KRIPTOGRAFI *DATABASE* MENGGUNAKAN ALGORITMA EL-GAMAL BERBASIS *WEB*

Fajar Ibnu Wicaksana[1)], **Ir. Siswanto, M.M**[2)]
Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Raya Ciledug, Pertukangan Utara Kebayoran Lama, Jakarta Selatan 12260
Telp. (021) 5853753, Fax. (021) 5866369
E-mail : dare631@gmail.com[1)] , *Siswanto@budiluhur.ac.id*[2)]

ABSTRAK

Perkembangan teknologi informasi dan telekomunikasi saat ini berkembang dengan sangat pesat berpengaruh pada penggunaan informasi data. Dimana, kemampuan untuk mengaskses dan menyediakan informasi secara cepat dan akurat menjadi efektif bagi sebuah perusahaan. Adapun dampak positif, yaitu dengan semakin canggihnya teknologi, maka dapat memudahkan seseorang untuk berinteraksi dan memudahkan pekerjaan sehingga lebih efekif dan efisien. Adapun dampak negatifnya dengan berkembangnya teknologi, yaitu dapat di pastikan semakin berkembangnya teknologi maka semakin berkembangnya pula kejahatan di dunia teknologi informasi. Masalah keamanan dan kerahasian database merupakan suatu hal yang sangat penting di dalam menjaga kerahasiaan informasi terutama yang berisi informasi database yang hanya boleh di ketahui isinya oleh pihak yang berhak saja. Untuk mengatasi keamanan data tersebut maka diperlukan cara untuk mengamankan informasi data tersebut agar tidak dapat di salah gunakan. Salah satu cara yang dapat digunakan untuk keamanan data adalah dengan menggunakan teknik kriptografi. Metode yang akan digunakan adalah algoritma El Gamal yang akan diimplementasikan pada aplikasi kriptografi berbasis web untuk mengamankan informasi database di PT. Berdikari Pondasi Perkasa.

Kata Kunci : Enkripsi dan Dekripsi, Database, El Gamal, PT. Berdikari Pondasi Perkasa.xii+58 halaman; 79 gambar; 6 tabel; 1 Lampiran.

1. PENDAHULUAN

1.1 Latar Belakang

PT. Berdikari Pondasi Perkasa terletak di Jl. P. Tubagus Angke No. 99 Jakarta. Didirikan pada tahun 1984 dengan spesialisasi di bidang pondasi, perbaikan tanah, konstruksi dermaga, lift berat dan penyewaan crane. PT. Berdikari Pondasi Perkasa didirikan oleh John Tanuwijaya yang merupakan direktur pelaksana pada saat ini. PT. Berdikari Pondasi Perkasa ini merupakan perusahaan terdepan di Indonesia dalam semua kompetensi inti yang telah disebutkan sebelumnya. PT. Berdikari Pondasi Perkasa berkomitmen penuh terhadap Quality and Helth Safety and Environment (QHSE). Tujuan dari PT. Berdikari Pondasi Perkasa adalah menciptakan tempat kerja bebas kecelakaan dan kejadian dimana kami bisa memberikan pekerjaan berkualitas tinggi, tepat waktu dan sesuai anggaran kepada client.Database secara umum merupakan susunan record data operasional lengkap dari suatu organisasi atau perusahaan, yang diorganisir dan disimpan di dalam media penyimpanan secara terintegrasi yang dapat dijadikan sebagai salah satu sumber dari setiap sistem informasi yang sedang berjalan sehingga mampu memenuhi informasi yang optimal yang dibutuhkan oleh para pengguna. Dengan adanya database, maka proses pemutakhiran informasi dapat dilakukan. Database dapat dibuat dengan menggunakan software yang ada seperti Microsoft SQL Server, Oracle, MySQL, Microsoft Access, dBase III, Paradox, FoxPro, dan lain-lain. Selanjutnya database dimaksud dapat diintegrasikan dengan aplikasi yang dibuat untuk melakukan beberapa operasi DBMS (Database Management System).Sering sekali record yang tersimpan di dalam database masih persis sama dengan teks-teks yang ditampilkan sebagai informasi akhir bagi pengguna. Serta untuk keamanan database itu sendiri belum maksimal dikarenakan tidak adanya password yang digunakan untuk database tersebut. Hal ini dapat mempermudah seorang kriptanalis maupun orang lain yang tidak mempunyai hak akses untuk dapat mengetahui secara langsung isi dari database tersebut serta dapat memberi peluang kepada mereka untuk melakukan pembocoran, mendistribusikan maupun melakukan modifikasi lain terhadap record database tersebut.

