ENKRIPSI FILE MENGGUNAKAN METODE XML SERIALIZER UNTUK PENGAMANAN FILE TUGAS KULIAH

Nur Arifah Juliyanti[1], Uning Lestari[2], Erfanti Fatkhiyah[3]
[1,2,3] Prodi Teknik Informatika, FTI, IST AKPRIND Yogyakarta
[1]green.arifah21@gmail.com, [2]Uning@akprind.ac.id, [3]Erfunthyie@yahoo.co.id

ABSTRACT

The system is built to secure a college student assignment files that can not be duplicated by others or other students. This system has several features which are features of student registration and lecturer, administrator login, login students, faculty login. As for the administrator has the features to manage and control all data of students and faculty, create a new user and delete existing users, since such rights are owned by the administrator only.

Serializer xml file encryption system for securing a college assignment file is built according to the design of the system is presented and carried out various development of a variety of previous data collection is done on campus institute of science and technology AKPRIND Yogyakarta. The system is built using MySQL database and PHP, it is intended that occurs efficiency during implementation in order to more quickly and easily.

Research manufacture xml serialization system is to reduce the risk of publication answers duty of every student who has been uploaded and faculty can bring value to correspond with what is done by the students.

Keywords: PHP, MySQL, Xml Serializer, Students, Faculty

INTISARI

Sistem dibangun untuk mengamanan file tugas kuliah mahasiswa agar tidak dapat terduplikasi oleh orang lain atau mahasiswa lain. Sistem ini memiliki beberapa fitur diantaranya adalah fitur registrasi mahasiswa dan dosen, *login administrator*, *login* mahasiswa, *login* dosen. Sedangkan untuk bagian administrator memiliki fitur untuk mengelola dan mengontrol seluruh data mahasiswa dan dosen, membuat user baru dan menghapus user yang ada, karena hak tersebut hanya dimiliki oleh *administrator*.

Sistem enkripsi file xml serializer untuk pengamanan file tugas kuliah ini dibangun sesuai dengan rancangan sistem yang dipaparkan dan dilakukan berbagai pengembangan dari berbagai pengumpulan data sebelumnya yang dilakukan di kampus institut sains dan teknologi akprind Yogyakarta. Sistem ini dibangun menggunakan database MySql dan Php, hal tersebut bertujuan agar terjadi efisiensi pada saat implementasi agar lebih cepat dan mudah.

Penelitian pembuatan sistem xml serialization ini untuk mengurangi resiko penduplikasi jawaban tugas dari setiap mahasiswa yang telah diupload dan dosen dapat memberika nilai yang sesuai dengan apa yang dikerjakan oleh mahasiswa.

Keyword : PHP, MySql, Xml Serializer, Mahasiswa, Dosen

PENDAHULUAN

Berbagai macam layanan komunikasi tersedia di *internet*, diantaranya adalah *web*, *e-mail*, milis, *newsgroup*, *e-learning* dan sebagainya. Dengan semakin maraknya orang memanfaatkan layanan komunikasi di *internet* tersebut, maka permasalahanpun bermunculan, apalagi ditambah dengan adanya *hacker* dan *cracker*.

Studi kasus yang ada saat ini adalah pada kampus Institut Sains dan Teknologi AKPRIND Yogyakarta adalah sebuah kampus yang memiliki 3 unit kampus baik kampus untuk pelaksanaan praktek maupun teori. Setiap mahasiswa mempunyai tugas kuliah baik yang bersifat individu maupun tugas kelompok. Namun, *file* tugas kuliah yang disimpan atau dikirimkan itu tidak mendapatkan perlindungan yang bisa membuat file tugas kuliah mahasiswa tersebut tercopy atau tercuri oleh pihak lain. Hal ini sangat berbahaya karena jenis *file* yang disimpan atau dikirimkan termasuk rahasia. Maka, untuk lebih melindungi keamanan data dari *file* yang dikirimkan tersebut, saat *file excel* atau

word melalui proses *upload*, *file excel* atau dokumen tersebut akan melalui proses steganografi sehingga akan menjadi sebuah *file* yang kemudian akan dilakukan proses posting atau ditampilkan web.

