KRIPTOGRAFI KLASIK TEKNIK SUBSITUSI UNTUK KEAMANAN DATA MENGGUNAKAN VB.Net 2008

Sri Andayani[1], Dionysius Spironabel Agista[2]
Jurusan Teknik Informatika Sekolah Tinggi Teknik Musi
Jl. Bangau no. 60 Palembang 30113
E-mail: andayani_s@sttmusi.ac.id[1], dionysius.agista@gmail.com[2]

Abstrak
Kriptografi sudah dikenal sejak berabad yang lalu. Kriptografi sejak dulu sampai sekarang digunakan untuk keamanan data. Kriptografi sendiri terdapat dua macam yaitu kriptografi klasik dan kriptografi modern. Penelitian ini bertujuan membangun aplikasi yang menerapkan kriptografi klasik dengan teknik substitusi. Beberapa algoritma pada teknik substitusi di antaranya adalah: *caesar chiper, affine chiper, monoalphabetic chiper* dan *vigenere chiper*. Kriptografi klasik mempunyai beberapa kelebihan yaitu: berbasis karakter, dapat menggunakan pena dan kertas dan termasuk dalam kriptografi kunci simetris, sedangkan alasan menggunakan kriptografi klasik yang telah lama tidak digunakan lagi adalah: dapat digunakan untuk mempelajari konsep dasar kriptografi, kriptografi klasik menjadi konsep dasar kriptografi modern dan dapat digunakan untuk memahami kelemahan sistem kode. Sebuah algoritma disebut *chiper* yang merupakan persamaan matematika yang digunakan untuk proses enkripsi dan deskripsi. Proses enkripsi adalah mengubah pesan asli dengan menggunakan sebuah kunci menjadi pesan yang tersembunyi atau tidak dikenali sedangkan proses deskripsi adalah proses mengubah kembali pesan yang tidak dikenali kembali pesan asli dengan menggunakan kunci yang sama. Algoritma-algoritma kriptografi klasik dibangun dengan menggunakan bahasa pemrograman visual basic.net 2008 dengan alasan tampilan visual lebih menarik dan penulisan source code lebih mudah dipahami.
Kata kunci: kriptografi klasik, enkripsi, deskripsi

Substituting Classical Cryptography Techniques For Data Security Using Vb.Net 2008

Abstract
Cryptography has been known since centuries ago. Cryptography since the beginning until now used for data security. Cryptography itself there are two kinds of classical cryptography and modern cryptography. This study aims to build applications that apply the classic cryptography with substitution technique. Some algorithms on substitution techniques include: caesar cipher, affine cipher, ciphers and vigenere monoalphabetic cipher. Classical cryptography has several advantages, namely: character-based, can use a pen and paper and included in the symmetric key cryptography, while using the excuse of classical cryptography which has long been used again is: it can be used to learn the basic concepts of cryptography, classical cryptography into the basic concepts of modern cryptography and can be used to understand the weaknesses of the system code. An algorithm called cipher which is a mathematical equation that is used to process the encryption and description. Encryption is the process of changing the original message using a key into a hidden message or not dikenalin while the description is the process of turning back the message that not dikenalin return the original message using the same key. Classical cryptographic algorithms built using a visual programming language in 2008 with the reasons basic.net more attractive visual appearance and writing source code easier to understand.
Kata Kunci: *classical cryptography, encryption, description*

1. PENDAHULUAN

1.1 Latar Belakang

Kriptografi merupakan ilmu dan seni untuk menjaga pesan agar aman. Kripto berasal dari kata *Crypto* yang artinya rahasia dan *graphy* berarti tulisan sehingga kriptografi dapat diartikan tulisan yang tersembunyi. Dengan adanya tulisan yang tersembunyi ini maka orang-orang tidak mengetahui bagaimana tulisan tersebut disembunyikan dan tidak tahu bagaimana cara membaca maupun menterjemahkan tulisan tersebut [2].