2. METODE PENELITIAN

Pada Penelitian ini dirancang sebuah sistem aplikasi berbasis web dengan menggunakan bahasa pemograman php, pada PT. Berdikari Pondasi Perkasa yang bergerak bidang pondasi, perbaikan tanah, konstruksi dermaga, lift berat dan penyewaan crane. Dengan melakukan metode enkripsi – dekripsi pada database menggunakan algoritma asimetris yaitu El-Gamal. Langkah-langkah yang di lakukan yaitu:

1) Tinjauan Lapangan *(Field Research)*

Penulisan dan Pengumpulan data yang di peroleh dari hasil penelitian yang telah di lakukan pada PT Berdikari Pondasi Perkasa antara lain :

a) Pengamatan (*Observation*)
   Proses Pengamatan akan dilakasanakan dengan cara mengamati secara langsung pertukaran data pada PT. Berdikari Pondasi Perkasa.
b) Wawancara (*Interview*)
   Kegiatan wawancara akan di laksanakan dengan cara mengajukan beberapa pertanyaan secara rinci pada bagian yang terkait dalam system penyimpanan data.

2) Penelitian Kepustakaan (*Library Research*)
   Penulis juga menggunakan sumber sumber bacaan baik buku maupun *e-book* hasil pencarian di *internet* dan cacatan perkuliahan yang berhubungan dengan penelitian ini.

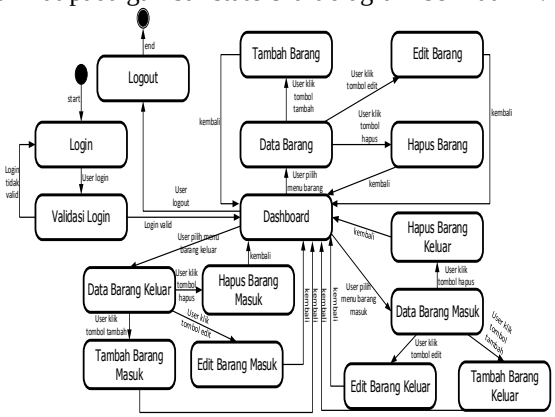
3. PEMBAHASAN

Permasalahan yang dihadapi oleh perusahaan yang menggunakan database adalah kurang terjaminnya kerahasiaan sebuah data yang tersimpan dalam database. Karena data yang tersimpan dalam database pun masih dapat di ambil oleh pihak lain yang tidak bertanggung jawab.Berdasarkan masalah tersebut, maka dibuatlah suatu aplikasi yang dapat melakukan proses enkripsi dan dekripsi ketika menyimpan data ke dalam database, agar setiap data yang tersimpan dapat terjaga kerahasiaan dan integritasnya. Proses enkripsi yaitu suatu proses melakukan perubahan bentuk suatu naskah dari yang bisa dimengerti menjadi tidak bisa dimengerti oleh manusia. Sedangkan proses dekripsi adalah suatu proses mengembalikan bentuk naskah yang sudah mengalami suatu proses enkripsi kedalam bentuk aslinya sehingga dapat dimengerti kembali.Pembuatan aplikasi ini diharapkan dapat menjadi solusi untuk menjamin kerahasian data dalam suatu database.

a. Rancangan *Unified Modelling Language* (UML)

Di dalam menggambarkan urutan proses pada aplikasi ini, digunakan Unified Modelling Language (UML) untuk memperjelas aliran proses, UML dibawah ini merupakan activity diagram yang menjabarkan cara kerja program untuk menjalankan proses dalam program. Di bawah ini akan digambarkan UML masing-masing proses.

