Keamanan Database Pada Sistem Informasi Layanan dan Pengaduan Dinas Pendidikan Provinsi Sumatera Selatan

Pandu Ridho Ekananda[1], Jemakmun[2], Andri[3]
Teknik informatika, fakultas ilmu computer Universitas Bina Darma
email : pandu.ridho96@gmail.com[1] jemakmun@binadarma.ac.id[2] , andrepro2007@gmail.com[3]

ABSTRAK

Dinas Pendidikan Provisi Sumatera Selatan merupakan bagian dari pemerintahan yang berfokus pada pendidikan khususnya sumatera selatan. Saat ini Dinas Pendidikan Provinsi Sumatera Selatan sedang membangun Sistem Informasi Layanan dan Pengaduan. Penelitian ini bertujuan untuk meningkatkan sistem keamanan *database* pada Sistem Informasi Layanan dan Pengaduan yang sedang di kembangkan oleh Dinas Pendidikan Provinsi Sumatera Selatan menggunakan metode Algoritma RC4 dalam menjaga kerahasiaan data dan kebocoran data baik dari pihak *ekternal* maupun pihak *internal*. Dengan menggunakan metode Algoritma RC4 diharapkan dapat menjaga kerahasiaan data dan meminimalisir tingkat kebocoran data.data yang digunakan merupakan data yang telah disediakan oleh Dinas Pendidikan Provinsi Sumatera Selatan berupa *database* kantor

***Kata Kunci**: Rc4, Keamanan, Database, Dinas Pendidikan Provinsi Sumatera Selatan*

ABSTRACT

The Education Office of the Provision of South Sumatra is part of a government that focuses on education especially in southern Sumatra. At present the South Sumatra Provincial Education Office is building a Complaint and Service Information System. This study aims to improve the database security system in the Service and Complaints Information System which is being developed by the Education Office of South Sumatra Province using the RC4 Algorithm method in maintaining data confidentiality and data leakage from both external and internal parties. By using the RC4 Algorithm method, it is expected to maintain the confidentiality of data and minimize the level of data leakage. Data used is data that has been provided by the Education Office of South Sumatra Province in the form of office databases.

Keywords: Rc4, Security, databases, Education Office of South sumatra Province

1. PENDAHULUAN

Pada era modern ini, hampir seluruh instansi, perusahaan, dan perkantoran telah menerapkan penggunaan sistem basis data dalam mengolah dan menyimpan informasiuntuk mendapatkan informasi dan layanan yang berguna bagi orang maupun organisasi yang membutuhkan.

Database telah lama menjadi bagian integral dari sistem dalam menjalankan bisnis, baik dalam bentuk awalnya, yaitu *file database* biasa maupun dalam bentuk sekarang ini, yaitu database berorientasi pada tingkat lanjut.

Dalam penelitian yang dilakukan oleh Jumrin, dengan judul "Aplikasi Sistem Keamanan Basis Data dengan Teknik Kriptografi RC4 *Stream Cipher*" menjelaskan Kebutuhan atas menyimpan dan mengakses informasi secara cepat menjadi hal-hal yang mendesak bagi tiap kalangan yang membutuhkan informasi, begitu pula web. Aplikasi - aplikasi web sekarang ini berpasangan dengan *database* [3]. Database yang dipakai untuk beragam kegunaan mulai dari menyimpan nama *user* dan *password*, sampai data pribadi orang. Oleh karena itu, pemahaman menyeluruh mengenai keamanan database pada sistem informasi harus mencakup juga lapisan databasenya dan

terpenting memahami juga bagaimana penyusup berusaha memasuki aplikasi untuk berusaha memperoleh akses kebagian-bagian yang dirahasiakan datanya.

Saat ini, keamanan *database* terhadap data di Dinas Pendidikan Provinsi Sumatera Selatan yang disimpan dalam basis data sudah menjadi persyaratan mutlak. Namun, bukan berarti data-data tersebut aman dari kebocoran informasi.

