PROTEKSI DOKUMEN *OFFICE* MENGGUNAKAN *XML WEB SERVICE* DENGAN ALGORITMA RSA BERBASIS *WEB* (STUDI KASUS : STIKOM)

Denny Setyawan [1], Soetam Rizky Wicaksono [2]
[1] Program Studi Sistem Informasi, STIKOM Surabaya
[2] Program Studi Sistem Informasi, STIKOM Surabaya. email: soetam@stikom.edu

Abstract: Data security is an important issue in data exchange, especially in cyber world. Because so many threats that threaten the data itself. When Office document exchange in Stikom, its encrypt is made when it's sent use RSA (Rivest-Shamin-Adleman) algorithm. User can download encrypted document from web application then to decrypt the document using desktop application. After that injecting the macros code are using Visual Basic Application (VBA). So, the office document which has injected with macros code only can be open when it's connected to an XML Web Service.

Keywords: Office document, XML Web Service, RSA, VBA

Keamanan data merupakan salah satu isu penting dalam pertukaran data, khususnya pertukaran data di dunia maya yang di dalamnya terdapat banyak ancaman untuk proses itu sendiri. Keamanan data, khususnya untuk dokumen bagi suatu organisasi yang mengasumsikan bahwa dokumen tersebut bernilai rahasia (*private and confidential*). Sama halnya dengan dokumen konvensional, dokumen dalam format digital pun membutuhkan aspek keamanan. Salah satu aspek keamanan dalam dokumen konvensional atau digital adalah orisinalitas. Seperti dokumen konvensional, dokumen digital pun harus terjamin keasliannya, bentuk dan isinya harus sesuai dengan yang dimaksud oleh pembuatnya.

Sebagai suatu institusi pendidikan, STIKOM Surabaya memerlukan suatu cara untuk pengamanan dokumen-dokumen yang penting. Misalnya dalam pengamanan dokumen soal ujian. Soal ujian yang dibuat oleh dosen dalam bentuk dokumen Word atau Excel dikirimkan secara *online* melalui jaringan lokal. Pada dokumen tersebut telah diberi program yang mengharuskan terkoneksi dengan *web service* pada jaringan lokal STIKOM untuk melakukan otentifikasi. Akibatnya, dokumen tersebut tidak bisa dibuka di tempat lain selain jaringan lokal STIKOM. Sehingga, dokumen tersebut hanya bisa dibuka oleh pihak yang berkewenangan saja.

Enkripsi dokumen dilakukan pada saat dokumen tersebut dikirim untuk lebih mengamankan data dari para *attacker*. Untuk mempermudah distribusi dokumen antara pengirim dan penerima, maka dibutuhkan sistem enkripsi yang bersifat publik yaitu dengan *public key cryptosystem*, salah satunya adalah dengan algoritma *Rivest-Shamir-Adleman* (*RSA*). *RSA* adalah sistem sandi yang saat ini praktis menjadi standar *de facto* dunia dalam kriptografi asimetrik di samping *Data Encryption Standard* (*DES*).

LANDASAN TEORI

Kriptografi adalah ilmu untuk menjaga keamanan pesan (Yusuf, 2004). Sedangkan, seseorang yang dianggap pakar dalam masalah kriptografi seringkali disebut sebagai kriptografer (Yusuf, 2004). Kata *cryptography* berasal dari kata Yunani *kryptos* (tersembunyi) dan *graphein* (menulis).

Dalam sebuah algoritma kriptografi selalu terdiri dari dua proses yaitu proses enkripsi dan proses deskripsi. Enkripsi adalah proses mengacak sebuah pesan atau teks sehingga arti yang sebenarnya tidak dapat diketahui. Deskripsi adalah proses pengembalian pesan atau teks yang terenkripsi menjadi normal kembali. Bentuk asli dari suatu teks yang akan dienkripsi disebut *plaintext*, sedangkan teks hasil enkripsi dapat disebut *chipertext* (Mao, 2004).

Algoritma *RSA* adalah metode kriptografi yang ditemukan oleh Ronald L. Rivest, Adi Shamir dan Leonard Adlleman pada tahun 1977. Algoritma *RSA* adalah sebuah blok *cipher algorithm* (algoritma yang bekerja per blok data) yang mengelompokkan *plaintext* menjadi blok-blok terlebih dahulu sebelum dilakukan enkripsi hingga menjadi *ciphertext* (Pfleeger, 1989).

