# Analisis Kriptografi Klasik Jepang

Ryan Setiadi (13506094)
*Program Studi Teknik Informatika*
*Sekolah Teknik Elektro dan Informatika*
*Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia*
*If16094@students.if.itb.ac.id*

***Abstract* — Kriptografi merupakan salah satu cara menyembunyikan pesan dengan cara mengubah pesan tersebut menjadi suatu pesan yang tidak bermakna. Tujuan dari penyembunyian pesan ini adalah agar pesan yang dikirimkan dari pihak si pengirim ke si pihak penerima tidak mudah dipecahkan oleh pihak ketiga. Biasanya pesan ini adalah pesan yang sangat penting dan rahasia. Olehkarena itu keamanan dan kerahasian pesan ini harus benar-benar terjamin sebelum pesan dikirimkan. Pesan itu juga harus dapat dideskripsikan ketika pesan tersebut sampai pada pihak penerima. Salah satu metode Kriptografi Klasik ini adalah dengan cara menSubtitusi tulisan yang ada dengan huruf lain sehingga menjadi suatu pesan yang tidak bermakna.**

***Kriptografi sudah dipakai sejak jaman dahulu, Kriptografi ini dinamakan kriptografi klasik. Kriptografi sering dipakai ketika pada masa perang berlangsung. Salah satu negara yang menggunakan Kriptografi adalah Jepang. Jepang terlibat langsung pada masa perang dunia I dan perang dunia II. Ada beberapa macam kriptografi yang digunakan oleh kapal perang Jepang, salah satunya adalah Uesugi checkerboard. Karena Jepang menggunakan tulisan (bahasa) yang berbeda dengan negara lainnya maka akan lebih sulit untuk mendeskripsikan pesan yang dikirimkan oleh pihak Jepang.***

***Pada Makalah ini akan dibahas bagaimana Jepang memakai Kriptografi pada perang dunia, apa saja yang mereka gunakan untuk menenkripsikan, mengirimkan, dan mendeskripsikan pesan dari satu tempat ke tempat lainnya. Cara menggunakan dan memecahkan kriptografi yang Jepang pakai akan diujicoba dan dianalisis keefektifanannya, sehingga akan dapat diketahui Kriptografi Klasik manakah yang lebih baik untuk digunakan pada masa itu.***

***Kata Kunci* — Kriptografi, Klasik, Jepang, Subtitusi**

## I. PENDAHULUAN

Kriptografi adalah sebuah seni atau ilmu kuno untuk menyembunyikan sesuatu dibalik sesuatu. Biasanya yang disembunyikan adalah tulisan karena tulisan merupakan suatu media yang paling mudah dan sering digunakan setiap harinya.Pesan tersebut mungkin sangat rahasia, rahasia, biasa-biasa saja, maupun pesan yang harus dipecahkan seperti pesan yang terdapat pada permainan puzzle anak-anak.

Kriptografi Klasik bisa dibilang adalah kriptografi yang sudah tidak digunakan lagi untuk merahasiakan pesan yang sangat rahasia dan rahasia. Ini dikarenakan rumus pemecahan kriptografi telah ditemukan oleh orang pada jaman dulunya. Akan tetapi Kriptografi Klasik ini adalah sumber dari segala Kriptografi. Kriptografi Klasik ini masih disukai orang karena sifatnya yang sederhana dan menarik.

Pada jaman ini orang telah menciptakan dan memakai Kriptografi yang lebih aman dengan menggunakan sistem biner. Kriptografi ini dinamakan dengan Kriptografi Modern. Kriptografi Modern menggunakan sistem berbasis komputer dalam penggunaannya. Kriptografi ini dinilai cukup rumit akan tetapi sangat berguna dalam menyembunyikan pesan yang rahasia. Kriptografi Modern tidak akan dibahas pada makalah ini.

Makalah ini berisi macam-macam Kriptografi Klasik beserta Kriptografi Klasik Jepang, cara menggunakan dan memecahkan kode, serta pengujian dan analisis kriptografi manakah yang lebih efektif untuk menyembunyikan pesan pada jaman dahulu.

## II. KONSEP TEORI

Sebelum memulai, ada tiga hal penting yang menjadi bagian dari Kriptografi.

