# PENGAMANAN DATA MySQL PADA *E-COMMERCE* DENGAN ALGORITMA AES 256

**Kartika Imam Santoso[1)], Wahyu Priyoatmoko[2)]**
[1]Sistem Informasi, [2]Teknik Informatika STMIK BINA PATRIA
Jl. Raden Saleh No.2, Magelang, 56116
Telp : (0293) 362993, Fax : (0293) 364461
E-mail : kartikaimams@gmail.com[1)], wepe1983@gmail.com[2)]

***Abstrak***

*Dengan banyaknya e-Commerce dan website yang yang dalam beberapa tahun terakhir menjadi target serangan hacker. Ancaman yang sering terjadi pada aplikasi web diantaranya merupakan ancaman SQL Injection dan pencurian data. Merancang, membangun dan mengimplementasikan keamanan data MySQL pada e-Commerce dengan Algoritma AES 256 menjadi salah satu cara mengatasinya. Selain itu juga untuk menghindari Kripanalisis untuk membaca pola penyandian untuk menemukan kunci.Hasil yang diharapkan adalah e-Commerce menjadi lebih aman datanya dari serangan hacker dan pencurian data dari pesaing bisnis.*

***Kata kunci:*** *AES 256, E-Commerce, SQL Injection, MySQL*

***Abstract***

*With the massive number of e-Commerce and websites becoming the target of hackers' attacks in recent years, threats that are commonly targeting web applications include SQL Injection and data theft. Designing, establishing, and implementing MySQL data security on e-Commerce with AES 256 Algorithm have become one solution of overcoming the issue. In addition, it is also used to avoid Kripanalisis Cryptanalysis to read the encryption pattern in finding the key. The result expected is to establish a more secure data of e-Commerce from the hackers' attacks and data theft from the business competitors.*

***Keywords:*** *AES 256, E-Commerce, SQL Injection, MySQL*

## 1. PENDAHULUAN

Sudah diketahui bersama bahwa perkembangan teknologi dan informasi semakin pesat. Teknologi Internet merupakan salah satu media informasi yang saat ini paling banyak digunakan karena memiliki banyak keunggulan terutama dalam efesiensi waktu serta murah. Salah satu contoh dari pemanfaatan Internet adalah aplikasi web.

Aplikasi web adalah aplikasi yang diakses menggunakan browser web melalui jaringan internet. Aplikasi web sangat bermanfaat untuk mempromosikan ataupun melakukan transaksi jual beli pada sebuah perusahaan melalui media Internet. Sebagai contoh, banyaknya perusahaan yang menjual produk dan promosi produk melalui *E-Commerce* dan *E-Bussiness*, dimana penjualan tersebut dilakukan secara elektronik. Aplikasi web sangat beragam, seperti toko online dan website yang berisi informasi yang dalam beberapa tahun terakhir menjadi target serangan *hacker*. Ancaman yang sering terjadi pada aplikasi web diantaranya merupakan ancaman *SQL Injection*. *SQL (Structure Query Language) Injection* adalah jenis ancaman yang mengizinkan *query SQL* dapat di-*inject* oleh *client* kemudian diteruskan oleh *server* untuk dieksekusi [3]. Ancaman ini terjadi pada database aplikasi web. *Cross-Site Scripting* atau sering dikenal dengan XSS adalah ancaman yang mengizinkan kode (*client side script*) dimasukan ke dalam suatu *website* yang dapat dijalankan pada sisi *client*.

*Database* menjadi sangat penting dalam perusahaan saat ini dan *database* berisi informasi yang merupakan aset perusahaan besar [10]. Keamanan web database adalah isu paling penting saat membangun sebuah situs web yang ditujukan untuk mendukung aktivitas *E-Commerce*. Namun demikian, banyak sekali pemilik bisnis yang tidak menyadari hal tersebut karena terbatasnya informasi dan seringkali karena terbenturnya oleh minimnya kapabilitas pihak pengembangnya. Padahal jika menginginkan adanya

Copyright © 2016 SESINDO

transaksi pemesanan dan pembelian dalam situs web *E-Commerce*, minimal harus dilengkapi fasilitas enkripsi data.

