

LAPORAN PRAKTIKUM 03
PROGRAM SEDERHANA ENKRIPSI DAN DEKRIPSI CAESAR



Di buat oleh :
Samuel Steven Prisma Hasiyono
V3420069
TIC

UNIVERSITAS SEBELAS MARET SURAKARTA
FAKULTAS SEKOLAH VOKASI
DE TEKNIK INFORMATIKA
2021

A. TUJUAN

- a. Mengenalkan pada mahasiswa tentang konsep kriptografi
- b. Mahasiswa mampu membuat program enkripsi sederhana

B. DASAR TEORI

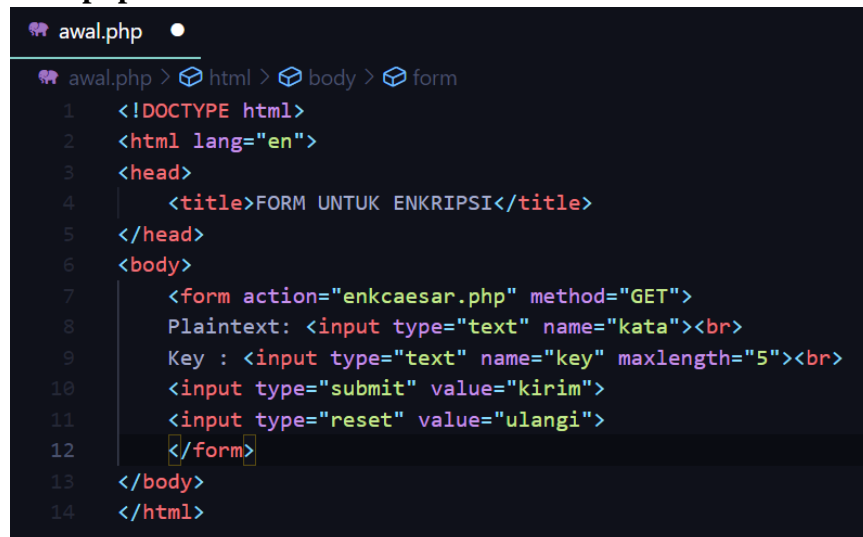
Kriptografi adalah ilmu untuk menjaga keamanan pesan. Terdapat 2 jenis kriptografi dipandang dari masanya, yaitu:

- a. Kriptografi Klasik
Caesar cipher, Affine cipher, Vigenere chipper
- b. Kriptografi modern
Terbagi menjadi dua, yaitu:
 - i. Kriptografi simetrik
Kriptografi yang menggunakan kunci yang digunakan untuk enkripsi maupun dekripsi
Contoh: RC4, DES, AES, IDEA
 - ii. Kriptografi asimetrik
Kriptografi yang terdapat dua kunci untuk enkripsi dan dekripsi
Contoh: RSA, DSA, El-gama

C. PETUNJUK PRAKTIKUM

Membuat form masukan/input untuk proses enkripsi

- a. Buat file untuk masukan plainteks dan key (bilangan), beri nama file **awal.php**



```
awal.php
awal.php > html > body > form
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4   <title>FORM UNTUK ENKRIPSI</title>
5 </head>
6 <body>
7   <form action="enkcaesar.php" method="GET">
8     Plaintext: <input type="text" name="kata"><br>
9     Key : <input type="text" name="key" maxlength="5"><br>
10    <input type="submit" value="kirim">
11    <input type="reset" value="ulangi">
12  </form>
13 </body>
14 </html>
```

Membuat proses enkripsi dengan Algoritma Caesar

- b. Buat file untuk melakukan proses enkripsi, beri nama file **enkcaesar.php**

```

awal.php      enkcaesar.php 1 X
enkcaesar.php > ...
1  <?php
2  $kalimat = $_GET["kata"];
3  $key=$_GET["key"];
4
5  for($i=0;$i<strlen ($kalimat) ;$i++) {
6      $kode [$i]=ord($kalimat[$i]); //rubah ASCII ke desimal
7      $b[$i]=(Skode[$i] + $key ) % 256; //proses enkripsi
8      $c[$i]=chr($b[$i]); //rubah desimal ke ASCII
9  }
10
11  echo "kalimat ASLI : " ;
12
13  for($i=0;$i<strlen ($kalimat) ;$i++) {
14      echo $kalimat [$i];
15
16  }
17  echo "<br>";
18  echo "hasil enkripsi : ";
19  $hsl = '';
20  for ($i=0;$i<strlen($kalimat) ;$i++) {
21      echo $c[$i];
22      $hsl = $hsl . $c[$i];
23  }
24  echo "<br>";
25  //simpan data di file
26  $fp = fopen ("enkripsi.txt","w");
27  fputs ($fp,$hsl) ;
28  fclose ($fp) ;
29  ?>

```

- c. Buat file untuk masukan key (berupa bilangan), agar bisa menghasilkan kembali plainteks maka key harus sama dengan proses enkripsi, beri nama file: **akhir.php**

```

awal.php      enkcaesar.php 1      akhir.php X
akhir.php > html > body > form
1  <!DOCTYPE html>
2  <html lang="en">
3  <head>
4
5      <title>Form untuk Deskripsi</title>
6  </head>
7  <body>
8      <form action="dekCaesar.php" method="get">
9          Key : <input type="text" name="key" maxlength="5">
10         <input type="submit" value="kirim">
11         <input type="reset" value="ulangi">
12     </form>
13
14 </body>
15 </html>

