

BAB I

Pendahuluan

A. Latar Belakang

Perkembangan informasi berbasis teknologi menjadi hal yang tidak terduga. Semakin cepatnya perkembangan teknologi informasi, membuat semakin mudahnya seseorang untuk mendapatkan informasi melalui internet dan media sosial. Melalui teknologi informasi, pemerintah semakin mudah memberikan bantuan untuk kesejahteraan masyarakat. Seperti dalam dunia pendidikan, pemerintah sudah memberikan banyak informasi dengan memanfaatkan teknologi informasi.

Pendidikan di sekolah sangat berperan penting untuk generasi penerus bangsa. Dengan teknologi informasi memberikan banyak kemudahan untuk ikut mengawasi dan memberikan bantuan kepada sekolah-sekolah. Pentingnya bagi sekolah untuk mengatur dan menjaga document dari pemerintah, menjadikan aspek yang sangat penting. Apalagi di era smartphone, penyebaran informasi semakin cepat dan mudah. Karena hampir setiap orang memiliki smartphone.

Document yang penting bagi pendidikan diantaranya data keuangan, karena data keuangan akan selalu dilakukan audit secara berkala setiap tiga bulan dan satu tahun sekali. Tentunya perlindungan data yang baik adalah hal yang dibutuhkan oleh setiap orang, apalagi menyangkut hal penting seperti data keuangan. Maupun berkas-berkas penting lainnya sangat perlu dijaga kerahasiannya.

Masih banyak saat ini yang melupakan bahwa pentingnya keamanan document. Padahal era digital, penyebaran informasi semakin mudah dan itu juga memicu pencurian data yang bisa merugikan berbagai pihak. Itu bisa menyebabkan tidak adanya lagi yang namanya privasi, padahal privasi menjadi hal penting untuk setiap satuan pendidikan.

Maka dari itu pentingnya suatu keamanan yang baik untuk mengamankan data. Agar keamanan data tetap terjaga kerahasiannya perlunya menerapkan kriptografi, karena kriptografi merupakan suatu proses pengamanan data dengan cara mengenkripsi dan mendeskripsikan data. Pemilihan kriptografi yang tepat akan mengurangi kemungkinan pencurian data, Algoritma blowfish dapat menjadi solusi untuk mengatasi keamanan data.

Algoritma Blowfish salah satu algoritma kriptografi yang menggunakan modern kunci simetris berbentuk cipher block. Algoritma Blowfish ini dapat mengenkripsi file dalam bentuk document seperti pdf, doc, xls. Pada penerapannya enkripsi dilakukan menggunakan kunci tertentu, sehingga

menghasilkan ciphertext berupa sandi. Ciphertext tersebut dapat dibuka jika menggunakan kunci yang sama ketika mengenkripsi. Algoritma Blowfish termasuk Open Cryptography Interface (OCI) adalah algoritma open source sehingga bebas paten, yang bisa dikembangkan siapa saja.

Dalam penelitian “Implementasi Algoritma Blowfish Untuk Enkripsi Dan Dekripsi Berbasis Java Swing” maka akan dilakukan penelitian yang berjudul “Penerapan Algoritma Blowfish Untuk Keamanan Document Berbasis Smartphone”. Penelitian ini berfungsi mengamankan data dengan algoritma blowfish pada pengguna smartphone android.

B. Rumusan Masalah

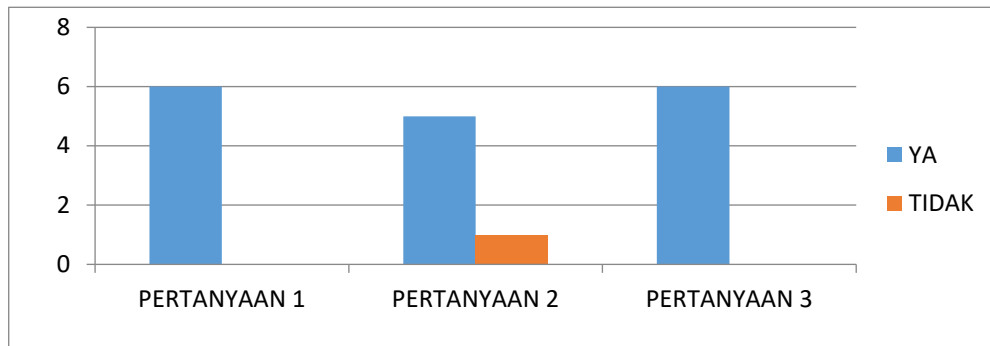
Sekolah Menengah Pertama Madani adalah sebuah lembaga yang bergerak dibidang pendidikan menengah pertama. Pendidikan yang terus berkembang tidak terlepas dari bantuan pemerintah pusat. Dengan memberi bantuan seperti dana Bantuan Operasional Sekolah (BOS), Bantuan Operasional Sekolah Daerah (BOSDA), Kartu Indonesia Pintar (KIP) dan sebagainya. Pengelolaan bantuan dari pemerintah tersebut memiliki aplikasi masing-masing dan biasanya di download berupa *file pdf*. Akan tetapi kemudahan penyebaran informasi melalui *smartphone* yang begitu cepat, data menjadi riskan disalahgunakan oleh pihak yang tidak bertanggungjawab.