Di era sekarang ini, kriptografi menjadi hal penting bagi keamanan komputer dan jaringan untuk menjamin keamanan data dan informasi. Data dan informasi yang dikirimkan menggunakan jaringan harus diamankan ancaman-ancaman keamanan yaitu: interupsi merupakan ancaman terhadap ketersediaan informasi dan data pada sistem, intersepsi merupakan ancaman terhadap kerahasiaan informasi dan data, modifikasi merupakan ancaman terhadap informasi dan data yang dimodifikasi dan fabrikasi merupakan ancaman terhadap informasi dan data yang ditiru dan dipalsukan. [1]

Di era sekarang ini, kriptografi menjadi hal penting bagi keamanan komputer dan jaringan untuk menjamin keamanan data dan informasi. Data dan informasi yang dikirimkan menggunakan jaringan harus diamankan ancaman-ancaman keamanan yaitu: interupsi merupakan ancaman terhadap ketersediaan informasi dan data pada sistem, intersepsi merupakan ancaman terhadap

kerahasiaan informasi dan data, modifikasi merupakan ancaman terhadap informasi dan data yang dimodifikasi dan fabrikasi merupakan ancaman terhadap informasi dan data yang ditiru dan dipalsukan. [1]

Informasi dan data pada komputer dan jaringan harus dijaga kerahasiaanya dengan memerhatikan beberapa aspek keamanan yaitu: 1. *Authentication*, informasi benar datang dari orang yang dikehendaki, 2. *Integrity*, keaslian pesan yang dikirim terjamin, 3. *Non-repudiation*, pengirim tidak dapat mengelak bahwa dialah yang mengirim informasi tersebut, 4. *Authority*, informasi tidak dapat dimodifikasi oleh orang yang tidak berhak, 5. *Confidentiality*, menjamin kerahasiaan, 6. *Privacy*, menjamin kerahasiaan data pribadi, 7. Availability, menjamin ketersediaan informasi yang dibutuhkan, 8. *Access Control* mengatur akses ke pengaturan informasi.

Untuk melaksanakan aspek keamanan tersebut maka digunakan algoritma kriptografi yang terdiri atas beberapa komponen yaitu: 1. Enkripsi, mengubah plaintext (teks asli) menjadi kode-kode yang tidak dimengerti, 2. Deskripsi, proses mengembalikan plaintext ke bentuk semula, 3. Kunci, kunci yang dipakai untuk proses enkripsi dan dekripsi (kunci rahasia/private key dan kunci umum/public key), 4. *Chiptertext*, suatu pesan yang telah melalui proses enkripsi, 5. *Plaintext*, teks asli sebelum dilakukan proses enkripsi, 6. Pesan, berupa data atau informais yang dikirim, 7. Cryptanalysis, analisis kode atau suatu ilmu untuk mendapatkan teks asli tanpa harus mengetahui kunci yang sah.

Algoritma kriptografi yang dikenal ada dua macam yaitu kriptografi klasik dan kriptografi modern. Kriptografi klasik sudah lama tidak dipergunakan karena berbasis karakter, hanya menggunakan pena dan kertas bisa dilakukan dan termasuk ke dalam kriptografi kunci simetris. Namun beberapa alasan perlu mempelajari kripografi klasik diantaranya adalah memberikan pemahaman konsep dasar kriptografi, dasar algoritma kriptografi modern dan memahami potensi kelemahan sistem kode. Di samping itu, kelemahan algoritma kriptografi klasik adalah kurangnya tingkat keamanan data tetapi karena metoda ini mudah implementasinya dan tidak perlu diuji secara mendalam maka algoritma ini masih sering digunakan. Contoh penggunaan algoritma ini untuk menggantikan enkripsi yang menggantikan huruf yang digunakan untuk mengirim pesan dengan huruf lain. [3]

Skema algoritma sandi akan disebut kunci-simetris apabila untuk setiap proses enkripsi maupun dekripsi data secara keseluruhan digunakan kunci yang sama. Skema ini berdasarkan jumlah data per proses dan alur pengolahan data didalamnya dibedakan menjadi dua kelas, yaitu *block-cipher* dan *stream-cipher*. *Stream-cipher* adalah algoritma sandi yang mengenkripsi data persatuan data, seperti bit, *byte, nible* atau per lima bit (saat data yang di enkripsi berupa data Boudout). Setiap mengenkripsi satu satuan data digunakan kunci yang merupakan hasil pembangkitan dari kunci sebelum.

