BAB I

PENDAHULUAN

I.1. Latar Belakang

Beberapa tahun terakhir ini terjadi perkembangan yang pesat pada teknologi, salah satunya adalah telepon selular (ponsel). Mulai dari ponsel yang hanya bisa digunakan untuk bicara dan sms hingga "ponsel cerdas" (*smartphone*) yang memiliki berbagai fungsi seperti multimedia, *multiplayer games*, transfer data, video *streaming* dan lain – lain. Berbagai perangkat lunak untuk mengembangkan aplikasi ponsel pun bermunculan, diantaranya yang cukup luas adalah android.

Salah satu fasilitas yang disediakan ponsel adalah untuk melakukan pengiriman data berupa pesan singkat melalui *short message service* (SMS). Namun dengan fasilitas SMS yang ada, timbul pertanyaan mengenai keamanan informasi jika seseorang ingin mengirimkan suatu informasi rahasia melalui fasilitas SMS.

Untuk menangani masalah keamanan ini, salah satu teknik yang sudah dikembangkan untuk mengamankan data adalah dengan menggunakan algoritma penyandian data. Algoritma penyandian data saat ini telah semakin banyak jumlahnya, sejalan dengan berkembangnya ilmu yang memperlajari penyandian data tersebut. Ilmu ini biasa disebut Kriptografi.

Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan *(Cryptography is the art and science of keeping messages secure).* Kata *"seni"* di dalam definisi di atas berasal dari fakta sejarah bahwa pada masa-masa awal sejarah kriptografi, setiap orang mungkin mempunyai cara yang unik untuk merahasiakan pesan. Cara-cara unik tersebut mungkin berbeda-beda pada setiap pelaku kriptografi sehingga setiap cara menulis pesan rahasia pesan mempunyai nilai estetika tersendiri. Pada perkembangan selanjutnya, kriptografi berkembang menjadi sebuah disiplin ilmu sendiri karena teknik-teknik kriptografi dapat diformulasikan secara matematik sehingga menjadi sebuah metode yang formal.

Vigenere Cipher merupakan salah satu algoritma kriptografi klasik untuk menyandikan suatu plaintext dengan menggunakan teknik substitusi. Vigenere cipher pada dasarnya cukup rumit untuk dipecahkan.

Android adalah sistem operasi berbasis Linux yang dirancang untuk perangkat seluler layar sentuh seperti telepon pintar dan komputer tablet. Android awalnya dikembangkan oleh Android, Inc. dengan dukungan finansial dari Google, yang kemudian membelinya pada tahun 2005. Sistem operasi ini dirilis secara resmi pada tahun 2007, bersamaan dengan didirikannya Open Handset Alliance, konsorsium dari perusahaan-perusahaan perangkat keras, perangkat lunak, dan telekomunikasi yang bertujuan untuk memajukan standar terbuka perangkat seluler. Ponsel Android pertama mulai dijual pada bulan Oktober 2008.

Sistem keamanan dalam perancangan aplikasi keamanan data SMS dirasakan penting karena dapat meningkatkan privasi dan kualitas keamanan komunikasi antara individu. Dengan dilatarbelakangi oleh perkembangan kecerdasan buatan

dan pentingnya sistem keamanan, maka penelitian ini diangkat dengan judul "**Rancang Bangun Aplikasi Keamanan Data SMS Dengan Menggunakan Kriptografi Vigenere Cipher Berbasis Android**".

I.2. Ruang Lingkup Permasalahan

I.2.1. Identifikasi Masalah

Masalah utama dalam perancangan aplikasi Keamanan data SMS ini adalah:

1. Keamanan data SMS pada jaringan selama ini dikirim dalam bentuk byte plain yang memungkinkan resiko diinteropsi oleh pihak yang tak berwenang.
2. Masih minimnya usaha yang dilakukan untuk pencegahan serangan *Men In The Middle* dalam pengiriman data.
3. Belum diketahui hasil analisis performance / kinerja algoritma kriptografi Vigenere Cipher.

