

DAFTAR PUSTAKA

- Budiman, I., Saori, S., Anwar, R. N., Fitriani, & Pangestu, M. Y. (2021). Analisis Pengendalian Mutu Dibidang Industri Makanan (Studi Kasus: UMKM Mochi Kaswari Lampion Kota Sukabumi). *Jurnal Inovasi Penelitian*, 1(10), 1–15. <https://doi.org/https://doi.org/10.47492/jip.v1i10.419>
- Diana, M., & Zebua, T. (2018). Optimalisasi Beaufort Cipher Menggunakan Pembangkit Kunci RC4 Dalam Penyandian SMS. *J-SAKTI (Jurnal Sains Komputer Dan Informatika)*, 2(1), 12–22. <https://doi.org/10.30645/j-sakti.v2i1.52>
- Fadlan, M., Sinawati, S., Indriani, A., & Bintari, E. D. (2019). Pengamanan Data Teks Melalui Perpaduan Algoritma Beaufort Dan Caesar Cipher. *Jurnal Teknik Informatika*, 12(2), 149–158. <https://doi.org/10.15408/jti.v12i2.12262>
- Ginting, N. F., & Ginting, M. (2017). Perbandingan Kriptografi RSA dengan Base64. *Jurnal Teknik Informatika Unika St. Thomas (JTIUST)*, 2(2), 47–52. <https://doi.org/https://doi.org/10.17605/jti.v2i2.190>
- Irawan, C., Hari Rachmawanto, E., Atika Sari, C., & Agus Sugianto, C. (2020). Super Enkripsi File Dokumen Menggunakan Beaufort Cipher Dan Transposisi Kolom. *Seminar Nasional LPPM*, 556–563.
- Kurniawan, R. (2017). Rancang Bangun Aplikasi Pengaman Isi File Dokumen Dengan Algoritma RSA. *Jurnal Ilmu Komputer Dan Informatika*, 1(1), 46–52. <https://doi.org/http://dx.doi.org/10.30829/algoritma.v1i01.1309>
- Megantara, R. A., & Rafrastara, F. A. (2019). Super Enkripsi Teks Kriptografi menggunakan Algoritma Hill Cipher dan Transposisi Kolom. *Prosiding SENDI_U 2019*, 85–92.
- Muchlis, B. S., Budiman, M. A., & Rachmawati, D. (2017). Teknik Pemecahan Kunci Algoritma Rivest Shamir Adleman (RSA) dengan Metode Kraitchik. *Jurnal & Penelitian Teknik Informatika*, 2(2), 49–64. <http://jurnal.polgan.ac.id/index.php/sinkron/article/view/75>
- Naing, H. H., & Aye, Z. M. (2020). Innovation Security of Beaufort Cipher by Stream Cipher Using Myanmar-Vigenere Table and Unicode Table. *WCSE 2020: 2020 10th International Workshop on Computer Science and Engineering, Wcse*, 55–56. <https://doi.org/10.18178/wcse.2020.02.009>
- Setiadi, D. R. I. M., Jatmoko, C., Rachmawanto, E. H., & Sari, C. A. (2018a). Kombinasi Cipher Subtitusi (Beaufort Dan Vigenere) Pada Citra Digital. *Proceeding SENDI_U*, 52–57. <https://www.unisbank.ac.id/ojs/index.php/sendu/article/view/5960>
- Setiadi, D. R. I. M., Jatmoko, C., Rachmawanto, E. H., & Sari, C. A. (2018b).

- Kombinasi DCT dan Beaufort Cipher Untuk Peningkatan Keamanan Hak Cipta Citra Digital. *Jurnal Sains & Teknologi*, 7(2), 188–197.
<https://doi.org/https://doi.org/10.23887/jstundiksha.v7i2.13795>
- Soediro. (2018). Prinsip Keamanan, Privasi, dan Etika dalam Undang-undang Informasi dan Transaksi Elektronik dalam Perspektif Hukum Islam. *Kosmik Hukum*, 18(2), 95–112.
- Subada, M. A. (2018). *Analisis Perbandingan Algoritma Even-Rodeh Code dan Algoritma Fibonacci Code Untuk Kompresi File Teks*. Universitas Sumatera Utara.
- Sugiarto, E., Setiadi, D. R. I. M., Fahmi, A., Rachmawanto, E. H., Sari, C. A., Sarker, M. K., & Widjajanto, B. (2020). Securing Text Messages using the Beaufort-Vigenere Hybrid Method. *Journal of Physics: Conference Series*, 1577(1). <https://doi.org/10.1088/1742-6596/1577/1/012032>
- Suhandinata, S., Rizal, R. A., Wijaya, D. O., Warren, P., & Srinjiwi, S. (2019). Analisis Performa Kriptografi Hybrid Algoritma Blowfish Dan Algoritma RSA. *JURTEKSI (Jurnal Teknologi Dan Sistem Informasi)*, 6(1), 1–10.
<https://doi.org/10.33330/jurteks.v6i1.395>
- Sutejo. (2021). Implementasi Algoritma Kriptografi RSA (Rivest Shamir Adleman) Untuk Keamanan Data Rekam Medis Pasien. *INTECOMS: Journal of Information Technology and Computer Science*, 4(1), 104–114.
<https://doi.org/10.31539/intecom.v4i1.2437>
- Syahputra, A., Sundari, S., & ... (2021). Implementasi algoritma Kriptografi Simetris Atbash Cipher dan Teknik Transposisi Segitiga Untuk Pengamanan File Teks. *Seminar ...*
[http://download.garuda.kemdikbud.go.id/article.php?article=2573820%5C&val=24090%5C&title=Implementasi algoritma Kriptografi Simetris Atbash Cipher dan Teknik Transposisi Segitiga Untuk Pengamanan File Teks](http://download.garuda.kemdikbud.go.id/article.php?article=2573820%5C&val=24090%5C&title=Implementasi%20algoritma%20Kriptografi%20Simetris%20Atbash%20Cipher%20dan%20Teknik%20Transposisi%20Segitiga%20Untuk%20Pengamanan%20File%20Teks)

Lampiran 1

LISTING PROGRAM

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <meta content="width=device-width, initial-scale=1.0" name="viewport">
  <title>Beaufort Cipher - RSA</title>
  <meta content="" name="description">
  <meta content="" name="keywords">
  <!-- Favicons -->
  <link href="assets/img/favicon.png" rel="icon">
  <link href="assets/img/apple-touch-icon.png" rel="apple-touch-icon">
  <!-- Google Fonts -->
  <link href="https://fonts.gstatic.com" rel="preconnect">
  <link
href="https://fonts.googleapis.com/css?family=Open+Sans:300,300i,400,400
i,600,600i,700,700i|Nunito:300,300i,400,400i,600,600i,700,700i|Poppins:3
00,300i,400,400i,500,500i,600,600i,700,700i" rel="stylesheet">
  <!-- Vendor CSS Files -->
  <link href="assets/vendor/bootstrap/css/bootstrap.min.css"
rel="stylesheet">
  <link href="assets/vendor/bootstrap-icons/bootstrap-icons.css"
rel="stylesheet">
  <link href="assets/vendor/boxicons/css/boxicons.min.css"
rel="stylesheet">
  <link href="assets/vendor/quill/quill.snow.css" rel="stylesheet">
  <link href="assets/vendor/quill/quill.bubble.css" rel="stylesheet">
  <link href="assets/vendor/remixicon/remixicon.css" rel="stylesheet">
  <link href="assets/vendor/simple-datatables/style.css"
rel="stylesheet">
  <!-- Template Main CSS File -->
  <link href="assets/css/style.css" rel="stylesheet">
</head>

<body>

  <!-- ===== Header ===== -->
  <header id="header" class="header fixed-top d-flex align-items-
center">
    <div class="d-flex align-items-center justify-content-between">
      <a href="index.php" class="logo d-flex align-items-center">
        
        <span class="d-none d-lg-block">UINSU</span>
      </a>
    </div>
  </header>
</body>
</html>
```

```

        </a>
        <i class="bi bi-list toggle-sidebar-btn"></i>
    </div><!-- End Logo -->

    <nav class="header-nav ms-auto">
        <ul class="d-flex align-items-center">
            <li class="nav-item dropdown pe-3">
                <a class="nav-link nav-profile d-flex align-items-center pe-0"
href="#" data-bs-toggle="dropdown">
                    
