CryptMAIL: Keamanan Ganda *Email* Menggunakan Algoritma Kriptografi

http://dx.doi.org/10.28932/jutisi.v8i2.4962

Riwayat Artikel
Received: 19 Juni 2022 | *Final Revision*: 27 Juli 2022 | *Accepted*: 2 Agustus 2022

Virra Retnowati A'izzah[#1], Dwi Ramti Asih[#2], Anggi Putri Meriani[#3], Alam Rahmatulloh[✉#4]

[#] *Informatika, Universitas Siliwangi*
Jl. Siliwangi No.24, Kahuripan, Tasikmalaya, 46115, Indonesia
[1]207006020@student.unsil.ac.id
[2]207006029@student.unsil.ac.id
[3]207006068@student.unsil.ac.id
✉Corresponding author: alam@unsil.ac.id

Abstrak **— Perkembangan teknologi dan informasi mengubah cara manusia dalam berkomunikasi. Email merupakan salah satu layanan surat menyurat secara online yang memudahkan pengguna dalam pertukaran informasi maupun berkomunikasi dengan pihak lain. Kemudahan yang ditawarkan menarik banyak orang untuk beralih menggunakan email sebagai media bertukar informasi, dan ini menjadikan peluang baru bagi *cybercriminals* untuk melakukan aksinya. Masalah pada email seperti kebocoran data atau informasi, penyalahgunaan *file* atau pencurian pesan karena kelalaian ataupun lainnya dapat terjadi. Salah satu cara untuk mengantisipasi hal tersebut adalah dengan mengimplementasikan Teknik Kriptografi. Kriptografi adalah sebuah Teknik enkripsi untuk menyembunyikan pesan *confidential* dari pesan *plaintext* menjadi pesan *chipertext* yang sulit dipahami. Dalam penelitian ini akan membahas tentang Implementasi kriptografi dengan algoritma AES-128 dan RC4 untuk enkripsi dan dekripsi pesan serta *file attachment* yang dikirim melalui email. Hasil penelitian ini adalah aplikasi berbasis web 'CryptMAIL' yang dapat mengenkripsi dan dekripsi pesan menggunakan algoritma kriptografi AES-128 dan RC4. Aplikasi 'CryptMAIL' ini diharapkan dapat memberikan keamanan ganda untuk mengantisipasi masalah keamanan pada email.**

Kata kunci— **AES-128; Email; Kriptografi; RC4.**

CryptMAIL: Multiple Email Security Using Cryptography Algorithms

Abstract ***— The development of technology and information has changed the way humans communicate. Email is an online correspondence service that makes it easier for users to exchange information and communicate with other parties. The convenience offered attracts many people to switch to using email as a medium for exchanging information, and this creates new opportunities for cybercriminals to take action. Problems with email such as data or information leaks, file misuse, or message theft due to the negligence of others can occur. One way to anticipate this is to implement Cryptographic Techniques. Cryptography is an encryption technique to hide confidential messages from plaintext messages into ciphertext messages that are difficult to understand. In this study, we will discuss the implementation of cryptography with the AES-128 and RC4 algorithms for the encryption and decryption of messages and file attachments sent via email. The result of this research is a web-based application 'CryptMAIL' that can encrypt and decrypt messages using the AES-128 and RC4 cryptographic algorithms. The 'CryptMAIL' application is expected to provide double security to anticipate security problems in email.***

Keywords— ***AES-128; Cryptography; Email; RC4.***

I. PENDAHULUAN

Saat ini seperti yang sudah diketahui merupakan zamannya revolusi industri 4.0, yang mana sudah tidak menjadi hal yang asing lagi bagi segala macam bidang teknologi dan informasi dapat dengan mudahnya diakses dan berkembang begitu pesat pula. Hal ini tentunya memungkinkan seluruh entitas didalamnya untuk dapat saling berkomunikasi kapan saja secara *realtime*. Perkembangan tersebut tentunya merubah kehidupan manusia secara tidak langsung. Salah satunya perkembangan internet jejaring media sosial sebagai sarana bertukar informasi maupun berbalas pesan. Dengan demikian adanya media sosial sangatlah memudahkan berbagai kalangan manusia di seluruh penjuru dunia untuk menciptakan dan melakukan berbagai pertukaran konten seperti pada saat yang terjadi sekarang ini [1].

Pandemi COVID19 yang mewabah selama 2 tahun ini berangsur-angsur menurun dan saat ini berada pada fase endemi. Namun, di beberapa bidang terutama di bidang pendidikan, pembelajaran masih dilakukan secara daring melalui media sosial dan sebagian tatap muka terbatas [2].

Salah satu media yang digunakan oleh pelajar maupun instansi pemerintah dan swasta adalah "Email". Email adalah salah satu layanan yang digunakan untuk berbalas pesan maupun bertukar informasi secara modern dan *realtime*. *Gmail* dan *Yahoo mail* merupakan platform email yang banyak dipakai saat ini [3]. Kemudahan yang ditawarkan kedua platform ini adalah waktu pengiriman yang cukup singkat dan efisien selain itu terdapat pula fitur yang memudahkan penggunanya agar dapat mengirimkan pesan ke beberapa orang yang dituju dalam sekali pengiriman. Tetapi dengan adanya kemudahan pasti disertai dengan adanya risiko, salah satunya dalam risiko aspek keamanan. Terkadang, pesan elektronik yang dikirim oleh pihak pengirim merupakan pesan *confidential* yang hanya boleh diketahui oleh beberapa pihak dengan otoritasnya. Namun, jika terjadi kesalahan pada penulisan alamat email yang dituju maka akan terjadi kebocoran data atau informasi yang dapat dibuka dan dibaca oleh orang yang tidak memiliki otoritasnya.

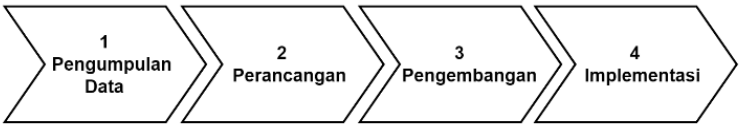
Guna mengantisipasi kesalahan tersebut, sangat penting untuk memperhatikan keamanan sistem informasi pada email. Kurangnya perhatian pada keamanan dari pengguna maupun penyedia jasa menjadi kesalahan fatal. Langkah pencegahan (*prevention*) merupakan salah satu metode dalam pengamanan data selain pengobatan (*recovery*) yang dapat dilakukan untuk meningkatkan keamanan informasi pada email dengan enkripsi data menggunakan teknik kriptografi email dengan algoritma AES-128 dan RC4. Kriptografi adalah sebuah Teknik untuk menyembunyikan pesan yang sifatnya *confidential* agar isi pesan tidak akan mudah dipahami oleh orang-orang yang tidak memiliki otoritas [4].

Penelitian ini dilakukan dengan mengambil beberapa jurnal atau penelitian terdahulu sebagai acuan dalam pengembangan aplikasi 'CryptMAIL', penelitian tersebut diantaranya adalah penelitian yang dilakukan oleh Indra R dan Pramusinto (2018), penelitian dilakukan terhadap penerapan aplikasi email menggunakan algoritma AES-128 dan RC4 berbasis web. Hasil yang didapat adalah pengamanan isi pesan email dan *file attachment* menggunakan teknik kriptografi dengan algoritma AES-128 dan RC4 mampu mengamankan pesan yang dikirim tanpa mengubah informasi yang dikirim, namun dalam pengunggahan *file* masih terbatas sehingga diharapkan pada penelitian selanjutnya dapat menerapkan ekstensi lainnya selain *docx, xls, pdf, rar* dan *zip* [5]. Penelitian lainnya adalah oleh Pramudito dan Kusumaningsih (2018). Pada penelitian ini merupakan Implementasi Algoritma AES-128 dan RC4 Untuk Pengamanan Email Pada Pt. Dinamika Hydro Engineering. Hasil dari penelitian ini adalah aplikasi pengamanan email dengan teknik kriptografi yang terjamin keamanannya dan pengembangannya masih belum adanya penambahan fitur seperti *forward email, reply email, folder trash,* dan *folder sent*. Maka diharapkan pada penelitian selanjutnya dapat menerapkan fitur-fitur tersebut [6]. Pada penelitian oleh Riyantono dan Pramusinto (2018), Penelitian ini pembuatan aplikasi untuk mengamankan surat elektronik (*email*) menggunakan algoritma AES-128 dan RC4 berbasis web pada Klinik Cahaya Madani. Hasil dari penelitiannya adalah aplikasi enkripsi surat elektronik (*email*) berbasis web yang dapat mengamankan dokumen penting yang bersifat rahasia pada Klinik Cahaya Madani dari pihak yang tidak bertanggung jawab. Aplikasi yang dihasilkan dapat mendekripsi data tanpa mengalami perubahan [7].

