

IDENTITAS PENULIS

Data Pribadi

Nama : Alex Gufron
Tempat/Tanggal Lahir : Pati, 11 Juli 1994
Jenis Kelamin : Laki-laki
Agama : Islam
Status : Belum Menikah
Kewarganegaraan : Indonesia
Alamat : Jl. Buaran II No.32A RT.09/013 Klender Duren
Sawit Jakarta Timur, 13470
No. Telepon/HP : 087781734927
Email : alex.gufron@esaunggul.ac.id



Riwayat Pendidikan

TK : RA. Al-Wathoniyah 05, Jakarta Timur (1999-2000)
SDN : SDN Cipinang 03 Pagi, Jakarta Timur (2000-2006)
SMP : MTS Ummul Quro Al-Islami, Bogor (2006-2009)
SMA : MA Ummul Quro Al-Islami, Bogor (2009-2012)
Pesantren : Pesantren Modern Ummul Quro Al-Islami (2006-2012)
Universitas : Universitas Esa Unggul, Program Studi Teknik Informatika (2013-Sekarang)

Riwayat Organisasi Internal Kampus

LDK IKMI : Ketua Dept. Syiar Periode 2014-2015
Ketua LDK IKMI Periode 2015-2016
BEM FASILKOM : Anggota Div. Keagamaan Periode 2014-2015
BEM Universitas : Sekretaris Jendral Periode 2016-2017
FALCER : Koordinator External Komunitas Periode 2015-2016

Riwayat Organisasi External Kampus

YBNJ : Sekretaris Yayasan Bhakti Nurul Jannah Periode 2012-2015
FSLDK JADEBEK : Anggota Komisi A bid. Syiar Agama Periode 2015-2017

Prestasi

PKM-DIKTI : Lolos Pendanaan Program Kreatifitas Mahasiswa-DIKTI
Kategori Karsa Cipta tahun 2014
ICT Smart City : Lolos nominasi pertama *ICT Smart City*
Institut Teknologi Bandung (ITB) tahun 2015
Indigo : Lolos nominasi pertama *Indigo Digital Nation* tahun 2016
MTQMN XV : Lolos nominasi 50 besar Aplikasi Islami tahun 2017
KRTI 2017 : Lolos nominasi 20 besar kategori Inovasi Teknologi Kontes
Robot Terbang tahun 2017

SURAT KETERANGAN PENELITIAN

a) Surat keterangan dari Fakultas



Jakarta, 18 Juli 2017

Nomor : 40/SP/KAPRODI-TIF/FASILKOM/EXT/VII/2017
Lampiran : -
Perihal : Surat Permohonan Izin Untuk Penelitian

Kepada Yth.
KASATLAK PRIMA
Team IAM PRIMA
Gedung PPITKON (KEMENPORA)
Jl. Gerbang Pemuda No. 3 RT. 1 RW. 3
Senayan, Tanah Abang
Jakarta Pusat, 10270

Dengan hormat,

Sehubungan dengan mata kuliah Tugas Akhir yang memerlukan data dan informasi bagi mahasiswa Fakultas Ilmu Komputer Program Studi Teknik Informatika, bersama ini kami sampaikan bahwa mahasiswa kami bermaksud untuk mencari beberapa data / informasi. Adapun nama mahasiswa tersebut adalah :

Nama : Alex Gufron
NIM : 2013-81-039

Demikianlah atas perhatian dan kerjasamanya, kami ucapkan terima kasih.

Hormat kami,



Universitas
Esa Unggul
FAKULTAS ILMU KOMPUTER
TEKNIK INFORMATIKA
Bambang Irawan, S.Kom, M.Kom
Ketua Program Studi Teknik Informatika

C.c : 1. Arsip.

b) Surat balasan dari IAM PRIMA



PROGRAM INDONESIA EMAS

Jakarta, 06 September 2017

Nomor : 723/PRIMA/IX/2017
Lampiran :
Perihal : **Penyelesaian Tugas Akhir
di Satlak Prima**

Kepada Yth
Ketua Program Studi Teknik
Informatika – Fakultas Ilmu
Komputer Teknik Informatika
UNIVERSITAS ESA UNGGUL
di
Jakarta

Dengan hormat,

Menunjuk surat saudara No. 40/SP/KAPRODI-TIF/FASILKOM/EXT/VI/2017 tanggal 18 Juli 2017 perihal Surat Permohonan Izin Untuk Penelitian, dengan ini disampaikan bahwa telah selesai melaksanakan tugas mencari data untuk Penelitian sehubungan dengan mata kuliah Tugas Akhir yang bersangkutan pada instansi kami Satlak PRIMA, pada bulan Juli 2017, Mahasiswa **Universitas Esa Unggul** atas nama :

Nama : **Alex Gufron**
Nim : **2013-81-039.**

Harapan kami, semoga hasil penelitian disamping bermanfaat bagi yang bersangkutan, apabila dari hasil penelitian terdapat temuan yang dapat meningkatkan system yang ada, bisa dinformasikan kepada Satlak PRIMA.

