
LAPORAN PRAKTIKUM

IDENTITAS PRAKTIKAN

Mata Kuliah	Praktikum Sistem Keamanan Data
NIM	V3420069
Nama	Samuel Steven Prisma Hasiyono
Tema	Vigenere dan Affine
Link project	

LANGKAH DAN HASIL PRAKTIKUM

Vigenere Chiper

1. Membuat form input untuk proses enkripsi seperti pada praktikum sebelumnya dengan nama file yaitu awal.php

```
awal.php ✕  
awal.php > ...  
1  <!DOCTYPE html>  
2  <html lang="en">  
3  <head>  
4      <meta charset="UTF-8">  
5      <meta http-equiv="X-UA-Compatible" content="IE=edge">  
6      <meta name="viewport" content="width=device-width, initial-scale=1.0">  
7      <title>FORM UNTUK ENKRIPSI</title>  
8  </head>  
9  <body>  
10     <form action="enkcaesar.php" method="get">  
11         Plainteks : <input type="text" name="kata"><br>  
12         Key : <input type="text" name="key" maxlength="5"><br>  
13         <input type="submit" value="kirim">  
14         <input type="reset" value="ulangi">  
15     </form>  
16 </body>  
17 </html>
```

2. Membuat algoritma vigenere untuk proses enkripsi dengan nama enkcaesar.php dengan menggunakan if-else untuk mengatur batas bawah uppercase dan lowercase, dimana batas bawah uppercase adalah 65 dan batas bawah lowercase 97. Selain itu juga menggunakan fungsi str_split untuk memecah array lalu dihitung menggunakan count. Pada proses ini kita menggunakan modulo 26 lalu ditambah dengan batas bawahnya, sehingga seperti di bawah ini

```
enkcaesar.php X
enkcaesar.php > ...
1  <?php
2  $kalimat = $_GET["kata"];
3  $kunci = $_GET["key"];
4  $plain_text = str_split($kalimat);
5  $n = count($plain_text);
6  $key = str_split($kunci);
7  $m = count($key);
8  $bataskode = 65;
9  $bataslow = 97;
10 $encrypted_text = '';
11 for ($i = 0; $i < $n; $i++) {
12     $cipher[$i] = ord($plain_text[$i]);
13     if ($cipher[$i] >= 65 && $cipher[$i] <= 90) {
14         $encrypted_text .= chr(((ord($plain_text[$i]) - $bataskode
15             + ord($key[$i % $m]) - $bataskode) % 26) + $bataskode);
16     } else if ($cipher[$i] >= 97 && $cipher[$i] <= 122) {
17         $encrypted_text .= chr(((ord($plain_text[$i]) - $bataslow
18             + ord($key[$i % $m]) - $bataslow) % 26) + $bataslow);
19     }
20 }
21
22 //digabungkan proses enkripsi
23 echo "kalimat ASLI : ";
24 for ($i = 0; $i < $n; $i++) {
25     echo $kalimat[$i];
26 }
27 echo "<br>";
28 echo "hasil enkripsi = ";
29 echo $encrypted_text;
30
31 echo "<br>";
32 //simpan data di file
33 $fp = fopen("enkripsi.txt", "w");
34 fputs($fp, $encrypted_text);
35 fclose($fp);
36
```

