

DAFTAR LAMPIRAN

Listing Program

Index.php

```
<?php include 'config.php'; ?>
<!DOCTYPE html>
<html>
<head>
<title>Aplikasi Pengamanan Dokumen</title>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">
<!-- CSS-->
<link rel="stylesheet" type="text/css" href="assets/css/main.css">
<link rel="stylesheet" href="assets/css/gaya.css">
<!-- HTML5 Shim and Respond.js IE8 support of HTML5 elements and
media queries-->
<!--if lt IE 9
script(src='https://oss.maxcdn.com/libs/html5shiv/3.7.0/html5shiv.js')
script(src='https://oss.maxcdn.com/libs/respond.js/1.4.2/respond.min.js')
-->
</head>
<body style="background-color:#355f64;">
<section class="material-half-bg">
<div class="cover-gaya"></div>
</section>
<section class="login-content">
<div class="logo">
<h2>Aplikasi Pengamanan Dokumen<b> AMAN</b></h2>
</div>
<div class="login-box">
<form class="login-form" action="auth.php" method="post"><img src="" alt="" srcset="">
<h3 class="login-head text-info">MAN</h3>
<div class="form-group">
<label class="control-label">Nama pengguna</label>
<input class="form-control" type="text" name="username" placeholder="masukan nama pengguna" autofocus autocomplete="off" required>
</div>
<div class="form-group">
<label class="control-label">Kata sandi</label>
```

```
<input class="form-control" type="password" name="password"
placeholder="masukan kata sandi" required>
</div>
<div class="form-group btn-container">
    <button class="btn btn-info btn-block" name="login">MASUK <i
class="fa fa-sign-in fa-lg"></i></button><br>
    <p style="font-size:10pt mb-3">&copy; Advanced Encryption Standard
(AES-128)</p>
</div>
</form>
</div>
</section>
</body>
<script src="assets/js/jquery-2.1.4.min.js"></script>
<script src="assets/js/essential-plugins.js"></script>
<script src="assets/js/bootstrap.min.js"></script>
<script src="assets/js/plugins/pace.min.js"></script>
<script src="assets/js/main.js"></script>
</html>
```