                    <span class="d-none d-md-block dropdown-toggle ps-
2">Mahyudi</span>
                </a><!-- End Profile Image Icon -->
            </li><!-- End Profile Nav -->
        </ul>
    </nav><!-- End Icons Navigation -->
</header><!-- End Header -->

<!-- ===== Sidebar ===== -->
<aside id="sidebar" class="sidebar">

    <ul class="sidebar-nav" id="sidebar-nav">
        <li class="nav-item">
            <a class="nav-link " href="index.php">
                <i class="bi bi-grid"></i>
                <span>Home</span>
            </a>
        </li><!-- End Dashboard Nav -->

        <li class="nav-item">
            <a class="nav-link collapsed" href="generate-key.php">
                <i class="bi bi-key"></i>
                <span>Bangkitkan Kunci</span>
            </a>
        </li><!-- End Components Bangkitkan Kunci Nav -->

        <li class="nav-item">
            <a class="nav-link collapsed" href="enkripsi.php">
                <i class="bi bi-file-earmark-lock"></i>
                <span>Enkripsi</span>
            </a>
        </li><!-- End Components Enkripsi Nav -->

        <li class="nav-item">

```

```

        <a class="nav-link collapsed" href="dekripsi.php">
            <i class="bi bi-file-earmark-lock"></i>
            <span>Dekripsi</span>
        </a>
    </li><!-- End Components Dekripsi Nav -->

    <li class="nav-heading">Pages</li>

    <li class="nav-item">
        <a class="nav-link collapsed" href="help.php">
            <i class="bi bi-info-circle"></i>
            <span>Help</span>
        </a>
    </li><!-- End Help Page Nav -->

    <li class="nav-item">
        <a class="nav-link collapsed" href="about.php">
            <i class="bi bi-person"></i>
            <span>About</span>
        </a>
    </li><!-- End About Page Nav -->
</ul>

</aside><!-- End Sidebar-->

<main id="main" class="main">

    <div class="pagetitle">
        <h1>Dashboard</h1>
        <nav>
            <ol class="breadcrumb">
                <li class="breadcrumb-item"><a href="index.php">Home</a></li>
                <li class="breadcrumb-item active">Dashboard</li>
            </ol>
        </nav>
    </div><!-- End Page Title -->

    <section class="section dashboard">
        <div class="row">
            <div class="col-xl-12">
                <div class="card">
                    <div class="card-body profile-card pt-4 d-flex flex-column
align-items-center">

```

```
<h5 class="text-center">Implementasi Kombinasi Algoritma  
Beaufort Cipher dan Algoritma RSA <br>
```

```
    Dalam Skema Super Enkripsi Untuk Pengamanan File  
Teks</h5><br>
```

```
    <br>
```

```
    <h5 class="text-center">Mahyudi<br>0701162010</h5><br>
```

```
    <h5 class="text-center">Program Studi Ilmu  
Komputer<br>Fakultas Sains dan Teknologi<br>Universitas Islam Negeri  
Sumatera Utara<br>Medan - 2022
```

```
    </h5>  
    <div class="social-links mt-2">  
        <a href="#" class="twitter"><i class="bi bi-  
twitter"></i></a>  
        <a href="#" class="facebook"><i class="bi bi-  
facebook"></i></a>  
        <a href="#" class="instagram"><i class="bi bi-  
instagram"></i></a>  
        <a href="#" class="linkedin"><i class="bi bi-  
linkedin"></i></a>
```

```
    </div>  
</div>  
</div>  
</div>  
</div>  
</section>  
</main><!-- End #main -->
```

```
<!-- ===== Footer ===== -->  
<footer id="footer" class="footer">  
    <div class="copyright">  
        &copy; Copyright <strong><span>NiceAdmin</span></strong>. All  
Rights Reserved
```

```
    </div>  
    <div class="credits">  
        Designed by <a href="https://bootstrapmade.com/"  
target="_blank">BootstrapMade</a>  
    </div>  
</footer><!-- End Footer -->
```

```
    <a href="#" class="back-to-top d-flex align-items-center justify-  
content-center"><i class="bi bi-arrow-up-short"></i></a>
```

```
<!-- Vendor JS Files -->
```

```

    <script src="assets/vendor/apexcharts/apexcharts.min.js"></script>
    <script
src="assets/vendor/bootstrap/js/bootstrap.bundle.min.js"></script>
    <script src="assets/vendor/chart.js/chart.min.js"></script>
    <script src="assets/vendor/echarts/echarts.min.js"></script>
    <script src="assets/vendor/quill/quill.min.js"></script>
    <script src="assets/vendor/simple-datatables/simple-
datatables.js"></script>
    <script src="assets/vendor/tinymce/tinymce.min.js"></script>
    <script src="assets/vendor/php-email-form/validate.js"></script>
    <!-- Template Main JS File -->
    <script src="assets/js/main.js"></script>

</body>
</html>

<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="utf-8">
    <meta content="width=device-width, initial-scale=1.0" name="viewport">
    <title>Beaufort Cipher - RSA</title>
    <meta content="" name="description">
    <meta content="" name="keywords">
    <!-- Favicons -->
    <link href="assets/img/favicon.png" rel="icon">
    <link href="assets/img/apple-touch-icon.png" rel="apple-touch-icon">
    <!-- Google Fonts -->
    <link href="https://fonts.gstatic.com" rel="preconnect">
    <link
href="https://fonts.googleapis.com/css?family=Open+Sans:300,300i,400,400
i,600,600i,700,700i|Nunito:300,300i,400,400i,600,600i,700,700i|Poppins:3
00,300i,400,400i,500,500i,600,600i,700,700i" rel="stylesheet">
    <!-- Vendor CSS Files -->
    <link href="assets/vendor/bootstrap/css/bootstrap.min.css"
rel="stylesheet">
    <link href="assets/vendor/bootstrap-icons/bootstrap-icons.css"
rel="stylesheet">
    <link href="assets/vendor/boxicons/css/boxicons.min.css"
rel="stylesheet">
    <link href="assets/vendor/quill/quill.snow.css" rel="stylesheet">
    <link href="assets/vendor/quill/quill.bubble.css" rel="stylesheet">
    <link href="assets/vendor/remixicon/remixicon.css" rel="stylesheet">

```



```

if($primaP && $primaQ)
{
    $time_start = microtime(true); // Timer mulai eksekusi

    //menghitung dan menampilkan n=p*q
    $nilaiN = gmp_mul($bilPrimaP,$bilPrimaQ);

    //menghitung dan menampilkan totient/phi=(p-1)(q-1)
    $nilaiTotient =
gmp_mul(gmp_sub($bilPrimaP,1),gmp_sub($bilPrimaQ,1));
    //echo 'totient='.gmp_strval($totient). "\n";

    //mencari e, dimana e merupakan coprime dari totient
    //e dikatakan coprime dari totient jika gcd/fpb dari e dan
totient/phi = 1
    for($nilaiE = 2;$nilaiE < 100;$nilaiE++) { //mencoba
perulangan max 100 kali,
        $gcd = gmp_gcd($nilaiE, $nilaiTotient);
        if(gmp_strval($gcd) == '1')
            break;
    }

    //menghitung & menampilkan d
    $i = 1;
    do {
        $res = gmp_div_qr(gmp_add(gmp_mul($nilaiTotient,$i),1),
$nilaiE);
        //echo '((totient*'. $i .' ) + 1) / e='.gmp_strval($res[0])." ";
        sisa= ".gmp_strval($res[1])."\n";
        $i++;
        if($i == 10000) //maksimal percobaan 10000
            break;
    } while(gmp_strval($res[1])!='0');
    $nilaiD = $res[0];

    $time_end = microtime(true); // Timer stop eksekusi
    // Waktu Eksekusi
    $duration = $time_end - $time_start;
}
}

} else if(isset($_POST['btnAutoGenerateKey'])) {
    $time_start = microtime(true); // Timer mulai eksekusi

    $rand1 = rand(100,500);

```

```

$rand2 = rand(500,900);

// mencari bilangan prima selanjutnya dari $rand1 &rand2
$bilPrimaP = gmp_nextprime($rand1);
$bilPrimaQ = gmp_nextprime($rand2);

//menghitung&menampilkan n=p*q
$nilaiN = gmp_mul($bilPrimaP,$bilPrimaQ);