Kriptografi klasik yang digunakan pada penelitian ini adalah lima teknik substitusi yang diimplementasikan dengan menggunakan bahasa pemrograman VB.Net 2008 dengan alasan karena pemrograman visual sehingga tampilan menjadi lebih menarik untuk dipelajari. Kelima teknik subsitusi tersebut adalah caesar chiper, affine cipher, mono alphabetic chiper, vigenere cipher dan beaufort cipher.

1.2 Tujuan Penelitian

Tujuan penelitian ini adalah membangun aplikasi kriptografi klasik menggunakan teknik substitusi.

1.3 Peneliti-peneliti Terdahulu

Studi literatur tersebut digunakan sebagai referensi dalam mengembangkan penelitian. Berikut referensi penelitian yang digunakan adalah:

Penelitian dengan judul "Pengamanan Data Informasi Menggunakan Kriptografik Klasik" berhasil mengimplementasikan kriptografi klasik menggunakan bahasa pemrograman C. Kriptografi klasik yang dipergunakan meliputi substitusi chiper dan transposisi chiper. [5]

Penelitian selanjutnya mengenai kriptografi klasik dengan judul "Implementasi Kriptografi Klasik Menggunakan Borland Delphi" berhasil juga diimplementasikan sehingga dapat lebih mengenal tentang konsep, dasar-dasar dan implementasi kriptografi sehingga ke depan akan lebih mudah memahami implementasi kriptografi modern.[2]

Penelitian mengenai kriptografi klasik juga dilakukan pada penelitian dengan judul "Penyandian Citra Menggunakan Metode Playfair Chiper". Penelitian ini diimplementasikan untuk menyandikan citra dengan format bmp 24 bit yang mempunyai ukuran 256x256 pixel. Citra yang akan diujikan terdiri dari 2 jenis citra yaitu citra dengan tingkat kontras yang berbeda serta citra dengan kategori tingkatan detail yang berbeda. Kunci yang digunakan untuk menyandikan citra menggunakan 2 jenis matrik yang mempunyai ordo 16x16. Hasil penelitian ini bahwa algoritma playfair dapat diterapkan untuk citra kualitas yang baik dan pada citra dengan kategori citra detail. [6]

Selanjutnya penelitian kriptografi klasik dengan judul "Implementasi Algoritma Hill Chiper dalam Penyandian Data". Hasil penelitian bahwa algoritma Hill Chiper sebagai bagian kriptografi klasik dapat diterapkan untuk penyandian data. [3]

Penelitian mengenai kriptografi dapat dikombinasi antara satu algoritma dengan algoritma lain dengan judul "Steganografi Menggunakan Metode Least Significant Bit Dengan Kombinasi Algoritma Kriptografi Vinegere dan RC4". Penelitian ini bertujuan memberikan proteksi ganda pada pesan rahasia di dalam sebuah gambar/citra digital. Penelitian ini membuat aplikasi yang diberi nama StegoKripto yang mengkombinasikan kriptografi dan steganografi. [4]

1.4 Landasan Teori

Caesar Chiper

Rumusan pada caesar chiper untuk enkripsi adalah:

$$C = E(p) = (P+K) \bmod (26) \quad (1)$$

Sedangkan untuk deskripsi adalah:

P = D(C) = (C-K) mode (26) (2)

Contoh:
Plaintext: AKU BELUM MAKAN
Kunci: 3
Chipertext: EOY FIPYQ QEOER

Affine Chiper

Rumusan pada affine chiper untuk enkripsi adalah:

C = (P x K1 + K2) mod 26 (3)

Sedangkan rumusan untuk deskripsi adalah:

P = x * (C – K2) mod 26 (4)

Untuk x = (K1 * bilangan prima) mod 26 (5)
Contoh:
Plaintext: AKU MAU MAKAN
Kunci 1: 6
Kunci 2: 23
Chipertext: XFN RXN RXFXX

