PERANCANGAN APLIKASI KRIPTOGRAFI E-MAIL DENGAN METODE COLUMNAR TRANSPOSITION CIPHER

Andre[1], Kristina[2], Sandi Tendean[3]
[1,3]Teknik Informatika, STMIK Widya Dharma, Pontianak
[2]Sistem Informasi, STMIK Widya Dharma, Pontianak
e-mail: [1]andreapheng@yahoo.co.id, [2]vinalim@yahoo.com, [3]sanditendean@gmail.com

Abstract

Columnar Transposition Cipher is one of cryptography technic or message security with simetris key. Message security through this technic do with put each the alphabet to column of the table in horizontal, then column of the table encrypted by the key word have decided before. After that write again each alphabet of the table in vertical for result ciphertext. Columnar Transposition Cipher technic can used for e-mail security contain text. Use this technic will help e-mail user to keep secrecy e-mail contain have saved in mail server, so that hackers can't know e-mail contain have saved in mail server except by people have a right to deseve the e-mail or have the decryption key. E-mail cryptography aplication design do with learn various literature have related with the Columnar Transposition Cipher material. The data collection technic used is study of literature that includes book, scientific journals, essay, and e-book have avaible from any resource. Systems analysis technique used is object-oriented technique and the modeling tool is Unified Modeling Language (UML). The programming language have use to design e-mail cryptography aplication is Microsoft Visual Basic 2010 programming language. The concusion have get trough this research is the Columnar Transposition Cipher technic can used to improve the security for e-mail delivery and to keep e-mail contain security have submit so that user privacy while using e-mail will not disturbed.

Abstrak

Columnar Transposition Cipher adalah salah satu teknik kriptografi atau pegamanan pesan dengan kunci simetris. Pengamanan pesan melalui teknik ini dilakukan dengan cara memasukkan setiap huruf pada kolom sebuah tabel secara horizontal, kemudian kolom tabel tersebut diacak berdasarkan kata kunci yang telah ditentukan. Setelah itu tuliskan kembali setiap huruf dari tabel tersebut secara vertikal untuk menghasilkan ciphertext. Teknik Columnar Transposition Cipher dapat digunakan untuk pengamanan *e-mail* yang berisikan teks. Penggunaan teknik ini akan membantu pengguna *e-mail* dalam menjaga kerahasian isi *e-mail* yang tersimpan pada *mail server*, sehingga peretas tidak dapat mengetahui isi *e-mail* kecuali oleh orang yang berhak menerima *e-mail* tersebut atau memiliki kunci dekripsi. Perancangan aplikasi kripstografi *e-mail* dilakukan dengan mempelajari berbagai literatur- literatur yang berhubungan dengan materi Columnar Transposition Cipher. Teknik pengumpulan data yang digunakan adalah studi literatur yang meliputi buku, jurnal ilmiah, skripsi, serta *e-book* yang didapatkan dari berbagai sumber. Teknik analisis sistem yang digunakan adalah teknik berorientasi objek dan alat pemodelannya adalah Unified Modeling Language (UML). Bahasa pemrograman yang digunakan untuk merancang aplikasi kriptografi *e-mail* adalah bahasa pemrograman Microsoft Visual Basic 2010. Kesimpulan yang diperoleh melalui penelitian ini adalah teknik Columnar Transposition Cipher dapat digunakan untuk meningkatkan keamanan selama pengiriman *e-mail* serta menjaga kerahasiaan isi *e-mail* yang dikirimkan sehingga privasi pengguna saat menggunakan *e-mail* tidak akan terganggu.

***Kata Kunci**: Kriptografi, Enkripsi, Dekripsi, E-Mail, Columnar Transposition Cipher*.

1. PENDAHULUAN

Perkembangan zaman modern saat ini begitu pesat, hal ini tentu saja tidak lepas dari peranan teknologi, yang terus berkembang dan terus maju dari waktu ke waktu. Komputer memiliki peranan yang begitu penting, karena hampir setiap aktivitas dalam masyarakat membutuhkan teknologi komputer. Salah satu aktivitas atau kegiatan yang sering dilakukan dengan memanfaatkan komputer adalah pengiriman data atau pesan.

Komputer memiliki berbagai media atau aplikasi yang dapat digunakan untuk pengiriman data atau pesan seperti aplikasi *chating*, *social media*, *short message service* (SMS), dan *e-mail.* Salah satu media atau aplikasi yang sering digunakan sebagai pengiriman data atau pesan adalah *e-mail*. *E-mail* atau *electronic mail* adalah surat elektronik yang dikirimkan melalui jaringan internet antara pengguna komputer. *E-mail* banyak

digunakan oleh pengguna komputer karena selain proses pengirimannya yang cepat, pengguna juga dapat melampirkan berbagai file dalam pesan yang dikirimkan seperti gambar, video, audio, dokumen atau jenis file lainnya.

Pihak layanan penyedia *e-mail* telah menerapkan suatu sistem keamanan untuk menghadapi berbagai kejahatan komputer melalui *e-mail.* Akan tetapi, meskipun sistem keamanan telah diterapkan pada proses pengiriman *e-mail*, privasi pengguna komputer dalam pengunaan *e-mail* tetap dapat terganggu. Penyebabnya adalah pencurian *e-mail* dari *mail server* masih dapat terjadi sehingga pengguna *e-mail* perlu berhati-hati dalam mengirimkan pesan yang bersifat pribadi atau rahasia melalui *e-mail*. Agar kemanan isi *e-mail* yang tersimpan pada *mail server* tidak terganggu, pengguna *e-mail* dapat menerapkan teknik kriptografi pada setiap proses pengiriman *e-mail*, sehingga peretas tidak dapat mengetahui isi *e-mail* yang dikirimkan kecuali penerima *e-mail* atau orang yang memiliki kunci dekripsi *e-mail* tersebut.