AES.php

```
<?php

class AES {

    var $sBox = array(
        array(0x63, 0x7C, 0x77, 0x7B, 0xF2, 0x6B,
0x6F, 0xC5, 0x30, 0x01, 0x67, 0x2B, 0xFE, 0xD7, 0xAB, 0x76),
        array(0xCA, 0x82, 0xC9, 0x7D, 0xFA, 0x59,
0x47, 0xF0, 0xAD, 0xD4, 0xA2, 0xAF, 0x9C, 0xA4, 0x72, 0xC0),
        array(0xB7, 0xFD, 0x93, 0x26, 0x36, 0x3F,
0xF7, 0xCC, 0x34, 0xA5, 0xE5, 0xF1, 0x71, 0xD8, 0x31, 0x15),
        array(0x04, 0xC7, 0x23, 0xC3, 0x18, 0x96,
0x05, 0x9A, 0x07, 0x12, 0x80, 0xE2, 0xEB, 0x27, 0xB2, 0x75),
        array(0x09, 0x83, 0x2C, 0x1A, 0x1B, 0x6E,
0x5A, 0xA0, 0x52, 0x3B, 0xD6, 0xB3, 0x29, 0xE3, 0x2F, 0x84),
        array(0x53, 0xD1, 0x00, 0xED, 0x20, 0xFC,
0xB1, 0x5B, 0x6A, 0xCB, 0xBE, 0x39, 0x4A, 0x4C, 0x58, 0xCF),
        array(0xD0, 0xEF, 0xAA, 0xFB, 0x43, 0x4D,
0x33, 0x85, 0x45, 0xF9, 0x02, 0x7F, 0x50, 0x3C, 0x9F, 0xA8),
        array(0x51, 0xA3, 0x40, 0x8F, 0x92, 0x9D,
0x38, 0xF5, 0xBC, 0xB6, 0xDA, 0x21, 0x10, 0xFF, 0xF3, 0xD2),
        array(0xCD, 0x0C, 0x13, 0xEC, 0x5F, 0x97,
0x44, 0x17, 0xC4, 0xA7, 0x7E, 0x3D, 0x64, 0x5D, 0x19, 0x73),
        array(0x60, 0x81, 0x4F, 0xDC, 0x22, 0x2A,
0x90, 0x88, 0x46, 0xEE, 0xB8, 0x14, 0xDE, 0x5E, 0x0B, 0xDB),
        array(0xE0, 0x32, 0x3A, 0x0A, 0x49, 0x06,
0x24, 0x5C, 0xC2, 0xD3, 0xAC, 0x62, 0x91, 0x95, 0xE4, 0x79),
        array(0xE7, 0xC8, 0x37, 0x6D, 0x8D, 0xD5,
0x4E, 0xA9, 0x6C, 0x56, 0xF4, 0xEA, 0x65, 0x7A, 0xAE, 0x08),
        array(0xBA, 0x78, 0x25, 0x2E, 0x1C, 0xA6,
0xB4, 0xC6, 0xE8, 0xDD, 0x74, 0x1F, 0x4B, 0xBD, 0x8B, 0x8A),
        array(0x70, 0x3E, 0xB5, 0x66, 0x48, 0x03,
0xF6, 0x0E, 0x61, 0x35, 0x57, 0xB9, 0x86, 0xC1, 0x1D, 0x9E),
        array(0xE1, 0xF8, 0x98, 0x11, 0x69, 0xD9,
0x8E, 0x94, 0x9B, 0x1E, 0x87, 0xE9, 0xCE, 0x55, 0x28, 0xDF),
        array(0x8C, 0xA1, 0x89, 0x0D, 0xBF, 0xE6,
0x42, 0x68, 0x41, 0x99, 0x2D, 0x0F, 0xB0, 0x54, 0xBB, 0x16)
    );

    // The inverse S-Box substitution table.
    var $invSBox = array(
        array(0x52, 0x09, 0x6A, 0xD5, 0x30,
0x36, 0xA5, 0x38, 0xBF, 0x40, 0xA3, 0x9E, 0x81, 0xF3, 0xD7, 0xFB),
        array(0x0B, 0x8F, 0x4D, 0x2E, 0x79, 0x5E, 0x33, 0x9C, 0x1A, 0x62,
0x80, 0x4C, 0x22, 0x0D, 0x5A, 0x3B, 0x9D, 0x1C, 0x64, 0x83,
0x4B, 0x29, 0x0A, 0x5B, 0x3F, 0x9E, 0x1E, 0x66, 0x85, 0x4E,
0x0C, 0x8B, 0x2D, 0x0F, 0x5C, 0x3D, 0x9F, 0x1F, 0x68, 0x87,
0x4A, 0x2B, 0x0D, 0x5D, 0x3E, 0x9A, 0x1G, 0x69, 0x8C, 0x2F,
0x0E, 0x8D, 0x2A, 0x0B, 0x5E, 0x3F, 0x9B, 0x1H, 0x6B, 0x8D,
0x4C, 0x2E, 0x0F, 0x5F, 0x3G, 0x9C, 0x1I, 0x6C, 0x8E, 0x2H,
0x0D, 0x8F, 0x2B, 0x0C, 0x5G, 0x3H, 0x9D, 0x1J, 0x6D, 0x8F,
0x4D, 0x2C, 0x0E, 0x5H, 0x3I, 0x9E, 0x1K, 0x6E, 0x8G, 0x2J,
0x0F, 0x8H, 0x2D, 0x0E, 0x5I, 0x3J, 0x9F, 0x1L, 0x6F, 0x8H,
0x4E, 0x2E, 0x0F, 0x5J, 0x3K, 0x9G, 0x1M, 0x6G, 0x8I, 0x2L,
0x0G, 0x8J, 0x2F, 0x0F, 0x5K, 0x3L, 0x9H, 0x1N, 0x6H, 0x8J,
0x4F, 0x2F, 0x0G, 0x5L, 0x3M, 0x9I, 0x1O, 0x6I, 0x8K, 0x2M,
0x0H, 0x8L, 0x2G, 0x0H, 0x5M, 0x3N, 0x9J, 0x1P, 0x6J, 0x8L,
0x4G, 0x2G, 0x0I, 0x5N, 0x3O, 0x9K, 0x1Q, 0x6K, 0x8M, 0x2O,
0x0I, 0x8N, 0x2H, 0x0I, 0x5O, 0x3P, 0x9L, 0x1R, 0x6L, 0x8N,
0x4H, 0x2H, 0x0J, 0x5P, 0x3Q, 0x9M, 0x1S, 0x6M, 0x8P, 0x2Q,
0x0J, 0x8P, 0x2I, 0x0J, 0x5Q, 0x3R, 0x9O, 0x1T, 0x6O, 0x8P,
0x4I, 0x2I, 0x0K, 0x5R, 0x3S, 0x9P, 0x1U, 0x6P, 0x8R, 0x2S,
0x0K, 0x8R, 0x2J, 0x0K, 0x5S, 0x3T, 0x9Q, 0x1V, 0x6Q, 0x8R,
0x4J, 0x2J, 0x0L, 0x5T, 0x3U, 0x9S, 0x1W, 0x6U, 0x8T, 0x2U,
0x0L, 0x8T, 0x2K, 0x0L, 0x5U, 0x3V, 0x9W, 0x1X, 0x6V, 0x8T,
0x4K, 0x2K, 0x0M, 0x5V, 0x3W, 0x9X, 0x1Y, 0x6W, 0x8V, 0x2W,
0x0M, 0x8V, 0x2L, 0x0M, 0x5W, 0x3X, 0x9Y, 0x1Z, 0x6X, 0x8V,
0x4L, 0x2L, 0x0N, 0x5X, 0x3Y, 0x9Z, 0x1A, 0x6Z, 0x8X, 0x2Y,
0x0N, 0x8X, 0x2M, 0x0N, 0x5Y, 0x3Z, 0x9A, 0x1B, 0x6A, 0x8X,
0x4M, 0x2M, 0x0O, 0x5Z, 0x3B, 0x9B, 0x1C, 0x6B, 0x8A, 0x2B,
0x0O, 0x8A, 0x2N, 0x0O, 0x5B, 0x3C, 0x9C, 0x1D, 0x6C, 0x8B,
0x4N, 0x2N, 0x0P, 0x5C, 0x3D, 0x9D, 0x1E, 0x6D, 0x8C, 0x2D,
0x0P, 0x8C, 0x2O, 0x0P, 0x5D, 0x3E, 0x9E, 0x1F, 0x6E, 0x8D,
0x4O, 0x2O, 0x0Q, 0x5E, 0x3F, 0x9F, 0x1G, 0x6F, 0x8E, 0x2F,
0x0Q, 0x8E, 0x2P, 0x0Q, 0x5F, 0x3G, 0x9G, 0x1H, 0x6G, 0x8F,
0x4P, 0x2P, 0x0R, 0x5G, 0x3H, 0x9H, 0x1I, 0x6H, 0x8G, 0x2H,
0x0R, 0x8G, 0x2Q, 0x0R, 0x5H, 0x3I, 0x9I, 0x1J, 0x6I, 0x8H,
0x4Q, 0x2Q, 0x0K, 0x5I, 0x3J, 0x9J, 0x1L, 0x6J, 0x8I, 0x2J,
0x0K, 0x8I, 0x2R, 0x0K, 0x5J, 0x3L, 0x9L, 0x1M, 0x6L, 0x8J,
0x4R, 0x2R, 0x0N, 0x5L, 0x3M, 0x9M, 0x1O, 0x6M, 0x8L, 0x2M,
0x0N, 0x8L, 0x2S, 0x0N, 0x5M, 0x3O, 0x9O, 0x1P, 0x6O, 0x8S,
0x4S, 0x2S, 0x0T, 0x5O, 0x3P, 0x9P, 0x1Q, 0x6P, 0x8T, 0x2P,
0x0T, 0x8T, 0x2U, 0x0T, 0x5P, 0x3Q, 0x9Q, 0x1R, 0x6Q, 0x8U,
0x4U, 0x2U, 0x0V, 0x5Q, 0x3R, 0x9R, 0x1S, 0x6R, 0x8V, 0x2R,
0x0V, 0x8V, 0x2W, 0x0V, 0x5R, 0x3S, 0x9S, 0x1T, 0x6S, 0x8W,
0x4W, 0x2W, 0x0X, 0x5S, 0x3T, 0x9T, 0x1U, 0x6T, 0x8X, 0x2X,
0x0X, 0x8X, 0x2Y, 0x0X, 0x5T, 0x3U, 0x9U, 0x1V, 0x6U, 0x8Y,
0x4Y, 0x2Y, 0x0Z, 0x5U, 0x3V, 0x9V, 0x1W, 0x6V, 0x8Z, 0x2Z,
0x0Z, 0x8Z, 0x2A, 0x0Z, 0x5V, 0x3W, 0x9W, 0x1B, 0x6W, 0x8A,
0x4A, 0x2A, 0x0C, 0x5W, 0x3B, 0x9B, 0x1D, 0x6B, 0x8C, 0x2B,
0x0C, 0x8C, 0x2E, 0x0C, 0x5B, 0x3D, 0x9D, 0x1F, 0x6D, 0x8E,
0x4E, 0x2E, 0x0G, 0x5D, 0x3F, 0x9F, 0x1H, 0x6F, 0x8G, 0x2F,
0x0G, 0x8G, 0x2I, 0x0G, 0x5F, 0x3H, 0x9H, 0x1J, 0x6H, 0x8I,
0x4I, 0x2I, 0x0K, 0x5H, 0x3J, 0x9J, 0x1L, 0x6J, 0x8K, 0x2J,
0x0K, 0x8K, 0x2M, 0x0K, 0x5J, 0x3L, 0x9L, 0x1N, 0x6L, 0x8M,
0x4M, 0x2M, 0x0O, 0x5L, 0x3N, 0x9N, 0x1P, 0x6N, 0x8O, 0x2N,
0x0O, 0x8O, 0x2Q, 0x0O, 0x5N, 0x3P, 0x9P, 0x1R, 0x6P, 0x8Q,
0x4Q, 0x2Q, 0x0S, 0x5P, 0x3R, 0x9R, 0x1T, 0x6R, 0x8S, 0x2R,
0x0S, 0x8S, 0x2U, 0x0S, 0x5R, 0x3T, 0x9T, 0x1V, 0x6T, 0x8U,
0x4U, 0x2U, 0x0X, 0x5T, 0x3V, 0x9V, 0x1W, 0x6V, 0x8X, 0x2X,
0x0X, 0x8X, 0x2Y, 0x0X, 0x5V, 0x3W, 0x9W, 0x1Z, 0x6W, 0x8Y,
0x4Y, 0x2Y, 0x0Z, 0x5W, 0x3Z, 0x9Z, 0x1A, 0x6Z, 0x8Z, 0x2Z,
0x0Z, 0x8Z, 0x2B, 0x0Z, 0x5Z, 0x3A, 0x9A, 0x1C, 0x6A, 0x8B,
0x4B, 0x2B, 0x0D, 0x5A, 0x3C, 0x9C, 0x1E, 0x6C, 0x8D, 0x2D,
0x0D, 0x8D, 0x2F, 0x0D, 0x5C, 0x3E, 0x9E, 0x1G, 0x6E, 0x8F,
0x4F, 0x2F, 0x0H, 0x5E, 0x3G, 0x9G, 0x1I, 0x6G, 0x8H, 0x2G,
0x0H, 0x8H, 0x2J, 0x0H, 0x5G, 0x3I, 0x9I, 0x1K, 0x6I, 0x8J,
0x4J, 0x2J, 0x0L, 0x5I, 0x3K, 0x9K, 0x1M, 0x6K, 0x8L, 0x2K,
0x0L, 0x8L, 0x2N, 0x0L, 0x5K, 0x3M, 0x9M, 0x1O, 0x6M, 0x8N,
0x4N, 0x2N, 0x0P, 0x5M, 0x3O, 0x9O, 0x1Q, 0x6O, 0x8P, 0x2O,
0x0P, 0x8P, 0x2R, 0x0P, 0x5O, 0x3Q, 0x9Q, 0x1S, 0x6Q, 0x8R,
0x4S, 0x2S, 0x0T, 0x5Q, 0x3R, 0x9R, 0x1U, 0x6R, 0x8T, 0x2T,
0x0T, 0x8T, 0x2V, 0x0T, 0x5R, 0x3U, 0x9U, 0x1W, 0x6U, 0x8V,
0x4V, 0x2V, 0x0X, 0x5U, 0x3W, 0x9W, 0x1Y, 0x6W, 0x8X, 0x2X,
0x0X, 0x8X, 0x2Z, 0x0X, 0x5W, 0x3Y, 0x9Y, 0x1A, 0x6Y, 0x8Z,
0x4Z, 0x2Z, 0x0B, 0x5Z, 0x3A, 0x9A, 0x1C, 0x6A, 0x8B, 0x2B,
0x0C, 0x8C, 0x2D, 0x0C, 0x5B, 0x3C, 0x9C, 0x1E, 0x6C, 0x8D,
0x4D, 0x2D, 0x0F, 0x5C, 0x3E, 0x9E, 0x1G, 0x6E, 0x8F, 0x2F,
0x0F, 0x8F, 0x2H, 0x0F, 0x5E, 0x3G, 0x9G, 0x1I, 0x6G, 0x8H,
0x4H, 0x2H, 0x0J, 0x5G, 0x3I, 0x9I, 0x1K, 0x6I, 0x8J, 0x2J,
0x0J, 0x8J, 0x2L, 0x0J, 0x5I, 0x3K, 0x9K, 0x1M, 0x6K, 0x8L,
0x4L, 0x2L, 0x0N, 0x5I, 0x3M, 0x9M, 0x1O, 0x6M, 0x8N, 0x2N,
0x0N, 0x8N, 0x2P, 0x0N, 0x5M, 0x3O, 0x9O, 0x1Q, 0x6O, 0x8P,
0x4Q, 0x2Q, 0x0R, 0x5O, 0x3P, 0x9P, 0x1S, 0x6P, 0x8R, 0x2R,
0x0R, 0x8R, 0x2T, 0x0R, 0x5P, 0x3S, 0x9S, 0x1U, 0x6S, 0x8T,
0x4U, 0x2U, 0x0V, 0x5T, 0x3U, 0x9U, 0x1W, 0x6U, 0x8V, 0x2V,
0x0V, 0x8V, 0x2X, 0x0V, 0x5U, 0x3W, 0x9W, 0x1Y, 0x6W, 0x8X,
0x4Y, 0x2Y, 0x0Z, 0x5W, 0x3X, 0x9X, 0x1A, 0x6X, 0x8Z, 0x2Z,
0x0Z, 0x8Z, 0x2B, 0x0Z, 0x5Z, 0x3A, 0x9A, 0x1C, 0x6A, 0x8B,
0x4B, 0x2B, 0x0D, 0x5A, 0x3C, 0x9C, 0x1E, 0x6C, 0x8D, 0x2D,
0x0D, 0x8D, 0x2F, 0x0D, 0x5C, 0x3E, 0x9E, 0x1G, 0x6E, 0x8F,
0x4F, 0x2F, 0x0H, 0x5E, 0x3G, 0x9G, 0x1I, 0x6G, 0x8H, 0x2G,
0x0H, 0x8H, 0x2J, 0x0H, 0x5G, 0x3I, 0x9I, 0x1K, 0x6I, 0x8J,
0x4J, 0x2J, 0x0L, 0x5I, 0x3K, 0x9K, 0x1M, 0x6K, 0x8L, 0x2K,
0x0L, 0x8L, 0x2N, 0x0L, 0x5K, 0x3M, 0x9M, 0x1O, 0x6M, 0x8N,
0x4N, 0x2N, 0x0P, 0x5M, 0x3O, 0x9O, 0x1Q, 0x6O, 0x8P, 0x2O,
0x0P, 0x8P, 0x2R, 0x0P, 0x5O, 0x3Q, 0x9Q, 0x1S, 0x6Q, 0x8R,
0x4S, 0x2S, 0x0T, 0x5Q, 0x3R, 0x9R, 0x1U, 0x6R, 0x8T, 0x2T,
0x0T, 0x8T, 0x2V, 0x0T, 0x5R, 0x3U, 0x9U, 0x1W, 0x6U, 0x8V,
0x4V, 0x2V, 0x0X, 0x5U, 0x3W, 0x9W, 0x1Y, 0x6W, 0x8X, 0x2X,
0x0X, 0x8X, 0x2Z, 0x0X, 0x5W, 0x3Y, 0x9Y, 0x1A, 0x6Y, 0x8Z,
0x4Z, 0x2Z, 0x0B, 0x5Z, 0x3A, 0x9A, 0x1C, 0x6A, 0x8B, 0x2B,
0x0C, 0x8C, 0x2D, 0x0C, 0x5B, 0x3C, 0x9C, 0x1E, 0x6C, 0x8D,
0x4D, 0x2D, 0x0F, 0x5C, 0x3E, 0x9E, 0x1G, 0x6E, 0x8F, 0x2F,
0x0F, 0x8F, 0x2H, 0x0F, 0x5E, 0x3G, 0x9G, 0x1I, 0x6G, 0x8H,
0x4H, 0x2H, 0x0J, 0x5G, 0x3I, 0x9I, 0x1K, 0x6I, 0x8J, 0x2J,
0x0J, 0x8J, 0x2L, 0x0J, 0x5I, 0x3K, 0x9K, 0x1M, 0x6K, 0x8L,
0x4L, 0x2L, 0x0N, 0x5I, 0x3M, 0x9M, 0x1O, 0x6M, 0x8N, 0x2N,
0x0N, 0x8N, 0x2P, 0x0N, 0x5M, 0x3O, 0x9O, 0x1Q, 0x6O, 0x8P,
0x4Q, 0x2Q, 0x0R, 0x5O, 0x3P, 0x9P, 0x1S, 0x6P, 0x8R, 0x2R,
0x0R, 0x8R, 0x2T, 0x0R, 0x5P, 0x3S, 0x9S, 0x1U, 0x6S, 0x8T,
0x4U, 0x2U, 0x0V, 0x5T, 0x3U, 0x9U, 0x1W, 0x6U, 0x8V, 0x2V,
0x0V, 0x8V, 0x2X, 0x0V, 0x5U, 0x3W, 0x9W, 0x1Y, 0x6W, 0x8X,
0x4Y, 0x2Y, 0x0Z, 0x5W, 0x3X, 0x9X, 0x1A, 0x6X, 0x8Z, 0x2Z,
0x0Z, 0x8Z, 0x2B, 0x0Z, 0x5Z, 0x3A, 0x9A, 0x1C, 0x6A, 0x8B,
0x4B, 0x2B, 0x0D, 0x5A, 0x3C, 0x9C, 0x1E, 0x6C, 0x8D, 0x2D,
0x0D, 0x8D, 0x2F, 0x0D, 0x5C, 0x3E, 0x9E, 0x1G, 0x6E, 0x8F,
0x4F, 0x2F, 0x0H, 0x5E, 0x3G, 0x9G, 0x1I, 0x6G, 0x8H, 0x2G,
0x0H, 0x8H, 0x2J, 0x0H, 0x5G, 0x3I, 0x9I, 0x1K, 0x6I, 0x8J,
0x4J, 0x2J, 0x0L, 0x5I, 0x3K, 0x9K, 0x1M, 0x6K, 0x8L, 0x2K,
0x0L, 0x8L, 0x2N, 0x0L, 0x5K, 0x3M, 0x9M, 0x1O, 0x6M, 0x8N,
0x4N, 0x2N, 0x0P, 0x5M, 0x3O, 0x9O, 0x1Q, 0x6O, 0x8P, 0x2O,
0x0P, 0x8P, 0x2R, 0x0P, 0x5O, 0x3Q, 0x9Q, 0x1S, 0x6Q, 0x8R,
0x4S, 0x2S, 0x0T, 0x5Q, 0x3R, 0x9R, 0x1U, 0x6R, 0x8T, 0x2T,
0x0T, 0x8T, 0x2V, 0x0T, 0x5R, 0x3U, 0x9U, 0x1W, 0x6U, 0x8V,
0x4V, 0x2V, 0x0X, 0x5U, 0x3W, 0x9W, 0x1Y, 0x6W, 0x8X, 0x2X,
0x0X, 0x8X, 0x2Z, 0x0X, 0x5W, 0x3Y, 0x9Y, 0x1A, 0x6Y, 0x8Z,
0x4Z, 0x2Z, 0x0B, 0x5Z, 0x3A, 0x9A, 0x1C, 0x6A, 0x8B, 0x2B,
0x0C, 0x8C, 0x2D, 0x0C, 0x5B, 0x3C, 0x9C, 0x1E, 0x6C, 0x8D,
0x4D, 0x2D, 0x0F, 0x5C, 0x3E, 0x9E, 0x1G, 0x6E, 0x8F, 0x2F,
0x0F, 0x8F, 0x2H, 0x0F, 0x5E, 0x3G, 0x9G, 0x1I, 0x6G, 0x8H,
0x4H, 0x2H, 0x0J, 0x5G, 0x3I, 0x9I, 0x1K, 0x6I, 0x8J, 0x2J,
0x0J, 0x8J, 0x2L, 0x0J, 0x5I, 0x3K, 0x9K, 0x1M, 0x6K, 0x8L,
0x4L, 0x2L, 0x0N, 0x5I, 0x3M, 0x9M, 0x1O, 0x6M, 0x8N, 0x2N,
0x0N, 0x8N, 0x2P, 0x0N, 0x5M, 0x3O, 0x9O, 0x1Q, 0x6O, 0x8P,
0x4Q, 0x2Q, 0x0R, 0x5O, 0x3P, 0x9P, 0x1S, 0x6P, 0x8R, 0x2R,
0x0R, 0x8R, 0x2T, 0x0R, 0x5P, 0x3S, 0x9S, 0x1U, 0x6S, 0x8T,
0x4U, 0x2U, 0x0V, 0x5T, 0x3U, 0x9U, 0x1W, 0x6U, 0x8V, 0x2V,
0x0V, 0x8V, 0x2X, 0x0V, 0x5U, 0x3W, 0x9W, 0x1Y, 0x6W, 0x8X,
0x4Y, 0x2Y, 0x0Z, 0x5W, 0x3X, 0x9X, 0x1A, 0x6X, 0x8Z, 0x2Z,
0x0Z, 0x8Z, 0x2B, 0x0Z, 0x5Z, 0x3A, 0x9A, 0x1C, 0x6A, 0x8B,
0x4B, 0x2B, 0x0D, 0x5A, 0x3C, 0x9C, 0x1E, 0x6C, 0x8D, 0x2D,
0x0D, 0x8D, 0x2F, 0x0D, 0x5C, 0x3E, 0x9E, 0x1G, 0x6E, 0x8F,
0x4F, 0x2F, 0x0H, 0x5E, 0x3G, 0x9G, 0x1I, 0x6G, 0x8H, 0x2G,
0x0H, 0x8H, 0x2J, 0x0H, 0x5G, 0x3I, 0x9I, 0x1K, 0x6I, 0x8J,
0x4J, 0x2J, 0x0L, 0x5I, 0x3K, 0x9K, 0x1M, 0x6K, 0x8L, 0x2K,
0x0L, 0x8L, 0x2N, 0x0L, 0x5K, 0x3M, 0x9M, 0x1O, 0x6M, 0x8N,
0x4N, 0x2N, 0x0P, 0x5M, 0x3O, 0x9O, 0x1Q, 0x6O, 0x8P, 0x2O,
0x0P, 0x8P, 0x2R, 0x0P, 0x5O, 0x3Q, 0x9Q, 0x1S, 0x6Q, 0x8R,
0x4S, 0x2S, 0x0T, 0x5Q, 0x3R, 0x9R, 0x1U, 0x6R, 0x8T, 0x2T,
0x0T, 0x8T, 0x2V, 0x0T, 0x5R, 0x3U, 0x9U, 0x1W, 0x6U, 0x8V,
0x4V, 0x2V, 0x0X, 0x5U, 0x3W, 0x9W, 0x1Y, 0x6W, 0x8X, 0x2X,
0x0X, 0x8X, 0x2Z, 0x0X, 0x5W, 0x3Y, 0x9Y, 0x1A, 0x6Y, 0x8Z,
0x4Z, 0x2Z, 0x0B, 0x5Z, 0x3A, 0x9A, 0x1C, 0x6A, 0x8B, 0x2B,
0x0C, 0x8C, 0x2D, 0x0C, 0x5B, 0x3C, 0x9C, 0x1E, 0x6C, 0x8D,
0x4D, 0x2D, 0x0F, 0x5C, 0x3E, 0x9E, 0x1G, 0x6E, 0x8F, 0x2F,
0x0F, 0x8F, 0x2H, 0x0F, 0x5E, 0x3G, 0x9G, 0x1I, 0x6G, 0x8H,
0x4H, 0x2H, 0x0J, 0x5G, 0x3I, 0x9I, 0x1K, 0x6I, 0x8J, 0x2J,
0x0J, 0x8J, 0x2L, 0x0J, 0x5I, 0x3K, 0x9K, 0x1M, 0x6K, 0x8L,
0x4L, 0x2L, 0x0N, 0x5I, 0x3M, 0x9M, 0x1O, 0x6M, 0x8N, 0x2N,
0x0N, 0x8N, 0x2P, 0x0N, 0x5M, 0x3O, 0x9O, 0x1Q, 0x6O, 0x8P,
0x4Q, 0x2Q, 0x0R, 0x5O, 0x3P, 0x9P, 0x1S, 0x6P, 0x8R, 0x2R,
0x0R, 0x8R, 0x2T, 0x0R, 0x5P, 0x3S, 0x9S, 0x1U, 0x6S, 0x8T,
0x4U, 0x2U, 0x0V, 0x5T, 0x3U, 0x9U, 0x1W, 0x6U, 0x8V, 0x2V,
0x0V, 0x8V, 0x2X, 0x0V, 0x5U, 0x3W, 0x9W, 0x1Y, 0x6W, 0x8X,
0x4Y, 0x2
```

```

        array(0x7C, 0xE3, 0x39, 0x82, 0x9B,
0x2F, 0xFF, 0x87, 0x34, 0x8E, 0x43, 0x44, 0xC4, 0xDE, 0xE9, 0xCB),
        array(0x54, 0x7B, 0x94, 0x32, 0xA6,
0xC2, 0x23, 0x3D, 0xEE, 0x4C, 0x95, 0x0B, 0x42, 0xFA, 0xC3, 0x4E),
        array(0x08, 0x2E, 0xA1, 0x66, 0x28,
0xD9, 0x24, 0xB2, 0x76, 0x5B, 0xA2, 0x49, 0x6D, 0x8B, 0xD1, 0x25),
        array(0x72, 0xF8, 0xF6, 0x64, 0x86, 0x68,
0x98, 0x16, 0xD4, 0xA4, 0x5C, 0xCC, 0x5D, 0x65, 0xB6, 0x92),
        array(0x6C, 0x70, 0x48, 0x50, 0xFD,
0xED, 0xB9, 0xDA, 0x5E, 0x15, 0x46, 0x57, 0xA7, 0x8D, 0x9D, 0x84),
        array(0x90, 0xD8, 0xAB, 0x00, 0x8C,
0xBC, 0xD3, 0x0A, 0xF7, 0xE4, 0x58, 0x05, 0xB8, 0xB3, 0x45, 0x06),
        array(0xD0, 0x2C, 0x1E, 0x8F, 0xCA,
0x3F, 0x0F, 0x02, 0xC1, 0xAF, 0xBD, 0x03, 0x01, 0x13, 0x8A, 0x6B),
        array(0x3A, 0x91, 0x11, 0x41, 0x4F, 0x67,
0xDC, 0xEA, 0x97, 0xF2, 0xCF, 0xCE, 0xF0, 0xB4, 0xE6, 0x73),
        array(0x96, 0xAC, 0x74, 0x22, 0xE7,
0xAD, 0x35, 0x85, 0xE2, 0xF9, 0x37, 0xE8, 0x1C, 0x75, 0xDF, 0x6E),
        array(0x47, 0xF1, 0x1A, 0x71, 0x1D,
0x29, 0xC5, 0x89, 0x6F, 0xB7, 0x62, 0x0E, 0xAA, 0x18, 0xBE, 0x1B),
        array(0xFC, 0x56, 0x3E, 0x4B, 0xC6,
0xD2, 0x79, 0x20, 0x9A, 0xDB, 0xC0, 0xFE, 0x78, 0xCD, 0x5A, 0xF4),
        array(0x1F, 0xDD, 0xA8, 0x33, 0x88,
0x07, 0xC7, 0x31, 0xB1, 0x12, 0x10, 0x59, 0x27, 0x80, 0xEC, 0x5F),
        array(0x60, 0x51, 0x7F, 0xA9, 0x19,
0xB5, 0x4A, 0x0D, 0x2D, 0xE5, 0x7A, 0x9F, 0x93, 0xC9, 0x9C, 0xEF),
        array(0xA0, 0xE0, 0x3B, 0x4D, 0xAE,
0x2A, 0xF5, 0xB0, 0xC8, 0xEB, 0xBB, 0x3C, 0x83, 0x53, 0x99, 0x61),
        array(0x17, 0x2B, 0x04, 0x7E, 0xBA,
0x77, 0xD6, 0x26, 0xE1, 0x69, 0x14, 0x63, 0x55, 0x21, 0x0C, 0x7D)
);

// Log table based on 0xe5
var $ltable = array(
    0x00, 0xff, 0xc8, 0x08, 0x91, 0x10, 0xd0, 0x36,
    0x5a, 0x3e, 0xd8, 0x43, 0x99, 0x77, 0xfe, 0x18,
    0x23, 0x20, 0x07, 0x70, 0xa1, 0x6c, 0x0c, 0x7f,
    0x62, 0x8b, 0x40, 0x46, 0xc7, 0x4b, 0xe0, 0x0e,
    0xeb, 0x16, 0xe8, 0xad, 0xcf, 0xcd, 0x39, 0x53,
    0x6a, 0x27, 0x35, 0x93, 0xd4, 0x4e, 0x48, 0xc3,
    0x2b, 0x79, 0x54, 0x28, 0x09, 0x78, 0x0f, 0x21,
    0x90, 0x87, 0x14, 0x2a, 0xa9, 0x9c, 0xd6, 0x74,
    0xb4, 0x7c, 0xde, 0xed, 0xb1, 0x86, 0x76, 0xa4,
    0x98, 0xe2, 0x96, 0x8f, 0x02, 0x32, 0x1c, 0xc1,
    0x33, 0xee, 0xef, 0x81, 0xfd, 0x30, 0x5c, 0x13,
    0x9d, 0x29, 0x17, 0xc4, 0x11, 0x44, 0x8c, 0x80,