Calon pelanggan atau konsumen dapat menemukan *website*, membaca dan melihat produk-produk, memesan dan membayar produk-produk tersebut secara online. Bagi pihak konsumen, menggunakan *E-Commerce* dapat membuat waktu berbelanja menjadi singkat [4]. Tidak perlu lagi berlama-lama mengelilingi pusat pertokoan untuk mencari barang yang diinginkan. Setiap penyedia layanan jasa *E-Commerce* berusaha untuk menyediakan suatu sistem yang dapat menjaga keamanan data dari transaksi-transaksi yang dilakukan oleh pelanggan [5]. Namun timbul permasalahan mengenai keamanan jaringan dan kebutuhan akan keamanan informasi pada *website E-Commerce* menjadi sangat penting untuk menjaga kerahasiaan data user maupun perusahaan [6].

Tetapi dibalik populernya penjualan secara *online*, banyak pengguna internet yang masih takut dalam melakukan transaksi, baik untuk membeli dan menjual barang di toko-toko virtual, maupun melakukan transaksi keuangan pada sistem *Internet Banking*. Resiko dalam melakukan transaksi di Internet sangat tinggi, karena selain beragamnya tujuan pengguna Internet, perangkat hukum yang menaungi keamanan dalam bertransaksi di Internet juga masih belum memadai. Pengambilan data nasabah dan data card untuk pembayaran juga sering juga dilakukan oleh *hacker* atau pesaing bisnis.

Tujuan penulisan artikel ini adalah untuk merancang, membangun dan mengimplementasikan keamanan data pada *E-Commerce* dengan *database MySQL* menggunakan Algoritma AES 256 untuk sebagai menghindari *Kripanalisis* untuk membaca pola penyandian untuk menemukan kunci dan isi data. *AES* telah dirancang dalam perangkat lunak dan perangkat keras dan bekerja dengan cepat dan efisien, bahkan pada perangkat kecil seperti ponsel pintar. Dengan ukuran blok yang besar dan ukuran kunci yang lebih panjang, *AES* akan memberikan keamanan lebih dalam jangka panjang [9].

## 2. TINJAUAN PUSTAKA

Implementasi pengamanan *E-Commerce* telah dilakukan, berikut ini antara lain penelitian dengan judul Penerapan Algoritma Gabungan *RC4* dan *BASE64* Pada Sistem Keamanan *E-Commerce*. Hasil dari penelitian ini adalah enkripsi pembayaran online oleh nasabah ke Bank dengan Algoritma RC4 dan BASE64 [5].

Kemudian penelitian dengan judul Implementasi Aplikasi Website *E-Commerce* Batik Sunda Dengan Menggunakan Protokol *Secure Socket Layer* (*SSL*). Hasil dari penelitian ini adalah pengamanan data yang ada pada setiap transaksi yang dilakukan user dan input data oleh admin dengan *HTTP over SSL* atau yang biasa diimplementasikan dengan *HTTPS* [6].

### 2.1 *E-Commerce*

*E-Commerce* merupakan kepanjangan dari *Electronic Commerce* yang berarti perdagangan yang dilakukan secara elektronik. Seperti halnya *e-mail* (*Electronic Mail*) yang artinya sudah diketahui yaitu pengiriman surat secara elektronik. Dalam buku *Introduction to Information Technology*, *e-commerce* berarti perdagangan elektronik yang mencakup proses pembelian, penjualan, transfer, atau pertukaran produk, layanan, atau informasi melalui jaringan komputer, termasuk Internet [8].

### 2.2 Keamanan Komputer

Keamanan komputer meliputi beberapa aspek diantaranya:

1. *Authentication*: agar penerima informasi dapat memastikan keaslian pesan tersebut datang dari orang yang dimintai informasi. Dengan kata lain informasi tersebut benar-benar dari orang yang dikehendaki.
2. *Integrity*: keaslian pesan yang dikirim melalui sebuah jaringan dan dapat dipastikan bahwa informasi yang dikirim tidak dimodifikasi oleh orang yang tidak berhak dalam perjalanan informasi tersebut.
3. *Nonrepudiation*: merupakan hal yang bersangkutan dengan si pengirim. Si pengirim tidak dapat mengelak bahwa dialah yang mengirim informasi tersebut.
4. *Authority*: informasi yang berada pada sistem jaringan tidak dapat dimodifikasi oleh pihak yang tidak berhak atas akses tersebut.
5. *Confidentiality*: merupakan usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. *Confidentiality* biasanya berhubungan dengan informasi yang diberikan kepada pihak lain.
6. *Privacy*: merupakan lebih ke arah data-data yang sifatnya pribadi.
7. *Availability*: aspek *availability* atau ketersediaan berhubungan dengan ketersediaan informasi ketika dibutuhkan. Sistem informasi yang diserang atau dijebol dapat menghambat atau meniadakan akses ke