1. Plain Teks -> pesan awal sebelum disembunyikan, biasanya diberi symbol P.
2. Kunci -> sebuah teks yang memegang peranan penting untuk menyembunyikan pesan, K.
3. Cipher Teks -> pesan yang telah disembunyikan, tidak memiliki makna berarti, C.

Disembunyikan disini adalah diubah tulisan tersebut dengan cara menggabungkan plain teks dengan kunci rahasia yang telah dibuat menjadi cipher teks. Proses penyembunyian pesan ini disebut sebagai Enkripsi(E) dan proses pengembalian pesan dari cipher teks menjadi plain teks adalah Dekripsi(D).

Ada dua cara yang dipakai dalam mengenkripsikan pesan Kriptografi Klasik, transposisi dan subtitusi. Cara

transposisi yaitu dengan cara menukar-nukar urutan plain teks sehingga menjadi kata yang sulit dibaca. Transposisi tidak menggunakan kunci dan harus ditebak urutan huruf yang benarnya. Kebanyakan orang memakai pola tersendiri sehingga mudah dikembalikan menjadi plain teks semula. Contoh dari cara transposisi dengan pola: Plainteks = kriptografi, pola = tiga huruf, dengan ini kita akan meloncat 2 huruf diantara huruf pertama dan huruf berikut, kemudian huruf tersebut disambungkan kembali. Huruf pertama adalah k dan 3 huruf berikutnya adalah p, disambungkan sehingga menjadi sebuah cipherteks = kpgfrttiioa. Sedangkan transposisi tanpa pola akan menghasilkan cipher teks yang lebih sulit ditebak(atau tidak untuk ditebak sama sekali), cipherteks = agtipkofitr.

Cara kedua adalah cara Subtitusi, mengubah satu persatu huruf pada plainteks menjadi cipherteks dengan kunci yang telah dibuat sebelumnya. Salah satu contoh adalah Caesar Cipher. Caesar Cipher memiliki algoritma sederhana dan sangat menarik. Plainteks yang ada digeser dua baris ke kanan sehingga huruf a menjadi huruf d, b menjadi huruf e, dan seterusnya.

**P: a b c d e ...**
**C: d e f g h ...**

Caesar Cipher termasuk salah satu Subtitusi abjad tunggal karena satu huruf hanya digantikan dengan satu cipherteks sehingga semua huruf yg sama akan memiliki cipherteks yang sama pula. Ada juga yang dinamakan dengan Subtitusi Homofonik, sebuah huruf plainteks diubah menjadi dua cipherteks yang memiliki homofon. Tidak akan dibahas karena kuncinya sangat banyak dan tidak memiliki aturan yang jelas.

Salah satu Cipher Klasik Subtitusi yang lebih tinggi daripada abjad tunggal adalah abjad majemuk. Satu huruf dapat diubah menjadi cipherteks yang berbeda tergantung pada kunci yang ada. Salah satu cipher ini adalah Vigenere Cipher.

## III. KRIPTOGRAFI KLASIK JEPANG

Kriptografi Jepang merupakan salah satu Kriptografi yang unik karena penggunaan bahasa Jepang berbeda dengan bahasa dunia lainnya.

Sistem Cipher yang digunakan adalah subtitusi sederhana yang dikenal sebagai Polybius square atau "checkerboard". Alphabet I-ro-ha berisi 48 huruf lebih banyak daripada alphabet biasa. Sehingga kotak tersebut berukuran 7 x 7 dengan satu kotak kosong. Setiap baris dan kolom diberi nomor satu sampai tujuh.

Cara menekripsikan pesan cukup mudah. Jika kita memiliki Plainteks seperti "saya ingin makan sushi" => "sushi wo tabetai", hanya tinggal mencari huruf tersebut pada kotak dan mengubahnya dengan angka baris dan kolom. Enkripsi = 75 67 25 32 16 32 11 atau 57 76 52 23 61 23 11. Beberapa huruf seperti be tidak terdapat pada tabel dikarenakan be adalah salah satu bentuk dari he, sehingga untuk dienkripsikan kalimat harus diubah menjadi bentuk romanji dasar. Hal ini menyebabkan kesalahartian sangat mudah terjadi terutama pada kata yang memiliki.