```

```

0xf3, 0x73, 0x42, 0x1e, 0x1d, 0xb5, 0xf0, 0x12,
0xd1, 0x5b, 0x41, 0xa2, 0xd7, 0x2c, 0xe9, 0xd5,
0x59, 0xcb, 0x50, 0xa8, 0xdc, 0xfc, 0xf2, 0x56,
0x72, 0xa6, 0x65, 0x2f, 0x9f, 0x9b, 0x3d, 0xba,
0x7d, 0xc2, 0x45, 0x82, 0xa7, 0x57, 0xb6, 0xa3,
0x7a, 0x75, 0x4f, 0xae, 0x3f, 0x37, 0x6d, 0x47,
0x61, 0xbe, 0xab, 0xd3, 0x5f, 0xb0, 0x58, 0xaf,
0xca, 0x5e, 0xfa, 0x85, 0xe4, 0x4d, 0x8a, 0x05,
0xfb, 0x60, 0xb7, 0x7b, 0xb8, 0x26, 0x4a, 0x67,
0xc6, 0x1a, 0xf8, 0x69, 0x25, 0xb3, 0xdb, 0xbd,
0x66, 0xdd, 0xf1, 0xd2, 0xdf, 0x03, 0x8d, 0x34,
0xd9, 0x92, 0x0d, 0x63, 0x55, 0xaa, 0x49, 0xec,
0xbc, 0x95, 0x3c, 0x84, 0x0b, 0xf5, 0xe6, 0xe7,
0xe5, 0xac, 0x7e, 0x6e, 0xb9, 0xf9, 0xda, 0x8e,
0x9a, 0xc9, 0x24, 0xe1, 0xa, 0x15, 0x6b, 0x3a,
0xa0, 0x51, 0xf4, 0xea, 0xb2, 0x97, 0x9e, 0x5d,
0x22, 0x88, 0x94, 0xce, 0x19, 0x01, 0x71, 0x4c,
0xa5, 0xe3, 0xc5, 0x31, 0xbb, 0xcc, 0x1f, 0x2d,
0x3b, 0x52, 0x6f, 0xf6, 0x2e, 0x89, 0xf7, 0xc0,
0x68, 0x1b, 0x64, 0x04, 0x06, 0xbf, 0x83, 0x38
);

// Inverse log table
var $atable = array(
    0x01, 0xe5, 0x4c, 0xb5, 0xfb, 0x9f, 0xfc, 0x12,
    0x03, 0x34, 0xd4, 0xc4, 0x16, 0xba, 0x1f, 0x36,
    0x05, 0x5c, 0x67, 0x57, 0x3a, 0xd5, 0x21, 0x5a,
    0x0f, 0xe4, 0xa9, 0xf9, 0x4e, 0x64, 0x63, 0xee,
    0x11, 0x37, 0xe0, 0x10, 0xd2, 0xac, 0xa5, 0x29,
    0x33, 0x59, 0x3b, 0x30, 0x6d, 0xef, 0xf4, 0x7b,
    0x55, 0xeb, 0x4d, 0x50, 0xb7, 0x2a, 0x07, 0x8d,
    0xff, 0x26, 0xd7, 0xf0, 0xc2, 0x7e, 0x09, 0x8c,
    0x1a, 0x6a, 0x62, 0x0b, 0x5d, 0x82, 0x1b, 0x8f,
    0x2e, 0xbe, 0xa6, 0x1d, 0xe7, 0x9d, 0x2d, 0x8a,
    0x72, 0xd9, 0xf1, 0x27, 0x32, 0xbc, 0x77, 0x85,
    0x96, 0x70, 0x08, 0x69, 0x56, 0xdf, 0x99, 0x94,
    0xa1, 0x90, 0x18, 0xbb, 0xfa, 0x7a, 0xb0, 0xa7,
    0xf8, 0xab, 0x28, 0xd6, 0x15, 0x8e, 0xcb, 0xf2,
    0x13, 0xe6, 0x78, 0x61, 0x3f, 0x89, 0x46, 0x0d,
    0x35, 0x31, 0x88, 0xa3, 0x41, 0x80, 0xca, 0x17,
    0x5f, 0x53, 0x83, 0xfe, 0xc3, 0x9b, 0x45, 0x39,
    0xe1, 0xf5, 0x9e, 0x19, 0x5e, 0xb6, 0xcf, 0x4b,
    0x38, 0x04, 0xb9, 0x2b, 0xe2, 0xc1, 0x4a, 0xdd,
    0x48, 0x0c, 0xd0, 0x7d, 0x3d, 0x58, 0xde, 0x7c,
    0xd8, 0x14, 0x6b, 0x87, 0x47, 0xe8, 0x79, 0x84,
    0x73, 0x3c, 0xbd, 0x92, 0xc9, 0x23, 0x8b, 0x97,

