah huruf E. Berbagai cipher klasik berhasil dipecahkan dengan teknik analisis frekuensi ini. Halaman pertama buku Al-Kindi, Manuscript for the Deciphering Cryptographic (sumber: wikipedia). Teknik analisis frekuensi masih digunakan di dalam kriptanalisis modern, tetapi karena cipher semakin rumit, maka pendekatan matematik masih tetap dominan dalam melakukan kriptanalisis. Perkembangan komputer pun ikut membantu kegiatan kriptanilisis. Sejarah kriptanalissi mencatat hasil gemilang seperti pemecahan Telegram Zimmermann yang membawa Amerika Serikat ke kancah Perang Dunia I, dan

pemecahan cipherteks dari mesin Enigma ikut andil mengakhiri Perang Dunia II [WIK06].

II. Beberapa Teknik Kriptanalisis

Ciphertext-only attack

Pada jenis serangan ini, kriptanalis mempunyai ciphertext dari beberapa data yang dienkripsikan dengan algoritma kriptografi yang sama. Tujuan kriptanalis adalah mendapatkan plaintext dari ciphertext atau lebih baik lagi menarik kesimpulan mengenai kunci yang digunakan.

Known-plaintext attack

Pada jenis serangan ini, kriptanalis tidak hanya memiliki ciphertext, tetapi juga plaintext dari ciphertext tersebut. Tujuan kriptanalis adalah menarik kesimpulan mengenai kunci yang digunkan untuk mengenkripsi data atau algoritma untuk mendekripsikan ciphertext.

Chosen-plaintext attack

Pada jenis serangan ini, kriptanalis selain mengetahui ciphertext dan plaintext, juga dapat memilih plaintext yang diinginkan yang biasanya memiliki lebih banyak informasi tentang kunci. Tujuan kriptanalis adalah menarik kesimpulan mengenai kunci yang diguankan untuk mengenkripsi data.

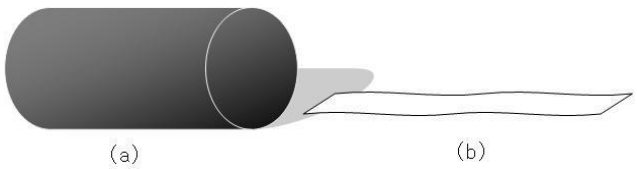
Adaptive-chosen-plaintext attack

Pada hal ini kriptanalis tidak hanya dapat memilih plaintext yang telah dienkripsi, tapi ia juga dapat memodifikasi pilihannya tersebut berdasarkan hasil enkripsi sebelumnya. Kriptanalis mengetahui blok palaintext yang lebih kecil dan kemudian memilih yang lainnya berdasarkan hasil enkripsi pertama, kedua dan seterusnya.

III. Sejarah Kriptanalisis Militer

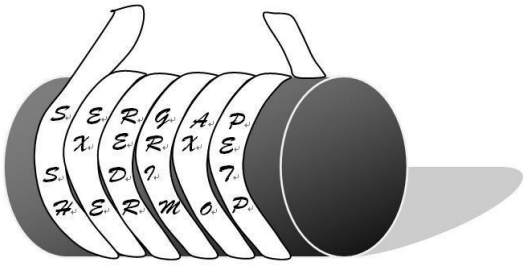
Scytale : Kriptografi Klasik

Archilochus sejerawan klasik Yunani pada abad ke-7 sebelum masehi menuliskan puisi tentang bagaimana tentara Sparta menggunakan alat yang disebut Scytale untuk menyembunyikan pesan. Scytale terdiri dari satu silider dan satu pita pesan panjang kain/kertas untuk ditulis seperti yang ditunjukkan oleh Gambar 1.



Gambar 1. (a) Silinder, yang digunakan untuk melilitkan pita pesan (b) Pita pesan bisa berupa kain atau kertas yang bisa dililitkan di silinder"

Untuk menyembunyikan pesan pertama kali yang dilakukan adalah melilitkan pita pesan itu pada silider sehingga menutupi permukaan silinder dan tidak saling tindih. Setelah itu, tulislah pesan yang ingin disembunyikan misalnya Leodinas ingin mengirim pesan ke komandan di lapangan **SERGAP XERXES DI THERMOPYLE BESOL**. Tulis huruf per huruf ke pita itu setelah dililitkan ke silinder seperti yang ditunjukkan oleh Gambar 2.