Dan ini juga di jelaskan pada penilitian yang dilakukan oleh Arifyanto dengan judul "Implementasi enkripsi basis data berbasis web dengan algoritma *stream chiper* RC4" Pengamanan terhadap jaringan komputer yang terhubung dengan *database* sudah tidak lagi menjamin keamanan data karena kebocoran data dapat disebabkan oleh "orang dalam" atau pihak-pihak yang langsung berkaitan dengan *database* seperti administrator *database*. Pentingnya enkripsi dan dekripsi dalam pengaduan agar tidak terbaca oleh siapapun agar menjadi rahasia bagi pemerintahan yang terkait dan siapa yang mengadu[1]. Terlebih lagi sistem informasi layanan dan pengaduan pada dinas pendidikan sumatera selatan ini masih dalam proses perkembangan jadi sangat dibutuhkan sekali pengamanan data yang baik.

Diperlukan adanya suatu sistem yang dapat membatasi hak akses maupun mengamankan informasi yang terkandung dalam data tersebut tanpacampur tangan administrator basis data. Untuk mengatasi masalah tersebut maka perlunya dibuat sistem keamanan *database* yang kuat dengan menggunakan metode *enkripsi sitematis* dalam *secure login* aplikasi tersebut sebagai salah satu cara dalam mengamankan *database*. Adapun algoritma yang dipakai dalam metode enkripsi ini adalah Algoritma *Stream Cipher RC4*. Dengan adanya sistem keamanan *database* ini, diharapkan keamanan *database* pada sistem informasi Diknas Pendidikan Provinsi Sumatera Selatan dapat mengamankan secara optimal dan terjamin kerahasiaanya.

2. METODOLOGI PENELITIAN

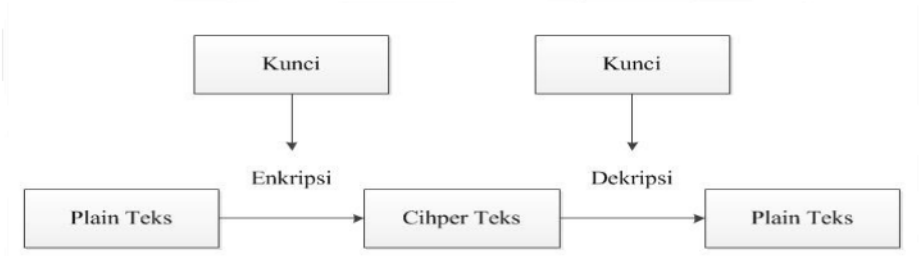
2.1 Keamanan Database

Keamanan *database* adalah suatu cara untuk melindungi *database* dari ancaman, baik dalam bentuk kesengajaan atau pun bukan. Ancaman adalah segala situasi atau kejadian baik secara sengaja maupun tidak yang bersifat merugikan dan mempengaruhi system serta secara konsekuensi terhadap perusahaan/organisasi yang memiliki system *database*. Keamanan *database* tidak hanya berkenaan dengan data yang ada pada *database* saja, tetapi juga meliputi bagian lain dari system *database,* yang tentunya dapat mempengaruhi *database* tersebut. Hal ini berarti keamanan *database* mencakup perangkat keras, perangkat lunak, orang dan data[3].

2.2 Kriptografi

Menurut Munir (2008), Kriptografi (*cryptography*) berasal dari bahasa Yunani: "*cryptos*" yang artinya "*secret*" (rahasia) dan "*graphein*" yang artinya "*writing*" (tulisan). Jadi kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan (*cryptography is the art andscience of keeping message secure*)[6].