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| 1 | i | ro | ha | ni | ho | he | to |
| 2 | chi | ri | nu | ru | wo | wa | ka |
| 3 | yo | ta | re | so | tsu | ne | na |
| 4 | ra | mu | u | i1 | no | o | ku |
| 5 | ya | ma | ke | fu | ko | e | te |
| 6 | a | sa | ki | yu | me | mi | shi |
| 7 | e | hi | mo | se | su | n | |

Sistem yang menggunakan "checkerboard" untuk mengubah alphabet menjadi angka dibuat oleh Polybius lebih dari 2000 tahun yang lalu. Ada tida kelebihan utama dari sistem ini. Pertama, mengubah huruf menjadi angka akan menghasilkan bermacam-macam kombinasi matematika yang tidak mudah untuk didekripsikan. Kedua, sistem checkerboard mengurangi jumlah karakter Pengurangan ini membuat pemecah kode menjadi lebih sulit untuk memecahkannya secara subtitusi satu demi satu. Dan yang ketika adalah walaupun sistem ini mengubah plainteks menjadi cipherteks yang dua kali lebih panjang, cipherteks ini dapat dibagi menjadi dua bagian.

Salah satu variasi dari Uesugi checkerboard adalah checkerboard waka poem. Waka poem adalah suatu puisi Jepang pada jaman dahulu.

| ***re*** | ***ku*** | ***fu*** | **yu** | **no** | **ki** | **a** | |
|---|---|---|---|---|---|---|---|
| e | a | ya | ra | yo | chi | i | **tsu** |
| hi | sa | ma | mu | ta | ri | ro | **re** |
| mo | ki | ke | u | re | nu | ha | **na** |
| se | yu | fu | i | so | ru | ni | **ku** |
| su | me | ko | no | tsu | wo | ho | **mi** |
| n | mi | e | o | ne | wa | he | **e** |
| | shi | te | ku | na | ka | to | **shi** |

Perbedaan dari Uesugi checkerboard pertama adalah dengan menggunakan huruf waka sebagai subtitusi plainteksnya," tsurenakumieshiakinoyufukure".

## IV. ENKRIPSI

Pada bagian ini akan dijelaskan lebih detail bagaimana cara menggunakan beberapa metode penenkripsian pesan menggunakan cipher subtitusi abjad tunggal, cipher subtitusi abjad majemuk, cipher transposisi dan cipher uesugi.

Chiper Subtitusi Abjad Tunggal

Seperti yang kita ketahui sebelumnya, prosesnya dilakukan dengan cara mengubah sebuah huruf plainteks dengan sebuah huruf cipherteks.

Ada beberapa cara yang dapat digunakan dan akan digolongkan dengan jenis-jenis kunci yang ada.

1. Kunci Geser

   Dilakukan dengan cara mengganti plainteks dengan kunci dari alphabet yang telah digeser sebelumnya. Salah satu contoh cipher ini adalah Caesar Cipher. Dapat digeser sebanyak 26 kemungkinan.

   Logika dasar: C = E(P)

   Keterangan: C = cipherteks, E = fungsi enkripsi, P = plainteks, D = fungsi dekripsi

   Rumus: E(P) = (P + N) mod 26

   N sebagai jumlah pergeseran. Pada Caesar Cipher, menggunakan kunci geser N = 3. Huruf A-Z menjadi angka 1 sampai 26, sehingga

   A => (0 + 3) mod 26 = 3 => D dan seterusnya

   Contoh kasus:

   P: Kriptografi sangat sulit

   K: N = 5

   C: Fmdkojbmsad nsibso npqdo

   Dengan A => F, B =>G, dan seterusnya. Kita dapat membuatnya menggunakan Microsoft Excel dengan mudah. Pertama buatlah huruf A-Z kebawah. Kemudia copylah kolom tersebut ke kolom sebelahnya. Cut kolom tersebut sejumlah N yang digeser dan Cut sisanya ke atas.

   Analisis:

   Kelebihan dari kunci geser ini adalah sangat mudah dipakai dan tidak merepotkan pengguna. Kekurangannya adalah hanya terdapat 26 kemungkinan sehingga mudah dipecahkan secara satu-satu sehingga tidak cocok digunakan untuk menyembunyikan pesan yang besifat rahasia. Kunci geser ini cocok digunakan untuk permainan mengasah otak.

2. Kunci Acak

   Sama seperti Kunci Geser, perbedaannya adalah tidak terdapat susunan kunci, satu huruf plaintext tetap menjadi satu huruf ciphertext akan tetapi tidak memiliki urutan. Terdapat 26! kemungkinan cipherteks.

