BAB I

PENDAHULUAN

I.1. Latar Belakang

Keaslian sebuah informasi merupakan suatu hal yang harus diperhatikan. Masalah tersebut penting karena jika sebuah informasi dapat di akses oleh orang yang tidak berhak atau tidak bertanggung jawab, maka keakuratan informasi tersebut akan diragukan, bahkan akan menjadi sebuah informasi yang menyesatkan (Paryati ; 2012 : 379).

Masalah keaslian dan kerahasiaan data merupakan hal yang sangat penting dalam suatu organisasi maupun pribadi. Apalagi jika data tersebut berada dalam suatu jaringan komputer yang terhubung/terkoneksi dengan jaringan lain. Hal tersebut tentu saja akan menimbulkan resiko bilamana informasi yang sensitif dan berharga tersebut diakses oleh orang-orang yang tidak berhak. Yang mana jika hal Tersebut sampai terjadi, kemungkinan besar akan merugikan bahkan membahayakan orang yang mengirim pesan atau menerima pesan, maupun organisasinya. Informasi yang terkandung di dalamnya pun bisa saja berubah sehingga menyebabkan salah penafsiran oleh penerima pesan. Selain itu data yang dibajak tersebut akan memiliki kemungkinan rusak bahkan hilang yang akan menimbulkan kerugian material yang besar.

MD5 merupakan fungsi hash satu arah yang didesain oleh Ronald Rivest dengan hash value 128 bit. Pada standard internet, MD5 telah dimanfaatkan secara bermacam-macam pada aplikasi keamanan, dan MD5 juga umum digunakan

untuk melakukan pengujian integritas sebuah file. Algoritma MD5 secara garis besar adalah mengambil pesan yang mempunyai panjang variabel diubah menjadi ‘sidik jari’ atau ‘intisari pesan’ yang mempunyai panjang tetap yaitu 128 bit. ‘Sidik jari’ ini tidak dapat dibalik untuk mendapatkan pesan, dengan kata lain tidak ada orang yang dapat melihat pesan dari ‘sidik jari’ MD5 (E.Z Adnan Kashogi ; 2012 : 1).

Alasan penulis mengambil judul penelitian “**Perancangan Aplikasi Pengecekan Berkas atau Data Dengan Menggunakan Algoritma MD5 Berbasis Android**” karena tidak adanya implementasi algoritma MD5 dalam pengembangan aplikasi Pengamanan Data.

I.2. Ruang Lingkup Permasalahan

I.2.1. Identifikasi Masalah

Permasalahan yang ada pada penelitian ini adalah :

1. Belum berkembangnya sebuah aplikasi yang memiliki sistem pengecekan keaslian sebuah berkas atau data.
2. Belum berkembang algoritma MD5 dalam sistem pengecekan berkas atau data.

I.2.2. Perumusan Masalah

Berdasarkan identifikasi masalah yang ditemukan oleh penulis dalam melakukan penelitian ini, maka perumusan masalah dapat dirumuskan sebagai berikut :

1. Bagaimana merancang sebuah aplikasi yang dapat mengecek keaslian sebuah data ?
2. Bagaimana melakukan perkembangan algoritma MD5 dalam sistem pengecekan keaslian sebuah berkas atau data ?

I.2.3. Batasan Masalah

Batasan masalah pada penelitian ini yaitu :

1. Aplikasi tidak dapat memberitahukan isi file mana yang telah diubah.
2. Data yang akan di enkripsi pada aplikasi ini adalah data berkas atau dokumen.
3. Bahasa pemrograman yang digunakan untuk membuat aplikasi adalah android studio.

I.3. Tujuan dan Manfaat

I.3.1. Tujuan

Tujuan penelitian ini yaitu :

1. Merancang sebuah aplikasi dengan memanfaatkan sistem pengecekan keaslian data yang dapat menjaga kerahasiaan dan keamanan data.
2. Merancang dan membangun sebuah aplikasi pengecekan keaslian berkas atau dengan dengan menggunakan Algoritma MD5

I.3.2. Manfaat

Manfaat penelitian ini yaitu :

1. Aplikasi pengecekan data dengan memanfaatkan sistem pengecekan keaslian data dapat menjaga kerahasiaan dan integritas pengiriman data pada aplikasi pengecekan keaslian data sehingga pengirim pesan dapat merasa nyaman dan aman dalam melakukan transfer data atau pesan
2. Implementasi Algoritma MD5 terhadap aplikasi pengecekan keaslian data dirancang untuk penggunaan memori yang seminimal mungkin dengan kecepatan proses yang maksimal

I.4. Metodologi Penelitian

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).