Copyright © 2016 SESINDO

informasi. [1]. Pada penelitian ini yang dibahas adalah aspek *Integrity, Authority, Confidentiality, Privacy dan Availability.*

### 2.3 *Database server*

*Database server* merupakan mesin yang berisi database, termasuk tabel, *procedure*, dan *trigger* yang menangani manajemen data, keamanan, dan penanganan kesalahan. *Database server* bertugas melayani permintaan *query database* dari *client.* [7]

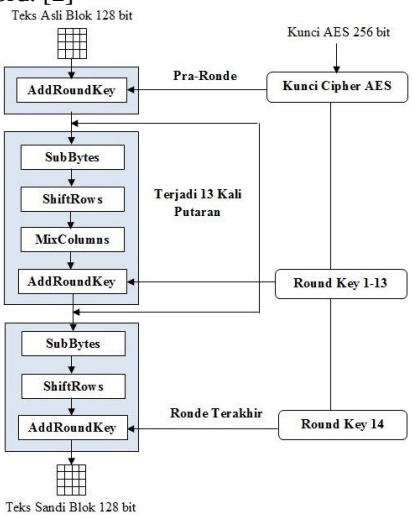
### 2.4 *MySQL*

*MySQL* merupakan standar penggunaan database di dunia untuk pengolahan data. *MySQL* adalah sebuah *server database open source* yang bekerja menggunakan *SQL Language (Structure Query Language)* umumnya digunakan bersama *PHP* untuk membuat aplikasi server yang dinamis dan *powerfull*.
Beberapa fitur yang dimiliki oleh *MySQL* antara lain :

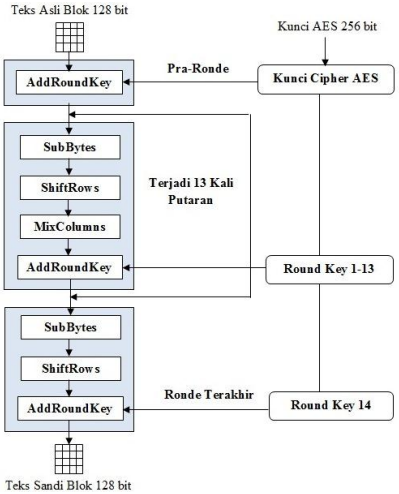
a. *MySQL* termasuk *RDBMS* (*Relationship Database Management System*) yaitu jenis *DBMS* (*Database Management System*) yang mendukung adanya *relationship* atau hubungan antar tabel.
b. *MySQL* memiliki arsitektur *client-server* dimana *server* database *MySQL* terinstal di *server* dan *client MySQL* dapat berada di komputer yang sama dengan *server* atau dapat juga di komputer lain yang berkomunikasi dengan *server* melalui jaringan bahkan *internet*.
c. *MySQL* mendukung *SQL standar*.
d. *MySQL* mendukung *sub select*, *views*, *store procedure*, *trigger*, *replication*, transaksi, dan *foreign key*.
e. *MySQL* tersedia fungsi *GIS*.
f. *MySQL* bersifat *free* (bebas didownload) dan *open source*.
g. *MySQL* stabil, tangguh dan juga bersifat fleksibel dengan berbagai pemrograman.
h. Arsitektur yang sangat baik dengan pilihan berbagai *storage engine*, seperti *MyISAM*, *InnoDB*, *MEMORY*, *BLACKHOLE*, *ARCHIVE* dan lain-lain.
i. *MySQL* memiliki security yang baik dan mendapat dukungan dari banyak komunitas (*AES128*). [7]

