IMPLEMENTASI METODE KRIPTOGRAFI IDEA pada PRIORITY DEALER untuk LAYANAN PEMESANAN dan LAPORAN PENJUALAN HAMDPHONE BERBASIS WEB

Kholidya Yuli Wardani, M.Zen S.Hadi, ST. MSc, Mike Yuliana, ST.MT.
Politeknik Elektronika Negeri Surabaya
Institut Teknologi Sepuluh Nopember,Kampus ITS,Surabaya 6011
e-mail : dyatelkomlj@student.eepis-its.edu

ABSTRAK-- Distributor adalah penyedia barang, yang mengklasifikasikan barang atau memilahnya berdasarkan jenis, ukuran, dan kualitasnya, yang kemudian didistribusikan kepada dealer atau priority dealer. Sebuah distributor memiliki beberapa priority dealer yang melakukan penjualan handphone langsung pada konsumen (*end user*). Sehingga priority dealer harus memberikan laporan hasil penjualan dan pemesanan pada distributor. Dengan perkembangan teknologi yang sangat pesat saat ini, Cara yang digunakan priority dealer ketika memberikan laporan pada distributor masih terbilang kuno karena priority dealer masih harus datang ke distributor langsung.hal ini tentu saja memakan waktu dan biaya. Padahal saat ini banyak system penjualan yang berbasis WEB dengan tujuan mempermudah saling bertukar informasi / data secara jarak jauh sehingga lebih efisien dan tidak mengeluarkan biaya, namun kelemahan menggunakan system WEB yaitu keamanan kerahasiaan pengiriman data tidak terjamin. Oleh karena itu pada proyek akhir ini dibuat suatu sistem Imlementasi Metode Kriptografi IDEA pada Priority Dealer untuk Layanan Penjualan dan Pemesanan Handphone berbasis WEB. Sehingga priority dealer tidak perlu datang langsung ke distributor hanya untuk melakukan pembelian dan pemesanan barang. Cukup dengan login pada WEB distributor server laporan penjualan dan pemesanan sudah dapat dilakukan oleh priority dealer dan keamanan kerahasiaan data atau pesan dapat terjamin dari pihak lain. Hasil dari proyek akhir ini yaitu Menghasilkan system layanan penjualan dan pemesanan Handphone berbasis WEB dengan menggunakan kriptografi dengan algoritma IDEA sehingga saat pengiriman data atau pesan dari distributor server ke priority dealer terjaga keamanannya.

Kata kunci : Kriptografi, IDEA, WEB server, Priority Dealer.

1. PENDAHULUAN

Distributor adalah penyedia barang, yang mengklasifikasikan barang atau memilahnya berdasarkan jenis, ukuran, dan kualitasnya, yang kemudian didistribusikan kepada dealer atau priority dealer. Sebuah distributor memiliki beberapa priority dealer yang melakukan penjualan handphone langsung pada konsumen (*end user*). Sehingga priority dealer harus memberikan laporan hasil penjualan dan pemesanan pada distributor. Dengan perkembangan teknologi yang sangat pesat saat ini, Cara yang digunakan priority dealer ketika memberikan laporan pada distributor masih terbilang kuno karena priority dealer masih harus datang ke distributor langsung.hal ini tentu saja memakan waktu dan biaya. Padahal saat ini banyak system penjualan yang berbasis WEB dengan tujuan mempermudah saling bertukar informasi/data secara jarak jauh sehingga lebih efisien dan tidak mengeluarkan biaya, namun kelemahan menggunakan system WEB yaitu keamanan kerahasiaan pengiriman data tidak terjamin.

Oleh karena itu pada proyek akhir ini akan dibuat suatu WEB server yang digunakan untuk pemesanan barang dan laporan hasil penjualan dengan dilengkapi *security network* yaitu menggunakan kriptografi dengan algoritma IDEA sehingga keamanan dan kerahasiaan dapat terjaga, saat melakukan komunikasi dan pertukaran informasi/data tidak dapat disadap pihak yang tidak berkepentingan.

2. Kriptografi

Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga. Menurut Bruce Scheiner dalam bukunya "Applied Cryptography", kriptografi adalah ilmu pengetahuan dan seni menjaga *message-message* agar tetap aman (secure).

