APLIKASI KRIPTOGRAFI MENGGUNAKAN ALGORITMA RC4 DAN DES UNTUK MENGAMANKAN PESAN EMAIL

Aldi Yuliansyah[1)], Noni Juliasari[2)].
Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
Telp. (021) 5853753, Fax. (021) 5866369
E-mail : aldiyuliansyah@gmail.com[1)], noni.juliasari@budiluhur.ac.id[2)]

ABSTRAK

Toko Hydroponic "Kannys Indoor Plant Rental" merupakan toko yang menggunakan aplikasi *email* dalam kegiatan bisnisnya dan memiliki beberapa pesan atau dokumen bersifat rahasia yang biasa diterima atau dikirim melalui aplikasi *email* seperti data karyawan, data pelanggan, data pemesanan, data transaksi, data keuangan, dan lain sebagainya. Oleh karena itu, isi pesan maupun dokumen yang diterima atau dikirim melalui aplikasi *email* toko harus terjaga keamanannya supaya tidak dapat diakses oleh pihak yang tidak bertanggung jawab. Terutama untuk keamanan berbisnis melalui aplikasi *email*. Karena pesan teks atau *file attachment* yang dikirim merupakan pesan yang bersifat rahasia dan pribadi, sehingga kerahasiaan dan keamanan pesan menjadi keutamaan bagi Toko Hydroponic "Kannys Indoor Plant Rental". Salah satu cara untuk meningkatkan keamanan dan menjaga kerahasiaan dalam bertukar pesan melalui aplikasi *email* adalah dengan menggabungkan aplikasi *email* dengan ilmu kriptografi yang menggunakan algoritma kunci simetris, dimana kunci enkripsi dan dekripsi yang dipakai merupakan kunci yang sama. Dalam pengembangan aplikasi pengamanan *email* ini penulis menggunakan metode pengembangan dengan metode *waterfall* untuk mempermudah dalam proses penelitian ini. Supaya aplikasi pengamanan *email* ini dapat terjamin kemanannya, aplikasi ini menggunakan ilmu kriptografi dengan 2 metode yaitu metode algoritma RC4 (*Rivest Code* 4) dan DES (*Data Encryption Standard*). Penelitian ini menghasilkan Aplikasi kriptografi menggunakan Algoritma RC4 dan DES untuk mengamankan pesan email. Dengan demikian, diharapkan Toko Hydroponic "Kannys Indoor Plant Rental" dapat mengirimkan pesan *email* atau *file attachment* yang bersifat rahasia dan pribadi tanpa takut ada orang lain yang tidak di inginkan dapat membuka atau meretas pesan *email* maupun *file attachment* yang dikirim atau diterima melalui aplikasi *email*.

Kata Kunci : Enkripsi, Dekripsi, Kriptografi, RC4, DES, Waterfall, File Attachment

1. PENDAHULUAN

Toko Hydroponic "Kannys Indoor Plant Rental" merupakan toko yang menggunakan aplikasi *email* dalam kegiatan bisnisnya. Baik untuk pertukaran informasi antar staff ataupun pertukaran informasi dengan klien atau pelanggan. Karena tingginya resiko pencurian data atau informasi melalui internet yang dilakukan oleh sejumlah orang terutama yang dilakukan oleh *Hacker*, oleh karena itu bisa dikatakan ilmu kriptografi merupakan salah satu solusi untuk mengatasi pencurian data atau bertukar informasi melalui internet. Terutama untuk keamanan berbisnis melalui *email*.

Toko Hydroponic "Kannys Indoor Plant Rental" merupakan toko yang memiliki beberapa pesan atau dokumen bersifat rahasia yang biasa diterima atau dikirim melalui aplikasi *email* seperti data karyawan, data pelanggan, data pemesanan, data transaksi, data keuangan, dan sebagainya. Oleh karena itu, isi pesan maupun dokumen yang diterima atau dikirim melalui *email* toko harus terjaga keamanannya supaya tidak dapat diakses oleh pihak yang tidak bertanggung jawab.

Atas dasar uraian diatas, maka pada penelitian ini, penulis melakukan implementasi terhadap pengamanan data serta isi pesan pada aplikasi *email* dengan menggunakan algoritma RC4 dan DES pada Toko Hydroponic "Kannys Indoor Plant Rental".

