PENERAPAN KRIPTOGRAFI CAESAR PADA PENGIRIMAN DAN PENERIMAAN PESAN

Dedy Setiawan

kakashi_setiawan@yahoo.com

Abstrak: Sandi Caesar merupakan sistem persandian klasik berbasis subtitusi. Enkripsi dan Dekripsi pada sistem persandian Caesar menggunakan operasi shift. Operasi shift merupakan operasi yang mensubtitusi suatu huruf menjadi huruf pada daftar alfabet yang berada di - *k* sebelah kanan atau sebelah kiri huruf tersebut.

Kata Kunci: Algoritma, Caesar, Pesan, Enkripsi, Dekripsi, Keamanan.

BAB I

PENDAHULUAN

Bila suatu saat anda ingin berkomunikasi atau berinteraksi melalui media atau alat komunikasi dengan orang lain, maka anda ingin pesan atau informasi yang anda kirimkan tersebut sampai ke pihak yang dituju dengan aman. Ini adalah masalah keamanan pesan yang dinamakan kerahasiaan (*Confidentiality*). Aman berarti anda menginginkan pesan yang dikirimkan sampai ke tujuan dengan lengkap, artinya isi dari pesan yang anda kirim tidak berubah atau diubah oleh lawan atau pihak yang tidak berkepentingan (*Data Integrity*). Aman bisa juga berarti penerima harus yakin bahwa pesan yang disampaikan kepadanya adalah pesan yang anda kirimkan, bukan dari orang lain yang berperan seperti anda dan anda yakin bahwa pesan yang anda kirimkan juga sampai ke penerima pesan yang berhak menerima pesan tersebut (*Authentication*). Jika suatu saat anda sebagai penerima pesan, maka anda tentu tidak menginginkan pengirim pesan membantah telah mengirimkan pesan kepada anda (*Repudiation*). Padahal anda yakin bahwa anda menerima pesan dari orang tersebut, namun jika pengirim membantah atau menyangkal telah mengirimkan pesan tersebut kepada anda, maka anda perlu membuktikan ketidakbenaran dari penyangkalan tersebut (*Non Repudiation*).

Beberapa dari masalah keamanan yang telah disebutkan diatas dapat terjadi pada kita semua tanpa terkecuali terutama di zaman yang modern seperti pada saat ini, dimana dalam kegiatan sehari-hari juga sudah banyak dari masyarakat melakukan pengiriman pesan. Hal ini sangat rentan terhadap aksi perentasan (*hacking)* untuk mencari informasi penting yang kita gunakan. Informasi atau pesan yang mudah terbaca sangat berbahaya jika orang yang tidak berhak mengetahuinya. Sebagai contoh jika informasi yang berisi data-data pekerjaan kita diketahui, maka orang lain dapat menyalahgunakan informasi atau data-data tersebut ataupun yang lebih berbahaya adalah terjadinya aksi pembajakan hasil karya kita. Masalah tersebut dapat diselesaikan dengan kriptologi. Dalam hal ini kriptologi yang paling mudah dipahami oleh orang awam adalah kriptografi substitusi dengan algoritma Caesar Cipher.

Teknik Penelitian

Didalam kegiatan penelitian ini, penulis melakukan pengumpulan data dengan cara:

1. Pengamatan (*Observation*)

   Penulis melakukan pengamatan langsung terhadap kegiatan yang berhubungan dengan pengiriman dan penerimaan pesan. Sehingga hasil dari kegiatan observasi tersebut diharapkan dapat mengetahui beberapa kekurangan dari pengiriman dan penerimaan pesan.

2. Studi Pustaka

   Penulis melakukan studi pustaka melalui beberapa literatur dan referensi yang berkaitan dengan pengiriman dan penerimaan pesan.

Variabel Penelitian

Variabel Tergantung *(Dependent Variabel)*

Pengiriman dan penerimaan pesan yang tepat sasaran.

Variabel Bebas *(Independent Variabel)*

Penggunaan sandi caesar.

Variabel Moderator

Penyandian informasi.

ANALISIS SWOT

Analisis SWOT adalah sebuah metode prosedur analisis kondisi yang mengklarifikasi kondisi suatu objek dalam empat kategori yaitu Kekuatan (*Strength),* Kelemahan (*Weekness*), Faktor Pendukung (*Opportunity*) dan Faktor Penghambat/Ancaman (*Threat*).

***Strength* (Kekuatan):**

1. Pesan yang sudah tersandi berupa pesan yang tidak mudah untuk diartikan maksudnya,
2. Kriptologi caesar merupakan yang paling mudah dipahami oleh orang banyak.

***Weakness* (Kelemahan):**

1. Sandi (pesan yang sudah dienkripsi) tersebut dapat dipecahkan (diketahui maksud isi dari pesan tersebut) dengan menggunakan *brute force attack,* yaitu dengan mencoba ke-26 kemungkinan geseran yang digunakan,
2. Sandi tersebut dipecahkan dengan cara analisis statistik *chipertext*.