//menghitung&menampilkan totient/phi=(p-1)(q-1)
$nilaiTotient =
gmp_mul(gmp_sub($bilPrimaP,1),gmp_sub($bilPrimaQ,1));
//echo 'totient='.gmp_strval($totient). "\n";

//mencari e, dimana e merupakan coprime dari totient
//e dikatakan coprime dari totient jika gcd/fpb dari e dan
totient/phi = 1
for($nilaiE = 2;$nilaiE < 100;$nilaiE++){ //mencoba perulangan
max 100 kali,
    $gcd = gmp_gcd($nilaiE, $nilaiTotient);
    if(gmp_strval($gcd) == '1')
        break;
}

//menghitung & menampilkan d
$i = 1;
do {
    $res = gmp_div_qr(gmp_add(gmp_mul($nilaiTotient,$i),1),
$nilaiE);
    //echo '((totient*'. $i. ') + 1) / e='.gmp_strval($res[0])." ";
    sisa= ".gmp_strval($res[1])."\n";
    $i++;
    if($i == 10000) //maksimal percobaan 10000
        break;
} while (gmp_strval($res[1])!='0');
$nilaiD = $res[0];

$time_end = microtime(true); // Timer stop eksekusi
// Waktu Eksekusi
$duration = $time_end - $time_start;
}
?>

<!-- Simpan kunci publik -->
<?php

```

```

if(isset($_POST['btnSavePubkey'])) {
    $data_n = $_POST["nilaiN"];
    $data_e = $_POST["nilaiE"];
    $file = fopen('KunciPublik.txt', 'a');
    ftruncate($file, 0); //Clear the file to 0bit
    $content = $data_n. PHP_EOL .$data_e;
    fwrite($file, $content);
    fclose($file);
}
?>

<!-- Simpan kunci privat -->
<?php
if(isset($_POST['btnSavePrivkey'])) {
    $data_n = $_POST["nilaiN"];
    $data_d = $_POST["nilaiD"];
    $file = fopen('KunciPrivat.txt', 'a');
    ftruncate($file, 0); //Clear the file to 0bit
    $content = $data_n. PHP_EOL .$data_d;
    fwrite($file, $content);
    fclose($file);
}
?>

<!-- ===== Header ===== -->
<header id="header" class="header fixed-top d-flex align-items-center">
    <div class="d-flex align-items-center justify-content-between">
        <a href="index.php" class="logo d-flex align-items-center">
            
            <span class="d-none d-lg-block">UINSU</span>
        </a>
        <i class="bi bi-list toggle-sidebar-btn"></i>
    </div><!-- End Logo -->
    <nav class="header-nav ms-auto">
        <ul class="d-flex align-items-center">
            <li class="nav-item dropdown pe-3">
                <a class="nav-link nav-profile d-flex align-items-center pe-0"
href="#" data-bs-toggle="dropdown">
                    
                    <span class="d-none d-md-block dropdown-toggle ps-2">Mahyudi</span>
                </a><!-- End Profile Iamge Icon -->
            </li><!-- End Profile Nav -->

```

```

        </ul>
    </nav><!-- End Icons Navigation -->
</header><!-- End Header -->

<!-- ===== Sidebar ===== -->
<aside id="sidebar" class="sidebar">

    <ul class="sidebar-nav" id="sidebar-nav">
        <li class="nav-item">
            <a class="nav-link " href="index.php">
                <i class="bi bi-grid"></i>
                <span>Home</span>
            </a>
        </li><!-- End Dashboard Nav -->

        <li class="nav-item">
            <a class="nav-link collapsed" href="generate-key.php">
                <i class="bi bi-key"></i>
                <span>Bangkitkan Kunci</span>
            </a>
        </li><!-- End Components Bangkitkan Kunci Nav -->

        <li class="nav-item">
            <a class="nav-link collapsed" href="enkripsi.php">
                <i class="bi bi-file-earmark-lock"></i>
                <span>Enkripsi</span>
            </a>
        </li><!-- End Components Enkripsi Nav -->

        <li class="nav-item">
            <a class="nav-link collapsed" href="dekripsi.php">
                <i class="bi bi-file-earmark-lock"></i>
                <span>Dekripsi</span>
            </a>
        </li><!-- End Components Dekripsi Nav -->

        <li class="nav-heading">Pages</li>

        <li class="nav-item">
            <a class="nav-link collapsed" href="help.php">
                <i class="bi bi-info-circle"></i>
                <span>Help</span>
            </a>
        </li><!-- End Help Page Nav -->

```

```

        <li class="nav-item">
            <a class="nav-link collapsed" href="about.php">
                <i class="bi bi-person"></i>
                <span>About</span>
            </a>
        </li><!-- End About Page Nav -->
    </ul>

</aside><!-- End Sidebar-->

<main id="main" class="main">

    <div class="pagetitle">
        <h1>Generate Key</h1>
        <nav>
            <ol class="breadcrumb">
                <li class="breadcrumb-item"><a href="index.php">Home</a></li>
                <li class="breadcrumb-item active">Bangkitkan Kunci RSA</li>
            </ol>
        </nav>
    </div><!-- End Page Title -->

    <section class="section">
        <div class="row">
            <div class="col-lg-8">
                <!-- Card with header and footer -->
                <div class="card">
                    <div class="card-header">Bangkitkan Kunci Publik dan Kunci
Privat Algoritma RSA</div>
                    <div class="card-body pt-3">
                        <!-- Multi Columns Form -->
                        <form id="enkripsi" name="enkripsi" method="post"
action="" class="row g-3">
                            <div class="col-md-6">
                                <label for="input-p" class="form-label">Bilangan Prima
p</label>

                                <?php if(isset($_POST['btnAutoGenerateKey'])) { ?>
                                    <input type="number" name="txtP" id="txtP"
placeholder="Nilai p" class="form-control" value="<?php echo $bilPrimaP;
?>" />

                                    <?php }else{ ?>
                                        <input type="number" name="txtP" id="txtP"
placeholder="Nilai p" class="form-control" value="<?php echo
isset($_POST['txtP']) ? $_POST['txtP'] : '' ?>" maxlength="3" />

```

```

        <?php } ?>
    </div>
    <div class="col-md-6">
        <label for="input-q" class="form-label">Bilangan Prima
q</label>

        <?php if(isset($_POST['btnAutoGenerateKey'])) { ?>
            <input type="number" name="txtQ" id="txtQ"
placeholder="Nilai q" class="form-control" value="<?php echo $bilPrimaQ;
?>" />

            <?php }else{ ?>
                <input type="number" name="txtQ" id="txtQ"
placeholder="Nilai q" class="form-control" value="<?php echo
isset($_POST['txtQ']) ? $_POST['txtQ'] : '' ?>" maxlength="3" />
                <?php } ?>
            </div>
            <div class="text-center pt-3">
                <button type="submit" name="btnAutoGenerateKey"
id="btnAutoGenerateKey" class="btn btn-success btn-sm">
                    <i class="bi bi-check-circle"></i> Auto Generate
Key</button>

                <button type="submit" name="btnGenerateKey"
id="btnGenerateKey" class="btn btn-outline-primary btn-sm">
                    <i class="bi bi-check-circle"></i> Generate
Key</button>

                <button type="submit" name="btnSavePubkey" class="btn
btn-outline-danger btn-sm">
                    <i class="bi bi-check-circle"></i> Save Public
Key</button>

                <button type="submit" name="btnSavePrivkey" class="btn
btn-outline-info btn-sm">
                    <i class="bi bi-check-circle"></i> Save Private
Key</button>
            </div>
            <div class="col-md-6 pt-3">
                <label for="nilai-n" class="form-label">Nilai n = (p *
q)</label>

                <?php
if(isset($_POST['btnGenerateKey']) || isset($_POST['btnAutoGenerateKey']))
{ ?>
                    <input type="number" name="nilaiN" id="nilaiN"
class="form-control" value="<?php echo $nilaiN; ?>" readonly>
                    <?php }else{ ?>
                        <input type="number" name="nilaiN" id="nilaiN"
class="form-control" value="<?php echo isset($_POST['nilaiN']) ?
$_POST['nilaiN'] : '' ?>" readonly>

```