RSA termasuk algoritma asimetri yang berarti memiliki sepasang kunci, yaitu kunci publik dan kunci privat. Dalam *RSA* hanya digunakan satu algoritma untuk melakukan enkripsi dan deskripsi. Perbedaannya hanya terletak pada eksponen yang digunakan. Kunci public (n,e) sebagai kunci enkripsi dan kunci privat (n,d) sebagai kunci deskripsi dimana d, e dan n adalah bilangan bulat positif (Kramer, 1999).

ASP.Net telah menyediakan *class* khusus untuk melakukan proses enkripsi dengen metode *RSA*. Class tersebut diturunkan dari *namespace Cryptography* dan ditempatkan sejajar dengan algoritma enkripsi yang lain seperti Rijndael, *SHA* dan *DES*. *Class RSA* memiliki properti dan method yang mampu melakukan *generate key*, enkripsi dan dekripsi. Panjang kunci minimal yang dapat dihasilkan dari *class RSA Crypto Service Provider* adalah 512 bit. Dengan demikian implementasi algoritma *RSA* menjadi lebih mudah.

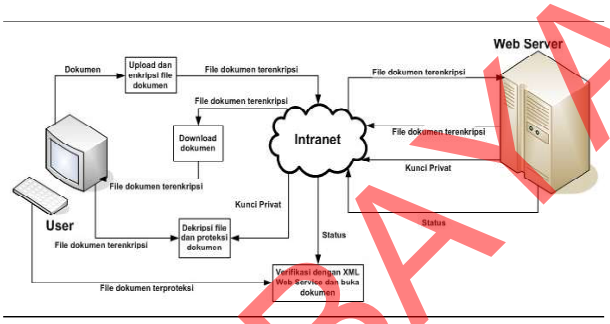
Visual Basic for Application (*VBA*) adalah bahasa pemrograman yang menyerupai *Visual Basic* dan memiliki beberapa tambahan kemampuan untuk membantu para programmer dalam mengembangkan aplikasi dengan lebih mudah. *VBA* terintegrasi langsung dengan suatu aplikasi induk sehingga menawarkan keunggulan terhadap kecepatan, kinerja proses, integrasi dengan aplikasi induk (kode berada dalam dokumen) dan kemampuan untuk membuat solusi tanpa menggunakan alat bantu tambahan.

VBA menyediakan suatu lingkungan pengembangan terintegrasi *Integrated Development Environment* (*IDE*), seperti halnya pemrograman dengan menggunakan *Visual Basic*, termasuk tampilan proyek, *properties* dan *debugging*. *VBA* juga mendukung form-form *Microsoft* untuk membuat *custom dialog box* dan kontrol *Active-X* untuk pengembangan tampilan antarmuka (*user interface*).

Web services merupakan perkembangan *distributed computing* dengan arsitektur n-tier. Keuntungan yang paling mendasar yang ditawarkan oleh *web services* adalah integrasi. Usaha untuk mengintegrasikan aplikasi, sistem, maupun platform yang berbeda sering mengalami kesulitan dan memerlukan proses yang panjang. *Web services* merupakan standar yang tepat sebagai alat pengintegrasian. *Web services* mampu mengintegrasikan aplikasi dan sistem dari *platform* yang berbeda karena menggunakan standar protokol *web* dalam interaksinya seperti *TCP/IP, HTTP, XML, SOAP, UDDI.* Terdapat 5 blok utama dalam *web services* antara lain *Discovery, Description, Message Format, Encoding* dan *Transport* (Short, 2003)..

PEMBAHASAN

Pada tahap ini diuraikan hasil dan pembahasan apakah sistem telah memenuhi *output* seperti yang diarapkan. Tetapi sebelumnya diberikan arsitektur dari sistem agar pembaca mengetahui bagaimana rancangan awal dari sistem ini.



Gambar 1 Arsitektur Sistem

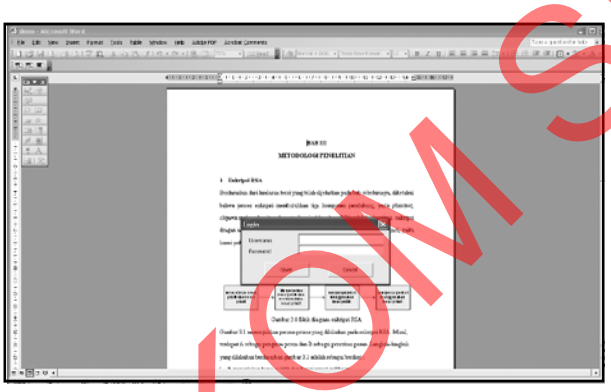
Dokumen yang dikirim oleh *user* kepada *user* lain akan dienkripsi terlebih dahulu menggunakan *RSA*. Sehingga, dokumen yang tersimpan dalam *server* berupa dokumen yang telah terenkripsi. Gambar 2 adalah *interface* ketika *upload* dokumen.