Demikian disampaikan, atas kerjasamanya diucapkan terima kasih

**Satuan Pelaksana Program Indonesia Emas
Ketua,**


Achmad Soetjipto
Laksamana TNI (Purn)

ALAMAT : GEDUNG PP-ITKON, KOMPLEK KEMENPORA
Jalan Gerbang Pemuda No. 3, Senayan, Jakarta 10270
Telp. (021) 5703915, Fax. (021) 5703915
E-mail : satlak.prima@gmail.com

SCRIPT ALGORITMA AES 128-bit

a) Fungsi enkripsi dan dekripsi

Fungsi enkripsi

```
<?php if ( ! defined('BASEPATH')) exit('No direct script access allowed');
```

```
if ( ! function_exists('initEn')){  
function initEn()  
{  
    $CI =& get_instance();  
    $CI->encryption->initialize(  
        array(  
            'cipher' => 'aes-128',  
            'mode' =>  
'CBC|CTR|CFB|CFB8|OFB|ECB|XTS',  
            'key' => 'apaajalah12345'  
        )  
    );  
    return $CI->encryption;  
}  
}
```

```
if ( ! function_exists('getEnc'))  
{  
    function getEnc($str)  
    {  
        return initEn()->encrypt($str);  
    }  
}
```

```
if ( ! function_exists('getDnc'))  
{  
    function getDec($str)  
    {  
        return initEn()->decrypt($str);  
    }  
}
```

Fungsi dekripsi

```
<?php if ( ! defined('BASEPATH')) exit('No direct script access allowed');
```

```
if ( ! function_exists('initEn')){  
function initEn()  
{
```

```

    $CI =& get_instance();
    $this->encryption->decrypt(
    $ciphertext,
    array(
        'cipher' => 'aes-128',
        'mode' => 'CBC|CTR|CFB|CFB8|OFB|ECB|XTS',
        'key' => 'apaajalah12345'
        'hmac_digest' => 'sha224'
        'hmac_key' => 'apaajalah12345'
    ));
    return $CI->decryption;
}
}

if ( ! function_exists('getEnc'))
{
    function getEnc($str)
    {

        return initEn()->encrypt($str);

    }
}

if ( ! function_exists('getDnc'))
{
    function getDec($str)
    {

        return initEn()->decrypt($str);

    }
}

```

b) Proses konversi data ke JSON

```

$('#modalPesan').on('show.bs.modal', function (event) {
    var button = $(event.relatedTarget); // Button that triggered
    the modal
    var recipient = button.data('whatever'); // Extract info from
    data-* attributes
    // If necessary, you could initiate an AJAX request here (and
    then do the updating in a callback).
    // Update the modal's content. We'll use jQuery here, but you
    could use a data binding library or other methods instead.
    //console.log(recipient);
    var json_data = {
        "accessID" : recipient,

```

```

    };
    var modal = $(this);
    $.ajax({
        type: "GET",
        dataType: "json",
        url: "http://localhost/kedaiderst/index.php/customer/get_pesanan",
        data: {json_data: JSON.stringify(json_data)},
        beforeSend: function() {
            $('#pesanan_loading').show();
        },
        success: function(data) {
            $('#pesanan_loading').hide();

            var arrmodal= modal.find('.item-list');
            arrmodal.empty();
            for(var i =0; i<data.result_barang.length;
i++)
            {
                var n = i+1;
                arrmodal.append("<tr> <td>"+
n +"</td><td><img class='bayar-gambar'
src='http://localhost/kedaiderst/uploads/'+ data.result_barang[i].gambar
+'"/></td> <td>"+ data.result_barang[i].nama_barang +"</td><td>"+
data.result_barang[i].harga_barang +"</td><td>"+
data.result_barang[i].banyak +"</td><td>"+
data.result_barang[i].banyak*data.result_barang[i].harga_barang
+"</td></tr>");
            }
            arrmodal.append("<tr><td
colspan='5'><b>Biaya
Pengiriman</b></td><td>"+data.biaya_pengiriman+"</td></tr>");
            arrmodal.append("<tr><td
colspan='5'><b>Total
Keseluruhan</b></td><td><b>"+data.total+"</b></td></tr>");
            modal.find('.status-
lunas').removeClass("label-danger");
            modal.find('.status-
lunas').removeClass("label-success");
            if(JSON.stringify(data.status_lunas) ===
JSON.stringify("Lunas"))