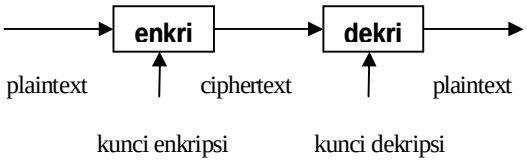
Konsep kriptografi sendiri telah lama digunakan oleh manusia misalnya pada peradaban Mesir dan Romawi walau masih sangat sederhana. Prinsip-prinsip yang mendasari kriptografi yakni:

- *Confidelity* (kerahasiaan) yaitu layanan agar isi pesan yang dikirimkan tetap rahasia dan tidak diketahui oleh pihak lain (kecuali pihak pengirim, pihak penerima / pihak-pihak memiliki ijin). Umumnya hal ini dilakukan dengan cara membuat suatu algoritma matematis yang mampu mengubah

data hingga menjadi sulit untuk dibaca dan dipahami.

- *Data integrity* (keutuhan data) yaitu layanan yang mampu mengenali / mendeteksi adanya manipulasi (penghapusan, pengubahan atau penambahan) data yang tidak sah (oleh pihak lain).
- *Authentication* (keotentikan) yaitu layanan yang berhubungan dengan identifikasi. Baik otentikasi pihak-pihak yang terlibat dalam pengiriman data maupun otentikasi keaslian data/informasi.
- *Non-repudiation* (anti-penyangkalan) yaitu layanan yang dapat mencegah suatu pihak untuk menyangkal aksi yang dilakukan sebelumnya (menyangkal bahwa pesan tersebut berasal dirinya).

Kriptografi itu sendiri terdiri dari dua proses utama yakni proses enkripsi dan proses dekripsi. Seperti yang telah dijelaskan di atas, proses enkripsi mengubah *plaintext* menjadi *ciphertext* (dengan menggunakan kunci tertentu) sehingga isi informasi pada pesan tersebut sukar dimengerti.



Gambar 1**.** Diagram proses enkripsi dan dekripsi

Peranan kunci sangatlah penting dalam proses enkripsi dan dekripsi (disamping pula algoritma yang digunakan) sehingga kerahasiaannya sangatlah penting, apabila kerahasiaannya terbongkar, maka isi dari pesan dapat diketahui.

3. Algoritma IDEA (*International Data Encryption Algorithm*)

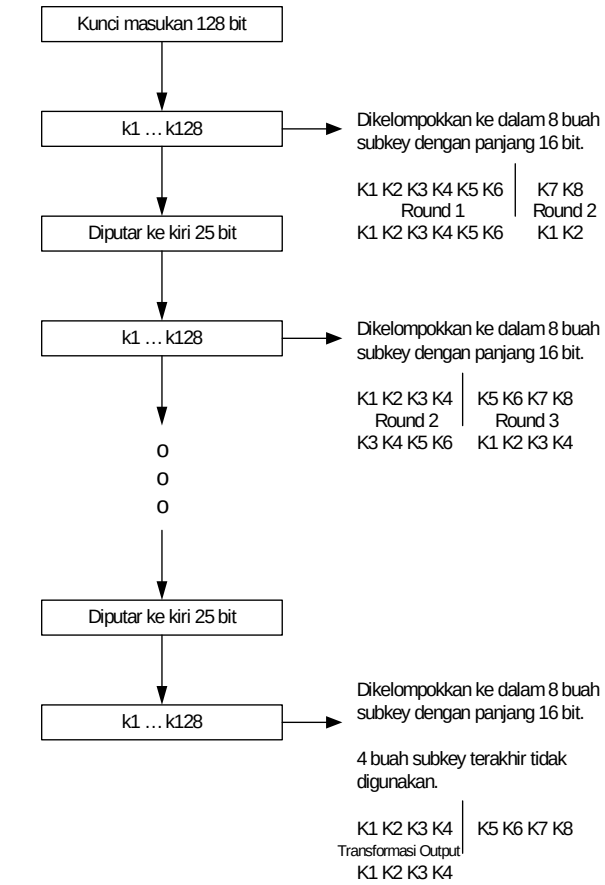
Dalam kriptografi, International Data Encryption Algorithm (IDEA) adalah algoritma ciper blok yang dibuat oleh Xuejia Lai and James Massey dari ETH Zurich dan dikenalkan pertama kali pada tahun 1991. Dirancang untuk menggantikan DES.

