BAB I
PENDAHULUAN

1.1 Latar Belakang Penelitian

Perkembangan teknologi informasi telah mengalami perkembangan pesat yang mempengaruhi semua aspek disegala bidang kehidupan manusia. Perkembangan teknologi informasi disertai dengan ketergantungan terhadap data dan informasi. Data dan informasi yang dibutuhkan oleh semua instansi baik personal maupun pemerintah. Namun, pada saat ini keamanan data menjadi isu yang sangat penting dalam proses pengiriman dan penerimaan data. Masalah keamanan data merupakan hal terpenting dalam sistem informasi, sehingga diperlukan sebuah algoritma pengamanan data dengan mekanisme enkirpsi dan dekripsi pesan yang biasa disebut dengan algoritma kriptografi (Munir, Sutikno, & Riyanto, 2015).

Email merupakan pesan elektronik yang memberikan kemudahan kepada pengguna untuk saling bertukar data dan informasi. Layanan email bisa didapatkan dengan gratis dan dengan segala kemudahan akses tanpa terhalang oleh ruang dan waktu. Penggunaan email dari tahun ke tahun mengalami perkembangan yang pesat. Hal ini dapat dilihat pada data yang dipublikasi oleh The Radicati Group, Inc. pada tabel berikut (Sara Radicati, 2016):

Table 1.1. ***Worldwide Daily Email Traffic***
Sumber : (Sara Radicati, 2016)

Daily Email Traffic	2012	2013	2014	2015	2016
Total Wolrldwide Emails Per Day (B) *% Change*	144.8	154.6 7%	165.8 *7%*	178.3 *8%*	192.2 *8%*
Business Emails Per Day (B) *% Change*	89.0	101.0 *13%*	114.3 *13%*	128.6 *13%*	143.8 12%
Consumer Emails Per Day (B) *% Change*	55.8	53.6 *-4%*	51.5 *-4%*	49.7 *-3%*	48.4 *-3%*

Dari tabel 1, dapat dilihat bahwa secara umum penggunaan email dari tahun ketahun mengalami peningkatan pengguna terutama disektor bisnis, dan walaupun pengguna email diluar itu mengalami sedikit penurunan. Namun dapat disimpulkan bahwa secara umum penggunaan email masih menjadi sarana yang paling banyak digunakan untuk bertukar informasi. Hal ini dapat dilihat bahwa pada tahun 2016, dalam sehari penggunaan email didunia mencapai angka 192.2 juta pengguna.

Walaupun begitu banyak digunakan dalam kegiatan sehari-hari, namun keamanan informasi yang ada pada email masih harus dijaga, karena telah terjadi beberapa kasus seperti yang terjadi pada tahun 2014 dinyatakan bahwa sebanyak 2,5 juta akun email *yahoo* telah diretas pada awal januari 2014. Pembobolan email *yahoo* ini dilakukan menggunakan akun pihak ketiga seperti Facebook, Netflix, Twitter, dan lainnya (Aditya, 2014). Kasus lainnya terjadi pada tahun 2016 dimana seperti yang dilansir *Reuters,* Kepala Keamanan Informasi dari Hold Security mengatakan bahwa ada ada sekitar 272.300.000 akun email yang telah dicuri dan dijual oleh pihak yang tidak bertanggung jawab. Selain itu, layanan surel milik Rusia juga telah kecolongan sebanyak 40 juta akun *Yahoo* Mail, 33 juta akun Hotmail, dan 24 juta akun Gmail (Reza, 2016). Peretasan akun email melalui pihak ketiga juga terjadi di Indonesia, seperti pada kasus lazada yang terjadi pada tahun 2016 (Iskandar, 2016). Selain itu, pada Juni 2012 6 juta akun Linkedln diretas dan diperjualbelikan oleh oknum tak bertanggung jawab, pada tahun 2016 kembali terjadi peretasan akun Linkedln oleh peretas asal Rusia. Sebanyak 117 juta email dan password Linkedln dijual ilegal di *marketplace ilegeal*. Harga akun yang dijual seharga 5 bitcoin atau setara 2.200 dollar AS (Rp 29, 7 jutaaan), sebagaimana dilaporkan *TheNextWeb* dan dihimpun KompasTekno (Bohang, 2016). Menurut Abdul Mumin Salifu dalam tesisnya, kasus *man in the middle* (MITM) *attack* memakan korban aplikasi berbasis TCP seperti *Telnet, rlogin, ftp, mail application, web browser*. Selain itu, terkhusus bahaya MITM dalam jaringan didapatkan data bahwa dalam waktu 24 jam, Black Hat mengklaim bisa mendapatkan 117 akun email. Sehinnga mereka bisa mengetahui pesan-pesan email yang ada.(Salifu, 2014).

Dari berbagai kasus peretasan akun email diatas, dikhawatirkan akan terjadi pencurian data dan informasi yang kita kirim dan terima di inbox email. Oleh karena itu, diperlukan sebuah solusi untuk mengamankan data dan informasi yang ada di inbox email kita. Salah satu solusi yang bisa digunakan adalah merubah pesan yang kita kirim agar menjadi pesan yang seolah-olah tidak bearti dan tidak langsung terbaca dengan mudah oleh pihak yang tidak bertanggung jawab. Oleh karena itu, kriptografi menjadi salah satu solusi untuk merahasiakan isi pesan yang dikirim dan diterima pada akun email.