Tujuan dan maksud penelitian ini adalah untuk membuat aplikasi yang diharapkan dapat meningkatkan keamanan pada aplikasi *email* untuk mengamankan pesan serta data atau dokumen penting di *email* Toko Hydroponic "Kannys Indoor Plant Rental" antara lain:

a. Dengan menggunakan ilmu kriptografi untuk meningkatkan keamanan pengiriman pesan serta dokumen melalui aplikasi *email*.
b. Dengan menggabungkan algoritma RC4 dan DES pada satu aplikasi untuk mengamankan pesan *email* yang dikirim atau yang diterima oleh Toko Hydroponic "Kannys Indoor Plant Rental".

Supaya penelitian ini lebih terarah dan tidak meluasnya pembahasan maka penulis memberikan beberapa batasan masalah yaitu :

a. Algoritma yang digunakan untuk mengamankan data atau informasi adalah algoritma RC4 dan DES.
b. Pesan atau dokumen yang di enkripsi dan dekripsi merupakan pesan atau dokumen yang dikirim dan diterima melalui aplikasi *email*.
c. Bahasa pemrograman yang digunakan yaitu *PHP*.
d. Database yang dipakai yaitu *MySQL*.
e. Batas ukuran *file attachment* yaitu 25MB.
f. Tipe *file attachment* yang dapat digunakan dalam aplikasi ini adalah *file* dengan ekstensi : **.doc*, **.jpeg*, **.png*, **.pst*, **.pptx*, **.docx*, **.pdf*, **.xls*, dan **.xlsx*

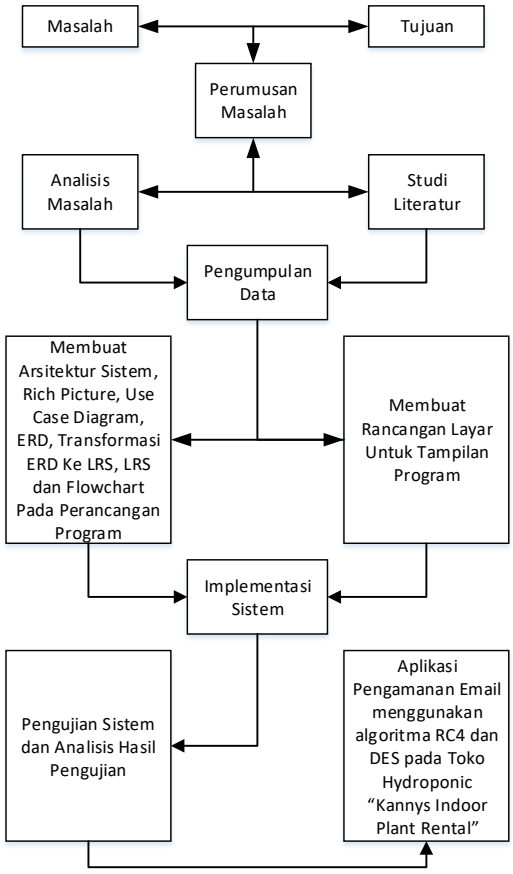
2. METODE PENELITIAN

Dalam pengembangan aplikasi pengamanan *email* ini penulis menggunakan metode *waterfall* untuk mempermudah dalam proses penelitian yang penulis lakukan [15].

a. Analisis (*Analysis/Requirement*)
   Pada tahap ini, penulis melakukan pengumpulan data atau kebutuhan dengan melakukan wawancara pada pemilik Toko Hydroponic "Kannys Indoor Plant Rental".
b. Desain (*Design*)
   Dalam proses ini, penulis mendesain rancangan layar dan *flowchart* dengan menggunakan aplikasi desain yaitu Ms. Visio 2016.
c. Pengkodean (*Coding*)
   Proses penerjemahan desain kedalam bentuk bahasa mesin yang kami gunakan adalah dengan bahasa pemrograman *PHP* dan menggunakan editor Notepad++.
d. Pengujian (*Testing*)
   Pada tahap ini, dilakukan pembuatan *prototype* yang akan di persentasikan pada pemilik Toko Hydroponic "Kannys Indoor Plant Rental" sebagai bentuk uji coba program.
e. Pemeliharaan (*Maintenance*)
   Dalam tahapan ini, dilakukan penyesuaian atau perubahan seiring dengan adaptasi perangkat lunak kepada *user*.

