



Hari/Tanggal :

Senin / 02.11.2020

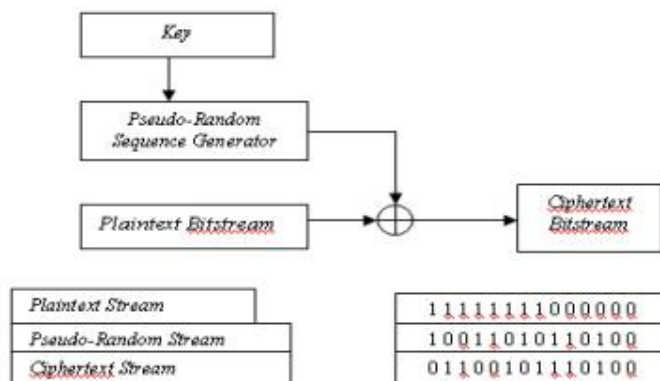
Ruang :

Lab RPL

Dosen : Fiddin Yusfida A'la,
S.T., M.Eng.

LAPORAN PRAKTIKUM

A. DASAR TEORI



Saat ini kebutuhan database semakin besar dan kompleks, secara otomatis akan diikuti dengan kebutuhan akan keamanan terhadap data yang tersimpan dari berbagai ancaman yang dapat berupa pengaksesan, perubahan serta perusakan data oleh pihak/user yang tidak mempunyai kewenangan. Terdapat beberapa level keamanan pada database, diantaranya: keamanan sistem operasi, keamanan sistem manajemen database, keamanan fisik dan keamanan dari segi user/manusia. Untuk menambah tingkat keamanan dapat dilakukan dengan cara mengimplementasikan kriptografi untuk melindungi query yang dikirimkan dan hasil query yang akan diterima selama keduanya berada dalam jaringan komputer. Algoritma kriptografi yang digunakan adalah RC4.

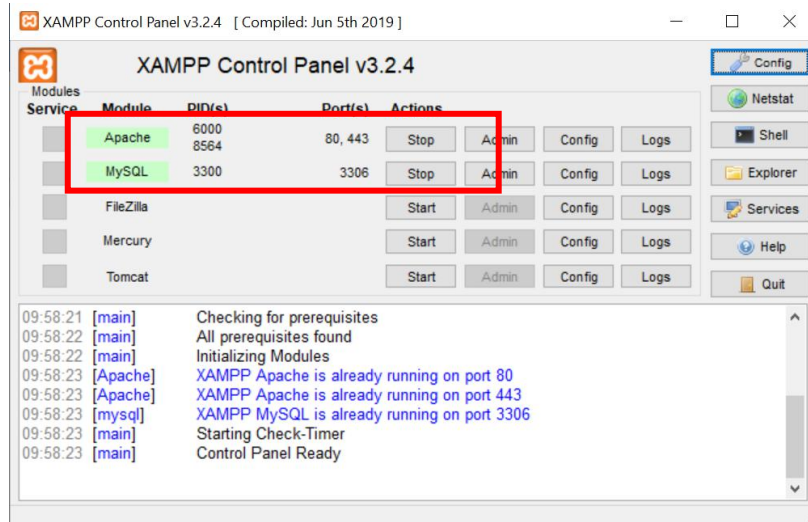
Algoritma kriptografi Rivest Code 4 (RC4) merupakan salah satu algoritma kunci simetris yang dibuat oleh RSA Data Security Inc (RSADSI). RC4 dipilih sebagai metode kriptografi karena proteksi query dan hasil query berdasarkan pada beberapa hal, yaitu:

1. Pengamanan transmisi database memerlukan suatu proses yang cepat, maka algoritma kriptografi simetris adalah solusi yang tepat.
2. RC4 merupakan algoritma stream cipher yang paling tepat dibandingkan dengan algoritma stream cipher yang lain untuk masalah transmisi query database seperti ini. Hal ini dikarenakan RC4 memiliki proses enkripsi yang cukup sederhana dan hanya melibatkan beberapa operasi saja per byte-nya.