Berdasarkan uraian di atas, maka akan dirancang suatu aplikasi kriptografi *e-mail* dengan menggunakan metode *Columnar Transposition Cipher* sehingga isi *e-mail* yang tersimpan pada *mail server* dapat lebih terjaga, dan keamanan dalam proses pengiriman *e-mail* lebih meningkat sehingga terhindar dari berbagai tindak kejahatan komputer.

2. METODE PENELITIAN

2.1 Rancangan Penelitian, Metode Pengumpulan Data, Teknik Analisis dan Perancangan Sistem, serta Aplikasi Perancangan Sistem

2.1.1 Rancangan Penelitian

Dalam penelitian ini penulis menggunakan desain penelitian dekriptif, yaitu dengan memaparkan/menjelaskan secara jelas dan sistematis mengenai langkah-langkah perancangan aplikasi kriptografi *e-mail* dengan metode *Columnar Transposition Cipher*.

2.1.2 Teknik Pengumpulan Data

Pengumpulan data dilakukan dengan cara melakukan studi kepustakaan yaitu pengumpulan berbagai sumber, literatur, buku, *e-book*, maupun referensi lainnya yang menyangkut pemikiran para ahli yang berkaitan dengan permasalahan yang diangkat oleh penulis.

2.1.3 Teknik Analisis dan Perancangan Sistem

Teknik analisis dan perancangan sistem yang digunakan adalah teknik berorientasi objek, sedangkan alat pemodelan yang digunakan adalah dengan diagram *Unified Modeling Language* (UML).

2.1.4 Aplikasi Perancangan Sistem

Aplikasi yang digunakan dalam merancang aplikasi kriptografi *e-mail* adalah aplikasi bahasa pemrograman Microsoft Visual Basic.NET 2010.

2.2 Landasan Teori

2.2.1 Program Aplikasi

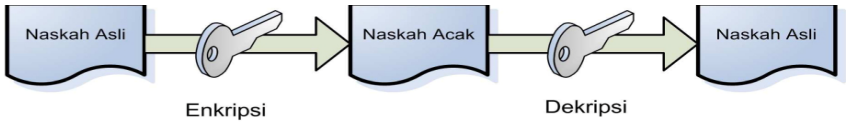
Program aplikasi pada komputer merupakan perangkat lunak siap pakai yang nantinya akan digunakan untuk membantu melaksanakan pekerjaan penggunanya.[1]

2.2.2 Rekayasa Perangkat Lunak

Rekayasa perangkat lunak (RPL atau SE [*Software Engineering*]) adalah suatu bidang profesi yang mendalami cara-cara pengembangan perangkat lunak termasuk pembuatan, pemeliharaan, manajemen organisasi pengembangan perangkat lunak, dan sebagainya.[2]

2.2.3 Kriptografi

Kriptografi adalah seni atau ilmu untuk menyembunyikan isi pesan.[3] Kriptografi adalah ilmu mengenai teknik enkripsi dimana data diacak menggunakan suatu kunci enkripsi menjadi sesuatu yang sulit dibaca oleh seseorang yang tidak memiliki kunci dekripsi.[4]



Gambar 1. Proses Kriptografi

2.2.4 Enkripsi

Proses enkripsi adalah proses pengacakan “naskah asli" (*plaintext*) menjadi “naskah acak" (*ciphertext*) yang “sulit untuk dibaca" oleh seseorang yang tidak mempunyai kunci dekripsi.[4]

2.2.5 Dekripsi

Dekripsi adalah proses mengubah data yang dienkripsi menjadi data yang dapat dibaca.[5]

2.2.6 Columnar Transposition Cipher

Dalam transposisi columnar lengkap setelah plaintext dituliskan pada kolom-kolom tabel yang telah disediakan, apabila terdapat kolom tabel yang kosong maka akan diisi dengan nilai kosong hingga seluruh kolom terisi. Ciphertext kemudian ditarik dari kolom-kolom secara vertikal menurut urutan kata kunci [6] Kata kunci

yang telah diberikan akan menjadi nama kolom pada tabel dan diurutkan secara alfabetik. Kemudian lakukan pembagian antara jumlah huruf dalam *cipher* dengan jumlah huruf kata kunci untuk mendapatkan jumlah baris dalam tabel. Masukkan setiap huruf dalam *cipher* ke dalam setiap kolom secara vertikal. Urutkan kembali nama kolom hingga membentuk kata kunci. Tuliskan setiap huruf dari setiap kolom dalam tabel secara horizontal untuk mendapatkan *plaintext.*[7]

3. HASIL DAN PEMBAHASAN

3.1 Analisa Algoritma Columnar Transposition Cipher

Teknik kriptografi *Columnar Transposition Cipher* merupakan kriptografi dengan kunci simetris, yaitu proses enkripsi dan dekripsi pesan dilakukan dengan menggunakan kata kunci yang sama. Proses enkripsi dan dekripsi pesan dengan metode *Columnar Transposition Cipher* akan dijelaskan sebagai berikut:

3.1.1 Proses Enkripsi

Setelah seluruh *plaintext* dan kata kunci selesai diketik, buat sebuah tabel dengan jumlah kolom sesuai jumlah huruf pada kata kunci, serta jumlah baris sesuai dengan jumlah huruf pada *plaintext* dibagi dengan jumlah huruf pada kata kunci. Setiap huruf pada kata kunci akan dijadikan sebagai nama kolom dalam tabel dan setiap*key ascii* huruf dalam *plaintext* dimasukkan secara horizontal ke masing-masing kolom pada tabel tersebut. Apabila baris terakhir dari tabel tidak terisi penuh atau terdapat kolom yang kosong, maka isi kolom tersebut dengan *key ascii* 32 yaitu spasi. Selanjutnya acak kolom dan isi tabel berdasarkan urutan alfabet pada kata kunci. Setelah kolom tabel diacak, tuliskan kembali setiap huruf dan spasi yang diperoleh dari *key ascii* dalam tabel tersebut untuk memperoleh *ciphertext.*