```

- d. Buat file untuk melakukan proses dekripsi, beri nama file : **dekCaesar.php**

```
dekCaesar.php > ...
1  <?php
2
3  $key = $_GET["key"];
4  $nmfile = "enkripsi.txt";
5  $fp = fopen($nmfile,"r"); // buka file hasil enkripsi
6  $isi = fread ($fp, filesize ($nmfile)) ;
7
8  for ($i=0;$i<strlen($isi) ;$i++) {
9  $kode [$i]=ord($isi[$i]); // rubah ASII ke desimal
10 $b[$i]=($kode[$i] - $key ) % 256; // proses dekripsi Caesar
11 $c[$i]=chr($b[$i]); //rubah desimal ke ASCII
12 }
13 echo "kalimat ciphertext : ";
14 for ($i=0;$i<strlen($isi) ;$i++) {
15 echo $isi[$i];
16 }
17 echo "<br>";
18 echo "hasil dekripsi =";
19 for ($i=0;$i<strlen($isi) ;$i++) {
20 echo $c[$i];
21 }
22
23 echo "<br>";
24
25 ?>
```

- e. Membuat form untuk proses enkripsi dokumen text (upload file)
- f. Buat file dengan nama **enkcaesar_file.php**

enkcaesar_file.php X



enkcaesar_file.php > b

```
1  <?php
2  $file_upload = $_FILES["file_upload"];
3  $key = $_POST["key"];
4  move_uploaded_file($file_upload['tmp_name'],
5  './uploaded_files.txt');
6  $kalimat = file_get_contents('./uploaded_files.txt');
7  for($i=0;$i <?php
8  {
9  $kode[$i]=o function file_get_contents ($filename,
10 $b[$i]=($ko $use_include_path = false, $context = null, $offset =
11 $c[$i]=chr( 0, $maxlen = null) {})
12 } Reads entire file into a string
13 echo "<b>ka file_get_contents
14 for($i=0;$i Reads entire file into a string
15 {
16 echo $kalim <?php
17 } function file_get_contents(
18 echo "<br>< string $filename,
19 echo "<b>ha bool $use_include_path = false,
20 $hsl = '';
21 for ($i=0;$i<strlen($kalimat);$i++)
22 {
23 echo $c[$i];
24 $hsl = $hsl . $c[$i];
25 }
26 echo "<br>";
27 //simpan data di file
28 $fp = fopen ("hasil_enkripsi.txt","w");
29 fputs ($fp,$hsl);
30 fclose($fp);
31 ?>
32 <br><br>
```

D. TUGAS TERSTRUKTUR

Program di atas akan menghasilkan chipertext berupa ASCII (256). Jika hasil chipertext

yang diinginkan hanya Alfabet saja (A-Z). Bagaimana caranya?

Uppercase

Kode dec 'A' = 65 (batas bawah)

Kode dec 'Z' = 90 (batas atas)

Lowercase

Kode dec 'a' = 97 (batas bawah)

Kode dec 'z' = 122 (batas atas)

Contoh Hasil (Uppercase)

Saya membuat file baru dengan nama Caesar-cipher.php

```
caesar-cipher.php X
caesar-cipher.php > ...
1  <?php
2
3  function geser_teks($string, $key) {
4      return implode('', array_map(function ($char) use ($key) {
5          return geser_karakter($char, $key);
6      }, str_split($string)));
7  }
8
9  function geser_karakter($char, $shift) {
10     $shift = $shift % 25;
11     $ascii = ord($char);
12     $shifted = $ascii + $shift;
13
14     if ($ascii >= 65 && $ascii <= 90) {
15         return chr(geser_huruf_besar($shifted));
16     }
17
18     if ($ascii >= 97 && $ascii <= 122) {
19         return chr(geser_huruf_kecil($shifted));
20     }
21
22     if ($ascii >= 33 && $ascii <= 58) {
23         return chr(geser_angka($shifted));
24     }
25
26     return chr($ascii);
27 }
28
29 function geser_angka($ascii) {
30     if ($ascii < 33) {
31         $ascii = 59 - (33 - $ascii);
32     }
```

caesar-cipher.php X

caesar-cipher.php > ...

```
34     if ($ascii > 58) {
35         $ascii = ($ascii - 58) + 32;
36     }
37     return $ascii;
38 }
39
40 function geser_huruf_besar($ascii) {
41     if ($ascii < 65) {
42         $ascii = 91 - (65 - $ascii);
43     }
44
45     if ($ascii > 90) {
46         $ascii = ($ascii - 90) + 64;
47     }
48
49     return $ascii;
50 }
51
52 function geser_huruf_kecil($ascii) {
53     if ($ascii < 97) {
54         $ascii = 123 - (97 - $ascii);
55     }
56
57     if ($ascii > 122) {
58         $ascii = ($ascii - 122) + 96;
59     }
60
61     return $ascii;
62 }
63
64 function enkripsi($plaintext, $key = 12) {
65     return geser_teks($plaintext, $key);
```

```

66     }
67
68     function dekripsi($ciphertext, $key = -12) {
69         return geser_teks($ciphertext, -$key);
70     }
71
72     // Usage
73     $plainText = "Foo Bar Baz 123";
74     $cipherText = enkripsi($plainText, 8);
75     echo "Plain Text: ".$plainText;
76     echo "<br/>";
77     echo "Cipher Text: ".$cipherText;
78     echo "<br/>";
79     echo "Dekripsi: ".dekripsi($cipherText, 8);

```

Hasil:

Plain Text: awasi asterix dan temannya obelix
 Cipher Text: ieiaq iabmzqf liv bmuivvgi wjmtqf
 Dekripsi: awasi asterix dan temannya obelix

Plain Text: AWASI ASTERIX DAN TEMANNYA OBELIXs
 Cipher Text: IEIAQ IABMZQF LIV BMUIVVGI WJMTQFa
 Dekripsi: AWASI ASTERIX DAN TEMANNYA OBELIXs

E. REFERENSI

<https://gist.github.com/egig/54992dfa08bf52d2ccbc64bc3199e1df>