# 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

```php
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>FORM UNTUK ENKRIPSI</title>
</head>
<body>
    <form action="enkcaesar.php" method="get">
    Plainteks : <input type="text" name="kata"><br>
    Key : <input type="text" name="key" maxlength="5"><br>
    <input type="submit" value="kirim">
    <input type="reset" value="ulangi">

    </form>
</body>
</html>
```

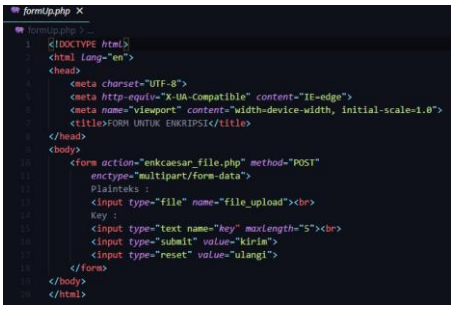
2. Membuat algoritma vigenere untuk proses enkripsi dengan nama enkcaesar.php dengan menggunakan if-else untuk mengatur batas bawah uppercase dan lowercase, dimana batas bawah uppercase adalah 65 dan batas bawah lowercase 97. Selain itu juga menggunakan fungsi str_split untuk memecah array lalu dihitung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

enkcaesar.php

```php
<?php
$kalimat = $_GET["kata"];
$kunci = $_GET["key"];
$plain_text = str_split($kalimat);
$n = count($plain_text);
$key = str_split($kunci);
$m = count($key);
$bataskode = 65;
$bataslow = 97;
$encrypted_text = '';
for ($i = 0; $i < $n; $i++) {
    $cipher[$i] = ord($plain_text[$i]);
    if ($cipher[$i] >= 65 &&  $cipher[$i] <= 90) {
        $encrypted_text .= chr(((ord($plain_text[$i]) - $bataskode
            + ord($key[$i % $m]) - $bataskode) % 26) + $bataskode);
    } else if ($cipher[$i] >= 97 &&  $cipher[$i] <= 122) {
        $encrypted_text .= chr(((ord($plain_text[$i]) - $bataslow
            + ord($key[$i % $m]) - $bataslow) % 26) + $bataslow);
    }
}

//digabungkan proses enkripsi
echo "kalimat ASLI : ";
for ($i = 0; $i < $n; $i++) {
    echo $kalimat[$i];
}
echo "<br>";
echo "hasil enkripsi =";
echo $encrypted_text;

echo "<br>";
//simpan data di file
$fp = fopen("enkripsi.txt", "w");
fputs($fp, $encrypted_text);
fclose($fp);
```

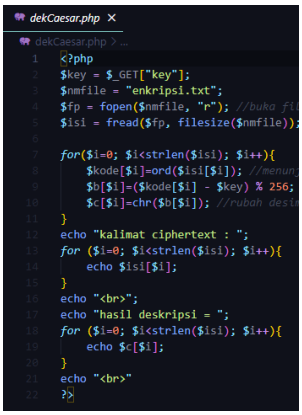
3. Untuk file-file selain yang saya tuliskan masih tetap menggunakan file yang sama dengan praktikum sebelumnya yaitu praktikum 3

```php
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Form untuk Deskripsi</title>
</head>
<body>
    <form action="dekCaesar.php" method="get">
        Key : <input type="text" name="key" maxlength="5" id=""><br>
        <input type="submit" value="kirim">
        <input type="reset" value="ulangi">
    </form>
</body>
</html>
```



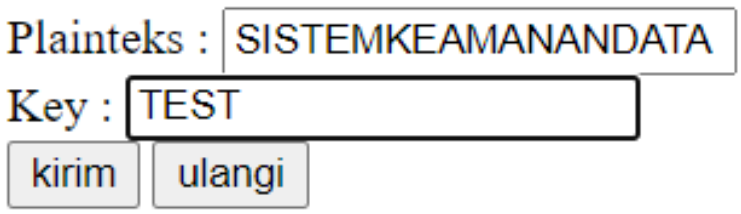
```php
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>FORM UNTUK ENKRIPSI</title>
</head>
<body>
    <form action="enkcaesar_file.php" method="POST"
        enctype="multipart/form-data">
        Plainteks :
        <input type="file" name="file_upload"><br>
        Key :
        <input type="text name="key" maxLength="5"><br>
        <input type="submit" value="kirim">
        <input type="reset" value="ulangi">
    </form>
</body>
</html>
```