Menurut Mollin (2007), proses kriptografi pada dasarnya sangat sederhana. Sebuah *plaintext* (m) akan dilewatkanpada proses enkripsi (E) sehingga menghasilkan suatu *ciphertext* (c). Kemudianuntuk memperoleh kembali *plaintext*, maka *ciphertext* (c) melalui proses dekripsi (D) yang akan menghasilkan kembali *plaintext* (m). Kriptografi modern selain memanfaatkan algoritma juga menggunakan kunci (*key*) untuk memecahkan masalah tersebut dengan (e)= kunci enkripsi dan (d) = kunci dekripsi. Mekanisme kriptografi seperti ini dinamakan kriptografi berbasis kunci[4]. Dengan demikian kriptosistemnya akan terdiri atas algoritma dan kunci, beserta segala *plaintext* dan *ciphertext*-nya. Proses enkripsi dan dekripsi dilakukan dengan menggunakan kunci ini seperti pada gambar berikut.



Gambar 1 Kriptografi Berbasis Kunci[4]

2.3 Algoritma RC4

Algoritma kriptografi Rivest Code 4 (RC4) ialah salah satu algoritma kunci simetris dibuat oleh RSA Data Security Inc (RSADSI) yang berbentuk stream chipper. Algoritma ini ditemukan pada tahun 1987 oleh Ronald Rivest dan menjadi simbol keamanan RSA (merupakan singkatan dari tiga nama penemu : Rivest Shamir Adleman). RC4 mempunyai panjang kunci dari 1 sampai 256 byte yang digunakan untuk menginisialisasikan tabel sepanjang 256 byte. Tabel ini digunakan untuk generasi yang berikut dari pseudo random yang menggunakan XOR dengan plainteks untuk menghasilkan cipherteks. Masing-masing elemen dalam tabel saling ditukarkan minimal sekali. Dan untuk merubahmenjadi plaintext semula, maka ciphertext nya akan dikenakan operasi XOR terhadap pseudo random bytenya[6].

2.4 Langkah – langkah Algoritma RC4

RC4 mempunyai sebuah S-Box, S0, S1,…, S255 yang berisi permutasi dari bilangan 0 sampai 255, dan permutasi merupakan fungsi dari kunci K dengan panjang yang variable[7].

1. Inisialisasi S-Box
   a. Isi S-Box secara berurutan, yaitu S0=0,S1=1,…, S255=255.
   b. Lakukan padding kunci K sehingga panjang kunci K = 256.
   c. Lakukan pertukaran dan pengisian pada S-Box dengan kunci K, sebagai berikut :

   j = 0
   for i = 0 to 255
   j = (j + Si + Ki) mod 256
   swap Si dan Sj

   Fungsi swap merupakan fungsi yang menukarkan nilai S ke-i dengan nilai S ke-j.
2. Proses enkripsi atau dekripsi RC4

   i = 0
   j = 0
   for idx = 0 to len-1
   i = (i + 1) mod 256
   j = (j+ Si) mod 256
   swap Si dan Sj
   t = (Si + Sj) mod 256
   k = St
   buffidx = k XOR buffidx

   Keterangan :

   1.Buff merupakan pesan yang akan dienkripsi atau dekripsi
   Len merupakan panjang dari buff yang berisi pesan yang telah dienkripsi atau dekripsi.

2.5 Metode Pengembangan Sistem

Dalam penelitian ini metode pengembangan sistem yang digunakan adalah Metode *Waterfall* (air terjun) merupakan metode pengembangan sistem perangkat lunak dengan menerapkan tahapan – tahapan dari model *Waterfall* (Air Terjun), Yaitu : Komunikasi, Perancangan, Pemodelan, dan penyerahan sistem/perangkat lunak ke pelanggan/pengguna[12].