3. ANALISA MASALAH DAN PERANCANGAN PROGRAM

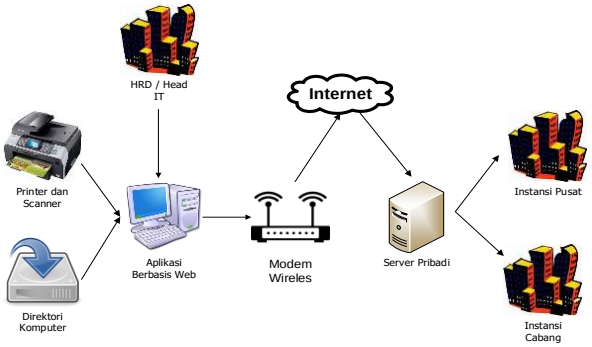
3.1 Alur Pikir Penelitian



Gambar 5: Alur Pikir Penelitian

3.1 Arsitektur Sistem

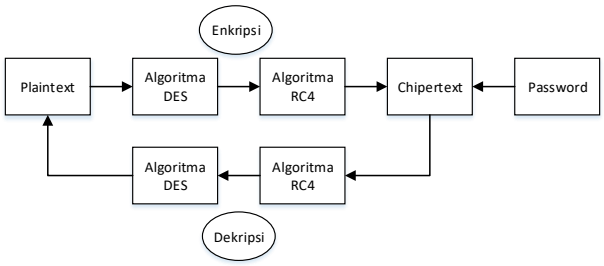
Arsitektur sistem menggambarkan garis besar proses dari keseluruhan sistem guna untuk memahami konsep aplikasi yang akan di bangun:



Gambar 6: Arsitektur sistem

3.2 *Rich Picture* Urutan Algoritma

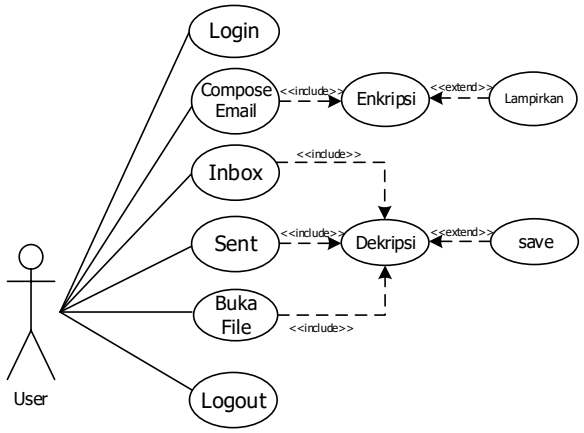
Gambar *rich picture* urutan algoritma dibawah ini menjelaskan tentang urutan algoritma yang akan terjadi saat melakukan proses enkripsi dan dekripsi.



Gambar 7: Rich Picture Urutan Algoritma

3.3 *Use Case Diagram*

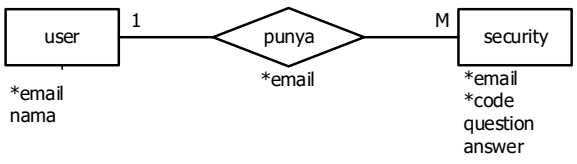
Diagram use case digunakan untuk mengetahui fungsi apa saja yang ada di dalam sebuah sistem dan siapa saja yang berhak menggunakan fungsi-fungsi tersebut.



Gambar 8: Use Case Diagram

3.4 *Entity Relationship Diagram* (ERD)

ERD merupakan gambaran untuk menjelaskan hubungan antar data dalam basis data berdasarkan objek-objek dasar data yang saling ber relasi atau berkaitan.