Menurut Rinaldi Munir (Munir, Kriptografi, 2007), algoritma kriptografi dapat memberikan layananan keamanan dalam bertukar data dan informasi. Layanan yang diberikan kriptografi adalah sebagai berikut:

1. Kerahasiaan (*confidentiality*) merupakan layanan yang ditujukan untuk menjaga agar pesan tidak dapat dibaca oleh pihak-pihak yang tidak berhak.
2. Integritas data (*data integrity*) adalah layanan yang menjamin bahwa pesan masih asli dan utuh atau belum pernah dimanipulasi dalam proses pengiriman dan penerimaan pesan.
3. Otentikasi (*autehentication*) merupakan layanan yang berhubungan dengan identifikasi kebenaran pihak-pihak yang berkomunikasi maupun mengidentifikasi kebenaran sumber pesan.
4. Nirpenyengkalan (*non-repudation*) merupakan layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengirim pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan.

Untuk menjaga keamanan data (kerahasian, integritas, nir penyangkalan, dan otentikasi data) saat pengiriman dan penerimaan email di jaringan terhadap serangan dan ancaman baik *passive attack, active attack* maupun *advance attack* maka diperlukan algoritma kriptografi untuk mengamankan isi pesan email yang akan dikirim. Algoritma camellia merupakan salah satu algoritma kriptografi yang bisa menjaga kerahasian isi pesan teks pada email.

Algoritma camellia memiliki keunggulan (Kazumuro Aokit, 2009) diantaranya memiliki *high level of security, efficeincy on multiple platforms, future developments.* Menurut Yiqun Lisa Yin (Yin, 2000), algoritma camellia merupakan sebuah *block cipher* enkripsi dan dekripsi data yang dikembangkan oleh NTT dan Mitsubishi yang dipublikasi pada tahun 2000 dengan *block sizes* 128 bits dengan panjang kunci 128,192, dan 256 bits.

Menurut Ahmad Rifqi Hadiyanto (Hadiyanto, 2004), algoritma kriptografi camellia dengan panjang kunci 128 bit memilki keamananan yang tinggi, kemampuan untuk diimplementasikan dalam berbagai macam platform, serta kebutuhan *resource memory* yang kecil. Selain itu, alasan penggunaan algoritma camellia dalam mengamankan informasi dalam pesan email yang akan dikirim adalah berdasarkan penelitian yang dilakukan oleh Jiajun Wen (Wen, 2014) yang menyimpulkan bahwa algoritma camellia dengan panjang kunci 128 bit tidak bisa dilakukan *differential attack.*

1.2 Rumusan Masalah

Adapun rumusan masalah dalam penelitian ini adalah:

1. Bagaimana mengimplementasikan algoritma camellia dengan key 128 bit pada proses pengiriman dan enkripsi email di *Yahoo mail client*?
2. Bagaimana mengimplementasikan algoritma camellia dengan key 128 bit pada proses pembacaan dan dekripsi email di *Yahoo mail client*?
3. Bagaimana performa waktu proses penggunaan algoritma camellia dengan panjang kunci 128 bit pada berbagai ukuran *plaintext* dan *chipertext* yang dienkripsi dan didekripsi?

1.3 Tujuan Penelitan

Adapun tujuan dari penelitian ini diantaranya:

1. Mendapatkan hasil implementasi algoritma camellia dengan key 128 bit pada proses pengiriman dan enkripsi email di *yahoo mail client.*
2. Mendapatkan hasil implementasi algoritma camellia dengan key 128 bit pada proses pembacaan dan dekripsi email di *yahoo mail client*.

3. Medapatkan data performa waktu proses penggunaan algoritma camellia dengan panjang kunci 128 bit pada saat enkripsi dan dekripsi berbagai ukuran *plaintext* dan *chipertext* pada *yahoo mail client*.

1.4 Batasan Masalah

Adapun batasan masalah pada penelitian ini diantaranya:

1. Kunci yang digunakan pada algoritma camellia dipenelitian ini dengan ukuran panjang 128 bit.
2. *Mail server* yang digunakan hanya *yahoo mail sever*.
3. Menu yang tersedia pada aplikasi *mail client* ini hanya *create mail, inbox,* dan *sent mail.*
4. Penelitian ini tidak membandingkan dengan algoritma kriptografi yang lain.
5. Pesan email yang dienkripsi maupun yang dienkripsi hanya berupa pesan teks (isi pesan email).
6. Sistem aplikasi yang dibangun menggunakan bahasa pemograman Java yang hanya bisa dijalankan pada personal komputer (*desktop application*).
7. Ukuran plainteks dan chiperteks pada penelitian ini menggunakan format ASCII (*American Standart Code for Information Interchange*).
8. Pada penelitian ini sistem tidak menerima inputan berupa *attachment file.*