PHP – Encryption

Early versions of PHP included mcrypt extension, that provided encryption/decryption capabilities. Due to lack of maintenance, the mycrypt extension has been deprecated and removed from PHP 7.2 version onwards. PHP now includes OpenSSL library that has an extensive functionality to support encryption and decryption features.

OpenSSL supports various encryption algorithms such as AES (Advanced Encryption Standard). All the supported algorithms can be obtained by invoking openssl_get_cipher_methods() function.

The two important functions in OpenSSL extension are –

- **openssl_encrypt()** – Encrypts data
- **openssl_decrypt()** – Decrypts data

The openssl_encrypt() Function

This function encrypts the given data with given method and key, and returns a raw or base64 encoded string –

```
openssl_encrypt(
   string $data,
   string $cipher_algo,
   string $passphrase,
   int $options = 0,
   string $iv = "",
   string &$tag = null,
   string $aad = "",
   int $tag_length = 16
): string|false
```

The function has the following **parameters** –

Sr.No	Parameter & Description
1	**data** The plaintext message data to be encrypted.
2	**cipher_algo**

	The cipher method.
3	**passphrase** The passphrase. If the passphrase is shorter than expected, padded with NULL characters; if the passphrase is longer than expected, it is truncated.
4	**options** options is a bitwise disjunction of the flags OPENSSL_RAW_DATA and OPENSSL_ZERO_PADDING.
5	**iv** A non-NULL Initialization Vector.
6	**tag** The authentication tag passed by reference when using AEAD cipher mode (GCM or CCM).
7	**aad** Additional authenticated data.
8	**tag_length** The length of the authentication tag. Its value can be between 4 and 16 for GCM mode.

The function returns the encrypted string on success or **false** on failure.

The openssl_decrypt() Function

This function takes a raw or base64 encoded string and decrypts it using a given method and key.

```
openssl_decrypt(
   string $data,
   string $cipher_algo,
   string $passphrase,
   int $options = 0,
   string $iv = "",
   ?string $tag = null,
   string $aad = ""
): string|false
```

The **openssl_decrypt()** function uses the same parameters as the **openssl_encrypt** function.

This function returns the decrypted string on success or false on failure.

Example

Take a look at the following example –

</> Open Compiler

```
<?php
   function sslencrypt($source, $algo, $key, $opt, $iv) {
      $encstring = openssl_encrypt($source, $algo, $key, $opt, $iv);
      return $encstring;
   }

   function ssldecrypt($encstring, $algo, $key, $opt, $iv) {
      $decrstring = openssl_decrypt($encstring, $algo, $key, $opt, $iv);
      return $decrstring;
   }

   // string to be encrypted
   $source = "PHP: Hypertext Preprocessor";

   // Display the original string
   echo "Before encryption: " . $source . "\n";
   $algo = "BF-CBC";
   $opt=0;
   $ivlength = openssl_cipher_iv_length($algo);
   $iv = random_bytes($ivlength);
   $key = "abcABC123!@#";

   // Encryption process
   $encstring = sslencrypt($source, $algo, $key, $opt, $iv);

   // Display the encrypted string
   echo "Encrypted String: " . $encstring . "\n";

   // Decryption process
   $decrstring = ssldecrypt($encstring, $algo, $key, $opt, $iv);

   // Display the decrypted string
   echo "Decrypted String: " . $decrstring;
?>
```

It will produce the following **output** –

```
Before encryption: PHP: Hypertext Preprocessor
Encrypted String:
Decrypted String:
```