I.2.2. Perumusan Masalah

Dalam penelitian skripsi ini, permasalahan yang akan dibahas oleh penulis adalah :

1. Bagaimana merancang sebuah aplikasi pada keamanan data SMS menggunakan algoritma Vigenere Cipher ?
2. Bagaimana meminimalisirkan pencegahan serangan *Men In The Middle* dalam pengiriman data ?
3. Bagaimana mempermudah pengetahuan *user* dalam menganalisis performance / kinerja algoritma kriptografi Vigenere Cipher ?

I.2.3. Batasan Masalah

Batasan masalah pada penelitian ini yaitu:

1. Data yang menjadi masukan terhadap sistem yaitu berupa huruf dan angka.
2. Keluaran sistem yang ditargetkan pada penelitian ini yaitu file yang telah di enkripsikan dengan Vigenere Cipher.
3. Algoritma yang digunakan untuk melakukan enkripsi data pada penelitian ini menggunakan algoritma Vigenere Cipher.
4. Bahasa pemrograman yang digunakan untuk membuat aplikasi yaitu *Android, intellij idea, java sdk, android sdk, genymotion.*
5. Pemodelan sistem dilakukan dengan UML 2.0.

I.3. Tujuan dan Manfaat

I.3.1. Tujuan

Adapun tujuan dari penelitian ini adalah :

1. Membuat aplikasi keamanan data SMS dalam jaringan yang dilengkapi keamanan data dengan algoritma Vigenere Cipher.
2. Meningkatkan jaminan keamanan dan privasi dalam proses keamanan data SMS saat pengguna melakukan komunikasi.
3. Mengetahui tingkat keamanan enkripsi data menggunakan algoritma Vigenere Cipher.
4. Mengetahui seberapa besar efektivitas enkripsi pada algoritma Vigenere Cipher.

I.3.2. Manfaat

Adapun manfaat dari penelitian ini yaitu:

1. Membuat sistem keamanan dan privasi dalam proses keamanan data SMS pada jaringan akan memberi kenyamanan pengguna dalam melakukan komunikasi.
2. meminimalkan terjadi penyadapan komunikasi oleh *Man In The Midle* akan mengurangi tingkat kejahatan *cyber*.
3. Diketahuinya tingkat keamanan enkripsi data menggunakan algoritma Vigenere Cipher akan meningkatkan kesadaran *programmer* lain dalam upaya menjaga data pribadi pengguna aplikasi yang dibuatnya.
4. Dapat diterapkan pada teknologi android dalam keamanan SMS.

I.4. Metodologi Penelitian

Metode penelitian yang dipakai oleh penulis adalah metode penelitian deskriptif atau disebut juga metode penelitian analitis. Dalam metode penelitian deskriptif ini penulis menggunakan beberapa metode yaitu:

a. Pengamatan (Observation)

Dalam metode pengamatan ini penulis diberi kesempatan untuk melakukan pengamatan secara langsung mengenai proses enkripsi keamanan data sms.

b. Wawancara (Interview)

Melakukan metode wawancara kepada pengguna android mengenai keamanan data sms.

c. Studi Kepustakaan (Library Research)

Penelitian ini dilakukan dengan mengumpulkan bahan-bahan pustaka yang berkaitan dengan akuntansi pendapatan pada perpustakaan-perpustakaan umum.

Penulis menggunakan metode penelitian deskriptif dikarenakan pemecahan masalah yang aktual yaitu masalah yang berkembang pada bidang *artifisial intelligence* yang sekarang sedang berkembang pesat. Dengan metode deskriptif, data yang telah penulis kumpulkan mula-mula disusun, dijelaskan, dianalisis, dan kemudian diimplementasikan dalam sebuah perangkat lunak.

1.4.1. Metode Pengembangan Perangkat Lunak

Metodologi atau teknik yang digunakan dalam pengembangan dan pembuatan perangkat lunak meliputi metodologi konvensional (sebelum pertengahan 1970-an), struktural klasik (mulai pertengahan 1970-an), struktural modern (mulai pertengahan 1980-an) dan *post modern* (mulai akhir 1980-an).