I.4.1. Jenis Data

Jenis penelitian pada skripsi ini adalah penelitian deskriptif yaitu penelitian yang menghasilkan data berupa kata-kata tertulis atau lisan dari orang-orang dan perilaku yang dapat diamati

I.4.2. Sumber Data

Salah satu pertimbangan dalam memilih masalah penelitian adalah ketersediaan sumber data. Penelitian kuantitatif lebih bersifat explanation (menerangkan, menjeleskan), karena itu bersifat to learn about the people (masyarakat objek), sedangkan penelitian kualitatif lebih bersifat understanding (memahami) terhadap fonemena atau gejala sosial**.** Data yang digunakan dalam penelitian ini diperoleh dari data file, nama file, lokasi, konten dokumen.

I.4.3. Metode Pengumpulan Data

Untuk mendapatkan kelengkapan informasi yang sesuai dengan fokus penelitian maka yang dijadikan teknik pengumpulan data adalah teknik dokumentasi, dokumen merupakan catatan peristiwa yang sudah berlalu. Dokumen bisa berbentuk tulisan, gambar, atau karya-karya.

I.4.4. Analisis Data

Analisis data dilakukan setelah peneliti melakukan pengumpulan data terhadap data yang akan dibutuhkan dalam melakukan Perancangan Aplikasi Pengecekan Keaslian Berkas atau Data Dengan Menggunakan Algoritma MD5 Berbasis Android.

I.5. Keaslian Penelitian

Berikut adalah beberapa jurnal penelitian terdahulu terkait judul penelitian skripsi ini pada tabel I.1 :

Tabel I.1. Keaslian Penelitian

No	Peneliti	Judul	Hasil
1	E.Z Adnan Kashogi (2012)	Algoritma Message Digest 5 (MD5)	Di dalam mengirimkan suatu pesan pada jaringan, kita menghadapi beberapa persoalan yaitu kerahasiaan (confidentiality), integritas data

			(menjamin pesan tidak diubah oleh orang lain), keaslian pesan (authentication), dan tak terbantahkan (non-repudiation). Untuk itu diperlukan suatu teknik kriptografi untuk menangani persoalan ini. Salah satu algoritma yang dipakai adalah Message Digest 5 (MD5). Message Digest 5 adalah fungsi hash kriptografi yang banyak digunakan sebagai alat untuk menjamin atau memberi garansi bahwa pesan yang dikirim akan sama dengan yang diterima dengan cara membandingkan 'sidik jari' kedua pesan tersebut. MD5 (1992) merupakan pengembangan dari MD4 (1990) dimana terjadi penambahan satu ronde. MD5 memproses teks masukan ke dalam blokblok bit sebanyak 512-bit, kemudian dibagi ke dalam 32-bit sub blok sebanyak 16 buah. Keluaran dari MD5 berupa 4 buah blok yang masing-masing 32-bit yang mana akan menjadi 128-bit yang biasa disebut nilai hash. Saat ini MD5 telah mendapat perhatian yang baru dari para peneliti setelah diumumkannya kerusakan pada MD5 yang ditemukan oleh Wang beserta tim risetnya dari Shandong University di Jinan China. Pada makalah ini penulis juga akan coba untuk membahas kerusakan yang ditemukan oleh Wang tersebut. Harapan penulis dengan makalah ini adalah dapat memberikan informasi tentang fungsi hash MD5, sehingga pembaca dapat lebih memahami fungsi hash MD5 dan juga mengetahui kekuatan dan kelemahannya
2	Rusdianto (2016)	Implementasi Algoritma Md5 Untuk Keamanan	Keamanan data dan informasi menarik banyak perhatian orang memastikan keaslian data atau dokumen masih terjaga, masalah ini