Dalam pengembangannya aplikasi ini menggunakan Algoritma AES-128 dan RC4. Advanced Encryption Standard (AES) merupakan algoritma *cryptographic* yang dapat digunakan untuk mengamankan data begitu pula dengan RC4. Algoritma RC4 mengenkripsi dengan mengkombinasikannya dengan plainteks dengan menggunakan bit-wise Xor (Exclusive-or) [8], [9].

Melihat permasalahan dari uraian diatas, aplikasi 'CryptMAIL' ini dimaksudkan untuk memberikan keamanan ganda, mengamankan isi pesan email dengan menggunakan teknik kriptografi, sehingga hanya orang yang bersangkutan yang dapat membaca data dan informasi yang diberikan pengirim. Dalam pengembangan aplikasi ini digunakan beberapa tahapan seperti pada Gambar 1, yaitu Pengumpulan Data, Perancangan, Pengembangan dan Implementasi.

II. METODE PENELITIAN



Gambar 1. Alur Metodologi

Dalam pengembangan aplikasi ini digunakan beberapa tahapan antara lain. Pengumpulan Data, Perancangan, Pengembangan dan Implementasi. Metode ini dipilih untuk melakukan pendekatan secara sistematis (Huang et al, 2005).

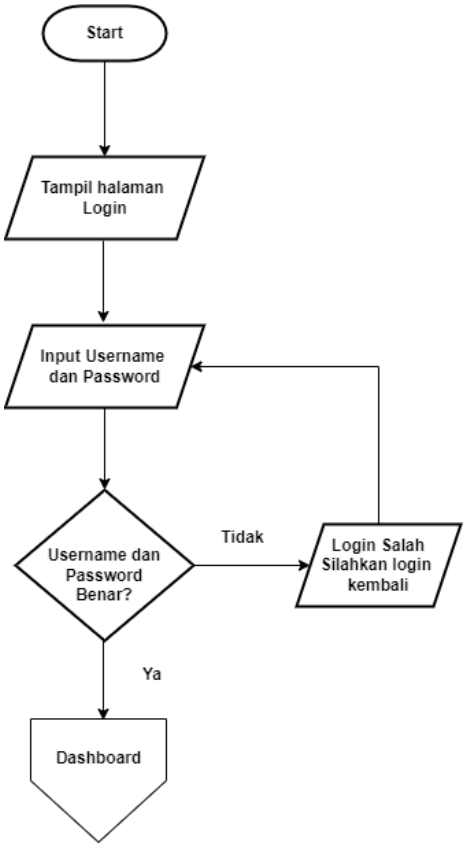
A. Pengumpulan Data

Dalam tahapan ini yang dilakukan adalah dengan cara melakukan studi literatur untuk mencari bahan yang mendukung dalam pendefinisian permasalahan melalui buku-buku ataupun internet, yang erat kaitannya dengan objek permasalahan [10]. Yang dapat digunakan sebagai acuan dalam pengembangan aplikasi yang dibuat. Maka dari itu sudah dilakukan pengumpulan beberapa jurnal sebagai contoh acuan seperti yang telah dibahas sebelumnya.

B. Perancangan

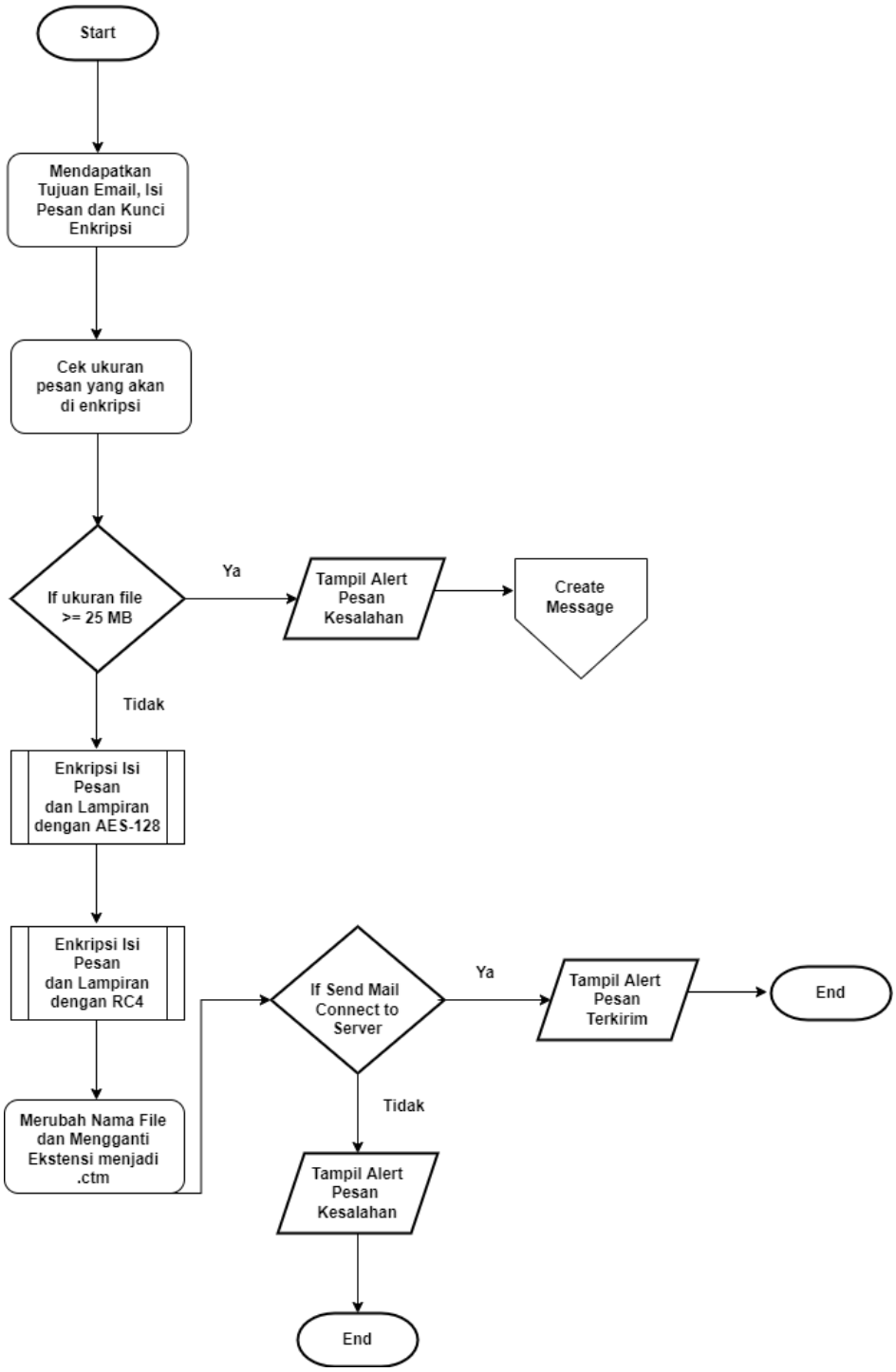
Rancangan aplikasi dimulai dari menu *log in*, kemudian setelah itu akan menampilkan *dashboard* yang berisi beberapa menu antara lain *create message, inbox, reply message, help* dan *others*. Kemudian menggunakan *Flowchart* (Alur Aplikasi) untuk mengetahui bagaimana sistem atau jalannya aplikasi secara terstruktur [11].

Rancangan yang pertama yaitu *flowchart* pada proses *log in*. Pada gambar 2 *flowchart* menggambarkan proses yang terjadi pada halaman *log in*. Jika *usermail* dan *password* yang dimasukkan benar maka akan diarahkan ke menu *dashboard*. Jika tidak maka akan dikembalikan pada tampilan halaman *log in* dan akan terdapat pesan *error*. Sehingga pengguna harus mengulang lagi memasukkan *usermail* dan *password* agar bisa *log in* ke *dashboard*.



