BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan telekomunikasi dewasa ini sangat pesat, seiring dengan kebutuhan masyarakat akan mobilitas komunikasi yang meningkat. Berbagai macam fasilitas teknologi telekomunikasi terus dikembangkan agar *user* dapat melakukan komunikasi suara, data dan gambar dengan baik. Peningkatan teknologi komputer tentu memberikan banyak manfaat bagi manusia di berbagai aspek kehidupan, salah satu manfaatnya yaitu untuk menyimpan data, baik data berupa teks ataupun data digital lain seperti gambar, suara dan video dalam menunjang teknologi komunikasi.

Penyimpanan berbagai data atau *file* dalam jumlah yang sangat besar, dapat dilakukan lebih efektif sejak adanya teknologi penyimpanan digital. Data penyimpanan dalam bentuk digital mulai mendampingi *form*at cetak pada media kertas ketika sejumlah pangkalan *storage online* mulai didirikan pada pertengahan tahun enampuluhan, kemudian media optik menyusul pada pertengahan tahun delapanpuluhan (McDonel, 1993 : 7).

Saat ini data yang banyak dimudahkan pengelolaannya dalam bentuk penyimpanan digital. Berbagai kelebihan dibandingkan penyimpanan data manual, seperti tidak memerlukan tempat penyimpanan sebesar penyimpanan fisik dan mempermudah manejemen dan pengelolaan membuat masyarakat mulai beralih dari penyimpanan fisik kepada penyimpanan digital. Kemudahan lainnya

dirasakan terutama pada *back-up file.* Demikian pula data kontak pada telepon genggam yang saat ini menjadi sumber data utama yang mengintegrasikan sebagian besar media sosial yang sedang *booming* seperti Line, WeChat, dan Whatsapp. Media komunikasi tersebut saat ini telah menjadikan nomor kontak menjadi salah satu sumber untuk menambah *friends list*. Seperti pada Line yang harus di *setting* terlebih dahulu untuk penambahan otomatis, Whatsapp yang langsung menambah dari daftar kontak, dan WeChat yang bisa menambah teman dengan mencari teman yang menggunakan aplikasi serupa pada nomor kontak.

Hal ini membuat data *backup* pada telepon genggam semakin penting mengingat maraknya kasus kehilangan atau kecurian telepon genggam yang kian marak terjadi. Umumnya, data kontak dan SMS sulit untuk didapatkan kembali.

Menurut hasil analisis ekonomi (Husnayain, 2007 : 61), kejahatan properti di Indonesia pada tahun 2003 - 2005 semakin meningkat terutama kejahatan properti pada daerah yang berkependudukan padat seperti DKI Jakarta dan kepuluan Riau. Pada tahun 2003 tingkat kejahatan properti di DKI Jakarta berada pada *level* 130 *pcrimrate*, 2004 pada *level* 175, dan 2005 pada *level* 400.

Menurut sumber dari surat kabar tribun tanggal 27 Desember 2012 yang bersumber dari Kepolisian Daerah Metropolitan Jakarta Raya (Polda Metro Jaya) mencatat bahwa tindak kejahatan pada tahun 2012 terjadi setiap 10 menit 6 detik dan kriminalitas yang paling banyak terjadi ialah kasu pencurian dengan pemberatan yang tercatat sebanyak 5682 kasus. Hal ini menjadikan kebutuhan akan aplikasi *backup* data pada telepon genggam semakin dirasakan perlu untuk dimiliki.

Teknologi yang semakin berkembang tidak hanya memberikan dampak positif, namun di satu sisi juga memudahkan *hacker* untuk mencuri data-data, malahan berbagai aplikasi hacking telah disediakan, bahkan diperjualbelikan seperti pada laman *http://en.softonic.com/s/hacking-application*, sehingga untuk menjadi seorang *hacker* tidak memerlukan lagi kemampuan yang begitu dalam sehingga keamanan data yang dikirimkan saat ini juga menjadi salah satu isu yang layak untuk diberikan perhatian.

Salah satu cara untuk mengatasi hal tersebut adalah dengan menggunakan enkripsi. Menurut Munir (2008: 3) Kriptografi adalah ilmu yang mempelajari teknik-teknik perhitungan secara matematik yang berhubungan dengan aspek keamanan, integritas data, serta otentikasi. Dengan mengimplementasikan kriptografi data yang asli nantinya diubah ke dalam bentuk lain sehingga sukar untuk dibaca langsung. Sistem ini nantinya mengimplementasikan enkripsi dengan algoritma Rijndael.