Monoalphabetic Chiper

Dalam perkembangannya, kriptografi klasik tidak hanya memilki kunci dalam bentuk angka saja tetapi juga menggunakan string. Kunci dapat berupa nama, alamat atau apa saja yang diinginkan oleh pengirim pesan. Penggunaan string sebagai kunci dalam algortima subtitusi disebut dengan *monoalphabetic chiper*. Pada metode ini string kunci menjadi huruf- huruf awal subtitusi dari *plaintext*. Setiap huruf dalam kunci hanya diperkenankan muncul sekali [2].
Berikut contoh penggunaan *monoalphabetic chiper*:
Kunci: TERNYATATIDDAKDATANG
Ekstrak kunci: TERNYAIDKG
Indeks Kunci:
TERNYAIDKGBCDFHJLMNOPQSUVWXYZ

Vigenere Chiper

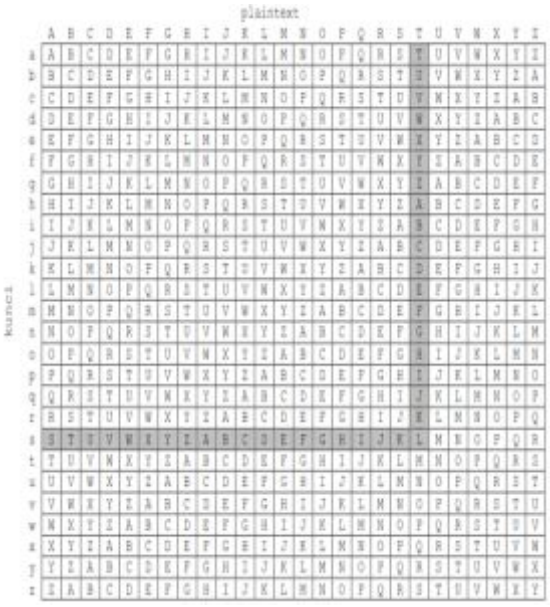
Pada kriptografi klasik ini menggunakan tabula recta pada Gambar 1 dengan rumusan:

C = (P + K) mod 26 (6)

Sedangkan untuk deskripsi adalah:

P = (C – K) mod 26 (7)

Contoh:
Plaintext: AKU AKAN PERGI KE TEMPAT PERTEMUAN
Kunci: RAHASIA
Indeks Kunci: RAH ASIA RAHAS IA RAHASI ARAHASIAR
Chipertext: RKB ACIN GEYGA SE KETPSB PVRAEECAE



Gambar 1. Tabula Recta

2. METODOLOGI PENELITIAN

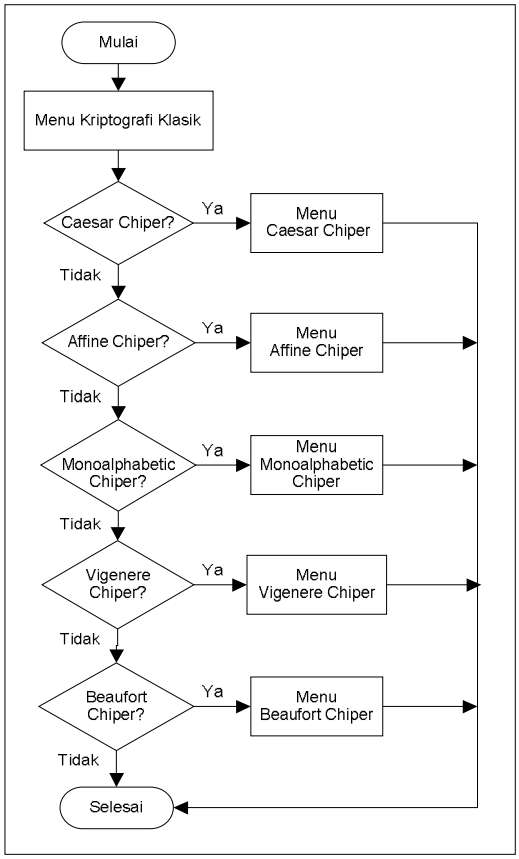
Adapun metodologi penelitian:

1. Pengumpulan Data
   Studi pustaka dengan mempelajari mengenai kriptografi klasik terutama teknik substitusi dan studi literatur dengan mempelajari jurnal publikasi yang membahas mengenai algoritma kriptografi klasik.
2. Perancangan sistem
   Melakukan perancangan sistem untuk kriptografi klasik teknik substitusi dengan menggunakan diagram alir (flowchart). Teknik substitusi yang digunakan adalah: Caesar Chiper, Affine Chiper, Monoalphabetic Chiper, Vigenere Chiper. Flowchart menggambarkan aliran data proses pemilihan kunci, enkripsi dan deskripsi data.
3. Implementasi Sistem
   Setelah menganalisis dan merancang sistem maka diimplementasikan dengan menggunakan bahasa pemrograman Microsoft Visual Basic.Net 2008.
4. Pengujian Sistem
   Menggunakan teknik pengujian whitebox terhadap *source code* pada tiap algoritma kriptografi klasik teknik substitusi.

