APLIKASI PENGAMANAN SURAT ELEKTRONIK (EMAIL) MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION STANDARD 128 (AES-128) DAN RIVEST CIPHER CODE 4 (RC4) BERBASIS WEB

Rauf Riyantono[1)], **Wahyu Pramusinto**[2)]
[1]Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
[1,2]Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
E-mail : raufriyantono83@gmail.com[1)], wahyu.pramisinto@budiluhur.ac.id[2)]

Abstrak

Klinik Cahaya Madani merupakan suatu instansi pelayanan kesehatan yang melayani pemeriksaan Gigi dan Umum oleh Dokter yang meliputi diagnose dan pengobatan. Klinik Cahaya Madani memiliki fasilitas berupa layanan pemeriksaan Gigi dan Umum. Dalam kegiatan operasional klinik, Klinik Cahaya Madani sering kali menggunakan surat elektronik (e-mail) untuk mengirim laporan berkala mengenai kegiatan yang berhubungan dengan penggunaan obat-obatan psikotropika dan narkotika, laporan data obat, data pasien serta rekam medik pasien. Untuk itu diperlukan pengamanan file yang dikirimkan melalui surat elektronik (e-mail) agar tidak dapat diakses oleh pihak yang tidak bertanggung jawab. Salah satu cara megamankan dokumen rahasia di surat elektronik (e-mail) tersebut adalah dengan menggunakan teknik kriptografi. Tujuan dari penelitian aplikasi ini adalah menghasilkan aplikasi enkripsi surat elektronik (e-mail) berbasis web yang dapat mengamankan dokumen rahasia di surat elektroni (e-mail) yang ada di Klinik Cahaya Madani, mudah dimengerti dan digunakan oleh pengguna serta memberikan kontribusi ilmu pengetahuan di bidang ilmu komputer khususnya topik keamanan komputer. Teknik kriptografi yang penulis gunakan adalah metode Advanced Encryption Standard (AES) dan Rivest Cipher 4 (RC4) Aplikasi ini dibangun dengan metode Waterfall, pada tahap pembangunan aplikasi ini menggunakan bahasa pemograman php berbasis web dengan menggunakan database MySQL.

Kata kunci: E-mail, *Advanced Encryption Standard* (AES), *Rivest Cipher* 4 (RC4)

1. PENDAHULUAN

1.1. LATAR BELAKANG

Klinik Cahaya Madani merupakan suatu instansi pelayanan kesehatan yang melayani pemeriksaan Gigi dan Umum oleh Dokter yang meliputi diagnose dan pengobatan. Dalam kegiatan operasional Klinik Cahaya Madani sering kali menggunakan surat elektronik (*e-mail*) untuk mengirim laporan berkala mengenai kegiatan yang berhubungan dengan penggunaan obat-obatan psikotropika dan narkotika, laporan data obat serta rekam medik pasien ke dokter. Dokumen tersebut dikirim oleh apoteker kepada dokter. Dokumen tersebut adalah dokumen rahasia karena berhubungan dengan kegiatan operasional Klinik Cahaya Madani dan pengobatan pasien sehingga diperlukan pengamanan dokumen yang dikirimkan melalui surat elektronik (*e-mail*) agar tidak dapat diakses oleh pihak yang tidak bertanggung jawab. Aplikasi surat elektronik (*e-mail*) pada dasarnya sudah aman karena memiliki *password*, namun jika *password user* di*hack* maka *hacker* bisa masuk ke surat elektronik (*e-mail*) atau kadang *user* lupa keluar dari surat elektronik (*e-mail*) sehingga isi surat elektronik (*e-mail*) bisa diakses oleh orang lain, sehingga diperlukan aplikasi pengamanan dokumen di surat elektronik (*e-mail*) yang memiliki dua pengamanan *password* dan dokumen yang telah terenkripsi. Berdasarkan uraian di atas penulis bermaksud untuk membuat suatu aplikasi untuk menyimpan dan mengamankan dokumen dan pesan yang akan dikirim dengan megimplementasikan metode Algoritma AES (*Advanced Encryption Standard*) 128 dan RC4 (*Rivest Cipher*) pada aplikasi pengamanan dokumen dan pesan dengan memanfaatkan fitur surat elektronik (*e-mail*) berbasis *Web*.

