BAB I

PENDAHULUAN

I.1. Latar Belakang

Kemajuan teknologi di bidang komputer memungkinkan ribuan orang dan komputer di seluruh dunia terhubung dalam satu dunia maya yang dikenal sebagai cyberspace atau Internet. Begitu juga ratusan organisasi seperti perusahaan, lembaga negara, lembaga keuangan, militer dan sebagainya. Tetapi kemajuan teknologi ini selalu diikuti dengan sisi buruk dari teknologi itu sendiri. Salah satunya adalah rawannya keamanan data sehingga menimbulkan tantangan dan tuntutan akan tersedianya suatu sistem pengamanan data yang sama canggihnya dengan kemajuan teknologi komputer itu sendiri. Ini adalah latar belakang berkembangnya sistem keamanan data untuk melindungi data yang ditransmisikan melalui suatu jaringan komunikasi.

Sekarang ini keamanan yang efektif dari suatu sistem sangat diperlukan untuk kegiatan bisnis sehari-hari. Sistem yang aman bisa memberikan tingkat kepercayaan yang tinggi kepada pengguna sehingga bisa memberi nilai tambah dan daya guna bagi sistem itu sendiri. Pengguna akan merasa nyaman dan aman ketika berhubungan dengan sistem yang bisa mengamankan data pengguna dari penyerang.

Ada beberapa cara melakukan pengamanan data yang melalui suatu saluran, salah satu diantaranya adalah kriptografi. Dalam kriptografi, data yang sangat rahasia akan disamarkan sedemikian rupa sehingga kalaupun data itu bisa

dibaca maka tidak bisa dimengerti oleh pihak yang tidak berhak. Data yang akan dikirimkan dan belum mengalami penyandian dikenal dengan isitilah plaintext, dan setelah disamarkan dengan suatu cara penyandian, maka plaintext ini akan berubah menjadi ciphertext. Salah satunya Algoritma yang dapat mengamankan data yang penulis bahas adalah Algoritma One Time Pad, adapun kelebihan OTP adalah mudah diimplementasikan tapi sulit untuk di tembus. Algoritma One Time Pad merupakan salah satu dari algoritma kunci. Sampai saat ini, algoritma One Time Pad masih dipercaya sebagai metode penyandian, kriptografi One Time Pad menggunakan kunci yang sama untuk enkripsi dan dekripsi, Dan berdasarkan uraian diatas penulis tertarik memilih judul **”Perancangan Dan Implementasi Enkripsi Dan Dekripsi File Dengan Algoritma One Time Pad Berbasis Android”**

I.2. Ruang Lingkup Permasalahan

I.2.1. Identifikasi Masalah

Berdasarkan latar belakang masalah yang telah dikemukakan, maka dapat di identifikasi hal-hal sebagai berikut :

1. Rawannya keamanan data sehingga menimbulkan tantangan dan tuntutan akan tersedianya suatu sistem pengamanan data.
2. Kerahasiaan merupakan faktor penting untuk menjaga isi informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka informasi.

I.2.2. Rumusan Masalah

Adapun rumusan masalah dari skripsi ini adalah

1. Bagaimana androi melakukan enkripsi file.
2. Bagaimana cara mengamankan data dengan menggunakan teknologi kriptografi berbasis android.
3. Bagaimana membuat sebuah penyandian data dengan menggunakan metode One Time Pad untuk mengamankan sebuah data dari orang-orang yang tidak berhak.

I.2.3. Batasan Masalah

Batasan masalah yang penulis kemukakan dalam sistem ini adalah:

1. Data yang digunakan berupa data file yang di enkripsi/dekripsi dalam bentuk Text.
2. Metode dan Algoritma yang di gunakan adalah *One Time Pad.*
3. Program dibuat berbasis android
4. Bahasa Pemrogram *Java*, dan *Eclipse*

I.3. Manfaat dan Tujuan Penelitian

I.3.1. Manfaat Penelitian :

1. Membuat sebuah program aplikasi untuk mengamankan data dalam aplikasi android
2. Membantu pengguna dalam mengamankan data dengan menggunakan algoritma One Time Pad.