3. HASIL DAN PEMBAHASAN

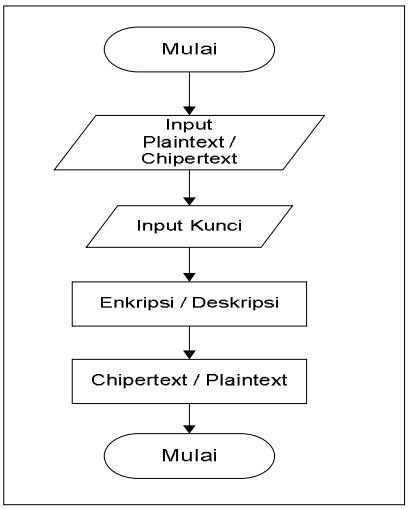
3.1 Diagram Alir Sistem

Gambar 2 memperlihatkan flowchat menu kriptografi klasik dimana disajikan menu-menu teknik substitusi sehingga user dapat memilih teknik apa yang diinginkan.



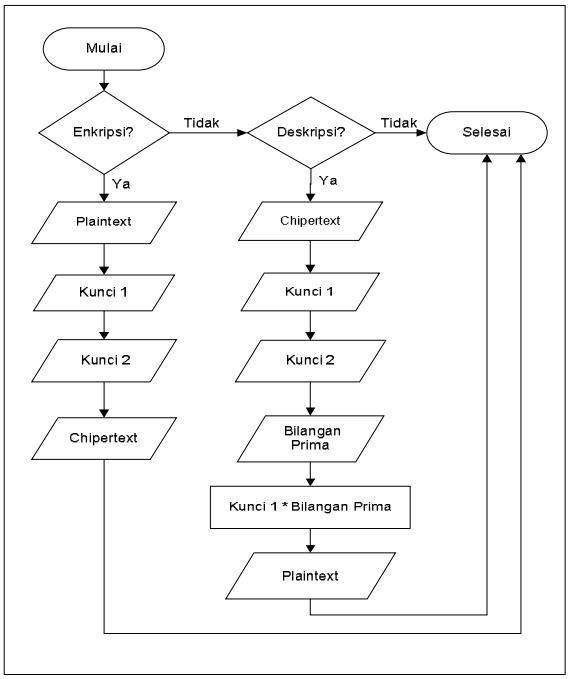
Gambar 2. Flowchart Menu Utama Kriptografi Klasik

Selanjutnya masuk ke dalam menu Caesar Chiper yang diperlihatkan pada Gambar 3. Pada proses ini, diawali dengan memasukkan plaintext, masukkan kunci lalu proses enkripsi. Untuk proses deskripsi diawali dengan memasukkan chipertext, memasukkan kunci dan hasil berupa plaintext.



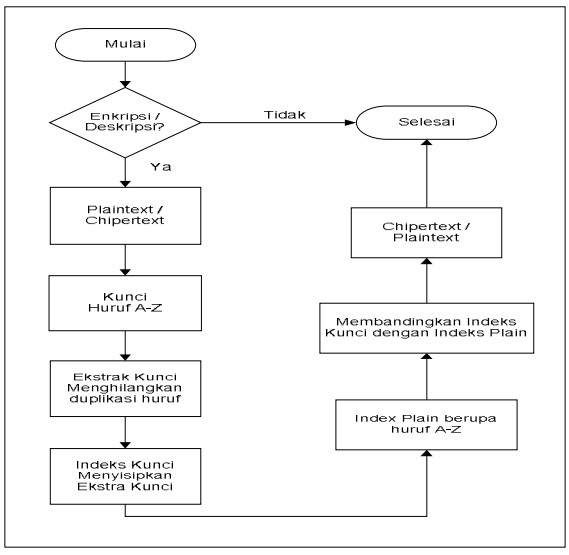
Gambar 3. Flowchart Kriptografi Klasik Caesar Chiper