```

```

0x95, 0x44, 0xdc, 0xad, 0x40, 0x65, 0x86, 0xa2,
0xa4, 0xcc, 0x7f, 0xec, 0xc0, 0xaf, 0x91, 0xfd,
0xf7, 0x4f, 0x81, 0x2f, 0x5b, 0xea, 0xa8, 0x1c,
0x02, 0xd1, 0x98, 0x71, 0xed, 0x25, 0xe3, 0x24,
0x06, 0x68, 0xb3, 0x93, 0x2c, 0x6f, 0x3e, 0x6c,
0x0a, 0xb8, 0xce, 0xae, 0x74, 0xb1, 0x42, 0xb4,
0x1e, 0xd3, 0x49, 0xe9, 0x9c, 0xc8, 0xc6, 0xc7,
0x22, 0x6e, 0xdb, 0x20, 0xbf, 0x43, 0x51, 0x52,
0x66, 0xb2, 0x76, 0x60, 0xda, 0xc5, 0xf3, 0xf6,
0xaa, 0xcd, 0x9a, 0xa0, 0x75, 0x54, 0x0e, 0x01
);

# key schedule
var $w;
# posisi cursor key schedule
var $pos_w = 0;
# Blok pada Data AES
var $Nb;
# Blok pada Key AES
var $Nk;
# Jumlah Looping / Putaran
var $Nr;

var $log;

# Constructor class AES
# Parameter $z = key AES
function AES($z) {

    # Blok Data AES
    $this->Nb = 4;

    # Menghitung Panjang Key
    # Panjang Key AES (16, 24, 32)
    # untuk mengelompokkan jenis AES (AES-128,
AES-192, AES-256)
    $this->Nk = strlen($z)/4;

    # Validasi untuk memfilter panjang key
    if ($this->Nk != 4 && $this->Nk != 6 && $this-
>Nk != 8)
        die("Key is " . ($this->Nk*32) . " bits long. *not* 128, 192, or
256.");
}

# Jumlah Putaran / looping pada proses enkripsi &
dekripsi