File tersebut dilakukan *download,* maka proses enkripsi tersebut akan melalui sebuah proses enkripsi lagi, yaitu *XML Serializer* yang mana proses tersebut akan dilakukan secara majemuk, sehingga proses pemecahan akan menjadi lebih sulit, sehingga *file* yang telah melalui proses pada aplikasi ini akan lebih aman. Kemudian saat hendak melakukan dekripsi harus melalui proses *login* sehingga hanya *user* yang berkepentingan yang dapat mengakses *file* tersebut.

Maka berdasarkan penjelasan di atas, sebuah system yang digunakan dalam mengamankan *file* tugas kuliah sangat dibutuhkan agar *file* tugas seorang mahasiswa tidak terduplikasi oleh pihak lain yang tidak berwenang.

TINJAUAN PUSTAKA

Kriptografi (*cryptography*) berasal dari bahasa Yunani yaitu *cryptos* yang artinya rahasia dan *graphein* yang artinya tulisan. Jadi, kriptografi adalah tulisan rahasia. Kriptografi adalah ilmu atau seni yang menggunakan matmatika untuk mengamankan suatu informasi. Algoritma kriptografi merupakan aturan untuk *enchipering* dan *deciphering* atau fungsi matematika yang digunakan untuk melakukan proses enkripsi dan dekripsi. Algoritma kriptografi terdiri dari tiga fungsi dasar yaitu enkripsi, dekripsi, dan kunci. Enkripsi atau penyandian adalah suatu proses pengubahan *plaintext* (informasi awal yang akan dirahasiakan) menjadi *ciphertext* (informasi yang sudah dirahasiakan) dengan sebuah algoritma tertentu dan menggunakan suatu kunci tertentu yang dipilih. Sementara dekripsi adalah proses pengembalian *ciphertext* menjadi *plaintext* oleh algoritma yang berkebalikan dengan algoritma enkripsi.

Konsep matematis yang menjadi dasar kriptografi adalah hubungan antara dua buah himpunan yang elemennya adalah *plaintext* dan himpunan lain yang elemennya adalah *ciphertext*. Fungsi yang memetakan kedua himpunan tersebut dinamakan fungsi enkripsi dan fungsi dekripsi. Dimisalkan P menyatakan *plaintext* dan C menyatakan *ciphertext*, maka fungsi enkripsi E akan memetakan P ke C, $E(P)$=C dan fungsi dekripsi D akan memetakan C ke P, $D(C)$=P Maka, persamaan ($E(P)$)=P harus benar dikarenakan proses enkripsi kemudian dekripsi mengembalikan lagi pesan menjadi pesan awal. (Fadhilah, 2012)

Algoritma Rijndael

Rijndael adalah algoritma yang beroperasi dalam *byte*, bukan dalam *bit*. Algoritma ini mampu melakukan enkripsi terhadap *plaintext* sebesar 16 *byte* atau 128 *bit*.

Algoritma *Rijndael* juga melakukan putaran enkripsi (*enciphering*) sebanyak 10 putaran namun bukan putaran yang merupakan jaringan *Feistel*. *Enciphering* pada *Rijndael* melibatkan empat proses yaitu :

1. *Sub Bytes*
2. *Shift Rows*
3. *Mix Columns*
4. *Add Round Key*

Secara umum, proses enkripsi dilakukan dengan *initial round* yaitu melakukan *XOR* antara *state* awal yang masih berupa *plaintext* dengan *cipher key*. Kemudian melakukan keempat proses diatas sebanyak 9 kali putaran, dan terakhir adalah *final round* yang melibatkan proses *sub bytes, shift rows,* dan *add round key*. (Eko Satria, 2009).