Proses Affine Chiper dapat dilihat pada Gambar 4. Di mana pada teknik menggunakan dua kunci. Pada teknik ini juga berbeda antara proses enkripsi dan deskripsi di mana pada proses deskripsi ditambahkan memasukkan bilangan prima yang akan dikalikan dengan kunci 1.



Gambar 4. Flowchart Kriptografi Klasik Affine Chiper

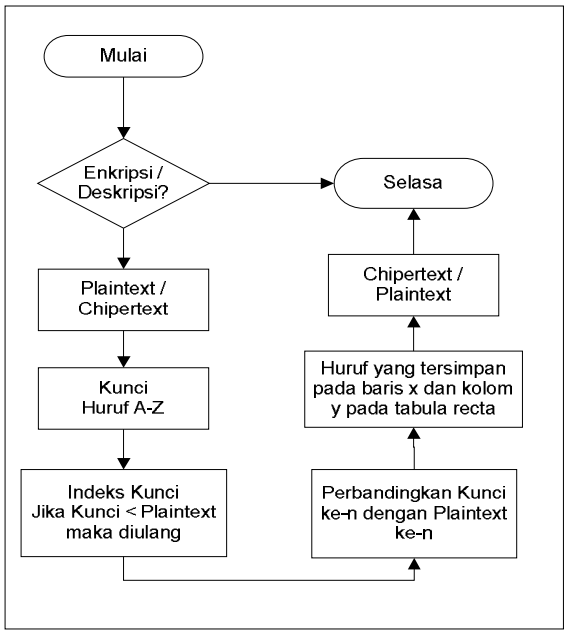
Selanjutnya proses algoritma kriptografi klasik monoalphabetic chiper dapat dilihat pada Gambar 5. Pada teknik ini dimasukkan plaintext, kunci yang terdiri dari huruf A sampai dengan Z, kemudian kunci akan diektrak dengan hanya menghitung satu kali huruf yang muncul berulang, kemudian kunci akan disisipkan ke deretan huruf A sampai dengan Z yang akan menghilangkan huruf yang sama dengan sama dengan kunci. Deretan huruf ini disebut dengan index kunci. Selanjutnya index kunci akan dibandingkan dengan index plain yang terdiri dari huruf A sampai dengan Z.



Gambar 5. Flowchart Kriptografi Klasik Monoalphabetic Chiper

Kriptografi klasik Vigenere menggunakan tabula recta seperti pada Gambar 6. Tabula recta digunakan untuk memperoleh teks kode dengan menggunakan kunci yang sudah ditentukan. Jika panjang kunci lebih pendek

daripada panjang teks asli (plaintext) maka penggunaan kunci diulang. Cara menentukan teks kode pada sistem, pada tabula recta dibuat posisi horizontal berupa plaintext dan vertikal untuk kunci terlihat pada Gambar 1.



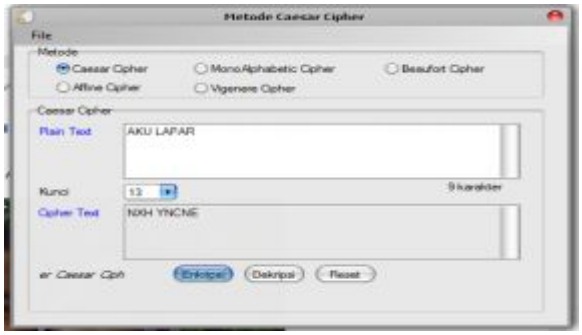
Gambar 6. Flowchart Kriptografi Klasik Vigenere

3.2 Implementasi Sistem

Caesar Chiper

Implementasi kriptografi klasik caesar chiper dapat dilihat pada source code di bawah ini:

```
Dim a As Integer
Cipher_Caesar.Text = vbNullString
For i = 1 To Len(Plain_Caesar.Text)
      a= Asc(Mid$(Plain_Caesar.Text.ToUpper, i, 1))
  Select Case a
  Case Is >=
  a = (a - 65 + Key_Caesar.SelectedIndex) Mod 26 + 65
  End Select
```