- Untuk file-file selain yang saya tuliskan masih tetap menggunakan file yang sama dengan praktikum sebelumnya yaitu praktikum 3

```

akhir.php
1 <!DOCTYPE html>
2 <html Lang="en">
3 <head>
4 <meta charset="UTF-8">
5 <meta http-equiv="X-UA-Compatible" content="IE=edge">
6 <meta name="viewport" content="width=device-width, initial-scale=1.0">
7 <title>Form untuk Deskripsi</title>
8 </head>
9 <body>
10 <form action="dekCaesar.php" method="get">
11 Key : <input type="text" name="key" maxlength="5" id=""><br>
12 <input type="submit" value="kirim">
13 <input type="reset" value="ulangi">
14 </form>
15 </body>
16 </html>

enkripsi.php
1 <?php
2 $file_upload = $_FILES["file_upload"];
3 $key = $_POST["key"];
4 move_uploaded_file(
5     $file_upload["tmp_name"],
6     './uploaded_files.txt'
7 );
8 $kalimat = file_get_contents('./uploaded_files.txt');
9 for ($i = 0; $i < strlen($kalimat); $i++) {
10     $kode[$i] = ord($kalimat[$i]); //merubah ASCII ke
11     $b[$i] = ($kode[$i] + $key) % 256; //proses enkripsi
12     $c[$i] = chr($b[$i]); //rubah desimal ke ASCII
13 }
14 echo "<b>kalimat ASLI : </b><br>";
15 for ($i = 0; $i < strlen($kalimat); $i++) {
16     echo $kalimat[$i];
17 }
18 echo "<br><br>";
19 echo "<b>hasil enkripsi = </b><br>";
20 $hsl = '';
21 for ($i = 0; $i < strlen($kalimat); $i++) {
22     echo $c[$i];
23     $hsl = $hsl . $c[$i];
24 }
25 echo "<br>";
26 //simpan data di file
27 $fp = fopen("hasil_enkripsi.txt", "w");
28 fputs($fp, $hsl);
29 fclose($fp);
30 >
31 <br><br>
32 <b>a <a href="hasil_enkripsi.txt"> Download File Here
33 </a></b>
34 >

enkripsi_file.php
1 <?php
2 $key = $_GET["key"];
3 $nfile = "enkripsi.txt";
4 $fp = fopen($nfile, "r"); //buka file
5 $isi = fread($fp, filesize($nfile));
6
7 for($i=0; $i<strlen($isi); $i++){
8     $kode[$i]=ord($isi[$i]); //menun
9     $b[$i]=($kode[$i] - $key) % 256;
10     $c[$i]=chr($b[$i]); //rubah des
11 }
12 echo "kalimat ciphertext : ";
13 for ($i=0; $i<strlen($isi); $i++){
14     echo $isi[$i];
15 }
16 echo "<br>";
17 echo "hasil deskripsi = ";
18 for ($i=0; $i<strlen($isi); $i++){
19     echo $c[$i];
20 }
21 echo "<br>"
22 >

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

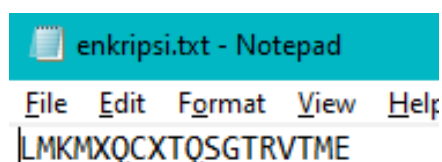
```

- Hasil Praktikum
 - Proses Enkripsi

Plainteks :

Key :

kalimat ASLI : SISTEMKEAMANANDATA
 hasil enkripsi = LMKMXQCXTQSGTRVTME



Affine Chiper

1. Memodifikasi form awal.php dari praktikum 3 seperti pada di bawah ini

```
awal.php ✕
awal.php > ...
1  <!DOCTYPE html>
2  <html>
3  <head>
4  <title>FORM UNTUK ENKRIPSI</title>
5  </head>
6  <body>
7  <form action="affine.php" method="get">
8  <h1> ENKRIPSI AFFINE</h1>
9  Plainteks : <input type="text" name="kata"><br>
10 a : <input type="number" name="key1"><br>
11 b : <input type="number" name="key2"><br>
12 <input type="submit" value="kirim">
13 <input type="reset" value="ulangi">
14 </form>
15 </body>
16 </html>
```

2. Membuat file bernama affine.php, file ini digunakan untuk proses enkripsi. Pada proses enkripsi masukkan perhitungan untuk mengubah ASCII plainteks ke decimal, perhitungan untuk kunci sandi dan plainteks, serta untuk mengubah decimal ke ASCII. Pada kunci pertama dimasukkan angka yang relatif prima dengan angka 26, sehingga disini saya menggunakan angka 7 untuk kunci pertama.

```
affine.php ✕
affine.php > ...
1  <?php
2  $kalimat = $_GET["kata"];
3  $kunci1 = $_GET["key1"];
4  $kunci2 = $_GET["key2"];
5
6  for($i=0;$i<strlen($kalimat);$i++){
7      $kode[$i]=ord($kalimat[$i]); //mengubah plainteks ke decimal
8      $b[$i]=((( $kunci1*($kode[$i]-65) ) + $kunci2) % 26)+65;
9      $c[$i]=chr($b[$i]); //mengubah decimal ke ASCII
10 }
11 echo "kalimat ASLI : ";
12 for($i=0;$i<strlen($kalimat);$i++){
13     echo $kalimat[$i];
14 }
15 echo "<br>";
16 echo "hasil enkripsi : ";
17 $hsl='';
18 for ($i=0;$i<strlen($kalimat);$i++)
19 {
20     echo $c[$i];
21     $hsl = $hsl . $c[$i];
22 }
23 echo "<br>";
24 echo "<br>";
25 //simpan data di file
26 $fp = fopen("enkripsi.txt","w");
27 fputs($fp,$hsl);
28 fclose($fp);
```