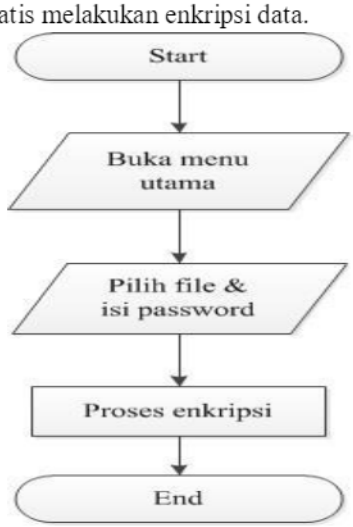
Menurut Roger S. Pressman (2012:46) Waterfall Model kadang dinamakan siklus *hidup klasik* (Class Life Cyle), dimana hal ini menyiratkan pendekatan yang sistematis dan berurutan (sekuensial) pada pengembangan perangkat lunak, yang dimulai dengan spesifikasi kebutuhan pengguna dan berlanjut melalui tahapan – tahapan perancangan (Planning), pemodelan (Modeling), konstruksi (Construction), serta penyerahan sistem perangkat lunak ke para pelanggan /pengguna (Deployment), yang akhirnya dengan dukungan berkelanjutan pada perangkat lunak yang lengkap yang dihasilkan.

Menurut Kadir (2003), Secara garis besar metode *waterfall* mempunyai langkah-langkah sebagai berikut : Analisa, Desain, Penulisan, Pengujian dan Penerapan serta Pemeliharaan[5].

2.6 Flowchart Enkripsi Program

Flowchart Enkripsi program merupakan rancangan tahapan proses enkripsi pada sistem yang akan dibuat. Berikut ini adalah desain rancangan flowchart enkripsi program.

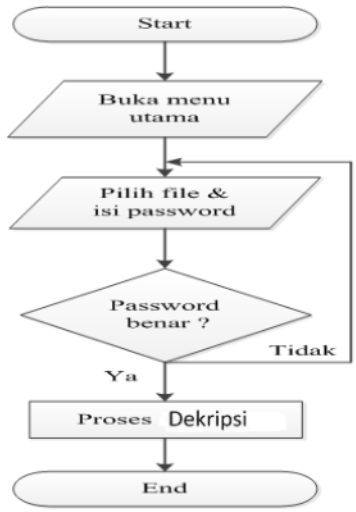
dimulai dengan membuka menu utama, kemudian memilih *file/database* yang akan di enkripsi dan memberikan *password* untuk dilakukan peng-enkripsi-an, setelah pengisian *password* selesai maka program akan secara otomatis melakukan enkripsi data.



Gambar 1 Flowchart Enkripsi Program

2.7 Flowchart Dekripsi Program

Flowchart Dekripsi program merupakan rancangan tahapan proses dekripsi pada sistem yang telah ter-enkripsi sebelumnya. Berikut ini adalah desain flowchart dekripsi program.



Gambar 2 Flowchar Dekripsi Program

dimulai dengan membuka menu utama, setelah itu memilih *file/database* yang telah ter-enkripsi sebelumnya dan memasukkan ulang *password* yang sudah terbuat sebelumnya, jika *password* benar maka akan lanjut ke proses pen-dekripsi-an data yang dilakukan program secara otomatis, jika password salah maka akan kembali ke menu pilih file dan memasukkan *password* yang benar.

3 . HASIL DAN PEMBAHASAN

Metode Enkripsi Dekripsi dengan menggunakan algoritma RC4 diterapkan dalam membangun sistem keamanan database pada sistem informasi dinas pendidikan provinsi sumatera selatan yang dapat meningkatkan keamanan database tersebut.

Hasil dari enkripsi/dekripsi akan ditampilkan pada sistem keamanan Database pada sistem Informasi Dinas Pendidikan Provinsi Sumatera Selatan. Berikut dibutuhkan perangkat keras (*Hardware*) dan perangkat lunak (*Software*).