1.2. RUMUSAN MASALAH

Rumusan masalah yang akan dibahas adalah Bagaimana mengimplementasikan Algoritma AES (*Advanced Encryption Standard*) 128 dan RC4 (*Rivest Cipher*) kedalam aplikasi pengiriman *email*. Bagaimana cara melakukan

pengamanan terhadap informasi atau pesan yang dikirim atau diterima melalui media *email* sehingga informasi tersebut bisa terjaga keamanannya?

1.3. TUJUAN PENELITIAN

Mengamankan dokumen dan pesan yang dikirim atau diterima melalui surat elektronik (*e-mail*) pada Klinik Cahaya Madani agar tidak dapat diketahui oleh orang yang tidak bertanggung jawab dalam satu aplikasi dengan algoritma AES (*Advanced Encryption Standard*) 128 dan RC4 (*Rivest Cipher*). Menghasilkan aplikasi enkripsi surat elektronik (*e-mail*) berbasis *web* yang diharapkan mudah dimengerti dan digunakan oleh pengguna**.**

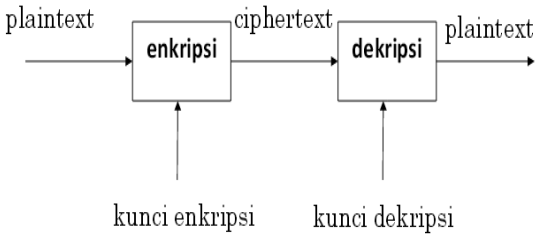
2. LANDASAN TEORI

2.1. KRIPTOGRAFI

Kriptografi berasal dari bahasa Yunani, menurut bahasa berasal dari dua kata yaitu kripto dan graphia. Kripto berarti *secret* (rahasia) dan *graphia* berarti *writing* (tulisan). Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain [2].

2.2. KRIPTOGRAFI SIMETRIS

Algoritma Simetri adalah salah satu jenis kunci pada algoritma kriptografi yang menggunakan kunci enkripsi yang sama dengan kunci dekripsinya. Bila mengirim pesan dengan menggunakan algoritma ini, si penerima pesan harus diberitahu kunci dari pesan tersebut agar bisa mendekripsikan pesan yang dikirim. Keamanan dari pesan yang digunakan algoritma ini tergantung pada kunci. Jika kunci tersebut diketahui oleh orang lain maka orang tersebut akan dapat melakukan enkripsi dan dekripsi terhadap pesan. Algoritma yang memakai kunci simetri seperti Data Encryption Standar (DES), RC2, RC4, RC5, RC6, International Data Encryption Algorithm (IDEA), Advanced Encryption Standard (AES), dan lain sebagainya.



Gambar 1. Skema Proses Kriptografi Simetris[2]

Plaintext P dienkripsi dengan kunci privat K menghasilkan fungsi $E_K(P) = C$ dimana C merupakan *ciphertext* hasil enkripsi *plaintext* P. Proses dekripsi *ciphertext* C memerlukan kembali kunci privat K untuk mendapatkan kembali *plaintext* dengan fungsi $D_K(C) = P$. [4]