3.1.2 Proses Dekripsi

Setelah seluruh *ciphertext* dan kata kunci selesai diketik, buat sebuah tabel dengan jumlah kolom sesuai jumlah huruf pada kata kunci, serta jumlah baris sesuai dengan jumlah huruf pada *ciphertext* dibagi dengan jumlah huruf pada kata kunci. Setiap huruf pada kata kunci dijadikan sebagai nama kolom dalam tabel. Urutkan kolom dalam tabel tersebut berdasarkan urutan alfabet pada kata kunci. Masukkan seluruh *key ascii* dari setiap huruf pada *ciphertext* scara vertikal ke setiap kolom dalam tabel yang telah diurutkan. Urutkan kembali setiap nama kolom dan isi kolom dalam tabel hingga nama kolom terbentuk menjadi kata kunci. Tuliskan kembali setiap huruf dan spasi yang diperoleh dari *key ascii* dalam tabel tersebut secara horizontal untuk memperoleh *plaintext.*

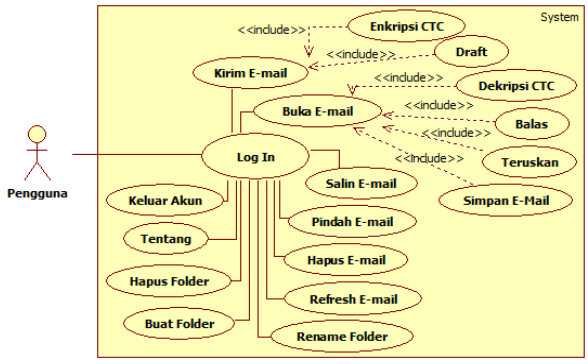
3.2 Analisis Aplikasi Kriptografi E-Mail

Aplikasi kriptografi *e-mail* digunakan untuk mengirimkan *e-mail* yang telah dienkripsi dan melakukan dekripsi pada *e-mail* yang berisi *ciphertext* dengan teknik *columnar transposition cipher*. Selain untuk pengiriman *e-mail*, melalui aplikasi ini pengguna juga dapat melakukan berbagai pengoperasian yang berkaitan dengan *e-mail* dalam akun pengguna seperti memindahkan *e-mail*, menyalin *e-mail*, membuat folder, mengubah nama folder, serta menghapus folder. Aplikasi kriptografi *e-mail* juga memungkinkan pengguna untuk menyimpan *e-mail* yang diterima dan *draft e-mail* ke dalam komputer pengguna dengan format .docx atau .txt.

3.3 Perancangan Unified Modeling Language

3.3.1 Diagram Use Case Aplikasi Kriptografi E-Mail

Melalui diagram *use case* pada Gambar 2 terdapat berbagai pengoperasian yang dapat dilakukan terhadap *e-mail* pengguna dengan menggunakan aplikasi kriptografi *e-mail* seperti kirim *e-mail*, buka *e-mail*, salin *e-mail*, pindah *e-mail*, hapus *e-mail*, *refresh*/memperbarui daftar *e-mail*, serta berbagai pengoperasian pada folder *e-mail* pengguna.

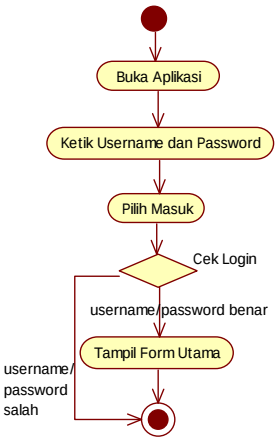


Gambar 2. Diagram Use Case Aplikasi Kriptografi E-Mail

3.3.2 Diagram Activity Log In

Pengguna harus melakukan *log in* terlebih dahulu sebelum menggunakan aplikasi kriptografi *e-mail*. Berbagai aktivitas yang harus dilakukan oleh pengguna saat proses *log in* dapat dilihat pada Gambar 3. Aktivitas pertama dimulai dengan pengguna membuka aplikasi kriptografi *e-mail*, kemudian mengetikkan *username* dan

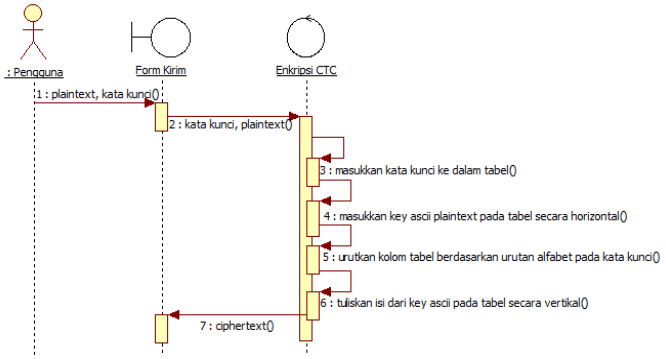
password dari akun *e-mail* pengguna. Setelah *username* dan *password* diketikkan pilih "Masuk", apabila *username* atau *password e-mail* salah, maka proses *log in* dibatalkan. Apabila benar maka akan ditampilkan "Form Utama" pada pengguna.