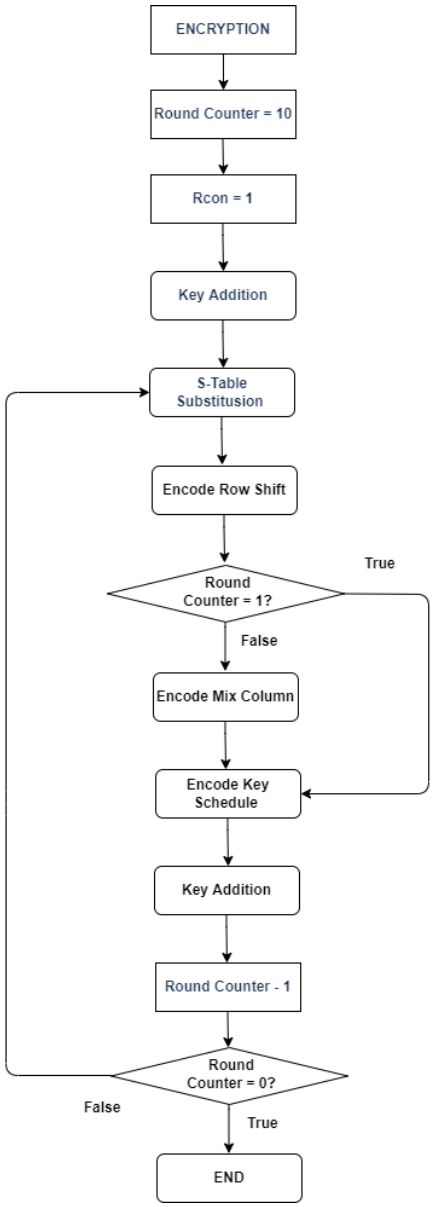
Gambar 2. *Flowchart* Proses Login

Rancangan yang kedua yaitu flowchart proses kirim email terenkripsi. Pada rancangan ini menjelaskan mengenai email yang dikodekan dari teks yang dapat dibaca ke berbagai *symbol* menggunakan kunci enkripsi, namun pada pengiriman pesannya juga harus dilihat ukuran *file* yaitu maksimal 25 MB. Setelah itu email akan dikirim ke penerima yang dituju. Adapun untuk membaca pesan, penerima mendeskripsi pesan menggunakan kunci enkripsi yang sama. Dimana pada proses ini pesan akan dienkripsi menggunakan algoritma AES-128 lalu dienkripsi lagi menggunakan algoritma RC4. Berikut rancangan prosesnya dapat dilihat pada Gambar 3.



Gambar 3. *Flowchart* Proses Kirim Email Terenkripsi

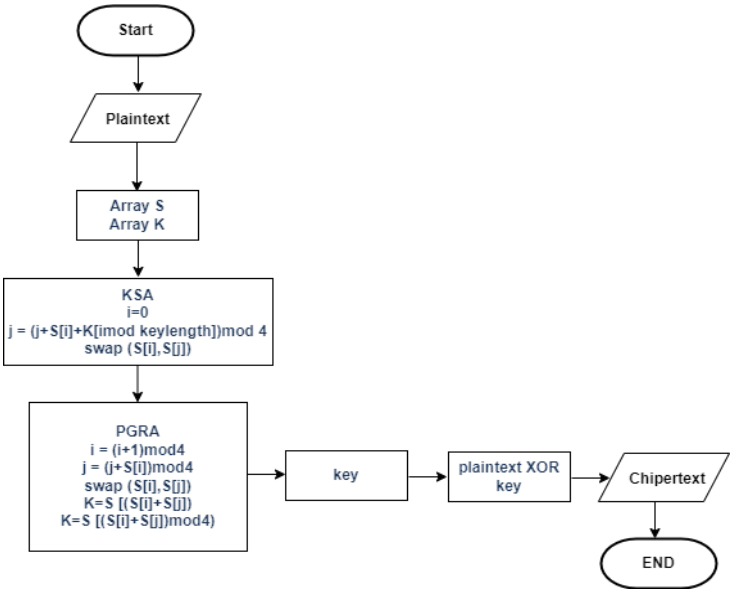
Rancangan yang ketiga yaitu *flowchart* proses enkripsi AES-128. Dimana proses enkripsi pada AES 128 merupakan transformasi terhadap *state* secara berulang dalam 10 ronde atau sesuai dengan. data yang diproses pada setiap ronde berupa data biner. Setiap ronde AES membutuhkan satu kunci hasil generasi kunci dan menggunakan 4 transformasi dasar yaitu *subbytes*, *shiftrows*, *mixcolumns*, dan *addroundkey*. Untuk penjelasannya dapat dilihat pada Gambar 4 ini.



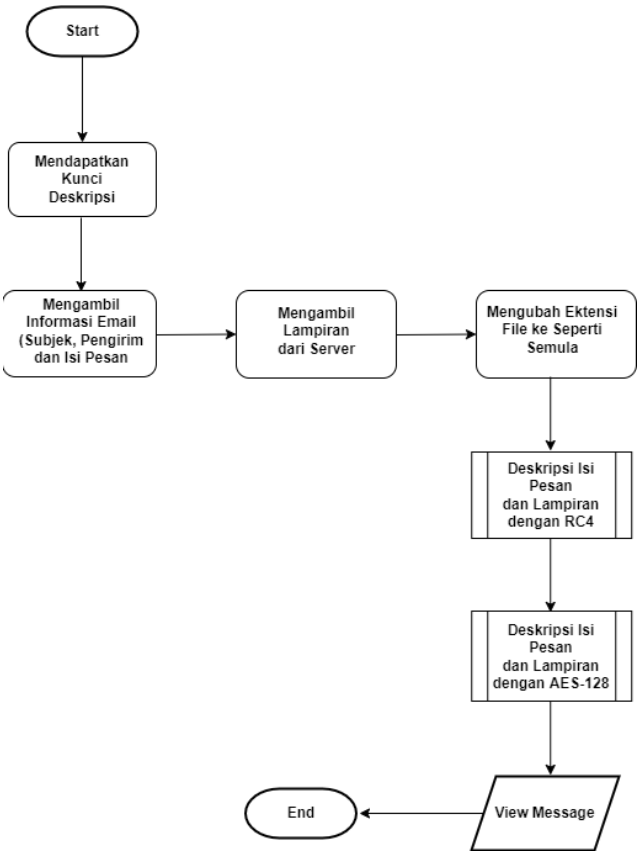
Gambar 4. *Flowchart* Proses Enkripsi AES-128

Rancangan yang keempat yaitu *flowchart* proses enkripsi RC4. Pada proses enkripsi RC4 memiliki proses enkripsi yang cukup sederhana dan hanya melibatkan beberapa operasi saja per byte-nya. Menurut hasil pengujian, kecepatan algoritma. yang nantinya akan menghasilkan chipertext. Untuk lebih jelasnya dapat dilihat pada gambar 5 [12].

Rancangan yang kelima yaitu *flowchart* proses dekripsi pesan. Proses dekripsi pesan tersebut dimulai dengan mendapatkan kunci deskripsi. Lalu mengambil informasi email. Lalu mengambil lampiran dari *server* kemudian mengubah ekstensi *file* ke seperti semula. Jika kunci dekripsi sama dengan kunci enkripsi maka akan mendeskripsi isi pesan dengan lampiran atau *file attachment* dengan RC4 yang dilanjut dengan dekripsi menggunakan algoritma AES-128. Setelah itu pesan dapat dilihat. Secara lengkapnya dapat dilihat pada gambar 6.



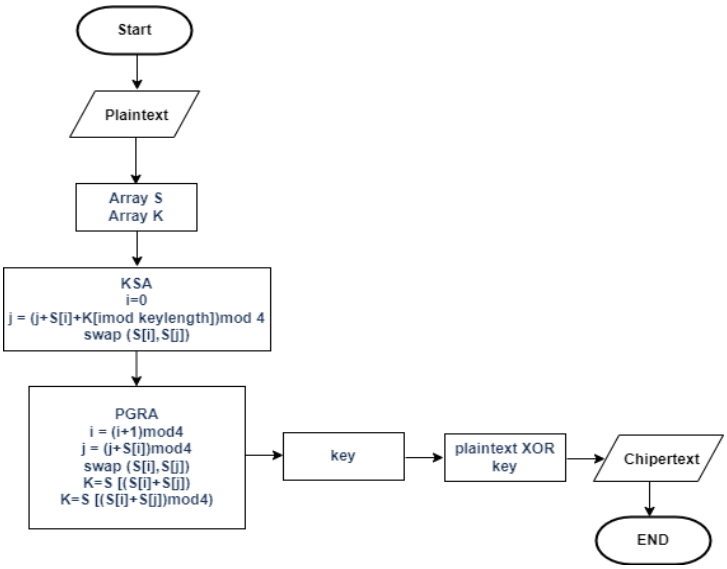
Gambar 5. *Flowchart* Proses Enkripsi RC4



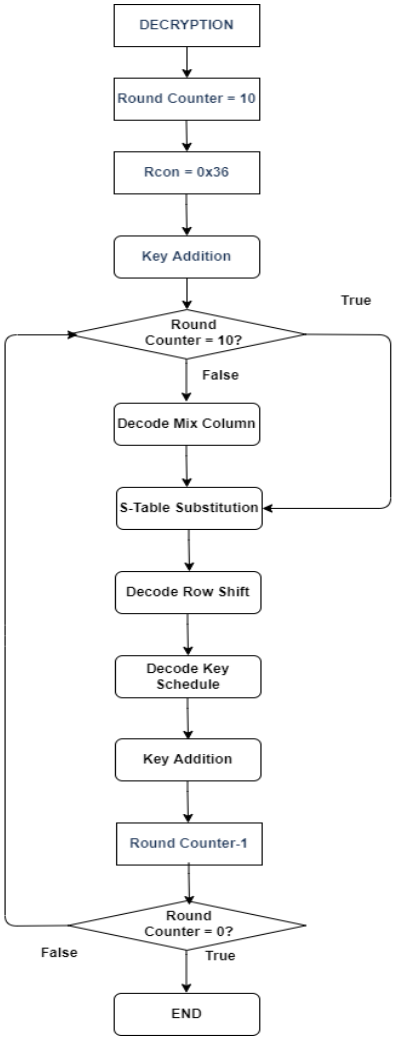
Gambar 6. *Flowchart* Proses Dekripsi Pesan