Rijndael merupakan algortima yang dijadikan basis untuk teknik enkripsi *Advanced Encryption Standard* (AES) untuk pengenkripsian data saat ini. Algoritma ini menggunakan kombinasi dari operasi *Exclusive-OR* (XOR), substitusi dengan S-Box, rotasi baris dan kolom, dan *mixcolomn.* Dari dokumen CNSS yang dipublikasikan pada tahun 2003 yang berjudul "*National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information*" mengatakan AES digunakan oleh pemerintah Amerika Serikat serta disetujui *National Security Agency* (NSA) untuk melindungi data untuk tingkat *top secret.*

Algoritma ini berjalan dengan waktu *processing* yang bagus dan dapat diimplementasikan pada komputer biasa (Selent, 2010:1). Menurut Seth dan Mishra (2011:3) yang menganalisa beberapa algoritma enkripsi lain yang sering digunakan (RSA, DES, AES) menyimpulkan bahwa algoritma AES terbukti menggunakan memori yang paling sedikit sehingga nantinya dapat diterapkan pada aplikasi *mobile* untuk sistem ini. Berikut disertakan tabel perbandingan algoritma Rijndael dengan beberapa algoritma lain (Munir, 2006:170).

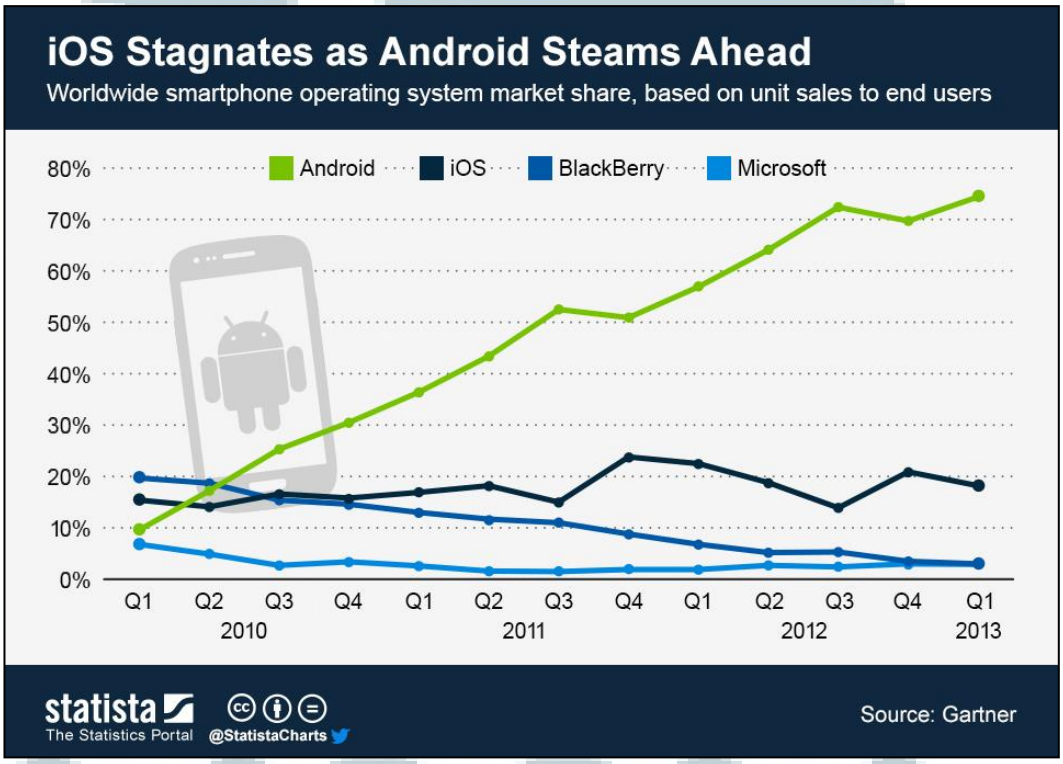
Tabel1.1 Perbandingan Algoritma (Munir, 2006:170)

Cipher	**Pembuat**	**Keterngan**
DES	IBM	*Too weak to use now*
Triple Des	IBM	*Second best choice*
GOST	Uni Soviet	*Good*
RC4	Ronald Rivest	*Some keys are weak*
RC5	Ronald Rivest	*Good but pattened*
Rijndael (AES)	Daemen and Rijmen	*Best choice*
Serpent	Anderson, Biham, Knudsen	*Very strong*
Twofish	Bruce Schneier	*Very strong, widely used*
Blowfish	Bruce Schneier	*Old and slow*
IDEA	Massey dan Xuejia	*Good but patened*

Berangkat dari latar belakang masalah tersebut, penelitian ini bertujuan untuk merancang sebuah aplikasi yang dapat memerintah *gadget* yang diinginkan untuk melakukan *back-up* data kontak dan SMS dari *gadget* lain. *Gadget* yang menerima perintah untuk *back-up* akan segera melakukan enkripsi data kontak dan SMS terlebih dahulu kemudian melakukan *upload* secara otomatis ke Dropbox. Kemudian *user* yang memerintah proses *back-up* dapat mengambil data dari Dropbox. Setelah itu *user* hanya perlu mengunduh data *back-up* tersebut dan

kemudian melakukan *restore* melalui aplikasi pada sistem ini. Melalui sistem ini diharapkan korban yang kehilangan telepon genggam memiliki kesempatan untuk mendapatkan kembali data kontak dan data SMS.

