PROTOTYPE APLIKASI WEB PENGAMAN DATA PRIBADI DENGAN KRIPTOGRAFI ONE TIME PAD (OTP)

Lalang Erawan[1*], **Suharnawi**[2]
[12] Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
Jl. Imam Bonjol 207 Semarang 50131
[*]Email: lalang.erawan@dsn.dinus.ac.id

Abstrak

Penelitian bertujuan untuk membuat prototype aplikasi web untuk mengamankan data pribadi para pengguna internet. Tujuan ini dilandasi oleh rentannya data pribadi tersebut terhadap peretasan maupun penyadapan ketika digunakan di internet. Maka sebaiknya pemilik data pribadi perlu melakukan langkah antisipasi untuk mencegah kerugian yang ditimbulkan akibat serangan tersebut. Teknik pengamanan yang diterapkan dalam aplikasi menggunakan algoritma kriptografi One Time Pad yang akan mengenkripsi pesan sehingga tersamarkan. Algoritma ini terbukti unbrekable karena password untuk enkripsi dan dekripsi hanya digunakan sekali dan panjangnya sama dengan panjang pesan. Data penelitian adalah sejumlah file yang akan diamankan dengan berbagai ukuran dan berjenis dokumen pengolah kata (docs), spreadsheet (xlsx), portable document (pdf), dan teks (txt). Metode pengembangan sistem yang digunakan adalah rekayasa web yang terdiri dari langkah komunikasi, perencanaan, pemodelan, konstruksi, dan penyebaran. Alat pemodelan menggunakan diagram UML. Rancangan aplikasi diuji dengan metode blackbox, dan uji kecepatan. Penelitian menghasilkan rancangan aplikasi web beserta prototypenya. Aplikasi ini akan dapat digunakan oleh para pengguna internet secara bebas untuk mengamankan file-file data pribadi yang akan mereka gunakan di internet. Meskipun file data pribadi sudah diproteksi, sebaiknya password yang digunakan untuk memproteksi dan membuka proteksi dikirim melalui media lain, misalnya saluran telepon, dengan tujuan untuk mengurangi potensi penyadapan data.

***Kata kunci**: Aplikasi Web; Kriptografi; One Time Pad*

1. PENDAHULUAN

1.1 Kriptografi

Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan. Pesan dapat berbentuk data atau informasi yang dikirim melalui saluran telekomunikasi atau yang disimpan didalam media rekam. Pesan yang tersimpan dapat berupa gambar, suara, video, atau berkas digital lainnya. Kriptografi terdiri dari beberapa elemen yang membentuk sebuah sistem yang disebut sistem kriptografi yang terdiri dari algoritma kriptografi, plainteks, chiperteks, dan kunci [1].

Sesuai definisinya, kriptografi bertujuan untuk memberikan layanan keamanan yang juga disebut aspek-aspek keamanan yang terdiri dari:

1) Kerahasiaan
   Atau confidentiality bertujuan untuk menjaga agar pesan tidak dapat dibaca oleh pihak-pihak yang tidak berhak. Dalam kriptografi layanan ini diwujudkan dengan menyandikan pesan menjadi chiperteks.
2) Integritas data
   Atau *data integrity* bertujuan untuk menjamin keaslian pesan atau belum dimanipulasi selama pengiriman. Dalam kriptografi layanan ini diwujudkan dengan menggunakan tanda tangan digital
3) Otentikasi
   Atau *authentication* bertujuan untuk memastikan identitas pihak-pihak yang berkomunikasi maupun kebenaran sumber pesan. Dalam kriptografi layanan ini berwujud tanda tangan digital.