Rancangan yang keenam yaitu *flowchart* proses dekripsi RC4. Pada proses dekripsi RC4 ini memiliki gambaran dari alur proses. Pada gambar alur apa saja yang terjadi pada proses pengubahan *ciphertext* ke *plaintext* (dekripsi) pada algoritma RC4. Untuk rancangan enkripsi RC4 dapat dilihat pada Gambar 7. *Flowchart* pada Gambar 7 sama halnya dengan *flowchart* enkripsi RC4 pada pembentukan kunci. Namun, setelah kunci (cipher) terbentuk, maka akan dilakukan proses dekripsi yaitu melakukan operasi *XOR*. antara *ciphertext* dengan kunci tersebut sehingga hasil akhirnya adalah sebuah *plaintext* [13].

p-ISSN : 2443-2210
e-ISSN : 2443-2229



Gambar 7. *Flowchart* Proses Dekripsi RC4



Gambar 8. *Flowchart* Proses Dekripsi AES-128

Rancangan yang ketujuh yaitu *flowchart* proses dekripsi AES-128. Hampir sama dengan proses enkripsi AES-128 pada Gambar 4 namun pada tahapannya ada yang dibalik tetapi prosesnya sama. Untuk lebih jelasnya dapat dilihat pada rancangan Gambar 8.

C. Pengembangan

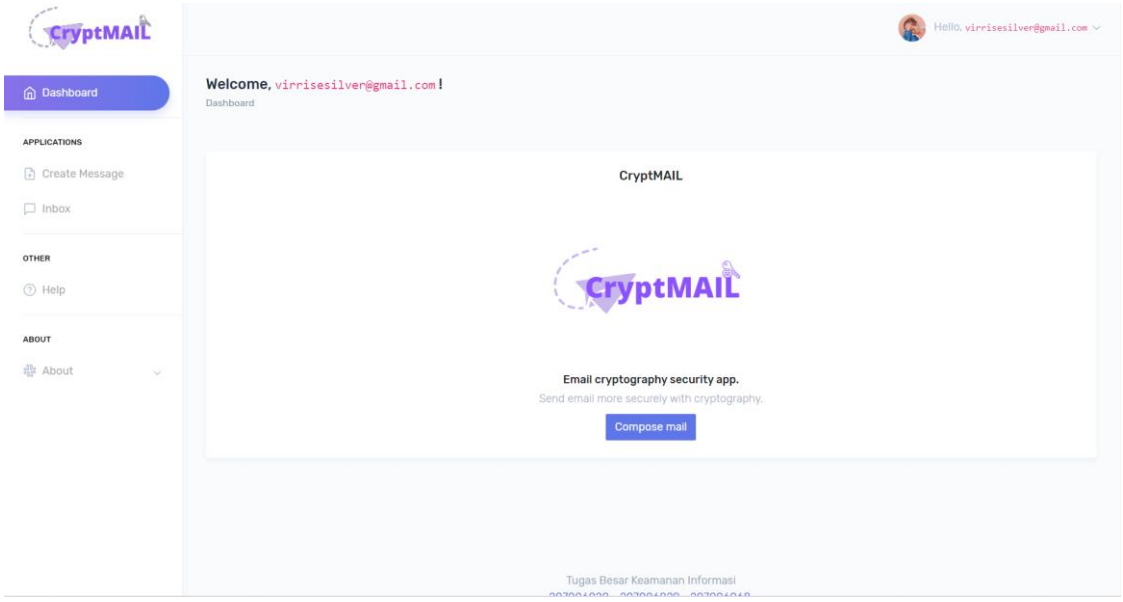
Metode selanjutnya yaitu pengembangan. Fitur *Reply Message* ditambahkan pada aplikasi yang telah dibuat untuk mempermudah pengguna agar dapat langsung membalas email yang diterima. Tidak hanya itu aplikasi ini juga sudah mampu mengirimkan berbagai jenis *file* dengan semua ekstensi, tetapi ukuran *file* harus kurang dari 25MB (≤25MB). Hal ini sebagai antisipasi untuk menghindari penguncian akun sementara pada akun *gmail* yang membatasi setiap pengguna, yaitu tidak melebihi 2500 MB per hari untuk unduh IMAP dan 500 MB per hari untuk unggah IMAP.

D. Implementasi

Metode yang terakhir yaitu implementasi. Pengimplementasian dari aplikasi ini dapat dilihat pada tampilan program yang telah dibuat. Semua fitur yang tersedia dalam aplikasi juga dapat digunakan dan berjalan dengan lancar.

III. HASIL DAN PEMBAHASAN

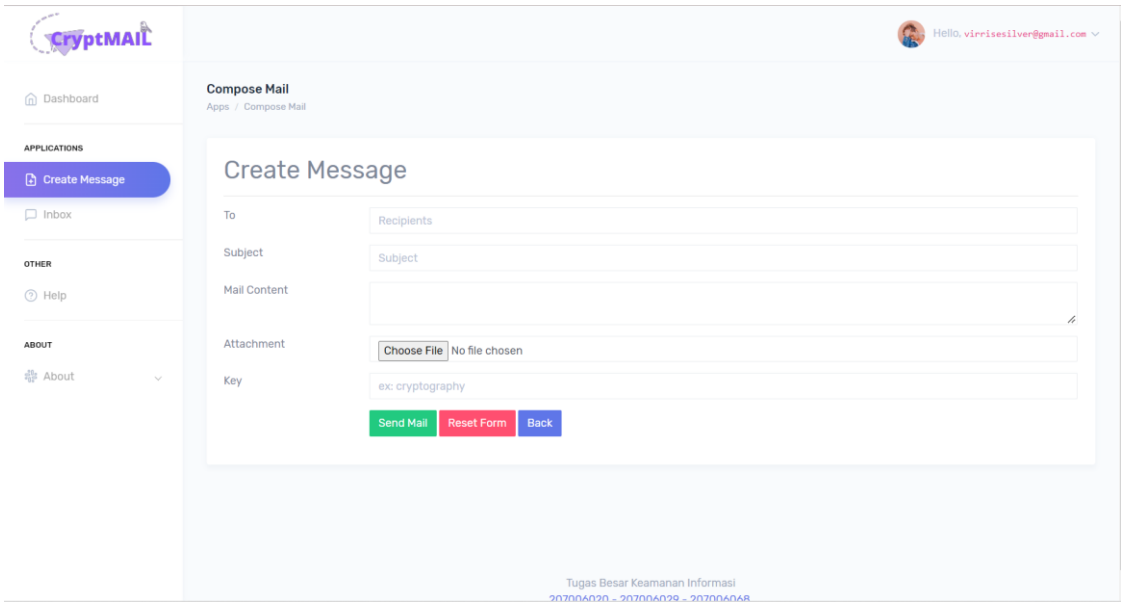
Aplikasi CyptMAIL merupakan aplikasi dengan keamanan ganda pada email menggunakan algoritma AES-128 dan RC4 untuk pengamanan pengiriman pesan elektronik seperti enkripsi dan dekripsi pesan elektronik berbasis web. Pada penelitian ini akan melakukan pengujian proses enkripsi dan dekripsi menggunakan akun *gmail* dan *yahoo mail*. Gambar 9 merupakan tampilan awal web ketika pengguna berhasil melakukan *log in* menggunakan akun *gmail* atau *yahoo mail*. Menu yang disediakan dalam aplikasi ini antara lain: *log in, dashboard, create message, inbox, reply message, help* dan *about*.