Gambar 3. Diagram Activity Log In

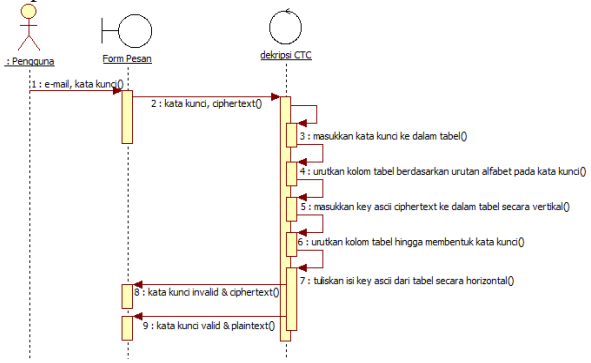
3.3.3 Sequence Diagram Enkripsi

Sequence diagram pada Gambar 4 merupakan gambaran aliran data yang terjadi saat proses enkripsi *e-mail* dengan metode *Columnar Transposition Cipher* dalam aplikasi kriptografi sedang berlangsung. Pengguna memberikan *input*-an berupa *plaintext* dan kata kunci pada "Form Kirim". Kata kunci dan *plaintext* akan melalui proses "Enkripsi CTC". Setiap huruf dalam kata kunci dijadikan sebagai nama kolom dan *plaintext* dimasukkan ke dalam tabel secara horizontal. Kolom tabel yang berisi kata kunci diurutkan berdasarkan urutan alfabet dalam kata kunci. Isi dari tabel dituliskan secara vertikal dari kolom kiri hingga kanan untuk menghasilkan *ciphertext*. *Ciphertext* yang telah dihasilkan ditampilkan pada "Form Kirim".



Gambar 4. Sequence Diagram Enkripsi

3.3.4 Sequence Diagram Dekripsi



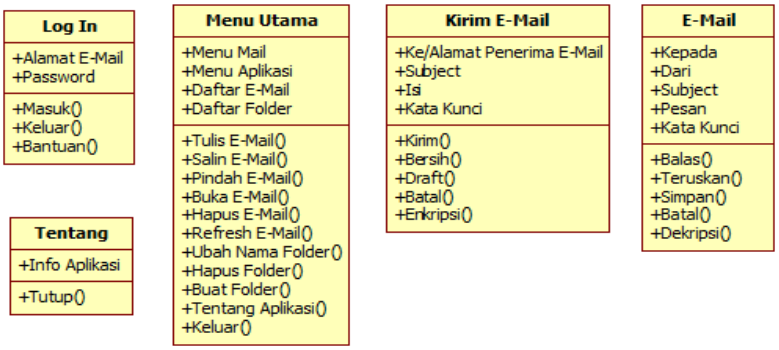
Gambar 5. Sequence Diagram Dekripsi

Sequence diagram pada Gambar 5 merupakan gambaran aliran data yang terjadi saat proses dekripsi dengan metode *Columnar Transposition Cipher* pada *e-mail* yang berisi *ciphertext* melalui aplikasi kriptografi sedang berlangsung. *E-mail* berisi *ciphertext* yang dibuka akan ditampilkan pada "Form Pesan" dan pengguna memberikan *input*-an kata kunci dalam form tersebut. Kata kunci dan *ciphertext* diproses melalui proses

"Dekripsi CTC". Kata kunci dimasukkan ke dalam tabel sebagai nama kolom dan kolom tabel diurutkan berdasarkan urutan alfabet pada kata kunci. *Ciphertext* dimasukkan ke dalam tabel secara vertikal dari kiri hingga kanan dan urutkan kembali nama kolom tabel hingga membentuk kata kunci. Isi dari tabel dituliskan kembali secara horizontal, apabila kata kunci salah, maka isi dari tabel akan menghasilkan *ciphertext* yang baru dan ditampilkan pada "Form Pesan". Apabila kata kunci benar, maka isi dari tabel akan menghasilkan *plaintext* dan ditampilkan pada "Form Pesan".

3.3.5 Class Diagram Aplikasi Kriptografi E-Mail

Class diagram pada Gambar 6 merupakan gambaran struktur logika dari aplikasi kriptografi *e-mail.* Terdapat 5 form yang menjadi struktur logika dalam aplikasi kriptografi *e-mail*, yaitu *form Log In*, *form* Menu Utama, *form* Kirim *E-Mail*, *form E-Mail*, dan *form* Tentang.



Gambar 6. Class Diagram Aplikasi Kriptografi E-Mail

3.3.6 Deployment Diagram Aplikasi Kriptografi E-Mail

Deployment diagram pada Gambar 7 merupakan gambaran penyebaran sistem yang terjadi selama penggunaan aplikasi kriptografi *e-mail*. Pengguna menggunakan komputer *client* menjalankan aplikasi kriptografi *e-mail*. Setelah aplikasi dijalankan, maka melalui jaringan internet, aplikasi akan terhubung dengan *Mail Server* sehingga pengguna dapat menggunakan akun *e-mail*-nya melalui aplikasi kriptografi.

Gambar 7. Deployment Diagram Aplikasi Kriptografi E-Mail

3.4 Tampilan Form Utama Aplikasi Kriptografi E-Mail

Form Utama pada Gambar 8 merupakan form yang akan ditampilkan pada penguna setelah melakukan proses *log in*. Form Utama memiliki berbagai menu, tombol, serta item yang dapat digunakan oleh pengguna sesuai fungsinya masing-masing seperti:

3.4.1 Menu Mail berfungsi untuk menampilkan berbagai submenu yang digunakan dalam pengoperasian *e-mail.*

Berbagai submenu dalam menu Mail yaitu:

a. Submenu Tulis E-Mail digunakan untuk menulis *e-mail* baru dan membuka Form Kirim Pesan.
b. Submenu Pindah E-Mail digunakan untuk memindahkan *e-mail* dari suatu folder ke folder yang lain dan menampilkan Input Box Pindah E-Mail.
c. Submenu Salin E-Mail digunakan untuk menyalin *e-mail* dari suatu folder ke folder yang lain dan menampilkan Input Box Salin E-Mail.

