Using PHP “openssl_encrypt” and “openssl_decrypt” to Encrypt and Decrypt Data

Article Number: 48 | Rating: Unrated | Last Updated: Sun, Oct 4, 2020 at 5:42 PM

```
<?php
//$key is our base64 encoded 256bit key that we created earlier. You will probably store and define this key in a config file.
$key='bRuD5WYw5wd0rdHR9yLlM6wt2vteuiniQBqE70nAuhU=';

functionmy_encrypt($data,$key){
    // Remove the base64 encoding from our key
    $encryption_key=base64_decode($key);
    // Generate an initialization vector
    $iv=openssl_random_pseudo_bytes(openssl_cipher_iv_length('aes-256-cbc'));
    // Encrypt the data using AES 256 encryption in CBC mode using our encryption key and initialization vector.
    $encrypted=openssl_encrypt($data,'aes-256-cbc',$encryption_key,0,$iv);
    // The $iv is just as important as the key for decrypting, so save it with our encrypted data using a unique separator (::)
    returnbase64_encode($encrypted.'::'.$iv);
}

functionmy_decrypt($data,$key){
    // Remove the base64 encoding from our key
    $encryption_key=base64_decode($key);
    // To decrypt, split the encrypted data from our IV - our unique separator used was "::"
    list($encrypted_data,$iv)=explode('::',base64_decode($data),2);
    returnopenssl_decrypt($encrypted_data,'aes-256-cbc',$encryption_key,0,$iv);
}

//our data to be encoded
$password_plain='abc123';
echo$password_plain."<br>";

//our data being encrypted. This encrypted data will probably be going into a database
//since it's base64 encoded, it can go straight into a varchar or text database field without corruption worry
$password_encrypted=my_encrypt($password_plain,$key);
echo$password_encrypted."<br>";

//now we turn our encrypted data back to plain text
$password_decrypted=my_decrypt($password_encrypted,$key);
echo$password_decrypted."<br>";
```

Reference:

https://bhoover.com/using-php-openssl_encrypt-openssl_decrypt-encrypt-decrypt-data/

Posted by: Saeed Nobakht - Sun, Oct 4, 2020 at 5:42 PM. This article has been viewed 1752 times.

Online URL: https://www.navel.ir/article/using-php-“openssl_encrypt”-and-“openssl_decrypt”-to-encrypt-and-decrypt-data-48.html