### 2.5 *AES* (*Advanced Encryption Standard*) / *RIJNDAEL*

Blok-blok data masukan dan kunci dioperasikan dalam bentuk array. Setiap anggota *array* sebelum menghasilkan keluaran *ciphertext* dinamakan dengan *state*. Setiap *state* akan mengalami proses yang secara garis besar terdiri dari empat tahap yaitu, *AddRoundKey*, *SubBytes*, *ShiftRows*, dan *MixColumns*. Kecuali tahap *MixColumns*, ketiga tahap lainnya akan diulang pada setiap proses sedangkan tahap *MixColumns* tidak akan dilakukan pada tahap terakhir. Proses enkripsi adalah kebalikan dari dekripsi.
Dalam proses enkripsi terjadi beberapa tahap, maka diperlukan *subkey-subkey* yang akan dipakai pada tiap tahap. Pengembangan jumlah kunci yang akan dipakai diperlukan karena kebutuhan *subkey-subkey* yang akan dipakai dapat mencapai ribuan bit, sedangkan kunci yang disediakan secara *default* hanya 128-256 bit. Jumlah total kunci yang diperlukan sebagai *subkey* adalah sebanyak Nb(Nr+1), dimana Nb adalah besarnya blok data dalam satuan *word*. Sedangkan Nr adalah jumlah tahapan yang harus dilalui dalam satuan word. [2]




*Gambar 1. Proses Enkripsi AES 256*




*Gambar 2. Proses Dekripsi AES 256*

Ada empat macam operasi yang dilakukan setiap putaran :

Copyright © 2016 SESINDO

a. Transformasi Subtitusi *Byte*

Dalam operasi ini, setiap *byte* yang akan dienkripsi disubtitusikan dengan nilai *byte* lain dengan menggunakan *S-box. S-box* dibuat dari *multiplicative inverse* dari angka yang diberikan dalam *Rijndael's finite field* yang kemudian ditransformasikan dengan *affine transformation* pada gambar 3 berikut ini :

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

*Gambar 3. Affine Transformation*

Hasilnya kemudian di-*xor* dengan 9910 atau 0x6316 atau 11000112. Operasi matriks dengan *xor* ini ekuivalen dengan persamaan:

$$b'_i = b_i \oplus b_{(i+4)mod8} \oplus b_{(i+5)mod8} \oplus b_{(i+6)mod8} \oplus b_{(i+7)mod8} \oplus c_i \quad (1)$$

dengan b', b, dan c adalah array 8 bit dan nilai c adalah 01100011. Proses tersebut menghasilkan masing-masing nilai dari elemen tabel *S-box* pada Tabel 1. Seperti yang telah diketahui sebelumnya, *AES* merupakan algoritma simetri, yang berarti tabel subtitusi yang dibutuhkan untuk mengenkripsi berbeda dengan untuk mendekripsi. Untuk acuan tersebut, digunakanlah tabel *S-box* inversi seperti pada tabel 2.

Tabel 1. *S-box*

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | a | b | c | d | e | f |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 63 | 7c | 77 | 7b | f2 | 6b | 6f | c5 | 30 | 01 | 67 | 2b | fe | d7 | ab | 76 |
| 1 | ca | 82 | c9 | 7d | fa | 59 | 47 | f0 | ad | d4 | a2 | af | 9c | a4 | 72 | c0 |
| 2 | b7 | fd | 93 | 26 | 36 | 3f | f7 | cc | 34 | a5 | e5 | f1 | 71 | d8 | 31 | 15 |
| 3 | 04 | c7 | 23 | c3 | 18 | 96 | 05 | 9a | 07 | 12 | 80 | e2 | eb | 27 | b2 | 75 |
| 4 | 09 | 83 | 2c | 1a | 1b | 6e | 5a | a0 | 52 | 3b | d6 | b3 | 29 | e3 | 2f | 84 |
| 5 | 53 | d1 | 00 | ed | 20 | fc | b1 | 5b | 6a | cb | be | 39 | 4a | 4c | 58 | cf |
| 6 | d0 | ef | aa | fb | 43 | 4d | 33 | 85 | 45 | f9 | 02 | 7f | 50 | 3c | 9f | a8 |
| 7 | 51 | a3 | 40 | 8f | 92 | 9d | 38 | f5 | bc | b6 | da | 21 | 10 | ff | f3 | d2 |
| 8 | cd | 0c | 13 | ec | 5f | 97 | 44 | 17 | c4 | a7 | 7e | 3d | 64 | 5d | 19 | 73 |
| 9 | 60 | 81 | 4f | dc | 22 | 2a | 90 | 88 | 46 | ee | b8 | 14 | de | 5e | 0b | db |
| a | e0 | 32 | 3a | 0a | 49 | 06 | 24 | 5c | c2 | d3 | ac | 62 | 91 | 95 | e4 | 79 |
| b | e7 | c8 | 37 | 6d | 8d | d5 | 4e | a9 | 6c | 56 | f4 | ea | 65 | 7a | ae | 08 |
| c | ba | 78 | 25 | 2e | 1c | a6 | b4 | c6 | e8 | dd | 74 | 1f | 4b | bd | 8b | 8a |
| d | 70 | 3e | b5 | 66 | 48 | 03 | f6 | 0e | 61 | 35 | 57 | b9 | 86 | c1 | 1d | 9e |
| e | e1 | f8 | 98 | 11 | 69 | d9 | 8e | 94 | 9b | 1e | 87 | e9 | ce | 55 | 28 | df |
| f | 8c | a1 | 89 | 0d | bf | e6 | 42 | 68 | 41 | 99 | 2d | 0f | b0 | 54 | bb | 16 |