Gambar 9. Tampilan Layar *Dashboard.*

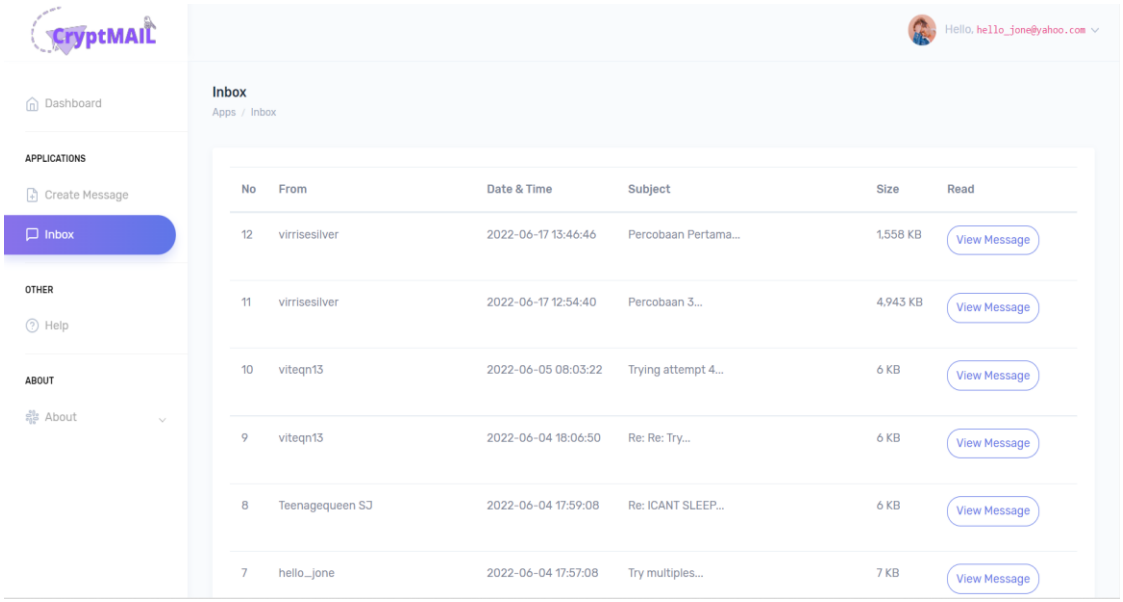
Gambar 10 merupakan tampilan layar untuk laman *Create Message*. *Create Message* ini berbentuk *form* yang terdiri dari *To*/ kepada siapa email akan dikirim, *Subject*/ subjek dari pesan email, *Mail Content*/ isi utama dari pesan email yang akan dikirim, *Attachment*/ *file* lampiran yang ingin dikirim, dan *Key*/ kunci yang digunakan untuk mengenkripsi dan dekripsi pesan.

p-ISSN : 2443-2210
e-ISSN : 2443-2229



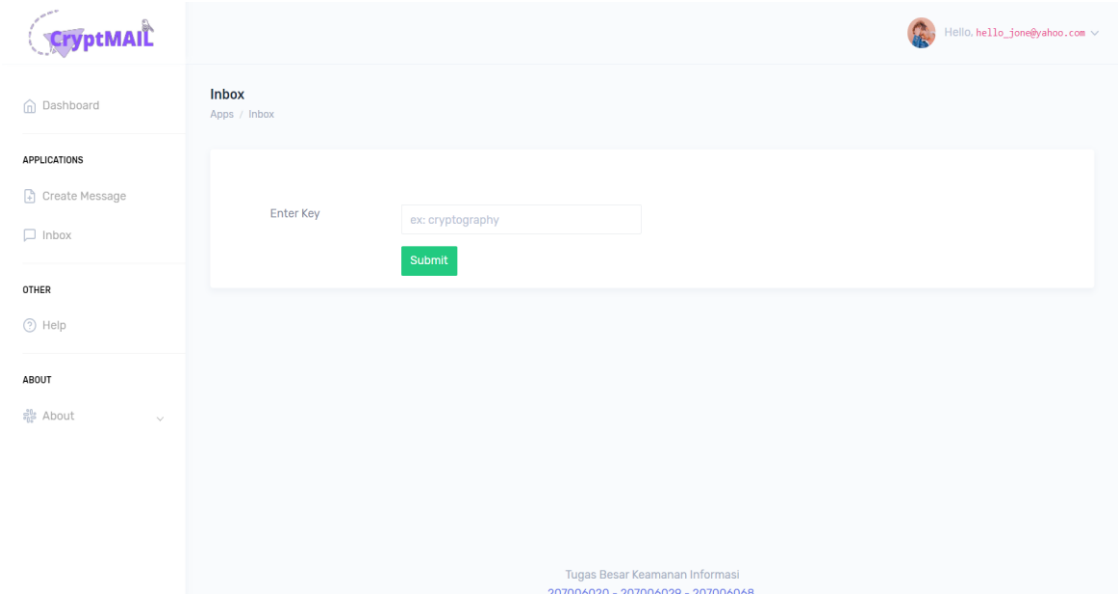
Gambar 10. Tampilan Layar *Create Message.*

Gambar 11 adalah tampilan laman *Inbox*. Laman ini berisi pesan yang masuk ke email pengguna.



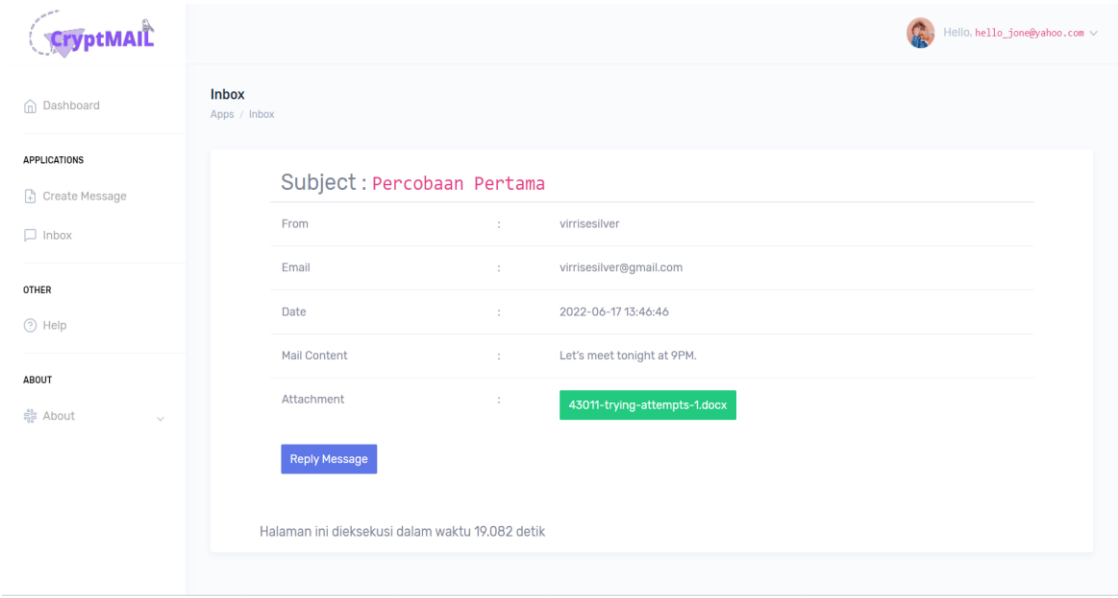
Gambar 11. Tampilan Layar *Inbox*

Gambar 12 merupakan tampilan Ketika pengguna ingin melihat atau membaca pesan yang masuk dengan mengklik *View Message*. Untuk dapat melihat pesan, pengguna diharuskan memasukkan *Key* atau kunci untuk dapat mendekripsi pesan email.



Gambar 12. Tampilan Layar *View Message – Enter Key*.

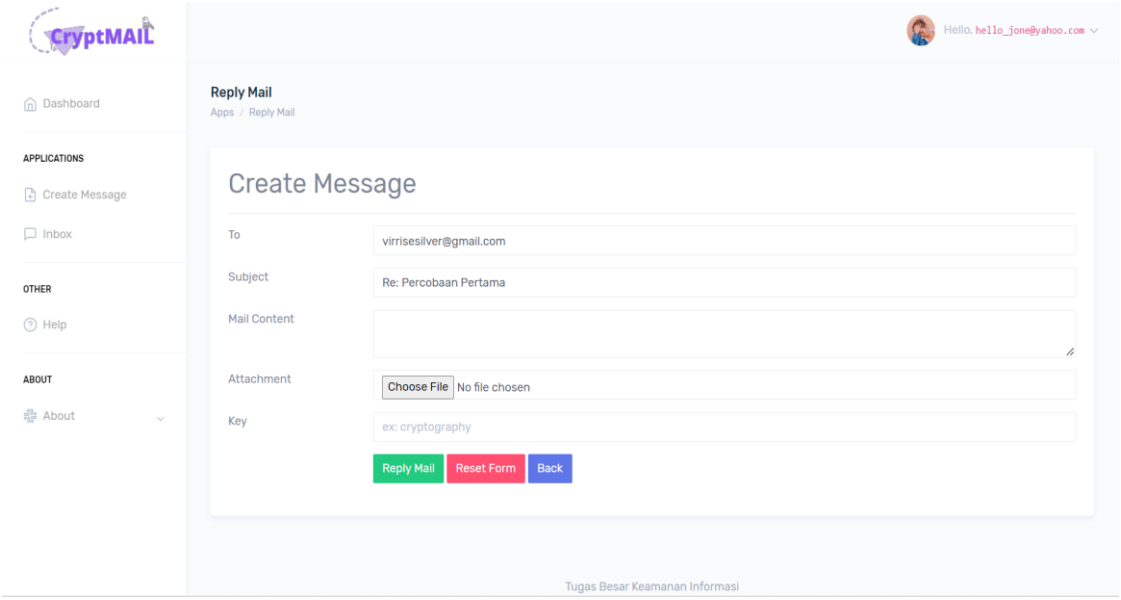
Gambar 13 adalah tampilan ketika pengguna memasukkan *Key* atau kunci yang benar. Pesan dan *file attachment* akan terdekrip dengan sukses.