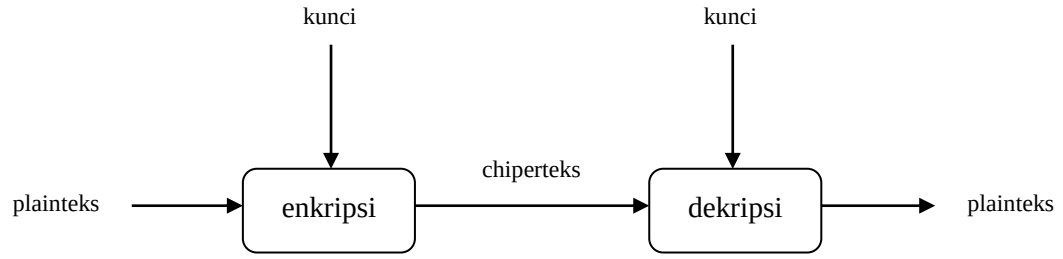
4) Nirpenyangkalan
Atau non-repudiation bertujuan untuk mencegah pihak yang berkomunikasi melakukan penyangkalan. Penyangkalan bisa terjadi dari pihak pengirim yang menyangkal telah melakukan pengiriman pesan atau dari pihak penerima yang menyangkal telah menerima pesan.

Berdasarkan sejarahnya, kriptografi dibagi menjadi kriptografi klasik dan modern. Berdasarkan kunci enkripsi dan dekripsi, kriptografi dibedakan menjadi kriptografi kunci simetri dan kunci nirsimetri. Kriptografi kunci simetri menggunakan kunci yang sama untuk mengenkripsi dan mendekripsi. Sedangkan kriptografi kunci nirsimetri menggunakan kunci yang berbeda. Semua kriptografi klasik merupakan kriptografi kunci simetris. Sedangkan kriptografi modern sebagian merupakan kriptografi kunci simetris seperti DES dan AES.

Pada dasarnya kriptografi kunci simetri beroperasi dalam salah satu dari dua jenis operasi, yaitu mode blok dan aliran. Mode blok beroperasi terhadap satu blok data setiap kali melakukan enkripsi dan dekripsi data. Mode aliran mengenkripsi dan mendekripsi 1 bit atau byte data setiap kalinya.

1.2 Algoritma One Time Pad

One time pad tergolong kedalam kriptografi klasik kunci simetri. Skema kriptografi kunci simetri dapat digambarkan sebagai berikut:



Gambar 1. Skema kriptografi kunci simetri

Rumus enkripsi algoritma one time pad dinyatakan sebagai penjumlahan modulo 26 dari satu karakter plainteks dengan satu karakter kunci:

$$c_i = (p_i + k_i) \bmod 26 \quad (1)$$

dimana:
c_i: karakter chiperteks ke-i
p_i: karakter plainteks ke-i
k_i: karakter kunci ke-i

Sedangkan rumus dekripsi one time pad adalah:

$$p_i = (c_i - k_i) \bmod 26$$

2. METODOLOGI

Pembangunan aplikasi menggunakan metode rekayasa web yang terdiri dari langkah-langkah:

1) Komunikasi
Pada langkah ini dilakukan pengumpulan data dan informasi mengenai aplikasi kriptografi berbasis web.
2) Perencanaan
Pada langkah ini pekerjaan dan jadwal pembangunan aplikasi diidentifikasi dan disusun.

3) Pemodelan
   Setelah pekerjaan dan jadwal pelaksanaan disusun, langkah selanjutnya adalah membuat model dari aspek-aspek aplikasi yang meliputi spesifikasi persyaratan fungsional, modul-modul program, database, dan arsitektur aplikasi.
4) Konstruksi
   Model-model yang dihasilkan pada langkah sebelumnya kemudian dijadikan dasar pembuatan kode-kode program dari aplikasi. Setelah kode program terbentuk maka dilakukan pengujian terhadap aplikasi menggunakan metode blackbox untuk memastikan fungsional aplikasi bekerja sesuai rancangan.
5) Penyebaran
   Pada langkah ini melibatkan calon pengguna aplikasi untuk mencoba aplikasi dan memberikan umpan balik. Perbaikan terhadap aplikasi akan dilakukan berdasarkan umpan balik yang diberikan calon pengguna. Proses perbaikan akan terus dilakukan sampai calon pengguna dapat menerima versi perbaikan aplikasi terakhir.

3. HASIL DAN PEMBAHASAN

Dari hasil pengumpulan data dan informasi diperoleh kesimpulan bahwa aplikasi untuk mengamankan data menggunakan kriptografi yang berbasis web yang dapat digunakan secara bebas oleh pengguna internet belum ditemukan. Aplikasi yang ditemukan menggunakan platform Android. Kelebihan aplikasi basis web dari basis android adalah tidak perlu menginstall aplikasi pada perangkat yang digunakan [3][4][5].