Tabel 2. *S-box* Inversi

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | a | b | c | d | e | f |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 52 | 09 | 6a | d5 | 30 | 36 | a5 | 38 | bf | 40 | a3 | 9e | 81 | f3 | d7 | fb |
| 1 | 7c | e3 | 39 | 82 | 9b | 2f | ff | 87 | 34 | 8e | 43 | 44 | c4 | de | e9 | cb |
| 2 | 54 | 7b | 94 | 32 | a6 | c2 | 23 | 3d | ee | 4c | 95 | 0b | 42 | fa | c3 | 4e |
| 3 | 08 | 2e | a1 | 66 | 28 | d9 | 24 | b2 | 76 | 5b | a2 | 49 | 6d | 8b | d1 | 25 |
| 4 | 72 | f8 | f6 | 64 | 86 | 68 | 98 | 16 | d4 | a4 | 5c | cc | 5d | 65 | b6 | 92 |
| 5 | 6c | 70 | 48 | 50 | fd | ed | b9 | da | 5e | 15 | 46 | 57 | a7 | 8d | 9d | 84 |
| 6 | 90 | d8 | ab | 00 | 8c | bc | d3 | 0a | f7 | e4 | 58 | 05 | b8 | b3 | 45 | 06 |
| 7 | d0 | 2c | 1e | 8f | ca | 3f | 0f | 02 | c1 | af | bd | 03 | 01 | 13 | 8a | 6b |
| 8 | 3a | 91 | 11 | 41 | 4f | 67 | dc | ea | 97 | f2 | cf | ce | f0 | b4 | e6 | 73 |
| 9 | 96 | ac | 74 | 22 | e7 | ad | 35 | 85 | e2 | f9 | 37 | e8 | 1c | 75 | df | 6e |
| a | 47 | f1 | 1a | 71 | 1d | 29 | c5 | 89 | 6f | b7 | 62 | 0e | aa | 18 | be | 1b |
| b | fc | 56 | 3e | 4b | c6 | d2 | 79 | 20 | 9a | db | c0 | fe | 78 | cd | 5a | f4 |
| c | 1f | dd | a8 | 33 | 88 | 07 | c7 | 31 | b1 | 12 | 10 | 59 | 27 | 80 | ec | 5f |
| d | 60 | 51 | 7f | a9 | 19 | b5 | 4a | 0d | 2d | e5 | 7a | 9f | 93 | c9 | 9c | ef |
| e | a0 | e0 | 3b | 4d | ae | 2a | f5 | b0 | c8 | eb | bb | 3c | 83 | 53 | 99 | 61 |
| f | 17 | 2b | 04 | 7e | ba | 77 | d6 | 26 | e1 | 69 | 14 | 63 | 55 | 21 | 0c | 7d |

b. Transformasi Pergeseran Baris

Pada operasi ini, *byte-byte* pada setiap baris digeser secara memutar dengan pergeseran yang berbeda dari tiap-tiap baris. Setiap baris digeser dengan aturan tertentu untuk jenis panjang blok yang berbeda. Baris pertama blok untuk semua jenis panjang blok (128, 196, dan 256 bit) tidak digeser. Baris kedua untuk semua jenis panjang blok digeser 1 ke kiri. Pergeseran baris ketiga dan keempat untuk panjang blok 128 dan 196 bit berbeda dengan 256 bit. Pada panjang blok 128 dan 196 bit, baris ketiga digeser ke kiri sebanyak dua kali dan baris keempat digeser ke kiri sebanyak tiga kali. Pada panjang blok 256 bit, baris ketiga digeser ke kiri sebanyak tiga kali dan baris keempat digeser ke kiri sebanyak empat kali. Untuk lebih jelasnya, proses tersebut dapat dilihat pada gambar 4 berikut.