```

```

        modal.find('.status-
lunas').addClass("label-success");
    else
        modal.find('.status-
lunas').addClass("label-danger");

    modal.find('.status-
lunas').text("+data.status_lunas+");

    modal.find('.token').html('<b>'+data.token+'</b>');
    modal.find('.tanggal-
pemesanan').text("+data.tanggal_pesanan+");
    modal.find('.kota-
pemesanan').text("+data.nama_kota+");

    modal.find('.alamat').text("+data.alamat+");
    }
});
});

```

c) **Proses link data ke enkripsi**

```

<table id="table_data" class="table table-hover">
    <thead>
        <tr>
            <th>No.</th>

            <th>Tanggal Pesanan</th>
            <th>Total Harga</th>
            <th>Token</th>
            <th>Status</th>
            <th>Detail</th>
        </thead>
        <tbody>
            <?php
                $n = 0;
                if($num_pesanan == 0)
                {
                    echo "<h3>Anda Belum Melakukan
                    Transaksi</h3>";
                }
                else{
                    foreach($result_pesanan as $row){
                        $n++;
                        if($row->status_lunas == 'Y')
                        {
                            $ststatus = "label-success";
                            $status = "Lunas";
                        }
                    }
                }
            }
        }
    }

```

```

else
{
    $status = "Belum Lunas";
    $ststatus = "label-danger";
}

?>
<tr>

<td><?php echo $n;?></td>
<td><?php echo tgl_indo($row->tanggal_pesanan);?></td>

<td><?php echo rupiah($row->total_harga);?></td>
<td><?php echo $row->token;?></td>

<td><?php echo "<span class='label
".$ststatus."'>".$status."</span>";?></td>
<td>
<!--<button class="btn btn-success"
onclick="window.location.href='<?php echo
site_url('customer/pembayaran/'.getEnc($row->kode_pesanan)); ?>'><i
class="fa fa-share-square-o"></i></button>-->
<button type="button" class="btn btn-success" data-toggle="modal" data-
target="#modalPesan" data-whatever="<?php echo getEnc($row-
>kode_pesanan); ?>'><i class="fa fa-share-square-o"></i></button>
</td>
</tr>
<?php }
}?>
</tbody>
</table>

```

d) Proses hasil enkripsi dan dekripsi

Proses hasil enkripsi

```

public function checkout_proses()
{

```

```

    $token = strtoupper(substr($this->random_val()."date('m1d')." . $this-
>random_val(),2, 11));

```

```

    $kota_pengiriman = explode("-", $_POST['kota_pengiriman']);

```

```

    $biaya_pengiriman = $kota_pengiriman[0];

```

```

    $kode_kota = $kota_pengiriman[1];

```

```

    $_SESSION['total'] += $biaya_pengiriman;

```

```

    $indata = array(
        "tanggal_pesanan" => date('Y-m-d'),

```



```

        "token" => $token,
        "total_harga" => $_SESSION['total'],
        "kode_customer" =>
$_SESSION['kode_customer'],
        "alamat" => $_POST['alamat'],
        "kode_kota" => $kode_kota
    );
    $this->ModelsKedai->insert("pesanan", $indata);

    $wh_data = array(
        "tanggal_pesanan" => $indata['tanggal_pesanan'],
        "token" => $token,
        "kode_customer" => $indata['kode_customer']
    );

    $pesanan_q = $this->ModelsKedai->select_arr('pesanan',$wh_data);
    $kode_pesanan = $pesanan_q->row()->kode_pesanan;

    foreach($_SESSION['cart'] as $cart)
    {
        $dt_data = array(
            "banyak" => $cart['banyak'],
            "kode_barang" => $cart['kode_barang'],
            "kode_pesanan" => $kode_pesanan
        );

        $this->ModelsKedai->insert("detail_pesanan", $dt_data);
    }
    unset($_SESSION['cart']);
    unset($_SESSION['total']);
    initEn();
    redirect("customer/pembayaran?x=".getEnc($kode_pesanan));
}

```

Proses hasil dekripsi

```

public function get_pesanan()
{
    initEn();
    $data_json = json_decode($_GET['json_data'], true);
    $kode_pesanan = getDec($data_json['accessID']);
    $bayar_q = $this->db->query("select * from barang,
detail_pesanan where barang.kode_barang = detail_pesanan.kode_barang
and detail_pesanan.kode_pesanan = '".$kode_pesanan."'");
}