```

```

    $this->Nr = $this->Nk + $this->Nb + 2;

    # Nb*(Nr+1) 32-bit words
    $this->w = array();
    # 2-D array of Nb columns and 4 rows
    $this->s = array(array());

    # memanggil function keyexpansion() yang ada di
class AES
    $this->keyexpansion($z);
}

# function untuk melakukan proses enkripsi
# function yang berhubungan :
#      addRoundKey(), subByte(), ShiftRow(), MixColumns()
function encrypt($input){

    # memecah inputan/data ke dalam bentuk String
    $data = str_split($input);

    $state = array();
    $count = 0;
    $this->pos_w = 0;

    for($i=0; $i<4; $i++){
        for($j=0; $j<4; $j++) {
            if ($count < count($data)){
                $this->state[$i][$j] = ord($data[$count]);
            } else{
                $this->state[$i][$j] = 0;
            }
            $count++;
        }
    }

    // AddRoundKey #1
    for($i=0; $i<4; $i++){

        for($j=0; $j < $this->Nb; $j++) {
            $this->state[$i][$j] = $this->state[$i][$j] ^
        $this->w[$i][$this->pos_w + $j];
        }
    }
    $this->pos_w = $this->pos_w + $this->Nb;
}

```

```

for ($i=0; $i<$this->Nr-1; $i++) {

    $this->state = $this->SubByte($this->state);

    $this->state = $this->ShiftRow($this->state);

    $this->state = $this->MixColumns($this->state);

    $this->state = $this->AddRoundKey($this->state);
    $this->pos_w = $this->pos_w + $this->Nb;

}

$this->state = $this->SubByte($this->state);

$this->state = $this->ShiftRow($this->state);

$this->state = $this->AddRoundKey($this->state);

$cipher = "";
foreach($this->state as $state){
    foreach($state as $data) {
        $cipher .= chr($data);
    }
}
return $cipher;
}

function decrypt($input){

$data = str_split($input);

$state = array();
$count = 0;
$this->pos_w = ((($this->Nr+1)*4));
$modulo = 0;

for($i=0; $i<4; $i++){
    for($j=0; $j<4; $j++) {
        $this->state[$i][$j] = ord($data[$count]);
        $count++;
    }
}
}