Dengan menggunakan algoritma RC4, diharapkan dapat meningkatkan tingkat keamanan transmisi data tanpa mengurangi performansi database secara signifikan.

B. LANGKAH-LANGKAH PRAKTIKUM

1. Jalankan server XAMPP dan buka aplikasi code editor, disini saya menggunakan Sublime Text



2. Selanjutnya buka code editor, dan buat file.php dengan nama index.php. Index.php ini akan menampilkan halaman yang pertama kali di akses

```
EXPLORER
...
index.php X
index.php
1 <html>
2 <head>
3 <title>FORM ENKRIPSI</title>
4 </head>
5 <body>
6 <form action="enkripsi.php" method="get">
7 <div style="text-align: center;"><span style="font-weight:
8 bold;">FORM ENKRIPSI</span>
9 </div>
10 Plainteks :
11 <br>
12 <textarea cols="50" rows="6" name="kata"
13 maxlength="255">
14 </textarea>
15 <br>
16 Key :
17 <input type="text" name="key" maxlength="16">
18 <br>
19 <input type="submit" value="Kirim">
20 <input type="reset" value="Reset">
21 <br>
22 <br>
23 Go to : <a href="form_dekripsi.php">FORM DEKRIPSI</a><br>
24 </form>
25 </body>
26 </html>
```

Pada file index.php ini berisi sebuah form yang didalamnya untuk menulis plainteks yang akan di enkripsi dan kuncinya serta diberikan action "form_dekripsi" untuk mengarah ke halaman berikutnya.

3. Selanjutnya buat file enkripsi.php dan menambahkan fungsi untuk permutasi acak S-Box.

```

1  <?php
2  error_reporting(0);
3  function setupkey()
4  { /*proses pengacakan kunci SBox*/
5      echo "<br>";
6      $kce = $_GET["key"];
7      echo "Kunci enkripsi = $kce";
8      echo "<br>";
9      //strlen => hitung jumlah string, ord => ngembaliin nilai unicode dari string karakter
10     for ($i = 0; $i < strlen($kce); $i++) {
11         $key[$i] = ord($kce[$i]); /*rubah ASCII ke desimal*/
12     }
13     global $m;
14     $m = array();
15     /*Proses inisialisasi S-Box (Array S) => array 256*/
16     for ($i = 0; $i < 256; $i++) {
17         $m[$i] = $i;
18     }
19
20     $j = $k = 0;
21     //proses pengacakan S-Box =>permutasi fungsi dan kunci
22     for ($i = 0; $i < 256; $i++) {
23         $a = $m[$i];
24         $j = ($j + $m[$i] + $key[$k]) % 256;
25         $m[$i] = $m[$j];
26         $m[$j] = $a;
27         $k++;
28         if ($k > 15) {
29             $k = 0;
30         }
31     }

```

- Pada script diatas, kunci “key” yang berada di form di GET untuk mengirimkan value/nilai, setelah itu key inputan akan dihitung jumlah stringnya dalam bentuk perulangan menggunakan fungsi “strlen” dan diubah dari ASCII ke desimal, selanjutnya masuk ke proses inisialisasi S-Box yang pertama menggunakan array dengan ukuran 256 bytes yang berisi permutasi bilangan 0-255.
- Selanjutnya proses pengecekan kedua yaitu dengan permutasi fungsi dan kunci menggunakan perulangan for.

