BAB I
PENDAHULUAN

1.1. Latar Belakang

Teknologi informasi yang berkembang saat ini, sejalan dengan peningkatan arus pengiriman dan penerimaan data. Hasil survei dari Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) (Isparmo, 2016) menunjukkan bahwa pengguna internet di Indonesia tahun 2016 telah mencapai lebih dari setengah penduduk Indonesia, yaitu 132,7 juta (51,8%) jiwa dari total populasi penduduk Indonesia yang mencapai 256 juta jiwa. Dengan jumlah tersebut, penggunaan internet tentu mengandung berbagai macam data dan informasi. Hal tersebut membuka peluang bagi para peretas untuk mendapatkan data atau informasi yang bersifat rahasia. Sehingga keamanan data menjadi topik terpenting dalam proses pengiriman dan penerimaan data.

Salah satu perputaran data saat ini terdapat pada *electronic mail* (email). Email merupakan surat elektronik, dimana pengiriman atau penerimaan surat dilakukan secara elektronik. Menurut John Rhoton (2000) dalam bukunya yang berjudul *Programmer's Guide to Internet Mail* berkata bahwa email adalah jembatan yang memudahkan kita untuk melakukan aktivitas dan memperoleh informasi di jejaring sosial. Terlihat pada pendaftaran akun di berbagai situs, jejaring sosial, *messenger*, dan sebagainya mengharuskan penggunanya memiliki akun email. Namun, penggunaan *password* yang sama untuk semua akun *online* masih ditemukan pada satu dari sepuluh pengguna jejaring sosial (Deliusno, 2017). Hal tersebut membuka peluang untuk meretas email pengguna dari berbagai jejaring sosial yang pengguna daftarkan. Sehingga data pada email dikhawatirkan dapat disalahgunakan dan tersebar luas.

Layanan email di Indonesia menurut survei internet APJII (Isparmo, 2016) telah digunakan melalui smartphone (84,6 juta pengguna) dan melalui komputer (46,4 juta pengguna) dengan didominasi oleh Google *Mail* (81,8 juta pengguna),

Yahoo (43,6 juta pengguna) dan email perusahaan (5 juta pengguna). Dari ketiga layanan email populer diatas, terdapat beberapa kasus pelanggaran

data keamanan akun yang terjadi. Sekitar satu juta akun Google *Mail* (G-Mail) beserta *password* yang telah terdekripsi diperjualbelikan di pasar gelap *darkweb* (satucode[dot]com, 2017). Dilansir dari Hackread, data tersebut didapat dari kasus peretasan pihak ketiga seperti layanan Last.fm Bircoin Security Forum, Tumblr, 000webhost, Adobe, Dropbox, Revolusi Flash, Lookbook dan Xbox360 ISO. Kasus peretas yang terkuak tahun 2016 adalah serangan peretasan satu miliar akun pengguna Yahoo (Bohang, 2016). Selain itu, Kaspersky Lab (IndoPress, 2016) menunjukan hasil laporan survei global selama tahun 2016 bahwa perusahaan kehilangan 43 persen datanya akibat peretas. Peretasan juga terjadi pada akun email milik staf Gedung Putih yang dilakukan oleh DC Leaks. Hal tersebut mengakibatkan tersebarnya sejumlah informasi sensitif.

Dari berbagai kasus peretas akun email diatas, selain pengamanan akun email pada *password* email, pengamanan juga perlu dilakukan pada isi pesan email. Pengamanan pesan yang dapat digunakan adalah dengan merubah pesan yang di kirim agar menjadi pesan yang seolah-olah tidak berarti, sehingga tidak mudah dimengerti oleh pihak lain yang tidak bertanggung jawab. Hal tersebut termasuk dalam tujuan kriptografi, yaitu kerahasiaan (*confendiality*), integritas data (*data integrity*), autentikasi (*authentication*), dan nir-penyangkalan (*non-repudiation*) (Munir, 2006). Oleh karena itu, kriptografi dapat menjadi salah satu solusi untuk merahasiakan isi pesan pada email.

Pada penelitian sebelumnya, pengamanan pesan email telah dilakukan oleh Albert Ginting dkk. (2015) dengan menggunakan algoritma RSA. Algoritma RSA membuat pesan menjadi lebih aman dengan adanya keunggulan dari RSA yaitu proses pembangkitan kunci RSA didasarkan pada dua bilangan prima yang dipilih secara acak. Sehingga akan menghasilkan hasil penyandian (*ciphertext*) yang berbeda-beda. Penelitian lain terkait pengaman email dilakukan oleh Lusiana Veronica dkk. (2010) menggunakan algoritma AES dan RSA. Algoritma RSA digunakan untuk proses penyandian (enkripsi) berkas lampiran saat pengiriman email karena memiliki tingkat keamanan yang tinggi dengan menghasilkan kunci (*subkey*) yang berbeda untuk setiap putaran proses penyandian. Sedangkan

algoritma RSA dipakai untuk pendistribusian kunci dari algoritma AES dan tanda tangan digital.

