BAB I
PENDAHULUAN

Dalam bab ini akan dibahas latar belakang dilaksanakannya penelitian, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian dan sistematika penulisan.

1.1 Latar Belakang

Instant Messaging merupakan alat komunikasi jalur pengiriman pesan yang dapat digunakan dalam jarak jauh. *Instant Messaging* muncul pertama kali pada tahun 1970 diawali dengan munculnya teknologi *Internet.* Pengiriman pesan pada *Instant Messaging* ini memanfaatkan *internet* sebagai media komunikasi. *Instant Messaging* merupakan alat komunikasi yang *powerfull* dikarenakan *Instant Messaging* bersifat *real-time,* mudah didapatkan, biaya terjangkau dan lebih cepat dalam pengiriman pesan.

Menurut Alexander Haryanto pada situs tirto.id pengguna layanan messenger di Indonesia pada tahun 2014 tercatat sebanyak 37,6 juta pengguna, meningkat di 2015 sebanyak 52,9 juta pengguna, 2016 sebanyak 62,6 juta pengguna dan diprediksikan akan terus meningkat pada 2017 (72,5 juta pengguna), 2018 (81,7 juta pengguna) dan 2019 sebanyak 91,6 juta pengguna. Berikut beberapa contoh layanan *Instant Messaging* yang banyak digunakan : WhatsApp menjadi aplikasi favourite di 109 negara atau 55,6 persen dari seluruh dunia, FB Messenger merupakan aplikasi yang difavoritkan di 49 negara, Line digunakan lebih dari 10 negara, dan BBM yang banyak digunakan di satu negara saja.

Pengguna *Instant Messaging* saat ini didominasi oleh para pengguna *platform android.* Menurut situs gs.statcounter.com saat ini di Indonesia Android (91,85 persen) memiliki jumlah pengguna yang lebih banyak dari IOS (5,75 persen), Nokia (0,33 persen), BlackBerry (0,2 persen), Series 40 (0,37 persen) dan *Unknown* (0,84 persen). Banyaknya pengguna *android* ini dikarenakan kelebihannya dibandingkan *IPhone*. Menurut Abi Royen pada situs abi-blog.com berikut beberapa kelebihan platform android : platform

android memiliki OS yang dapat dimodifikasi (*open source*), *User Interface* yang lebih mudah, Memiliki slot untuk MicroSD.

Dengan banyaknya pengguna *Instant Messaging* maka semakin banyak juga developer yang berlomba-lomba membuat aplikasi pengiriman pesan dengan berbagai macam jenis pesan yang dikirim seperti pesan text, gambar, video maupun dalam bentuk suara. Dengan banyaknya aplikasi *Instant Messaging* saat ini, banyak juga hacker yang mencoba mengambil data user untuk disalahgunakan seperti kasus tahun 2014 dimana terdapat hacker yang berhasil membobol jutaan akun pengguna gmail, menurut berita yang beredar hacker tersebut berhasil mencuri informasi hampir 5 juta akun email. Informasi ini bersisi alamat beserta password para pengguna.

Masalah keamanan merupakan suatu aspek yang sangat penting dalam pengiriman data maupun informasi melalui jaringan. Hal ini disebabkan oleh kemajuan di bidang jaringan computer dengan konsep open system nya sehingga akan memudahkan untuk pihak lain masuk kedalam jaringan tersebut. Hal tersebut dapat mengakibatkan proses pengiriman data itu tidak akan aman.

Menurut chin-chen chang (Departement of Computer Science and Informatin Engineering, National Chung Cheng University, Chaiyi, Taiwan) menyebutkan bahwa tingkat keamanan menggunakan media gambar telah menjadi topik penting dalam dunia komputer. Salah satu kelemahan penggunaan media informasi media gambar ini adalah mudahnya dimanipulasi oleh pihak-pihak yang memiliki kepentingan didalamnya. Terlebih jika file gambar tersebut memiliki sifat kerahasiaan yang tinggi. Seperti data-data pribadi, dokumen kenegaraan atau data medis rumah sakit.

Data-data yang diambil dapat disalahgunakan seperti memanipulasi data gambar dengan merubahnya atau menggabungkannya dengan gambar lain sehingga akan membentuk gambar baru dan menggunakannya untuk kepentingan pribadi seperti menyebarkan berita hoax atau melakukan penipuan dengan menggunakan gambar baru tersebut. Salah satu kasus yang

ditemukan peneliti dilingkungan sekitar adalah adanya penggunaan data gambar bukan miliknya yang digunakan untuk melakukan penipuan terhadap pengguna lain dengan cara menggunakan data gambar tersebut sebagai photo profile miliknya.