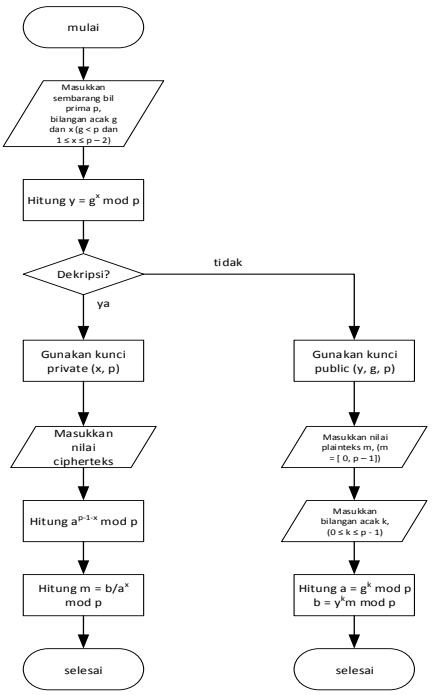
Pada Statechart Diagram Aplikasi Enkripsi El-Gamal menjelaskan tentang bagaimana proses yang terjadi dalam aplikasi yang dibuat. Dimulai dari login, lalu terdapat validasi login. Bila validasi gagal maka akan kembali ke login, jika validasi berhasil maka akan menuju dashboard aplikasi. Dari dashboard user bisa memilih data barang, data barang masuk, data barang keluar. Pada data barang user bisa memilih tambah barang, edit barang, hapus barang. Setelah selesai maka akan kembali ke dashboard. Pada data barang masuk, user bisa tambah barang masuk, edit barang masuk, hapus barang masuk. Setelah selesai maka akan kembali ke dashboard. Pada data barang keluar, user bisa tambah barang keluar, edit barang keluar, hapus barang keluar. Setelah selesai makan akan kembali ke dashboard. Statechart diagram aplikasi dapat dilihat pada gambar state chart diagram berikut ini :



Gambar 1. Statechart Diagram Kriptografi El-Gamal

b. Flowchart Algoritma El-Gamal

Flowchart Proses Enkripsi AlgoritmaEl-Gamal :

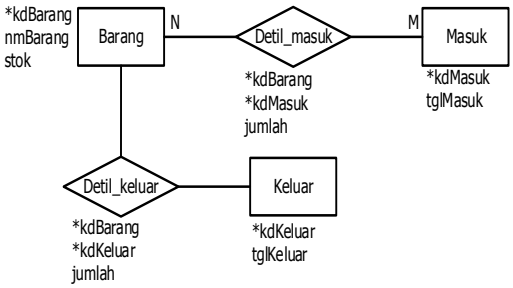


Gambar 2 *flowchart* proses algoritma El-Gamal

c. Rancangan Basis Data

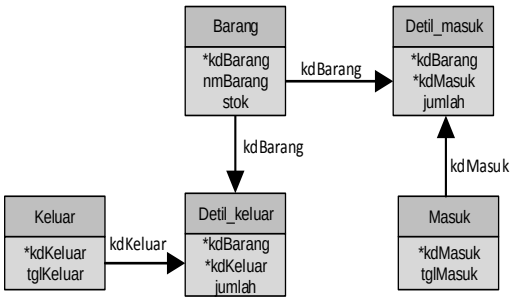
Berikut ini adalah struktur-struktur tabel yang digunakan dalam pembuatan aplikasi ini:

1) *Entity Relationship Diagram* (ERD)