IDEA beroperasi pada blok plaintext 64-bit dan panjang kuncinya 128 bit. Algoritma yang sama digunakan untuk enkripsi dan dekripsi. Sebagaimana algoritma enkripsi yang lain, IDEA menggunakan confusion dan diffusion. Berbeda dengan DES yang menggunakan permutasi dan subtitusi untuk confusion dan diffusion. IDEA menggunakan operasi aljabar yang tidak kompatibel.

a. Pembentukan Kunci

Proses pembentukan ini dimulai dengan membagi 128 *bit key* menjadi 8 buah 16 *bit subkey*. Ini merupakan delapan *subkey* pertama untuk algoritma dengan perincian enam *subkey* pertama untuk putaran (*round*) 1 dan dua *subkey* terakhir untuk putaran 2. *Key* dirotasikan 25 bit ke kiri dan dibagi menjadi 8 *subkey* lagi. Ini merupakan delapan *subkey* kedua untuk algoritma dengan perincian empat *subkey* pertama untuk putaran 2 dan empat *subkey* terakhir untuk putaran 3. Algoritma hanya menggunakan 52 buah *subkey* dengan perincian 6 buah *subkey* untuk 8 putaran ditambah 4 buah *subkey* untuk transformasi output.

Proses pembentukan kunci dapat dilihat pada gambar 2.3 di bawah ini :



Gambar 2. *Proses Pembentukan Kunci untuk IDEA*

b. Enkripsi

Proses enkripsi algoritma IDEA adalah sebagai berikut, Pertama – tama, *plaintext* 64 *bit*

dibagi menjadi 4 buah sub blok dengan panjang 16 *bit*, yaitu X1, X2, X3, X4. Empat sub blok ini menjadi masukan bagi iterasi tahap pertama algoritma. Total terdapat 8 iterasi. Pada setiap iterasi, 4 sub blok di-XOR-kan, ditambahkan, dikalikan dengan yang lain dan dengan 6 buah *subkey* 16 bit. Diantara iterasi sub blok kedua dan ketiga saling dipertukarkan. Akhirnya 4 buah sub blok dikombinasikan dengan 4 *subkey* dalam transformasi output. Pada setiap tahapan, urutan berikut ini dikerjakan :

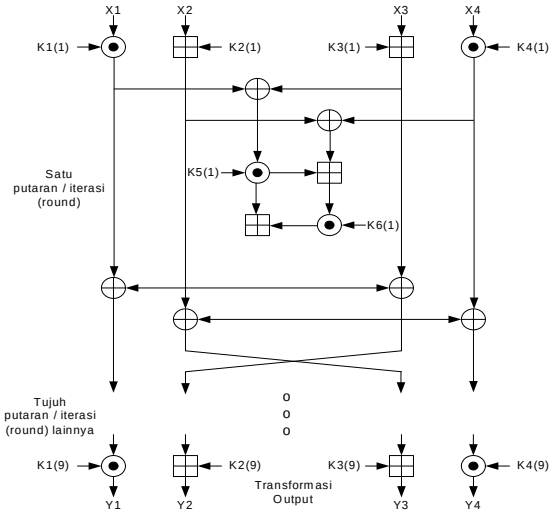
1. Kalikan X1 dengan K1 mod $(2^{16} + 1)$.
2. Tambahkan X2 dengan K2 mod 2^{16}.
3. Tambahkan X3 dengan K3 mod 2^{16}.
4. Kalikan X4 dengan K4 mod $(2^{16} + 1)$.
5. XOR hasil dari step 1 dan 3.
6. XOR hasil dari step 2 dan 4.
7. Kalikan hasil step 5 dengan K5 mod $(2^{16} + 1)$.
8. Tambahkan hasil step 6 dan 7 mod 2^{16}.
9. Kalikan hasil step 8 dengan K6 mod $(2^{16} + 1)$.
10. Tambahkan hasil dari step 7 dan 9.
11. XOR hasil dari step 1 dan 9.
12. XOR hasil dari step 3 dan 9.
13. XOR hasil dari step 2 dan 10.
14. XOR hasil dari step 4 dan 10.