3.4.2 Menu Aplikasi berfungsi untuk menampilkan berbagai submenu yang digunakan dalam pengoperasian aplikasi. Berbagai submenu dalam menu Aplikasi yaitu:

a. Submenu Tentang digunakan untuk menampilkan Form Tentang yang berisikan informasi aplikasi kriptografi.
b. Submenu Keluar digunakan untuk keluar dari akun *e-mail* pengguna dan menampilkan kembali Form Log In.

3.4.3 *Pop up* menu Folder berfungsi untuk menampilkan berbagai submenu yang digunakan dalam pengoperasian folder, dan hanya dapat ditampilkan saat pengguna mengklik kanan pada area daftar folder. Berbagai submenu dalam *pop up* menu Folder yaitu:

a. Submenu Buat Folder digunakan untuk membuat folder baru dalam akun *e-mail* pengguna dan menampilkan Input Box Buat Folder.
b. Submenu Rename Folder digunakan untuk mengubah nama folder dalam akun *e-mail* pengguna dan menampilkan Input Box Rename Folder.

c. Submenu Hapus Folder digunakan untuk menghapus folder dalam akun *e-mail* pengguna dan menampilkan Input Box Hapus Folder.

3.4.4 Tombol Buka berfungsi untuk membuka *e-mail* dan menampilkan Form Pesan.

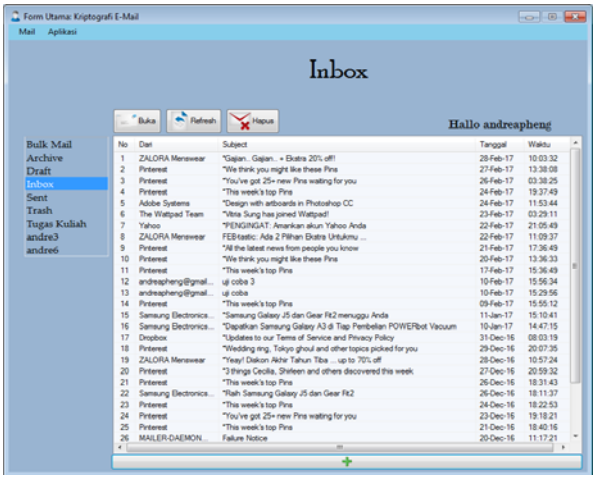
3.4.5 Tombol Refresh berfungsi untuk memperbarui daftar *e-mail.*

3.4.6 Tombol Hapus berfungsi untuk menghapus *e-mail*.

3.4.7 Tombol Tambah berfungsi untuk menambah jumlah *e-mail* yang ditampilkan dalam daftar *e-mail*.

3.4.8 Daftar Folder berfungsi untuk menampilkan seluruh folder yang terdapat dalam akun *e-mail* pengguna.

3.4.9 Daftar E-mail berfungsi untuk menampilkan daftar *e-mail* dari tiap folder.



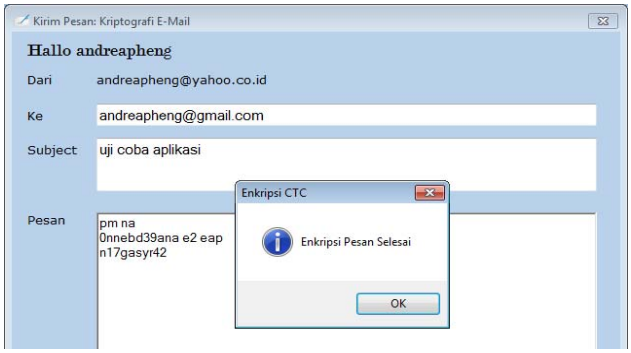
Gambar 8 Form Utama Aplikasi Kriptografi E-Mail

3.5 Uji Coba Perangkat Lunak

3.5.1 Black Box Testing

a. Pengujian Proses Enkripsi

Berdasarkan hasil pengujian proses enkripsi pada Gambar 9, apabila pengguna menekan “Tombol Enkripsi” yang terdapat pada “Form Kirim Pesan”, maka *plaintext* atau isi *e-mail* yang telah dituliskan oleh pengguna akan melalui “Proses Enkripsi CTC”. Setelah *plaintext* menjadi *ciphertext*, pengguna menerima pesan pemberitahuan pesan telah selesai dienkripsi.



Gambar 9. Hasil Pengujian Proses Enkripsi

b. Pengujian Proses Dekripsi

1) Pengujian Input Kata Kunci Salah

Gambar 10. Hasil Pengujian Input Kata Kunci Salah

Berdasarkan hasil pengujian proses dekripsi pada Gambar 10, apabila pengguna menekan "Tombol Dekripsi" dan memasukkan kata kunci yang salah melalui "Input Box Dekripsi", maka *e-mail ciphertext* yang telah melalui "Proses Dekripsi CTC" dengan kata kunci yang salah akan menghasilkan *ciphertext* yang baru.

2) Pengujian Input Kata Kunci Benar

Berdasarkan hasil pengujian proses dekripsi pada Gambar 11, apabila pengguna menekan "Tombol Enkripsi" dan memasukkan kata kunci yang benar melalui "Input Box Dekripsi", maka *e-mail ciphertext* yang telah melalui "Proses Dekripsi CTC" dengan kata kunci yang benar akan menghasilkan *plaintext*.