***Opportunity* (Faktor Pendukung) :**

1. Penggunaan banyak karakter dalam proses enkripsi.

***Threat* (Faktor Penghambat/Ancaman) :**

1. Penggunaan *brute force attack*,
2. Diketahuinya kunci.

BAB II

HASIL DAN PEMBAHASAN

Algoritma Caesar

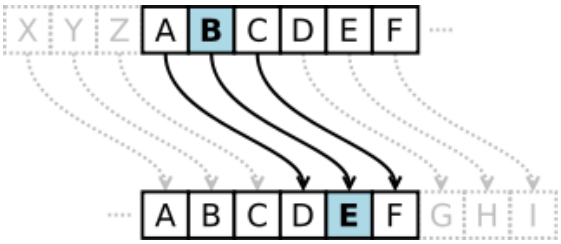
Substitusi kode yang pertama kali digunakan dalam dunia penyandian dikenal dengan kode Caesar, karena penyandian ini terjadi pada saat pemerintahan salah satu raja romawi kuno bernama Julius Caesar. Caranya dengan mengganti posisi huruf awal dengan alphabet atau disebut dengan algoritma ROT3. Caesar Cipher merupakan salah satu algoritma cipher tertua dalam kriptografi dan paling diketahui dalam perkembangan ilmu kriptografi. Caesar cipher merupakan salah satu dari jenis cipher substitusi yang membentuk cipher dengan cara melakukan penukaran karakter pada plainteks menjadi tepat satu karakter pada *ciphertext*. Teknik seperti ini disebut juga sebagai cipher abjad tunggal. Algoritma kriptografi Caesar Cipher sangat mudah untuk digunakan. Inti dari algoritma kriptografi ini adalah melakukan pergeseran terhadap semua karakter pada *plaintext* dengan nilai pergeseran yang sama

Cara Kerja Sandi Caesar

Cara kerja sandi ini dapat diilustrasikan dengan membariskan dua set alfabet. Alfabet sandi disusun dengan cara menggeser alfabet biasa ke kanan atau ke kiri dengan angka tertentu (angka ini disebut kunci/*key*). Misalnya sandi Caesar dengan kunci 3, adalah sebagai berikut:

Alfabet Biasa:
ABCDEFGHIJKLMNOPQRSTUVWXYZ

Alfabet Sandi:
DEFGHIJKLMNOPQRSTUVWXYZABC



Gambar 2.1 Kerja kriptografi caesar

Untuk menyandikan sebuah pesan atau informasi, pengirim cukup mencari setiap huruf yang hendak disandikan di alfabet biasa, lalu tuliskan huruf yang sesuai pada alfabet sandi. Untuk memecahkan sandi tersebut gunakan cara sebaliknya. Contoh penyandian sebuah pesan adalah sebagai berikut:

Teks terang: kirim pasukan ke sayap kiri

Teks tersandi: NLULP SDVXNDQ NH VDBDS NLUL

Proses penyandian (enkripsi) dapat dilakukan secara matematis dengan menggunakan operasi modulus lalu dengan mengubah huruf-huruf tersebut menjadi angka, A = 0, B = 1,..., Z = 25. Sandi (E_n) dari "huruf" x dengan menggeseran *n* secara matematis dituliskan dengan,

$$E_n(x) = (x + n) \mod 26.$$

Sedangkan pada proses pemecahan kode (dekripsi), hasil dekripsi (D_n) adalah

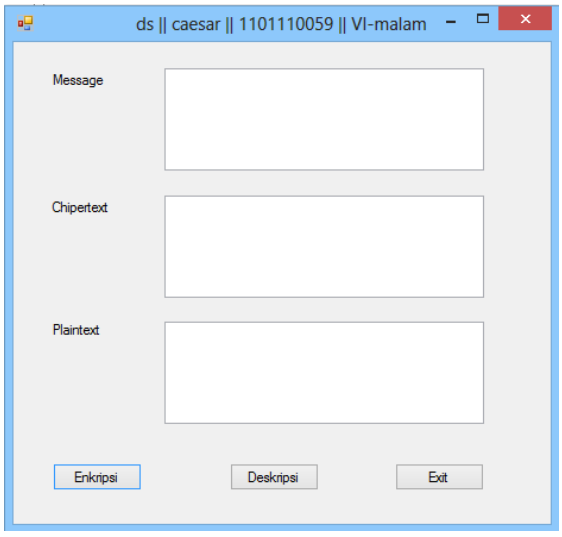
$$D_n(x) = (x - n) \mod 26.$$

Setiap huruf yang sama digantikan oleh huruf yang sama disepanjang pesan, sehingga sandi Caesar digolongkan sebagai *substitusi monoalfabetik* yang berbanding terbalik dengan *substitusi polialfabetik.*

Analisis

1. Pesan yang digunakan dapat berupa data *alphanumeric*, *variabel character, float, numeric*, dll.
2. Pesan yang dienkripsi bukan lagi pesan yang sama dengan pesan yang diisikan sehingga pesan yang dimiliki oleh pengirim hanya diketahui oleh pengirim dan penerima itu sendiri, sehingga untuk kerahasiaannya lebih terjamin.