Output dari setiap *round* adalah empat sub blok yang dihasilkan pada langkah 11, 12, 13 dan 14. Sub blok 12 dan 13 di-*swap* (kecuali untuk putaran terakhir) sehingga *input* dari putaran berikutnya adalah hasil kombinasi dari langkah 11 13 12 14.

Setelah 8 putaran, akan dilakukan tranformasi output berikut :

1. Kalikan X1 dengan subkey K1 mod $(2^{16} + 1)$.
2. Tambahkan X2 dengan subkey K2 mod 2^{16}.
3. Tambahkan X3 dengan subkey K3 mod 2^{16}.
4. Kalikan X4 dengan subkey K4 mod $(2^{16} + 1)$.

Proses enkripsi algoritma IDEA dapat dilihat pada gambar berikut ini :



Gambar 3. *Proses Enkripsi Algoritma IDEA*

c. Dekripsi

Proses dekripsi sama persis dengan proses enkripsi. Perbedaannya hanya terletak pada aturan dari subkey-nya. Urutan *subkey* terbalik dengan proses enkripsi dan *subkey*-nya di-*inverse*-kan. *Subkey* pada langkah transformasi output pada proses enkripsi di-*inverse*-kan dan digunakan sebagai *subkey* pada putaran 1 pada proses dekripsi. *Subkey* pada putaran 8 di-*inverse*-kan dan digunakan sebagai *subkey* pada putaran 1 dan 2 pada proses dekripsi. Demikian seterusnya.

Proses dekripsi menggunakan algoritma yang sama dengan proses enkripsi tetapi 52 buah subblok kunci yang digunakan masing-masing merupakan hasil turunan 52 buah subblok kunci enkripsi. Pada kasus ini akan diambil invers dari operasi penambahan oleh mod 2^{16} dan perkalian mod 2^{16} +1, tergantung pada operasi yang dibuat pada fase enkripsi. Setiap subkunci dekripsi adalah salah satu dari invers penambahan atau perkalian yang berkorespondensi dengan subkunci enkripsi.

3. PHP (*Personal Home Page*)

PHP adalah skrip bersifat *server-side* yang ditambahkan ke dalam HTML. PHP merupakan *Hypertext Processor*. Skrip yang terdapat pada PHP akan membuat suatu aplikasi yang dapat terintegrasi ke dalam HTML, sehingga suatu halaman web tidak lagi bersifat statis, namun menjadi bersifat dinamis. Untuk dapat menghubungkan program PHP dengan database MySQLyaitu dengan mengkoneksikan keduanya. PHP telah menyediakan fungsi yang dapat melakukan koneksi dengan MySQL. Untuk

menghubungkan dengan database maka, dapat menggunakan fungsi mysql_connect().

```
mysql_connect (hostname, username, $pass)
```

Sintaks di atas, memiliki komponen dan fungsinya yang dapat dijelaskan sebagai berikut :

- Hostname : alamat server tempat menyimpan server MySQL, apabila terletak pada komputer lokal, anda dapat menggunakan alamat "*localhost*". Sedangkan apabila berada di komputer lain, maka menggunakan alamat nomor IP address.
- Username : nama user yang dimiliki oleh server database yang dituju. Jadi, harus memiliki hak akses terhadap database MySQL yang dituju.
- Pass : password yang sesuai dengan *username* yang digunakan. Apabila username dan password belum ada, maka dapat mendaftarkannya terlebih dahulu.

4. Database MySQL

MySQL merupakan *Relation Database Management System (RDBMS)* yang didistribusikan secara gratis dibawah lisensi *GPL (General Public License). D*imana setiap orang bebas untuk menggunakan MySQL, namun tidak boleh dijadikan turunan yang bersifat *closed source* atau komersial. MySQL sebenarnya merupakan turunan salah satu konsep utama dalam database sejak lama, yaitu *SQL (Structure Query Language)*. SQL adalah sebuah konsep pengoperasian *database*, terutama untuk seleksi dan pemasukan data, yang memungkinkan pengoperasian data dikerjakan dengan mudah secara otomatis.