```

```

$pesanan_r = $this->ModelsKedai-
>select_where("pesanan"."kode_pesanan", $kode_pesanan)->row();
$biaya_pengiriman_r = $this->ModelsKedai-
>select_where("kota_pengiriman"."kode_kota",$pesanan_r->kode_kota)-
>row();
    $data['biaya_pengiriman'] = $biaya_pengiriman_r-
>biaya_pengiriman;
    $data['nama_kota'] = $biaya_pengiriman_r->nama_kota;
    $data['result_barang'] = $bayar_q->result();
    $data['total'] = rupiah($pesanan_r->total_harga);
    $data['token'] = $pesanan_r->token;
    $data['token'] = $pesanan_r->token;
    $data['alamat'] = $pesanan_r->alamat;
    $data['tanggal_pesanan'] = tgl_indo($pesanan_r->tanggal_pesanan);
    if($pesanan_r->status_lunas == 'N')
        $data['status_lunas'] = 'Belum Lunas';
    else
        $data['status_lunas'] = 'Lunas';
        $json_out = json_encode($data);
        echo $json_out;
}

```

***Script* Algoritma Implementasi IAM PRIMA**

a) Inisiasi fungsi pada script koding

```
<?php if ( ! defined('BASEPATH')) exit('No direct script access allowed');
//nama class harus sama dengan nama file dan diawali dengan huruf besar
class Home extends CI_Controller {
    function __construct()
    {
        parent::__construct();
        $this->load->database();
        $this->load->library('session');
        $this->load->helper(array('form', 'url'));
        $this->load->model('ModelActivityUser');
        date_default_timezone_set('Asia/Jakarta');

        if(!$this->session->userdata("login")){
            redirect("login/form");
        }
    }
    function index(){
        $session = $this->session->userdata("login");
        $name      = $session["name"];
        $username   = $session["username"];
        $gambar     = $session["gambar"];
        $role_type  = $session["role_type"];
        $role_name  = $session["role_name"];
        $group_id   = $session["group_id"];
        $this->ModelActivityUser-
>setActivityUser($username,6,4);
        $data["gambar"] = $gambar;
        $data["name"] = $name;
        $data["username"] = $username;
        $data["role_type"] = $role_type;
        $data["role_name"] = $role_name;
        $data["page"] = "home/home";
        $this->load->view("layout",$data);
    }
    public function logout(){
        $session = $this->session->userdata("login");
```

```

        $name = $session["name"];
        $username = $session["username"];
        $this->ModelActivityUser-
>setActivityUser($username,2,7);
        $this->load->library('session');
        $this->load->helper('url');
        $this->session->unset_userdata('login');
        redirect('home','refresh');
    }

```

b) Fungsi enkripsi dan dekripsi

```

//NAMBAHIN YANG DARI GUFRON
    public function mysql_aes_key($key)
    {
        $new_key = str_repeat(chr(0), 16);
        for($i=0,$len=strlen($key);$i<$len;$i++)
        {
            $new_key[$i%16] = $new_key[$i%16] ^ $key[$i];
        }
        return $new_key;
    }
    public function aes_encrypt($val)
    {
        $key = mysql_aes_key('Ralf_S_Engelschall__trainofthoughts');
        $pad_value = 16-(strlen($val) % 16);
        $val = str_pad($val, (16*(floor(strlen($val) / 16)+1)),
chr($pad_value));
        return mcrypt_encrypt(MCRYPT_RIJNDAEL_128, $key, $val,
MCRYPT_MODE_ECB, mcrypt_create_iv(
mcrypt_get_iv_size(MCRYPT_RIJNDAEL_128,
MCRYPT_MODE_ECB), MCRYPT_DEV_URANDOM));
    }
    public function aes_decrypt($val)
    {
        $key = mysql_aes_key('Ralf_S_Engelschall__trainofthoughts');
        $val = mcrypt_decrypt(MCRYPT_RIJNDAEL_128, $key, $val,
MCRYPT_MODE_ECB, mcrypt_create_iv(
mcrypt_get_iv_size(MCRYPT_RIJNDAEL_128,
MCRYPT_MODE_ECB), MCRYPT_DEV_URANDOM));
    }

```

```

        return rtrim($val, "..16");
    }
c) Proses hasil enkripsi dan dekripsi
    public function random_val()
    {
        return substr(md5(uniqid(rand(), true)), 0, 5);
    }

    public function getEncription($str)
    {
        initEn();
        //return getEnc($str);
        echo getEnc($str);
    }

    public function getDecription()
    {
        $enc = $_GET['x'];
        initEn();
        //return getDec($str);
        echo getDec($enc);
    }
}

```