S

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| $S_{0,0}$ | $S_{0,1}$ | $S_{0,2}$ | $S_{0,3}$ | $S_{0,4}$ | $S_{0,5}$ | $S_{0,6}$ | $S_{0,7}$ |
| $S_{1,0}$ | $S_{1,1}$ | $S_{1,2}$ | $S_{1,3}$ | $S_{1,4}$ | $S_{1,5}$ | $S_{1,6}$ | $S_{1,7}$ |
| $S_{2,0}$ | $S_{2,1}$ | $S_{2,2}$ | $S_{2,3}$ | $S_{2,4}$ | $S_{2,5}$ | $S_{2,6}$ | $S_{2,7}$ |
| $S_{3,0}$ | $S_{3,1}$ | $S_{3,2}$ | $S_{3,3}$ | $S_{3,4}$ | $S_{3,5}$ | $S_{3,6}$ | $S_{3,7}$ |

↓

S'

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| $S_{0,0}$ | $S_{0,1}$ | $S_{0,2}$ | $S_{0,3}$ | $S_{0,4}$ | $S_{0,5}$ | $S_{0,6}$ | $S_{0,7}$ |
| $S_{1,1}$ | $S_{1,2}$ | $S_{1,3}$ | $S_{1,4}$ | $S_{1,5}$ | $S_{1,6}$ | $S_{1,7}$ | $S_{1,0}$ |
| $S_{2,3}$ | $S_{2,4}$ | $S_{2,5}$ | $S_{2,6}$ | $S_{2,7}$ | $S_{2,0}$ | $S_{2,1}$ | $S_{2,2}$ |
| $S_{3,4}$ | $S_{3,5}$ | $S_{3,6}$ | $S_{3,7}$ | $S_{3,0}$ | $S_{3,1}$ | $S_{3,2}$ | $S_{3,3}$ |

*Gambar 4. Operasi pada Blok 256 bit*

c. Transformasi Percampuran Kolom

Transformasi ini mengoperasikan blok pada masing masing kolomnya. Setiap kolom diperlakukan sebagai *four-term polynomial* dengan cara *Galois Field (GF*) (28) dan dimodulokan dengan x tetap a(x), yaitu a(x) = {03}x3 + {01}x2 + {01}x + {02} Hal ini dapat dituliskan sebagai perkalian matriks sebagai berikut :

Copyright © 2016 SESINDO

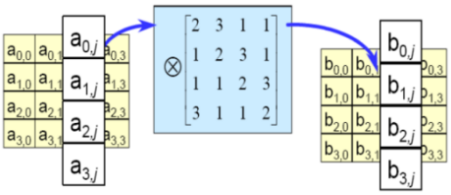
$$s'(x) = a(x) \otimes s(x)$$

$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix} \quad (2)$$

dengan c adalah letak kolom, sehingga hasilnya

$$\begin{aligned} s'_{0,c} &= (\{02\} \bullet s_{0,c}) \oplus (\{03\} \bullet s_{1,c}) \oplus s_{2,c} \oplus s_{3,c} \\ s'_{0,c} &= s_{0,c} \oplus (\{02\} \bullet s_{1,c}) \oplus (\{03\} \bullet s_{2,c}) \oplus s_{3,c} \\ s'_{0,c} &= s_{0,c} \oplus s_{1,c} \oplus (\{02\} \bullet s_{2,c}) \oplus (\{03\} \bullet s_{3,c}) \\ s'_{0,c} &= (\{03\} \bullet s_{0,c}) \oplus s_{1,c} \oplus s_{2,c} \oplus (\{02\} \bullet s_{3,c}) \end{aligned} \quad (3)$$

Transformasi ini dapat diilustrasikan pada gambar 5 berikut ini :



*Gambar 5. Ilustrasi Transformasi Percampuran Kolom*

Operasi transformasi ini tidak digunakan dalam putaran terakhir, baik untuk enkripsi maupun dekripsi.