2.3. ALGORITMA AES (*Advanced Encryption Standard*)

Advanced Encryption Standard (AES) dipublikasikan oleh NIST (National Institute of Standard and Technology) pada tahun 2001 yang digunakan untuk menggantikan algortima DES yang semakin lama semakin mudah untuk dibobol. AES diperoleh dari hasil kompetisi yang diadakan NIST tahun 1997. Pada tahap pertama 15 peserta dari 21 peserta lolos ke tahap erikutnya berdasarkan penilaian tingkat keamanan, harga, algortima dan karakteristik implementasi. Sepuluh dari 15 peserta tersebut gugur pada tahap berikutnya karena dianggap kurang aman dan efektif. Pada Agustus 1999 dipilih lima kandidat dari tahap seleksi akhir, yaitu MARS (IBM, Amerika Serikat), RSA (RSA corp., Amerika Serikat), Rijndael (Belgia), Serpent (Israel, Norwegia, Inggris), dan Twofish (Counterpane, Amerika Serikat). Pada tahap ini NIST memberikan penilaian pada general security, implementasi software dan hardware, ruang lingkup, implementasi atas serangan, enkripsi dan dekripsi, kemampuan kunci, dan kemampuan lain seperti fleksibilitas dan kepotensialan untuk tingkat instruksi paralel. Akhirnya, 2 Oktober 2000 terpilihlah algoritma Rijndael yang dibuat oleh Dr. Vincent Rijment dan Dr. Joan Daemen sebagai pemenang. Algoritma ini termasuk jenis simetri yang disebut juga sebagai algoritma konvensional, yaitu algoritma yang menggunakan kunci enkripsi dan kunci dekripsi yang sama. AES menggunakan sandi blok kunci simetrik dengan ukuran kunci bervariasi, yaitu 128 bit, 192 bit, dan 256 bit. Pemerintah Amerika Serikat telah mengadopsi AES sebagai standar enkripsi. Standar ini terdiri dari 3 blok cipher, yaitu AES-128, AES-192, dan AES256 yang diadopsi dari koleksi yang lebih besar yang awalnya diterbitkan sebagai Rijndael. AES telah dianalisis secara luas dan sekarang digunakan di seluruh dunia, seperti halnya dengan pendahulunya, Data Encryption Standard (DES) [6].

2.4. RC4 (*Rivest Cipher 4*)

Algoritma RC4 adalah algoritma kriptografi simetrik. Disebut algoritma kriptografi simetrik karena menggunakan kunci yang sama untuk mengenkripsi ataupun mendekripsi suatu pesan, data, ataupun informasi. Kunci enkripsi didapat dari sebuat 256 bit *state-array (KSA)* yang diinisialisasi dengan sebuah *key* tersendiri dengan panjang 1-256 bit. Setelah itu, *state-array* tersebut akan diacak kembali dan diproses untuk menghasilkan sebuah kunci enkripsi yang akan di-XOR-kan dengan plainteks ataupun cipherteks. Secara umum, algoritma RC4 terbagi menjadi dua, inisalisasi *state-array* dan penghasilan kunci enkripsi serta pengenkripsiannya[6].

2.5. SURAT ELEKTRONIK (E-MAIL)

Electronic mail (surat elektronik, *e-mail*) adalah sebuah metode menggubah, mengirim, menyimpan, dan menerima pesan melalui sistem komunikasi elektronik. Istilah *e-mail* meliputi sistem yang berdasar pada *Simple Mail Transfer Protocol* (SMTP) dan sistem intranet yang memungkinkan pengguna dalam satu organisasi mengirimkan pesan kepada satu sama lain. Seringkali kelompok organisasi tersebut menggunakan *internet protocol* sebagai layanan *e-mail* internal. Format dari sebuah pesan *e-mail* dari internet didefinisikan di RFC 2822 dan seri dari RFC yang secara keseluruhan disebut sebagai *Multipurpose Internet MailExtensions* (MIME)