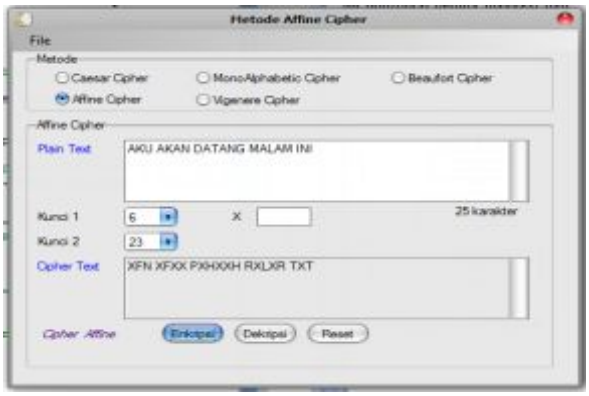


Gambar 8. Interface Kriptografi Klasik Caesar Chiper

Affine Chiper

Implementasi kriptografi klasik affine chiper dapat dilihat di bawah ini:

```
Dim a As Integer
Cipher_Affine.Text = vbNullString
For i As Integer = 1 To Len(Plain_Affine.Text)
   a= Asc(Mid$(Plain_Affine.Text.ToUpper, i, 1))
   Select Case a
      Case Is >= 65
       a = (((a - 65) * Key_Affine.SelectedIndex + Key2_Affine.SelectedIndex) Mod 26) + 65
   End Select
```



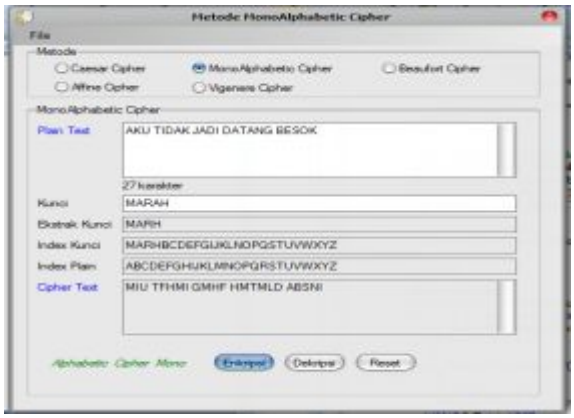
Gambar 9. Interface Kriptografi Klasik Affine Chiper

Monoalphabetic Chiper

Implementasi enkripsi kriptografi klasik monoalphabetic chiper dapat dilihat di bawah ini:

```
'fungsi ekstraksi kunci
    Dim huruf As String = Key_Mono.Text
    Dim hapus As String = vbNullString
    Dim a As Integer
    Ekstrak_Mono.Text = vbNullString
    For i As Integer = 1 To Len(Key_Mono.Text)
      a = Asc(Mid$(Key_Mono.Text, i, 1))
      If InStr(1, huruf, Chr(a)) > 0 Then
        hapus &= Chr(a)
        huruf = Replace(huruf, Chr(a), vbNullString)
        Ekstrak_Mono.Text = hapus
      End If
    Next
  'fungsi untuk menambah karakter
    Index_Mono.Text = vbNullString
    Dim tambah As String = vbNullString
    For i As Integer = Asc("A") To Asc("Z")
      IF InStr(1, Key_Mono.Text, Chr(i)) = 0 Then '
     tambah &= Chr(i)
       Index_Mono.Text = Ekstrak_Mono.Text & tambah
      End If
    Next
    Dim b As Integer
    Cipher_Mono.Text = vbNullString
    For i = 1 To Len(Plain_Mono.Text)
      b = Asc(Mid$(Plain_Mono.Text, i, 1))
      If b >= 65 Then
        b = (Index_Plain_Mono.Text.IndexOf(Index_Mono.Text(b - 65)) + 65)
        'B di enkripsi menjadi A
        Cipher_Mono.Text &= Chr(b)
      ElseIf b = 32 Then
        Cipher_Mono.Text &= " "
      ElseIf b = 10 And 32 Then
        Cipher_Mono.Text &= vbNewLine
```

```
        End If
    Next
```