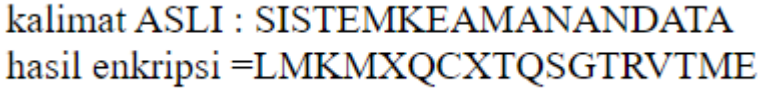
```php
<?php
$file_upload = $_FILES["file_upload"];
$key = $_POST["key"];
move_uploaded_file(
    $file_upload['tmp_name'],
    './uploaded_files.txt'
);
$kalimat = file_get_contents('./uploaded_files.txt');
for ($i = 0; $i < strlen($kalimat); $i++) {
    $kode[$i] = ord($kalimat[$i]); //merubah ASCII ke
    $b[$i] = ($kode[$i] + $key) % 256; //proses enkrip
    $c[$i] = chr($b[$i]); //rubah desimal ke ASCII
}
echo "<b>kalimat ASLI : </b><br>";
for ($i = 0; $i < strlen($kalimat); $i++) {
    echo $kalimat[$i];
}
echo "<br><br>";
echo "<b>hasil enkripsi = </b><br>";
$hsl = '';
for ($i = 0; $i < strlen($kalimat); $i++) {
    echo $c[$i];
    $hsl = $hsl . $c[$i];
}
echo "<br>";

//simpan data di file
$fp = fopen("hasil_enkripsi.txt", "w");
fputs($fp, $hsl);
fclose($fp);
?>
<br><br>
<b><a href="hasil_enkripsi.txt"> Download File Here
    </a></b>
```

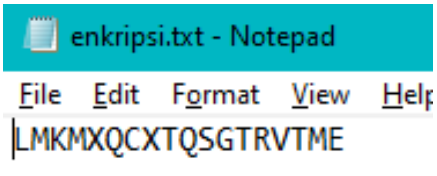


```php
<?php
$key = $_GET["key"];
$nmfile = "enkripsi.txt";
$fp = fopen($nmfile, "r"); //buka fi
$isi = fread($fp, filesize($nmfile));

for($i=0; $i<strlen($isi); $i++){
    $kode[$i]=ord($isi[$i]); //menun
    $b[$i]=($kode[$i] - $key) % 256;
    $c[$i]=chr($b[$i]); //rubah desi
}
echo "kalimat ciphertext : ";
for ($i=0; $i<strlen($isi); $i++){
    echo $isi[$i];
}
echo "<br>";
echo "hasil deskripsi = ";
for ($i=0; $i<strlen($isi); $i++){
    echo $c[$i];
}
echo "<br>"
?>
```

4. Hasil Praktikum
    - Proses Enkripsi



# Affine Chiper

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

awal.php

```php
<!DOCTYPE html>
<html>
<head>
<title>FORM UNTUK ENKRIPSI</title>
</head>
<body>
<form action="affine.php" method="get">
<h1> ENKRIPSI AFFINE</h1>
Plainteks : <input type="text" name="kata"><br>
a : <input type="number" name="key1"><br>
b : <input type="number" name="key2"><br>
<input type="submit" value="kirim">
<input type="reset" value="ulangi">
</form>
</body>
</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

```php
<?php
$kalimat = $_GET["kata"];
$kunci1 = $_GET["key1"];
$kunci2 = $_GET["key2"];

for($i=0;$i<strlen($kalimat);$i++){
    $kode[$i]=ord($kalimat[$i]);//mengubah plainteks ke decim
    $b[$i]=((($kunci1*($kode[$i]-65) ) + $kunci2) % 26)+65;
    $c[$i]=chr($b[$i]);//mengubah decimal ke ASCII
}
echo "kalimat ASLI : ";
for($i=0;$i<strlen($kalimat);$i++){
    echo $kalimat[$i];
}
echo "<br>";
echo "hasil enkripsi : ";
$hsl='';
for ($i=0;$i<strlen($kalimat);$i++)
{
    echo $c[$i];
    $hsl = $hsl . $c[$i];
}
echo "<br>";
echo "<br>";
//simpan data di file
$fp = fopen("enkripsi.txt","w");
fputs($fp,$hsl);
fclose($fp);
```

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

coba.php

```php
<?php
$kunci1=7;
$kunci2=10;
$isi = "CZOLNE";
$a_inv = 0;
$flag = 0;
$batas = 65;
for($i=0;$i<26;$i++){
    $flag = ($kunci1*$i)%26;

    if($flag == 1){
        $a_inv = $i;
    }
}
for($i=0; $i<strlen($isi); $i++){
    $kode[$i]=ord($isi[$i]); //menunjukan huruf atau lamb
    $b[$i]=(($a_inv*(($kode[$i] -$batas)- $kunci2))% 26);
    if($b[$i]<0){
        $b[$i] = 26 - abs($b[$i]);
    }
    $hasil = $b[$i]+$batas;
    echo chr($hasil);
    echo '</br>';
    //$c[$i]=chr($b[$i]); //Tak MAtiin yaa bund ntar diut
}
// echo $a_inv;
echo "kalimat ciphertext : ";
for ($i=0; $i<strlen($isi); $i++){
    echo $isi[$i];
}
echo "<br>";
echo "hasil deskripsi = ";
//for ($i=0; $i<strlen($isi); $i++){
    //echo $c[$i];
//}
echo "<br>"