Metodologi pengembangan perangkat lunak yang penulis gunakan adalah *post modern* yang populer digunakan mulai akhir 1980-an. Metodologi ini mencirikan adanya paradigma *objectoriented* dan multimedia. Beberapa *tool* yang bisa digunakan sebagai alat pengembangan dan pembuatan program yang berorientasi objek (*ObjectOrientedProgramming*).

1.4.2. Prosedur Perancangan

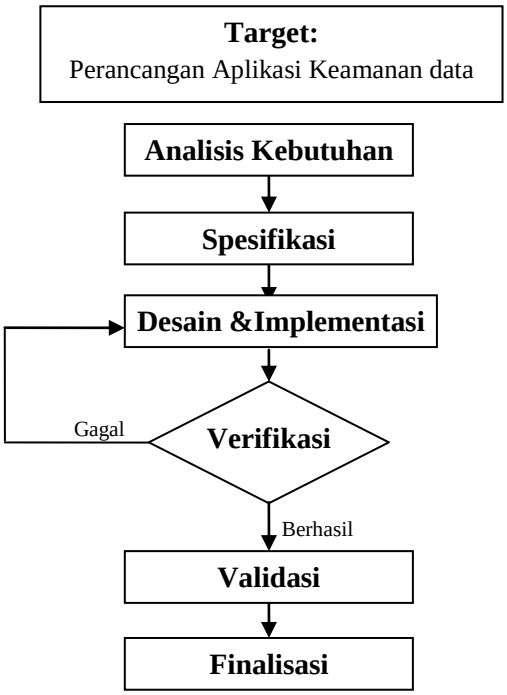
Merupakan tata cara dan langkah-langkah yang diperlukan untuk mencapai tujuan perancangan yang dilakukan. Langkah-langkahnya adalah :

a. Menganalisis permasalahan keamanan yang ada dalam aplikasi Keamanan data SMS.

b. Merancang sistem yang baru dengan menggunakan model UML (*Unified Modeling Language*).

c. Membuat aplikasi dengan bahasa pemrograman *Android, intellij idea, java sdk, android sdk, genymotion.*.

Berikut adalah skema dalam malaksanakan penelitian :



Gambar 1. Prosedur Perancangan

Pada gambar prosedur perancangan sistem di atas dapat diuraikan ke dalam beberapa tahap yaitu Tujuan Penelitian, tahap Analisa (*Analisys*), Spesifikasi, tahap Perancangan (*Design*) dan tahap Penerapan (Implementasi), Verifikasi serta tahap Validasi. Dan kegiatan yang dilakukan pada tiap-tiap tahap adalah sebagai berikut :

1. Target/Tujuan Penelitian

Target penelitian ini yaitu menjawab, menganalisa dan merancang sebuah aplikasi sesuai dengan perumusan masalah yang telah dikemukakan oleh penulis dalam melakukan penelitian, adapun perumusan masalah penelitian yaitu :

a. Bagaimana merancang sebuah aplikasi pada keamanan data SMS menggunakan algoritma Vigenere Cipher ?
b. Bagaimana meminimalisirkan pencegahan serangan *Men In The Middle* dalam pengiriman data ?
c. Bagaimana mempermudah pengetahuan *user* dalam menganalisis performance / kinerja algoritma kriptografi Vigenere Cipher ?

2. Analisis Kebutuhan

Tujuan utama tahap analisis kebutuhan sistem adalah untuk mengetahui syarat kemampuan atau kriteria yang harus dipenuhi oleh sistem agar keinginan pemakai sistem dapat terwujud. Tahap analisis ini terbagi menjadi dua, yaitu analisis kebutuhan sistem fungsional dan analisis kebutuhan sistem nonfungsional yang dapat dilihat pada Tabel I.1 dan Tabel I.2 dibawah ini:

Tabel I.1. Kebutuhan Sistem Fungsional

No	Kebutuhan	Rincian Kebutuhan
1.	Target Pengguna	– Masyarakat
3.	Fungsi Sistem	– Meningkatnya jaminan keamanan dan privasi dalam proses keamanan data SMS pada jaringan akan memberi kenyamanan pengguna dalam melakukan komunikasi. – Kecilnya kemungkinan terjadi penyadapan

		komunikasi oleh *Man In The Midle* akan mengurangi tingkat kejahatan *cyber*. – Diketahuinya tingkat keamanan enkripsi data menggunakan algoritma Vigenere Cipher akan meningkatkan kesadaran *programmer* lain dalam upaya menjaga data pribadi pengguna aplikasi yang dibuatnya.
4.	Perangkat Lunak	– *Android, intellij idea, java sdk, android sdk, genymotion.*
5.	Prosedur	– Mendaftarkan data keanggotaan – Melakukan otentikasi akses – Melakukan komunikasi Keamanan data SMS – Memasukkan kunci publik untuk membaca data Keamanan data SMS yang telah terenkripsi.
6.	Pelaksana Sistem	– *User*
7.	Pengolah Sistem	– *Programmer*

Tabel I.2. Kebutuhan Sistem Nonfungsional

No	Kebutuhan	Rincian Kebutuhan
1.	Sistem Operasi	– Minimal Windows XP SP 2

2.	Prosesor	– Minimal Intel DualCore
3.	RAM	– Minimal 2GB
4.	Hardisk	– Minimal 120GB
5.	Monitor/LCD	– Minimal Resolusi 1024x768

3. Spesifikasi dan Desain

   Perancangan sistem menggunakan bahasa pemrograman *Android, intellij idea, java sdk, android sdk, genymotion* . Spesifikasi komputer yang digunakan minimal *Intel* DualCore, *RAM* 2GB serta *Hard Drive* 120Gb dan Model yang digunakan dalam merancang sistem informasinya adalah dengan model UML (*Unified Modeling Language*).

4. Implementasi dan Verifikasi

   Berisi langkah-langkah yang dilakukan dalam pembuatan alat serta tahapan-tahapan pengujian yang dilakukan untuk masing-masing blok peralatan yang dirancang.

5. Validasi

a. Berisi langkah-langkah yang dilakukan saat pengujian peralatan secara keseluruhan, besaran-besaran yang akan diuji, dan ukuran untuk menilai apakah alat sudah bekerja dengan baik sesuai spesifikasi.

I.6. Sistematika Penulisan

Adapun sistematika penulisan yang diajukan dalam skripsi ini adalah sebagai berikut :

BAB I : **PENDAHULUAN**

Dalam bab ini dijelaskan latar belakang penulisan skripsi, ruang lingkup permasalahan, tujuan dan manfaat, metodologi penelitian, dan sistematika penulisan skripsi.

BAB II : **TINJAUAN PUSTAKA**

Dalam bab ini dicantumkan teori-teori yang relevan yang dijadikan dasar dalam membangun "*Rancang Bangun Aplikasi Keamanan Data SMS Dengan Menggunakan Kriptografi Vigenere Cipher Berbasis Android*".

BAB III : **ANALISIS MASALAH DAN RANCANGAN PROGRAM**

Bab ini berisikan tentang analisa sistem yang sedang berjalan, evaluasi sistem yang berjalan, disain sistem, desain data, hubungan antar entitas, perancangan basis data, desain arsitektur, *Unified Modelling Language* (UML), struktur program, desain antarmuka, desain *input*, desain *output*, dan struktur menu pada program aplikasi yang dibangun.

BAB IV : **HASIL DAN UJI COBA**

Berisikan tentang tampilan hasil aplikasi yang dirancang, pembahasan hasil aplikasi yang dirancang, pengujian serta kelebihan dan kekurangan dari aplikasi yang dirancang.

BAB V : **KESIMPULAN DAN SARAN**

Berisikan kesimpulan dari penelitian dan hasil akhir yang diperoleh dari perancangan aplikasi, serta saran-saran yang berisi hal-hal penting untuk diperhatikan atau dijalankan pada masa yang akan datang untuk kesempurnaan hasil penelitian selanjutnya.