1. Perangkat Keras (*Hardware*)

Spesifikasi perangkat keras yang digunakan dalam membuat Sistem keamana *database* pada sistem Informasi Dinas Pendidikan Provinsi Sumatera Selatan sebagai berikut :

a. Intel® celeron® Processor N2840
b. HDD 500 GB
c. Memory 2 GB DDR3 L

2. Perangkat Lunak (*Software*)

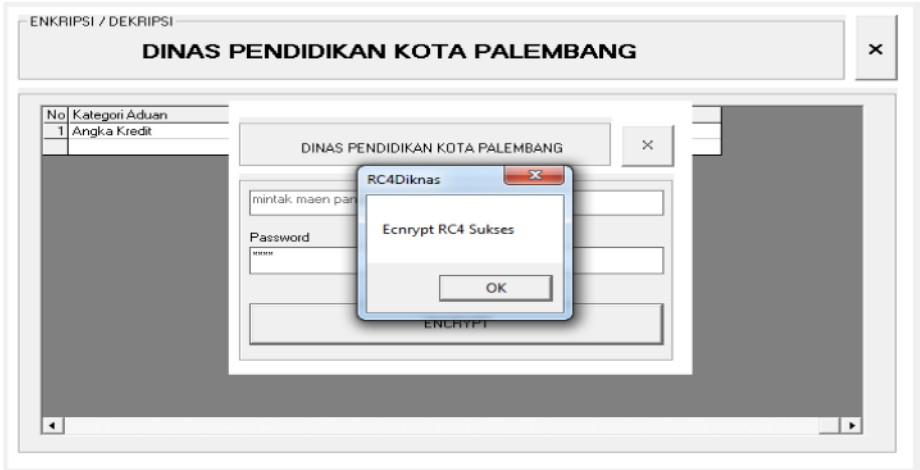
Adapun beberapan *Software* yang dibutuhkan untuk membuat sistem keamanan *database* pada Sistem Informasi Dinas Pendidikan Provinsi Sumatera Selatan adalah sebagai berikut :

a. Sistem Operasi Windows 7
b. Microsoft office
c. MySQL
d. PHP
e. Xampp
f. Visual Basic 6.0

3.1 Pengujian Aplikasi

1. Pengujian Enkripsi Teks

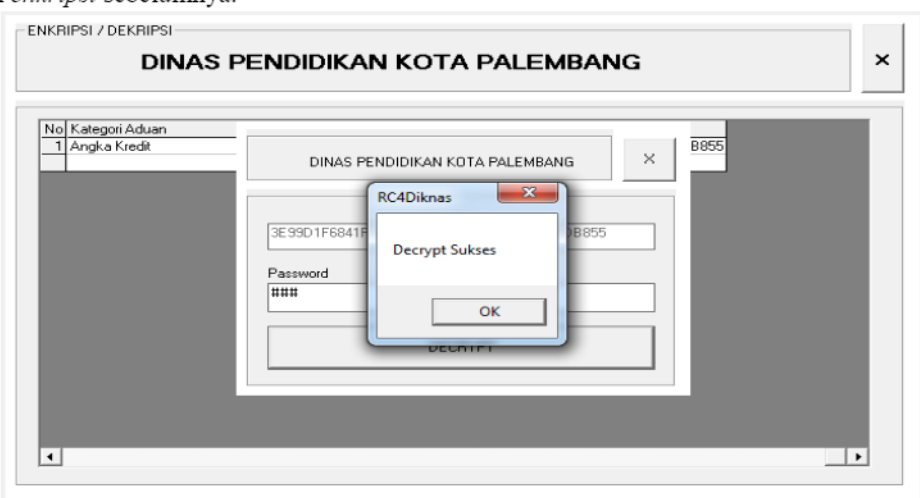
Pengujian enkripsi pertama berupa pengenkripsian *teks*, pertama klik *RC4 Cloumn* Pengaduan, dan kemudian masukkan *password,* kemudian klik ENCRYPT.