Gambar 9. Interface Kriptografi Klasik Monoalphabetic Chiper

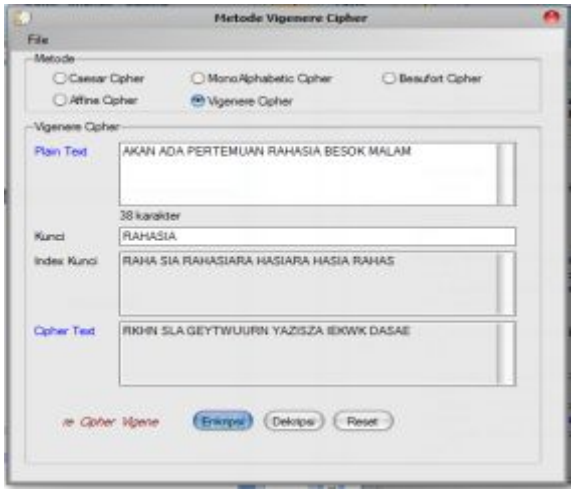
Vigenere Chiper

Implementasi enkripsi kriptografi klasik vigenere chiper dapat dilihat di bawah ini:

```
Dim a, b, c, index As Integer
        index = 0
        Index_Vigenere.Text = vbNullString
        Cipher_Vigenere.Text = vbNullString

 'fungsi membuat kunci sepanjang plaintext
 For i = 1 To Len(Plain_Vigenere.Text)
If index = Len(Key_Vigenere.Text) Then
            index = 1
    Else
            index += 1
 End If
     a = Asc(Mid$(Plain_Vigenere.Text, i, 1))
     b = Asc(Mid$(Key_Vigenere.Text, index, 1))

 'fungsi enkripsi ; C = (P + K) mod 26
     c = ((a + b) Mod 26) + 65
If a >= 65 Then
     Index_Vigenere.Text &= Chr(b)
     Cipher_Vigenere.Text &= Chr(c)
         ElseIf a = 32 Then
            index -= 1
            Cipher_Vigenere.Text &= " "
            Index_Vigenere.Text &= " "
         ElseIf a = 10 And 13 Then
            index += 1
            Cipher_Vigenere.Text &= vbNewLine
            Index_Vigenere.Text &= vbNewLine
         End If
      Next
```



Gambar 11. Interface Kriptografi Klasik Vigenere Chiper

4. SIMPULAN

Berdasarkan hasil penelitian dan pembahasan serta rumusan masalah dan hipotesis yang diajukan dalam penelitian dapat diambil kesimpulan yaitu: kriptografi klasik teknik substitusi diantaranya adalah: caesar chiper, affine chiper, monoalphabetic chiper dan vigenere chiper berhasil dibangun dengan menggunakan bahasa pemrograman VB.Net 2008.

DAFTAR PUSTAKA

[1] Ariyus, Dony., *"Pengantar Ilmu Kriptografi"*, Penerbit Andi, Yogyakarta, 2008.

[2] Fairuzabadi, Muhammad., "Implementasi Kriptografi Klasik Menggunakan Borland Delphi", Jurnal Dinamika Informatika, Vol.2 No.2, Yogyakarta, 2010.

[3] Hasugian, Abdul Halim., "Implementasi Algoritma Hill Chiper dalam Penyandian Data", Pelita Informatika Budi Darma, Vol.IV No.2, ISSN: 2301-9425, 2013

[4] Rakhmat, Basuki dan Fairuzabadi, Muhammad., "Steganografi Menggunakan Metode Least Significant Bit Dengan Kombinasi Algoritma Kriptografi Vinegere dan RC4", Jurnal Dinamika Informatika, Vol. 5, No.2, Yogyakarta, 2010.

[5] Sasongko, Jati., "Pengamanan Data Informasi Menggunakan Kriptogtafi Klasik", Jurnal Teknologi Informasi DINAMIK Vol.X No.3, ISSN: 0854-9524, 2005.

[6] Setyaningsih, Emy., "Penyandian Citra Menggunakan Metode Playfair Chiper", Jurnal Teknologi, Vol.2 No.2, 2005.