

BAB I

PENDAHULUAN

I.1. Latar Belakang

Kebutuhan masyarakat untuk berkomunikasi secara tidak langsung membuat terciptanya metode pengiriman pesan pada zaman tradisional yaitu dengan surat.

Tetapi dengan surat, pengiriman pesan dapat sampai dalam waktu yang lama.

Perkembangan teknologi membuat lahirnya sebuah alat yang

merupakan cikal bakal terbentuknya *Short Messaging Service* (SMS)

yaitu *pager*. Namun,

dengan kebutuhan masyarakat akan pengiriman pesan yang cepat,

akurat dan aman membuat para ahli teknologi menciptakan sebuah alat yaitu ponsel.

Ponsel atau mobile pertama kali diciptakan sudah dilengkapi dengan fitur

SMS. Teknologi SMS dikembangkan pertama kali oleh *Friedhelm Hillebrand*,

Bernard Ghillebaert, dan *Oculy Silaban*.

Kemudian muncul organisasi-organisasi yang

menciptakan standar teknologi SMS sehingga membuat teknologi SMS

bisa digunakan di seluruh dunia. Dikembangkannya standarisasi SMS dimulai tahun

1985 oleh paya kerjasama antara Perancis dan Jerman. Saat sebuah pesan atau data

menjadi penting dan bersifat *privasi* maka diperlukan perlindungan terhadap data

tersebut. Oleh karena itu para pakar menciptakan sebuah metode algoritma untuk menga

mankan data. Metode ini disebut metode *enkripsi* dan *dekripsi* (Rudy Hendrayanto; 2012).

Dengan adanya kemungkinan penyadapan data, maka aspek keamanan dalam pertukaran informasi menjadi sangat penting karena suatu komunikasi data jarak jauh belum tentu memiliki jalur transmisi yang aman dari penyadapan sehingga keamanan informasi menjadi bagian penting dalam dunia informasi itu sendiri. Saat ini perlindungan informasi menjadi lebih perlu diperhatikan.

Sangat sulit untuk mengamankan pesan atau informasi yang sangat rahasia dari orang-orang yang tidak bertanggung jawab dan tidak berkepentingan. Ada berbagai macam algoritma enkripsi dengan karakteristik masing-masing yang bisa digunakan salah satunya adalah algoritma DES. DES (*Data Encryption Standard*) merupakan algoritma enkripsi yang paling banyak dipakai dunia, yang diadopsi oleh NIST (*National Institute of Standards and Technology*) sebagai standar pengolahan informasi federal A. Oleh karena itu berdasarkan uraian di atas penulis ingin membuat Skripsi kuliah ini dengan merancang dan membuat sebuah aplikasi komputer dengan judul **"Perancangan Aplikasi *Enkripsi* Dan *Deskripsi* SMS Menggunakan Metode DES Berbasis *Android*"**.

I.2. Ruang Lingkup Masalah

I.2.1. Identifikasi Masalah

Berdasarkan identifikasi permasalahan di atas, maka penulis merumuskan masalah yaitu:

1. Bagaimanacarasupaya pesansingkat ini tidak diretas oleh orang yang tidak bertanggung jawab.
2. BagaimanamerancangaplikasienkripsiSMS menggunakan metode DES.
3. BagaimanasupayaaplikasienkripsiSMS lebih mudah digunakan oleh kalangan masyarakat dan berjalan dengan baik.

I.2.2. Rumusan Masalah

Rumusan masalah dalam pembahasan dan permasalahan yang akan dihadapi dalam perancangan aplikasi ini :

1. BagaimanacarasupayaSMS ini tidak diretas oleh orang yang tidak bertanggung jawab ?
2. Bagaimanamerancangaplikasienkripsidan deskripsi SMS menggunakan metode DES ?
3. BagaimanasupayaaplikasienkripsiSMS lebih mudah digunakan oleh kalangan masyarakat dan berjalan dengan baik ?

I.2.3. Batasan Masalah

Sesuai dengan topik yang diangkat dalam penelitian ini, maka pembatasan masalah yang akan dibahas hanya meliputi :

1. Perancangan aplikasi hanya sebatas mengenai enkripsi SMS.
2. Perancangan aplikasi hanya membahas tentang menggunakan metode kriptografi DES.

3. Perancangan aplikasi yang akan dibangun menggunakan bahasa pemrograman *Java*.

I.3. Tujuan Dan Manfaat

I.3.1. Tujuan

Adapun tujuan dari penelitian penulis ini adalah :

1. Merancang aplikasi enkripsi SMS, masyarakat tidak takut akan keamanan data yang mereka kirimkan kepada orang tertentu dan bersifat rahasia.
2. Memberikan keamanan pesanyang dikirimkan oleh pengirim data agar terhindar dari orang yang ingin meretas pesan rahasia.
3. Aplikasi ini dirancang supaya orang lebih berhati-hati dalam mengirimkan pesan yang sangat rahasia.