   Logika dasar: Pi = Ci

   Rumus: tidak ada karena tidak terurut

   Cara mudah untuk menggunakan Cipher ini adalah dengan cara menuliskan semua Abjad pada Excel dan memasangkannya dengan Abjad berbeda. Dikarenakan tidak boleh ada abjad yang serupa, coretlah abjad yang telah digunakan sebelumnya.

   Analisis:

   Kelebihan dari kunci Acak adalah lebih aman dan lebih rumit untuk dipecahkan dengan kemungkinan 26!. Bisa juga dikombinasikan dengan cara menghilangkan spasi antara kata sehingga menambah kerumitan cipherteks untuk dipecahkan. Kekurangannya adalah masih kurang rumit karena konsep Subtitusi Abjad Tunggal ini hanya mengubah satu huruf menjadi satu huruf cipherteks yang sama.

   Contoh Kasus:

   P: Kriptografi sangat sulit

   K:

| | | |
|---|---|---|
| x | A | J |
| x | B | P |
| x | C | F |
| x | D | T |
| x | E | G |
| x | F | E |
| x | G | U |
| x | H | Y |
| x | I | Q |
| x | J | C |
| x | K | N |
| x | L | I |
| x | M | B |
| x | N | A |
| x | O | H |
| x | P | V |
| x | Q | Z |
| x | R | K |
| x | S | D |
| x | T | X |
| x | U | W |
| x | V | L |
| x | W | O |
| x | X | R |
| x | Y | M |
| x | Z | S |

   C: Nkqvxhukeq djaujx dwiqx

Subtitusi Abjad Majemuk

Sama halnya dengan Subtitusi Abjad Tunggal yaitu mengubah huruf plainteks menjadi huruf cipherteks, namun kunci penting di sini adalah kunci yang akan digabungkan dengan plainteks. Sehingga memungkinkan sebuah huruf plainteks memiliki beberapa huruf cipherteks.

Ada beberapa cara yang digunakan tetapi untuk Subtitusi Abjad Majemuk hanya akan dibahas Vigenere Cipher.

Vigenere Cipher

Untuk menenkripsikan pesan dengan ala vigenere pertama-tama kita butuhkan sebuah table vigenere.

| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| B | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A |
| C | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B |
| D | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C |
| E | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D |
| F | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E |
| G | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F |
| H | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G |
| I | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H |
| J | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I |
| K | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J |
| L | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K |
| M | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L |
| N | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M |
| O | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
| P | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
| Q | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P |
| R | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q |
| S | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R |
| T | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S |
| U | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T |
| V | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U |
| W | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V |
| X | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W |
| Y | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X |
| Z | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y |

Tabel ini kita butuhkan untuk menkombinasikan Plainteks dengan kunci. Pada tabel terdapat baris dan kolom yang diurutkan dari A ke Z. Keduanya simetris sehingga dapat digunakan dengan baris terlebih dahulu maupun kolom terlebih dahulu.

Contoh kasus:

P: Kriptografi sangat sulit

K:susahsekalis usahse kalis

Kunci yang digunakan harus lebih kecil sama dengan plainteks yang ada. Jika kunci kurang dari plainteks maka kunci akan diulangi sampai panjang plainteks.

Cara menSubtitusikannya cukup mudah, yaitu dengan cara melihat baris dan kolom tabel. Plainteks K dengan Kunci s jika digabungkan akan menjadi cipherteks C. metode ini harus dilakukan secara teliti karena mungkin terdapat kesalahan pembacaan huruf.

Cara lainnya adalah dengan menggunakan Rumus Subtitusi normal

C = (P + K) mod 26

Akan menghasilkan nilai yang sama dengan tabel.

Vigenere mempunyai kelebihan pada jumlah kombinasi cipherteks yang dihasilkan karena satu huruf plainteks mungkin dapat menghasilkan 26 kemungkinan huruf. Sehingga semakin panjang plainteksnya akan semakin aman.

Cipher Transposisi

Transposisi adalah cara mengubah urutan dari plainteks tanpa mengubah plainteks tersebut. Urutan yang ada bisa berpola maupun benar-benar acak.

Contoh kasus:

P: Kriptografi sangat sulit

Dengan cara berpola kita dapat mengubahnya menjadi beberapa huruf perkolom.