3.1 Pembangkit Password

Pembangkit kunci untuk algoritma one time pad pada pembangunan aplikasi ini menggunakan metode seperti yang diusulkan oleh Pratama [2]. Metode ini cukup sederhana dalam implementasinya tetapi tetap menghasilkan deretan kunci yang diperlukan dengan baik. Metode pembangkit kunci ini menggunakan karakter ‘A’ sampai dengan ‘Z’. Langkah-langkah pembakitan kunci sebagai berikut:

1) Karakter terakhir dari kunci dijumlahkan dengan n-1 karakter sebelumnya (n adalah panjang kunci asli), kemudian jumlah tersebut dikenakan modulo 26.
2) Hasil modulo merupakan karakter baru yang kemudian digabungkan dengan kunci sebelumnya menjadi kunci baru.
3) Proses kembali mengulang langkah pertama sampai kunci sepanjang plaintext.

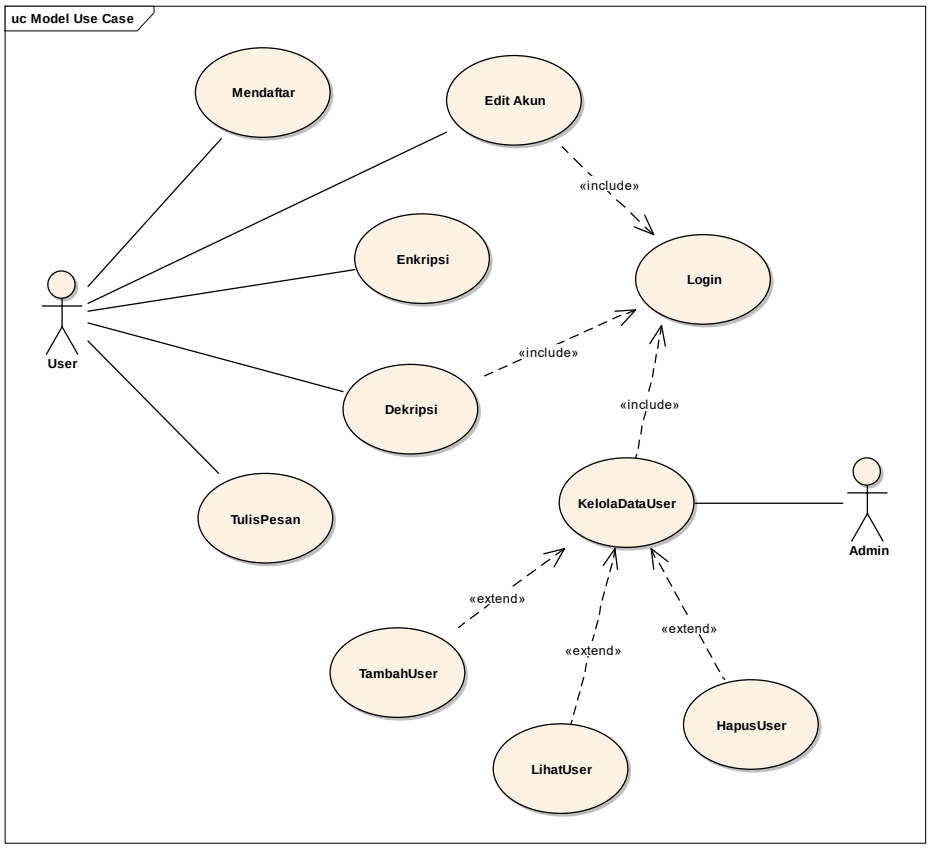
Berdasarkan langkah-langkah diatas, diperoleh rumus sebagai berikut untuk menghasilkan kunci ke-i:

$$k_i = (k_i\text{-}n + k_i\text{-}1) \bmod 26 \quad (2)$$

dimana:
i = n+1, n+2, ...
ki = karakter kunci ke-i (A=0,B=1,...)
n = panjang kunci asli

3.2 Pemodelan Aspek-aspek Aplikasi

Pada langkah pemodelan, fungsi-fungsi yang dapat dilakukan oleh aplikasi diidentifikasi menggunakan diagram use case sebagai berikut:



Gambar 2. Diagram Use Case Fungsional Aplikasi

Diagram use case diatas kemudian dijelaskan menggunakan skenario use case yang ditunjukkan pada tabel 1 dan tabel 2.