Pada penelitian ini, pengamanan pesan email akan menggunakan kombinasi dua algoritma kriptografi. Algoritma pertama yang digunakan adalah algoritma simetri, yaitu algoritma BC3. Pada penelitian sebelumnya, Arif Sasongko dkk. (2011) menjelaskan bahwa algoritma BC3 merupakan algoritma kriptografi *secret-key* yang dikembangkan dengan dua pertimbangan: ketahanan dari berbagai serangan dan efisiensi dalam implementasinya. Pada penelitiannya, algoritma BC3 diimplementasikan pada perangkat keras. Hasil kinerja dari BC3 lebih baik saat dibandingkan dengan algoritma AES yang diimplementasikan juga pada perangkat keras, seperti yang ditujukan pada Tabel 1.1.

Tabel 1. 1 Perbandingan Hasil Kinerja Algoritma BC3 dan AES

Sumber: (Sasongko, Hidayat, Kurniawan, & Sutikno, 2011)

Kriteria	BC3 (128 bit)	AES (128 bit)
Elemen Logika	3098	10338
Proses *Randomizing* (Enkripsi/Dekripsi)	11 clock cycles	54 clock cycles
Ekspansi Kunci	17 clock cycles	10 clock cycles

Waktu performa algoritma BC3 pada perangkat keras juga dibandingkan dengan implementasi yang dilakukan pada perangkat lunak, hasilnya lebih baik dalam proses ekspansi kunci maupun *randomizing* (enkripsi/dekripsi) seperti yang ditunjukan pada Tabel 1.2.

Tabel 1. 2 Perbandingan Waktu Performa Algoritma BC3

Sumber: (Sasongko, Hidayat, Kurniawan, & Sutikno, 2011)

Kriteria	BC3 pada Perangkat Keras (Asumsikan menggunakan pediode waktu tercepat (30.620ns))	BC3 pada Perangkat Lunak (pada AMD Duron Processor 1.2 GHz)
Proses Ekspansi Kunci	0.55454 us	0.7731 us

Kriteria	BC3 pada Perangkat Keras (Asumsikan menggunakan pediode waktu tercepat (30.620ns))	BC3 pada Perangkat Lunak (pada AMD Duron Processor 1.2 GHz)
Proses *Randomizing* (Enkripsi/Dekripsi)	0.35882 us	0.71865 us

Sebelumnya algoritma BC3 diimplementasikan pada perangkat lunak yaitu dengan menggunakan bahasa C (Kurniawan, Algoritma Enkripsi Indonesia BC3, 2008). Pada kecepatan proses enkripsi, algoritma BC3 lebih unggul dibandingkan algoritma Camellia dan memiliki selisih 0.032 detik dibawah AES. Namun pada proses ekspansi kunci, BC3 jauh lebih baik dibandingkan algoritma kriptografi simetri yang lain, seperti AES dan CAMELIA. Tabel 1.3. merupakan perbandingan BC3 dan beberapa algoritma lainnya dengan menggunakan Intel Celeron 1,3Ghz dengan 512MB memori.

Tabel 1. 3 *Perbandingan Implementasi Algoritma Kriptografi pada Perangkat Lunak*

Sumber: (Sasongko, Hidayat, Kurniawan, & Sutikno, 2011)

Algorithm	Excryption Time for 128 millions bit (in second)	Key expansion time
AES	0.453	1.063
BC2	0.765	0.378
BC3	0.485	0.390
Camellia	1.187	1.172
Khazad	0.687	1.063
IDEA	2.235	1.523

Algoritma BC3 termasuk algoritma kriptografi simetri, yang berarti algoritma ini hanya memiliki satu kunci untuk proses enkripsi dan dekripsinya. Hal tersebut menimbulkan permasalahan tentang pendistribusian kunci BC3. Pendistribusian kunci BC3 harus melalui proses yang aman karena jika kunci tersebut diketahui oleh pihak lain, maka pihak tersebut dapat mengetahui isi pesan yang dikirim.