3. ANALISA MASALAH DAN RANCANGAN LAYAR

3.1. ANALISA MASALAH

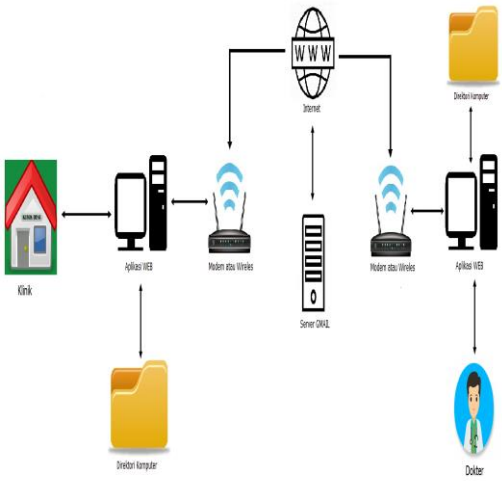
Pada Klinik Cahaya Madani keamanan data di dalam pengiriman dan penerimaan data sangat penting untuk menjamin bahwa data yang dikirim tidak jatuh ke pihak yang tidak berwenang, terutama jika data tersebut bersifat sangat rahasia. Namun data-data tersebut bisa dengan mudah jatuh ke pihak ketiga bila pihak ketiga dapat melihat setiap data yang dikirim atau diterima pihak pertama, pihak pertama disini adalah dokter Klinik Cahaya Madani. Keamanan data di *e-mail* tidaklah terjamin karena data selalu ada resiko yang terbuka untuk umum, dalam sebuah artian semua isinya dapat dibaca oleh orang yang tidak berkepentingan. Hal ini disebabkan karena *e-mail* itu akan melewati *server* sebelum sampai tujuan. Dan tidak tertutup kemungkinan ada orang yang menyadap *e-mail* yang dikirimkan tersebut. Untuk itu perlu dilakukan implementasi kriptografi pengamanan data pada *e-mail* untuk menjaga kerahasiaan dokumen laporan.

3.2. PENYELESAIAN MASALAH

Berdasarkan analisa diatas maka penulis telah melakukan evaluasi untuk menjaga keamanan pasan teks agar isi pesan tersebut tetap utuh kepada penerima. Yaitu dengan menggunakan aplikasi kriptografi. Aplikasi kriptografi tersebut dapat menenkripsi dan mendekripsi pesan teks dengan beberapa metode yang dapat diterapkan. Dari banyaknya metode yang ada, penulis menggunakan metode Algoritma AES 128 *(Advanced Encryption Standard)* dan RC4 *(Rivest Cipher 4)*. Karena pada metode Algoritma AES 128 *(Advanced Encryption Standard)* dan RC4 *(Rivest Cipher 4)*.

3.3. ARSITEKTUR SISTEM

Aplikasi ini menghubungkan apotek dengan pemilik dan bersifat dua arah,dimana pemilik atau apotek dapat menerima dan mengirim pesan terenkripsi. Dapat dilihat pada gambar 2 dokumen yang berasal dari direktori komputer apotek yang bersifat rahasia seperti data obat, data pasien dan rekam medis pasien yang telah di enkripsi melalui aplikasi web yang memanfaatkan fitur email kepada pemilik, yang selanjutnya pemilik akan menerimanya dan mendekripsikan pesan terenkripsi dengan aplikasi yang sama.



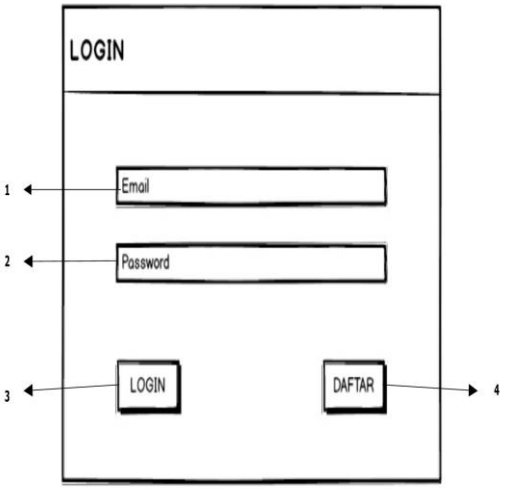
Gambar 2. Arsitektur Sistem

3.4. RANCANGAN LAYAR

Rancangan layar merupakan rancangan masukan atau rancangan input pada layar komputer dengan model dan fungsi yang tertata dengan baik sehingga mengurangi kesalahan pada saat memasukkan data. Rancangan layar merupakan suatu hal yang penting dalam membangun suatu aplikasi. Tampilan yang dibuat haruslah menarik, tidak membingungkan dan mudah dimengerti