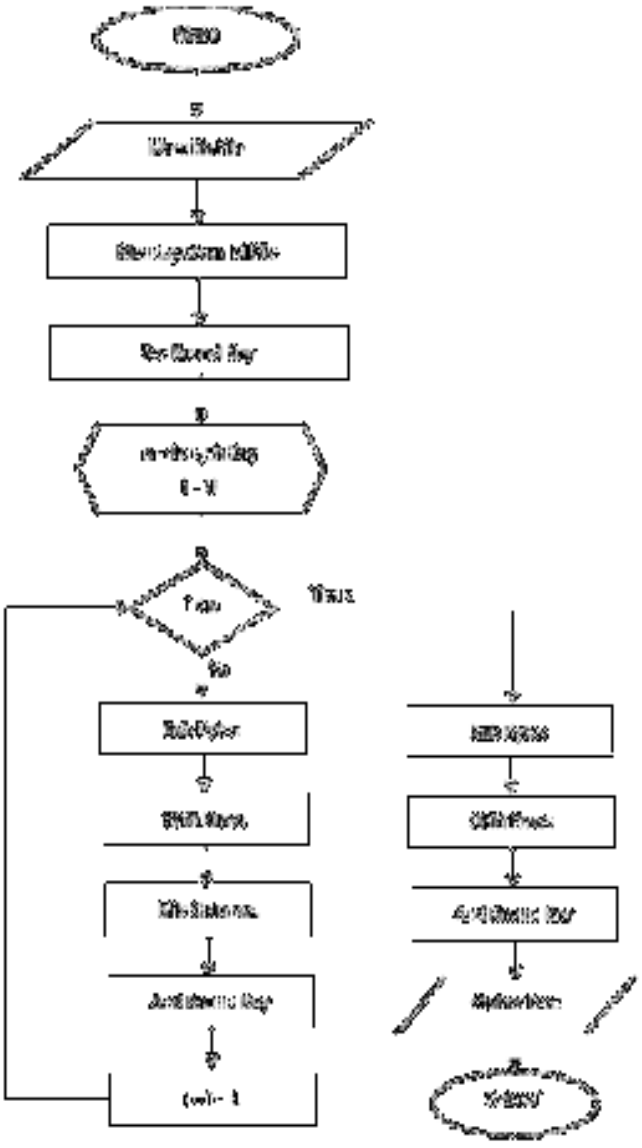
Enkripsi

Enkripsi mempunyai algoritma untuk mengenkripsi data. Data yang telah terenkripsi disebut sebagai *ciphertext*. Rumus ini memerlukan sebuah variable untuk mengembalikan data tersebut kembali ke bentuk asal. Variabel ini biasa disebut kunci. Tanpa kunci, seseorang sangat sulit bahkan hampir tidak mungkin, untuk dapat memecahkan kode enkripsi tersebut. Maka kunci ini memegang peranan vital di dalam enkripsi. (Dwi Kurnia Basuki,2011).