Gambar2. Penggunaan Scytale untuk menulis pesan

Setelah semua karakter pada pesan ditulis pisahkan pita pesan dan silinder dan karakter-karakter pada pita pesan sekarang seperti tidak memiliki makna. Jika pita pesan dibentangkan akan terbaca sebagai berikut:

“S SHYSEX ELOREDREKGRIM AX OB PETPE”

Tentunya mata-mata Xerxes bila membaca perintah ini tidak tahu maknanya. Namun bila anak buah Leonidas mendapat pita pesan ini dia hanya butuh silinder dengan ukuran sama lalu melilitkannya lagi ke silinder itu seperti pada

Gambar 2 dan akan terbaca pesan sesungguhnya.

Formula Matematika

Penyandian dengan Scytale dipandang dari sudut matematika modern sebenarnya sangat sederhana. Tekniknya disebut transposisi (perpindahan posisi) karakter ke posisi lain tanpa mengubah isi karakter tersebut. Bisa dilihat karakter yang terdapat di plaintext dan ciphertext tidak berubah jumlah dan jenisnya hanya saja posisinya berpindah. Silinder Scytale dapat dipandang sebagai kunci seberapa jauh transposisi dilakukan. Misalnya pada satu lingkup silinder, silender melewati **p** karakter berarti transposisi karakter di pesan asli ke karakter di pesan sandi sejauh **p**. Kita bisa menganggap silender sebagai tabel dengan jumlah baris **p**. Banyaknya kolom tergantung dengan panjang pita pesan misal panjang pita pesan adalah n maka banyaknya kolom adalah **n/p** bila **n** habis dibagi **p** atau **(n/p) + 1** bila n tidak habis dibagi **p** dengan "/" pembagian bilangan integer.

Dengan Text[i] menandakan karakter ke-i teks Text, sandi untuk Text dapat disusun baris per baris berdasarkan Tabel 1 sampai baris ke p . Sehingga teks untuk sandi bisa disusun sebagai berikut:

Sandi = "Text[1] Text[p + 1] Text[2p + 1] ... Text[2] Text[p+2] Text[2p+2] ... Text[p] Text[2p] ...Text[n]"

atau bila dirumuskan karakter ke-i untuk teks Sandi adalah

Sandi[i] = Text[((i * p)/n) + ((i * p) mod n)]

dengan operasi mod adalah operasi sisa bagi (modulus).

Pemecahan Kode

Seandainya pengantar pesar Leonidas tertangkap oleh pasukan Xerxes atau mata-mata Xerxes mampu membaca teks sandi yang dikirim meskipun pada awalnya mereka melihat teks sandi tidak berarti namun bisa saja ahli-ahli pemecah kode Persia melakukan "Attack" terhadap sandi meskipun hanya dapat sandinya saja untuk tahu apa pesan yang dikirim Leonidas. Karena yang menjadi rahasia hanyalah silender maka pemecahan kode sandi dapat dilakukan dengan melakukan proses yang sama dengan penyandian dengan menerka p dari p=1,..,n dengan n panjang pesan. Cukup dengan paling banyak n pesan rahasia Leonidas dapat dibongkar oleh pemecah kode.

```
p=1 -> S SHYSEX ELOREDREKGRIM AX OB PETPE
p=2 -> SSYE LRDEGI A BPTE HSXEOERKRM XO EP
p=3 -> SHEERRGMAOPP YXLEER XBEESS ODKI T
p=4 -> SY REIABT SEEKMX PSELDG PEHXORR OE
p=5 -> SSLRIXP EOEM E SXRK OT H EG BP YEDRA E
p=6 -> SERGAP XERXES DI THERMOPYLE BESOK
```

Meskipun sederhana Scytale merupakan metode sandi pertama yang terdokumentasi oleh sejarahwan dan digunakan untuk keperluan praktis dalam militer. Kita dapat lihat disini penyandian dengan Scytale dapat dengan mudah dipecahkan dan akhir kata

“sbdjuoeeaalnlknraeae ,hsmrb iajemIatalan ajd”.

IV. Monoalphabetic Encryption System

Kita ingat bahwa substitusi Monoalphabetic adalah sistem enkripsi dimana setiap terjadinya surat plaintext tertentu diganti dengan surat cyphertext. Misalnya, substitusi Caesar monoalphabetic sementara Vigenere tidak. Sebuah enkripsi Bukit 2x2 adalah substitusi monoalphabetic bertindak pada pasangan huruf. Perlu diingat bahwa definisi dari sebuah substitusi monoalphabetic memungkinkan untuk kemungkinan bahwa dua surat yang berbeda plaintext digantikan oleh surat cyphertext yang sama. Namun, untuk memecahkan sistem ini menggunakan serangan plaintext diketahui, kita akan memerlukan bahwa setiap dua huruf plaintext yang berbeda digantikan oleh dua huruf cyphertext yang berbeda.