- Untuk file-file selain yang saya tuliskan masih tetap menggunakan file yang sama dengan praktikum sebelumnya yaitu praktikum 3

```
coba.php <?php
1 <?php
2 $kunci1=7;
3 $kunci2=10;
4 $isi = "CZOLNE";
5 $a_inv = 0;
6 $flag = 0;
7 $batas = 65;
8 for($i=0;$i<26;$i++){
9     $flag = ($kunci1*$i)%26;
10
11     if($flag == 1){
12         $a_inv = $i;
13     }
14 }
15 for($i=0; $i<strlen($isi); $i++){
16     $kode[$i]=ord($isi[$i]); //menunjukan huruf atau lamb
17     $b[$i]=((($a_inv*($kode[$i] - $batas) - $kunci2))% 26);
18     if($b[$i]<0){
19         $b[$i] = 26 - abs($b[$i]);
20     }
21     $hasil = $b[$i]+$batas;
22     echo chr($hasil);
23     echo '<br>';
24     // $c[$i]=chr($b[$i]); //Tak Matiiin yaa bund ntar diut
25 }
26 // echo $a_inv;
27 echo "kalimat ciphertext : ";
28 for ($i=0; $i<strlen($isi); $i++){
29     echo $isi[$i];
30 }
31 echo "<br>";
32 echo "hasil deskripsi = ";
33 //for ($i=0; $i<strlen($isi); $i++){
34 //echo $c[$i];
35 //}
36 echo "<br>"
37
38
39 ?>
```

```
dekCaesar.php <?php
1 <?php
2 // $key = $_GET["key"];
3 $kunci1 = $_GET["key1"];
4 $kunci2 = $_GET["key2"];
5 $nmfile = "enkripsi.txt";
6 $fp = fopen($nmfile, "r"); //buka file hasil en
7 $isi = fread($fp, filesize($nmfile));
8
9 $a_inv = 0;
10 $flag = 0;
11
12 for($i=0;$i<26;$i++){
13     $flag = ($kunci1*$i)%26;
14
15     if($flag == 1){
16         $a_inv = $i;
17     }
18 }
19 // for($i=0; $i<strlen($isi); $i++){
20 //     $kode[$i]= ord($isi[$i]); //menunjukan huruf
21 //     $b[$i]=((1/$kunci1)*($kode[$i] - $kunci2));
22 // }
23 for($i=0; $i<strlen($isi); $i++){
24     $kode[$i]=ord($isi[$i]); //menunjukan huruf
25     $b[$i]=($a_inv*($kode[$i] - $kunci2))% 256;
26     $c[$i]=chr($b[$i]); //rubah desimal ke ASCII
27 }
28 echo "kalimat ciphertext : ";
29 for ($i=0; $i<strlen($isi); $i++){
30     echo $isi[$i];
31 }
32 echo "<br>";
33 echo "hasil deskripsi = ";
34 for ($i=0; $i<strlen($isi); $i++){
35     echo $c[$i];
36 }
37 echo "<br>"
38
39 ?>
```

```
enkcaesar.php <?php
1 <?php
2 $kalimat = $_GET["kata"];
3 $key = $_GET["key"];
4 for($i=0;$i<strlen($kalimat);$i++){
5     $kode=ord($kalimat[$i]);
6     // $b[$i]=($kode[$i]+$key)%256;
7     for($j=0;$j<$key;$j++){
8         $kode++;
9     }
10    $c[$i]=chr($kode);
11    // $c[$i]=chr($b[$i]);
12 }
13 echo "kalimat ASLI : ";
14 for($i=0;$i<strlen($kalimat);$i++){
15     echo $kalimat[$i];
16 }
17 echo "<br>";
18 echo "hasil enkripsi : ";
19 $hsl='';
20 for ($i=0;$i<strlen($kalimat);$i++)
21 {
22     echo $c[$i];
23     $hsl = $hsl . $c[$i];
24 }
25 echo "<br>";
26 //simpan data di file
27 $fp = fopen("enkripsi.txt", "w");
28 fputs($fp, $hsl);
29 fclose($fp);
30
31
32 ?>
```

```
enkcaesar.php <?php
1 <?php
2 $kalimat = $_GET["kata"];
3 $kunci = $_GET["key"];
4 // $kalimat = "SISTEMKEAMANANDATA";
5 // $kunci = "DATA";
6 $plain_text = str_split($kalimat);
7 $n = count($plain_text);
8 $key = str_split($kunci);
9 $m = count($key);
10 $bataskode = 65;
11 $bataslow = 97;
12 $encrypted_text = '';
13 // if ($key[0])
14 for ($i = 0; $i < $n; $i++) {
15     $cipher[$i] = ord($plain_text[$i]);
16     // if($cipher[$i] < 65)
17     if ( $cipher[$i] >= 65 && $cipher[$i] <= 90 ) {
18         $encrypted_text .= chr(((ord($plain_text[$i]) - $bataskode
19             + ord($key[$i % $m]) - $bataskode) % 26) + $bataskode);
20     } else if ( $cipher[$i] >= 97 && $cipher[$i] <= 122 ) {
21         $encrypted_text .= chr(((ord($plain_text[$i]) - $bataslow
22             + ord($key[$i % $m]) - $bataslow) % 26) + $bataslow);
23     }
24 }
25
26 //digabungkan proses enkripsi
27 echo "kalimat ASLI : ";
28 for ($i = 0; $i < $n; $i++) {
29     echo $kalimat[$i];
30 }
31 echo "<br>";
32 echo "hasil enkripsi =";
33 echo $encrypted_text;
34
35 echo "<br>";
36 //simpan data di file
37 $fp = fopen("enkripsi.txt", "w");
38 fputs($fp, $encrypted_text);
39 fclose($fp);
```