Gambar 13. Tampilan Layar *View Message.*

Gambar 14 merupakan tampilan dari fitur *Reply Message*. Pengguna hanya perlu mengisikan *Mail Content*/ isi pesan, *Attachment/ file* lampiran dan *Key/* kunci. Sedangkan untuk *form To*/ email penerima dan *Subject*/ subjek pesan akan terisi secara otomatis.

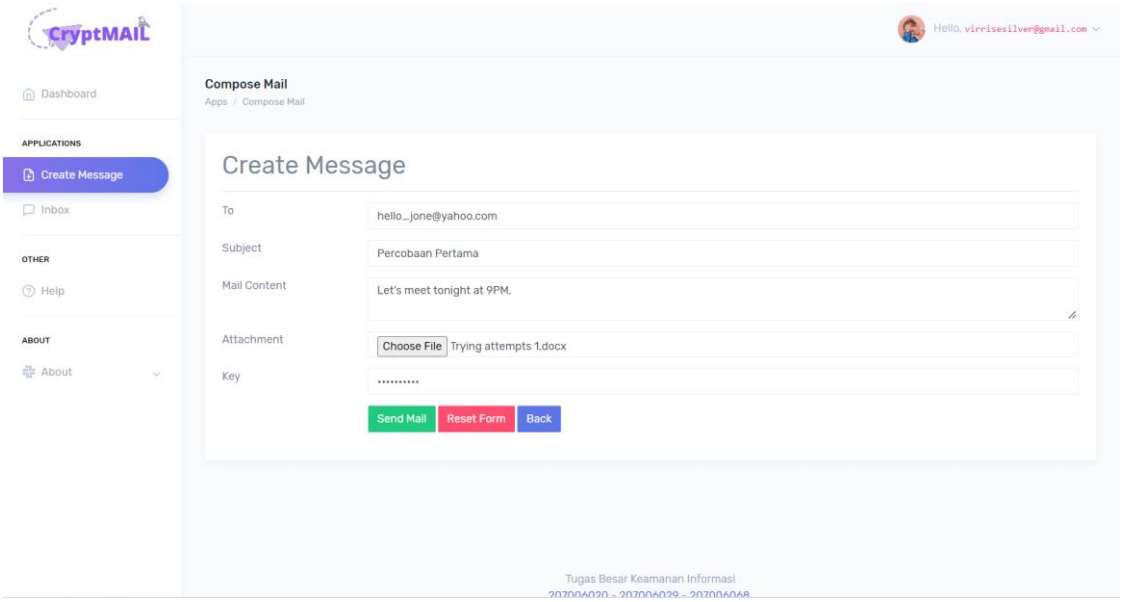
p-ISSN : 2443-2210
e-ISSN : 2443-2229



Gambar 14. Tampilan Layar *Reply Message.*

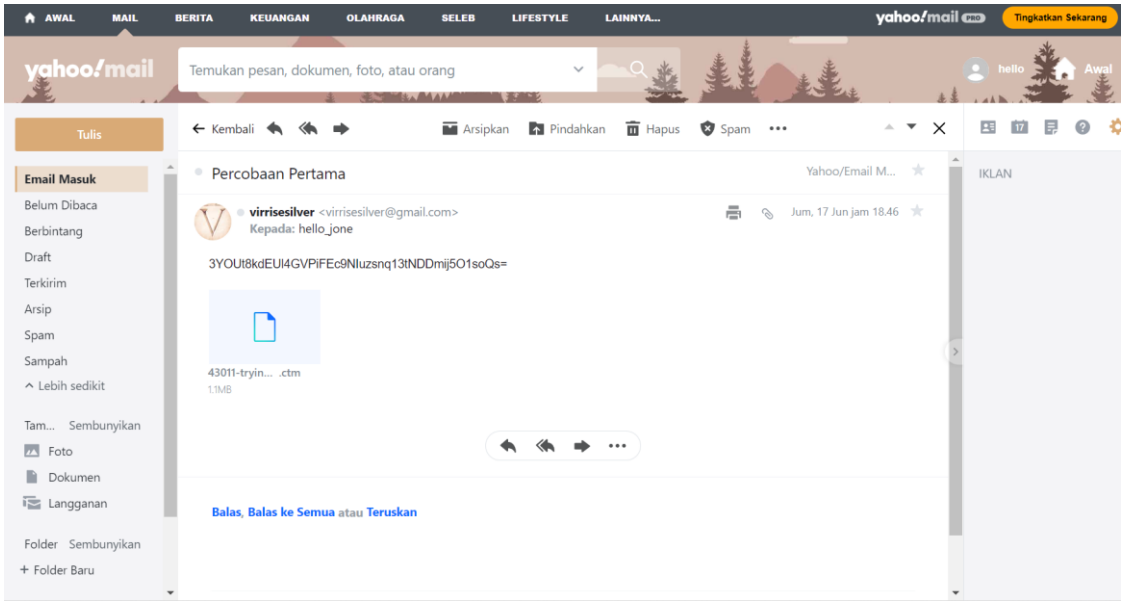
A. Pengujian Enkripsi Pada Program Aplikasi

Pengujian awal adalah uji coba proses enkripsi pesan email dari *gmail* ke *yahoo mail.* Gambar 15 merupakan tampilan untuk percobaan 1.



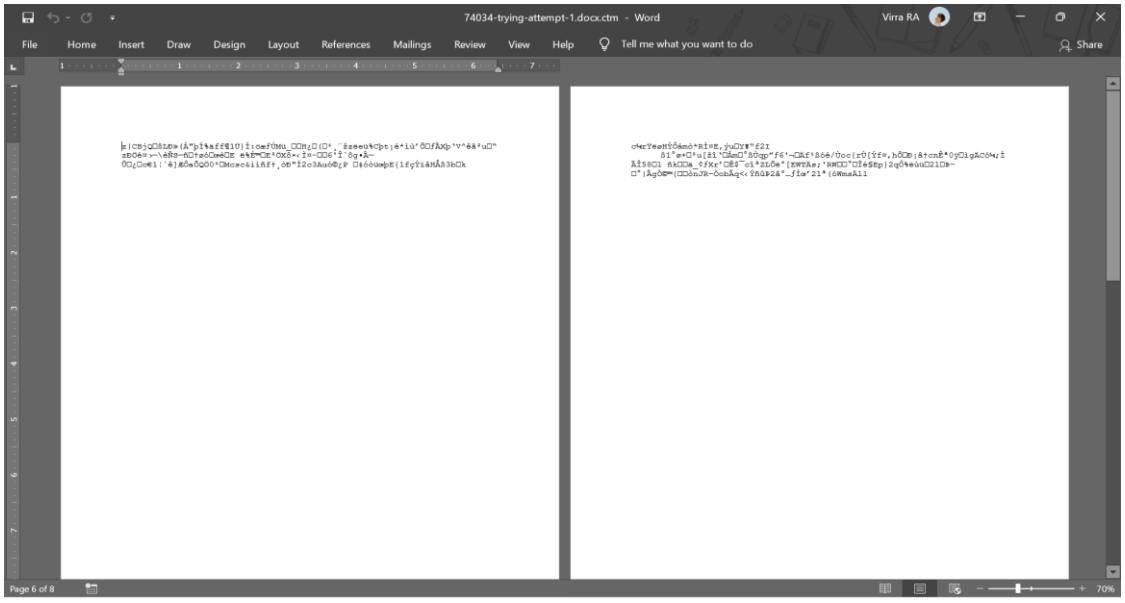
Gambar 15. Percobaan 1 Enkripsi Pesan.

Gambar 16 merupakan tampilan hasil enkripsi pesan menggunakan algoritma AES-128 dan RC4 yang terkirim dari *gmail* ke *yahoo mail*. Proses enkripsi akan diproses menggunakan algoritma AES-28 lebih dulu lalu dienkripsi lagi menggunakan algoritma RC4 untuk keamanan ganda.



Gambar 16. Enkripsi Percobaan 1 – Tampilan pada *yahoo mail.*

Pesan yang terkirim akan ter enkripsi menjadi *chipertext* dan ekstensi *file* berubah menjadi *.ctm. Gambar 17 merupakan tampilan *file* yang telah terenkripsi. Percobaan ini dilakukan juga pada *file* berekstensi lain seperti mp3, png dan lainnya.