Berikut ini merupakan tampilan dari aplikasi pengenkripsian dan pendekripsian pesan:



Gambar 2.2 Tampilan aplikasi kriptografi caesar.

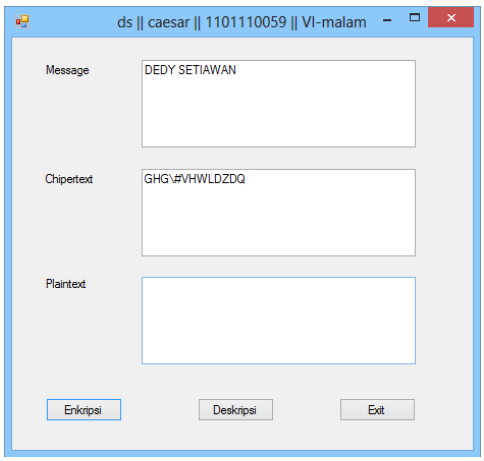
Source Code

```
Public Class Form1
    Private Sub Button1_Click(sender As Object,
e As EventArgs) Handles Button1.Click
        Dim x As String = ""
        Dim xkalimat As String = ""
        For i = 1 To Len(TextBox3.Text)
            x = Mid(TextBox3.Text, i, 1)
            x = Chr(Asc(x) + 3)
            xkalimat = xkalimat + x
        Next
        TextBox1.Text = xkalimat
    End Sub
    Private Sub Button2_Click(sender As Object,
e As EventArgs) Handles Button2.Click
        Dim x As String = ""
        Dim xkalimat As String = ""
        For i = 1 To Len(TextBox3.Text)
            x = Mid(TextBox3.Text, i, 1)
            x = Chr(Asc(x) - 3)
          xkalimat = xkalimat + x
        Next
        TextBox2.Text = xkalimat
    End Sub
    Private Sub Button3_Click(sender As Object,
e As EventArgs) Handles Button3.Click
        Dim tanya As String
        tanya = MsgBox("Anda Yakin Ingin Keluar
?",          MsgBoxStyle.Question          +
MsgBoxStyle.YesNo)
        If tanya = vbYes Then
            Me.Close()
        Else
            Exit Sub
End If
End Sub
End Class
```

Pengujian Aplikasi

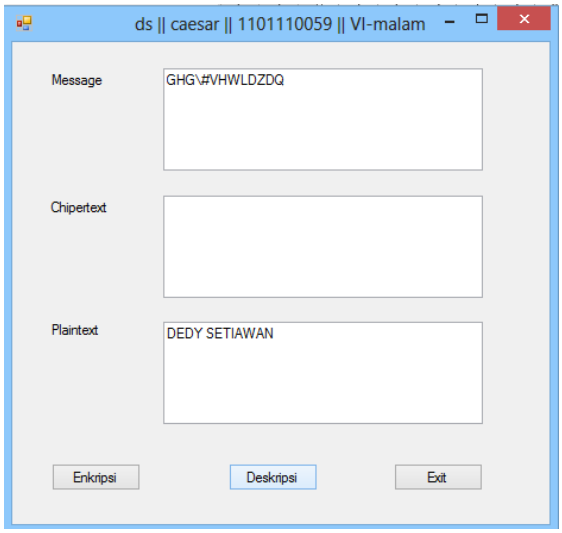
Pengujian aplikasi ini dilakukan untuk menguji nilai keakuratan dari program dalam implementasinya. Pengujiannya dilakukan dengan cara pengguna memasukan pesan yang akan disandikan maupun yang akan diterjemahkan. Kemudian pesan yang akan diisikan, diubah oleh aplikasi menjadi sandi atau sandi yang diterjemahkan.

Pengujian Penyandian Pesan



Gambar 2.3 Tampilan aplikasi kriptografi caesar saat melakukan penyandian

Pengujian Penerjemahan Pesan



Gambar 2.4 Tampilan aplikasi kriptografi caesar saat melakukan penerjemahan sandi

BAB III

KESIMPULAN DAN SARAN

Berdasarkan hasil dari pengujian aplikasi dan pembahasan dari materi di atas, maka kesimpulan yang didapatkan adalah sebagai berikut:

Semakin besar ukuran kunci, semakin lama waktu yang dibutuhkan untuk melakukan pencarian terhadap kunci.

Algoritma kriptografi klasik caesar dapat digunakan atau diterapkan untuk penyandian maupun penerjemahan sandi informasi dari pengirim ke penerima.

Perlunya dilakukan bermacam-macam variasi dalam proses penyandian agar tidak mudah untuk didekripsikan.

BAB IV

DAFTAR PUSTAKA

http://id.wikipedia.org/wiki/Sandi_Caesar (diakses 29 juni 2014 jam 7.03 wib)

http://www.academia.edu/4695705/Caesar_chiper (diakses 29 Juni 2014 jam 7.19 wib)

Sadikin,rifki (2012).kriptografi untuk keamanan jaringan. Yogyakarta: Penerbit ANDI.