```

        <?php } ?>
    </div>
    <div class="col-md-6 pt-3">
        <label for="nilai-totien" class="form-label">Nilai
Totient = (p - 1)(q - 1)</label>
        <?php
if(isset($_POST['btnGenerateKey'])||isset($_POST['btnAutoGenerateKey']))
{ ?>
            <input type="number" name="nilaiTotient"
id="nilaiTotient" class="form-control" value="<?php echo $nilaiTotient;
?>" readonly>
            <?php }else{ ?>
                <input type="number" name="nilaiTotient"
id="nilaiTotient" class="form-control" value="<?php echo
isset($_POST['nilaiTotient']) ? $_POST['nilaiTotient'] : '' ?>"
readonly>
            <?php } ?>
        </div>
        <div class="col-md-6">
            <label for="nilai-e" class="form-label">Nilai
e</label>
            <?php
if(isset($_POST['btnGenerateKey'])||isset($_POST['btnAutoGenerateKey']))
{ ?>
                <input type="number" name="nilaiE" id="nilaiE"
class="form-control" value="<?php echo $nilaiE; ?>" readonly>
                <?php }else{ ?>
                    <input type="number" name="nilaiE" id="nilaiE"
class="form-control" value="<?php echo isset($_POST['nilaiE']) ?
$_POST['nilaiE'] : '' ?>" readonly>
                <?php } ?>
            </div>
            <div class="col-md-6">
                <label for="nilai-d" class="form-label">Nilai
d</label>
                <?php
if(isset($_POST['btnGenerateKey'])||isset($_POST['btnAutoGenerateKey']))
{ ?>
                    <input type="number" name="nilaiD" id="nilaiD"
class="form-control" value="<?php echo $nilaiD; ?>" readonly>
                    <?php }else{ ?>
                        <input type="number" name="nilaiD" id="nilaiD"
class="form-control" value="<?php echo isset($_POST['nilaiD']) ?
$_POST['nilaiD'] : '' ?>" readonly>
                    <?php } ?>
                </div>
            </div>
        </div>
    </div>

```

```

        </div>
        <div class="col-md-6">
            <label for="public-key" class="form-label">Kunci
Publik (n, e)</label>
            <?php
if(isset($_POST['btnGenerateKey'])||isset($_POST['btnAutoGenerateKey']))
{ ?>
                <input type="text" name="publicKey" id="publicKey"
class="form-control" value="<?php echo $nilaiN . ', ' . $nilaiE; ?>"
readonly>
                <?php }else{ ?>
                <input type="text" name="publicKey" id="publicKey"
class="form-control" value="0" readonly>
                <?php } ?>
            </div>
            <div class="col-md-6">
                <label for="private-key" class="form-label">Kunci
Privat (n, d)</label>
                <?php
if(isset($_POST['btnGenerateKey'])||isset($_POST['btnAutoGenerateKey']))
{ ?>
                    <input type="text" name="privateKey" id="privateKey"
class="form-control" value="<?php echo $nilaiN . ', ' . $nilaiD; ?>"
readonly>
                    <?php }else{ ?>
                    <input type="text" name="privateKey" id="privateKey"
class="form-control" value="0" readonly>
                    <?php } ?>
                </div>
            </form><!-- End Multi Columns Form -->
        </div>
        <div class="card-footer">
            <?php
if(isset($_POST['btnGenerateKey'])||isset($_POST['btnAutoGenerateKey']))
{ ?>
                <p class="text-center"><i>Running Time <span
class="badge bg-primary"><?php echo $duration; ?></span> Detik</i></p>
                <?php } ?>
            </div>
        </div><!-- End Card with header and footer -->
    </div>
    <div class="col-lg-4">
        <!-- Card with header and footer -->
        <div class="card">
            <div class="card-header">Cek Bilangan Prima</div>

```



```

<div class="card-body pt-3">
  <!-- Vertical Form -->
  <form method="post" action="" class="row g-3">
    <div class="col-12">
      <label for="input-bil-prima" class="form-label">Masukkan Angka</label>
      <input type="number" name="txtAngka" class="form-control" value="<?php echo isset($_POST['txtAngka']) ? $_POST['txtAngka'] : '' ?>" required>
    </div>
    <div class="text-center pt-3">
      <button type="submit" name="btnCekPrima" id="btnCekPrima" class="btn btn-secondary btn-sm">
        <i class="bi bi-check-circle"></i> Cek
      Angka</button>
    </div>
  </form><br>

<?php
  if (isset($_POST['btnCekPrima']))
  {
    $n = $_POST['txtAngka'];
    $prima = true;
    for($i = 2; $i <= ($n / 2); $i++)
    {
      if(($n % $i) == 0)
      {
        $prima = false;
        break; //untuk menghentikan looping pada program
      }
    }
    if($prima)
    {
      echo '
      <h6>
        <span class="badge border-primary border-1 text-primary">Angka</span>
        <span class="badge bg-success">'. $n .'</span><b>
        <span class="badge border-success border-1 text-success">Adalah Bilangan Prima</span>
      </h6>';
    } else {
      echo '
      <h6>

```

```

        <span class="badge border-primary border-1 text-
primary">Angka</span>
        <span class="badge bg-danger">'.$n.'</span>
        <span class="badge border-danger border-1 text-
danger">Bukan Bilangan Prima</span>
    </h6>';
    }
}
?>

</div>
</div>
</div>
</div>
</section>

</main><!-- End #main -->

<!-- ===== Footer ===== -->
<footer id="footer" class="footer">
    <div class="copyright">
        &copy; Copyright <strong><span>NiceAdmin</span></strong>. All
Rights Reserved
    </div>
    <div class="credits">
        Designed by <a href="https://bootstrapmade.com/"
target="_blank">BootstrapMade</a>
    </div>
</footer><!-- End Footer -->

    <a href="#" class="back-to-top d-flex align-items-center justify-
content-center"><i class="bi bi-arrow-up-short"></i></a>

<!-- Vendor JS Files -->
<script src="assets/vendor/apexcharts/apexcharts.min.js"></script>
<script
src="assets/vendor/bootstrap/js/bootstrap.bundle.min.js"></script>
<script src="assets/vendor/chart.js/chart.min.js"></script>
<script src="assets/vendor/echarts/echarts.min.js"></script>
<script src="assets/vendor/quill/quill.min.js"></script>
<script src="assets/vendor/simple-datatables/simple-
datatables.js"></script>
<script src="assets/vendor/tinymce/tinymce.min.js"></script>
<script src="assets/vendor/php-email-form/validate.js"></script>

```



```

<!-- Template Main JS File -->
<script src="assets/js/main.js"></script>

</body>
</html>

<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <meta content="width=device-width, initial-scale=1.0" name="viewport">
  <title>Beaufort Cipher - RSA</title>
  <meta content="" name="description">
  <meta content="" name="keywords">
  <!-- Favicons -->
  <link href="assets/img/favicon.png" rel="icon">
  <link href="assets/img/apple-touch-icon.png" rel="apple-touch-icon">
  <!-- Google Fonts -->
  <link href="https://fonts.gstatic.com" rel="preconnect">
  <link
href="https://fonts.googleapis.com/css?family=Open+Sans:300,300i,400,400
i,600,600i,700,700i|Nunito:300,300i,400,400i,600,600i,700,700i|Poppins:3
00,300i,400,400i,500,500i,600,600i,700,700i" rel="stylesheet">
  <!-- Vendor CSS Files -->
  <link href="assets/vendor/bootstrap/css/bootstrap.min.css"
rel="stylesheet">
  <link href="assets/vendor/bootstrap-icons/bootstrap-icons.css"
rel="stylesheet">
  <link href="assets/vendor/boxicons/css/boxicons.min.css"
rel="stylesheet">
  <link href="assets/vendor/quill/quill.snow.css" rel="stylesheet">
  <link href="assets/vendor/quill/quill.bubble.css" rel="stylesheet">
  <link href="assets/vendor/remixicon/remixicon.css" rel="stylesheet">
  <link href="assets/vendor/simple-datatables/style.css"
rel="stylesheet">
  <!-- Template Main CSS File -->
  <link href="assets/css/style.css" rel="stylesheet">
</head>

<body>

  <!-- Enkripsi RSA -->
  <?php
    $cipherteksRSA = "";

```

```

if(isset($_POST['btnEnkripRSA'])) {
    $kunciN = $_POST['txtN'];
    $kunciE = $_POST['txtE'];
    $plaintexts = $_POST['txtCipherteksBeaufort'];