Gambar 3 Pengujian Enkripsi Teks

2. Pengujian Dekripsi Teks

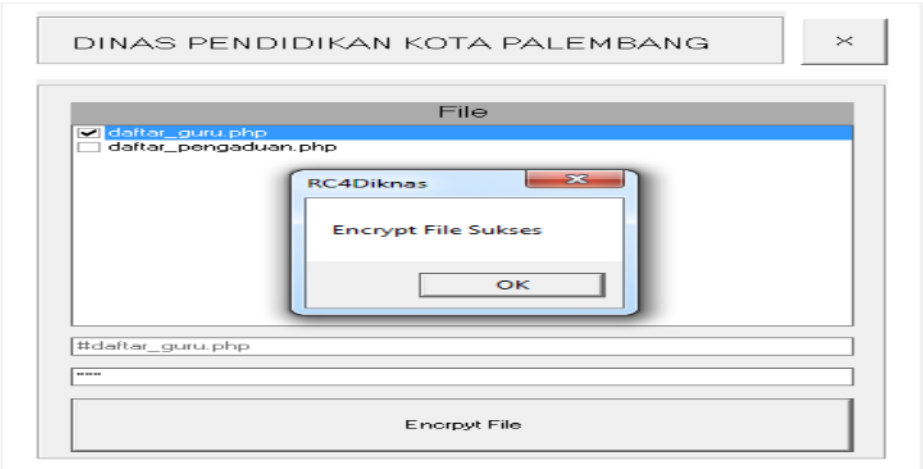
Setelah *teks* terenkripsi maka *teks* berubah menjadi *teks* yang tidak dapat dibaca. *Dekripsiteks* ini bertujuan untuk mengembalikan *teks* yang telah terenkripsi sebelumnya agar dapat dibaca dengan cara yang sama seperti pengenkripsian sebelumnya dan memasukkan *password* yang sama seperti *enkripsi* sebelumnya.



Gambar 4 Pengujian Dekripsi Teks

3. Pengujian Enkripsi File

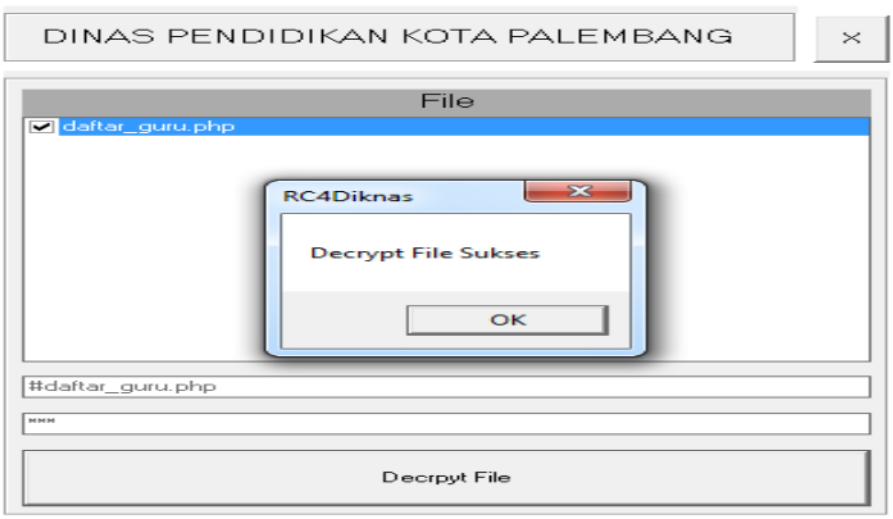
Pengujian *enkripsi file* ini bertujuan untuk melindungi *file* agar tidak dapat terbaca oleh siapapun terdapat *file* penting yang harus di *enkripsi* sebagai contoh penulis membuat dua *file* yaitu *daftar_guru.php* dan *daftar_pengaduan.php*. Cara pengenkripsiannya sama seperti pengenkripsian *teks* yang telah dijelaskan sebelumnya. Pertama klik *RC4 Laporan* dan kemudian klik *encryptFile*, pilih file akan di *enkripsi* dan masukkan *password.*



Gambar 5 Pengujian Enkripsi File

1. Pengujian Dekripsi File

Pengujian dekripsi *file* adalah mengembalikan *file* yang telah terenkripsi sebelumnya agar dapat terbaca lagi setelah pengenkripsian.*file* yang telah di *enkripsi* sebelumnya akan berpindah ke menu *Decrypt File.*Proses *dekripsi file* sama seperti *enkripsi file* sebelumnya dan memasukkan password yang sama dengan *enkrispsi* sebelumnnya.