Keandalan suatu sistem *database* (DBMS) dapat diketahui dari cara kerja *optimizer*nya dalam melakukan proses perintah-perintah SQL, yang dibuat oleh user maupun program-program aplikasinya. Sebagai *database server*, MySQL dapat dikatakan lebih unggul dibandingkan dengan *database server* yang lainnya dalam query data.

SQL adalah bahasa standar yang digunakan untuk mengakses database server. Pada awalnya dikembangkan oleh IBM, namun telah diadopsi dan digunakan sebagai standar industri. Dengan menggunakan SQL, proses akan database menjadi lebih *user-friendly* dibandingkan menggunakan dBASE dan *chipper* yang masih menggunakan perintah-perintah pemrograman.

5. Distributor dan Priority Dealer

Distributor adalah perantara yang menyalurkan produk dari pabrik (*manufacturer*) ke priority dealer. Distributor mendistribusikan /menjual barang/product prinsipal, dengan mendapat keuntungan, distributor bertanggung jawab atas ketersediaan barang principal sesuai perjanjian yang telah disepakati. Setelah suatu produk dihasilkan oleh pabrik, produk tersebut dikirimkan (dan biasanya juga sekaligus dijual) ke suatu distributor. Tugas distributor adalah penyedia barang, yang mengklasifikasikan barang atau memilahnya berdasarkan jenis, ukuran, dan kualitasnya, yang kemudian didistribusikan kepada dealer atau priority dealer.

Priority dealer merupakan dealer resmi yang diakui oleh principal. Principal adalah pembuat/pabrik/pemilik dari product yang didistribusikan barang/productnya pada distributor. Kerja dari priority dealer ini adalah berjualan dimana priority dealer ini menjual handphone dengan membelinya di distributor. Barang yang dijual pada priority dealer ini mayoritas adalah produk dari principal misal priority dealer nokia maka handphone yang dijual oleh priority dealer 70-80% (mayoritas) adalah handphone nokia. Jaringan penjualan dari priority dealer ini sudah bertaraf nasional. Priority dealer ini biasanya menjual produk tersebut ke pelanggan.

6. PERANCANGAN ARSITEKTUR

Gambar 4: Blok diagram sistem

Dari gambar 4 dapat dijelaskan prinsip kerja sistem sebagai berikut :

Dalam sistem ini dibuat interaksi antara *server* dan *client* yang yang berbasis WEB menggunakan kriptografi dengan metode IDEA yang diimplementasikan pada priority dealer untuk layanan laporan hasil penjualan dan pemesanan handphone. Distributor server memiliki beberapa client yaitu priority dealer, masing – masing priority dealer memiliki ID (username dan password) sehingga mampu mengakses WEB distributor server untuk melakukan permintaan dan pemesanan barang kemudian distributor server akan mengirimkan informasi tentang ketersediaan permintaan barang pada priority dealer. Pada pengiriman data yang dilakukan oleh priority dealer ke distributor server akan dilakukan enkripsi dengan menggunakan metode IDEA.

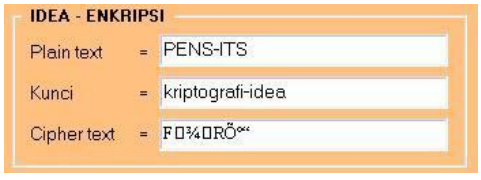
Setelah itu data akan didekripsi disisi server sehingga priority dealer dapat mengakses web layanan pemesanan dan penjualan barang, jumlah pemesanan dan instansi yang memesan secara *real time*. Lalu server akan memberikan informasi ke pelanggan total harga yang harus dibayar. Priority dealer yang dapat melakukan pemesanan barang online hanya priority dealer yang telah terdaftar pada distributor server. Bila ada priority dealer baru maka harus mendaftar pada distributor server secara manual.

7. PENGUJIAN DAN HASIL

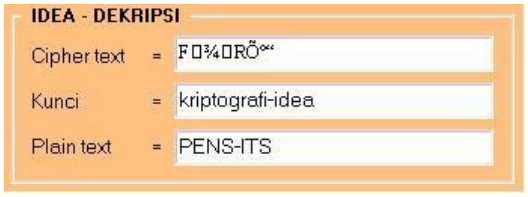
Pada proyek akhir ini dilakukan pengujian dan analisa system terhadap performansi dari kriptografi IDEA.