Xml Serializer

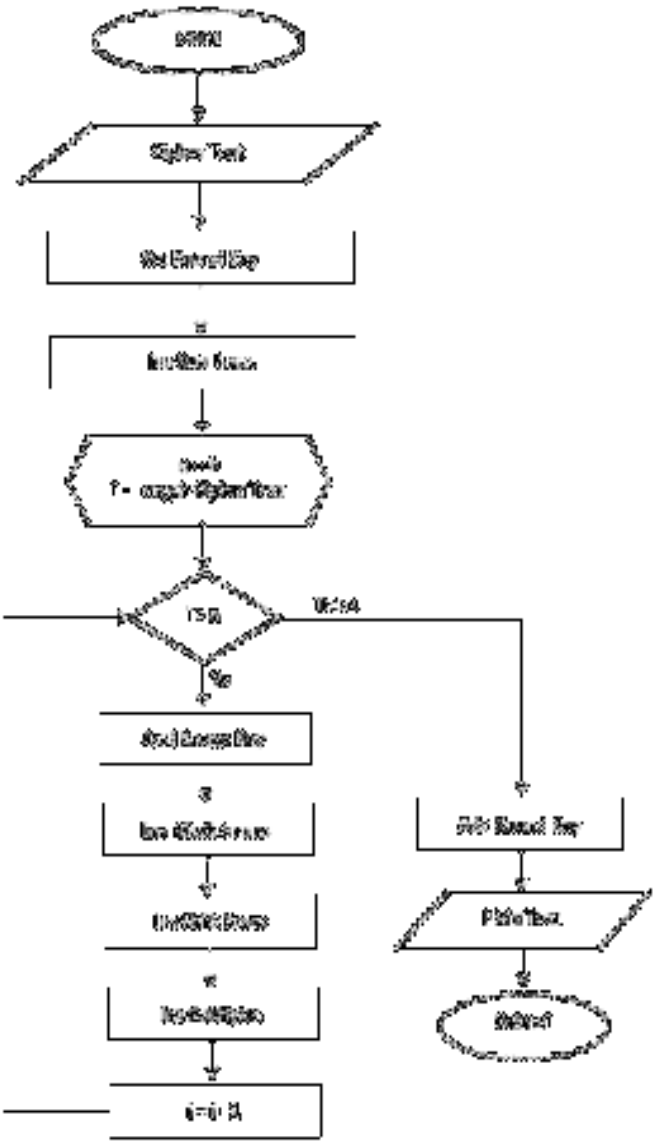
XML adalah salah satu bahasa Markup Language yang merupakan penyerderhanaan dari SGML (*Standard Generalized Markup Language*). XML dikembangkan oleh W3C dengan tujuan untuk melengkapi atau mengatasi keterbatasan pada teknologi HTML yang telah menjadi dasar layanan berbasis web saat ini. Pada penggunaannya, XML memiliki dua fungsi yaitu sebagai format dokumendan format pertukaran data pada sebuah sistem yang terdistribusi. Saat ini XML memegang peranan penting bagi sebagian transaksi informasi yang dilakukanmelalui internet, karena XML telah menjadi sebuah format struktur pertukaran data yang dilakukan antar *web service* di internet. (Aris Puji Widodo,2003)