Gambar 3. *Entity Relationship Diagram*

2) *Logical Relational Structure* (LRS)



Gambar 4. *Logical Relational Structure*

3) *Spesifikasi* Basis Data

a) Tabel*User*

Nama Tabel : user
Isi : data*user*
Media : *Harddisk*
PrimaryKey : username

Tabel 1 Spesifikasi Tabel *User*

Nama Field	Type	Lebar	Keterangan
username	Varchar	50	*Username* untuk login
password	Text	50	*Password* untuk login
tglLahir	Date	10	Tanggal Lahir *User*
noTelp	Varchar	50	No Telp *User*
mobile	Varchar	50	No Mobile *User*
email	Varchar	50	*Email User*

b) Tabel Barang

Nama Tabel : Barang
Isi : berisidata barang
Media : *Harddisk*
PrimaryKey : kdBarang

Tabel Spesifikasi Tabel *Barang*

Nama Field	Type	Lebar	Keterangan
kdBarang	Text	5	Kode Barang
nmBarang	Text	50	Nama Barang
stok	integer	5	Stok barang

c) TabelMasuk

Nama Tabel : Masuk
Isi : berisidata*barang masuk*
Media : *Harddisk*
PrimaryKey : kdMasuk

Tabel Spesifikasi Tabel Masuk

Nama Field	Type	Lebar	Keterangan
kdMasuk	Text	5	Kode Masuk
tglMasuk	Date	10	Tanggal Masuk

d) TabelKeluar

Nama Tabel : Keluar
Isi : berisidata*barang keluar*
Media : *Harddisk*
PrimaryKey : kdKeluar

Tabel Spesifikasi Tabel Keluar

Nama Field	Type	Lebar	Keterangan
kdKeluar	Text	5	Kode Keluar
tglKeluar	Date	10	Tanggal Keluar

e) Tabel Detil_masuk

Nama Tabel : Detil_masuk
Isi : berisidata detilbarang masuk
Media : *Harddisk*
PrimaryKey : kdBarang, kdMasuk

Tabel Spesifikasi Tabel Detil_masuk

Nama Field	Type	Lebar	Keterangan
kdBarang	Text	5	Kode Barang
kdMasuk	Text	5	Kode Masuk
Jumlah	integer	5	Jumlah Barang Masuk

f) Tabel Detil_keluar

Nama Tabel : Detil_keluar
Isi : berisidata detilbarang keluar
Media : *Harddisk*
PrimaryKey : kdBarang, kdKeluar

Tabel Spesifikasi Tabel Detil_keluar

Nama Field	Type	Lebar	Keterangan
kdBarang	Text	5	Kode Barang
kdKeluar	Text	5	Kode Keluar
Jumlah	integer	5	Jumlah Barang Keluar

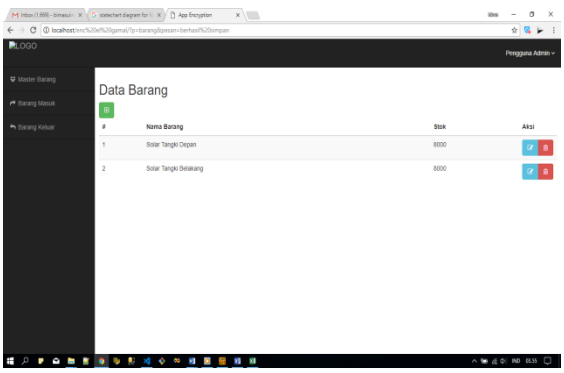
4. HASIL PENGUJIAN

Pengujian Program

Pada bagian ini dapat diuraikan mengenai pengujian enkripsi, dekripsi database. Pengujian tersebut akan mengamankan data di dalam database.