Selanjutnya tambahkan script untuk melakukan enkripsi

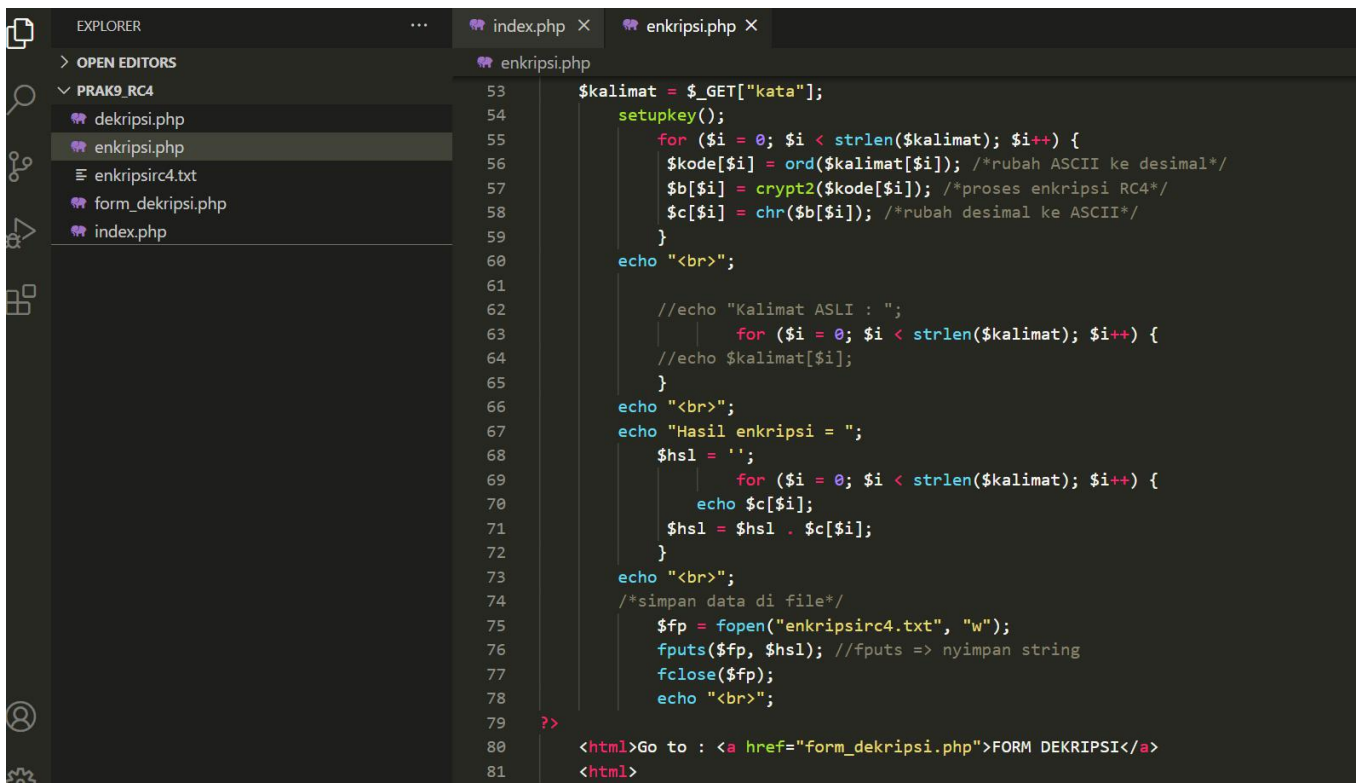
```

31     }
32 }
33
34
35 function crypt2($inp)
36 { //pembangkitan kunci
37     global $m;
38     $x = 0;
39     $y = 0;
40     $bb = '';
41     $x = ($x + 1) % 256;
42     $a = $m[$x];
43     $y = ($y + $a) % 256;
44     $m[$x] = $b = $m[$y];
45     $m[$y] = $a;
46     /*proses XOR antara plaintext dengan kunci
47     dengan $inp sebagai plaintext
48     dan $m sebagai kunci*/
49     $bb = ($inp ^ $m[(($a + $b) % 256)]) % 256; //^ adalah xor
50     return $bb;
51 }

```

Selanjutnya masuk ke perhitungan XOR antara plaintext dengan kunci dan \$inp itu sebagai plaintext nya serta \$m sebagai key.