Gambar 9: Rancangan ERD

3.5 Algoritma Proses Enkripsi RC4

Algoritma proses enkripsi RC4 dijelaskan seperti di bawah ini.

```
1.   Start
2.   Masukkan Kunci
3.   Inisialisasi Kunci Internal
4.   Baca File
5.   If EOF Then
6.       Simpan Hasil File
7.       End
8.   Else
9.       Baca File Tiap 256 Bit
10.      If < 256 Bit Then
11.          Buat Padding Sampai 256 Bit
12.      End If
13.      Proses Enkripsi
14.      Hasil Enkripsi
15.      Kembali Ke Baris 4
16.  End If
```

3.6 Algoritma Proses Dekripsi RC4

Algoritma proses dekripsi RC4 dijelaskan seperti di bawah ini.

```
1.   Start
2.   Masukkan Kunci
3.   Inisialisasi Kunci Internal
4.   Masukkan Enkripsi
5.   Baca Hingga Akhir File
6.   If EOF Then
7.       If Has Padding Then
8.           Hapus Padding
9.   End If
10.      Hasil Dekripsi
11.      Simpan File
12.      End
13.  Else
14.      Baca 256 Bit Berkas Dekripsi
15.      Proses Dekripsi
16.      Kembali Ke Baris 6
17.  End If
```

3.7 Algoritma Proses Enkripsi DES

Algoritma proses enkripsi algoritma DES dijelaskan seperti di bawah ini.

```
1.   Start
2.   Masukkan Berkas awal
3.       Masukkan Kunci
4.       Inisialisasi Kunci Internal
5.           If Kunci=8 Then
6.              Baca File Hingga Akhir File
7.              If EOF Then
8.               End
9.              Else
10.               Baca 64 Bit Berkas Awal
11.               If Berkas Awal<64 Bit Then
12.                 Padding Sampai 64 Bit
13.               End If
14.                Enkripsi
15.                Output Hasil Enkripsi
```

```
16.                Kembali ke Baris 8
17.              End If
18.            Else
19.              Pesan Eror
20.              Kembali ke Baris 3
21.            End If
```

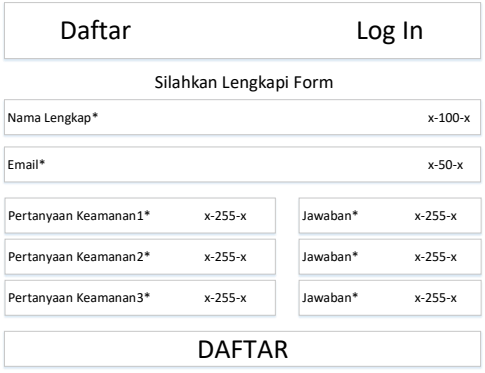
3.8 Algoritma Proses Dekripsi DES

Algoritma proses dekripsi DES dijelaskan seperti di bawah ini.

```
1.          Start
2.          Masukkan Berkas awal
3.          Masukkan Kunci
4.          Inisialisasi Kunci Internal
5.            If Kunci=8 Then
6.              Baca File Hingga Akhir File
7.              If EOF Then
8.               If Has Padding Then
9.                Output Berkas Hasil Dekripsi
10.               End
11.              Else
12.               Hapus Padding
13.              End If
14.             Else
15.              Baca 64 Bit Berkas Awal
16.              If Berkas Awal<64 Bit Then
17.                Padding Sampai 64 Bit
18.              End If
19.              Else
20.               Enkripsi
21.               Kembali ke Baris 8
22.            End If
23.          Else
24.            Pesan Error
25.            Kembali ke Baris 3
26.          End If
```

3.9 Rancangan Layar *Form* Daftar

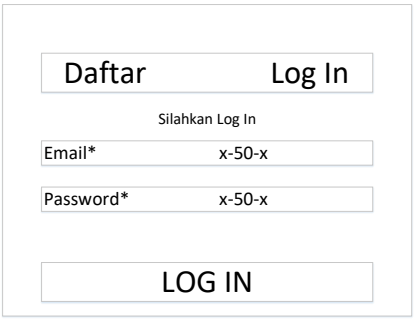
Pada *form* ini terdapat kolom Nama Lengkap, *Email*, *Password*, 3 pertanyaan keamanan dan 3 jawaban yang harus di isi. *Form* ini digunakan agar *user* dapat memiliki *Email* dan *Password* yang valid untuk dapat melakukan *login* di *form Log In.*



Gambar 10: Rancangan Layar Form Daftar

3.10 Rancangan Layar *Form Log In*

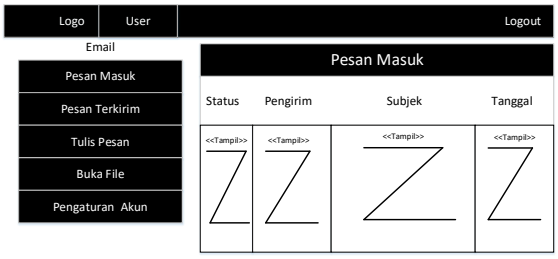
Form ini digunakan untuk dapat masuk ke dalam akun *user* atau menu utama aplikasi.