Gambar 11. Hasil Pengujian Input Kata Kunci Benar

3.5.2 White Box Testing

a. Pengujian Kode Enkripsi

1) Langkah Enkripsi 1

Gambar 12 merupakan "Kode Program Langkah Enkripsi 1" dari *columnar transposition cipher* atau CTC. Apabila contoh *plaintext* "PENGAMANAN PESAN DENGAN ENKRIPSI DAN DEKRIPSI" dengan kata kunci "KRIPTOGRAFI" melalui "Kode Program Langkah Enkripsi 1", maka hasilnya adalah tabel enkripsi dengan kolom yang telah berisi seluruh karakter kata kunci seperti Gambar 13.

```
Private Sub enkripsi()
    Dim banyakteks, kode, z, urutan, banyakbaris As Integer
    Dim plain(30), kunci(30), q, text As String
    Dim daftar As ListViewItem

    ListView1.Items.Clear()
    ListView2.Items.Clear()
    banyakteks = RichTextBox1.TextLength
    plaintext = RichTextBox1.Text
    kode = katakunci.Length

    z = 0
    For i = 1 To kode
        kunci(z) = Mid(katakunci, i, 1)
        z = z + 1
    Next
    daftar = New ListViewItem(kunci)
    ListView1.Items.Add(daftar)
    daftar = New ListViewItem(kunci)
    ListView2.Items.Add(daftar)
```

Gambar 12. Kode Program Langkah Enkripsi 1

1	2	3	4	5	6	7	8	9	10	11
K	R	I	P	T	O	G	R	A	F	I

Gambar 13. Hasil Kode Program Langkah Enkripsi 1

2) Langkah Enkripsi 2

Gambar 14 merupakan "Kode Program Langkah Enkripsi 2" dari *columnar transposition cipher* atau CTC. Hasil dari contoh *plaintext* yang telah melalui "Kode Program Langkah Enkripsi 2" adalah setiap karakter dalam *plaintext* dijadikan *keyascii* dan dimasukkan dalam tabel enkripsi, apabila terdapat bagian yang kosong maka bagian tersebut diisi angka 32 seperti Gambar 15.

```
For i = 1 To banyakteks

    For m = 0 To kode - 1
        If i > banyakteks And m <= kode - 1 Then
            plain(m) = "32"
        Else
            plain(m) = Asc(Mid(RichTextBox1.Text, i, 1))
        End If

        i = i + 1
    Next
    daftar = New ListViewItem(plain)
    ListView1.Items.Add(daftar)
    daftar = New ListViewItem(plain)
    ListView2.Items.Add(daftar)
    i = i - 1
Next
```

Gambar 14. Kode Program Langkah Enkripsi 2

1	2	3	4	5	6	7	8	9	10	11
K	R	I	P	T	O	G	R	A	F	I
80	69	78	71	65	77	65	78	65	78	32
80	69	83	65	78	32	68	69	78	71	65
78	32	69	78	75	82	73	80	83	73	32
68	65	78	32	68	69	75	82	73	80	83
73	32	32	32	32	32	32	32	32	32	32

Gambar 15. Hasil Kode Program Langkah Enkripsi 2

3) Langkah Enkripsi 3

Gambar 16 merupakan "Kode Program Langkah Enkripsi 3" dari *columnar transposition cipher* atau CTC. Hasil dari contoh *plaintext* yang telah melalui "Kode Program Langkah Enkripsi 3" adalah setiap kolom beserta isi kolom dalam tabel enkripsi diurutkan sesuai urutan alfabet pada kata kunci seperti Gambar 17.

```
banyakbaris = ListView1.Items.Count - 1
For i = 0 To kode - 1
    urutan = 1000
    For m = 0 To kode - 1
        If ListView1.Items(0).SubItems(m).Text <> "**" Then
            If Asc(ListView1.Items(0).SubItems(m).Text) < urutan Then
                z = m
                urutan = Asc(ListView1.Items(0).SubItems(m).Text)
            End If
        End If
    Next
    For y = 0 To banyakbaris
        ListView2.Items(y).SubItems(i).Text = ListView1.Items(y).SubItems(z).Text
        ListView1.Items(y).SubItems(z).Text = "**"
    Next
Next
```

Gambar 16. Kode Program Langkah Enkripsi 3

1	2	3	4	5	6	7	8	9	10	11
A	F	G	I	I	K	O	P	R	R	T
65	78	65	78	32	80	77	71	69	78	65
78	71	68	83	65	80	32	65	69	69	78
83	73	73	69	32	78	82	78	32	80	75
73	80	75	78	83	68	69	32	65	82	68
32	32	32	32	32	73	32	32	32	32	32

Gambar 17. Hasil Kode Program Langkah Enkripsi 3

4) Langkah Enkripsi 4

Gambar 18 merupakan "Kode Program Langkah Enkripsi 4" dari *columnar transposition cipher* atau CTC. Hasil dari contoh *plaintext* yang telah melalui "Kode Program Langkah Enkripsi 4" adalah *keyascii* yang merupakan isi dari setiap kolom pada tabel enkripsi, diubah menjadi bentuk karakter dan dituliskan kembali secara vertikal seperti Gambar 19.

```
        RichTextBox1.Text = ""
        text = ""
        For i = 0 To kode - 1
            For m = 1 To banyakbaris
                text = text + Chr(ListView2.Items(m).SubItems(i).Text)
            Next
        Next
        RichTextBox1.Text = text
        RichTextBox1.ReadOnly = True
    End Sub
```

Gambar 18. Kode Program Langkah Enkripsi 4

```
ANSI NGIP ADIK NSEN  A S PPNDIM RE GAN  EE A NEPR ANKD
```