Contoh kasus lain menurut Rusdi Anto pada penelitian *Kasus-kasus Cyber Crime sebagai Dampak Perkembangan Teknologi Komunikasi yang Meresahkan Masyarakat* adalah pencurian dokumen yang terjadi saat utusan khusus Presiden Susilo Bambang Yudhoyono yang dipimpin Menko Perekonomian Hatta Rajasa berkunjung ke Korea Selatan. Kunjungan tersebut antara lain untuk melakukan pembicaraan kerja sama jangka pendek dan jangka panjang di bidang pertahanan. Delegasi Indonesia beranggotakan 50 orang berkunjung ke Seoul untuk membicarakan kerja sama ekonomi termasuk kemungkinan melakukan pembelian jet tempur latih supersonic T-50 Golden Eagle buatan korsel. Kemudian anggota DPR yang membidangi Pertahanan (Komisi I) menyatakan, berdasarkan informasi dari Kemhan data yang diduga dicuri merupakan data rencana kerja sama pembuatan 50 unit pesawat tempur di PT.Dirgantara Indonesia. Modus dari kejahatan tersebut ialah melakukan pencurian data secara tidak sah.

Kemudian terdapat juga kasus Carding, salah satu jenis *Cyber Crime* yang terjadi di Bandung sekitar Tahun 2003. Carding merupakan kejahatan yang dilakukan untuk mencuri nomor kartu kredit milik orang lain dan digunakan dalam transaksi perdagangan internet.

Kebocoran data ini dapat menyebabkan bermacam-macam kasus seperti beredarnya SMS peawaran kredit, gambar/video porno, nomor kartu kredit, dan lain sebagainya. Kejadian seperti ini dapat disebabkan karena beberapa faktor yaitu adanya perilaku masyarakan yang senang membagikan data pribadi maupun teman dekatnya, kecerobohan pemilik data dalam mengelola data rahasia, saat ini sudah marak fenomena yang menggunakan teknik “social engineering” yang dilakukan pihak tidak bertanggung jawab seperti penipuan hadiah undian, pelanggaran etika atau aturan internal yang dilakukan oleh individu dan/atau kelompok dalam mengelola informasi,

lemahnya manajemen informasi yang diberlakukan dan dipraktikan oleh suatu organisasi, adanya proses digitalisasi dari koleksi data sekunder yang dimiliki oleh suatu komunitas tertentu yang diunggak ke dunia internet, menjamurnya para "pemulung data" di dunia internet, perilaku software rancangan khusus yang diperuntukkan untuk mengoleksi beragam data dan informasi pribadi, dan memang ada kesengajaan dari pihak-pihak tertentu untuk melakukan kegiatan kriminal baik melalui domain eksternal maupun internal.

Sehingga untuk mencegah terjadinya pembobolan dan pencurian data digunakanlah aplikasi kriptografi untuk menjaga kerahasian data pada *Instant Messaging*. Kriptografi itu sendiri bisa diartikan sebagai proses mengubah kembali data yang terenkripsi menjadi bentuk yang dapat dipahami, artinya kriptografi dapat diartikan sebagai proses untuk melindungi data dalam arti yang luas (*Oppliger, 2005).* Kriptografi merupakan metode untuk mengamankan data baik berupa teks maupun gambar. Metode ini dilakukan dengan penyandian atau pengacakan data asli sehingga pihak lain yang tidak memiliki hak akses tidak akan dapat memperoleh informasi yang ada didalamnya. Namun metode ini tidak efisien dikarenakan algoritma nya dirahasiakan, sehingga munculah algoritma baru dengan menggunakan kerahasiaan pada kuncinya. Sehingga algoritmanya akan dapat dipelajari dan diketahui banyak orang namun kunci yang dimiliki itu dirahasiakan. Hukum Kerchkoff menyatakan "Algoritma tidak perlu dirahasiakan, tetapi kuncinya harus rahasia".

Kriptografi sendiri terdiri dari dua jenis yaitu klasik dan modern. Kriptografi yang akan digunakan dalam aplikasi ini adalah kriptografi modern dan salah satu algoritma yang mendukung kriptografi ini adalah Algoritma Elgamal.