I.3.2. Manfaat

Adapun manfaat yang akan diperoleh dari aplikasi yang akan dibangun ini adalah:

1. Agar dapat terhindar dari ancaman fabrikasi, intersepsi, interupsi dan modifikasi mengakibatkan kesalahan dalam penerimaan informasi.
2. Dapat menyajikan informasi pesan yang dijamin keasliannya.
3. Diharapkan dengan adanya aplikasi ini dapat menjagadari ancaman terhadap kerahasiaan data.

I.4. Metodologi Penelitian

1. Analisa Tentang Sistem Yang Ada

Pada tahapan analisis sistem, peneliti melakukan analisis sistem yang adadanmempelajarisistem yang sedangberjalandengancaramelakukanpengumpulan data. Adapun beberapa teknik pengumpulan data yang dilakukan oleh penelitiadalah:

a. StudiKepustakaan (*Library Research*)

Penulismelakukanstudipustakadengancaramempelajari, menelitidanmenelaahberbagailiteratur-literaturdariperpustakaan yang bersumberdaribuku-buku, jurnalilmiah, situs-situs di *internet*, danbacaan-bacaan yang adakaitannyadenganenkripsidandekripsi SMS.

b. StudiLapangan (*Field Research*)

Adapun teknik pengumpulan data yang penulis lakukanyaitu :

1. Wawancara (*Interview*)

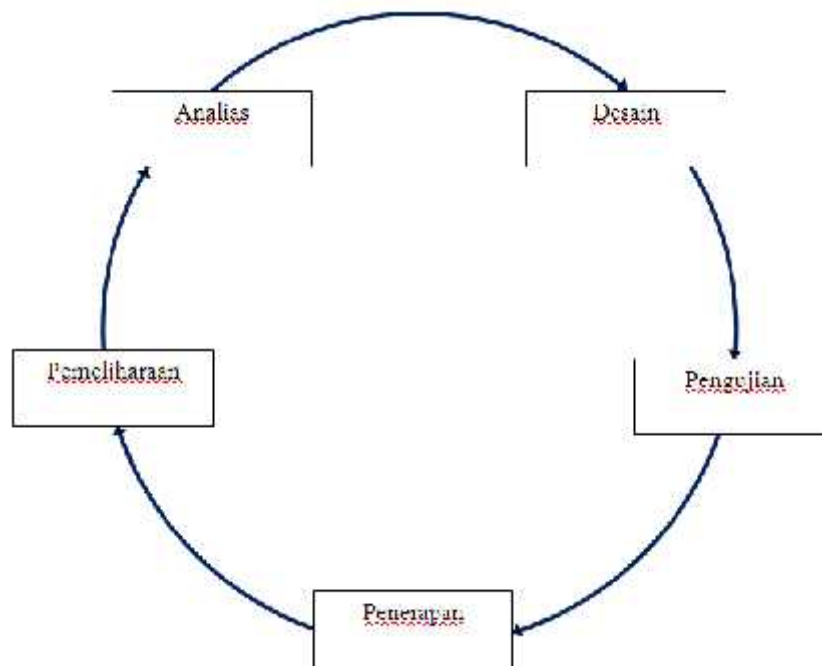
Penulismengadakantanya jawabsecaralangsungdenganpengguna SMS tentangkeamanan SMS.

2. PengamatanLangsung (*Observation*)

Penulismelakukankegiatandenganmengamatilangsungkondisikeamanan SMS dariancaman-ancaman yang ada.

2. Perancangan Sistem

Langkah-langkah yang dilakukan untuk mencapai tujuan perancangan adalah sebagaimana ditunjukkan pada gambar 1:



Gambar I.1. SDCL

Keterangan :

1. Analisis Data adalah analisis, kebutuhan yang diperlukan untuk merancang sistem pendukung keputusan adalah sebagai berikut :

Tabel I.1. Analisis Kebutuhan

No	Kebutuhan	Keterangan
1.	Data	<ul style="list-style-type: none"> • Data pesan

2.	PerangkatKeras	<ul style="list-style-type: none"> • Komputer PC dan Laptop minimal <i>Intel Pentium</i>
3.	PerangkatLunak	<ul style="list-style-type: none"> • <i>Java</i> • <i>Eclipse</i>
4	PelaksanaSistem	<ul style="list-style-type: none"> • Pengguna SMS

2. Desain

Pada tahapan desain yang dilakukandalampembuatan system danaplikasi yang akandirancangpenulisadalah :

- a. Mendesain sistem dengan menggunakan UML (*Unified Modeling Language*).
- b. Menggunakan aplikasi *Eclipse* untuk mendesain aplikasi
- c. Menggunakan aplikasi *visio* untuk menggambarkan *flowchart* sistem

3. Pengujian

Pada tahapan pengujian sistem maka penulis melakukan pengujian secara *black-box*, yang meliputi pengujian fungsional dan ketahanan sistem. Dari hasil pengujian sistem inilah dapat diketahui kesesuaian hasil perancangan dengan analisis kebutuhan yang diharapkan.