```

```

// AddRoundKey #1
$this->pos_w = ($this->pos_w)-4;
for($i=0; $i<4; $i++){
    $x = 0;
    for($j= $this->pos_w; $j < (($this->Nr+1)*4);
$j++) {

    $y = $x++;

    $this->state[$i][$y] = $this->state[$i][$y]
^ $this->w[$i][$j];

}

}

for ($i=0; $i<$this->Nr-1; $i++) {

$this->state = $this->InvShiftRow($this->state);

$this->state = $this->InvSubByte($this->state);

$this->pos_w = ($this->pos_w)- $this->Nb;
$this->state = $this->AddRoundKey($this->state);

$this->state = $this->InvMixColumns($this-
>state);

}

$this->state = $this->InvShiftRow($this->state);

$this->state = $this->InvSubByte($this->state);

$this->pos_w = ($this->pos_w)- $this->Nb;
$this->state = $this->AddRoundKey($this->state);

$plain = "";
foreach($this->state as $state) {
    foreach($state as $data) {
        $plain .= chr($data);
    }
}

return $plain;
}

```

```

# function untuk menggabungkan DATA dengan KUNCI
# State XOR Key Schedule
function AddRoundKey($data) {

    $state = array();
    for($i=0; $i<4; $i++){

        $this->temp_w = $this->pos_w;
        for($j=0; $j < $this->Nb; $j++) {

            $state[$i][$j] = $data[$i][$j] ^ $this-
>w[$i][$this->pos_w+$j];
        }
    }
    return $state;
}

function SubByte($data){

    $state = $data;
    for($i=0; $i<$this->Nb; $i++){
        for($j=0; $j<4; $j++) {
            $state[$i][$j] =
>subword($state[$i][$j]);
        }
    }
    return $state;
}

function ShiftRow($data){

    $state = array();

    for($i=0; $i<4; $i++){
        for($j=0; $j<$this->Nb; $j++) {

            $state[$i][$j] = $data[$i][($j+$i)%4];
        }
    }
}

```

```

        return $state;

    }

function MixColumns($data){

    $state = array();

    for ($i=0; $i < $this->Nb; $i++) {
        $state[0][$i] = $this->mult(0x02,$data[0][$i]) ^ $this->mult(0x03,$data[1][$i]) ^ $this->mult(0x01,$data[2][$i]) ^ $this->mult(0x01,$data[3][$i]);
        $state[1][$i] = $this->mult(0x01,$data[0][$i]) ^ $this->mult(0x02,$data[1][$i]) ^ $this->mult(0x03,$data[2][$i]) ^ $this->mult(0x01,$data[3][$i]);
        $state[2][$i] = $this->mult(0x01,$data[0][$i]) ^ $this->mult(0x01,$data[1][$i]) ^ $this->mult(0x02,$data[2][$i]) ^ $this->mult(0x03,$data[3][$i]);
        $state[3][$i] = $this->mult(0x03,$data[0][$i]) ^ $this->mult(0x01,$data[1][$i]) ^ $this->mult(0x01,$data[2][$i]) ^ $this->mult(0x02,$data[3][$i]);
    }
    return $state;
}

function InvSubByte($data){

    $state = $data;

    for($i=0; $i<$this->Nb; $i++){
        for($j=0; $j<4; $j++) {
            $state[$i][$j] = $this->invSub($state[$i][$j]);
        }
    }
    return $state;
}

function InvShiftRow($data){

    $state = array();

    for($i=0; $i<4; $i++){

```

```

        for($j=0; $j<$this->Nb; $j++) {

            $state[$i][($j+$i)%4] = $data[$i][$j];

        }

    }

    return $state;

}

function InvMixColumns($data){

    $state = array();

    for ($i=0; $i < $this->Nb; $i++) {
        $state[0][$i] = $this->mult(0x0e,$data[0][$i]) ^ $this->mult(0x0b,$data[1][$i]) ^ $this->mult(0x0d,$data[2][$i]) ^ $this->mult(0x09,$data[3][$i]);
        $state[1][$i] = $this->mult(0x09,$data[0][$i]) ^ $this->mult(0x0e,$data[1][$i]) ^ $this->mult(0x0b,$data[2][$i]) ^ $this->mult(0x0d,$data[3][$i]);
        $state[2][$i] = $this->mult(0x0d,$data[0][$i]) ^ $this->mult(0x09,$data[1][$i]) ^ $this->mult(0x0e,$data[2][$i]) ^ $this->mult(0x0b,$data[3][$i]);
        $state[3][$i] = $this->mult(0x0b,$data[0][$i]) ^ $this->mult(0x0d,$data[1][$i]) ^ $this->mult(0x09,$data[2][$i]) ^ $this->mult(0x0e,$data[3][$i]);
    }

    return $state;
}

function mult($a, $b) {
    $sum = $this->ltable[$a] + $this->ltable[$b];
    $sum %= 255;
    // Get the antilog
    $sum = $this->atable[$sum];
    return ($a == 0 ? 0 : ($b == 0 ? 0 : $sum));
}

# function untuk melakukan Generate Key
function keyexpansion($key){

    # memecah String menjadi Array per karakter
    $arrkey = str_split($key);
}

```

```

# variable untuk kursor index String Key
$count = 0;

# konstanta Rcon
static $rcon = array(
    array(0x01,0x00,0x00,0x00),
    array(0x02,0x00,0x00,0x00),
    array(0x04,0x00,0x00,0x00),
    array(0x08,0x00,0x00,0x00),
    array(0x10,0x00,0x00,0x00),
    array(0x20,0x00,0x00,0x00),
    array(0x40,0x00,0x00,0x00),
    array(0x80,0x00,0x00,0x00),
    array(0x1b,0x00,0x00,0x00),
    array(0x36,0x00,0x00,0x00)
);

# Salin Key ke variable w (Key Schedule)
# ord() : untuk mendapatkan nilai ASCII dari suatu
karakter
for($i=0; $i<$this->Nb; $i++){
    for($j=0; $j<4; $j++) {
        $this->w[$i][$j] = ord($arrkey[$count]);
        $count++;
    }
}

# posisi cursor rcon()
$count_rcon = 0;
# proses Generate Key
# function yang berhubungan : subword() , rotword()
for( $i=4; $i<44; $i++){
    for($j=0; $j<4; $j++) {
        # mengambil nilai columns w(i-1)
        $wmin1      = $this->w[$j][$i-1];
        # mengambil nilai columns w(i-4)
        $wmin4      = $this->w[$j][$i-4];
        # melakukan pengecekan apakah i
merupakan awal dari block
        if ($i%4==0) {

            # Proses rotword()
            if($j!=3)
                $wmin1      =      $this-
>w[$j+1][$i-1];
        }
    }
}

```

```

        else
            $wmin1      =      $this-
>w[0][$i-1];

                # melakukan XOR pada : w(i-1)
XOR w(i-4) XOR rcon()
                # w(i-1) mengalami proses
subword() : pertukaran dengan data dari table sBox
                $this->w[$j][$i]      =      $this-
>subword($wmin1) ^ $wmin4 ^ $rcon[$count_rcon][$j];

                # cursor rcon() berpindah ke rcon
selanjutnya
if ($j==3) $count_rcon++;

} else {
    # bukan merupakan awal block
    # melakukan XOR pada : w(i-1)
    $this->w[$j][$i]      =      $wmin1
}

# mengembalikan nilai array w[][] setelah mengalami
proses keyexpansion
return $this->w;
}

function rotword($w, $row, $col){
    return (($row==0)? $w[3][$col] : $w[$row-1][$col]);
}

function subword($byte){
    # menghitung panjang inputan yang sudah dikonversikan
menjadi HEX
    # jika panjang inputan 2
    if (strlen(dechex($byte)) == 2) {
        # konversi inputan kedalam bentuk HEX
        # memecah inputan menjadi array
        $hex   = str_split(dechex($byte));

        # karakter ke-1 menjadi index baris
        $r      = hexdec($hex[0]);
        # karakter ke-2 menjadi index kolom
}

```

```

        $c          = hexdec($hex[1]);

    } else {
        # jika panjang inputan 1
        $r = 0;
        # inputan menjadi index kolom
        $c = $byte;
    }

    # mengembalikan nilai table sBox berdasarkan index baris
& kolom
    # r : baris | c : kolom
    return $this->sBox[$r][$c];
}

function invSub($byte){
    if (strlen(dechex($byte)) == 2) {
        $hex  = str_split(dechex($byte));
        $r    = hexdec($hex[0]);
        $c    = hexdec($hex[1]);

    } else {
        $r = 0;
        $c = $byte;
    }

    return $this->invSBox[$r][$c];
}

?>