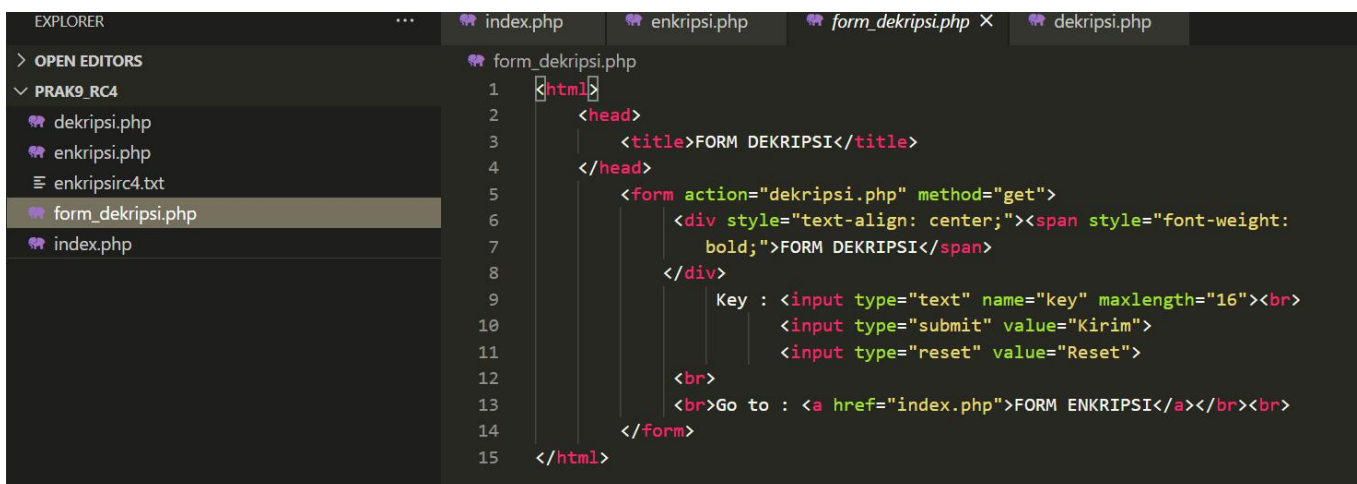
Selanjutnya tambah script untuk menampilkan pesan hasil dari enkripsi



```
53 $kalimat = $_GET["kata"];
54 setupkey();
55 for ($i = 0; $i < strlen($kalimat); $i++) {
56     $kode[$i] = ord($kalimat[$i]); /*rubah ASCII ke desimal*/
57     $b[$i] = crypt2($kode[$i]); /*proses enkripsi RC4*/
58     $c[$i] = chr($b[$i]); /*rubah desimal ke ASCII*/
59 }
60 echo "<br>";
61
62 //echo "Kalimat ASLI : ";
63 for ($i = 0; $i < strlen($kalimat); $i++) {
64     //echo $kalimat[$i];
65 }
66 echo "<br>";
67 echo "Hasil enkripsi = ";
68 $hsl = '';
69 for ($i = 0; $i < strlen($kalimat); $i++) {
70     echo $c[$i];
71     $hsl = $hsl . $c[$i];
72 }
73 echo "<br>";
74 /*simpan data di file*/
75 $fp = fopen("enkripsirc4.txt", "w");
76 fputs($fp, $hsl); //fputs => nyimpan string
77 fclose($fp);
78 echo "<br>";
79
80 <html>Go to : <a href="form_dekripsi.php">FORM DEKRIPSI</a>
81 </html>
```

- Selanjutnya value “kata” di GET yang berasal dari form inputan di index.php, lalu masuk ke perhitungan string menggunakan strlen dan merubah dari ASCII ke desimal selanjutnya proses enkripsi RC4 dan dirubah lagi dari desimal ke ASCII seperti semula, lalu di print.
- Selanjutnya hasil file proses enkripsi RC4 di tulis menggunakan perintah “fopen => w” dan “fputs” untuk di simpan dalam bentuk string (enkripsirc4.txt) selanjutnya “fclose” ini untuk menutup file yang sudah tidak diproses lagi.