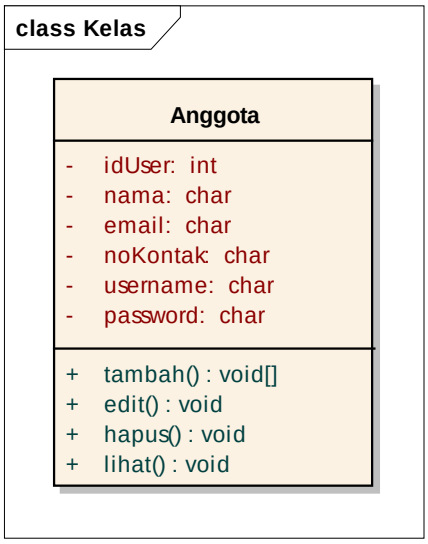
Tabel1. Skenario Usecase Enkripsi

Nama Use Case	**Enkripsi**
Deskripsi	Pengguna diminta untuk memasukkan file plaintext yang akan diacak dan password untuk mengacak pesan dalam file plaintext. Hasil proses berupa file chipertext yang siap diunduh dan password maupun file plaintext dan chipertext tidak disimpan kedalam database untuk alasan keamanan. Pengguna dapat mengirimkan password pembuka file chipertext melalui email atau media lain yang aman ke penerima pesan.
Aktor	Pengguna
Prakondisi	-
Langkah-langkah	
Aktor	Sistem
1. Memilih Menu Enkripsi	2. Menampilkan Form Enkripsi
3. Memasukkan file plaintext dan password	4. Membangkitkan pasword sepanjang file plaintext
	5. Mengacak pesan dalam file plaintext dengan password yang dibangkitkan
	6. Menulis hasil pengacakan ke file
	7. Membuat link untuk mengunduh file
Postkondisi	Terbentuk file chipertext yang siap diunduh

Tabel2. Skenario Usecase Dekripsi

Nama Use Case	Dekripsi
Deskripsi	Pengguna diminta untuk memasukkan file chipertext yang akan dibuka berikut password untuk membukanya. Hasil proses berupa file plaintext yang siap diunduh.
Aktor	Pengguna
Prakondisi	File chipertext sudah dibuat dan pengguna sudah melakukan login ke aplikasi
Langkah-langkah	
Aktor	Sistem
1. Memilih Menu Dekripsi	2. Menampilkan Form Dekripsi
3. Memasukkan file chipertext dan password	4. Membangkitkan pasword sepanjang file chipertext
	5. Mengembalikan pesan kedalam bentuk awal sebelum diacak dengan password yang dibangkitkan
	6. Menulis hasil dekripsi menjadi file plaintext.
	7. Membuat Link untuk mengunduh file plaintext
Postkondisi	Link untuk mengunduh file plaintext terbentuk

Database yang digunakan dalam aplikasi meminimalkan informasi yang perlu disimpan untuk meningkatkan keamanan aplikasi. Maka file-file pengguna maupun hasil enkripsi dan dekripsi tidak akan disimpan kedalam database. Demikian juga halnya dengan password yang digunakan untuk proses enkripsi. Dengan demikian aplikasi ini hanya menggunakan satu tabel yang digunakan untuk menyimpan data keanggotaan. Data ini perlu disimpan karena fitur dekripsi tidak dapat diakses kecuali pengguna memiliki akun aplikasi. Hal ini dilakukan agar fitur dekripsi tidak mudah untuk disalahgunakan. Adapun rancangan database aplikasi sebagai berikut:

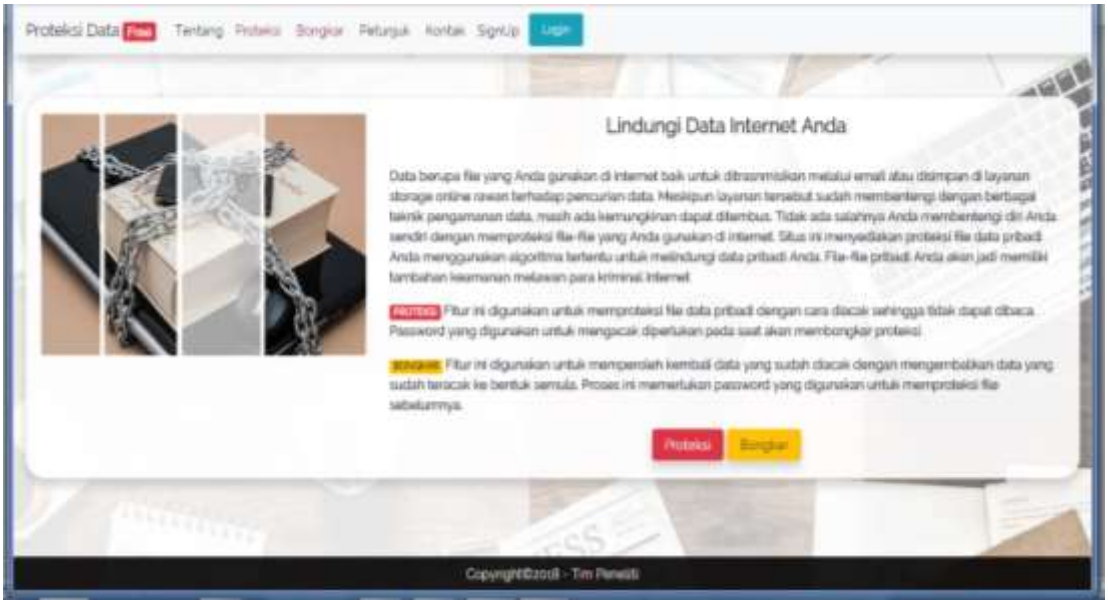


Gambar 3. Diagram Kelas Rancangan database aplikasi

3.3 Prototype Aplikasi

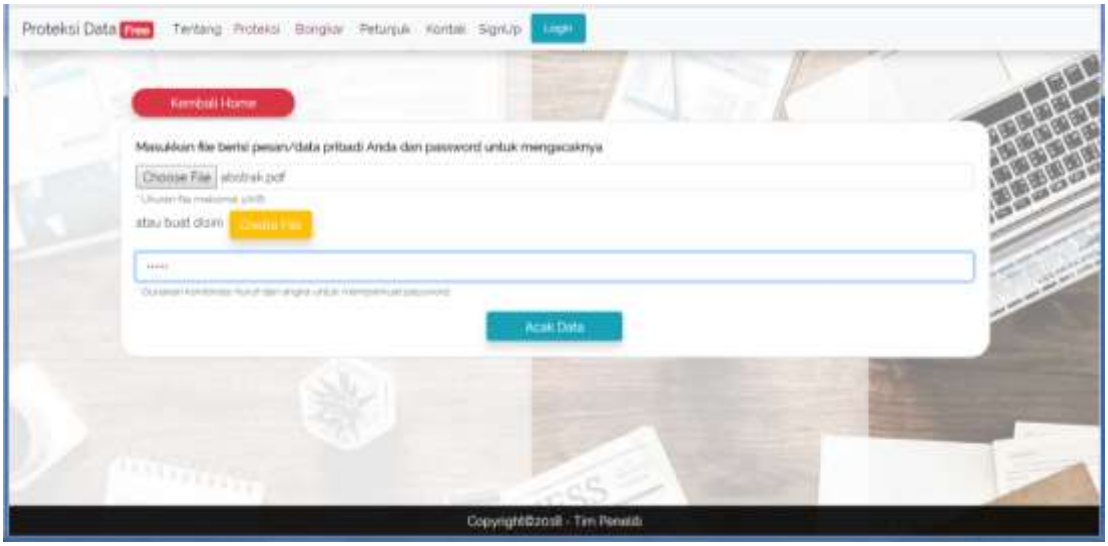
Setelah aspek-aspek aplikasi dimodelkan maka tahap konstruksi dilakukan. Hasil dari tahap konstruksi kemudian diuji coba oleh calon pengguna untuk memperoleh umpan balik.