7.1 Pengujian dan Analisa Implementasi Metode Enkripsi/Dekripsi IDEA dan Integrasi Client Server

Pengujian enkripsi/dekripsi IDEA akan dilakukan pada data *string* dimana tujuan dari pengujian ini adalah untuk mengetahui kebenaran dari metode enkripsi/dekripsi IDEA yang telah dibuat.



Gambar 5 : *Cipher text* Hasil Enkripsi



Gambar 4.10 : *plain text* Hasil Dekripsi

Hasil pengujian diatas dilakukan dengan menampilkan *ciphertext* hasil enkripsi, dan hasil dekripsi kemudian dibandingkan dengan teks aslinya menggunakan metode IDEA. Dari proses enkripsi/dekripsi IDEA pada data string berupa huruf ,angka dan metakarakter (*plain text*) tersebut terlihat bahwa metode enkripsi/dekripsi yang dibuat telah teruji kebenarannya, karena *string* yang terenkripsi (*cipher text*) setelah didekripsi kembali ke *string* aslinya (*plain text*).

7.2 Pengujian, Perbandingan dan Analisa Linieritas Hasil Enkripsi

Tabel 4.1: Panjang karakter asli dan simbol enkripsi metode IDEA

Karakter Asli	Jumlah Karakter	Hasil Enkripsi	Jumlah Karakter
zunkiest	**8**	**P◆qÈŸäƒ**	**8**
27071988	**8**	**ûì]Šæ¬**	**7**
PENS-ITS	**8**	**F◆¾RÕº“**	**8**
lidya_07	**8**	**8rúkÎâîD**	**8**
@gleo$_88	**8**	**o´\ šÈwü**	**7**
@r$en*07	**8**	**±qD`å**	**8**
donkdonk	**8**	**2œY.qÄý**	**8**
Gho_Zila	**8**	**Y28×2‘×**	**8**
27@Gmail	**8**	**£D%◆æM>**	**8**
Yahoo.co	**8**	**AÝZq‡ãy®**	**8**

Dapat diketahui bahwa jumlah karakter teks asli (*plain text*) dan jumlah karakter hasil enkripsi *cipher text* dari teks tersebut sama panjangnya yaitu 64 bit atau 8 karakter. Sehingga dapat dikatakan bahwa metode enkripsi IDEA ini adalah linier.

7.3 Pengujian dan Analisa Waktu Enkripsi/Dekripsi Enkripsi Menggunakan Metode IDEA

Pengujian waktu proses enkripsi/dekripsi dilakukan pada karakter huruf , angka, dan metakarakter menggunakan algoritma IDEA. Pengujian ini dilakukan untuk bentuk karakter dan panjang karakter. Proses perhitungan waktu proses enkripsi/dekripsinya menggunakan program PHP pada sisi *client* mulai dari *client* mengirimkan informasi yang kemudian dienkripsi, *server* melakukan proses dekripsi hingga *client* mendapat informasi hasil dekripsi dari *server*.

Berikut ini adalah tabel hasil pengukuran waktu enkripsi/dekripsi untuk karakter huruf sepanjang 8 karakter dengan panjang kunci 16 karakter:

Tabel 4.4: Perhitungan Waktu pada Enkripsi / Dekripsi Metode IDEA

Karakter Asli	Waktu Enkripsi/Dekripsi (detik)
zunkiest	**0.083041**
27071988	**0.075453**
PENS-ITS	**0.08254**
lidya_07	**0.023345**
@gleo$_88	**0.026347**
@r$en*07	**0.123432**
donkdonk	**0.081547**
Gho_Zila	**0.094338**
27@Gmail	**0.082075**
Yahoo.co	**0.082312**

Dari tabel 4.4 dapat diketahui bahwa pada metode enkripsi IDEA, waktu yang diperlukan untuk proses enkripsi/dekripsi dari client ke server adalah 0.023345 detik sampai 0.123432 detik. Hal ini menujukkan bahwa bentuk karakter berpengaruh terhadap waktu proses enkripsi/dekripsi IDEA.