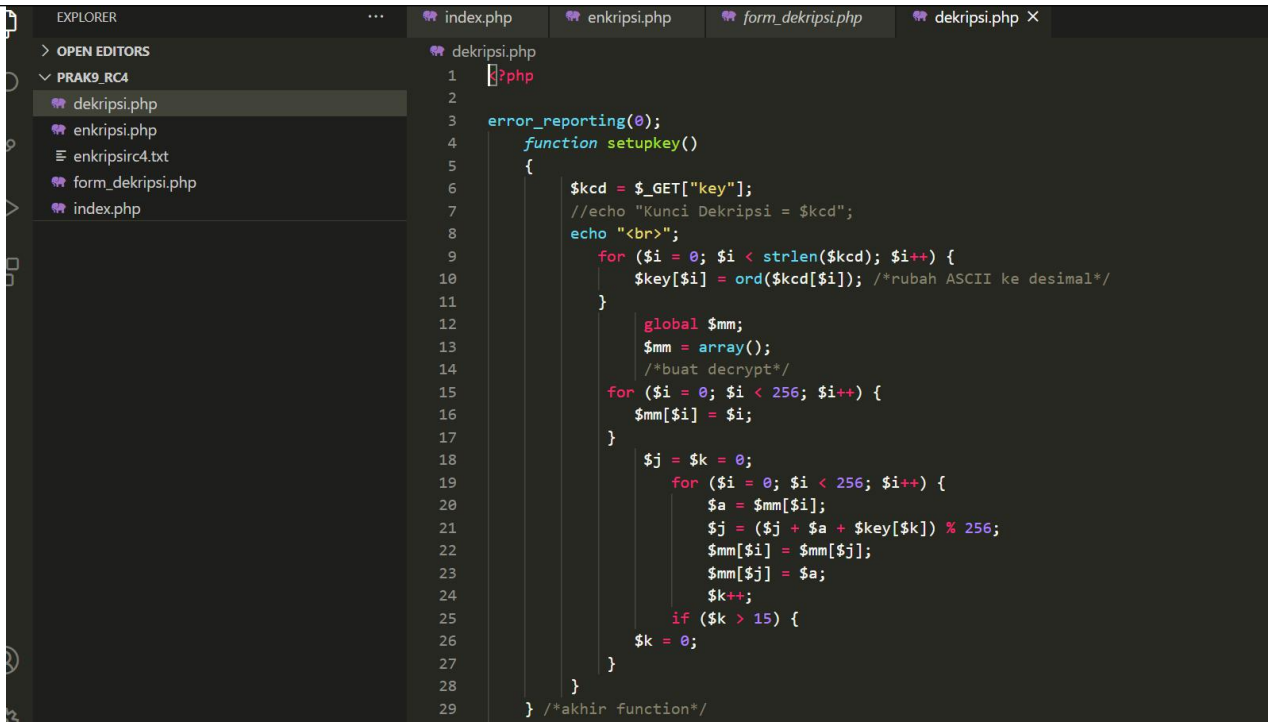
4. Selanjutnya buat file untuk form dekripsi



```
1 <html>
2 <head>
3     <title>FORM DEKRIPSI</title>
4 </head>
5 <form action="dekripsi.php" method="get">
6     <div style="text-align: center;"><span style="font-weight:
7         bold;">FORM DEKRIPSI</span>
8     </div>
9     Key : <input type="text" name="key" maxlength="16"><br>
10         <input type="submit" value="Kirim">
11         <input type="reset" value="Reset">
12     <br>
13     <br>Go to : <a href="index.php">FORM ENKRIPSI</a></br><br>
14 </form>
15 </html>
```

File diatas berisi sebuah form untuk inputan yang berisi kunci dan tombol kirim serta tombol reset untuk mengulang. Di akhir terdapat action “dekripsi.php” untuk proses dekripsi.