Setelah beberapa kali perbaikan maka dihasilkan aplikasi yang sesuai dengan harapan calon pengguna. Adapun versi terakhir aplikasi adalah sebagai berikut:



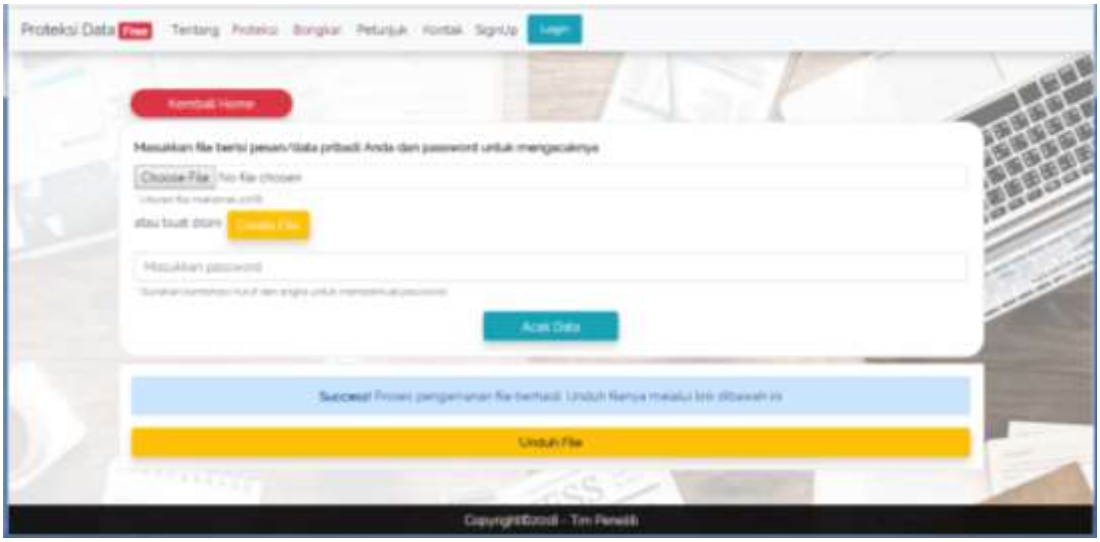
Gambar 4. Halaman awal aplikasi

Pada halaman pertama aplikasi pengguna dapat memilih menu ‘Proteksi’ untuk mengenkripsi file data yang akan menampilkan sebuah form:



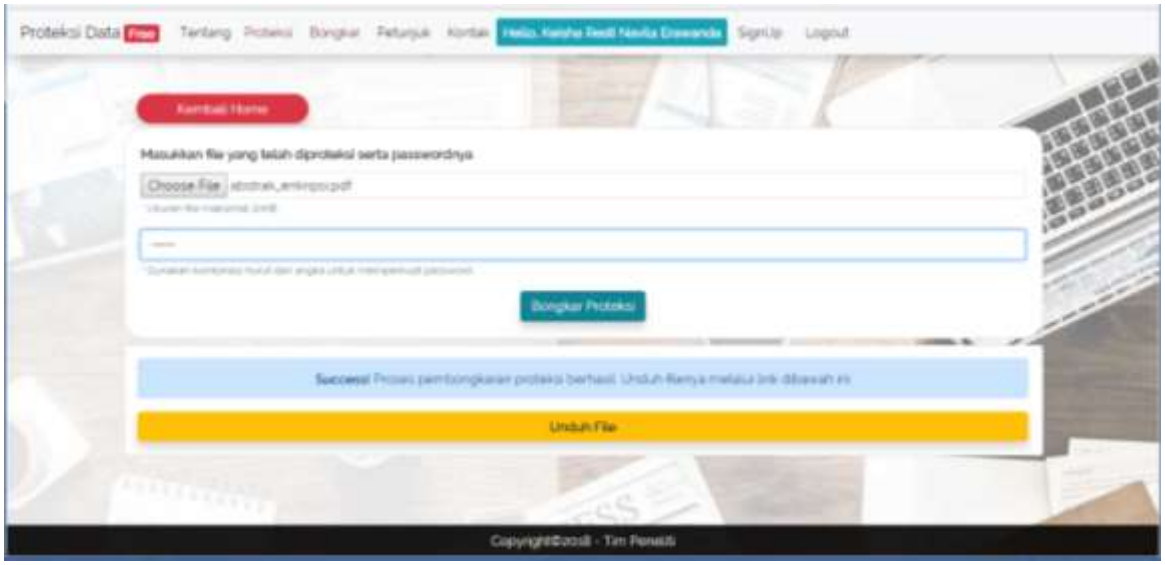
Gambar 5. Form untuk mengenkripsi file data pribadi pengguna