?>
```

dekCaesar.php

```php
<?php
// $key = $_GET["key"];
$kunci1 = $_GET["key1"];
$kunci2 = $_GET["key2"];
$nmfile = "enkripsi.txt";
$fp = fopen($nmfile, "r"); //buka file hasil en
$isi = fread($fp, filesize($nmfile));

$a_inv = 0;
$flag = 0;

for($i=0;$i<26;$i++){
    $flag = ($kunci1*$i)%26;

    if($flag == 1){
        $a_inv = $i;
    }
}
// for($i=0; $i<strlen($isi); $i++){
//     $kode[$i]= ord($isi[$i]);
//     $b[$i]=((1/$kunci1)*($kode[$i]-$kunci2))
// }
for($i=0; $i<strlen($isi); $i++){
    $kode[$i]=ord($isi[$i]); //menunjukan huruf
    $b[$i]=($a_inv*($kode[$i] - $kunci2))% 256;
    $c[$i]=chr($b[$i]); //rubah desimal ke ASCI
}
echo "kalimat ciphertext : ";
for ($i=0; $i<strlen($isi); $i++){
    echo $isi[$i];
}
echo "<br>";
echo "hasil deskripsi = ";
for ($i=0; $i<strlen($isi); $i++){
    echo $c[$i];
}
echo "<br>"
?>
```

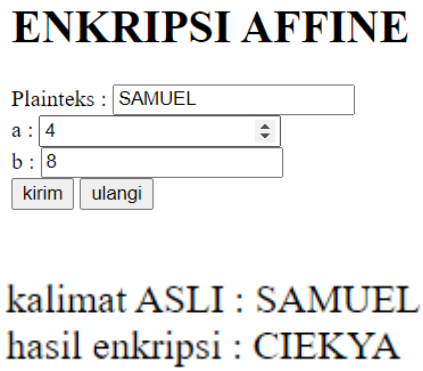
enkcaesarr.php

```php
<?php
$kalimat = $_GET["kata"];
$key = $_GET["key"];
for($i=0;$i<strlen($kalimat);$i++){
    $kode=ord($kalimat[$i]);
    // $b[$i]=($kode[$i]+$key)%256;
    for($j=0;$j<$key;$j++){
        $kode++;
    }
    $c[$i]=chr($kode);
    // $c[$i]=chr($b[$i]);
}
echo "kalimat ASLI : ";
for($i=0;$i<strlen($kalimat);$i++){
    echo $kalimat[$i];
}
echo "<br>";
echo "hasil enkripsi : ";
$hsl='';
for ($i=0;$i<strlen($kalimat);$i++)
{
    echo $c[$i];
    $hsl = $hsl . $c[$i];
}
echo "<br>";
//simpan data di file
$fp = fopen("enkripsi.txt","w");
fputs($fp,$hsl);
fclose($fp);


?>
```

enkcaesar.php

```php
<?php
$kalimat = $_GET["kata"];
$kunci = $_GET["key"];
// $kalimat = "SISTEMKEAMANANDATA";
// $kunci = "DATA";
$plain_text = str_split($kalimat);
$n = count($plain_text);
$key = str_split($kunci);
$m = count($key);
$bataskode = 65;
$bataslow = 97;
$encrypted_text = '';
// if ($key[0])
for ($i = 0; $i < $n; $i++) {
    $cipher[$i] = ord($plain_text[$i]);
    // if($cipher[$i] < 65)
    if ( $cipher[$i] >= 65 &&  $cipher[$i] <= 90) {
        $encrypted_text .= chr(((ord($plain_text[$i]) - $bataskode
            + ord($key[$i % $m]) - $bataskode) % 26) + $bataskode);
    } else if ( $cipher[$i]>= 97 &&  $cipher[$i] <= 122) {
        $encrypted_text .= chr(((ord($plain_text[$i]) - $bataslow
            + ord($key[$i % $m]) - $bataslow) % 26) + $bataslow);
    }
}

//digabungkan proses enkripsi
echo "kalimat ASLI : ";
for ($i = 0; $i < $n; $i++) {
    echo $kalimat[$i];
}
echo "<br>";
echo "hasil enkripsi =";
echo $encrypted_text;

echo "<br>";
//simpan data di file
$fp = fopen("enkripsi.txt", "w");
fputs($fp, $encrypted_text);
fclose($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.