    $time_start = microtime(true); // Timer mulai eksekusi

    //pesan dikodekan menjadi kode ascii, kemudian di enkripsi per
    karakter
    for($i = 0;$i < strlen($plaintexts);++$i) {
        //rumus enkripsi  $c = m^e \text{ mod } n$ 
        $cipherteksRSA.=
(gmp_mod(gmp_pow(ord($plaintexts[$i]),$kunciE),$kunciN));
        //tiap karakter hasil enkripsi dipisahkan dengan "."
        if($i != strlen($plaintexts) - 1) {
            $cipherteksRSA.= ".";
        }
    }

    $time_end = microtime(true); // Timer stop eksekusi
    // Waktu Eksekusi
    $duration = $time_end - $time_start;
}
?>

<!-- Simpan Hasil Enkripsi (Cipherteks)-->
<?php
if(isset($_POST['btnSaveCipherteks'])) {
    $data_cipherteks = trim($_POST['txtCipherteksRSA']);
    $file = fopen('HasilEnkripsi.txt', 'a');
    ftruncate($file, 0); //Clear the file to 0bit
    $content = $data_cipherteks;
    fwrite($file, $content);
    fclose($file);
}
?>

<!-- ===== Header ===== -->
<header id="header" class="header fixed-top d-flex align-items-
center">
    <div class="d-flex align-items-center justify-content-between">
        <a href="index.php" class="logo d-flex align-items-center">
            
            <span class="d-none d-lg-block">UINSU</span>
        </a>

```

```

        <i class="bi bi-list toggle-sidebar-btn"></i>
    </div><!-- End Logo -->
    <nav class="header-nav ms-auto">
        <ul class="d-flex align-items-center">
            <li class="nav-item dropdown pe-3">
                <a class="nav-link nav-profile d-flex align-items-center pe-0"
href="#" data-bs-toggle="dropdown">
                    
                    <span class="d-none d-md-block dropdown-toggle ps-
2">Mahyudi</span>
                </a><!-- End Profile Image Icon -->
            </li><!-- End Profile Nav -->
        </ul>
    </nav><!-- End Icons Navigation -->
</header><!-- End Header -->

<!-- ===== Sidebar ===== -->
<aside id="sidebar" class="sidebar">

    <ul class="sidebar-nav" id="sidebar-nav">
        <li class="nav-item">
            <a class="nav-link " href="index.php">
                <i class="bi bi-grid"></i>
                <span>Home</span>
            </a>
        </li><!-- End Dashboard Nav -->

        <li class="nav-item">
            <a class="nav-link collapsed" href="generate-key.php">
                <i class="bi bi-key"></i>
                <span>Bangkitkan Kunci</span>
            </a>
        </li><!-- End Components Bangkitkan Kunci Nav -->

        <li class="nav-item">
            <a class="nav-link collapsed" href="enkripsi.php">
                <i class="bi bi-file-earmark-lock"></i>
                <span>Enkripsi</span>
            </a>
        </li><!-- End Components Enkripsi Nav -->

        <li class="nav-item">
            <a class="nav-link collapsed" href="dekripsi.php">
                <i class="bi bi-file-earmark-lock"></i>

```



```

        <form id="enkripsi" name="enkripsi" method="post"
action="" class="row g-3" enctype="multipart/form-data">
        <!-- <div class="col-md-12">
            <label for="file-kunci-rsa" class="form-
label">Masukkan Kunci Publik RSA</label>
            <input type="file" name="file-kunci" id="file-kunci"
class="form-control">
        </div> -->
        <div class="col-md-4">
            <button type="submit" name="btnReadKunci"
id="btnReadKunci" class="btn btn-secondary btn-sm">
                <i class="bi bi-check-circle"></i> Read Kunci Publik
RSA</button>
        </div>
        <div class="col-md-4">
            <?php if(isset($_POST['btnReadKunci'])) {
                $fileKunci = fopen("KunciPublik.txt", "r");
                $kunciN = fgets($fileKunci); //fgets -> untuk
mengambil baris pertama dari file teks
                fclose($fileKunci);
            ?>
            <!-- <label for="n" class="form-label">Nilai n</label>
-->
            <input type="text" name="txtN" id="txtN" value="<?php
echo $kunciN; ?>" class="form-control" placeholder="Kunci Publik RSA
(n)">
            <?php }else{ ?>
            <!-- <label for="n" class="form-label">Nilai n</label>
-->
            <input type="text" name="txtN" id="txtN" class="form-
control" placeholder="Kunci Publik RSA (n)">
            <?php } ?>
        </div>
        <div class="col-md-4">
            <?php if(isset($_POST['btnReadKunci'])) {
                $fileKunci = "KunciPublik.txt";
                $lines = file($fileKunci); //file teks dimasukkan
kedalam array
                $kunciE = $lines[1]; // untuk mengambil baris kedua
dari file teks
            ?>
            <!-- <label for="e" class="form-label">Nilai e</label>
-->

```

```

        <input type="text" name="txtE" id="txtE" value="<?php
echo $kunciE; ?>" class="form-control" placeholder="Kunci Publik RSA
(e)">
        <?php }else{ ?>
        <!-- <label for="e" class="form-label">Nilai e</label>
-->
        <input type="text" name="txtE" id="txtE" class="form-
control" placeholder="Kunci Publik RSA (e)">
        <?php } ?>
</div>
<div class="col-md-12">
    <label for="file-plainteks" class="form-
label">Masukkan File Teks (Plainteks)</label>
    <input type="file" name="file" id="file" class="form-
control">
</div>
<div class="col-md-12">
    <textarea id="txtPlainteks" name="txtPlainteks"
class="form-control" placeholder="Plainteks" style="height:
100px"></textarea>
</div>
<div class="col-md-12">
    <label for="kunci-beaufort" class="form-
label">Masukkan Kunci Beaufort Cipher</label>
    <input type="text" id="txtKeyBeaufort" class="form-
control" placeholder="Kunci Beaufort Cipher">
</div>
<div class="text-center pt-3">
    <button type="button" onclick="enkripsiBeaufort()"
class="btn btn-outline-danger btn-sm"><i class="bi bi-check-circle"></i>
Enkripsi Beaufort</button>
    <button type="submit" name="btnEnkripRSA"
id="btnEnkripRSA" class="btn btn-outline-primary btn-sm"><i class="bi
bi-check-circle"></i> Enkripsi RSA</button>
    <button type="submit" name="btnSaveCipherteks"
id="btnSaveCipherteks" class="btn btn-outline-success btn-sm"><i
class="bi bi-check-circle"></i> Simpan Cipherteks</button>
</div>
<div class="col-md-6 pt-3">
    <label for="hasil-enkripsiBeaufort" class="form-
label">Hasil Enkripsi (Cipherteks) Beaufort Cipher</label>
    <textarea id="txtCipherteksBeaufort"
name="txtCipherteksBeaufort" class="form-control"
placeholder="Cipherteks Beaufort Cipher" style="height:
100px"></textarea>

```



```

        </div>
        <div class="col-md-6 pt-3">
            <label for="hasil-enkripsiRSA" class="form-
label">Hasil Enkripsi (Cipherteks) RSA</label>
            <?php if(isset($_POST['btnEnkripRSA'])) { ?>
                <textarea name="txtCipherteksRSA"
id="txtCipherteksRSA" class="form-control" placeholder="Cipherteks RSA"
style="height: 100px" readonly><?php echo $cipherteksRSA;
?></textarea>

                <?php } else { ?>
                    <textarea name="txtCipherteksRSA"
id="txtCipherteksRSA" class="form-control" placeholder="Cipherteks RSA"
style="height: 100px" readonly><?php echo
isset($_POST['txtCipherteksRSA']) ? $_POST['txtCipherteksRSA'] : ''
?></textarea>

                <?php } ?>
            </div>
        </form>
    </div><!-- End Card -->
    <div class="card-footer">
        <?php if(isset($_POST['btnEnkripRSA'])) { ?>
            <p class="text-center"><i>Running Time <span
class="badge bg-primary"><?php echo $duration; ?></span> Detik</i></p>
            <?php } ?>
        </div>
    </div><!-- End Column -->

</div><!-- End Row -->
</section>

</main><!-- End #main -->

<!-- ===== Footer ===== -->
<footer id="footer" class="footer">
    <div class="copyright">
        &copy; Copyright <strong><span>NiceAdmin</span></strong>. All
Rights Reserved
    </div>
    <div class="credits">
        Designed by <a href="https://bootstrapmade.com/"
target="_blank">BootstrapMade</a>
    </div>
</footer><!-- End Footer -->

```