Aplikasi ini dibuat pada sistem operasi Android, sebagai sistem operasi yang paling banyak digunakan saat ini. Terbukti dari penggunaannya yang dapat dilihat pada grafik di bawah.



Gambar 1.1 Statistik 5 Besar Mobile OS di Dunia Dalam Kurun Waktu 2010 sampai dengan 2013
(sumber : www.statista.com/chart/1099/smartphone-operating-system-market-share/)

Dari gambar di atas dapat dilihat penggunaan dari sistem operasi Android dari tahun ke tahun semakin meningkat dibandingkan *Operating System* lainnya. Hal menarik lainnya dari sistem operasi Android ialah pengguna dapat menulis aplikasi Android sendiri sehingga nantinya tentu akan semakin banyak *developer*

yang memberikan sumbangsih agar Android ini semakin berkembang (Burnette, 2008 : 12). Monopoli pasar dan pembuatan aplikasi sendiri inilah menjadi salah satu alasan utama aplikasi ini dibangun pada sistem operasi Android.

Selain dari pengguna Android yang semakin meningkat, Google yang menawarkan sinkronasi kontak untuk setiap pengguna Android dengan email gmail saat ini masih terbatas dengan kontak yang disimpan dengan tipe *link* Google, sehingga kontak yang disimpan pada *device* ataupun kartu SIM, tidak akan tersinkronisasi. Pada kontak di Android tidak dapat dilakukan pemindahan tipe penyimpanan dari tipe *device* ataupun kartu SIM ke tipe *link* goggle untuk memindahkan dari tipe lain kepada tipe *link* Google, haruslah dilakukan peng-*input*-an lagi nomor kontak baik secara manual ataupun *import* kontak. Padahal dalam pratiknya masih banyak pengguna Android yang masih menyimpan data pada *device* ataupun kartu SIM.

Bertolak dari masalah di atas aplikasi ini nantinya dapat menjadi salah satu alternatif maupun pelengkap untuk melakukan *backup* kontak, baik yang tersimpan dengan tipe *link* Google, *device*, maupun kartu SIM. Pada aplikasi ini juga menawarkan fitur *backup* SMS yang belum ditawarkan *sync* Google.

Berdasarkan latar belakang yang telah dikemukakan di atas, judul yang diambil dalam skripsi ini adalah “Implementasi Algoritma Enkripsi Rijndael pada Aplikasi Remote Kontrol Backup Berbasis Android”.

1.2 Rumusan Masalah

Dari gejala masalah yang dijelaskan pada bagian latar belakang, maka rumusan masalah yang akan dibahas dalam penelitian ini adalah bagaimana

membangun aplikasi *remote* kontrol *backup* dengan impelementasi algoritma enkripsi Rijndael dengan basis sistem operasi Android.

1.3 Batasan Masalah

Adapun batasan masalah pada penelitian ini, yaitu:

1. Aplikasi ini dibuat dengan menggunakan bahasa pemrograman Java dan *framework* Android SDK;
2. Aplikasi dibangun untuk *smartphone* Android versi 2.3 (Gingerbread) (API *level* 9) ke atas;
3. *Backup* hanya terbatas pada data kontak dan *Short Message Service* (SMS);
4. Kedua *smartphone* harus terhubung dengan internet untuk menjalankan sistem;
5. *Smartphone* yang akan di *backup* datanya haruslah sudah melakukan *sign-in* ke Dropbox terlebih dahulu.

1.4 Tujuan Penelitian

Penelitian ini bertujuan untuk:

1. Membangun aplikasi yang dapat memberikan instruksi kepada *smartphone* yang berada di lokasi yang berbeda untuk melakukan *backup* kontak dan SMS dan melakukan *upload* ke Dropbox.

2. Mengimplementasikan algoritma enkripsi Rijndael dalam membuat aplikasi ini, dengan tujuan untuk pengamanan data *backup* dari *hacker*.

1.5 Manfaat Penelitian

Manfaat praktis penelitian ini adalah sebagai berikut:

1. Melindungi data kontak dan SMS para pengguna aplikasi ini.
2. Memberikan kesempatan kepada pengguna aplikasi untuk mendapatkan kembali data kontak dan SMS dari *smartphone* jikalau terjadi kehilangan ataupun kecurian.
3. Menyediakan salah satu sarana untuk memindahkan data kontak dan SMS antar *gadget* Android.

Manfaat akademis penelitian adalah sebagai berikut:

1. Menjadi wawasan baru bagi mahasiswa Teknik In*form*atika mengenai Algoritma Rijndael dalam enkripsi data kontak dan SMS pada *smartphone* berbasis Android.
2. Menjadi acuan bagi peneliti berikutnya pada topik yang sama mengenai *auto back-up* pada *smartphone* berbasis Android.