Untuk mengenkripsi (mendekripsi) menggunakan Applet di bawah ini, hanya memotong dan paste Anda plaintext (cyphertext) ke dalam textarea, pilih Encrypt (Decrypt) dan mulai memasukkan kunci Anda. Plaintext (cyphertext) akan dikodekan (decode) sebagai Anda memasukkan kunci. Untuk memasukkan klik, kunci pertama di bawah persegi (di atas) plaintext (cyphertext) huruf yang Anda inginkan untuk mengenkripsi (dekripsi). Alun-alun sekarang harus disorot

dengan warna kuning. Sekarang ketik cyphertext yang sesuai (plaintext) huruf. Alun-alun ke kanan sekarang harus disorot. Untuk menghapus surat, klik pada kotak yang sesuai dan cukup tekan Kembali Ruang atau Del Bar Space dan tombol panah dapat digunakan untuk siklus melalui tombol tanpa menyuntingnya. Perhatikan bahwa huruf yang belum terjadi dalam kunci yang diarsir abu-abu.

Untuk istirahat substitusi monoalphabetic menggunakan serangan plaintext diketahui, kita dapat mengambil keuntungan dari fakta bahwa setiap pasangan huruf dalam pesan plaintext asli diganti dengan sepasang huruf dengan pola yang sama. Dengan kata lain, jika dua surat paintext yang berbeda, maka huruf yang bersangkutan mereka cyphertext juga harus berbeda. Untuk menggambarkan hal ini, jika kita tahu bahwa kata "AMUNISI" muncul dalam plaintext, maka kita dapat mencari string dari 10 huruf berurutan dari cyphertext yang memiliki pola sebagai berikut:

- The 2nd and 3rd letters are the same
- The 5th and 10th letters are the same (and different from the 2nd letter)
- The 6th and 8th letters are the same (and different from the 2nd and 5th letters
- All other letters are distinct.

Setelah kami telah menemukan semua kecocokan yang mungkin, kita dapat menggunakan statistik chi-kuadrat untuk menentukan mana yang pertandingan yang paling mungkin untuk plaintext diketahui.

V. Polyalphabetic Substitution

Ide untuk menggunakan cipher substitusi yang mengubah selama pesan adalah langkah maju yang sangat penting dalam kriptografi. Buku david Kahn, The codebreakers, memberikan laporan lengkap tentang asal-usul ide ini selama Renaissance Italia.

Bentuk paling awal dari cipher polyalphabetic dikembangkan oleh Leon Battista Alberti oleh 1467. Sistem-Nya yang terlibat menulis cipherteks dalam huruf kecil, dan menggunakan huruf kapital sebagai simbol, indikator disebut, untuk menunjukkan ketika perubahan substitusi, sekarang dan kemudian melalui pesan. Alfabet plaintext pada disk cipher nya dalam rangka, dan termasuk angka 1 sampai 4 untuk membentuk codeword dari kosakata kecil.

Selanjutnya, bentuk yang lebih modern diciptakan, yang mengubah substitusi untuk setiap huruf:

Sebuah sistem progresif-kunci, di mana kunci digunakan satu setelah yang lain dalam urutan normal. Ini pertama kali diterbitkan secara anumerta, dalam sebuah buku oleh Johannes Trithemius yang muncul pada 1518. ABCD kunci ... Z digunakan dengan huruf biasa dalam bentuk digambarkan di dalamnya.

Sebuah kata kunci yang menunjukkan huruf untuk digunakan pada gilirannya. Meskipun sistem ini adalah apa yang disebut Vigenère, itu berasal Giovan Batista Belaso pada tahun 1553. Pada 1563, Giovanni Battista Porta menambahkan penggunaan huruf diramu untuk sistem ini.

Para autokey sistem, di mana kunci mulai pilihan alfabet, tetapi pesan itu sendiri menentukan huruf digunakan untuk bagian-bagian selanjutnya dari pesan. Meskipun bentuk ini tidak dapat digunakan pertama kali diusulkan oleh Girolamo Cardano, Blaise de itu Vigenère yang mengusulkan bentuk modern dari cipher autokey pada 1585.