```
<a href="#" class="back-to-top d-flex align-items-center justify-content-center"><i class="bi bi-arrow-up-short"></i></a>
```

```
<!-- Vendor JS Files -->
<script src="assets/vendor/apexcharts/apexcharts.min.js"></script>
<script
src="assets/vendor/bootstrap/js/bootstrap.bundle.min.js"></script>
<script src="assets/vendor/chart.js/chart.min.js"></script>
<script src="assets/vendor/echarts/echarts.min.js"></script>
<script src="assets/vendor/quill/quill.min.js"></script>
<script src="assets/vendor/simple-datatables/simple-
datatables.js"></script>
<script src="assets/vendor/tinymce/tinymce.min.js"></script>
<script src="assets/vendor/php-email-form/validate.js"></script>
<!-- Template Main JS File -->
<script src="assets/js/main.js"></script>

<!-- Open File Teks -->
<script>
    const $output = document.getElementById('txtPlainteks');
    document.getElementById('file').onchange = function() {
        // ambil file yang dipilih oleh user
        const file = this.files[0];

        // cek apakah file bertipe .txt
        if (file.type === 'text/plain') {
            // cek ukuran file, tidak boleh melebihi 169 kb
            if (file.size > 169 * 1000) {
                alert("Ukuran file teks terlalu besar, maksimal 169 kb");
                this.value = null; // reset file input
                return;
            }
            // jika file bertipe .txt, baca isi file menggunakan FileReader
            const reader = new FileReader();
            reader.onload = function(progressEvent) {
                // Entire file
                const text = this.result;
                $output.innerHTML = text;

                // By lines
                var lines = text.split('\n');
                for (var line = 0; line < lines.length; line++) {
                    console.log(lines[line]);
                }
            }
        }
    }

```

```

    };
    reader.readAsText(file);
} else {
    // jika file bukan bertipe .txt, tampilkan pesan error
    alert("File yang dipilih bukan merupakan file .txt");
    // console.error('File yang dipilih bukan merupakan file .txt');
    this.value = null;
    return;
}
};
</script>

```

```

<!-- Enkripsi Beaufort Cipher -->

```

```

<script>

```

```

function isUpperCase(letter) {
    var l = letter.charCodeAt();
    if(l > 64 && l < 91) {
        return true;
    } else {
        return false;
    }
}

```

```

function isLowerCase(letter) {
    let l = letter.charCodeAt();
    if(l > 96 && l < 123) {
        return true;
    } else {
        return false;
    }
}

```

```

function isLetter(letter) {
    if(isLowerCase(letter) || isUpperCase(letter)) {
        return true;
    } else {
        return false;
    }
}

```

```

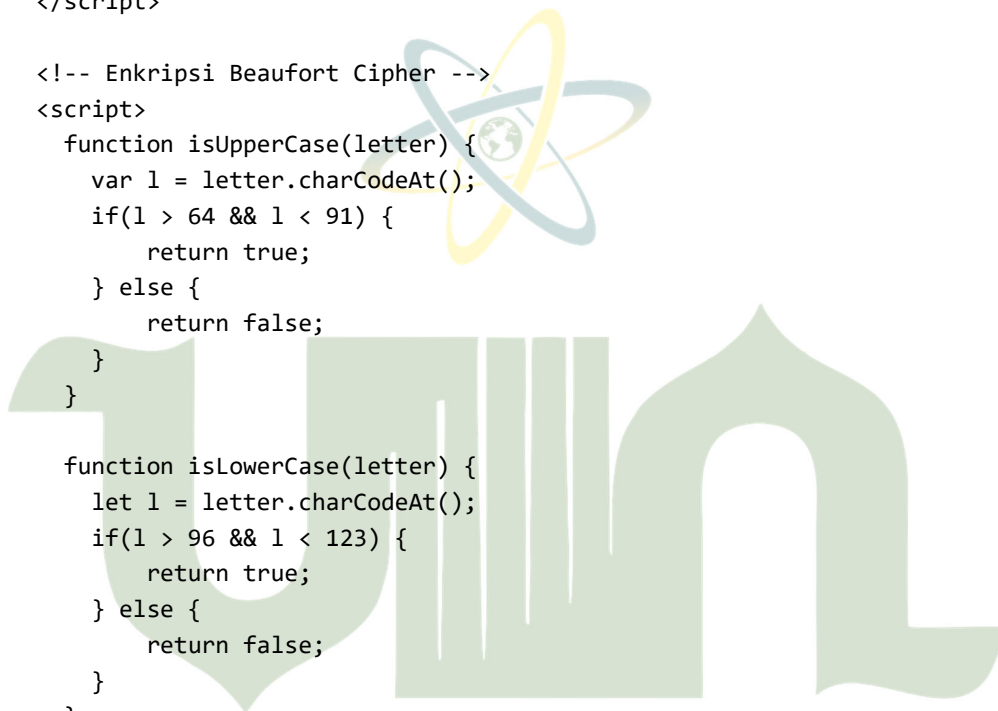
function mod(n, m) {
    return ((n % m) + m) % m;
}

```

```

function enkripsiBeaufort() {

```



UNIVERSITAS ISLAM NEGERI
SUMATERA UTARA MEDAN

```

let encrypted = "";
plaintext = document.getElementById("txtPlainteks").value;
key = document.getElementById("txtKeyBeaufort").value;

if (plaintext==" " && key==" ") {
    return alert("Plainteks dan Kunci Beaufort tidak boleh kosong");
}
else if(plaintext=="") {
    return alert("Plainteks tidak boleh kosong");
}
else if(key=="") {
    return alert("Kunci Beaufort tidak boleh kosong");
}

let j = 0;
for (let i = 0; i < plaintext.length; i++) {
    let currentLetter = plaintext[i];
    const A = 65; // A = 65 adalah nilai desimal dalam tabel ASCII
    const a = 97; // a = 97 adalah nilai desimal dalam tabel ASCII

    if(isUpperCase(currentLetter)) {
        let Pi = (currentLetter.charCodeAt(0) - A);
        let Ki = (key[j % key.length].toUpperCase().charCodeAt() - A);
        let upperLetter = mod(Ki - Pi, 26);

        encrypted += String.fromCharCode(upperLetter + A);

        j++;
    } else if(isLowerCase(currentLetter)) {
        let Pi = (currentLetter.charCodeAt() - a);
        let Ki = (key[j % key.length].toLowerCase().charCodeAt() - a);
        let lowerLetter = mod(Ki - Pi, 26);

        encrypted += String.fromCharCode(lowerLetter + a);

        j++;
    } else {
        encrypted += currentLetter;
    }
}
document.getElementById("txtCipherteksBeaufort").innerHTML=encrypt
ed;
}
</script>

```

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

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <meta content="width=device-width, initial-scale=1.0" name="viewport">
  <title>Beaufort Cipher - RSA</title>
  <meta content="" name="description">
  <meta content="" name="keywords">
  <!-- Favicons -->
  <link href="assets/img/favicon.png" rel="icon">
  <link href="assets/img/apple-touch-icon.png" rel="apple-touch-icon">
  <!-- Google Fonts -->
  <link href="https://fonts.gstatic.com" rel="preconnect">
  <link
href="https://fonts.googleapis.com/css?family=Open+Sans:300,300i,400,400
i,600,600i,700,700i|Nunito:300,300i,400,400i,600,600i,700,700i|Poppins:3
00,300i,400,400i,500,500i,600,600i,700,700i" rel="stylesheet">
  <!-- Vendor CSS Files -->
  <link href="assets/vendor/bootstrap/css/bootstrap.min.css"
rel="stylesheet">
  <link href="assets/vendor/bootstrap-icons/bootstrap-icons.css"
rel="stylesheet">
  <link href="assets/vendor/boxicons/css/boxicons.min.css"
rel="stylesheet">
  <link href="assets/vendor/quill/quill.snow.css" rel="stylesheet">
  <link href="assets/vendor/quill/quill.bubble.css" rel="stylesheet">
  <link href="assets/vendor/remixicon/remixicon.css" rel="stylesheet">
  <link href="assets/vendor/simple-datatables/style.css"
rel="stylesheet">
  <!-- Template Main CSS File -->
  <link href="assets/css/style.css" rel="stylesheet">
</head>

<body>

  <!-- Dekripsi RSA -->
  <?php
    $plainteksRSA = "";
    if(isset($_POST['btnDekripRSA']))
    {
```

```

    $kunciN = $_POST['txtN'];
    $kunciD = $_POST['txtD'];
    //pesan hasil enkripsi (cipherteks) dipecah menjadi array dengan
    batasan "."
    $cipherteks = explode(".",$_POST['txtCipherteks']);
    foreach($cipherteks as $nilai)
    {
        //rumus dekripsi  $m = c ^ d \text{ mod } n$ 
        $plaintextsRSA.=
chr(gmp_strval(gmp_mod(gmp_pow($nilai,$kunciD),$kunciN)));
    }
}
?>

<!-- Simpan Hasil Dekripsi (Plainteks)-->
<?php
    if(isset($_POST['btnSavePlainteks'])) {
        $data_plainteks = trim($_POST['txtPlainteksBeaufort']);
        $file = fopen('HasilDekripsi.txt', 'a');
        ftruncate($file, 0); //Clear the file to 0bit
        $content = $data_plainteks;
        fwrite($file, $content);
        fclose($file);
    }
?>

<!-- ===== Header ===== -->
<header id="header" class="header fixed-top d-flex align-items-
center">
    <div class="d-flex align-items-center justify-content-between">
        <a href="index.php" class="logo d-flex align-items-center">
            
            <span class="d-none d-lg-block">UINSU</span>
        </a>
        <i class="bi bi-list toggle-sidebar-btn"></i>
    </div><!-- End Logo -->
    <nav class="header-nav ms-auto">
        <ul class="d-flex align-items-center">
            <li class="nav-item dropdown pe-3">
                <a class="nav-link nav-profile d-flex align-items-center pe-0"
href="#" data-bs-toggle="dropdown">
                    
                    <span class="d-none d-md-block dropdown-toggle ps-
2">Mahyudi</span>