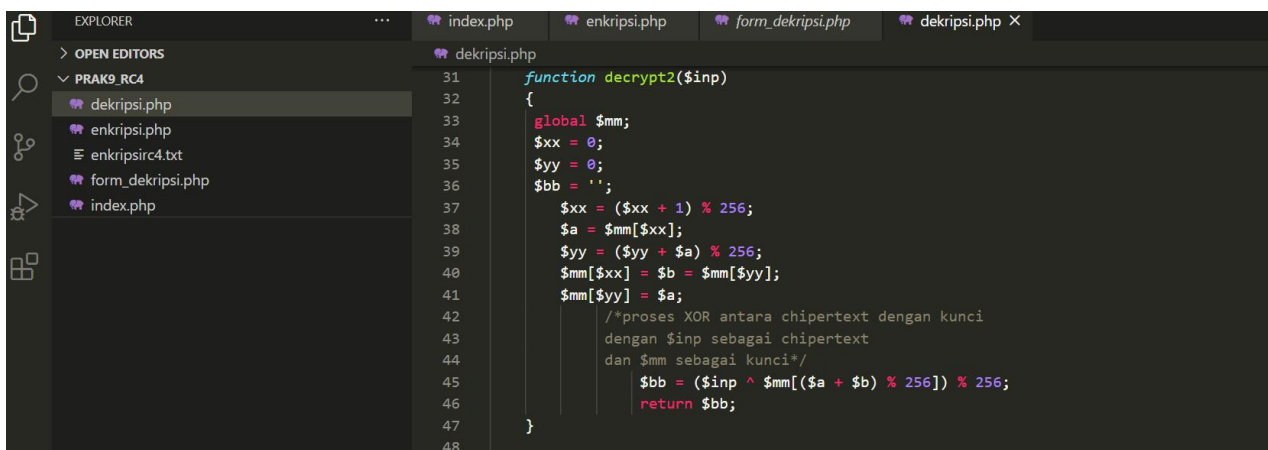
5. Selanjutnya buat file bernama dekripsi.php untuk proses keynya dengan menggunakan kotak substitusi S-Box



```
1  <?php
2
3  error_reporting(0);
4  function setupkey()
5  {
6      $kcd = $_GET["key"];
7      //echo "Kunci Dekripsi = $kcd";
8      echo "<br>";
9      for ($i = 0; $i < strlen($kcd); $i++) {
10         $key[$i] = ord($kcd[$i]); /*rubah ASCII ke desimal*/
11     }
12     global $mm;
13     $mm = array();
14     /*buat decrypt*/
15     for ($i = 0; $i < 256; $i++) {
16         $mm[$i] = $i;
17     }
18     $j = $k = 0;
19     for ($i = 0; $i < 256; $i++) {
20         $a = $mm[$i];
21         $j = ($j + $a + $key[$k]) % 256;
22         $mm[$i] = $mm[$j];
23         $mm[$j] = $a;
24         $k++;
25         if ($k > 15) {
26             $k = 0;
27         }
28     }
29 } /*akhir function*/
```

Pertama, script diatas mengambil key dengan cara di“GET” dari form dekripsi, selanjutnya dihitung jumlah panjang string dari key tersebut menggunakan stlrn dan di looping(for).