Gambar 19. Hasil Kode Program Langkah Enkripsi 4

b. Pengujian Kode Program Dekripsi

1) Langkah Dekripsi 1

Gambar 20 merupakan "Kode Program Langkah Dekripsi 1" dari *columnar transposition cipher* atau CTC. Apabila contoh *ciphertext* "ANSI NGIP ADIK NSEN A S PPNDIM RE GAN EE A NEPR ANKD" dengan kata kunci "KRIPTOGRAFI" melalui "Kode Program Langkah Dekripsi 1", maka hasilnya adalah tabel dekripsi dengan kolom yang telah berisi seluruh karakter kata kunci seperti Gambar 21.

```
Private Sub dekripsi()
    Dim banyakteks, kode, z, urutan, banyakbaris, d As Integer
    Dim plain(30), kunci(30), g As String
    Dim daftar, daftar2 As ListViewItem

    ListView1.Items.Clear()
    ListView2.Items.Clear()
    banyakteks = RichTextBox1.TextLength
    kode = katakunci.Length

    z = 0
    For i = 1 To kode
        kunci(z) = Mid(katakunci, i, 1)
        z = z + 1
    Next
    daftar = New ListViewItem(kunci)
    ListView1.Items.Add(daftar)
    daftar2 = New ListViewItem(kunci)
    ListView2.Items.Add(daftar2)
```

Gambar 20. Kode Program Langkah Dekripsi 1

1	2	3	4	5	6	7	8	9	10	11
K	R	I	P	T	O	G	R	A	F	I

Gambar 21. Hasil Kode Program Langkah Dekripsi 1

2) Langkah Dekripsi 2

Gambar 22 merupakan "Kode Program Langkah Dekripsi 2" dari *columnar transposition cipher* atau CTC. Hasil dari "Kode Program Langkah Dekripsi 2" adalah kata kunci yang terdapat dalam tabel dekripsi diurutkan sesuai urutan alfabet seperti Gambar 23.

```
For i = 0 To kode - 1
    urutan = Asc(ListView1.Items(0).SubItems(i).Text)
    For m = i + 1 To kode - 1
        If Asc(ListView1.Items(0).SubItems(m).Text) < urutan Then
            z = urutan
            urutan = Asc(ListView1.Items(0).SubItems(m).Text)
            ListView1.Items(0).SubItems(m).Text = Chr(z)
            ListView1.Items(0).SubItems(i).Text = Chr(urutan)
        End If
    Next

Next
```

Gambar 22. Kode Program Langkah Dekripsi 2

1	2	3	4	5	6	7	8	9	10	11
A	F	G	I	I	K	O	P	R	R	T

Gambar 23. Hasil Kode Program Langkah Dekripsi 2

3) Langkah Dekripsi 3

Gambar 24 merupakan "Kode Program Langkah Dekripsi 3" dari *columnar transposition cipher* atau CTC. Hasil dari contoh *ciphertext* yang telah melalui "Kode Program Langkah Dekripsi 3" adalah setiap karakter dalam *ciphertext* dijadikan *keyascii* dan dimasukkan dalam tabel dekripsi seperti Gambar 25.

```
For i = 1 To banyakteks
    For m = 0 To kode - 1
        If i > banyakteks And m <= kode - 1 Then
            plain(m) = "32"
        Else
            plain(m) = "32"
        End If
        i = i + 1
    Next
    daftar = New ListViewItem(plain)
    ListView1.Items.Add(daftar)
    daftar2 = New ListViewItem(plain)
    ListView2.Items.Add(daftar2)
    i = i - 1
Next
banyakbaris = ListView1.Items.Count
d = 1
For i = 0 To kode - 1
    For m = 1 To banyakbaris - 1
        If d <= banyakteks Then
            ListView1.Items(m).SubItems(i).Text = Asc(Mid(RichTextBox1.Text, d, 1))
            d = d + 1
        End If
    Next
Next
```

Gambar 24. Kode Program Langkah Dekripsi 3

1	2	3	4	5	6	7	8	9	10	11
A	F	G	I	I	K	O	P	R	R	T
65	78	65	78	32	80	77	71	69	78	65
78	71	68	83	65	80	32	65	69	69	78
83	73	73	69	32	78	82	78	32	80	75
73	80	75	78	83	68	69	32	65	82	68
32	32	32	32	32	73	32	32	32	32	32

Gambar 25. Hasil Kode Program Langkah Dekripsi 3

4) Langkah Dekripsi 4

Gambar 26 merupakan "Kode Program Langkah Dekripsi 4" dari *columnar transposition cipher* atau CTC. Hasil dari contoh *ciphertext* yang telah melalui "Kode Program Langkah Enkripsi 4" adalah setiap kolom beserta isi kolom dalam tabel dekripsi yang sebelumnya telah terurut akan diurutkan kembali hingga membentuk kata kunci seperti Gambar 27.

```
For i = 0 To kode - 1
    For m = 0 To kode - 1
        If ListView1.Items(0).SubItems(m).Text = ListView2.Items(0).SubItems(i).Text Then
            For w = 1 To banyakbaris - 1
                ListView2.Items(w).SubItems(i).Text = ListView1.Items(w).SubItems(m).Text
            Next
            ListView1.Items(0).SubItems(m).Text = "##"
            Exit For
        End If
    Next
Next
```

Gambar 26. Kode Program Langkah Dekripsi 4

1	2	3	4	5	6	7	8	9	10	11
K	R	I	P	T	O	G	R	A	F	I
80	69	78	71	65	77	65	78	65	78	32
80	69	83	65	78	32	68	69	78	71	65
78	32	69	78	75	82	73	80	83	73	32
68	65	78	32	68	69	75	82	73	80	83
73	32	32	32	32	32	32	32	32	32	32