```

```

        </a><!-- End Profile Iamge Icon -->
    </li><!-- End Profile Nav -->
</ul>
</nav><!-- End Icons Navigation -->
</header><!-- End Header -->

<!-- ===== Sidebar ===== -->
<aside id="sidebar" class="sidebar">

    <ul class="sidebar-nav" id="sidebar-nav">
        <li class="nav-item">
            <a class="nav-link " href="index.php">
                <i class="bi bi-grid"></i>
                <span>Home</span>
            </a>
        </li><!-- End Dashboard Nav -->

        <li class="nav-item">
            <a class="nav-link collapsed" href="generate-key.php">
                <i class="bi bi-key"></i>
                <span>Bangkitkan Kunci</span>
            </a>
        </li><!-- End Components Bangkitkan Kunci Nav -->

        <li class="nav-item">
            <a class="nav-link collapsed" href="enkripsi.php">
                <i class="bi bi-file-earmark-lock"></i>
                <span>Enkripsi</span>
            </a>
        </li><!-- End Components Enkripsi Nav -->

        <li class="nav-item">
            <a class="nav-link collapsed" href="dekripsi.php">
                <i class="bi bi-file-earmark-lock"></i>
                <span>Dekripsi</span>
            </a>
        </li><!-- End Components Dekripsi Nav -->

        <li class="nav-heading">Pages</li>

        <li class="nav-item">
            <a class="nav-link collapsed" href="help.php">
                <i class="bi bi-info-circle"></i>
                <span>Help</span>
            </a>

```

```

</li><!-- End Help Page Nav -->

<li class="nav-item">
  <a class="nav-link collapsed" href="about.php">
    <i class="bi bi-person"></i>
    <span>About</span>
  </a>
</li><!-- End About Page Nav -->
</ul>

</aside><!-- End Sidebar-->

<main id="main" class="main">

<div class="pagetitle">
  <h1>Dekripsi</h1>
  <nav>
    <ol class="breadcrumb">
      <li class="breadcrumb-item"><a href="index.php">Home</a></li>
      <li class="breadcrumb-item active">Dekripsi</li>
    </ol>
  </nav>
</div><!-- End Page Title -->

<section class="section">
  <div class="row">

    <div class="col-xl-12">
      <div class="card">
        <div class="card-header">Dekripsi Cipherteks Dengan
        Algoritma RSA dan Beaufort Cipher</div>
        <div class="card-body pt-3">
          <!-- Multi Columns Form -->
          <form id="dekripsi" name="dekripsi" method="post"
          action="" class="row g-3" enctype="multipart/form-data">
            <!-- <div class="col-md-10">
              <label for="file-kunci" class="form-label">Masukkan
              Kunci Privat RSA</label>
              <input type="file" name="file-kunci" id="file-kunci"
              class="form-control">
            </div> -->
            <div class="col-md-4">
              <button type="submit" name="btnReadKunci"
              id="btnReadKunci" class="btn btn-secondary btn-sm">

```



```

        <i class="bi bi-check-circle"></i> Read Kunci Privat
RSA</button>
    </div>
    <div class="col-md-4">
        <?php if(isset($_POST['btnReadKunci'])) {
            $fileKunci = fopen("KunciPrivat.txt", "r");
            $kunciN = fgets($fileKunci); //fgets -> untuk
mengambil baris pertama dari file teks
            fclose($fileKunci);
        ?>
        <!-- <label for="n" class="form-label">Nilai n</label>
-->
        <input type="text" name="txtN" id="txtN" value="<?php
echo $kunciN; ?>" class="form-control" placeholder="Kunci Publik RSA
(n)">
        <?php }else{ ?>
        <!-- <label for="n" class="form-label">Nilai n</label>
-->
        <input type="text" name="txtN" id="txtN" class="form-
control" placeholder="Kunci Publik RSA (n)">
        <?php } ?>
    </div>
    <div class="col-md-4">
        <?php if(isset($_POST['btnReadKunci'])) {
            $fileKunci = "KunciPrivat.txt";
            $lines = file($fileKunci); //file teks dimasukkan
kedalam array
            $kunciD = $lines[1]; // untuk mengambil baris kedua
dari file teks
        ?>
        <!-- <label for="d" class="form-label">Nilai d</label>
-->
        <input type="text" name="txtD" id="txtD" value="<?php
echo $kunciD; ?>" class="form-control" placeholder="Kunci Publik RSA
(d)">
        <?php }else{ ?>
        <!-- <label for="d" class="form-label">Nilai d</label>
-->
        <input type="text" name="txtD" id="txtD" class="form-
control" placeholder="Kunci Publik RSA (d)">
        <?php } ?>
    </div>
    <div class="col-md-12">
        <label for="file-plainteks" class="form-
label">Masukkan File Teks (Cipherteks)</label>

```

```

        <input type="file" name="file" id="file" class="form-
control">
    </div>
    <div class="col-md-12">
        <textarea name="txtCipherteks" id="txtCipherteks"
class="form-control" placeholder="Cipherteks" style="height:
100px"></textarea>
    </div>
    <div class="col-md-12">
        <label for="kunci-beaufort" class="form-
label">Masukkan Kunci Beaufort Cipher</label>
        <input type="text" name="txtKeyBeaufort"
id="txtKeyBeaufort" class="form-control" placeholder="Kunci Beaufort
Cipher">
    </div>
    <div class="text-center pt-3">
        <button type="submit" name="btnDekripRSA"
id="btnDekripRSA" class="btn btn-outline-primary btn-sm"><i class="bi
bi-check-circle"></i> Dekripsi RSA</button>
        <button type="button" onclick="dekripsiBeaufort()"
class="btn btn-outline-danger btn-sm"><i class="bi bi-check-circle"></i>
Dekripsi Beaufort</button>
        <button type="submit" name="btnSavePlainteks"
id="btnSavePlainteks" class="btn btn-outline-success btn-sm"><i
class="bi bi-check-circle"></i> Simpan
Plainteks</button>
    </div>
    <div class="col-md-6 pt-3">
        <label for="hasil-dekripsiRSA" class="form-
label">Hasil Dekripsi (Plainteks) RSA</label>
        <?php if(isset($_POST['btnDekripRSA'])) { ?>
            <textarea name="txtPlainteksRSA"
id="txtPlainteksRSA" class="form-control" style="height: 100px"
placeholder="Plainteks RSA"> <?php echo $plaintextsRSA; -?></textarea>
            <?php }else{ ?>
                <textarea name="txtPlainteksRSA"
id="txtPlainteksRSA" class="form-control" style="height: 100px"
placeholder="Plainteks RSA"><?php echo isset($_POST['txtPlainteksRSA'])
? $_POST['txtPlainteksRSA'] : '' ?></textarea>
            <?php } ?>
        </div>
    <div class="col-md-6 pt-3">
        <label for="hasil-dekripsiBeaufort" class="form-
label">Hasil Dekripsi (Plainteks) Beaufort Cipher</label>