4. Hasil praktikum

- Proses Enkripsi

Pada kunci pertama dimasukkan angka yang relatif prima dengan angka 26, sehingga disini saya menggunakan angka 7 untuk kunci pertama, hal ini berguna untuk nantinya dalam proses dekripsi affine.

ENKRIPSI AFFINE

Plainteks :

a :

b :

kalimat ASLI : SAMUEL

hasil enkripsi : CIEKYA

TUGAS TERSTRUKTUR(TT)

Soal:

1. Terapkan algoritma dekripsi pada vigenere chipper
Untuk melakukan dekripsi pada Vigènere Cipher, digunakan kebalikan dari fungsi enkripsinya. Secara matematis, dekripsi Vigènere Cipher dengan jumlah karakter sebanyak 26 adalah sebagai berikut.
Karakter cipherteks: $p_i(c) = (c - k_i) \bmod 26$
A=0... Z=25
2. Terapkan algoritma dekripsi untuk affine cipher. Dekripsi : $D(x) = a^{-1}(x - b) \bmod m$
Mencari a^{-1} dapat menggunakan potongan code berikut ini

```
int a_inv = 0;
int flag = 0;

for (inti = 0; i < 26; i++) {
    flag = (a*i)%26;
    if (flag == 1) {
        a_inv = i;
    }
}
```

1. Melanjutkan pada praktikum vigenere di atas dengan membuat file dekCaesar.php untuk melakukan proses dekripsi pada vigenere
 - Pada file ini terdapat perulangan for seperti praktikum di atas dan juga terdapat syarat. Dikarenakan syarat pada tugas terstruktur yaitu batas bawah untuk uppercase 65 dan batas atas yaitu 90. Selain itu untuk lowercase memiliki batas bawa 97 dan batas atas yaitu 122. Dengan adanya syarat ini maka kita menggunakan (if-else). Jika kalimat berupa uppercase lalu diubah ke ASCII dan akan terletak di antara 65 hingga 90 maka akan diolah dengan rumus sebagai berikut :

❖ $\$dek_text[\$i] = ((\$dek[\$i] - (\text{ord}(\$kunci[\$i \% \$m])) \% 26) + \$bataskode);$

Jika masih terdapat bilangan ASCII dibawah 65 maka akan ditambah 26

Jika kalimat berupa lowercase lalu diubah ke ASCII dan akan terletak di antar 97 hingga 122 maka akan diolah dengan rumus sebagai berikut :

❖ $\$dek_text[\$i] = ((\$dek[\$i] - (\text{ord}(\$kunci[\$i \% \$m])) \% 26) + \$bataslow);$