3.5. RANCANGAN LAYAR FORM LOGIN

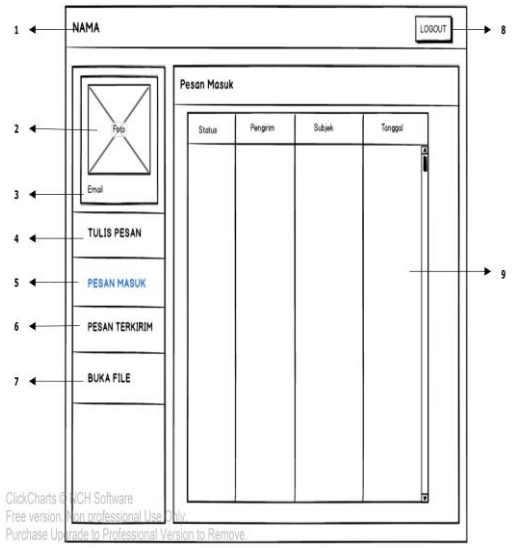
Rancangan layar form *login* merupakan *form* awal ketika *user* membuka aplikasi. *User* akan diminta untuk memasukkan *Gmail address* dan *password* sebelum mengakses *form* menu home. Berikut adalah rancangan layar *form login.*



Gambar 3. Rancangan layar form login

3.6. RANCANGAN LAYAR FORM PESAN MASUK

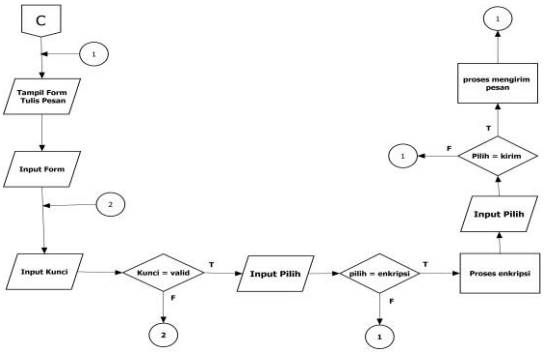
Form ini akan muncuk jika user mengklik tombol pesan masuk. Form ini digunakan untuk melihat pesan yg diterima user. Disini user dapat memilih pesan yang iningn dibaca.



Gambar 4. Pesan Masuk

3.7. FLOWCHART PROGRAM

Flowchart ini menjelaskan alur proses *form* Tulis Pesan. Pada proses ini *user* bisa membuat pesan baru dan mengirimkan kepada penerima. *User* juga dapat menuliskan isi konten pesan dan melampirkan *file* lalu mengenkripsikannya.



Gambar 5. Flowchart Program

3.8. ALGORITMA ALUR PROSES

Flowchart ini menjelaskan alur proses saat kita mengklik menu pesan masuk. Pada *form* ini *user* bisa memilih salah satu pesan untuk membukanya, dan di menu pesan ini terdiri dari pesan terkirim dan pengaturan akun. User dapat memilih menu yang diinginkan.

```
1.   Tampil form pesan masuk
2.   Input pilih
3.   If pilih = pesan
4.     Ke halaman baca pesan
5.   Else
6.       if pilih = pengaturan akun then
7.       Ke halaman pesan terkirim
8.       Else
9.           if pilih = pengaturan akun then
10.          Ke halaman pengaturan akun
11.          Else
12.            Kembali ke baris 1
13.          End if
14.      End if
15.  End if
16.  End
```

4. HASIL DAN PEMBAHASAN

4.1. TAMPOLAN LAYAR HALAMAN LOGIN

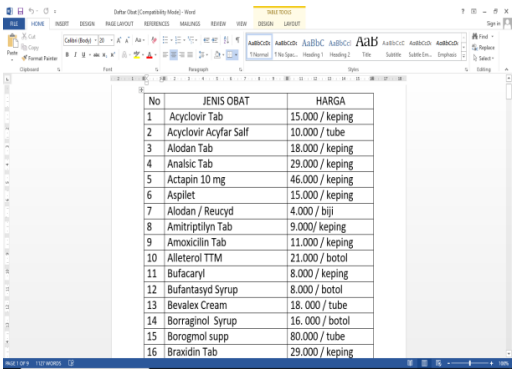
Tampilan layar halaman *login* merupakan layar yang menjadi penghubung ke halaman utama. Berikut adalah gambar tampilan layar halaman *login*

Gambar 6. Form login

4.2. UJI COBA PROGRAM

Dalam pengujian aplikasi ini, dilakukan pengujian terhadap hasil dari proses enkripsi file dan dekripsi file berformat docx.dan xlsx.