8. KESIMPULAN

Dari hasil pengujian dan analisa pada bab sebelumnya, maka dapat diambil beberapa kesimpulan sebagai berikut :

1. IDEA menerima masukan berupa 64-bit plaintext dan 128-bit kunci, dan menggunakan subkey 16-bit. Keduanya sama-sama beroperasi dalam 64-bit block, yang terdiri dari 8 putaran identik dan sebuah output transformation. IDEA memiliki fungsi enkripsi yang kuat dan aman. Namun kesederhanaan pada key schedule yang dimiliki IDEA mengakibatkan IDEA memiliki kunci yang lemah. Proses enkripsi pada IDEA menggunakan campuran operasi dari tiga kelompok aljabar, yaitu addition modulo, multiplication modulo, dan bitwise XOR. Campuran ketiga operasi inilah yang menjamin keamanan IDEA.
2. Waktu yang diperlukan oleh algoritma IDEA untuk mengenkripsi dan mendekripsi waktu yang diperlukan untuk proses enkripsi/dekripsi serarah dari client ke server adalah 1,125 detik -1,492 detik . Waktu enkripsi/dekripsi bolak-balik yaitu dari client ke server dan server ke client adalah 1,265 detik - 1,625 detik. Hal ini menujukkan bahwa panjang karakter berpengaruh terhadap waktu proses enkripsi/dekripsi IDEA. Sedangkan waktu proses enkripsi/dekripsi menggunakan software AES adalah 0,3-0,4 detik. Hal ini menujukkan bahwa panjang karakter tidak berpengaruh signifikan terhadap waktu proses enkripsi/dekripsi *software* AES.
3. Aplikasi integrasi *client server* tidak dapat mensupport karakter huruf kapital dan *form choicegroup*. Hal ini disebabkan karena dalam pemrograman IDEA perlu dilakukan konvert data beberapa kali untuk memasukan data inputan ke dalam fungsi enkrip dan dekrip, sedangkan pada PHP dapat langsung mengenali berbagai tipe data tanpa mengkonvert

9. SARAN

Untuk penelitian lebih lanjut, menggunakan dua metode enkripsi/dekripsi untuk

diimplementasikan pada suatu sistem informasi sehingga perbandingan dan analisanya dapat lebih akurat, dan menggunakan metode kriptografi yang memiliki kunci yang asimetris sehingga orang lain sulit untuk menggunakan kunci tersebut untuk mendekripsi *chippertext*.

10. DAFTAR PUSTAKA

[1] Fahmi, Ahmad *"Perancangan Perangkat Lunak Pembelajaran Metode Kriptografi IDEA"* **,** Proyek akhir PENS-ITS, 2009.

[2] Gregorius S. Budhi ST., MT. **"***Fungsi Hash SNEFRU dan Metode Enkripsi IDEA untuk Keamanan Dokumen Elektronik***"** jurnal IDEA-SNEFRU, UK Petra, 2009.

[3] Zen S Hadi,*"Modul teori MySQL Internet Programing*", Diktat ajar PENS-ITS, Surabaya, 2009.

[4] Zen S Hadi,"*Modul teori PHP Internet Programing*", Diktat ajar PENS-ITS, Surabaya, 2009.

[5] Jaja, "*Keamanan komputer dan jaringan kriptografi*", Proyek akhir Universitas Subang, 2008.

[6] Dyah Retnowulan *"Pembuatan Sistem Pengamanan Informasi Pemesanan Barang di Toko Komputer Berbasis J2ME Menggunakan Algoritma RC4*", Proyek akhir PENS-ITS, 2010.

[7] Jethefer Stevens, "*Studi Perbandingan Algoritma IDEA dengan DES"*, Proyek akhir, ITB, 2006.

[8] Ilham M. Said dan Harunur Rasyid, "*Implementasi Pengamatan Database dengan Oracle Security Server*", Diktat ajar Universitas Muhammadiyah Gresik, 2005.

[9] Andara Livia, "*Studi Perbandingan International Data Encryption Algorithm (IDEA) dan TheFast Data Encipherment Algorithm (FEAL)*", Proyek akhir ITB, 2010.

[10] Sarwono Sutikno, Aditya Timur Baladika, Marta Dinata A., dan Sigit Dewantoro VLSI Research Group, "*Penerapan Alur Desain Alliance Dalam Perancangan Core Prosesor Kripto IDEA*", Diktat ajar ITB, 2009.