Gambar 27. Hasil Kode Program Langkah Dekripsi 4

5) Langkah Dekripsi 5

Gambar 28 merupakan "Kode Program Langkah Dekripsi 5" dari *columnar transposition cipher* atau CTC. Hasil dari contoh *ciphertext* yang telah melalui "Kode Program Langkah Dekripsi 5" adalah *keyascii* yang merupakan isi dari setiap kolom pada tabel dekripsi, diubah menjadi bentuk karakter dan dituliskan kembali secara horizontal seperti Gambar 29.

```
    RichTextBox1.Text = ""
    For i = 1 To banyakbaris - 1
        For m = 0 To kode - 1
            RichTextBox1.Text = RichTextBox1.Text + Chr(ListView2.Items(i).SubItems(m).Text)
        Next
    Next
    RichTextBox1.Text = RTrim(RichTextBox1.Text)

End Sub
```

Gambar 28. Kode Program Langkah Dekripsi 5

PENGAMANAN PESAN DENGAN ENKRIPSI DAN DEKRIPSI

Gambar 29. Hasil Kode Program Langkah Dekripsi 5

4. KESIMPULAN

Berdasarkan penjelasan pada bab-bab sebelumnya dapat diambil kesimpulan mengenai perancangan aplikasi kriptografi *e-mail* dengan metode *columnar transposition cipher* yaitu sebagai berikut:

a. Aplikasi kriptografi *e-mail* dengan metode *columnar transposition cipher* dapat digunakan untuk meningkatkan keamanan dalam pengiriman *e-mail* serta menjaga isi atau kerahasiaan *e-mail* yang tersimpan pada *mail server*.
b. Algoritma *columnar transposition cipher* dapat digunakan untuk peningkatan keamanan pengiriman *e-mail* karena *e-mail* yang telah dienkripsi dengan algoritma *columnar transposition cipher* akan dienkripsi kembali oleh sistem keamanan yang digunakan pihak layanan penyedia *e-mail* selama proses pengiriman *e-mail*.
c. Aplikasi kriptografi *e-mail* dengan metode *columnar transposition cipher* mengacak isi *e-mail* yang dikirimkan menjadi kalimat yang tidak dapat dibaca oleh siapapun selain oleh pihak yang berhak menerima *e-mail* tersebut atau memiliki kunci enkripsi.

5. SARAN

Berikut saran-saran yang dapat diberikan untuk pengunaan serta pengembangan lebih lanjut aplikasi kriptografi *e-mail* dengan metode *columnar transposition cipher* sehingga aplikasi dapat digunakan dan berjalan lebih optimal, yaitu:

a. Antivirus yang terpasang pada komputer harap dimatikan terlebih dahulu sebelum menggunakan aplikasi kriptografi *e-mail*, karena antivirus tersebut dapat memeriksa *e-mail* yang dikirimkan oleh pengguna dan mengubah isi *e-mail* yang telah dienkripsi.
b. Bagi pengguna yang pertamakali menggunakan aplikasi kriptografi *e-mail*, maka pengguna perlu memberikan izin melalui akun *e-mail* pengguna agar aplikasi dapat mengakses *e-mail* tersebut.
c. Algoritma *columnar transposition cipher* yang diterapkan dalam aplikasi dapat dipadukan dengan algoritma kriptografi lainnya agar menghasilkan tingkat pengamanan pesan yang lebih baik.
d. Jenis *e-mail* yang diamankan dapat dikembangkan tidak hanya untuk ymail dan gmail saja, namun juga untuk *e-mail* jenis lainnya.
e. Aplikasi kriptografi *e-mail* dapat dikembangkan untuk pengamanan *e-mail* yang tidak hanya berisikan teks, namun juga *e-mail* yang memiliki lampiran.

f. Tampilan aplikasi kriptografi *e-mail* dapat dikembangkan lagi dengan tampilan yang lebih menarik.

UCAPAN TERIMA KASIH

Dalam penulisan ini, penulis telah benyak mendapatkan bantuan berupa bimbingan, petunjuk, data, saran maupun dorongan moral dari berbagai pihak, maka pada kesempatan ini penulis mengucapkan terima kasih kepada civitas akademika STMIK Widya Dharma Pontianak, kepada keluarga, beserta teman tercinta yang telah banyak memberikan bantuan dan dorongan selama penulis menjalani studi hingga selesainya penulisan ini.

DAFTAR PUSTAKA

[1] Yasin, Verdi. (2012). *Rekayasa Perangkat Lunak Berorientasi Objek*. Mitra Wacana Media. Jakarta.
[2] Simarmata, Janner. (2010). *Rekayasa Perangkat Lunak*. Edisi 1. Andi. Yogyakarta.
[3] Arryawan, Eko., SmitDev Community. (2010). *Anti Forensik (Uncensored): Mengatasi Investigasi Komputer Forensik*. PT Elex Media Komputindo. Jakarta.
[4] Kromodimoeljo, Sentot. (2010). *Teori dan Aplikasi Kriptografi*. SPK IT Consulting. Jakarta.
[5] Shelly, Gary B., Misty E. Vermaat. (2012). *Menjelajah Dunia Komputer-Hidup dalam Era Digital*. Edisi 15 (judul asli : Discovering Computers 2010: Living in Digital World). Penerjemah Chriswan Sungkono. Salemba Infotek. Jakarta.
[6] Dooley, John F. (2013). *A Brief History of Cryptology and Cryptographic Algorithms*. Springer International Publishing. Cham.
[7] Sutherland, Denise., Mark E. Koltko-Rivera, PhD. (2010). *Cracking Codes & Cryptograms For fgbh Dummies*. Wiley Publishing, Inc. Indianapolis.