Gambar 11: Rancangan Layar Form Log in

3.11 Rancangan Layar *Form* Pesan Masuk

Setelah berhasil *login*, *user* langsung masuk ke dalam *form* Pesan Masuk. Di dalam *form* ini *user* dapat melihat semua pesan masuk yang terdiri dari Status, Pengirim, Subjek dan Tanggal.



Gambar 12: Rancangan Layar Form Pesan Masuk

4. HASIL DAN PEMBAHASAN

4.1 Implementasi Kebutuhan Program

Sebelum masuk pada tahap pemasangan aplikasi, ada beberapa kebutuhan yang harus dipenuhi yaitu perangkat keras maupun perangkat lunak.

a. Implementasi Kebutuhan Perangkat Keras

Spesifikasi *hardware* (perangkat keras) yang digunakan dalam pengoperasian aplikasi adalah sebagai berikut :

1) Processor Intel(R) Core(TM) I3-350M processor (2,26GHz, 3 MB L3 cache)
2) RAM Memori 2 GB
3) Harddisk 320 GB
4) Monitor 14.0”

b. Implementasi Kebutuhan Perangkat Lunak

Spesifikasi *software* (perangkat lunak) yang digunakan dalam pengoperasian aplikasi adalah sebagai berikut :

1) Sistem Operasi Microsoft Windows 7 Ultimate
2) Google Chrome atau Mozilla Firefox
3) MySQL-Font atau phpMyadmin

4) XAMPP Control Panel

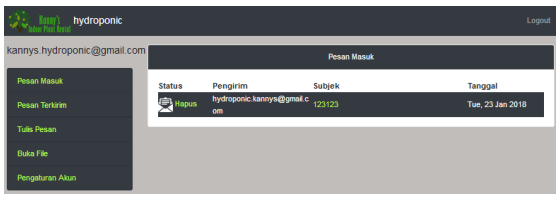
4.2 Tampilan Layar *Form* Daftar

Pada saat memulai aplikasi akan langsung menampilkan *form* daftar. Di dalam *form* daftar terdapat beberapa kolom yang harus di isi agar user dapat memiliki *Email* dan *Password* yang valid untuk dapat melakukan *login* di form *Log In*.

Gambar 13: Tampilan Layar Form Daftar

4.3 Tampilan Layar *Form* Pesan Masuk

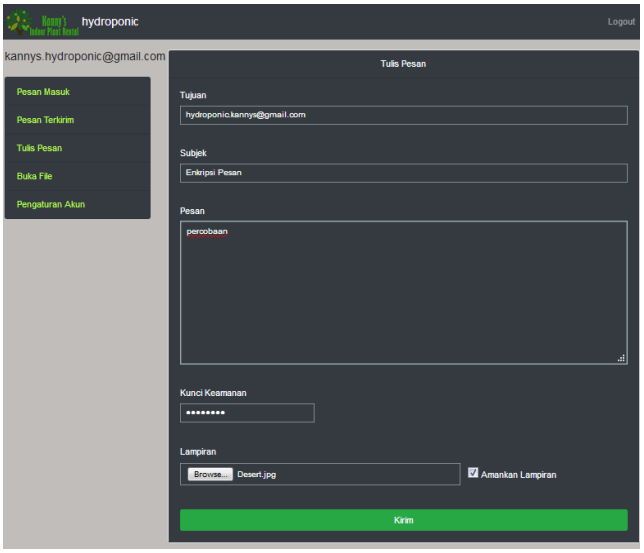
Setelah Log In berhasil aplikasi akan langsung menampilkan *form* Pesan Masuk. Di dalam *form* ini *user* dapat melihat pesan *email* yang sudah masuk dan dapat menghapus pesan *email* yang sudah masuk.