Metodologi Penelitian
Flowchart Enkripsi



Gambar 1 Flowchart proses enkripsi

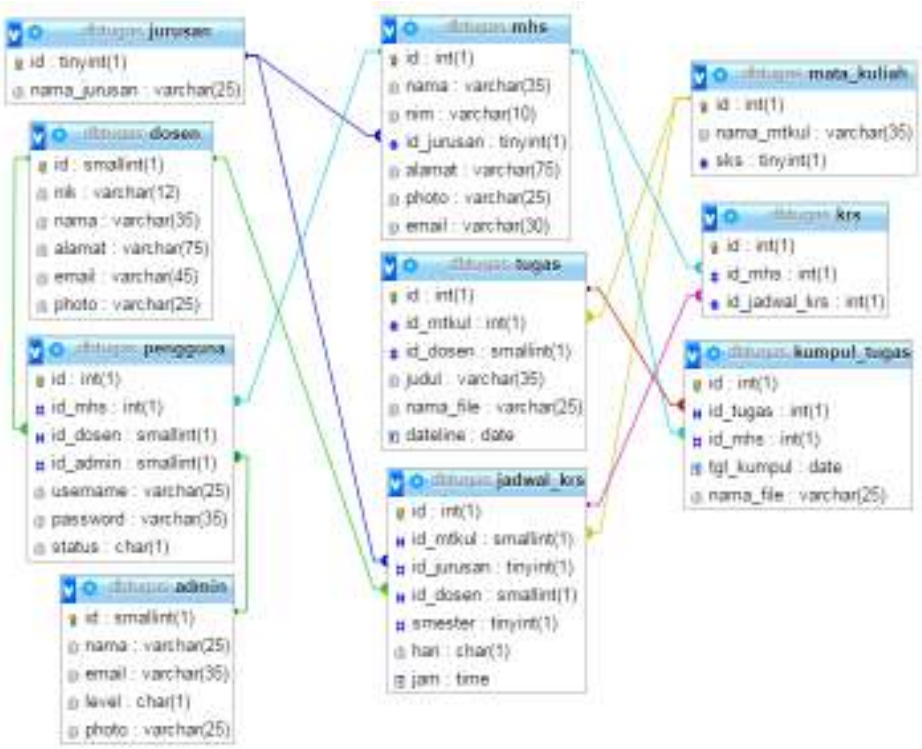
Flowchart Dekripsi



Gambar 2 Flowchart proses dekripsi

Relasi Antar Tabel

Relasi tabel ini digunakan dala membangun sistem enkripsi untuk pengamanan file tugas kuliah. Relasi terdiri dari sepuluh tabel yang mendefinisikan masing-masing fungsi dalam sistem ini. Ditunjukkan pada gambar 3.



Gambar 3 Relasi Antar Tabel

PEMBAHASAN

Sistem enkripsi file xml serializer untuk pengamanan file tugas kuliah ini dibangun sesuai dengan rancangan sistem yang dipaparkan di bab III dan dilakukan berbagai pengembangan dari berbagai pengumpulan data sebelumnya yang dilakukan di kampus institut sains dan teknologi akprind Yogyakarta. Sistem ini dibangun menggunakan database MySql dan Php, hal tersebut bertujuan agar terjadi efisiensi pada saat implementasi agar lebih cepat dan mudah.

Cara kerja dari sistem xml serialization adalah pertama melakukan proses login yang terbagi menjadi 3 user antara lain admin, mahasiswa, dan dosen. User admin bertugas untuk mengatur user dan menghapus user serta mengatur alur sistem. Untuk user mahasiswa bertugas untuk menginput krs untuk mengentri mata kuliah yang akan diambil, serta mengupload tugas yang telah dienkrip. Sedangkan user untuk dosen bertugas untuk memposting tugas, mendownload tugas dan akan melakukan proses deskrip. Sebelum file dideskrip dilakukan proses filenya dicapture, kemudian file barunya dibuka lalu dikombinasi dengan key. Kemudian php akan mengenerek file baru kedalam bentuk xml.

1. **Halaman login**
   Halaman Login untuk admin, dosen, dan mahasiswa.