Tabel berikut ini berisi 26 kompak huruf, masing-masing diberi label dengan huruf alfabet:

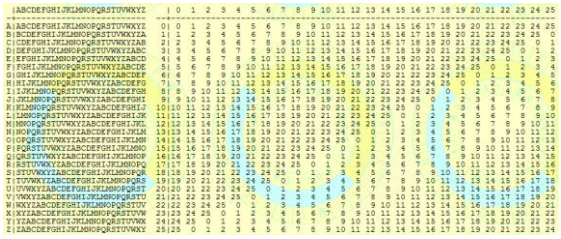
```
B C D E F   ZABCDEFGHIJKLMNOPQRSTUVWXY
G H I J K   UVWXYZABCDEFGHIJKLMNOPQRST
L M N O P   PQRSTUVWXYZABCDEFGHIJKLMNO
Q R S T U   KLMNOPQRSTUVWXYZABCDEFGHIJ
V W X Y Z   FGHIJKLMNOPQRSTUVWXYZABCDE

B G L Q V   ABCDEFGHIJKLMNOPQRSTUVWXYZ
C H M R W   BCDEFGHIJKLMNOPQRSTUVWXYZA
D I N S X   CDEFGHIJKLMNOPQRSTUVWXYZAB
E J O T Y   DEFGHIJKLMNOPQRSTUVWXYZABC
F K P U Z   EFGHIJKLMNOPQRSTUVWXYZABCD
```

Sebuah alfabet tidak ditampilkan, karena dalam alfabet itu, setiap surat itu sendiri singkatan, dan sebagainya, jika tidak dilakukan, tidak perlu mendongak dalam tabel. Untuk alfabet lain, gunakan huruf yang mengindikasikan alfabet untuk menemukan baris antara lima besar, dan baris diantara lima bawah; menggunakan dua baris, baris atas singkatan plaintext, yang lebih rendah untuk cipher.

Jadi, untuk alfabet Q, baris atas KLMNO dimulai ... dan baris bawah dimulai ABCDE ..., dan begitu K menjadi A, T menjadi G, dan A menjadi Q dalam alfabet.

Jika Anda berpikir dari A apa-apa saat berdiri untuk nol, B untuk 1, sampai dengan Z 25, ini set tertentu dari huruf adalah lebih dari 26 penambahan modulo dari plaintext dan kunci untuk mendapatkan ciphertext. Edaran disk atau skala geser dapat digunakan untuk melakukan penambahan. Ini, mungkin, dapat lebih mudah dilihat jika kita menunjukkan tablo Vigenère secara penuh, disertai dengan tabel untuk Modulo-26 Selain itu:



Dan, tentu saja, bukan tabel Modulo-26 tambahan untuk 26-huruf alfabet kami, meja Vigenere dapat dibangun untuk alfabet apapun. Jadi, modulo-24 Selain itu akan digunakan untuk alfabet Yunani, modulo-32 tambahan untuk alfabet Rusia, atau, seperti yang ditunjukkan pada gambar di sebelah kiri, modulo-22 tambahan untuk alfabet Ibrani. Di sini, tabel ini ditulis dari kanan ke kiri, ke arah yang sama seperti biasanya digunakan untuk menulis bahasa Ibrani.

Pesan "Seandainya kau ada di sini" dapat dienkripsi oleh tiga metode yang mungkin, menggunakan Siam sebagai kata kunci:

Kata kunci:

- Pesan: WISHYOUWEREHERE
- Kunci: SIAMESESIAMESES
- Cipher: OQSTCGYOMRQLWVW

Progresif kunci:

- Pesan: WISHYOUWEREHERE
- Kunci: SIAMESETJBNFTFU
- Cipher: OQSTCGYPNSRMXWY

Autokey:

- Pesan: WISHYOUWEREHERE
- Kunci: SIAMESEWISHYOUW
- Cipher: OQSTCGYSMJLFSLA

Untuk kunci progresif, kata kunci, diikuti oleh kata kunci maju satu posisi pada satu waktu melalui alfabet, digunakan. Hanya menggunakan ABCDEF ... sebagai kunci tidak akan cukup unik untuk melayani sebagai cipher nyata.

Tabel yang ditampilkan di sini dapat dianggap sebagai meja untuk penambahan huruf, yang setara dengan itu, modulo 26 dimana A singkatan untuk 0, B singkatan 1, melanjutkan ke Z, yang akan berdiri untuk 25.

