Metode Enkripsi Untuk Multiple Database Format Berbasis XML

Suyanto
Universitas Bina Darma
Jalan Jenderal Ahmad Yani No.12, Palembang
Pos-el : suyanto@mail.binadarma.ac.id

ABSTRAK

Berkembangnya teknologi pengolahan data, telah menuntut penerapan sistem komputerisasi di segala bidang. Seluruh bagian dari organisasi atau perusahaan telah menerapkan berbagai aplikasi untuk memenuhi kebutuhan operasional mereka. Aplikasi yang diterapkan secara terpisah menimbulkan masalah sendiri apabila aplikasi-aplikasi tersebut memerlukan data yang sama, maka pertukaran data menjadi solusi alternatif. Persyaratan keamanan data pada proses pertukaran database menjadi masalah baru dalam proses tersebut. Untuk menjamin keamanan data pada proses pertukaran, metode enkripsi merupakan jalan yang terbaik. Dengan menerapkan enkripsi pada data yang dipertukarkan, maka data dijamin aman dan hanya dapat dibaca oleh orang yang benar-benar membutuhkan. Metode penelitian yang digunakan pada penelitian ini adalah metode action research sedangkan metode pengembangan sistem yang digunakan adalah *Prototype Model*. Hasil penelitian ini adalah sebuah aplikasi yang mampu membaca database access, oracle dan sql server, kemudian mengenkripsi tabel yang diinginkan dan mampu mentransform ke format xml. Dengan xml, database (tabel) dapat dibaca oleh aplikasi lain meskipun dengan platform yang berbeda.

Kata Kunci : Enkripsi, Dekripsi, Keamanan, Basis Data,Tersandikan, *Xml*

1. Pendahuluan

Dengan berkembangnya pengolahan data, tidak jarang satu aplikasi menggunakan database yang sama untuk aplikasi yang lainnya. Jalan yang bisa ditempuh adalah dengan cara mengkopi database yang dibutuhkan tersebut dari satu aplikasi ke aplikasi yang lain. Hal ini merupakan jalan pintas, agar aplikasi yang membutuhkan data tadi bisa dioperasikan. Begitu seterusnya sehingga kegiatan kopi database merupakan suatu kebutuhan dari aplikasi tersebut. Melihat kondisi diatas, maka keamanan data menjadi suatu hal yang sangat penting. Karena bukan hal yang mustahil bahwa data yang dipertukarkan akan disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab untuk memenuhi kebutuhan pribadi, maka perlu teknik khusus untuk mengamankan database yang dipertukarkan tersebut.

Permasalahan yang dibahas pada penelitian ini adalah bagaimana memanfaatkan metode *symmetric encryption substitution cipher* untuk *multiple* format database, sedangkan tujuan penelitian ini adalah menerapkan metode enkripsi untuk keamanan data pada proses pertukaran data / database sehingga data yang tersimpan mempunyai *Privacy / Confidentiality,* Integritas *(Integrity), Availability* dan *Authentication* yang terjamin. Manfaat yang akan diperoleh dari penelitian ini adalah : 1) Data hasil enkripsi terjamin kerahasiaannya. 2) Untuk menjaga keaslian/keutuhan data. 3) Terjaminnya keabsahan data. 4) Mencegah terjadinya penyangkalan dari pemilik atau pengirim data.

Kebutuhan keamanan sistem komputer dapat dikategorikan menjadi aspek-aspek sebagai berikut (Rahardjo, 2002) :1. *Privacy / Confidentiality* Inti utama aspek *privacy* atau *confidentiality* adalah usaha untuk menjamin informasi dari orang yang tidak mempunyai hak mengakses. *Privacy* menjelaskan data-data yang sifatnya *private sedang confidentiality* berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu dan hanya diperbolehkan untuk keperluan tersebut. 2. *Integritas* bagian ini akan menekankan bahwa informasi tidak boleh diubah tanpa ijin pemilik informasi. Serangan virus dan trojan, dan juga pemakai lain yang mengubah informasi tanpa ijin merupakan contoh masalah yang dihadapi. Sebuah e-mail dapat saja disadap di tengah jalan, diubah

isinya (*altered*, *tampered* dan *modified*), kemudian diteruskan ke alamat yang dituju. Dengan kata lain, integritas dari informasi sudah tidak terjamin. Penggunaan enkripsi dan tanda digital, dapat mengatasi masalah ini. 3.*Authentication* Bagian ini berhubungan dengan metode untuk menjamin bahwa informasi benar-benar asli, dan orang yang menerima atau memberikan informasi adalah betul-betul orang yang dituju, atau *server* yang kita tuju adalah benar-benar *server* yang asli. 4. *Availability* Aspek *availability* atau ketersediaan berhubungan dengan ketersediaan informasi ketika dibutuhkan. Sistem informasi yang diserang atau dijebol dapat menghambat atau meniadakan akses ke informasi.