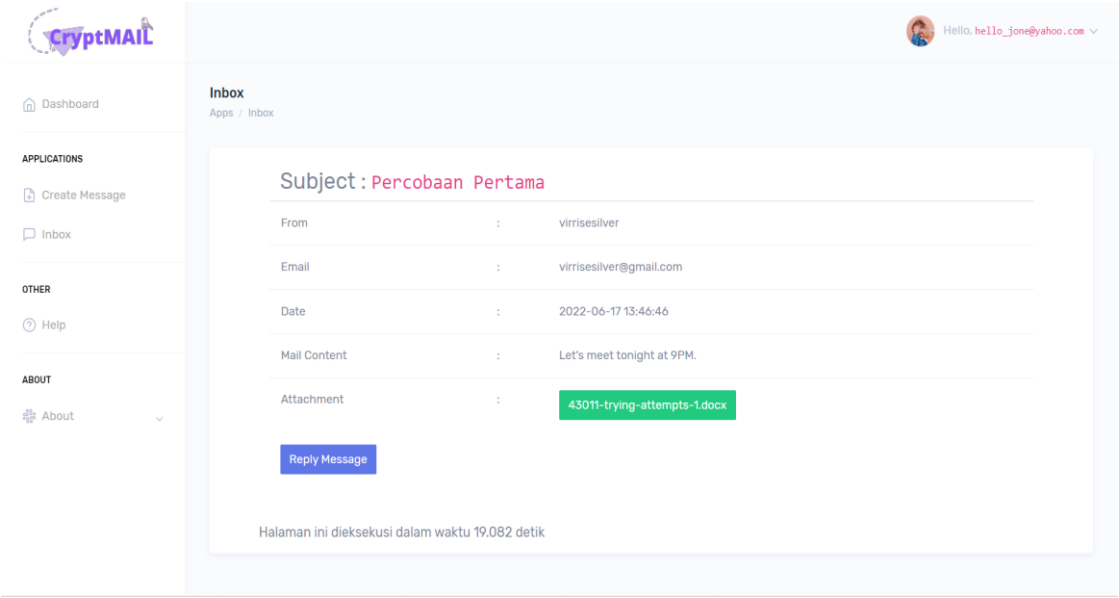


Gambar 17. Enkripsi Percobaan 1 – Tampilan *file attachment* *.docx setelah dienkripsi

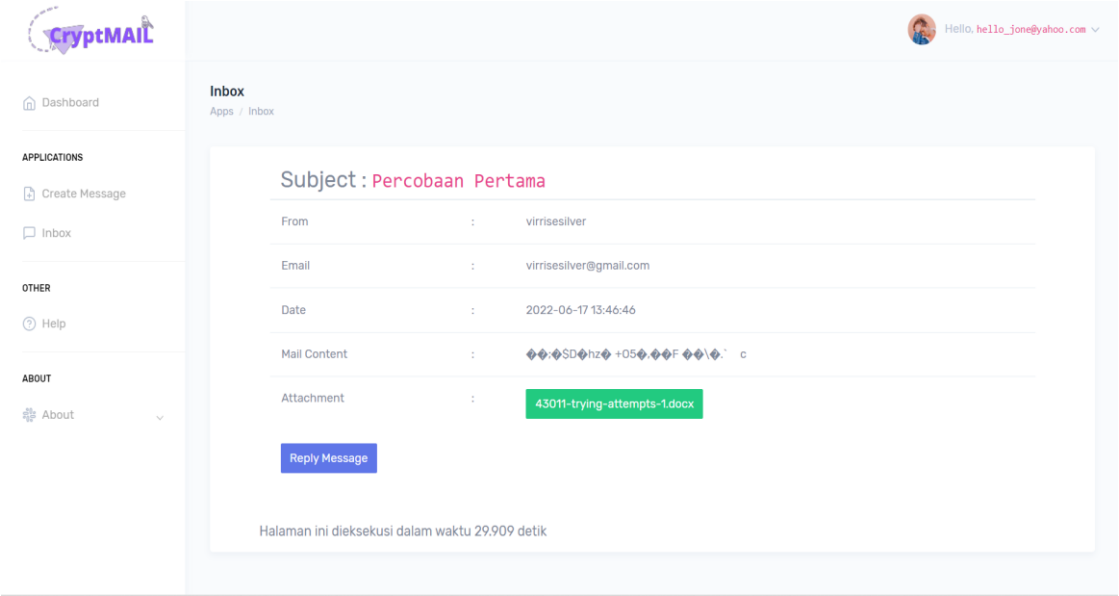
B. Pengujian Dekripsi Pada Program Aplikasi

Proses dekripsi dilakukan di aplikasi CryptMAIL untuk pengguna dapat membaca pesan yang diterima. Gambar 18 merupakan tampilan hasil ketika pengguna memasukkan *Key*/ kunci yang benar dan pesan berhasil di dekrip**.** Gambar 19 adalah tampilan ketika pengguna memasukkan *Key/* kunci yang salah. Proses dekrip gagal dan pesan maupun *file attachment* tidak akan terbaca. Pada proses dekripsi ini program akan mendekripsi pesan dan *file* menggunakan algoritma RC4 lebih dulu lalu didekripsi lagi menggunakan algoritma AES-128.

p-ISSN : 2443-2210
e-ISSN : 2443-2229

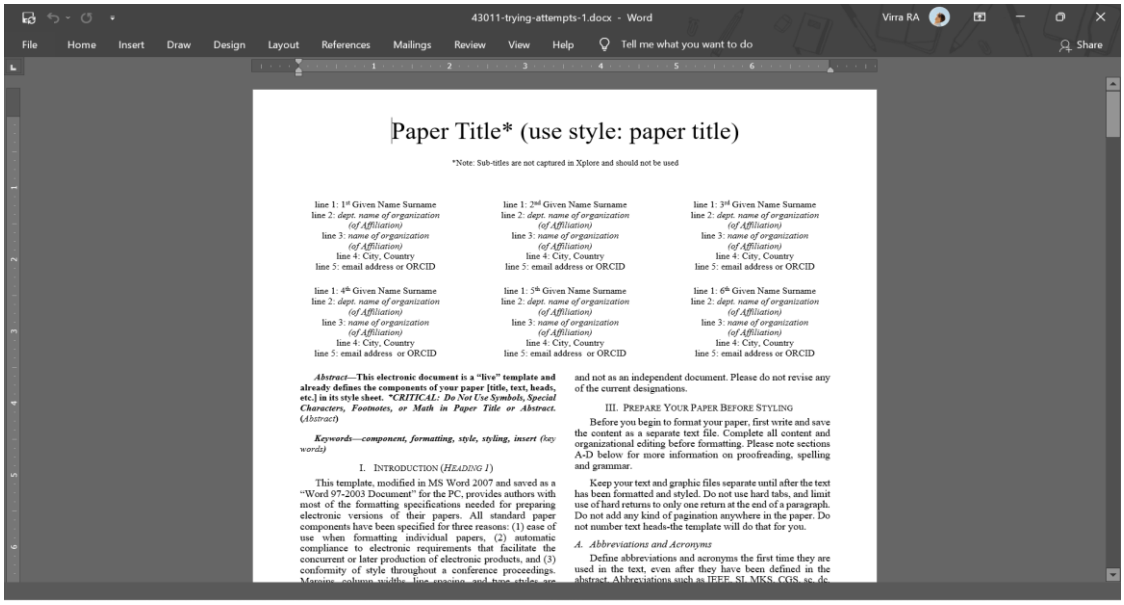


Gambar 18. Dekripsi Percobaan 1 berhasil.



Gambar 19. Dekripsi Percobaan 1 gagal

Ketika proses dekrip berhasil *file attachment* akan dipulihkan dan kembali berekstensi seperti semula. Gambar 20 merupakan tampilan *file attachment* yang berhasil didekripsi. Percobaan proses dekripsi dilakukan juga pada *file* berekstensi lain seperti mp3, png dan lainnya.



Gambar 20. Dekripsi Percobaan 1 – Tampilan *file attachment* *.docx setelah berhasil di dekripsi.

C. Hasil Pengujian Program Aplikasi

Tabel 1 merupakan hasil uji coba dari proses enkripsi yang dilakukan terhadap pengiriman email antara *gmail* dan *yahoo* dengan format *file attachment* yang berbeda.

TABEL 1
HASIL UJI COBA ENKRIPSI

No	Proses Enkripsi						
	Plaintext	***File***	***Key***	***Chipertext***	***File* Terenkripsi**	***Size File***	***Time***
1	Let's meet tonight at 9PM.	Trying attempts 1.docx	Percobaan1	3YOUt8kdEUl4GVPiFEc9NIuzsnq13tNDDmij5O1soQs=	43011-trying-attempts-1.docx.ctm	1.12 MB	27.897 sec
2	I will play this song when I arrive as a signal	SUPER JUNIOR - I Think I [128 kbps].mp3	Percobaan2	En7/A2oBvp7f8gWhatHqKseHII9z/aaYmMsiS/Hyj2KzyLuM5s23909/G/zFax7K	69271-super-junior---i-think-i-[128-kbps].mp3.ctm	3.15 MB	53.315 sec
3	Please make this picture even more interesting, and send the new design soon	Percobaan3.png	Percobaan3	XYRkasunWpW1MJy1xE7q2NBbQpzsqjWlUZUc+LX28ucehA+m+omkfnKwXXZouvo49F+IbT2QSWVv3jYgIKrPwmgM6DYJmKZsERpbuSeRQCk=	60017-percobaan3.png.ctm	3.56 MB	83.925 sec

Tabel 2 merupakan hasil uji coba dari proses dekripsi dari pesan masuk yang terenkripsi