Krip
Togr
Afis
Anga
Tsul
It

Selajutnya kita menyambungkan teks yang sudah dipisahkan perkolom yang ada mulai dari kolom pertama sehingga akan dihasilkan cipherteks ktaatirofnstigiguprsal.

Kelebihan dari transposisi ini adalah enkripsi yang cukup sederhana sehingga tidak perlu memikirkan kunci yang dibutuhkan. Kelemahannya adalah sangat lemah untuk digunakan pada pesan yang rahasia.

Cocok digunakan untuk permainan anak karena sifatnya yang mengasah otak hanya dengan cara membaca tulisan secara loncat tiga huruf.

Cipher Uesugi, Uesugi checkerboard

Menggunakan checkerboard berukuran 7 x 7 untuk menampung 48 huruf I-ro-ha. Setelah dienkripsikan cipherteks akan berbentuk angka.

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| 1 | i | ro | ha | ni | ho | he | to |
| 2 | chi | ri | nu | ru | wo | wa | ka |
| 3 | yo | ta | re | so | tsu | ne | na |
| 4 | ra | mu | u | i1 | no | o | ku |
| 5 | ya | ma | ke | fu | ko | e | te |
| 6 | a | sa | ki | yu | me | mi | shi |
| 7 | e | hi | mo | se | su | n | |

Untuk menggunakan cipher ini kita harus menggunakan langkah tambahan yaitu dengan cara mengubah plainteks non-Jepang kedalam bahasa Jepang.

Terjemahan bahasa Jepang mungkin akan lebih panjang atau lebih pendek tergantung dari konteks kalimat yang diterjemahkan. Olehkarena itu panjang cipherteks akan berbeda dari panjang plainteks semula.

Contoh kasus:

P: Kriptografi sangat sulit

Pt: Kuriputogurafi wa totemo muzukashi

K: tabel di atas

Dengan demikian kita dapat mengubah huruf romanji kedalam cipherteks uesugi sehingga akan menghasilkan

C: 76224571741314126271753724577276

Secara kolom dan baris dan dapat pula dibaca dari baris ke kolom sehingga menghasilkan cipherteks yang berbeda.

Kelebihan dari cipher uesugi adalah mudah digunakan dengan tingkat keamanan yang tinggi dikarenakan bermacam-macam kunci yang mungkin dihasilkan. Selain itu cipherteksnya berupa angka sehingga tidak akan mudah dipecahkan oleh orang. Kelemahannya adalah kemungkinan makna ganda dari huruf yang memilik bentuk lainnya. Akan tetapi kelemahan sistem

ini dapat ditutupi dengan memperbesar checkerboard dan menambah jumlah kata didalamnya.

## V. DEKRIPSI

Setelah pesan itu dienkripsikan menjadi sebuah pesan yang tidak bermakna, apa yang akan dilakukan selanjutnya dengan pesan yang tidak bermakna tersebut?

Pesan itu tidak adak memiliki arti apa-apa sebelum pesan itu didekripsikan menjadi plainteks atau pesan yang berarti. Olehkarena itu Kriptanalisis dibutuhkan. Kriptanalisis adalah orang atau agen yang bertujuan untuk memecahkan kode, juga bisa disebut sebagai code breaker. Umumnya mereka ada professional yang bekerja pada pihak keamanan untuk mengetes apakah sistem keamanan(enkripsi) suatu perusahaan yang dibuat telah cukup aman dan sulit dipecahkan.

Kriptografi klasik yang artinya kriptografi yang sudah kuno dan tidak dipakai ini memiliki solusi pemecahan untuk mendekripsikan pesan. Berikut ini adalah cara untuk mendekripsikan cipher:

Subtitusi Abjad Tunggal Kunci Geser

1. Langkah pertama adalah dengan cara menerka suatu teks cipher berulang-ulang kali
2. Setelah menemukan satu kata yang bermakna, maka kita dapat mencari kuncinya dengan cara menghitung N penggeseran huruf
3. Setelah mendapat N maka semua cipherteks dapat diubah menjadi plainteks dengan rumus
   P = (C – N) mod 26