4. Penerapan

Pada tahapan penerapan aplikasi dilakukan pada saat semua sistem telah diujidengan baik. Aplikasi yang telah diujisebelumnya akanditerapkan.

5. Pemeliharaan

Pada pemeliharaan sistem yang perlu dilakukan untuk menjaga semua data-data yang telah tersimpan ke dalam aplikasi agar tidak hilang atau terinfeksi virus adalah sebagai berikut :

- a. Melakukan perawatan terhadap komponen-komponen *hardware* dan *software*.
- b. Menggunakan program anti virus agar data maupun *file* tidak terinfeksi atau dirusak oleh virus.
- c. Menerapkan pemeliharaan sistem aplikasi dengan melakukan proses *update*.

I.5. Keaslian Penelitian

Sebagai bukti penelitian yang akan dibuat, maka penelitian akan dibandingkan terhadap penelitian sejenis yang pernah dilakukan. Penelitian pertama yang diangkat oleh Andi Riski Alvianto dan Darmajid dari Institut Teknologi Sepuluh Nopember dengan judul “Pengaman Pengiriman Pesan Via SMS dengan Algoritma RSA Berbasis Android” dan penelitian kedua diangkat oleh Nina Anindyawati dan Nina Anindyawati dari Universitas Sebelas Maret dengan judul “Pembangunan Aplikasi Penyembunyian Pesan Menggunakan Metode *End Of File* (EOF) ke dalam Citra Digital Terhadap Pesan yang Terenkripsi Dengan Algoritma RSA” perbandingannya dapat dilihat pada tabel I.1 di bawah ini :

Tabell.2.PerbandinganSistem Lama dan Yang Akan Dirancang

No	JenisLuaran	IndikatorCapaian
1	ISSN :2337-3520 (2301-928X Print)	JURNAL SAINS DAN SENI ITS Vol. 4, No.1, (2015)
Penelitianpertama : PengamanPengirimanPesan Via SMS denganAlgoritma RSA Berbasis Android		
1.	Target	MerancangperangkatlunakpengamananPesan Via SMS
2.	Solusi	Solusididapatdenganmetode RSA
3.	Bahasapemrograman	<i>java</i>
Penelitiankedua : Pembangunan AplikasiPenyembunyianPesanMenggunakanMetode <i>End Of File</i> (EOF) kedalam Citra Digital TerhadapPesan yang TerenkripsiDenganAlgoritma RSA		
2	ISSN : 2301–7201	JURNAL ITSMART Vol 1. No 1. Juni 2012
1.	Target	Merancangaplikasipenggabungansteganografidanenkripsi datapesan
2.	Solusi	Solusididapatdenganmetode EOF dan RSA
3.	Bahasapemrograman	<i>Visual Basic 6.0</i>
Penelitian yang akandibuat : Perancangan Aplikasi <i>Enkripsi Dan Deskripsi</i> SMS Menggunakan Metode DES Berbasis <i>Android</i>		
1.	Target	aplikasikeamanan SMS
2.	Solusi	SolusididapatdenganmetodeDes
3.	Bahasapemrograman	<i>Java</i>

I.6. SistematikaPenulisan

SistematikapenulisanSkripsiiniadalahsebagaiberikut.

BAB I PENDAHULUAN

Dalam bab ini penulis menguraikan mengenai latar belakang, ruang lingkup permasalahan, tujuan dan manfaat, metode penelitian, lokasi penelitian dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Dalam bab ini mencakup uraian penyelesaian secara teoritis serta konsep baru dalam penyelesaian masalah berkenaan dengan sistem dan fokus kajian. Adapun landasan teori yang diuraikan oleh penulis adalah: penjelasan mengenai sistem, informasi, materi tentang digunakan, serta metode konseptual yang menggambarkan cara kerja dari sistem yang akan dirancang.

BAB III ANALISIS DAN PERANCANGAN

Pada bab ini berisi analisa sistem yang sedang berjalan, perancangan proses dalam bentuk diagram UML yang mencakup analisa dan perancangan sistem pengolahan data yang mencakup seluruh aktivitas yang terjadi pada sistem yang akan dibangun.

BAB IV HASIL DAN UJI COBA

Dalam bab ini penulis menguraikan tentang tampilan hasil sistem yang dirancang beserta pembahasannya, kelebihan dan kekurangan sistem yang dirancang.

BAB V KESIMPULAN DAN SARAN

Dalam bab ini penulis menguraikan tentang kesimpulan dan saran untuk meningkatkan kualitas dari aplikasi yang sudah dirancang.