Salah satu mekanisme untuk meningkatkan keamanan data dalam database adalah dengan menggunakan teknologi enkripsi. Data-data yang disimpan dalam database diubah sedemikian rupa sehingga tidak mudah dibaca. Jadi enkripsi adalah proses yang dilakukan untuk mengamankan sebuah data (yang disebut *plaintext*) menjadi data yang tersembunyi (disebut *ciphertext*). *Ciphertext* adalah data yang sudah tidak dapat dibaca dengan mudah. Menurut ISO 7498-2, terminologi yang lebih tepat digunakan adalah "*encipher*". Proses sebaliknya, untuk mengubah *ciphertext* menjadi *plaintext*, disebut dekripsi. Menurut ISO 7498-2, terminologi yang lebih tepat untuk proses ini adalah "*decipher*" (Rahardjo:2002).

Pengetahuan yang mempelajari tentang enkripsi adalah kriptografi. Yang dimaksud dengan kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Sedangkan menurut Prasetyo (2006:372) Kriptografi adalah suatu ilmu pengetahuan (atau lebih tepatnya suatu seni) yang mengenkripsi informasi sehingga sepenuhnya terlihat berbeda dari aslinya. Selain itu Munir (2006) menjelaskan Kriptografi adalah ilmu dan seni untuk menjaga keamaan pesan atau data.

Enkripsi diperlukan terutama dikarenakan adanya kebutuhan untuk pertukaran data dari satu database ke database lain atau adanya kebutuhan pengiriman data. Dengan data yang terenkripsi maka apabila sampai data tersebut disadap orang atau dibuka orang yang tidak tepat maka dia tidak akan bisa menemukan data apapun.

Terdapat beberapa cara untuk melakukan enkripsi (Suryana dkk, 2007:3) yaitu: Enkripsi Simetris (*symmetric encryption*) dan Asimetris (*asymmetric encryption*). Algoritma Enkripsi simetris (*symmetric encryption*) ini menggunakan sebuah kunci rahasia yang sama (*private key*) untuk melakukan proses enkripsi dan dekripsinya. Algoritma ini termasuk dalam algoritma kriptografi klasik yang terdiri dari: s*ubstitution cipher* dan *transposition cipher*.

Cara kerja dari algoritma s*ubstitution cipher* ini adalah dengan menggantikan setiap karakter dari *plaintext* dengan karakter lain. Algoritma ini pertama kali digunakan oleh julius caesar, dan disebut juga sebagai *shift cipher*, yaitu dengan cara menggeser urutan abjadnya. Substitusi ini dikenal juga dengan c3 (pada caesar menggeser 3 posisi). Secara umum sistem *cipher* caesar dapat ditulis Zi = cn(pi). Zi adalah karakter *ciphertext*, Cn adalah transformasi substitusi alfabet, n adalah jumlah pergeseran huruf, dan pi adalah karakter plaintext (Kelompok 124 IKI-83408 MTI UI, 2005). Sedangkan algoritma *transposition cipher* diperoleh dengan mengubah posisi *plaintext*nya. Dengan kata lain, algoritma ini melakukan *transpose* terhadap rangkaian karakter di dalam teks. Nama lain untuk metode ini adalah permutasi, karena *transpose* setiap karakter di dalam teks sama dengan mempermutasikan karakter-karakter tersebut.

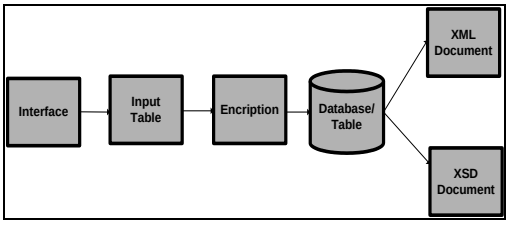
Guna mendukung bermacam-macam format database, maka hasil enkripsi kemudian digenerate menjadi format XML. XML adalah sebuah bahasa markup yang digunakan untuk mengolah meta data (informasi tentang data) yang menggambarkan struktur dan tujuan data yang terdapat dalam dokumen XML, namun tidak mencerminkan format tampilan data tersebut. XML adalah sebuah standar sederhana yang bisa dipakai untuk menggambarkan data teks dengan cara deskripsi diri (*self-describing*).