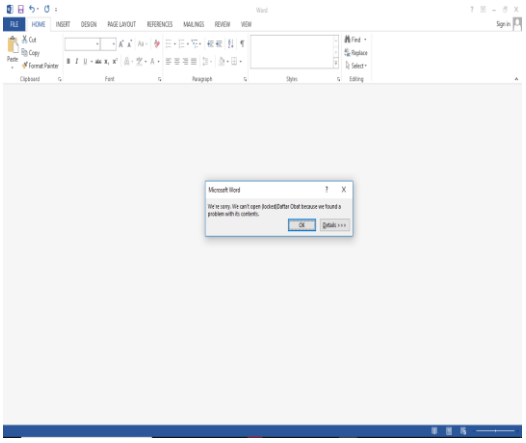
4.3. FILE FORMAT DOCX



No	JENIS OBAT	HARGA
1	Acyclovir Tab	15.000 / keping
2	Acyclovir Acyfar Salf	10.000 / tube
3	Alodan Tab	18.000 / keping
4	Analsic Tab	29.000 / keping
5	Actapin 10 mg	46.000 / keping
6	Aspilet	15.000 / keping
7	Alodan / Reucyd	4.000 / biji
8	Amitriptilyn Tab	9.000/ keping
9	Amoxicilin Tab	11.000 / keping
10	Alleterol TTM	21.000 / botol
11	Bufacaryl	8.000 / keping
12	Bufantasyd Syrup	8.000 / botol
13	Bevalex Cream	18. 000 / tube
14	Borraginol Syrup	16. 000 / botol
15	Borogmol supp	80.000 / tube
16	Braxidin Tab	29.000 / keping

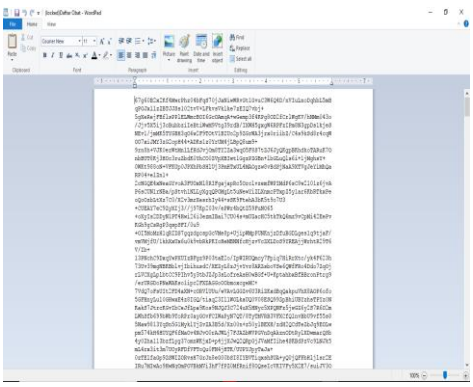
Gambar 7. Tampilan Isi File Format docx

Setelah *file* Word di enkripsi maka *file* tidak dapat dibuka kembali dan akan muncul pesan *error*.



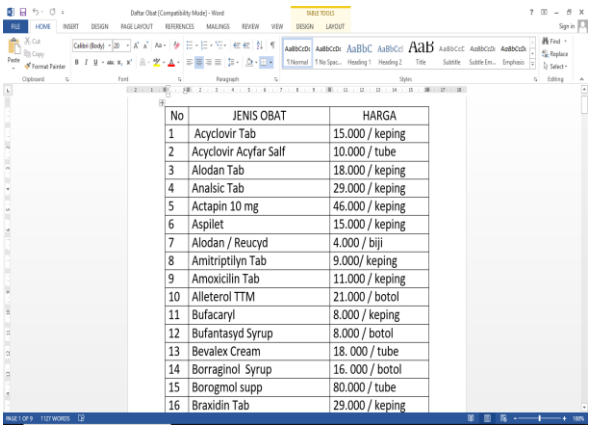
Gambar 8. Pesan Error File Format Docx Setelah Di Enkripsi