```

Encrypt.php

```

<?php
session_start();
include('../config.php');
if(empty($_SESSION['username'])){
header("location:../index.php");
}
$last = $_SESSION['username'];
$sqlupdate = "UPDATE users SET last_activity=now() WHERE
username='$last'";
$queryupdate = mysqli_query($connect,$sqlupdate);
?>

```

```

<!DOCTYPE html>
<html>
<?php
$user = $_SESSION['username'];
$query = mysqli_query($connect,"SELECT fullname,job_title,last_activity
FROM users WHERE username='$user'");
$data = mysqli_fetch_array($query);
?>
<head>
<title><?php echo $data['fullname']; ?> - Aplikasi Pengamanan
Dokumen</title>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">
<link rel="stylesheet" type="text/css" href="../assets/css/main.css">
    <link rel="stylesheet" type="text/css" href="../assets/css/gaya.css">
    <!-- HTML5 Shim and Respond.js IE8 support of HTML5 elements and
media queries-->
    <!--if lt IE 9
script(src='https://oss.maxcdn.com/libs/html5shiv/3.7.0/html5shiv.js')
script(src='https://oss.maxcdn.com/libs/respond.js/1.4.2/respond.min.js')
-->
</head>
<body class="sidebar-mini fixed">
<!-- NAVBAR SIDEBAR -->
<?php include('navmenu.php'); ?>
<div class="content-wrapper">
<div class="page-title">
<div>
<h1><i class="fa fa-file"></i> Enkripsi Berkas</h1>
</div>
<div>
<ul class="breadcrumb">
<li><i class="fa fa-home fa-lg"></i></li>
<li><a href="index.php">Dashboard</a></li>
<li>Enkripsi Berkas</li>
</ul>
</div>
</div>
<div class="row">
<div class="col-md-12">
<div class="card">
<div class="card-body">
<form class="form-horizontal" method="post" action="encrypt-
process.php" enctype="multipart/form-data">
<fieldset>

```

```

<legend>Enkripsi</legend>
<div class="form-group">
    <label class="col-lg-2 control-label"
for="inputPassword">Tanggal</label>
    <div class="col-lg-4">
        <input class="form-control" id="inputTgl" type="text"
placeholder="Tanggal" name="datenow" value=<?php echo date("Y-m-
d");?>" readonly>
    </div>
</div>
<div class="form-group">
    <label class="col-lg-2 control-label"
for="inputFile">Berkas</label>
    <div class="col-lg-4">
        <input class="form-control" id="inputFile"
placeholder="Input File" type="file" name="file" required>
    </div>
</div>
<div class="form-group">
    <label class="col-lg-2 control-label"
for="inputPassword">Password</label>
    <div class="col-lg-4">
        <input class="form-control" id="inputPassword"
type="password" placeholder="Password enkripsi berkas" name="pwdfile"
required>
    </div>
</div>
<div class="form-group">
    <label class="col-lg-2 control-label"
for="textArea">Keterangan</label>
    <div class="col-lg-4">
        <textarea class="form-control" id="textArea" rows="3"
name="desc" placeholder="Keterangan berkas"></textarea>
    </div>
</div>
<div class="form-group">
    <label class="col-lg-2 control-label" for="textArea"></label>
    <div class="col-lg-2">
        <input type="submit" name="encrypt_now" value="Enkripsi
Berkas" class="form-control btn btn-primary">
    </div>
    </div>
</fieldset>
</form>
</div>
</div>

```

```

    </div>
    </div>
    </div>
    </div>
<script src="../assets/js/jquery-2.1.4.min.js"></script>
<script src="../assets/js/essential-plugins.js"></script>
<script src="../assets/js/bootstrap.min.js"></script>
<script src="../assets/js/plugins/pace.min.js"></script>
<script src="../assets/js/main.js"></script>
</body>
</html>

```

Encrypt-process.php

```

<?php
session_start();
include "../config.php"; //memasukan koneksi
include "AES.php"; //memasukan file AES

if (isset($_POST['encrypt_now'])) {
    $user      = $_SESSION['username'];
    $key       =
mysqli_escape_string($connect,substr(md5($_POST["pwdfile"]), 0,16));
    $deskripsi = mysqli_escape_string($_POST['desc']);

    $file_tmpname = $_FILES['file']['tmp_name'];
    //untuk nama file url
    $file      = rand(1000,100000)."-".$_FILES['file']['name'];
    $new_file_name = strtolower($file);
    $final_file  = str_replace(' ','-',$new_file_name);
    //untuk nama file
    $filename   = rand(1000,100000)."-".pathinfo($_FILES['file']['name'],
PATHINFO_FILENAME);
    $new_filename = strtolower($filename);
    $finalfile  = str_replace(' ','-',$new_filename);
    $size      = filesize($file_tmpname);
    $size2     = (filesize($file_tmpname))/1024;
    $info      = pathinfo($final_file );
    $file_source = fopen($file_tmpname, 'rb');
    $ext       = $info["extension"];

    if( $ext=="docx" || $ext=="doc" || $ext=="txt" || $ext=="pdf" || $ext=="xls"
|| $ext=="xlsx" || $ext=="ppt" || $ext=="pptx"){
        }else{
            echo("<script language='javascript'>

```

```

window.location.href='encrypt.php';
window.alert('Maaf, file yang bisa dienkrip hanya word, excel, text, ppt
ataupun pdf.');
</script>");
exit();
}

if($size2>3084){
echo("<script language='javascript'>
window.location.href='home.php?encrypt';
window.alert('Maaf, file tidak bisa lebih besar dari 3MB.');
</script>");
exit();
}

$sql1 = "INSERT INTO file VALUES ('','$user', '$final_file',
'$finalfile.rda', '$size2', '$key', now(), '1', '$deskripsi')";
$query1 = mysqli_query($connect,$sql1) or die(mysql_error());

$sql2 = "select * from file where file_url =''";
$query2 = mysqli_query($connect,$sql2) or die(mysql_error());

$url = $finalfile.".rda";
$file_url = "file_encrypt/".$url";

$sql3 = "UPDATE file SET file_url ='$file_url' WHERE file_url =''";
$query3 = mysqli_query($connect,$sql3) or die(mysql_error());

$file_output = fopen($file_url, 'wb');

$mod = $size%16;
if($mod==0){
    $banyak = $size / 16;
} else{
    $banyak = ($size - $mod) / 16;
    $banyak = $banyak+1;
}

if(is_uploaded_file($file_tmpname)){
    ini_set('max_execution_time', -1);
    ini_set('memory_limit', -1);
    $aes = new AES($key);

    for($bawah=0;$bawah<$banyak;$bawah++){
        $data = fread($file_source, 16);
        $cipher = $aes->encrypt($data);

```

```

        fwrite($file_output, $cipher);
    }
    fclose($file_source);
    fclose($file_output);

    echo("<script language='javascript'>
        window.location.href='encrypt.php';
        window.alert('Enkripsi Berhasil..');
    </script>");

} else{
    echo("<script language='javascript'>
        window.location.href='encrypt.php';
        window.alert('Encrypt file mengalami masalah..');
    </script>");

}
}

```

Decrypt.php

```

<?php
session_start();
include('../config.php');
if(empty($_SESSION['username'])){
header("location:../index.php");
}
$last = $_SESSION['username'];
$sqlupdate = "UPDATE users SET last_activity=now() WHERE
username='$last'";
$queryupdate = mysqli_query($connect,$sqlupdate);
?>
<!DOCTYPE html>
<html>
<?php
$user = $_SESSION['username'];
$query = mysqli_query($connect,"SELECT fullname,job_title,last_activity
FROM users WHERE username='$user'");
$data = mysqli_fetch_array($query);
?>
<head>
<title><?php echo $data['fullname']; ?> - Aplikasi Pengamanan
Dokumen</title>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">
<link rel="stylesheet" type="text/css" href="../assets/css/main.css">