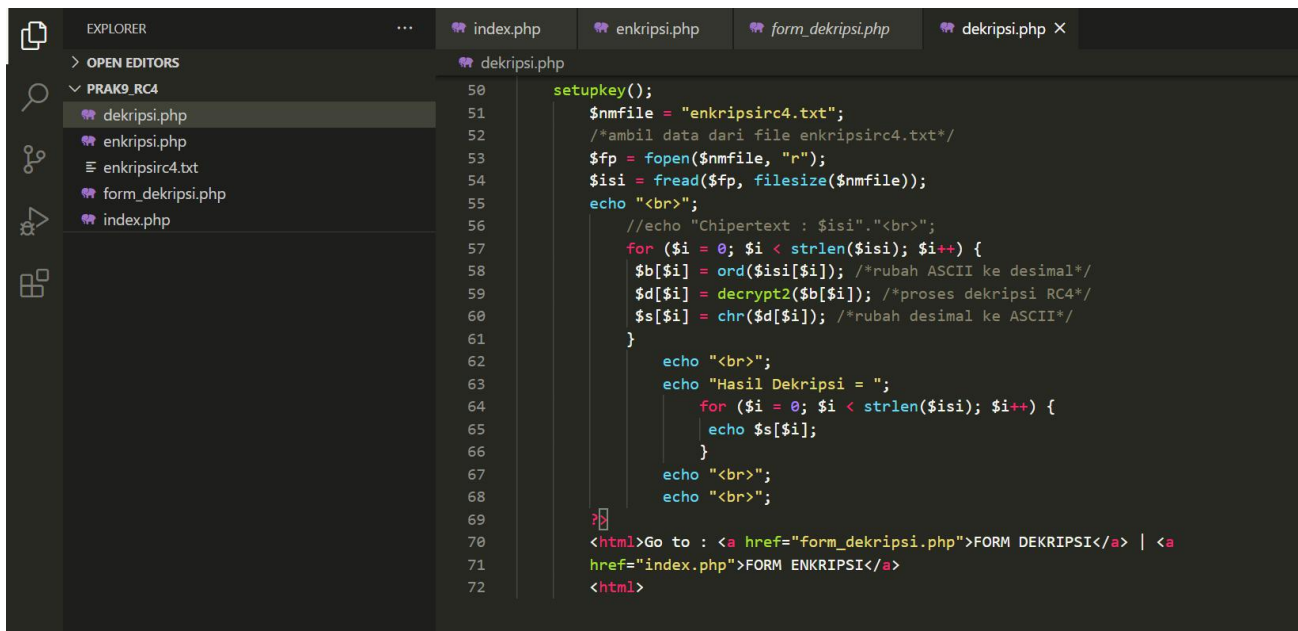
Selanjutnya tambahkan script untuk melakukan Dekripsi



```
31 function decrypt2($inp)
32 {
33     global $mm;
34     $xx = 0;
35     $yy = 0;
36     $bb = '';
37     $xx = ($xx + 1) % 256;
38     $a = $mm[$xx];
39     $yy = ($yy + $a) % 256;
40     $mm[$xx] = $b = $mm[$yy];
41     $mm[$yy] = $a;
42     /*proses XOR antara chipertext dengan kunci
43     dengan $inp sebagai chipertext
44     dan $mm sebagai kunci*/
45     $bb = ($inp ^ $mm[(($a + $b) % 256)]) % 256;
46     return $bb;
47 }
48
```

Lalu masuk ke proses XOR dengan kunci \$inp sebagai chipertext dan \$mm sebagai kuncinya.

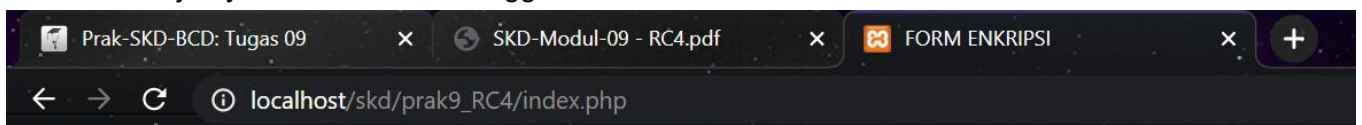
Selanjutnya tambah script untuk menampilkan pesan hasil dari dekripsi



```
50  setupkey();
51  $nmfile = "enkripsirc4.txt";
52  /*ambil data dari file enkripsirc4.txt*/
53  $fp = fopen($nmfile, "r");
54  $isi = fread($fp, filesize($nmfile));
55  echo "<br>";
56  //echo "Chipertext : $isi."<br>";
57  for ($i = 0; $i < strlen($isi); $i++) {
58      $b[$i] = ord($isi[$i]); /*rubah ASCII ke desimal*/
59      $d[$i] = decrypt2($b[$i]); /*proses dekripsi RC4*/
60      $s[$i] = chr($d[$i]); /*rubah desimal ke ASCII*/
61  }
62
63  echo "<br>";
64  echo "Hasil Dekripsi = ";
65  for ($i = 0; $i < strlen($isi); $i++) {
66      echo $s[$i];
67  }
68  echo "<br>";
69
70  <html>Go to : <a href="form_dekripsi.php">FORM DEKRIPSI</a> | <a
71  href="index.php">FORM ENKRIPSI</a>
72  </html>
```