Jika file docx yang telah dienkripsi tersebut dibuka menggunakan wordpad



Gambar 9 File Docx Setelah Di Enkripsi dan di Buka Dengan Wordpad

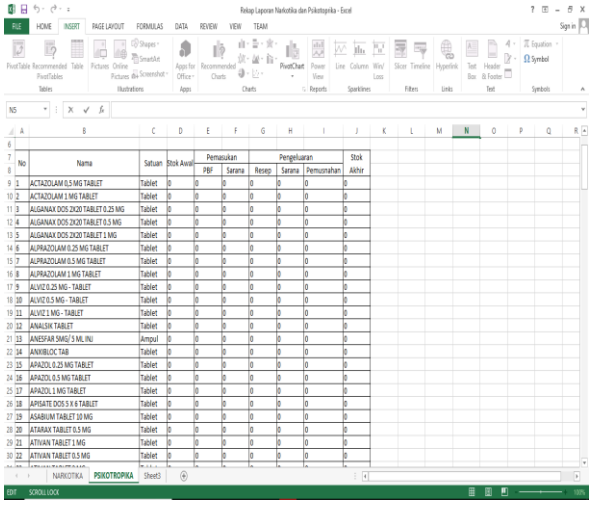
Agar *file* yang sudah di enkripsi dapat dibuka kembali menjadi *file* asli maka harus dilakukan proses dekripsi *file*. Hasil dari *file* dekripsi



No	JENIS OBAT	HARGA
1	Acyclovir Tab	15.000 / keping
2	Acyclovir Acyfar Salf	10.000 / tube
3	Alodan Tab	18.000 / keping
4	Analsic Tab	29.000 / keping
5	Actapin 10 mg	46.000 / keping
6	Aspilet	15.000 / keping
7	Alodan / Reucyd	4.000 / biji
8	Amitriptilyn Tab	9.000/ keping
9	Amoxicilin Tab	11.000 / keping
10	Alleterol TTM	21.000 / botol
11	Bufacaryl	8.000 / keping
12	Bufantasyd Syrup	8.000 / botol
13	Bevalex Cream	18. 000 / tube
14	Borraginol Syrup	16. 000 / botol
15	Borogmol supp	80.000 / tube
16	Braxidin Tab	29.000 / keping

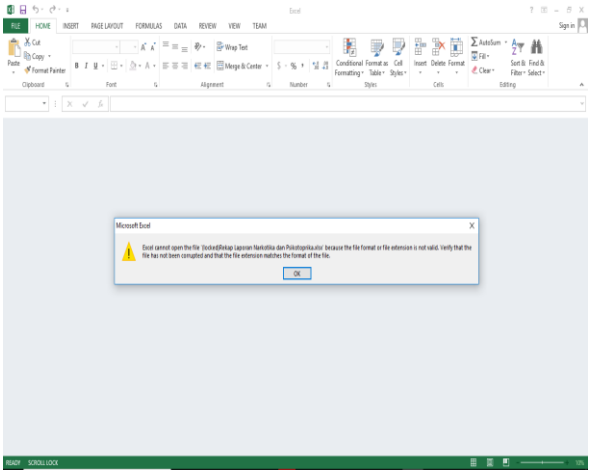
Gambar 10. File Format docx Hasil Dekripsi

4.4. FILE FORMAT XLSX



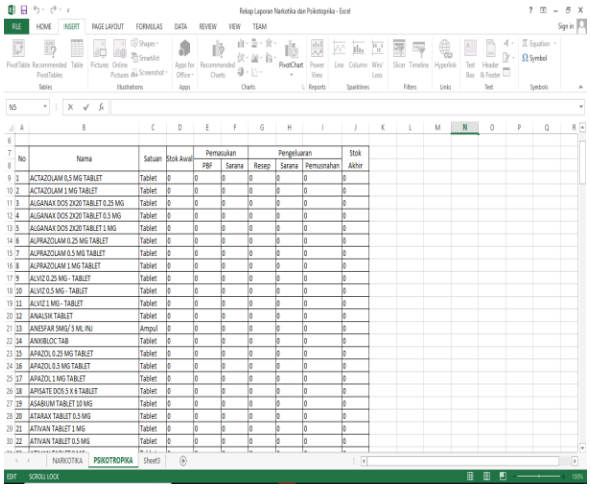
Gambar 11. Tampilan Isi File Format xlsx

Setelah *file* Excel di enkripsi maka *file* tidak dapat dibuka kembali dan akan muncul pesan *error*



Gambar 12. Pesan Error File Format Docx Setelah Di Enkripsi

Agar *file* yang sudah di enkripsi dapat dibuka kembali menjadi *file* asli maka harus dilakukan proses dekripsi *file*



Gambar 13. File Format xlsx Hasil Dekripsi

4.5. TABEL PENGUJIAN

Dalam pengujian kali ini dibahas perbandingan antar proses enkripsi dan dekripsi *file*. *File* yang diuji adalah jenis *file* yang berformat docx dan xlsx. Pengujian ini dilakukan untuk melihat perbandingan antara ukuran *file* asli dan ukuran *file* setelah di lakukan enkripsi serta waktu proses pada saat enkripsi dan waktu proses dekripsi.