Gambar 14: Tampilan Layar Form Pesan Masuk

4.4 Tampilan Layar Proses Enkripsi

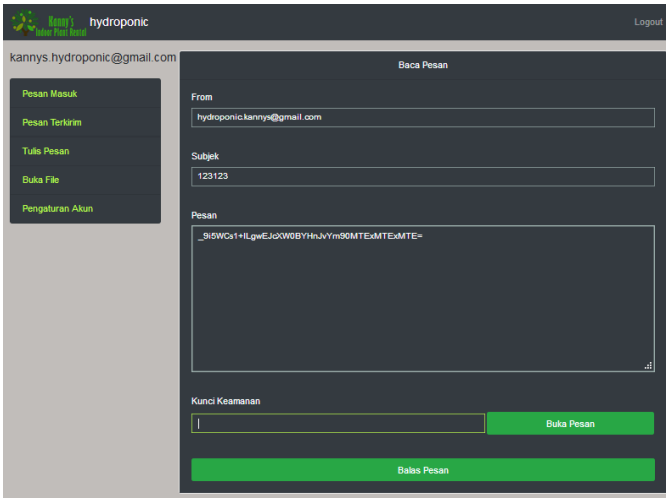
Pada proses ini *user* melakukan pengiriman pesan email seperti biasa dengan memasukkan 8 karakter kunci keamanan. Seperti pada gambar berikut:



Gambar 15: Tampilan Layar Proses Enkripsi

4.5 Tampilan Layar Proses Dekripsi

Jika *user* sudah meng-klik tombol Buka Kunci Keamanan dan berhasil melakukan verifikasi, maka akan muncul tombol Buka Pesan yang berfungsi untuk mendekrip isi pesan. seperti pada gambar dibawah ini:



Gambar 16: Tampilan Layar Proses Dekripsi

4.6 Kelebihan dan Kekurangan

Setelah dilakukan analisa dari hasil implementasi aplikasi, dapat ditemukan beberapa kelebihan dan kekurangan dari aplikasi ini, yaitu sebagai berikut :

1) Kelebihan

a) Aplikasi pengamanan email dengan metode RC4 dan DES untuk mengenkripsi file dan isi konten pesan ke dalam chipertext memiliki tampilan aplikasi yang sederhana sehingga memudahkan user dalam megoperasikan aplikasi.

b) Aplikasi keamanan email dengan metode RC4 dan DES untuk mengenkripsi file dan isi konten pesan ke dalam chipertext tergolong cepat dan tidak ada kendala.
c) Aplikasi pengamanan email dengan metode RC4 dan DES untuk mengdekripsi file dan isi konten pesan ke dalam plaintext tergolong cepat dan tidak ada kendala.
d) Aplikasi pengamanan email dengan metode RC4 dan DES untuk mengenkripsi file dan isi kontenpesan ke dalam chipertext tidak mengalami perubahan setelah dan sesudah dienkripsi.
e) Aplikasi pengamanan email dengan metode RC4 dan DES untuk mengdekripsi file dan isi konten pesan ke dalam plaintext tidak mengalami perubahan setelah dan sesudah didekripsi.
f) Aplikasi pengamanan email dengan metode RC4 dan DES untuk mengenkripsi file dan isi konten pesan akan dapat bermanfaat bagi Toko Hydroponic "Kannys Indoor Plant Rental" yang sifatnya rahasia dari pihak yang tidak bertanggung jawab.

2) Kekurangan

a) Aplikasi pengamanan *email* ini tidak dapat mengirim pesan dalam bentuk *plaintext*
b) Kunci Keamanan yang digunakan dalam Aplikasi pengamanan *email* ini diharuskan 8 karakter
c) Batas ukuran *file attachment* yaitu 25MB.
d) Tipe *file attachment* yang digunakan dalam aplikasi ini adalah *file* dengan ekstensi : **.doc*, **.jpeg*, **.png*, **.pst*, **.pptx*, **.docx*, **.pdf*, **.xls*, dan **.xlsx*.