Algoritma Elgamal merupakan algoritma enkripsi asimetris yang berarti bahwa kunci yang digunakan untuk enkripsi akan berbeda dengan kunci yang digunakan pada proses dekripsi pesan. Algoritma Elgamal merupakan algoritma yang keamanannya sulit dipecahkan karena terdapat

kesulitan dalam penghitungan logaritma diskret pada modulo prima yang besar sehingga sampai saat ini belum ada solusi untuk memecahkan kekuatan enkripsi tersebut dengan cepat. Keunikan algoritma Elgamal dibandingkan enkripsi asimetris lainnya adalah hasil enkripsi pesan dapat berbeda untuk plainteks yang sama dengan menggunakan kunci public yang sama. Keunikan tersebut merupakan kelebihan yang dimiliki oleh algoritma elgamal.

Ada pula penelitian tentang sistem enkripsi *Instant Messaging* pada *platform android* (Rizky Riadhy, 2014). Dalam penelitian ini peneliti menggunakan algoritma RSA untuk pengamanan data, dan data yang diamankan oleh peneliti merupakan data text saja. Dalam penelitian ini peneliti juga menyarankan agar pesan yang dapat dienkripsi tidak hanya pesan teks. Peneliti menyarankan untuk meneliti pengamanan data gambar, video, atau file di penelitian berikutnya.

Pada penelitian yang dilakukan oleh Andro Alif Rakhman dan Achmad Wahid Kurniawan tentang Implementasi Algoritma Kriptografi RSA dan Vigenere Cipher Pada Gambar Bitmap 8 Bit menjelaskan pada kesimpulan penelitian bahwa hasil citra setelah melakukan enkripsi ukurannya akan menjadi lebih besar karena adanya penambahan bit.

Sehingga pada penelitian ini akan digunakan Algoritma Elgamal agar keamanan data dalam bentuk pesan gambar pada *Instant Messaging* dapat semakin terjaga, sehingga nantinya aplikasi *Instant Messaging* akan memiliki keamanan yang baik dan data pengguna yang terdapat pada aplikasi akan terjaga dari pihak yang dapat menyalahgunakan data tersebut.

1.2 Rumusan Masalah

Rumusan masalah yang akan dibahas pada penelitian ini adalah sebagai berikut.

1. Bagaimana Algoritma Elgamal Bekerja mengamankan pesan gambar pada platform Android.

2. Bagaimana efektifitas dan akurasi sistem enkripsi *Instant Messaging* dengan menggunakan Elgamal pada platform Android dengan berbagai macam *device*.

1.3 Batasan Masalah

Batasan masalah dalam penelitian ini adalah sebagai berikut.

1. Pesan yang dikirimkan pada platform Android berupa pesan gambar dengan format JPEG.
2. *Instant Messaging* yang dibuat hanya untuk pengiriman gambar.
3. Platform yang digunakan adalah Android.
4. Sistem Enkripsi menggunakan Elgamal.

1.4 Tujuan

Dengan adanya permasalahan yang telah dirumuskan, maka tujuan dari penelitian ini adalah sebagai berikut.

1. Memberikan sebuah gambaran cara kerja sistem enkripsi dengan menggunakan Algoritma Elgamal dalam mengamankan pesan gambar pada *Instant Messaging* yang diterapkan pada platform Android.
2. Mengetahui efektifitas dan akurasi sistem enkripsi *Instant Messaging* dengan menggunakan Elgamal pada platform Android dengan berbagai macam *device*.

1.5 Manfaat Penelitian

Dengan dilakukannya penelitian ini diharapkan dapat memberikan manfaat sebagai berikut :

1. Dapat memberikan keamanan yang baik dalam *Instant Messaging* pada platform Android
2. Dapat mengetahui cara kerja Algoritma Elgamal pada *Instant Messaging.*

1.6 Sistematika Penulisan

Sistematika penulisan dalam penelitian ini adalah sebagai berikut.:

BAB 1 PENDAHULUAN

Bab ini berisi latar belakang penelitian, identifikasi masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan dokumen proposal tugas akhir ini.

BAB 2 TINJAUAN PUSTAKA

Bab ini berisi materi-materi hasil literature, teori-teori tentang Kriptografi, Algoritma Elgamal dan File Citra, definisi kutipan dan istilah yang digunakan dalam penelitian.

BAB 3 METODOLOGI PENELITIAN

Bab ini berisi penjelasan langkah-langkah yang akan dilakukan dalam penelitian. Seperti langkah-langkah dalam pembangkitan kunci, enkripsi pada pengiriman pesan dan dekripsi pada saat melakukan penerimaan pesan.

BAB IV HASIL PENELITIAN DAN PEMBAHASAN

Bab ini berisi uraian tentang hasil penelitian dan pembahasan terhadap hasil penelitian yang dilakukan

BAB V KESIMPULAN DAN SARAN

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