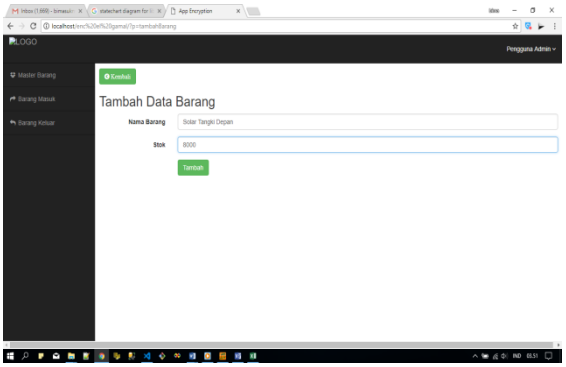
a) Tampilan Menu Data Barang

Berikut ini adalah tampilan menu data barang



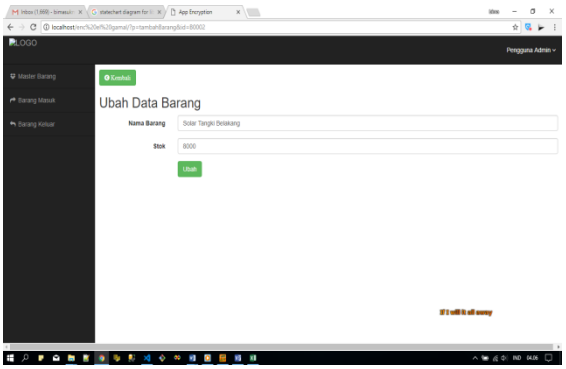
Gambar 5. Tampilan Menu Data Barang

b) Tampilan Menu Tambah Data Barang
Berikut ini adalah tampilan menu tambah data barang



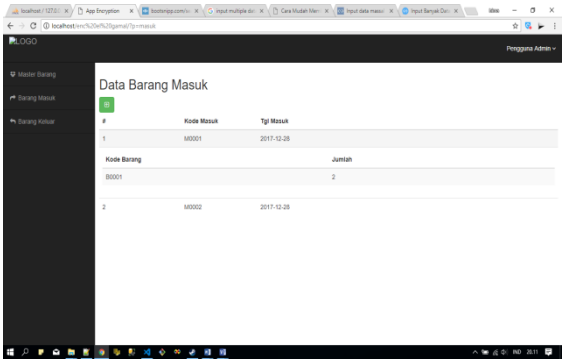
Gambar 6. Tampilan Menu Tambah Data Barang

c) Tampilan Menu Ubah Data Barang
Berikut ini adalah tampilan menu ubah data barang



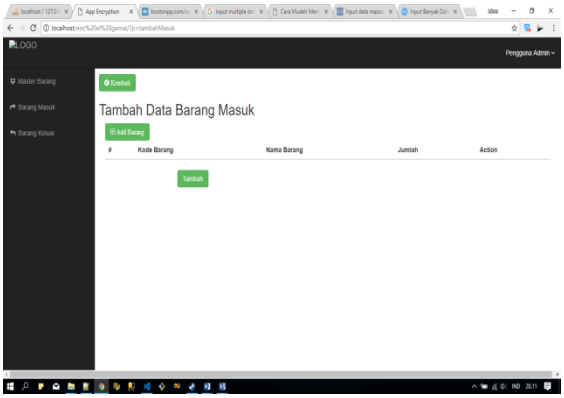
Gambar 7. Tampilan Menu Ubah Data Barang

d) Tampilan Menu Data Barang Masuk
Berikut ini adalah tampilan menu data barang masuk



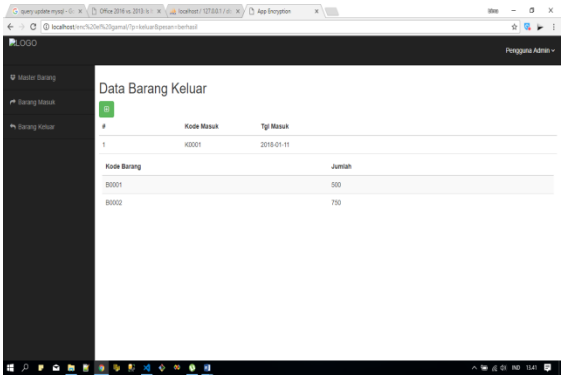
Gambar 8. Tampilan Menu Data Barang Masuk

e) Tampilan Menu Tambah Barang Masuk
Berikut ini adalah tampilan menu tambahdata barang