Tabel 1. Hasil Enkripsi dan Dekripsi File

5. KESIMPULAN

Nama File	Ukuran file		
	Asli	Enkripsi	Dekripsi
Daftar obat.docx	19 kb	26 kb	19 kb
Laporan narkotika.xlsx	11 kb	15 kb	11 kb
Laporan Psikotropika.xlsx	17 kb	22 kb	17 kb
Enzim.docx	35 kb	46 kb	35 kb
SOH.docx	31 kb	418 kb	31 kb

Setelah melalui proses pembuatan dan pengujian dalam penelitian ini, maka dapat diberikan kesimpulan, antara lain:

a. Dengan adanya aplikasi kriptografi menggunakan metode *Advanced Encryption Standard* (AES) dan *Rivest Cipher 4* (RC4) ini dapat mengamankan dokumen penting atau informasi yang ada di Klinik Cahaya Madani agar dapat lebih aman kerahasiaannya dari orang-orang yang tidak bertanggung jawab.
b. Teknik kriptografi dengan metode *Advanced Encryption Standard* (AES) dan *Rivest Cipher 4* (RC4) pada aplikasi mengamanan dokumen data obat dan data lapora narkotika, psikotropika yang akan dikirim dengan memanfaatkan media surat elektronik (*e-mail*) berbasis web berhasil di implementasikan pada Klinik Cahaya Madani.
c. Aplikasi ini juga dapat mengembalikan data yang sudah diamankan kriptografi menggunakan metode *Advanced Encryption Standard* (AES) dan *Rivest Cipher 4* (RC4) menjadi data yang orisinil tanpa mengalami perubahan sedikitpun.
d. Aplikasi ini juga mudah digunakan oleh banyak pengguna.
e. Waktu untuk mengenkripsi pesan berbanding lurus dengan ukuran teks dan ukuran file yang akan dienkripsi, semakin kecil ukuran teks dan *file* nya maka semakin cepat waktu pengenkripsiannya.

Beberapa saran yang dapat diberikan untuk pengembangan aplikasi dengan harapan menghasilkan penelitian yang lebih baik lagi selanjutnya, berikut saran yang dapat diberikan:

a. Aplikasi ini hanya dapat menyisipkan file *.docx, *.xlsx dan untuk itu kedepannya perlu dikembangkan untuk menambahkan *file extension* lainnya.
b. Fitur masih sangat sederhana diharapkan dapat ditambahkan beberapa fitur seperti drafts , forward, spam dan starred.
c. Dalam pengembangannya, aplikasi ini dapat menggunakan metode kompresi sehingga ukuran file yang dienkripsi dapat lebih diminimalisir

6. DAFTAR PUSTAKA

[1]. Agung, H. & Ferry, 2016. *Kriptografi Menggunakan Hybrid Cryptosystem dan Digital Signature*. , 2016(x), pp.34–45.

[2]. Ariyus, Donny 2008, *Pengantar Ilmu Kriptografi Teori, Analisis, dan Implementasi*, Yogyakarta: C.V Andi Offset.

[3]. Kromodimoeljo, Sentot 2010, *Teori dan Aplikasi Kriptografi*, Jakarta: SPK IT Consulting.

[4]. Munir, Rinaldi, 2006, *Kriptografi*, Bandung: Informatika.

[5]. Pandiangan, H. & Sijabat, S., 2016. *Perancangan Media Pengiriman Pesan Teks Dengan Menggunakan Algoritma RC4 Berbasis Web*. , 19(1), pp.63–71.

[6]. Primartha, R., 2013. *Penerapan Enkripsi dan Deskripsi File Menggunakan Algoritma Advanceb Encrypyion Standard (AES).* , 2(1), pp.13–18.