Pada script ini mengambil data dari file yang sudah otomatis dibuat dengan cara membuka file “enkripsirc4.txt” menggunakan “fopen” dan membaca menggunakan “fread”, selanjutnya masuk ke perulangan untuk menghitung jumlah kata menggunakan “strlen” dan merubah dari ASCII ke desimal, lalu merubah lagi dari desimal ke ASCII menggunakan for array.

6. Selanjutnya kita demokan menggunakan web browser



FORM ENKRIPSI

Plainteks :

MAWAR

Key :

Go to : [FORM DEKRIPSI](#)

Hasil dari plainteks “MAWAR” dan menggunakan kunci “bunga”

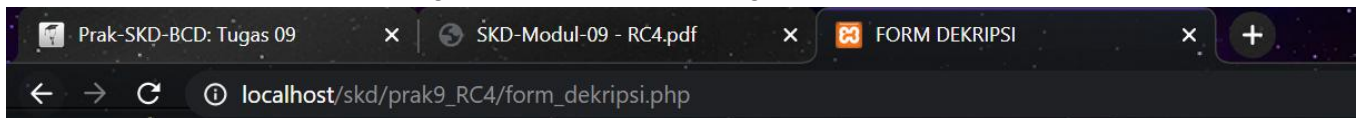


Kunci enkripsi = bunga

Hasil enkripsi = p9Wa[TG

Go to : [FORM DEKRIPSI](#)

Masuk ke form dekripsi dan menetikkan kata kunci “bunga”

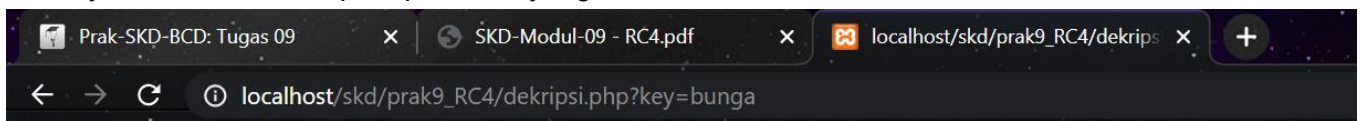


FORM DEKRIPSI

Key :

Go to : [FORM ENKRIPSI](#)

Hasilnya akan kembali seperti plainteks yang awal kita buat



Hasil Dekripsi = MAWAR

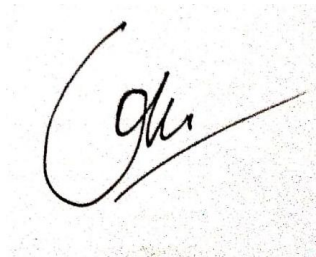
Go to : [FORM DEKRIPSI](#) | [FORM ENKRIPSI](#)

KESIMPULAN

Dari hasil praktikum yang telah dilakukan dapat diambil kesimpulan bahwa Algoritma (RC4) merupakan salah satu algoritma kunci simetris dengan metode kriptografi karena proteksi query dan RC4 memiliki proses enkripsi yang cukup sederhana dan hanya melibatkan beberapa operasi saja per byte-nya.

DAFTAR PUSTAKA

- Anshori, A., 2020. *Algoritma RC4 Sebagai Perkembangan Metode Kriptografi*. [online] Academia.edu. Available at: <https://www.academia.edu/35395928/Algoritma_RC4_sebagai_Perkembangan_Metode_Kriptografi> [Accessed 10 November 2020].
- tandi, b., 2020. *Kumpulan Tutorial: Tutorial Enkripsi Algoritma RC4 Dengan PHP*. [online] Kumpulan Tutorial. Available at: <<http://www.punyacara.com/2018/05/tutorial-enkripsi-algoritma-rc4-dengan.html>> [Accessed 10 November 2020].



(Luthfi Puji Ningtyas – M3118051)