# 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]-(ord($kunci[$i % $m])))%26)+$bataskode;

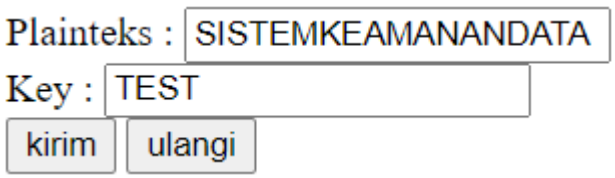
       Jika masih terdapat bilangan ASCII dibawah 65 maka akan ditambah 26

     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]-(ord($kunci[$i % $m])))%26)+$bataslow;

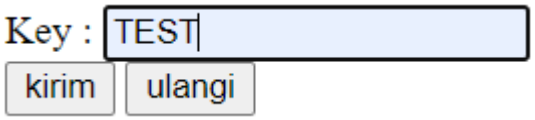
       Jika masih terdapat bilangan ASCII dibawah 97 maka akan ditambah 26

```php
<?php
$key = $_GET["key"];
$nmfile = "enkripsi.txt";
$fp = fopen($nmfile, "r"); //buka file hasil enkripsi
$isi = fread($fp, filesize($nmfile));
$enk_text = str_split($isi);
$n = count($enk_text);
$kunci = str_split($key);
$m = count($kunci);
$bataskode = 65;
$bataslow = 97;

for ($i = 0; $i < $n; $i++) {
    $dek[$i] = ord($enk_text[$i]);
    if ( $dek[$i] >= 65 &&  $dek[$i] <= 90) {
        $dek_text[$i] =(($dek[$i]-(ord($kunci[$i % $m])))%26)+$bataskode;
        if($dek_text[$i]<65){
            $dek_text[$i]+=26;
        }
    } else if ($dek[$i]>= 97 &&  $dek[$i] <= 122) {
         $dek_text[$i] =(($dek[$i]-(ord($kunci[$i % $m])))%26)+$bataslow;
         if($dek_text[$i]<97){
            $dek_text[$i]+=26;
         }
    }
}
echo "kalimat ciphertext : ";
for ($i=0; $i<strlen($isi); $i++){
    echo $isi[$i];
}
echo "<br>";
echo "hasil deskripsi = ";
for ($i=0; $i<strlen($isi); $i++){
    echo chr($dek_text[$i]);
    // echo ($dek_text[$i]);
}
echo "<br>"

?>
```

2. Hasil Praktikum




kalimat ASLI : SISTEMKEAMANANDATA
hasil enkripsi =LMKMXQCXTQSGTRVTME




kalimat ciphertext : LMKMXQCXTQSGTRVTME
hasil deskripsi = SISTEMKEAMANANDATA

- **Dekripsi Affine**

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


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 ×

dekaffine.php > ...

```php
<?php
$kunci1 = $_GET["key1"];
$kunci2 = $_GET["key2"];
$nmfile = "enkripsi.txt";
$fp = fopen($nmfile, "r"); //buka file hasil enkripsi
$isi = fread($fp, filesize($nmfile));

$batas = 65;
$a_inv = 0;
$flag = 0;
for($i=0;$i<26;$i++){
    $flag = ($kunci1*$i)%26;

    if($flag == 1){
        $a_inv = $i;
    }
}
for($i=0; $i<strlen($isi); $i++){
    $kode[$i]=ord($isi[$i]); //menunjukan huruf atau lamban
    $b[$i]=(($a_inv*(($kode[$i] -$batas)- $kunci2))% 26); /
    if($b[$i]<0){
        //diberi ini karena terdapat hasil dari pengurangan
        $b[$i] = 26 - abs($b[$i]); //fungsi abs untuk menen
    }
    $hasil[$i] = $b[$i]+$batas;
    $c[$i]=chr($hasil[$i]);
}
// echo $a_inv;
echo "kalimat ciphertext : ";
for ($i=0; $i<strlen($isi); $i++){
    echo $isi[$i];
}
echo "<br>";
echo "hasil deskripsi = ";
for ($i=0; $i<strlen($isi); $i++){
    echo $c[$i];
}
// echo($c[$i]);
echo "<br>"
```

Hasil praktikum

**ENKRIPSI AFFINE**

Plainteks : SAMUEL
a : 3
b : 7
kirim ulangi

kalimat ASLI : SAMUEL
hasil enkripsi : JHRPTO