Algoritma kedua pada penelitian ini akan menggunakan algoritma asimetri, yaitu algoritma RSA. Keunggulan algoritma RSA menurut Chandra (Chandra, 2016) terletak pada keamanan yang lebih tinggi dibandingkan algoritma simetris, namun membutuhkan waktu komputasi yang lebih lama. Hal tersebut membuat protokol kriptografi modern saat ini memilih untuk menggabungkan algoritma simetri dan asimetri untuk memperoleh keunggulan pada masing-masing algoritma. Pada penelitian Rojali Budi Permadi (2014) dan Herbert Siregar dkk. (2017) menggunakan algoritma AES dan RSA untuk pengamanan data. Algoritma AES digunakan sebagai enkripsi data yang dikirimkan dan algoritma RSA untuk enkripsi kunci dari algoritma AES. Namun kedua algoritma tersebut bukan diimplementasikan pada pengiriman email, melainkan sistem e-voting oleh Rojali (2014) dan sistem disposisi surat oleh Herbert dkk. (2017).

Pada penelitian ini, algoritma BC3 akan digunakan sebagai pengamanan isi pesan email. Sedangkan algoritma RSA akan digunakan untuk pengamanan kunci dari algoritma BC3. Kombinasi dari kedua algoritma ini diharapkan berpengaruh terhadap tujuan kriptografi yaitu, kerahasiaan dan integritas data.

1.2. Rumusan Masalah

Dari penjelasan pada bagian latar belakang, maka rumusan masalah dalam penelitian ini adalah:

1. Bagaimana mengimplementasikan algoritma BC3 dan RSA pada proses penyandian dan pengungkapan kembali pesan email?
2. Bagaimana pengaruh algoritma BC3 dan RSA pada sistem keamanan pesan email terhadap tujuan kriptografi, yaitu kerahasiaan dan integritas data?
3. Bagaimana hasil pengujian terhadap lama waktu proses dan kecepatan dalam penggunaan algoritma BC3 dan RSA pada berbagai ukuran *plaintext* dan *ciphertext*?

1.3. Tujuan Penelitian

Adapun tujuan dari penelitian ini sebagai berikut:

1. Menerapkan algoritma BC3 dan RSA pada proses penyandian dan pengungkapan kembali pesan email.
2. Mengetahui pengaruh algoritma BC3 dan RSA pada sistem keamanan pesan email terhadap tujuan kriptografi, yaitu kerahasiaan dan integritas data.
3. Mendapatkan data lama waktu proses dan kecepatan penggunaan algoritma BC3 pada saat penyandian dan pengungkapan kembali pesan terenkripsi dengan berbagai ukuran *plaintext* dan *ciphertext*.

1.4. Batasan Masalah

Dalam penelitian ini dilakukan pembatasan masalah antara lain adalah:

1. Pesan email yang digunakan untuk enkripsi maupun dekripsi hanya berupa *plaintext* atau *ciphertext*.
2. Ukuran *plaintext* dan *ciphertext* pada penelitian ini menggunakan format ASCII (*American Standart Code for Information Interchange*).
3. Penelitian ini tidak membandingan dengan algoritma kriptografi yang lain.
4. *Mail server* yang digunakan *server* Google Mail.
5. Pengiriman hanya dapat dilakukan kepada satu akun alamat email.
6. Sistem aplikasi yang dibangun menggunakan bahasa pemrograman Matlab yang hanya dapat dijalankan pada personal komputer (*desktop application*).
7. Pembangkitan kunci RSA menggunakan dua bilangan prima dengan rentang 10 sampai 100.

1.5. Sistematika Penulisan

Adapun sistematika penulisan skripsi ini adalah sebagai berikut

BAB I PENDAHULUAN

Bab ini berisi latar belakang masalah yang melandasi dilakukannya penelitian mengenai sistem keamanan pesan *electronic mail* (email) menggunakan algoritma BC3 dan RSA. Kemudian memaparkan solusi yang penulis tawarkan serta harapan penulis terhadap penelitian ini. Selain

itu, pada bab ini akan diuraikan mengenai rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, serta sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini berisi penjelasan tentang teori-teori keamanan data dan informasi, kriptografi, algoritma BC3, algoritma RSA yang digunakan dalam penelitian.

BAB III METODE PENELITIAN

Bab ini berisi penjelasan langkah-langkah yang akan dilakukan dalam penelitian.

BAB IV HASIL PENELITIAN DAN PEMBAHASAN

Bab ini membahas mengenai hal-hal yang dilakukan selama penelitian berlangsung, mulai dari pembangunan perangkat lunak, hingga pengujian sistem keamanan data email menggunakan algoritma BC3 dan algoritma RSA yang akan digunakan untuk menjawab apa yang sudah dirumuskan dalam rumusan masalah.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi tentang kesimpulan dari keseluruhan penelitian yang telah dilakukan, serta saran dari penulis untuk kegiatan penelitian selanjutnya terkait dengan topik yang sedang dibahas.