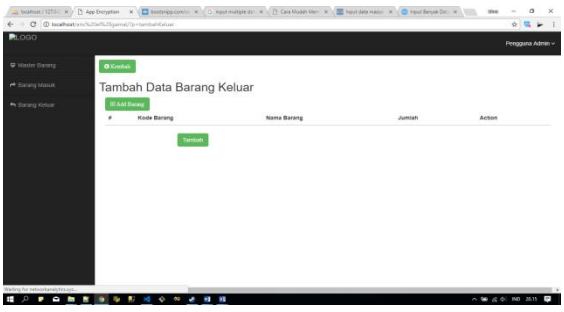
Tampilan Menu Tambah BarangMasuk

f) Tampilan Menu Data Barang Keluar
Berikut ini adalah tampilan menu data barang keluar



Gambar 9. Tampilan Menu Data BarangKeluar

g) Tampilan Menu Tambah Data Barang Keluar
Berikut ini adalah tampilan menu data barang keluar



Gambar 10. Tampilan Menu Tambah Data Barang Keluar

1) Tabel Pengujian

Tabel pengujian membahasa perbandingan antara data sebelum dan sesudah di enkripsi dalam database.

1. Tampilan Hasil Pengujian Proses Enkripsi
Berikut ini adalah tampilan Hasil Pengujian Proses Enkripsi

Tabel 1 Hasil Pengujian Proses Enkripsi

No	Jenis Kegiatan	Teks Asli	Hasil Enkripsi
1	Tambah Data Barang	Solar Tangki Depan	131 27 131 535 131 573 131 281 131 497 131 26 131 230 131 281 131 332 131 205 131 370 131 611 131 26 131 217 131 446 131 91 131 281 131 332
2	Tambah Data Barang	Solar Tangki Belakang	131 27 131 535 131 573 131 281 131 497 131 26 131 230 131 281 131 332 131 205 131 370 131 611 131 26 131 458 131 446 131 573 131 281 131 370 131 281 131 332 131 205
3	Tambah Data Barang	7200	131 166 131 445 131 39 131 39
4	Tambah Data Barang Masuk	100	131 242 131 39 131 39
5	Tambah Data Barang Keluar	500	131 407 131 39 131 39

2. Tampilan Hasil Pengujian Proses Dekripsi
   Berikut ini adalah tampilan Hasil Pengujian Proses Dekripsi

Tabel 2 Hasil Pengujian Proses Dekripsi

#	Nama Barang	Stok
1	Solar Tangki Depan	7200
2	Solar Tangki Belakang	7010

2) Analisa Program

Analisa hasil uji coba merupakan tahap terakhir yang perlu dilakukan dalam pengembangan suatu aplikasi perangkat lunak. Analisa hasil uji coba bertujuan untuk mengetahui hasil yang telah dicapai oleh aplikasi yang dibuat dan menentukan kekurangan dan kelebihan aplikasi yang dibuat. Berdasarkan pengujian aplikasi untuk proses enkripsi dan dekripsi yang telah dilakukan pada data yang di masukkan ke database dapat ditemukan beberapa kelebihan dan kekurangan dari aplikasi ini, yaitu sebagai berikut:

Kelebihan:

1. Data yang tersimpan di database menjadi lebih aman karena data dienkripsi menggunakan kriptografi El Gamal.
2. Proses enkripsi dekripsi data tergolong cepat.