I.3.2. Tujuan Penelitian

1. Sebagai bahan pembelajaran untuk mengerti algoritma *One Time Pad* dalam penyandian data.
2. Menambah wawasan penulis tentang bagaimana merancang serta mengembangkan kemampuan tentang kriptografi terutama algoritma *One Time Pad.*

I.4. Metodelogi Penelitian

Tahapan yang dilaksanakan pada saat penelitian adalah sebagai berikut:

1. Metode Pengumpulan Data

   Beberapa metode pengumpulan data yang dilakukan oleh penulis yaitu:

   a. Studi kepustakaan (*library search*)

      Untuk mendapatkan hasil teori yang valid untuk dijadikan sebuah landasan, penulis mencari beberapa buku referensi dari beberapa perpustakaan seperti mencari buku tentang keamanan data, kriptografi dan *Algoritma One Time Pad*.

   b. Pengumpulan data melalui *surfing* (*field research*)

      Pencarian atau penjelajahan untuk mencari data yang dapat dijadikan landasan penulis yang sesuai melalui internet, seperti mencari file artikel yang membahas masalah kriptografi, keamanan data dan *Algoritma One Time Pad.*

c. Wawancara (*interview*)

Melakukan konsultasi atau tanya jawab secara langsung kepada orang yang lebih megetahui tentang kriptografi dan *Algoritma One Time Pad* yang penulih bahas.

2. Metode Perancangan Sistem

a. Analisis Kebutuhan

Analisis kebutuhan adalah yaitu analisa Algoritma One Time Pad yang dilakukan untuk menentukan input dan output yang diinginkan berdasarkan rumus yang di ada.

b. Analisa dan Perancangan Sistem

Perancangan sistem merupakan tahapan yang dilakukan untuk membuat sebuah rancangan program berdasarkan input dan output yang diinginkan.

c. Implementasi Sistem

Setelah pembuatan perancangan sistem maka langkah selanjutnya adalah mengimplementasi hasil perancangan ke dalam program

d. Evaluasi Sistem

Evaluasi merupakan langkah setelah *Algoritma One Time Pad* dimplementasikan untuk mengetahui kesalahan atau trouble yang mungkin terjadi, sampai dipastikan sistem dapat berjalan dengan sempurna.

e. Penulisan laporan penelitian

Ini adalah tahap akhir dari penelitian .

I.5. Keaslian Penelitian

Adapun keaslian penelitian yang dibuat oleh penulis dapat dilihat pada Tabel I.1. sebagai berikut :

Tabel I.1. Keaslian Penelitian

No.	Materi Perbandingan	Instrumen
JUDUL : ANALISIS KRIPTOGRAFI MENGGUNAKAN ALGORITMA *VIGENERE CIPHER* DENGAN MODE OPERASI *CIPHER BLOCK CHAINING* (CBC)		
1	Nama Peneliti	Erna Kumalasari Nurnawati (2008)
	Hasil Penelitian	1. File hasil enkripsi disimpan menggunakan nama yang sama dengan file asli tetapi ekstensinya menggunakan enc. 2. Pada saat proses enkripsi dan dekripsi dibutuhkan memori yang sangat besar yang mengakibatkan proses menjadi lama. Untuk itu penulis membatasi panjang kunci sampai dengan 10 karakter. 3. Algoritma *Vigenere Cipher* asli hanya menampung 26 huruf alfabeth dalam bentuk huruf kecil sedangkan tanda baca lain tidak dapat terbaca. Sehingga perlu dilakukan suatu pengevaluasian yaitu dengan memperluas jangkauan 26 huruf alfabeth tersebut menjadi 256 karakter ASCII. Dari pengevaluasian tersebut maka algoritma *Vigenere Cipher* asli tersebut disebut dengan algoritma ***Vigenere Cipher +***. 4. Panjang kunci mempengaruhi waktu untuk pengenkripsian dan pendekripsian *file*. Semakin panjang kata kunci yang digunakan maka semakin cepat waktu yang dibutuhkan.
JUDUL : APLIKASI KRIPTOGRAFI FILE MENGGUNAKAN ALGORITMA BLOWFISH		
2	Nama Peneliti	Suriski Sitinjak, Yuli Fauziah, Juwairiah (2010)
	Hasil Penelitian	Berdasarkan keseluruhan proses yang