Gambar 4 Halaman Login

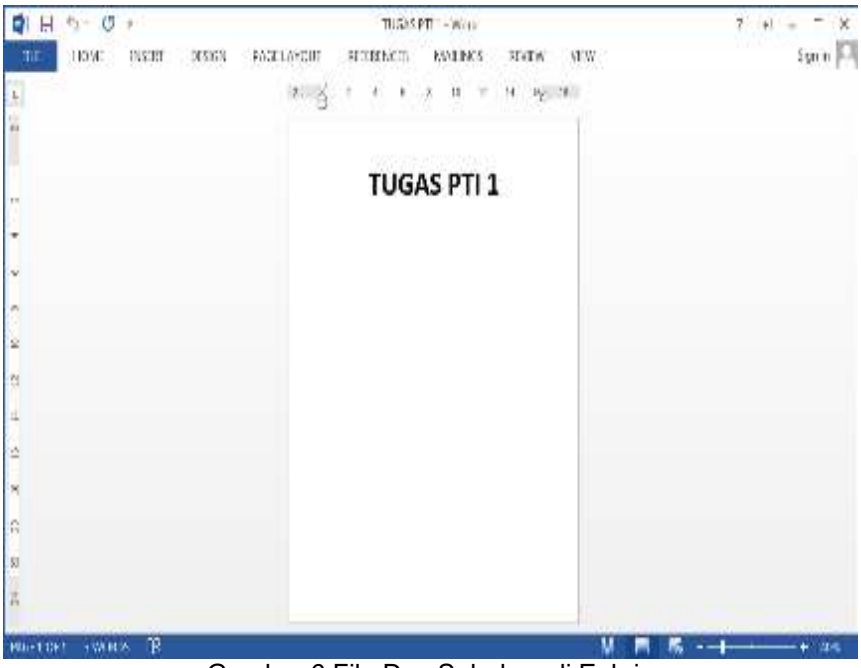
2. **Halaman Encrypted**

Halaman tugas encrypted ini berisi tugas kuliah setiap mahasiswa yang sudah dilakukan enkrip, agar tiap tugas mahasiswa tidak mudah terduplikasi oleh orang lain dan tugas ini akan langsung didownload oleh dosen yang bersangkutan. Ditunjukan pada gambar 5

Gambar 5 Halaman Encrypted

3. **Komparasi File**

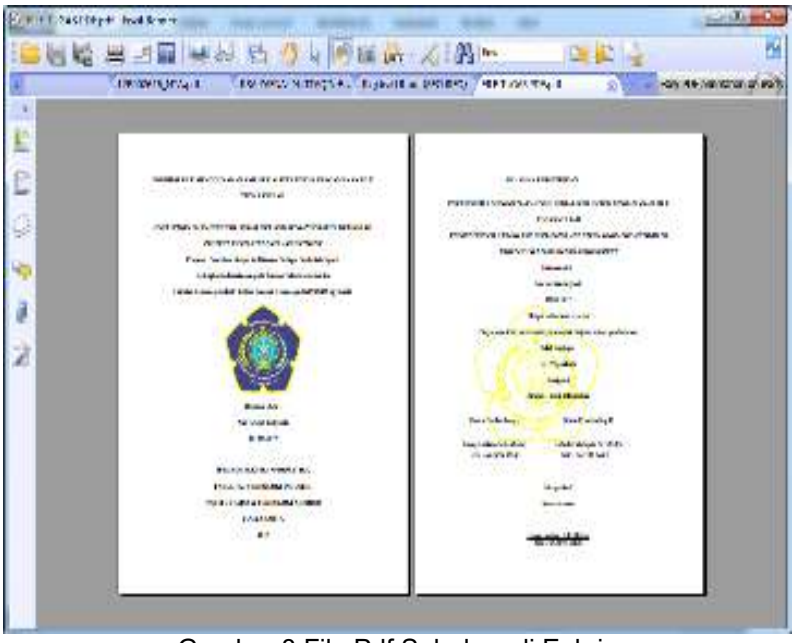
Halaman ini berisi file sederhana yang belum di enkrip dan di simpan menjadi file doc. ditunjukkan pada gambar IV.3. Hasil enkripsi ditunjukkan pada gambar 6, Original File (Size 11.0 KB).