Kekurangan:

1. Hasil ciphertext Enkripsi El Gamal mempunyai panjang dua kali lipat dari plaintext nya

5. KESIMPULAN DAN SARAN

1) Kesimpulan

Berdasarkan hasil analisa yang telah kami lakukan terhadap permasalahan dan aplikasi yang dikembangkan, maka dapat ditarik suatu kesimpulan, sebagai berikut yaitu :

a. Aplikasi kriptografi ini menggunakan algoritma El Gamal sebagai sistem keamanan database aplikasi ini.
b. Mengamankan informasi data perusahaan menjadi rahasian agar tidak bisa di ketahui oleh pihak yang tidak bertanggungjawab.
c. Dengan adanya aplikasi kriptografi ini, proses keamanan database menjadi lebih aman.

2) Saran

Selain menarik beberapa kesimpulan, dapat pula diajukan saran-saran yang mungkin bisa dijadikan pertimbangan dalam pengembangan sistem, antara lain:

a. Aplikasi yang dibuat perlu adanya pengembangan algoritma yang bisa di tingkatkan.
b. Aplikasi yang dibuat perlu ditingkatkan. Karena hanya mencangkup transaksi perusahaan makan perlunya pengembangan aplikasi lebih lanjut.

DAFTAR PUSTAKA

[1] Dahria, M., Rahim, A. & Jaya, H., 2012. Issn : perangkat lunak pembelajaran kriptografi metode wake (word auto key encryption). Jurnal Ilmiah Saintikom, 11(3), pp.143–162.

[2] Al-Anshori, Faqihuddin, Eko Ariwibowo, 2014, Implementasi Algoritma Kriptografi Kunci Public ElGamal untuk proses Enkripsi dan Dekripsi guna Pengamanan File Data, Jurnal Informatika Februari 2014.

[3] Ariwibowo, Eko, 2008, Aplikasi Pengamanan Dokumen Office dengan Algoritma Kriptografi Kunci Asimetris ElGamal, Jurnal Informatika Vol.2, No.2, Juli 2008.

[4] Arjana, Putu H, Dkk, 2012, Implementasi Enkripsi Data Dengan Algoritma Vigenere Cipher, SENTIKA, 2089-9815.

[5] Fauzan, Ahmad, 2013, Kriptografi Visual Dengan Memanfaatkan Algoritma Elgamal Untuk Citra Berwarna, Bandung : ITB.

[6] Febriansyah, 2012, Sistem Pengiriman Pesan Menggunakan Sistem keamanan Kriptografi Modern. Sumatera Selatan : Universitas Sriwijaya.

[7] Namira, 2013, Pengoptimalan Sistem Kemanan Data Dalam Sistem Database Online pada PT. Nagasa. Surabaya : Insitut Teknologi Sepuluh Nopember.

[8] Sadikin, Rifki, 2012, Kriptografi untuk Keamanan Jaringan, Yogyakarta: Andi.

[9] Sharma, 2012, Optimalisasi Dalam Kemanan Sistem Database Menggunakan Sistem Keamanan Modern. Surakarta : Universitas Muhammadiyah Surakarta.

[10] Widyartono, Agustinus, 2011, Algoritma Elagamal Untuk Enkripsi Data Menggunakan GNUPG, Jurnal Teknologi dan Informatika Vol.1 No.1 Januari 2011.

[11] Yusmantoro, Sandi, Edy Hermansyah, Rusdi Efendi, 2014, Rancang Bangun Aplikasi Pengamanan Keaslian Surat Izin Tempat Usaha Menggunakan Algoritma ElGamal dan Secure Hash Algorithm 256 Studi Kasus: Badan Pelayanan Perizinan Terpadu (BPPT) Kota Bengkulu, Jurnal Rekursif, Vol.2, No.1 Maret 2014.

[12] Zelvina, Anandia, Syahril Efendi, Dedy Arisandi, 2012, Perancangan Aplikasi Pembelajaran Kriptografi Kunci Publik ElGamal untuk Mahasiswa, Jurnal Dunia Teknologi Informasi Vol.1, No.1, (2012) 56-62.