Gambar 2 Halaman Kirim Dokumen

Gambar 3 Halaman *Download* Dokumen

Gambar 4 *Form* Hasil Dekripsi

Sebelum dokumen yang telah terdekripsi tersebut disimpan, injeksi kode-kode macro dilakukan. Injeksi tersebut bertujuan agar dokumen hanya dapat dibuka jika terkoneksi dengan XML *Web Service*. Pada saat dokumen dibuka, akan muncul *form login* yang mengharuskan untuk *user* memasukkan *username* dan *password* (lihat Gambar 5). *Username* dan *password* tersebut akan divalidasi menggunakan *XML Web Service*. Hanya *user* yang berhak yang dapat menggunakan dokumen tersebut.



Gambar 5 *Open* Dokumen

Uji coba *upload* dilakukan pada aplikasi *web* yang telah dilakukan hosting pada sebuah *web hosting* dengan *bandwitch* 2 Gb dan alokasi kapasitas pada *server* 50 Mb. Uji coba menggunakan koneksi *Speedy* dengan kecepatan 263 Kbps. *User* yang ingin melakukan proses *download* dokumen dapat mengakses halaman *inbox* dan melihat detil dari isi *inbox* Dokumen yang telah dilakukan proses *download* oleh *user* masih berupa dokumen yang terenkripsi. Proses dekripsi dokumen dilakukan menggunakan aplikasi desktop. Dekripsi dokumen dilakukan menggunakan *RSA* dengan kunci privat yang diambil melalui *XML Web Service*. Setelah dokumen terdekripsi, isi dari dokumen tersebut akan ditampilkan pada *Viewer* menurut tipe dokumen.

SIMPULAN

Secara umum sistem Proteksi Dokumen *Office* Menggunakan *XML Web Service* dengan Algoritma *RSA* Berbasis *Web* telah berfungsi sebagaimana yang diharapkan. Untuk itu, dapat diambil beberapa kesimpulan dari sistem ini sebagai berikut:

1. Algoritma *RSA* dapat melindungi dokumen sehingga lebih mengamankan dokumen pada sistem pertukaran dokumen.
2. Aplikasi *web* yang dibuat dapat menangani *upload* dan *download* secara aman karena mengimplementasikan algoritma *RSA* untuk melindungi data.
3. Otentifikasi dokumen dapat dilakukan menggunakan *VBA,* sehingga validitas data lebih terjamin.
4. Dokumen yang telah terenkripsi mengalami pembengkakan ukuran rata-rata sebesar dua kali lipat dari ukuran dokumen semula.
5. Dekripsi tidak dapat dilakukan, jika komputer tidak terkoneksi dengan *XML Web Services.*
6. Dokumen tidak dapat dibuka jika komputer tidak terkoneksi dengan *XML Web Services.*

Adapun saran-saran untuk pengembangan sistem antara lain:

1. Aplikasi dapat dikembangkan untuk mengenkripsi file-file lain selain dokumen *Microsoft Excel* dan *Microsoft Word.*
2. Algoritma *RSA* dapat dikombinasikan dengan algoritma simetris untuk lebih meningkatkan keamanan data.
3. Menerapkan algoritma kompresi data agar pembengkakan ukuran data setelah terenkripsi dapat diperkecil.

RUJUKAN

Kramer, P. 2002. *Encryption and Decryption with RSA Algorithm Mathematics and The Computer*. Jakarta: Informatika.

Kurniawan, Y. 2004. *Kriptografi: Keamanan Internet dan Jaringan Komunikasi*. Bandung: Informatika.

Mao, W. 2004. *Modern Cryptography*. New Jersey: Prentice-Hall.

Munir, R. 2006. *Kriptografi*. Bandung: Informatika.

Santina, GAPL. 2006. *Rancang bangun Aplikasi Sistem Pemesanan Tiket Menggunakan Web Services*. Skripsi tidak diterbitkan. Surabaya: Program Studi Strata Satu Sarjana Komputer STIKOM Surabaya.

Short, S. 2003. *Building XML Web Services For The Microsoft .Net Platform*. Jakarta: PT Elex Media Komputindo.

Tjoenedi, FK. 2004. *Pembuatan Program Digital Signature Authentication File dengan ECDSA di*

Bidang Penjualan Hardware. Skripsi tidak diterbitkan. Surabaya: Program Studi Strata Satu Sarjana Komputer STIKOM Surabaya.