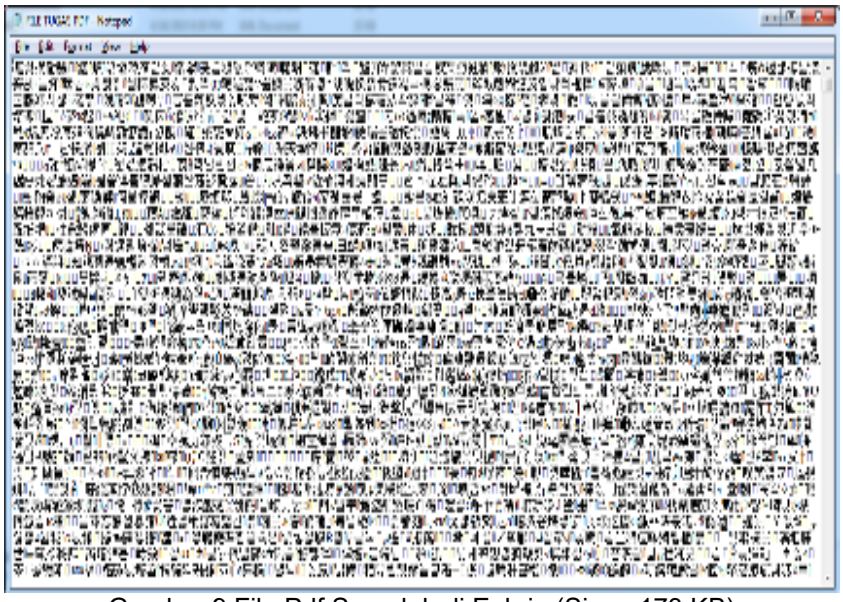
Gambar 6 File Doc Sebelum di Enkrip

Gambar 7 File Sesudah di Enkrip (sieze : 17 KB)

Halaman ini file pdf dan belum di enkrip. Ditunjukkan pada gambar 8. Hasil enkripsi jenis file pdf ditunjukkan pada gambar 9. Original File (Size 115 KB)