Sistem kata kunci polos dapat dipecahkan dengan metode Kasiski, mencari urutan berulang huruf dalam pesan, dan menghitung jumlah huruf di antara mereka. Dari sini, mudah untuk menemukan faktor umum, dan menentukan panjang kata kunci yang digunakan. Hal ini memungkinkan satu jenis huruf ke dalam yang enciphered dengan alfabet yang sama. Jika huruf yang normal digunakan, melihat profil dari jumlah frekuensi membuat solusi trivial.

Untuk dua metode lainnya, kriptanalisis SD hanya memungkinkan solusi untuk normal (atau setidaknya diketahui) huruf. Kasus progresif kunci dapat dibuat untuk menghasilkan periode yang jika terlihat tidak untuk surat diulang, tapi untuk jarak diulang dalam alfabet antara huruf yang berdekatan, ini mengurangi gerakan lambat keluar kata kunci melalui alfabet. Autokey pada dasarnya dapat diselesaikan dengan brute force sidang pada panjang kata kunci awalnya. Tentu saja, sistem ini masih bisa diselesaikan dengan campuran huruf, tetapi metode yang lebih maju diperlukan, melibatkan statistik atau beberapa pesan dengan kunci yang sama.

Selain menggunakan huruf diramu untuk keamanan yang lebih besar, ada sistem lain yang penting sejarah.

Para Gronsfeld, yang menambahkan kunci numerik untuk plaintext, berarti bahwa hanya ada sepuluh setara mungkin untuk setiap huruf,

tapi lebih mudah dilakukan dengan tangan tanpa meja atau slide atau disk. Sistem Porta menggunakan meja kecil; paruh pertama dari alfabet adalah stasioner sedangkan babak kedua pindah, dan setara untuk huruf dalam setiap setengah alfabet ditemukan di setengah lainnya.

Tabel untuk sistem Porta (dikonversi ke huruf alfabet 26-modern) adalah sebagai berikut:

```
      ABCDEFGHIJKLM
      -------------
  AB |NOPQRSTUVWXYZ
  CD |OPQRSTUVWXYZN
  EF |PQRSTUVWXYZNO
  GH |QRSTUVWXYZNOP
  IJ |RSTUVWXYZNOPQ
K KL |STUVWXYZNOPQR
e MN |TUVWXYZNOPQRS
y OP |UVWXYZNOPQRST
  QR |VWXYZNOPQRSTU
  ST |WXYZNOPQRSTUV
  UV |XYZNOPQRSTUVW
  WX |YZNOPQRSTUVWX
  YZ |ZNOPQRSTUVWXY
```

Para Gronsfeld, dan, bahkan lebih mudah, Porta, karena mereka hanya mengijinkan beberapa surat, tetapi tidak yang lain, sebagai setara untuk setiap huruf plaintext yang diberikan, dapat diserang melalui kelemahan ini.

Dalam mencoba untuk merancang sebuah sandi yang, seperti Gronsfeld, cocok untuk aritmatika mental, saya menggunakan (untuk abjad Inggris) metode mewakili nomor sebagai huruf yang digunakan oleh Ibrani kuno dan Yunani kuno:

```
A 1   J 10   S 100
B 2   K 20   T 200
C 3   L 30   U 300
D 4   M 40   V 400
E 5   N 50   W 500
F 6   O 60   X 600
G 7   P 70   Y 700
H 8   Q 80   Z 800
I 9   R 90
```

Kemudian, aturan untuk encipherment adalah ini:

a) Jika huruf plaintext dan kunci di kolom yang sama, mereka menambahkan:

B (2) + F (6) = H (8)

L (30) + J (10) = M (40)

b) Jika huruf plaintext dan kunci dalam dua kolom yang berbeda, angka nol mereka ditambahkan, dan huruf di kolom ketiga yang tidak berisi kunci atau plaintext yang mengandung jumlah tersebut diambil:

D (4) + L (30) = Y (700)

W (500) + K (20) = G (7)

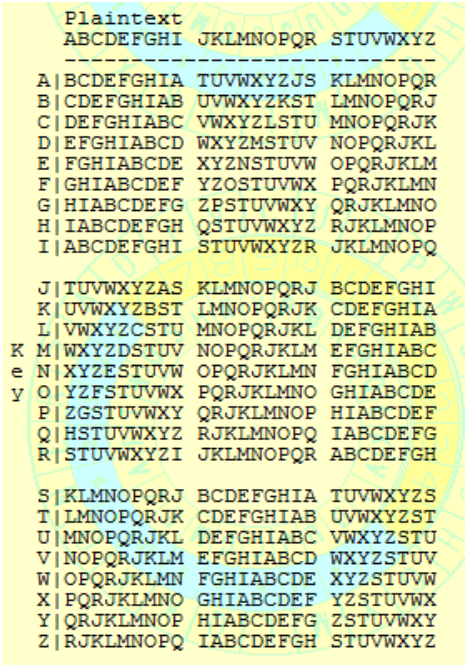
Jika kita memiliki alfabet 27 huruf, kita hanya harus menambahkan bahwa ketika jumlah lebih besar dari 9, kurangi 9 (di tempat yang sesuai digit):