Gambar 6 Pengujian Dekripsi File

4 . KESIMPULAN

Berdasarkan hasil dan pembahasan yang membahas tentang Keamanan Database pada Sistem Informasi Dinas Pendidikan Provinsi Sumatera Selatan pada bab sebelumnya, penulis mendapatkan beberapa kesimpulan sebagai berikut:

1. Data yang di input akan di simpan pada database dalam keadaan terenkripsi sehingga keamanan dan kerahasiaan datanya dapat terjaga.
2. Algoritma RC4 *stream Cipher* dapat diimplementasikan untuk merubah *file* basis data asli dalam bentuk *file* basis data terenkripsi yang hasil akhirnya dikonversi dalam bentuk *hexadecimal*.

3. Teknik Enkripsi Dekripsi dapat menjaga keamanan data pada sistem Informasi dinas pendidikan provinsi sumatera selatan.
4. Enkripsi *RC4 Stream Cipher* ini dapat diimplementasikan pada Aplikasi dengan menggunakan bahasa pemrograman visual basic 6.0 dan database Mysql.

DAFTAR PUSTAKA

[1] Arifyanto A.E. 2013. *Implementasi Enkripsi Basis Data Berbasis Web Dengan Algoritma Stream Cipher RC4.* Dokumen Karya Ilmiah Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Dian Nuswantoro Semarang.

[2] Haji W.H, Mulyono S. 2012. *Implementasi RC4 Stream Cipher Untuk Keamanan Basis Data.* Universitas Mercu Buana Jakarta. Seminar SNATI 2012

[3] Jumrin, Sutardi, Subardin. 2016. *Aplikasi Sistem Keamanan Basis Data Dengan Menggunakan Teknik Kriptografi RC4 Stream Cipher*. Universitas Halu Oleo. Jurnal semanTIK . Vol 2, No 1.

[4] Mollin, R. A. 2007. *An Introduction to Cryptography*. 2nd ed. Florida: Chapman&Hall/CRC..

[5] Munir, Rinaldi. 2006. *Diktat Kuliah Kriptografi*. Bandung. Program Studi Tenik Informatika, Institut Teknologi Bandung.

[6] Munir, Rinaldi. 2008. *Belajar Ilmu Kriptografi*. Yogyakarta. Penerbit Andi..

[7] Munir, Rinaldi. 2011. *Kriptografi Keamanan*. Bandung. Informatika Bandung.

[8] Riyanto. 2011. *Membuat Sendiri Aplikasi E-Commerce dengan PHP & MySQLMenggunakan CodeIgneter &JQuery*. Yogyakarta: Pener*bit* Andi.

[9] Saputra Y.R.*Keamanan Sistem Database*diakses dari https://www.academia.edu/7612178/KEAMANAN_SISTEM_DATABASE pada tanggal 21 maret 2018..

[10] Saragih U.S. 2017. *Implementasi Enkripsidan Dekripsi Dengan Metode RC4 Untuk Pengamanan Data Sistem Informasi*, Bandar Lampung. Skripsi. Hal. 52-54.

[11] Sutarman. 2012. *Pengantar Teknologi Informasi*. Jakarta: PT. Bumi Aksara.

[12] Yasin, Verdi. 2012. *Rekayasa Perangkat Lunak Berorientasi Objek*. Jakarta: Mitra Wacana Media.