5. KESIMPULAN

Berdasarkan hasil analisa yang telah saya lakukan terhadap permasalahan dan aplikasi yang dikembangkan, maka dapat ditarik suatu kesimpulan, sebagai berikut:

a. Dengan adanya aplikasi kriptografi menggunakan metode *Rivest Code 4* (RC4) dan *Data Encyption Standard* (DES) ini dapat mengamankan dokumen penting atau informasi yang ada di Toko Hydroponic "Kannys Indoor Plant Rental" supaya dapat lebih aman kerahasiaannya dari orang-orang yang tidak bertanggung jawab.
b. Aplikasi ini juga dapat mengembalikan data yang sudah diamankan kriptografi menggunakan metode *Rivest Code 4* (RC4) dan *Data Encyption Standard* (DES) menjadi data aslinya.
c. Aplikasi ini juga mudah digunakan.

DAFTAR PUSTAKA

[1] Donny Ariyus, *Kriptografi Keamanan Data Dan Komunikasi*, Yogyakarta: Graha Ilmu, 2006.
[2] Donny Ariyus, *Pengantar Ilmu Kriptografi Teori, Analisis, dan Implementasi*, Yogyakarta: C.V Andi OFFSET, 2008.
[3] Donny Ariyus, *Keamanan Multimedia*, Yogyakarta: Andi Publisher, 2009.
[4] R. F. Churchhouse, *Codes And Ciphers: Julius Caesar, The Enigma And The Internet*, United Kingdom: The Press Syndicate Of The University Of Cambridge, 2004.
[5] Reza Fahlevi, *Perancangan Aplikasi Email – Recaiver Dengan Menerapkan Metode Secure Socket Layer*, Jurnal Pelita Informatika STMIK Budi Darma, Vol. VII, No. 3, 2301-9425, 2014.
[6] Horst Feistel, *Cryptography and Computer Privacy*, Scientific American, Vol. 228, No. 5, pp. 15-23, 1973.
[7] Rudy Hendrayanto, and A. Ramadona Nilawati, *Program Aplikasi Enkripsi dan Dekripsi SMS Pada Ponsel Berbasis Android Dengan Algoritma DES*, Prosiding Seminar Ilmiah Nasional Komputer dan Sistem Intelijen (KOMMIT 2012) Universitas Gunadarma Vol. 7, 2302-3740, 2012.
[8] Sentot Kromodimoeljo, *Teori dan Aplikasi Kriptografi*, Jakarta: SPK IT Consulting, 2010.
[9] J. Alfred Menezes, Paul C. Van Oorschot, and Scott A. Vanstone, *Handbook of Applied Cryptography*, Boca Raton: CRC Press, 1996.
[10] Rinaldi Munir, *Kriptografi*, Bandung: Informatika Bandung, 2006.
[11] Nurcahyo Budi Nugroho, Zulfian Azmi, and Saiful Nur Arif, *Aplikasi Keamanan Email Menggunakan Algoritma RC4*, Jurnal SAINTIKOM, Vol.15, No. 3, 1978-6603, 2016.
[12] Henri Pandiangan, and Salomo Sijabat, *Perancangan Media Pengiriman Pesan Teks Dengan Penyandian Pesan Menggunakan Algoritma RC4 Berbasis Web*, Jurnal Matik Penusa Vol. 19 No. 1, 2088-3943, 2016.
[13] Mico Pardosi, *Email Gratis Yahoo ! Indonesia*, Surabaya: Dua Selaras, 2006.
[14] Rifkie Primartha, *Penerapan Enkripsi Dan Dekripsi File Menggunakan Algoritma Data Encryption Standard (DES)*, Jurnal Sistem Informasi (JSI), Vol. 3, No. 2, 2355-4614, 2011.
[15] W. Winston Royce, *Managing The Development of Large Software Systems*, Los Angeles: Proc. IEEE WESCON, 1970.
[16] B. Schneier, *Applied Cryptography – Protocol, Algorithms, and Source Code in C Second Edition*, New York: John Wiley & Sons, Inc, 1996.
[17] Ernita Sitohang, *Perangkat Aplikasi Keamanan Data Text Menggunakan Electronic Codebook Dengan Algoritma DES*, Jurnal Pelita

Informatika STMIK Budi Darma, Vol.V, No. 3, 2301-9425, 2013.

[18] W. Stallings, *Cryptography and Network Security Principles and Practices Fourth Edition*, New Jersey: Prentice Hall, 2005.