		Dokumen	begitu urgen untuk dan menyentuh berbagai bidang termasuk saluran komunikasi yang aman, teknik enkripsi data yang kuat dan dipercaya dibutuhkan untuk menjaga database. Message Digest 5 (MD) adalah Sebuah metode kriptografi yang menggunakan kunci seperti password dalam melakukan proses enkripsinya dan mengunakan kunci yang sama untuk melakukan proses dekripsinya sehingga akan dihasilkan dokumen yang sama dengan dokumen aslinya. Data plaintex yang telah dienkripsi akan menghasilkan sebuah chipertex yang tidak dapat dibaca oleh orang lain. Chipertex inilah yang akan dikirimkan ke pihak kedua sehingga akan memiliki kerahasiaan yang bisa diandalkan. Data chipertex yang dihasilkan akan berubah-ubah sesuai masukan data kunci password yang diberikan. Sistem ini dibuat dengan bahasa pemprokraman Visual Basic.Net.
3	Yudi Prayudi (2015)	Kompleksitas Waktu Untuk Algoritma MD5	Integritas bukti digital adalah salah satu issue penting dalam aktivitas digital forensics. Secara umum, bukti digital tidak boleh mengalami perubahan apapun dalam setiap tahap digital forensics. Dalam hal ini, fungsi hash secara umum dalam digital forensics telah digunakan untuk kepentingan menjaga integritas bukti digital. Sebagai sebuah fungsi matematis yang kemudian diterjemahkan dalam sebuah algoritma, ternyata penggunaan fungsi hash juga memiliki sejumlah issue seputar kompleksitas. Berdasarkan cara kerja dan karakteristik algoritma MD5 ternyata kompleksitas waktu dari algoritma tersebut adalah Big O (n) atau fungsi asimtotik linier. Dengan demikian secara umum bertambahnya input

			(panjang message yang akan dicarikan nilai fungsi hash MD5) akan sebanding pula dengan bertambahnya waktu secara linier
4	Rezza Mahyudin (2012)	Algoritma Message Digest 5 (MD5) Dalam Aplikasi Kriptografi	Masalah keamanan dan kerahasiaan merupakan salah satu aspek penting dari suatu pesan, data, atau informasi. Dalam hal ini sangat terkait dengan betapa pentingnya pesan, data, atau informasi tersebut dikirim dan diterima oleh pihak atau orang yang berkepentingan, serta apakah pesan, data, atau informasi tersebut masih authenticity. Pesan, data, atau informasi akan menjadi kurang berguna lagi apabila di tengah jalan informasi itu disadap atau dibajak oleh orang yang tidak berhak atau berkepentingan. Message Digest 5 (MD5) adalah salah satu alat untuk memberi garansi bahwa pesan yang dikirim akan sama dengan pesan yang diterima, hal ini dengan membandingkan ‘sidik jari’ atau ‘intisari pesan’ kedua pesan tersebut. MD5 merupakan pengembangan dari MD4 dimana terjadi penambahan satu ronde. MD5 memproses teks masukkan ke dalam blok-blok bit sebanyak 512 bit, kemudian dibagi ke dalam 32 bit sub blok sebanyak 16 buah. Keluaran dari MD5 berupa 4 buah blok yang masing-masing 32 bit yang mana akan menjadi 128 bit yang biasa disebut nilai hash. Makalah ini bertujuan untuk membahas proses prencanaan dan menganalisa proses keutuhan atau perubahan pesan dengan menggunakan MD5 dan juga dapat menganalisa hasil keluaran dari MD5 yang berupa kecepatan dari proses aplikasi yang dibuat

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 tentang teori-teori dan metode yang berhubungan dengan topik yang dibahas atau permasalahan yang sedang dihadapi yaitu berupa pembahasan mengenai sistem jaringan, UML, ERD dan normalisasi.

BAB III : ANALISIS DAN DESAIN SISTEM

Pada bab ini mengemukakan tentang analisa sistem yang sedang berjalan, evaluasi sistem yang berjalan dan desain sistem secara detail.

BAB IV : HASIL DAN UJI COBA

Pada bab ini menerangkan hasil dan pembahasan program yang dirancang serta kelebihan dan kekurangan sistem yang dirancang.

BAB V : KESIMPULAN DAN SARAN

Pada bab ini berisi kesimpulan penulisan dan saran dari penulis sebagai perbaikan di masa yang akan datang untuk sistem.