```

```

        <textarea id="txtPlainteksBeaufort"
name="txtPlainteksBeaufort" class="form-control" style="height: 100px"
placeholder="Plainteks Beaufort Cipher"></textarea>
    </div>
</form>
</div><!-- End Card -->
</div><!-- End Column -->

</div><!-- End Row -->
</section>

</main><!-- End #main -->

<!-- ===== Footer ===== -->
<footer id="footer" class="footer">
    <div class="copyright">
        &copy; Copyright <strong><span>NiceAdmin</span></strong>. All
Rights Reserved
    </div>
    <div class="credits">
        Designed by <a href="https://bootstrapmade.com/"
target="_blank">BootstrapMade</a>
    </div>
</footer><!-- End Footer -->

<a href="#" class="back-to-top d-flex align-items-center justify-
content-center"><i class="bi bi-arrow-up-short"></i></a>

<!-- Vendor JS Files -->
<script src="assets/vendor/apexcharts/apexcharts.min.js"></script>
<script
src="assets/vendor/bootstrap/js/bootstrap.bundle.min.js"></script>
<script src="assets/vendor/chart.js/chart.min.js"></script>
<script src="assets/vendor/echarts/echarts.min.js"></script>
<script src="assets/vendor/quill/quill.min.js"></script>
<script src="assets/vendor/simple-datatables/simple-
datatables.js"></script>
<script src="assets/vendor/tinymce/tinymce.min.js"></script>
<script src="assets/vendor/php-email-form/validate.js"></script>
<!-- Template Main JS File -->
<script src="assets/js/main.js"></script>

<!-- Open File Teks -->
<script>
    const $output = document.getElementById('txtCipherteks');

```

```

document.getElementById('file').onchange = function() {
// ambil file yang dipilih oleh user
const file = this.files[0];

// cek apakah file bertipe .txt
if (file.type === 'text/plain') {
// jika file bertipe .txt, baca isi file menggunakan FileReader
const reader = new FileReader();
reader.onload = function(progressEvent) {
// Entire file
const text = this.result;
$output.innerText = text;

// By lines
var lines = text.split('\n');
for (var line = 0; line < lines.length; line++) {
console.log(lines[line]);
}
};
reader.readAsText(file);
} else {
// jika file bukan bertipe .txt, tampilkan pesan error
alert("File yang dipilih bukan merupakan file .txt");
// console.error('File yang dipilih bukan merupakan file .txt');
this.value = null; // reset input file
return;
}
};
</script>

```

```

<!-- Deripsi Beaufort Cipher -->

```

```

<script>

```

```

function isUpperCase(letter) {
var l = letter.charCodeAt();
if(l > 64 && l < 91) {
return true;
} else {
return false;
}
}

```

```

function isLowerCase(letter) {
let l = letter.charCodeAt();
if(l > 96 && l < 123) {
return true;
}
}

```

```

    } else {
        return false;
    }
}

function isLetter(letter) {
    if(isLowerCase(letter) || isUpperCase(letter)) {
        return true;
    } else {
        return false;
    }
}

function mod(n, m) {
    return ((n % m) + m) % m;
}

function dekripsiBeaufort() {
    let decrypted = "";
    let enc = document.getElementById("txtPlainteksRSA").value;
    let key = document.getElementById("txtKeyBeaufort").value;

    if (enc=="" && key=="") {
        return alert("Cipherteks dan Kunci Beaufort tidak boleh kosong");
    }
    else if(enc=="") {
        return alert("Cipherteks tidak boleh kosong");
    }
    else if(key=="") {
        return alert("Kunci Beaufort tidak boleh kosong");
    }

    let j = 0;
    for (let i = 0; i < enc.length; i++) {
        let currentLetter = enc[i];
        const A = 65; // A = 65 adalah nilai desimal dalam tabel ASCII
        const a = 97; // a = 97 adalah nilai desimal dalam tabel ASCII

        if(isUpperCase(currentLetter)) {
            let Ci = (currentLetter.charCodeAt(0) - A);
            let Ki = (key[j % key.length].toUpperCase()).charCodeAt(0) - A;
            let upperLetter = mod(Ki - Ci, 26);

            decrypted += String.fromCharCode(upperLetter + A);
        }
    }
}

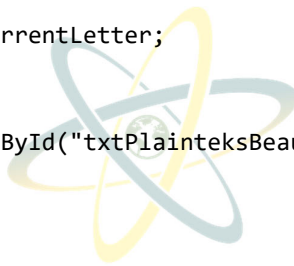
```

```
j++;
} else if(isLowerCase(currentLetter)) {
    let Ci = (currentLetter.charCodeAt(0) - a);
    let Ki = (key[j % key.length].toLowerCase()).charCodeAt(0) - a;
    let lowerLetter = mod(Ki - Ci, 26);

    decrypted += String.fromCharCode(lowerLetter + a);

    j++;
} else {
    decrypted += currentLetter;
}
}
document.getElementById("txtPlainteksBeaufort").innerHTML=decrypted;
d;
}
</script>

</body>
</html>
```



UNIVERSITAS ISLAM NEGERI
SUMATERA UTARA MEDAN

Lampiran 2

DAFTAR RIWAYAT HIDUP
(*CURRICULUM VITAE*)



Nama : Mahyudi
Nim : 0701162010
Tempat, Tanggal Lahir : Deli Tua, 09 Desember 1997
Jenis Kelamin : Laki - laki
Alamat : Jl. Sejarah DS. IX
Kel/Desa : Mekar Sari
Kecamatan : Deli Tua
Kabupaten : Deli Serdang
Kode Pos : 20355
Agama : Islam
Status Nikah : Belum Menikah
Nama Orang Tua :
Ayah : Muhammad Haris, SE
Ibu : Maisyaroh Tanjung, S.Pd

PENDIDIKAN FORMAL

2004 – 2010 : SD Negeri 101797 Deli Tua
2010 – 2013 : SMP Negeri 2 Deli Tua
2013 – 2016 : SMK Swasta Istiqlal Deli Tua
2016 – 2023 : Universitas Islam Negeri Sumatera Utara Medan











Lampiran 3

Buku Laporan Kegiatan Akademik Mahasiswa Fakultas SAINTEK UIN SU Medan

KARTU BIMBINGAN SKRIPSI


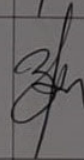
Semester Gasal/Genap Tahun Akademik /

Nama : Mahyudi	Pembimbing I : Yusuf Ramadhan Nasution
NIM : 0721162016	Pembimbing II : Abdul Halim Hasugian
Prog. Studi : ILMU KOMPUTER	SK Pembimbing :
Judul Skripsi : Implementasi kombinasi Algoritma Beaufort Cipher dan Algoritma RSA dalam skema Suber Enkripsi untuk Pengamanan File Teks	

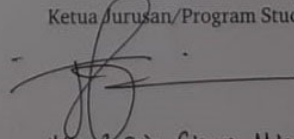
P E R T	PEMBIMBING I			PEMBIMBING II		
	Tgl.	Materi Bimbingan	Tanda Tangan	Tgl.	Materi Bimbingan	Tanda Tangan
I	09/02/2022	Perbaiki Bab I dan kelengkapan Aplikasi		17-01-2022	Perbaiki Bab I, II, III	
II	31/05/2022	Conto Aplikasi Jadi Web		16-02-2022	ACC Bab I, II Perbaiki Bab III	
III	21/06/2022	Ac. Sampul		15-03-2022	ACC Bab III lengkapi buku	
IV	20/08/2022	Perbaiki Bab II		30-03-2022	layat Seminar	
V	20/08/2022	Ac. Judul		03-01-2023	Perbaiki Bab IV, V	

32

Buku Laporan Kegiatan Akademik Mahasiswa Fakultas SAINTEK UIN SU Medan

VI				11-01 2023	ACL Bab IV, V	
VII				16-01 2023	Lanjut Sidang	
VIII						
IX						
X						

Medan, 20
An. Dekan
Ketua Jurusan/Program Studi


Ilka Zulfira, S.kom., N.kom
NIP. 198506042015031006

Catatan: Pada saat bimbingan, kartu ini harus diisi dan ditandatangani oleh pembimbing