d. Transformasi Penambahan Kunci

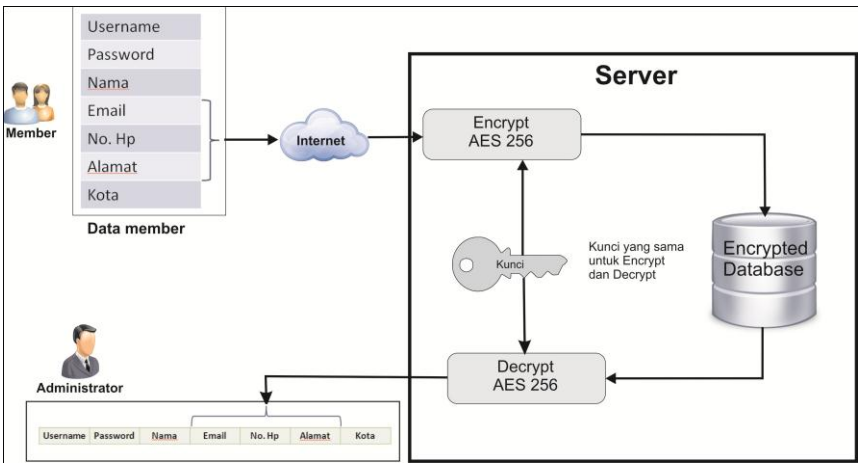
Dalam operasi transformasi ini, digunakanlah upakunci untuk masing-masing putaran yang berasal dari kunci utama dengan menggunakan jadwal kunci *Rijndael* (*Rijndael's key schedule*) yang ukuran upakunci tersebut sama dengan ukuran blok yang akan diproses. Upakunci tersebut kemudian di-*xor* dengan blok input sehingga diperoleh hasilnya.

## 3. PEMBAHASAN

Tahapan yang dilakukan pada sistem enkripsi dan dekripsi terdiri dari :

a. Memilih tabel dan field yang akan di enkripsi. Tabel yang di enkripsi adalah tabel *member* yang berisi *field username*, *password*, nama, *email*, no-hp, alamat, kota.
   *Field password* di enkripsi menggunakan fungsi *Hash MD5*.
   *Field email*, no-hp, alamat di enkripsi menggunakan AES 256, ini yang menjadi inti dari penelitian.
b. Setelah dipilih field email, no-hp dan alamat, maka selanjutnya mengimplementasikan enkripsi *AES* 256 yang prosesnya di gambar 1 pada Form untuk proses memasukkan data member seperti terlihat pada gambar 7.
c. Selanjutnya mengimplementasikan dekripsi *AES 256* yang prosesnya di gambar 2, diterapkan pada halaman administrator pada menu lihat data member.

Bagan cara kerja proses enkripsi dan dekripsi menggunakan *AES 256* pada *E-Commerce* bisa dilihat pada gambar 6 berikut ini :




*Gambar 6. Cara kerja sistem enkripsi dan dekripsi pada e-Commerce*

Copyright © 2016 SESINDO

Tampilan *form* registrasi member pada gambar 6. Pada form ini user memasukkan data pribadi yang diperlukan, yang kemudian akan disimpan pada tabel member dengan proses enkripsi *AES 256*.


*Gambar . Form Registrasi Member*

Tabel *Member* yang terenkripsi pada *field email*, ho-hp dan alamat sebagian tampilan datanya bisa dilihat pada gambar 7.

| nama_lengkap | email | aktivasi | cek_aktivasi |
|---|---|---|---|
| Kartika Imam santoso | 80aCQ5lrddbkisjkKD3HKCkDhyp+88a4mzIQngxXH74=\|aZx49... | 123456 | 123456 |
| wahyu pyiyoatmoko | x2P9+oxjEP3RRuDJsbxlvxmhRHhUBDWyikId+8G+kiA=\|tLJBS... | 123456 | 123456 |
| M Abdul Muin | 37m+sz+J+HBYCWOr+2yUeblxL6rXHPDulgQN8UTSF8s=\|ZQsfw... | 123456 | 123456 |

| no_telp | alamat | kota |
|---|---|---|
| 6nlivUQjO9AbOsNIzhyMJ/DED/Opl+sVWSBqnloVlY0=\|bRQKO... | NTu83032XF57pcgDs1z7EZQuslCsIYu4ZvO9i5rRu+vADpWi4Z... | Kab Grobogan |
| n5lkf/xSMfZfXrEuR1q1vqsPxoAcv/vnvAuBi1V2qRQ=\|mYWS+... | SgmzmAMQuqa2HHbHUyf8BCdz+rRbjIBhRKkfdCGwgul=\|iKvzl... | Magelang |
| MVZX8RSXY7L3LGFuixzXW4ZhEwDn4wTo6BPuANkd87M=\|ae/yK... | lZchoRPgnM2xNgJ8T/dyqjlvDsnTnLzSMmlD9/E6l/Y=\|TTSNi... | Magelang |