Subtitusi Abjad Majemuk Kunci Acak

1. Dapat menggunakan Cara Dekripsi Kunci Geser, akan tetapi lebih sulit karena tidak memiliki pola
2. Hitunglah jumlah huruf yang ada pada cipherteks
3. Gantilah huruf terbanyak dengan huruf E dan kombinasi dua huruf dengan TH, juga tiga huruf dengan THE.
4. Carilah sebuah kata yang mudah diterka dan cobalah memasukan huruf selain THE untuk menghasilkan suatu kata bermakna
5. Ulangi langkah empat sampai berhasil mengubah semua cipherteks menjadi plainteks

Subtitusi Abjad Majemuk: Vigenere Cipher

Untuk mendekripsikan kode Vigenere ada beberapa hal yang perlu diketahui, semakin panjang kunci maka semakin sulitlah cipherteks tersebut untuk dipecahkan. Olehkarena itu pada bagian ini hanya akan dibahas bagaimana cara memecahkan kode Vigenere dengan kunci yang pendek.

1. Carilah dua buah cipherteks yang sama panjang lebih dari lima huruf untuk keakuratannya.
2. Hitung jarak antara dua cipherteks tersebut dan carilah jarak terpendek.
3. Bagilah cipherteks tersebut menjadi panjang terdekat dua buah cipherteks yang sama ke dalam beberapa kolom
4. Carilah huruf terbanyak pada tiap barisnya dan ubah huruf tersebut dengan menggunakan metode subtitusi kunci acak
5. Setelah mendapatkan kunci maka semua cipherteks dapat didekripsikan dengan menggunakan rumus yang sama.

Transposisi

Untuk cipher transposisi tidak dimiliki cara pemecahan yang mudah. Satu-satunya cara untuk mendekripsikan cipherteks adalah dengan cara menemukan pola yang tepat. Pola tersebut dapat ditemukan dengan cara menebak berapakah huruf tersebut dilewati setelah hutuf pertama sehingga akan menghasilkan kata yang bermakna

Uesugi Cipher

Salah satu cara mendekripsikan cipherteks dengan mudah adalah dengan cara memiliki salinan kunci checkerboard. Jika tidak, satu-satunya cara adalah dengan cara memasukan ke49 kombinasi huruf kedalam checkerboard sehingga jikadigunakan akan menghasilkan kata yang bermakna.

## VI. ANALISIS

Dari kelima medote enkripsi, kelimanya memiliki perbedaan dalam cara menenkripsi sebuah pesan.

Berikut ini adalah jumlah kemungkinan sebuah huruf cipherteks dari lima metode sebelumnya.

1. Kunci Geser memiliki 26 kemungkinan
2. Kunci Acak memiliki 26! kemungkinan
3. Vigenere memiliki 26 kemungkinan setiap hurufnya dan juga disesuaikan dengan panjang kunci, sehingga jika panjang kunci = panjang plainteks akan menghasilkan 26 ^ plainteks.
4. Transposisi memiliki kemungkinan sepanjang plainteks tersebut, jika plainteks tersebut berjumlah 20 huruf, maka kemungkinannya adalah 20!.
5. Uesugi Cipher memiliki kemungkinan 49! yang didapat dari jumlah kotak checkerboard dan juga dikalikan dua karena cipherteks dapat berupa dua bentuk yang berbeda

Metode-metode ini memiliki kelebihan dan kelemahan masing-masing. Metode tersebut dapat dipakai untuk menenkripsikan pesan sederhana yang sifatnya tidak terlalu rahasia untuk jaman sekarang ini.

## VII. KESIMPULAN

Dari bermacam-macam cipher klasik, Vigenere dan Uesugi adalah cipher yang memiliki tingkat keamanan tinggi. Hal ini dikarenakan jumlah kemungkinan

jawaban yang cukup besar sehingga akan membutuhkan waktu dalam membuat kunci pemecahan.

Pada jaman modern ini, sarana komunikasi sudah sangat berkembang sehingga tidak diperlukan lagi kriptografi klasik. Namun konsep dari kriptografi klasik tetap dipakai sampai saat ini untuk membuat cipher yang lebih efektif dan lebih aman.

## REFERENCES


[1] Munir, Rinaldi. Kriptografi, Penerbit Informatika, 2006.

[2] http://en.wikipedia.org/wiki/Japanese_cryptology_from_the_1500s_to_Meiji


## 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, 21 Maret 2012

ttd

Ryan Setiadi(13506094)