TABEL 2
HASIL UJI COBA DEKRIPSI

No	Proses Enkripsi						
	Chipertext	***File* Terenkripsi**	***Key***	***Plaintext***	***File* Terdekripsi**	***Size File***	***Time***
1	3YOUt8kdEUl4GVPiFEc9NIuzsnq13tNDDmij5O1soQs=	43011-trying-attempts-1.docx.ctm	Percobaan 1	Let's meet tonight at 9PM.	43011-trying-attempts-1.docx	1.12 MB	19.082 sec
2	En7/A2oBvp7f8gWhatHqKseHII9z/aaYmMsiS/Hyj2KzyLuM5s23909/G/zFax7K	69271-super-junior---i-think-i-[128-kbps].mp3.ctm	Percobaan 2	I will play this song when I arrive as a signal	69271-super-junior---i-think-i-[128-kbps].mp3	3.15 MB	55.919 sec
3	XYRkasunWpW1MJy1xE7q2NBbQpzsqjWlUZUc+LX28ucehA+m+omkfnKwXXZouvo49F+IbT2QSWVv3jYgIKrPwmgM6DYJmKZsERpbuSeRQCk=	60017-percobaan3.png.ctm	Percobaan 3	Please make this picture even more interesting, and send the new design soon	60017-percobaan3.png	3.56 MB	56.661

Dapat dilihat dari tabel 1 dan 2 adanya keterkaitan antara banyaknya karakter pesan dan *file attachment* yang akan di enkripsi atau dekripsi dengan waktu. Pada percobaan 1 ukuran *file attachmen*t yang dikirim adalah 1.12 MB, waktu yang dibutuhkan untuk proses enkripsi adalah 27.897 detik dan proses dekripsi membutuhkan waktu 19.082 detik. Pada percobaan 2 ukuran *file attachment* yang dikirim adalah 3.15 MB, waktu yang dibutuhkan untuk proses enkripsi adalah 53.315 detik dan proses dekripsi membutuhkan waktu 55.919 detik. Sedangkan pada percobaan 3 ukuran *file attachment* sebesar 3.56 MB, waktu yang dibutuhkan pada proses enkripsi adalah 83.925 detik dan proses dekripsi membutuhkan waktu 56.661 detik.

Dengan data yang didapat bahwa waktu yang diperlukan pada proses enkripsi dan dekripsi pesan dan *file attachment* berbanding lurus dengan ukuran/ *size* dari isi pesan dan *file attachment*. Semakin besar ukuran *file attachment* dan isi pesan maka waktu yang dibutuhkan aplikasi dalam proses enkripsi maupun dekripsi pesan akan semakin lama. Selain *size*/ ukuran isi pesan dan *file attachment*, koneksi internet juga menjadi salah satu pengaruh dalam kecepatan proses enkripsi dan dekripsi.

Pada percobaan 1 *file attachment* yang dikirim adalah 1.12 MB, setelah melalui proses enkripsi dan dekripsi ukurannya yaitu 1.12 MB. Percobaan 2 *file attachment* yang dikirim berukuran 3.15 MB, setelah melalui proses enkripsi dan dekripsi ukurannya yaitu 3.15 MB. Pada percobaan 3 ukuran *file attachment* adalah 3.56 MB, setelah melalui proses enkripsi dan dekripsi ukuran *file* adalah 3.56 MB. Maka didapatkan bahwa proses enkripsi dan dekripsi tidak mengubah ukuran dari *file attachment* yang dikirim.

IV. SIMPULAN

Berdasarkan hasil pengujian yang dilakukan, Aplikasi Kriptografi Email 'CryptMAIL' ini berhasil melakukan pengamanan pesan email (*gmail* dan *yahoo mail*) dengan lebih aman menggunakan algoritma AES-128 dan RC4. Proses enkripsi dan dekripsi dengan algoritma AES-128 dan RC4 berhasil diimplementasikan pada isi pesan email dan *file attachment* yang dikirim. Melalui uji coba aplikasi ini terbukti memberikan keamanan ganda pada pesan email yang dikirim untuk mengantisipasi adanya kelalaian dalam menuliskan alamat email penerima yang dapat mengakibatkan kebocoran informasi. Pesan hanya dapat didekripsi melalui aplikasi CryptMAIL dan pengguna membutuhkan kunci yang sama dengan kunci enkripsi pesan pengirim. Dengan kata lain, pihak ketiga tidak dapat membaca pesan sebagai *plaintext* tetapi sebagai *chipertext* jika tidak dengan aplikasi CrpytMAIL dan tidak mempunyai kunci yang sesuai. Aplikasi ini dapat mengirimkan *file* dengan semua ekstensi, tetapi ukuran *file* harus kurang dari 25MB (≤25MB). Ini untuk menghindari penguncian akun

sementara pada akun *gmail.* Penggunaan algoritma lain sebagai tambahan atau pengganti seperti algoritma RC6, RSA atau lainnya dapat menjadi pertimbangan untuk penelitian berikutnya untuk dapat menambah keamanan pada email maupun efisiensi dalam kecepatan enkripsi dan dekripsi pesan.

UCAPAN TERIMA KASIH

Ucapan terimakasih ditujukan kepada pembimbing dan rekan-rekan yang telah memberikan dukungan dan banyak membantu dalam membuat dan menyelesaikan penelitian ini.

DAFTAR PUSTAKA

[1] A. Ahmad, "Perkembangan Teknologi Komunikasi dan Kesenjangan Informasi: Akar Informasi dan Berbagai Standarnya," *Jurnal Dakwah Tabligh*, vol. 13, no. 1, pp. 137-149, 2012.

[2] F. Firman and S. R. Rahman, "Pembelajaran Online di Tengah Pandemi Covid-19," *Indonesian Journal of Educational Science (IJES)*, vol. 2, no. 2, pp. 81-89, 2020.

[3] M. I. Zulfikar, G. Abdillah and A. Komarudin, "Kriptografi untuk Keamanan Pengiriman Email Menggunakan Blowfish dan Rivest Shamir Adleman (RSA)," *Seminar Nasional Aplikasi Teknologi Informasi (SNATi)*, pp. 19-26, 2019.

[4] R. S. N. Aswita, I. Gunawan, Z. M. Nasution, S. and H. S. Tambunan, "Implementasi Algoritma Aes & Rc4 Terhadap Keamanan Data Produk Benih Sayuran di PT. Ewindo," *Jurnal Sosial Sains*, vol. 1, no. 1, pp. 461-468, 2021.

[5] R. A. Indra and W. Pramusinto, "Aplikasi Email (Electronic Mail) Menggunakan Algoritma Advanced Encryption Standard(AES-128) dan Algoritma Rivest Cipher 4 (RC4) Berbasis Web," *Skanika*, vol. 1, no. 2, pp. 725-731, 2018.

[6] A. G. Pramudito and D. Kusumaningsih, "Implementasi Algoritma Aes 128 Dan Rc4 Untuk Pengamanan Email Pada Pt. Dinamika Hydro Engineering," *Skanika*, vol. 1, no. 3, pp. 869-876, 2018.

[7] R. Riyantono, "Aplikasi Pengamanan Surat Elektronik (Email) Menggunakan Algoritma Advanced Encryption Standard 128 (Aes-128) dan Rivest Cipher Code 4 (Rc4) Berbasis Web," *Skanika*, vol. 1, no. 2, pp. 725-731, 2018.

[8] A. Rahmatulloh and R. Munir, "Pencegahan Ancaman Reverse Engineering Source Code PHP dengan Teknik Obfuscation Code pada Extension PHP," in *Konferensi Nasional Informatika*, Bandung, 2015.

[9] A. Rahmatulloh, Keamanan Source Code PHP Menggunakan Teknik Obfuscation, Tasikmalaya: Pena Persada, 2020.

[10] N. A. Ilham, "Implementasi Konsep Pemrograman Berorientasi Objek Pada Aplikasi Sistem Parkir Menggunakan Bahasa Pemrograman Java," *Jurnal Edukasi Elektro*, vol. 3, no. 2, pp. 63-69, 2020.

[11] W. Winarti, M. Ihsan and N. Wulandari, "Perancangan Sistem Informasi Penjualan Berbasis Web pada Toko Campus Mart Unimuda Sorong dengan PHP dan MySql," *JURNAL PETISI (Pendidikan Teknologi Informasi)*, vol. 1, no. 1, pp. 44-56, 2020.

[12] R. Munir and S. A. B. R. Kristoforus JB, "ALGORITMA AES – 128 AES (Advanced Encryption Standard)," 2012. [Online]. Available: https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2017-2018/Advanced-Encryption-Standard-(AES)-(2018).pdf.

[13] B. Purba, F. A. Gulo, N. I. Utami and Y. A. Sihotang, "Pengamanan File Teks menggunakan Algoritma RC4," *Seminar Nasional Teknologi Komputer & Sains (SAINTEKS)*, pp. 420-425, 2020.