*Gambar 7. Tampilan data pada Tabel Member*

Berdasarkan hasil percobaan dengan enkripsi *AES 256* ditemukan hasil bahwa hasil enkripsi dengan kunci statis atau tetap, dihasilkan *ciphertext* yang berbeda-beda. Hal ini tentu saja akan mempersulit kriptanalisis untuk mengetahui isi data dan mencari pola dari enkripsi.

## 4. SIMPULAN DAN SARAN

Berdasarkan penelitian yang telah dilakukan yaitu proses enkripsi dan dekripsi menggunakan *AES 256* pada data *E-Commerce* pada *database MySQL* maka :

### 4.1 Simpulan

a. Hasil dari penelitian ini adalah Enkripsi dengan *AES 256* pada data *MySQL E-Commerce* yang menghasilkan *ciphertext* yang tidak sama meskipun kuncinya sama (statis).
b. Penerapan Enkripsi dengan *AES 256* pada *MySQL* untuk *E-Commerce* sulit untuk dibuat dibaca polanya oleh kriptanalisis.
c. Enkripsi dengan *AES 256* pada data *MySQL* pada *E-Commerce* menjadikan data konsumen menjadi lebih aman dari pihak-pihak yang ingin mendapatkannya, misalnya *Hacker* atau pesaing bisnis.

### 4.2 Saran

a. Agar *AES 256* bisa diterapkan tidak hanya pada *database E-Commerce* saja, tetapi pada aplikasi lainnya.
b. Agar bisa dikembangkan agar kunci tidak statis, tetapi menjadi kunci dinamis.
c. Agar bisa dikembangkan ke bit yang lebih tinggi lagi misal *AES 512*, sehingga menjadi lebih kuat hasil enkripsinya.

Copyright © 2016 SESINDO

## 5. DAFTAR RUJUKAN


[1] Ariyus, D., 2006. *Computer Security*. Yogyakarta : Penerbit Andi.

[2] Dharmawan, E.A., 2013). Perlindungan Web pada Login Sistem Menggunakan Algoritma Rijndael. Jurnal EECCIS, 7(1) : pp.77-84.

[3] Digdo, G.P., 2012. Analisis Serangan dan Keamanan pada Aplikasi Web. Jakarta: Elex Media Komputindo.

[4] Fauziah dan Agustina, I., 2008. Analisis dan Perancangan Prototype Aplikasi *Colaborative Commerce*. KOMMIT (Seminar Ilmiah Nasional Komputer dan Sistem Intelijen), Depok, 20-21 Agustus 2008. Indonesia.

[5] Christanto, F.W., Rahangiar A.P., De Fretes F. 2012. Penerapan Algoritma Gabungan RC4 dan Base 64 pada Sistem Keamanan e-Commerce. SNATI (Seminar Nasional Aplikasi Teknologi Informasi). Yogyakarta, 15-16 Juni 2012. Indonesia

[6] Rosmala, D., Djatmiko, M.D., Julianto, B., 2012. Implementasi Aplikasi Website E-Commerce Batik Sunda Dengan Menggunakan Protokol *Secure Socket Layer* (SSL). Jurnal Informatika. 3 (3). pp.58-67

[7] Saputra, A., 2011. Panduan Praktis Menguasai Database Server MySQL. Jakarta: PT. Elex Media Komputindo.

[8] Turban, E., Rainer, R.K.Jr., Potter, R.E., 2005. *Introduction to Information Technology*, New York: John Wiley & Sons, Inc

[9] Aleisa, N., 2015. *A Comparison of the 3DES and AES Encryption Standards*. *International Journal of Security and Its Applications*. 9 (7), pp.241-246

[10] Basharat, I., Azam, F., Muzaffar, A.W., 2012. Database *Security and Encryption : A Survey Study*. *International Journal of Computer Applications. 47 (12), pp.28-34*


Copyright © 2016 SESINDO

*Halaman ini sengaja dikosongkan*

Copyright © 2016 SESINDO