Pada isian pertama form proteksi diatas pilih file berisi data pribadi yang akan diproteksi, pada gambar diatas dipilih file berjenis pdf yaitu ‘abstrak.pdf’. Isian kedua adalah password yang akan digunakan untuk memproteksi. Tekan tombol ‘Acak Data’ untuk memulai proses proteksi. Setelah proses selesai maka pengguna akan memperoleh sebuah link untuk mengunduh file yang telah dienkripsi:



Gambar 6. Link untuk mengunduh file hasil

Untuk membuka proteksi atau menjalankan dekripsi terhadap file hasil enkripsi pengguna harus login terlebih dahulu baru bisa memilih menu ‘Bongkar’ yang akan menampilkan form dekripsi:



Gambar 7. Form untuk proses dekripsi

Masukkan file hasil enkripsi sebelumnya kedalan isian pertama kemudian pada isian kedua masukkan password yang tadi digunakan untuk mengenkripsi.Setelah itu klik tombol ‘Bongkar Proteksi’ maka akan tampil link untuk mengunduh file hasil dekripsi berisi data yang sudah tidak teracak lagi.

4. KESIMPULAN

Aplikasi web pengaman data pribadi ini menggunakan chiper yang terbukti *unbreakable* sehubungan dengan panjangnya kunci dan password sekali pakai. Dari sisi teknik enkripsi yang digunakan, kekuatan proteksi terhadap file data pribadi tidak diragukan lagi. Fungsi-fungsi aplikasi juga dapat bekerja sesuai rancangan fungsionalnya. Agar keamanan data pribadi lebih terjamin lagi, pengiriman password yang digunakan kepada pihak penerima sebaiknya menggunakan media telekomunikasi lain, misalnya lewat saluran telepon.

UCAPAN TERIMA KASIH

Penelitian ini merupakan penelitian skema PSN (Penelitian Strategis Nasional) dengan dana hibah dari Kemenristekdikti. Kami mengucapkan banyak terima kasih kepada Kemenristekdikti untuk kesempatan yang kami peroleh untuk mengembangkan gagasan kami tentang aplikasi untuk mengamankan data pribadi berbasi web. Kami juga berterima kasih kepada Universitas Muria Kudus yang memungkinkan kami untuk menyampaikan gagasan ini. Semoga kerjasama ini dapat memberikan manfaat bagi semua pihak dan masyarakat.

DAFTAR PUSTAKA

Mahmudi, Ali, Mantja, Sandy Nataly, Rozikin, Achmad, (2016), Aplikasi Kriptografi dan Steganografi Menggunakan Metode Least Significant Bit (LSB) dan One Time Pad (OTP), Jurnal MATICS vol. 8 no. 1

Munir, Rinaldi, (2009), Kriptografi, Informatika, Bandung, pp. 2-96

Pratama, Arief, (2010), Pembangkit kunci untuk Chiper One-time Pad, Jurusan Teknik Informatika Sekolah Teknik Elektro dan Informatika ITB, Bandung

Pratiwi, Lis Endah, Marwati, Rini, Yusnitha, Isnie, (2014), Program Aplikasi Kriptografi Penyandian One Time Pad Menggunakan Sandi Vigenere, EurekaMatika vol. 2, no. 1

Zaenah, Purnama, Bambang Eka, (2015), An Analysis of Encryption and Decryption Application by Using One Time Pad Algorithm, IJACSA vol. 6 no. 9