```

```

<link rel="stylesheet" type="text/css" href="../assets/css/gaya.css">
<link rel="stylesheet" type="text/css"
href="../assets/plugins/datatables/css/jquery.dataTables.css">
<!-- HTML5 Shim and Respond.js IE8 support of HTML5 elements and
media queries--&gt;
&lt;!--if lt IE 9
script(src='https://oss.maxcdn.com/libs/html5shiv/3.7.0/html5shiv.js')
script(src='https://oss.maxcdn.com/libs/respond.js/1.4.2/respond.min.js')
--&gt;
&lt;/head&gt;
&lt;body class="sidebar-mini fixed"&gt;
&lt;!-- NAVBAR SIDEBAR --&gt;
&lt;?php include('navmenu.php'); ?&gt;
&lt;div class="content-wrapper"&gt;
&lt;div class="page-title"&gt;
&lt;div&gt;
&lt;h1&gt;&lt;i class="fa fa-file"&gt;&lt;/i&gt;Dekripsi Berkas&lt;/h1&gt;
&lt;/div&gt;
&lt;div&gt;
&lt;ul class="breadcrumb"&gt;
&lt;li&gt;&lt;i class="fa fa-home fa-lg"&gt;&lt;/i&gt;&lt;/li&gt;
&lt;li&gt;&lt;a href="index.php"&gt;Dashboard&lt;/a&gt;&lt;/li&gt;
&lt;li&gt;Dekripsi Berkas&lt;/li&gt;
&lt;/ul&gt;
&lt;/div&gt;
&lt;/div&gt;
&lt;div class="row"&gt;
&lt;div class="col-md-12"&gt;
&lt;div class="card"&gt;
&lt;div class="card-body"&gt;
&lt;div class="table-responsive"&gt;
&lt;table id="file" class="table striped"&gt;
&lt;thead class="bg-primary"&gt;
&lt;tr&gt;
&lt;td width="5%"><strong>No</strong></td>
<td width="20%"><strong>Nama Sumber  
Berkas</strong></td>
<td width="20%"><strong>Nama Berkas  
Enkripsi</strong></td>
<td width="20%"><strong>Path Berkas</strong></td>
<td width="15%"><strong>Status Berkas</strong></td>
<td width="10%"><strong>Opsi</strong></td>
</tr>
</thead>
<tfoot class="bg-primary">
<tr>

```

```

<td width="5%">><strong>No</strong></td>
<td width="20%">><strong>Nama Berkas</strong></td>
<td width="20%">><strong>Nama Berkas
Enkripsi</strong></td>
<td width="20%">><strong>Path Berkas</strong></td>
<td width="15%">><strong>Status Berkas</strong></td>
<td width="10%">><strong>Opsi</strong></td>
</tr>
</tfoot>
<tbody>
<?php
$i = 1;
$query = mysqli_query($connect,"SELECT * FROM file
where status=1");
while ($data = mysqli_fetch_array($query)) { ?>
<tr>
<td><?php echo $i; ?></td>
<td><?php echo $data['file_name_source']; ?></td>
<td><?php echo $data['file_name_finish']; ?></td>
<td><?php echo $data['file_url']; ?></td>
<td><?php if ($data['status'] == 1) {
echo "Enkripsi";
}elseif ($data['status'] == 2) {
echo "Dekripsi";
} else {
echo "Status Tidak Diketahui";
}
?></td>
<td>
<?php
$a = $data['id_file'];
if ($data['status'] == 1) {
echo '<a href="decrypt-file.php?id_file='.$a.'" class="btn
btn-warning">Dekripsi Berkas</a>';
}elseif ($data['status'] == 2) {
echo '<a href="encrypt.php" class="btn btn-
success">Enkripsi Berkas</a>';
} else {
echo '<a href="decrypt.php" class="btn btn-danger">Data
Tidak Diketahui</a>';
}
?>

</td>
</tr>
<?php

```

Decrypt-process.php

```
<?php
session_start();
include "../config.php"; //memasukan koneksi
include "AES.php"; //memasukan file AES

$idfile = mysqli_escape_string($connect,$_POST['fileid']);
$pwdfile = mysqli_escape_string($connect, substr(md5($_POST["pwdfile"]),
0,16));
$query = "SELECT password FROM file WHERE id_file='".$idfile' AND
password='".$pwdfile."'";
$sql = mysqli_query($connect,$query);
```

```

if(mysqli_num_rows($sql)>0){
    $query1 = "SELECT * FROM file WHERE id_file='".$idfile."'";
    $sql1 = mysqli_query($connect,$query1);
    $data = mysqli_fetch_assoc($sql1);

    $file_path = $data["file_url"];
    $key = $data["password"];
    $file_name = $data["file_name_source"];
    $size = $data["file_size"];

    $file_size = filesize($file_path);

    $query2 = "UPDATE file SET status='2' WHERE id_file='".$idfile."'";
    $sql2 = mysqli_query($connect,$query2);

    $mod = $file_size%16;

    $aes = new AES($key);
    $fopen1 = fopen($file_path, "rb");
    $plain = "";
    $cache = "file_decrypt/".$file_name;
    $fopen2 = fopen($cache, "wb");

    if($mod==0){
        $banyak = $file_size / 16;
    }else{
        $banyak = ($file_size - $mod) / 16;
        $banyak = $banyak+1;
    }

    ini_set('max_execution_time', -1);
    ini_set('memory_limit', -1);
    for($bawah=0;$bawah<$banyak;$bawah++){

        $filedata = fread($fopen1, 16);
        $plain = $aes->decrypt($filedata);
        fwrite($fopen2, $plain);
    }
    $_SESSION["download"] = $cache;

    echo("<script language='javascript'>
        window.open('download.php', '_blank');
        window.location.href='history.php';
        window.alert('Berhasil mendekripsi file.');
    </script>
    ");
}

```

```

}else{
echo("<script language='javascript'>
    window.location.href='decrypt-file.php?id_file=$idfile';
    window.alert('Maaf, Password tidak sesuai.');
</script>");
}
?>

```

History.php

```

<?php
session_start();
include('../config.php');
if(empty($_SESSION['username'])){
header("location:../index.php");
}
$last = $_SESSION['username'];
$sqlupdate = "UPDATE users SET last_activity=now() WHERE
username='$last'";
$queryupdate = mysqli_query($connect,$sqlupdate);
?>
<!DOCTYPE html>
<html>
<?php
$user = $_SESSION['username'];
$query = mysqli_query($connect,"SELECT fullname,job_title,last_activity
FROM users WHERE username='$user'");
$data = mysqli_fetch_array($query);
?>
<head>
<title><?php echo $data['fullname']; ?> - Aplikasi Pengamanan
Dokumen</title>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">
<link rel="stylesheet" type="text/css" href="../assets/css/main.css">
    <link rel="stylesheet" type="text/css" href="../assets/css/gaya.css">
    <link rel="stylesheet" type="text/css"
href="../assets/plugins/datatables/css/jquery.dataTables.css">
    <!-- HTML5 Shim and Respond.js IE8 support of HTML5 elements and
media queries-->
    <!-- if lt IE 9
    script(src='https://oss.maxcdn.com/libs/html5shiv/3.7.0/html5shiv.js')
    script(src='https://oss.maxcdn.com/libs/respond.js/1.4.2/respond.min.js')
-->

```

```
</head>
<body class="sidebar-mini fixed">

<?php include('navmenu.php'); ?>
<div class="content-wrapper">
<div class="page-title">
<div>
<h1><i class="fa fa-dashboard"></i> Daftar Berkas Enkripsi dan
Dekripsi</h1>
</div>
<div>
<ul class="breadcrumb">
<li><i class="fa fa-home fa-lg"></i></li>
<li><a href="index.php">Dashboard</a></li>
<li>Daftar Berkas</li>
</ul>
</div>
</div>
<div class="row">
<div class="col-md-12">
<div class="card">
<div class="card-body">
<div class="table-responsive">
<table id="file" class="table striped">
<thead class="bg-primary">
<tr>
<td><strong>ID File</strong></td>
<td><strong>Nama pengguna</strong></td>
<td><strong>Nama Berkas</strong></td>
<td><strong>Nama Berkas Enkripsi</strong></td>
<td><strong>Ukuran Berkas</strong></td>
<td><strong>Tanggal</strong></td>
<td><strong>Status Enkripsi</strong></td>
<td><strong>Opsi</strong></td>
</tr>
</thead>
<!--
<tfoot class="bg-primary">
<tr>
<td><strong>ID Berkas</strong></td>
<td><strong>Nama pengguna</strong></td>
<td><strong>Nama Berkas Sumber</strong></td>
<td><strong>Nama Berkas Enkripsi</strong></td>
<td><strong>Ukuran Berkas</strong></td>
<td><strong>Tanggal</strong></td>
<td><strong>Status</strong></td>
```



```
";  
echo "<a  
href='file_decrypt/$namabrks' class='btn btn-success'>Download</a>";  
  
}else {  
echo "<span class='btn btn-danger'>Status Tidak  
Diketahui</span>";  
}  
?></td>  
  
</tr>  
<?php  
>  
</tbody>  
</table>  
</div>  
</div>  
</div>  
</div>  
</div>  
</div>  
<script src="../assets/js/jquery-2.1.4.min.js"></script>  
<script type="text/javascript">  
$(document).ready(function() {  
$('#file').dataTable({  
"bPaginate": true,  
"bLengthChange": false,  
"bFilter": true,  
"bInfo": true,  
"bAutoWidth": true,  
"order": [0, "asc"]  
});  
});  
</script>  
<script src="../assets/js/essential-plugins.js"></script>  
<script src="../assets/js/bootstrap.min.js"></script>  
<script src="../assets/plugins/datatables/js/jquery.dataTables.js"></script>  
<script src="../assets/js/plugins/pace.min.js"></script>  
<script src="../assets/js/main.js"></script>  
</body>  
</html>
```