Dalam buku NIIT (2009) yang berjudul "*Introduction to Web Content Development"* menjelaskan tentang XML sebagai berikut :

- *XML is a text-based markup language that enables storage of data in a structured format.*
- *XML is a cross-platform, hardware and software independent markup language that enables structured data transfer between heterogeneous systems.*
- *XML is used as a common data interchange format in a number of applications.*

Karena XML bersifat mudah untuk dibaca dan ditulis baik oleh manusia maupun komputer, maka XML merupakan sebuah format yang dapat digunakan untuk pertukaran data (*interchange*) antar aplikasi dan platform yang berbeda (*platform independent*). Metode deskripsi data XML (*self-describing*) membuatnya menjadi pilihan efektif untuk aplikasi bisnis ke bisnis, transfer antar jaringan komputer, *e-business*, serta aplikasi terdistribusi. XML bersifat *extensible*, sehingga bisa digunakan pada pemrograman yang berbeda-beda bahasa, dan datanya dapat ditransfer dengan mudah melalui protokol standar internet seperti HTTP tanpa dibatasi oleh *firewall*.

Kerangka pikir pengembangan perangkat lunak yang akan dibangun dapat digambarkan sebagai berikut :

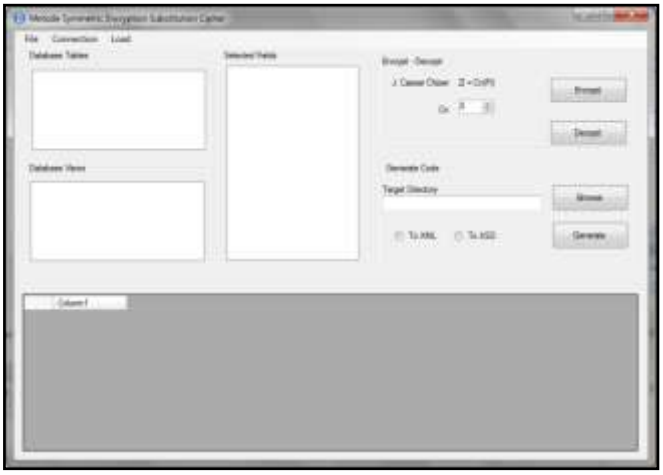


Gambar 1. Kerangka Pikir Pengembangan Aplikasi

2. Pembahasan

Hasil dari penelitian ini adalah berupa perangkat lunak enkripsi yang dibuat dengan menggunakan bahasa pemrograman C# yang merupakan bagian dari Microsoft Visual Studio 2005. Perangkat lunak ini merupakan perangkat lunak aplikasi atau perangkat lunak bantu (*tools*) yang dimaksudkan untuk membantu bagian administrator database dalam melakukan pemindahan data dari database satu dengan database yang lain. Perangkat lunak ini dibutuhkan untuk menjamin keamanan data yang dipindahkan dengan cara mengenkripsi. Selain itu perangkat lunak ini bisa mengubah data menjadi format XML. Hal ini bertujuan agar data tersebut bisa dibaca dan diterima oleh database yang mempunyai format yang berbeda atau dengan kata lain bisa dibaca pada platform yang berbeda.

Sebelum melakukan enkripsi, user harus menentukan format database yang akan dibaca terlebih dahulu. Format database yang bisa dibaca oleh perangkat lunak ini antara lain : SQL Server Server, *Microsoft Access* dan *Oracle*. Selain itu, user harus menentukan jumlah pergeseran digit karakter sekaligus sebagai kunci enkripsi. Tampilan perangkat lunak ini sebagai berikut:



Gambar 2. Tampilan Menu Utama *Symmetric Encryption*

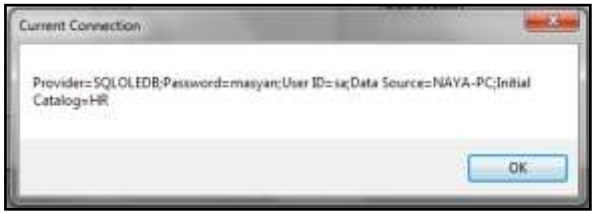
Pada menu File ini hanya berisi menu *Close*. Menu ini berfungsi untuk keluar dari aplikasi. Sedangkan Menu *Connection* berfungsi untuk menentukan dan memilih jenis koneksi database yang akan digunakan serta menampilkan informasi koneksi database yang sedang terkoneksi, sehingga menu ini memiliki dua sub menu yaitu : *Open a New Connection* dan *View Current Connection. Open a New Connection* berguna untuk membuat koneksi baru sedangkan *View Current Connection* berfungsi menampilkan jenis koneksi yang sedang terjadi. Untuk memilih koneksi database, user harus mengerti jenis database apa yang akan diprosesnya, karena jenis database yang berbeda memerlukan jenis koneksi yang berbeda pula. Menu *Connection* ini mempunyai tiga macam jenis koneksi yaitu : Access dan Oracle serta SQL Server.

Berikut ini adalah menu koneksi database melalui SQL Server. Formulir yang perlu diisikan pada *form* ini antara lain : Nama Server (*Server Name*), Nama Database (*SQL Server Initial Catalog*), *User Id* dan *Password*. *Server Name*, diisi dengan nama server dimana database yang akan dienkripsi tersebut disimpan. Apabila servernya lokal, maka biasanya nama server tersebut diisi sesuai nama komputer lokal tersebut. *SQL Server Initial Catalog,* diisi berdasarkan nama database yang akan dibaca. *User Credentials : User Id* dan *Password,* diisi sesuai login user dan *Password* untuk akses database pada SQL Server. Untuk Server lokal, biasanya dengan User Id : sa. *Use Integrated Sequrity* digunakan bila login SQL Servernya menggunakan *Windows Authentication* artinya user id dan passwordnya sesuai dengan user id dan passswordnya windows yang digunakan pada server lokal. Setelah semua form diisi maka untuk mengetahui koneksi berhasil atau tidak user menekan tombol *Test.*

Berikutnya adalah menu koneksi database melalui Access. Formulir yang perlu diisikan pada *form* ini antara lain : Nama Database, *User Id* dan *Password* jika ada. Untuk pengisian nama database dengan cara menekan tombol *Browse* dan arahkan pencarian file ke path dimana database access disimpan. Setelah semua isian diisi lengkap, langkah berikutnya adalah menekan tombol *Test* untuk mengetahui keberhasilan dari koneksi, dan menekan tombol OK bila koneksi sudah berhasil.

Koneksi database yang lain adalah menu koneksi database melalui Oracle. Formulir yang perlu diisikan pada *form* ini antara lain : Nama Database, *User Id* dan *Password*. Untuk pengisian nama database dengan cara mengetikkan langsung melalui form isian. Setelah semua isian diatas diisi lengkap, langkah berikutnya adalah menekan tombol *Test* untuk mengetahui keberhasilan dari koneksi, dan menekan tombol OK bila koneksi sudah berhasil.

Setelah berhasil melakukan koneksi database baik database SQL Server, Access maupun Oracle, maka untuk melihat koneksi yang sedang berjalan saat ini dengan cara mengklik menu *View Current Connection.* Adapun tampilan dari menu tersebut sebagai berikut:



Gambar 3. Tampilan Menu *View Current Connection*

Tampilan *View Current Connection* diatas dilakukan dengan koneksi SQL Server, dengan nama *server* NAYA-PC, nama database HR, User Id sa dan password masyan. Dengan sudah adanya koneksi database seperti yang tersebut diatas, maka data tabel baru bisa dipanggil melalui menu *Load.*

Menu *Load* berguna untuk memanggil data dari database yang telah terkoneksi. Dari menu ini akan menampilkan daftar tabel dari database yang bersangkutan. Daftar tabel tersebut akan ditampilkan pada data list. Setelah tabel-tabel tersebut ditampilkan, user bisa memilih salah satu tabel yang akan dienkripsi. Pada saat user memilih tabel, maka sistem akan menampilkan seluruh data (*record*) ke dalam datagrid, sehingga user bisa melihat isi dari tabel yang bersangkutan. Adapun tampilan hasil dari *Load data for Current Connection* sebagai berikut:

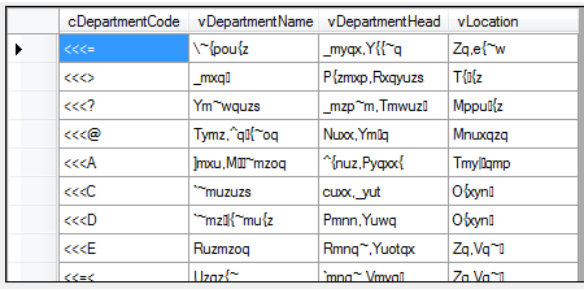

Gambar 4. Tampilan Menu *Load Data for Current Connection*

Dari menu ini, maka user baru bisa memilih menu *Encrypt, Decrypt* dan *Generate*. Sebelum memilih *Encrypt*, user harus menentukan dulu nilai Cn (nilai pergeseran karakter). Berdasarkan nilai Cn inilah data akan dienkrip dengan cara menggeser karakter tersebut sebanyak n karakter.

Hasil dari enkripsi bisa dilihat di gambar berikut ini:

cDepartmentCode	vDepartmentName	vDepartmentHead	vLocation
0001	Production	Samuel Moore	New York
0002	Sales	Donald Fleming	Houston
0003	Marketing	Sandra Hawkins	Addison
0004	Human Resource	Bill Mayse	Abilene
0005	Quality Assurance	Robin Dmello	Hampstead
0007	Training	Will Smith	Columbus
0008	Transportation	Dabb Mike	Columbus
0009	Finance	Faber Michel	New Jersy
0010	Inventory	Taber James	New Jersy

Gambar 5. Sebelum Dienkripsi



	cDepartmentCode	vDepartmentName	vDepartmentHead	vLocation
▶	<<<=	\~{pou{z	_myqx,Y{{~q	Zq,e{~w
	<<<>	_mxq	P{zmxp,Rxqyuzs	T{
	<<<?	Ym~wquzs	_mzp~m,Tmwuz	Mppu{z
	<<<@	Tymz,^q{~oq	Nuxx,Ym	Mnuxqzq
	<<<A	]mxu,M~mzoq	^{nuz,Pyqxx{	Tmy qmp
	<<<C	`~muzuzs	cuxx,_yut	O{xyn
	<<<D	`~mz{~mu{z	Pmnn,Yuwq	O{xyn
	<<<E	Ruzmzoq	Rmnq~,Yuotqx	Zq,Vq~
	<<=<	Uzqz{~	`mnq~,Vmvq	Zq,Vq~

Gambar 6. Setelah Dienkripsi dengan Cn=12

Tabel yang telah dienkripsi bisa dipertukarkan ke aplikasi lain yang membutuhkan tabel tersebut. Supaya tabel bisa dibaca oleh aplikasi dengan platform yang berbeda, maka pada aplikasi ini menyediakan menu untuk men-generate ke dalam format XML.

3. Kesimpulan

Dari penelitian yang telah dilakukan, didapatkan kesimpulan:

a. Penelitian ini menghasilkan sebuah perangkat lunak aplikasi pemanfaatan metode *symmetric encryption substitution cipher.*
b. Aplikasi metode *symmetric encryption substitution cipher* bisa digunakan untuk mengenkripsi 3 jenis database, yaitu: SQL Server 2005 (*SQL Server* 9.0.1399), *Microsoft Access* 2003 dan *Oracle Database 10g*.
c. Proses enkripsi dapat dilakukan berulang-ulang dengan key yang berbeda-beda sesuai nilai Cn.
d. Hasil enkripsi bisa digenerate ke dalam format XML atau XSD tanpa mengubah data sumbernya.

Daftar Rujukan

Kelompok 124 IKI-83408 MTI UI. 2005. *Cryptography*, http://bebas.vlsm.org/v06/Kuliah/MTI-Keamanan-Sistem-Informasi/2005/124/124P-04-draft-Cryptography.pdf. Diakses Tanggal 20 Nopember 2010.

Munir, R, 2006, *Kriptografi***,** Penerbit Informatika, Bandung

NIIT, 2009, *Introduction to Web Content Development***,** NIIT, India

Prasetyo, D. D, 2006, *Pemgrograman Aplikasi Database Vb.net 2005* + *Cd*, Elex Media Komputindo, Jakarta

Rahardjo, B, 2002, *Keamanan Sistem informasi Berbasis Internet***,** PT. Insan Komunikasi Indonesia, Bandung

Suryana, Aulya dkk, 2007, *Enkripsi***,** Sekolah Tinggi Manajemen Informatika Dan Teknik Komputer (STMIK), STIKOM, Bali