Jika masih terdapat bilangan ASCII dibawah 97 maka akan ditambah 26

```

dekCaesar.php > ...
1  <?php
2  $key = $_GET["key"];
3  $nmfile = "enkripsi.txt";
4  $fp = fopen($nmfile, "r"); //buka file hasil enkripsi
5  $isi = fread($fp, filesize($nmfile));
6  $enk_text = str_split($isi);
7  $n = count($enk_text);
8  $kunci = str_split($key);
9  $m = count($kunci);
10 $batascode = 65;
11 $bataslow = 97;
12
13 for ($i = 0; $i < $n; $i++) {
14     $dek[$i] = ord($enk_text[$i]);
15     if ( $dek[$i] >= 65 && $dek[$i] <= 90 ) {
16         $dek_text[$i] = (($dek[$i] - (ord($kunci[$i % $m])))%26) + $batascode;
17         if ($dek_text[$i] < 65) {
18             $dek_text[$i] += 26;
19         }
20     } else if ($dek[$i] >= 97 && $dek[$i] <= 122) {
21         $dek_text[$i] = (($dek[$i] - (ord($kunci[$i % $m])))%26) + $bataslow;
22         if ($dek_text[$i] < 97) {
23             $dek_text[$i] += 26;
24         }
25     }
26 }
27 echo "kalimat ciphertext : ";
28 for ($i=0; $i<strlen($isi); $i++){
29     echo $isi[$i];
30 }
31 echo "<br>";
32 echo "hasil deskripsi = ";
33 for ($i=0; $i<strlen($isi); $i++){
34     echo chr($dek_text[$i]);
35     // echo ($dek_text[$i]);
36 }
37 echo "<br>"
38
39 ?>

```

2. Hasil Praktikum

Plainteks :

Key :

kalimat ASLI : SISTEMKEAMANANDATA
 hasil enkripsi = LMKMXQCXTQSGTRVTME

Key :

kalimat ciphertext : LMKMXQCXTQSGTRVTME
 hasil deskripsi = SISTEMKEAMANANDATA

- **Dekripsi Affine**

1. Membuat file untuk inputan pada proses dekripsi yaitu file akhir.php



```
1 <!DOCTYPE html>
2 <html Lang="en">
3
4 <head>
5   <meta charset="UTF-8">
6   <meta http-equiv="X-UA"
7   <meta name="viewport" content="width=device-width, initial-scale=1.0">
8   <title>Form untuk Deskripsi</title>
9 </head>
10
11 <body>
12   <form action="dekaaffine.php" method="get">
13     a : <input type="number" name="key1"><br>
14     b : <input type="number" name="key2"><br>
15     <input type="submit" value="kirim">
16     <input type="reset" value="ulangi">
17   </form>
18 </body>
19
20 </html>
```

2. Membuat file untuk mendekripsikan hasil dari cipherteks agar kembali ke plainteks. Pada file ini terdapat \$kunci1 dan \$kunci2 untuk mengambil data dari akhir.php dan juga \$isi merupakan variabel yang digunakan untuk membaca dan mengambil data dari file enkripsi

```

dekaffine.php 1 X
dekaffine.php > ...
1  <?php
2  $kunci1 = $_GET["key1"];
3  $kunci2 = $_GET["key2"];
4  $nmfile = "enkripsi.txt";
5  $fp = fopen($nmfile, "r"); //buka file hasil enkripsi
6  $isi = fread($fp, filesize($nmfile));
7
8  $batas = 65;
9  $a_inv = 0;
10 $flag = 0;
11 for($i=0;$i<26;$i++){
12     $flag = ($kunci1*$i)%26;
13
14     if($flag == 1){
15         $a_inv = $i;
16     }
17 }
18 for($i=0; $i<strlen($isi); $i++){
19     $kode[$i]=ord($isi[$i]); //menunjukkan huruf atau lamban
20     $b[$i]=((($a_inv*($kode[$i] - $batas) - $kunci2))% 26); /
21     if($b[$i]<0){
22         //diberi ini karena terdapat hasil dari pengurangan
23         $b[$i] = 26 - abs($b[$i]); //fungsi abs untuk menen
24     }
25     $hasil[$i] = $b[$i]+$batas;
26     $c[$i]=chr($hasil[$i]);
27 }
28 // echo $a_inv;
29 echo "kalimat ciphertext : ";
30 for ($i=0; $i<strlen($isi); $i++){
31     echo $isi[$i];
32 }
33 echo "<br>";
34 echo "hasil deskripsi = ";
35 for ($i=0; $i<strlen($isi); $i++){
36     echo $c[$i];
37 }
38 // echo($c[$i]);
39 echo "<br>"

```

Hasil praktikum

ENKRIPSI AFFINE

Plainteks :

a :

b :

kalimat ASLI : SAMUEL

hasil enkripsi : JHRPTO