		dilakukan untuk membangun Aplikasi Kriptografi File menggunakan Algoritma Blowfish ini dapat disimpulkan bahwa aplikasi ini telah berhasil dibangun dan dapat berfungsi sesuai tujuan, yaitu mengamankan data ataupun informasi yang berupa file (plainteks) dengan mengacak file tersebut sehingga tidak dapat dibaca atau dimengerti. Aplikasi ini juga telah berhasil mengembalikan file yang telah diacak tersebut (cipherteks) seperti semula dengan menggunakan kunci yang sama sewaktu enkripsi. Selain itu, aplikasi ini dapat digunakan untuk melihat kinerja algoritma Blowfish dalam pengimplementasiannya, yaitu bagaimana kecepatan proses enkripsi/dekripsi jika dikaitkan dengan ukuran dari sebuah file. Kecepatan proses enkripsi/dekripsi bergantung pada besarnya ukuran file, semakin besar ukuran file semakin banyak waktu yang dibutuhkan untuk enkripsi/dekripsi. Terjadi penambahan byte pada file hasil enkripsi yang mengakibatkan ukuran file enkripsi dan file plainteks sedikit berbeda, tetapi ketika file enkripsi dikembalikan (didekripsi) ukuran file akan kembali seperti ukuran file plainteksnya.
JUDUL : **Implementasi Algoritma One Time Pad Pada Penyimpanan Data Berbasis Web**		
2	Nama Peneliti	**Hengky Mulyono, Rodiah (2013)**
	Hasil Penelitian	Berdasarkan pada analisis hasil pengujian terhadap implementasi algoritma *One Time Pad* pada aplikasi penyimpanan data dan informasi dapat di ambil kesimpulan bahwa aplikasi penyimpanan data dan informasi dengan mengimplementasikan algoritma *One Time Pad* ini dapat menjaga keamanan dan kerahasiaan data atau informasi yang tersimpan didalamnya dan dapat memastikan bahwa *user* yang mengakses data maupun informasi pada sistem tersebut adalah *user* yang benar-benar memiliki

		wewenang dalam hal ini adalah pihak yang memiliki kunci dari data atau informasi yang disimpan.
JUDUL : PERANCANGAN APLIKASI *MOBILE CITY DIRECTORY* YOGYAKARTA BERBASIS ANDROID		
3	Nama Peneliti	**Gusti Ngurah Darma P, Sigit Purnomo WP, Kusworo Anindito3**
	Hasil Penelitian	Aplikasi *mobile city directory* Yogyakarta ini diharapkan dapat membantu pengguna dalam memberikan informasi tentang tempat-tempat di Yogyakarta, sehingga pengguna tidak mengalami kesulitan dalam mencari lokasi suatu tempat dan dapat mengetahui informasi lain mengenai tempattempat di yogyakarta. Selain itu penelitian tentang perancangan aplikasi mobile city directory yogyakarta ini dapat dijadikan referensi untuk penelitian yang relevan dengan penelitian ini untuk dapat lebih dikembangkan lagi.
JUDUL : MOBILE GIS FASILITAS UMUM UNTUK PENGGUNA JALAN BERBASIS ANDROID		
4	Nama Peneliti	Fadhoelor Rohman, Agung Budi Cahyono
	Hasil Penelitian	- Dapat didesain dan dikembangkan aplikasi SIG fasilitas umum untuk pengguna jalan berbasis *mobile phone* dengan pemograman bahasa Java. - Aplikasi *mobile phone* dapat diakses pada telepon genggam dengan sistem operasi Android minimal - Aplikasi *mobile phone* dapat memberikan informasi tentang lokasi fasilitas umum, jarak dan waktu tempuh dari lokasi pengguna menuju lokasi fasilitas umum. - Aplikasi *mobile phone* dapat menampilkan fasilitas umum untuk pengguna jalan di Madura yaitu SPBU sebanyak 35, Kantor Polisi sebanyak 11, dan Puskesmas/Rumah Sakit sebanyak 9. - Informasi jarak pada aplikasi mobile phone merupakan jarak rute jalan terpendek berdasar metode perhitungan jarak dari Google Maps.

I.6. Sistematika Penulisan

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

BAB I : PENDAHULUAN

Pada bab ini menerangkan tentang latar belakang, ruang lingkup permasalahan, tujuan dan manfaat, metode penelitian dan sistematika penulisan.

BAB II : TINJAUAN PUSTAKA

Pada bab ini menerangkan teori dasar yang berhubungan dengan program yang dirancang serta bahasa pemrograman yang digunakan.

BAB III : ANALISA DAN DESAIN SISTEM

Pada bab ini mengemukakan analisa masalah program yang akan dirancang dan rancangan program yang digunakan pada penulisan Skripsi ini.

BAB IV : HASIL DAN PEMBAHASAN

Pada bab ini mengemukakan tentang hasil implementasi sstem yang dirancang mencakup uji coba sistem, tampilan serta perangkat yang dibutuhkan. Analisa sistem dirancang untuk mengetahui kelebihan dan kekurangan sistem yang dibuat.

BAB V : KESIMPULAN DAN SARAN

Dalam bab ini berisikan berbagai kesimpulan yang dapat dibuat berdasarkan uraian yang telah disimpulkan, serta saran kepada perusahaan.