Pengelolaan Bantuan Operasional Sekolah (BOS) di SMP Madani meliputi banyak pihak diantaranya Kepala Sekolah, Wakil Kepala Sekolah, Bendahara dan Tenaga Administrasi. Dengan kemajuan teknologi untuk memudahkan proses penyebaran informasi, pengelola Bantuan Operasional Sekolah (BOS) SMP Madani sudah menggunakan *smartphone*. Akan tetapi dalam penyebarannya sistem keamanan masih lemah. Setelah dilakukan penyebaran kuesioner kepada Staff SMP Madani dengan sample responden 6 didapatkan hasil yaitu *document file* berbentuk pdf perlu dilakukan sebuah sistem keamanan dalam penyebarannya, maka dari itu dibuatkan aplikasi untuk mendukung keamanan *document* tersebut. Untuk lebih jelasnya dapat dilihat di gambar 1.1 grafik hasil kuesioner dibawah.

Tabel 1. 1 Contoh kuesioner

No.	Pertanyaan	Ya	Tidak
1.	Apakah Bapak/Ibu pernah menerima <i>file document</i> dari bantuan operasional sekolah dari pemerintah?		

2.	Apakah Bapak/Ibu pernah mengedit atau menyebarkan kepada staff lainnya?		
3	Jika <i>file document</i> tadi pernah dikelola Bapak/Ibu, perlukah keamanan dalam <i>document</i> tersebut?		



1. Identifikasi Masalah

Identifikasi masalah dalam pengamanan *document* dengan menggunakan Algoritma Blowfish diantaranya sebagai berikut :

- Masih lemahnya keamanan data *file document* di SMP Madani.
- Belum efektifnya proses pengamanan data *file document* di SMP Madani.

2. Problem Statement

Setelah dilakukan penyebaran kuesioner kepada Staff SMP Madani dengan sample responden sebanyak 6 orang didapatkan hasil yaitu terdapat suatu permasalahan karena masih lemahnya keamanan data *file document* dan belum efektifnya proses untuk mengamankan *file document* tersebut, maka diambil kesimpulan perlunya aplikasi pengamanan *document* untuk menjaga kerahasiaan data sekolah agar tidak disalahgunakan oleh orang lain.

3. Research Question

- Bagaimana penerapan Algoritma Blowfish Untuk Keamanan *Document* Berbasis *Smartphone*?
- Seberapa kuat dan efektifnya Algoritma Blowfish Untuk Keamanan *Document* Berbasis *Smartphone*?

C. Maksud dan Tujuan Penelitian

1. Maksud Penelitian

Maksud penelitian ini untuk menerapkan Algoritma Blowfish untuk membuat keamanan *document* dengan menggunakan *smartphone*.

2. Tujuan Penelitian

Dalam penelitian ini terdapat beberapa tujuan dari permasalahan yang ada diantaranya :

- a. Meningkatkan keamanan data *file document* dengan menggunakan Algoritma Blowfish.
- b. Meningkatkan efektifitas proses keamanan data *file document* dengan menggunakan aplikasi.
- c. Mengembangkan prototype aplikasi keamanan data *file document* dengan menggunakan Algoritma Blowfish.
- d. Mengukur tingkat keamanan data *file document* dengan menggunakan Algoritma Blowfish.

D. Spesifikasi Produk yang Diharapkan

Spesifikasi produk ini berupa aplikasi untuk mengamankan *file document*.

Sehingga diharapkan dapat :

1. Dapat mempermudah pengguna
2. Menggunakan *smartphone* android.
3. Dapat merahasiakan informasi pada *file document* agar keamanan terjaga
4. Memiliki proses enkripsi dan dekripsi.
5. Memiliki tampilan yang *responsive*.

E. Signikasi Pengembangan

Dalam penelitian ini diharapkan agar informasi yang berada didalam *file document* tidak diketahui oleh orang lain yang bukan staff SMP Madani untuk menghindari penyalahgunaan data operasional sekolah.

F. Asumsi dan Keterbatasan Penelitian

1. Asumsi Penelitian

Dengan prosedur yang dilakukan saat ini di SMP Madani membutuhkan waktu yang lama untuk mengamankan *document* dengan menggunakan sistem ini karena *file* yang akan di enkripsi maupun di dekripsi harus dicari secara manual.

2. Keterbatasan Penelitian

- a. *Document* yang digunakan hanya *file pdf*.
- b. Kunci diperlukan untuk mendekripsi *document*.
- c. Algoritma Blowfish tidak bisa digunakan untuk mengenkripsi video dan gambar.

G. Definisi Istilah dan Operasional

Terdapat beberapa istilah yang disebutkan pada penelitian ini, yaitu :

1. *Smartphone* adalah telepon genggam yang mempunyai kemampuan dengan penggunaan dan fungsi yang menyerupai komputer.
2. Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman.
3. Enkripsi adalah proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus.
4. Deskripsi merupakan kebalikan dari Enkripsi, upaya pengolahan data menjadi sesuatu yang dapat diutarakan secara jelas.
5. pdf (Portable Document Format), doc (Document), xls (Excel Spreadsheet).
6. *Document* (berasal dari bahasa Latin: documentum) adalah sebuah tulisan yang memuat informasi. Biasanya, dokumen ditulis di kertas dan informasinya ditulis memakai tinta baik memakai tangan atau memakai media elektronik
7. *File* adalah kumpulan berbagai informasi yang berhubungan dan juga tersimpan di dalam media penyimpanan.
8. *Responsive* adalah sebuah metode tampilan beradaptasi jika dibuka dari perangkat mobile berukuran kecil maupun perangkat komputer dengan ukuran monitor besar. Ukuran huruf, user interface, gambar dan tata letak akan menyesuaikan dengan lebar layar dan resolusi layar monitor yang tersedia.