M (40) + Q (80) = L (30)

Untuk alfabet 26 huruf, mudah untuk memodifikasi aturan (a): jika dua huruf berada di kolom ketiga, kurangi 800 bukan 900.

U (300) + Y (700) = T (200)

Aturan (b) diubah dengan cara ini: selalu kurangi 9, jika huruf cipher dan tombol huruf menghasilkan 900 sebagai hasilnya, menggunakan bukan surat yang akan diproduksi oleh enciphering surat dengan nilai 900 dengan tombol huruf. Karena tidak ada surat dengan nilai tersebut, ketika salah satu diproduksi oleh menguraikan, menguraikan 900 dengan kunci untuk mendapatkan huruf plaintext benar.



```
    Plaintext
    ABCDEFGHI JKLMNOPQR STUVWXYZ
    ----------------------------
  A|BCDEFGHIA TUVWXYZJS KLMNOPQR
  B|CDEFGHIAB UVWXYZKST LMNOPQRJ
  C|DEFGHIABC VWXYZLSTU MNOPQRJK
  D|EFGHIABCD WXYZMSTUV NOPQRJKL
  E|FGHIABCDE XYZNSTUVW OPQRJKLM
  F|GHIABCDEF YZOSTUVWX PQRJKLMN
  G|HIABCDEFG ZPSTUVWXY QRJKLMNO
  H|IABCDEFGH QSTUVWXYZ RJKLMNOP
  I|ABCDEFGHI STUVWXYZR JKLMNOPQ

  J|TUVWXYZAS KLMNOPQRJ BCDEFGHI
  K|UVWXYZBST LMNOPQRJK CDEFGHIA
  L|VWXYZCSTU MNOPQRJKL DEFGHIAB
K M|WXYZDSTUV NOPQRJKLM EFGHIABC
e N|XYZESTUVW OPQRJKLMN FGHIABCD
y O|YZFSTUVWX PQRJKLMNO GHIABCDE
  P|ZGSTUVWXY QRJKLMNOP HIABCDEF
  Q|HSTUVWXYZ RJKLMNOPQ IABCDEFG
  R|STUVWXYZI JKLMNOPQR ABCDEFGH

  S|KLMNOPQRJ BCDEFGHIA TUVWXYZS
  T|LMNOPQRJK CDEFGHIAB UVWXYZST
  U|MNOPQRJKL DEFGHIABC VWXYZSTU
  V|NOPQRJKLM EFGHIABCD WXYZSTUV
  W|OPQRJKLMN FGHIABCDE XYZSTUVW
  X|PQRJKLMNO GHIABCDEF YZSTUVWX
  Y|QRJKLMNOP HIABCDEFG ZSTUVWXY
  Z|RJKLMNOPQ IABCDEFGH STUVWXYZ
```

VI. Kesimpulan

1. Keberhasilan kriptanalisis tergantung kepada kombinasi matematis, keingintahuan, intuisi, keuletan, sumberdaya komputasi yang memadai, dan seringkali keberuntungan.

2. *Monoalphabetic Encryption System* dan *Polyalphabetic Substitution* merupakan dua metode yang yang sering digunakan dalam kriptanalisis khususnya dalam bidang militer.

REFERENSI

http://www.informatika.org/~rinaldi/Buku/Kriptografi/Bab-1_Pengantar%20Kriptografi.pdf (waktu akses : Jumat 9 Desember 2011; 18.45)

http://tutorialkuliah.blogspot.com/2009/08/tugas-kuliah-tentang-kriptanalisis.html (waktu akses : Sabtu 10 Deseember 2011; 22.19)

http://blog.sivitas.lipi.go.id/blog.cgi?isiblog&1148517408&&&1036007025&&1289621686&rifk001&1289621570 (waktu akses : Sabtu 10 Desember 2011; 23.56)

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, 11 Desember 2011

ttd

Sonny Theo Tumbur Manurung

13510027