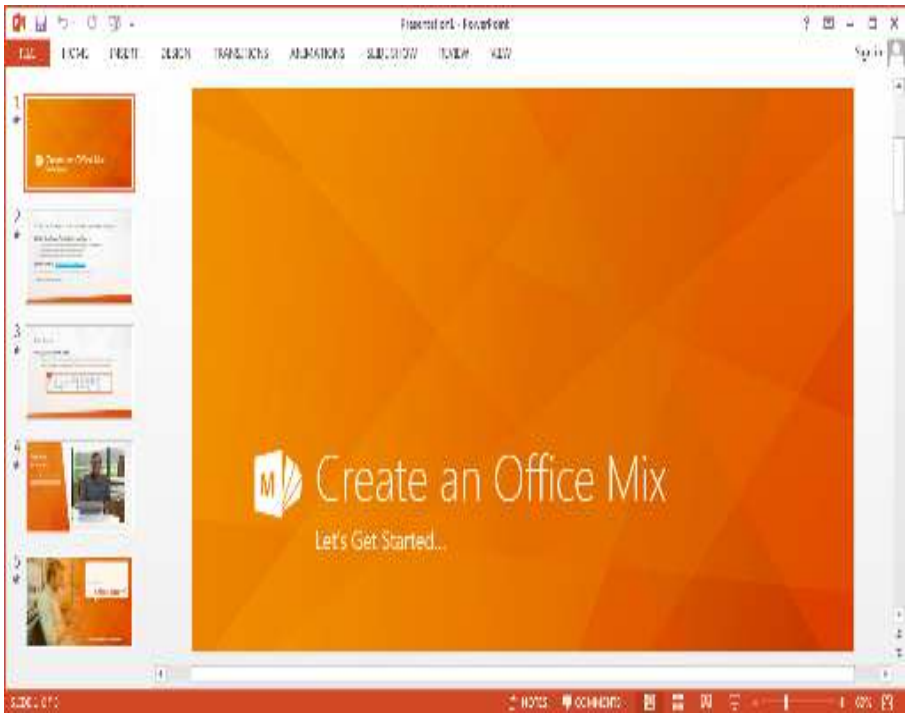


Gambar 8 File Pdf Sebelum di Enkrip

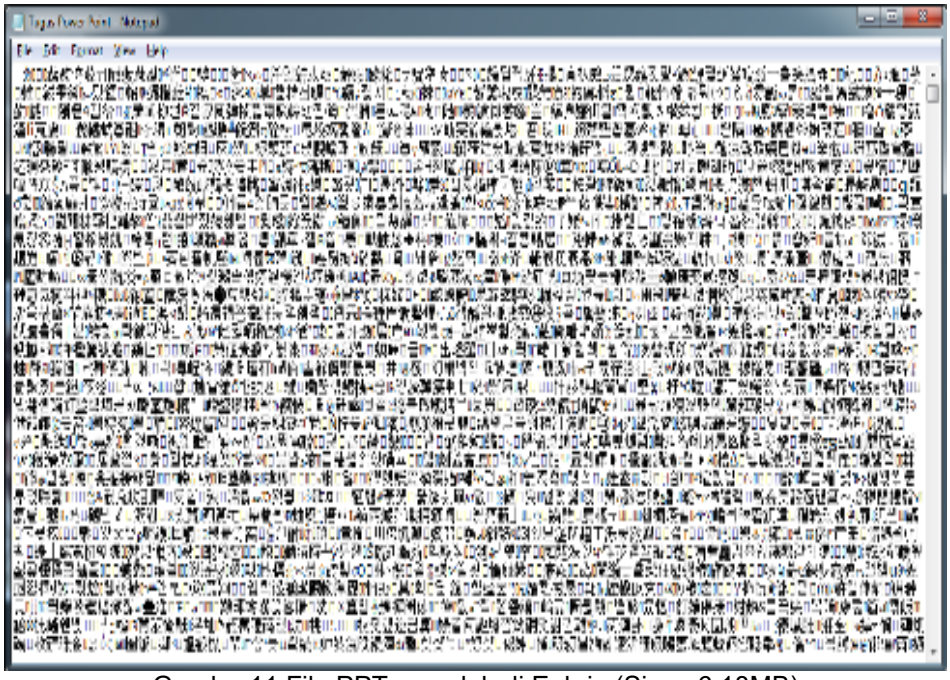


Gambar 9 File Pdf Sesudah di Enkrip (Size : 173 KB)

Halaman ini berisi file ppt dan file ini belum terenkrip. Ditunjukkan pada gambar 8. Hasil enkripsi jenis file ppt ditunjukkan pada gambar IV.8, Original File (Size 4.05MB)



Gambar 10 File PPT sebelum di Enkrip



Gambar11 File PPT sesudah di Enkrip (Size : 6.18MB)

KESIMPULAN

Berdasarkan perancangan, hasil dan pembahasan yang ada pada bagian sebelumnya, maka dapat diambil kesimpulan sebagai berikut :

1. Penelitian ini telah berhasil membuat sistem pengamanan file tugas kuliah, dibuktikan dengan adanya sistem ini mahasiswa dapat mengerjakan tugas-tugas yang diberikan dosen dan tidak dapat menduplikasi hasil tugas teman sendiri.
2. Sistem ini dibangun menggunakan bahasa pemrograman php dan menggunakan database mysql, serta menggunakan metode xml serializer.
3. Mampu mendekripsi file doc dan pdf.
4. Sistem ini terdapat tiga user yaitu admin, dosen dan mahasiswa dan masing-masing sudah mendapatkan pekerjaannya yang sesuai.
5. Dapat diterapkan pada sistem pengumpulan tugas sesungguhnya, karena sistem xml serialization telah terhubung pada sistem krs dan kemahasiswaan.
6. Dapat mendekrip file secara bersamaan sehingga mudah untuk dosen melakukan proses pendeskripsian file.

DAFTAR PUSTAKA

Ananta, DE., 2003. Skripsi Pembuatan Program Aplikasi Penyembunyian Data Dengan Metode Steganography, *Skripsi*, STIKOM, Surabaya.

Andi, 2003, *Memahami Model Enkripsi dan Security Data*. Semarang.

Anhar, 2010, *Panduan Menguasai Php & MySql Secara Otodidak*, MediaKita, Jakarta.

Aris, P.W., 2003 Transformasi Dokumen XML, Jurnal Matematika Dan Komputer.

Dwi Kurnia Basuki, 2011, *Enkripsi dan Steganografi* ,Yogyakarta.

Eko Satria. 2009. Studi Algoritma RIJNDAEL Dalam Sistem Keamanan Data, *Skripsi* Universitas Sumatera Utara Medan, Medan.

Fadhilah Hanifah, 2012, *Aplikasi algoritma*, FMIPA UI, Jakarta.

Kadir. 2003, *Dasar Pemrograman Web Dinamis Menggunakan Php*, Penerbit ANDI, Yogyakarta.