

aes_decrypt

WMMEGA FW >= 2.1147 WM-M2 FW >= 3.1147

Decrypt AES-encrypted data in **string**

Description

string aes_decrypt (**string** \$data , **int** \$length , **string** \$key , **string** \$iv)

Decrypts the string \$data with length \$length bytes. Pass the encryption key and iv value in the corresponding fields.

Parameter

\$data: AES-encrypted string - it should be a multiple of 16 bytes long

\$length: length of encrypted string

\$key: Encryption key - this should be multiples of 16 bytes long. A 16 character string will yield 128-bit encryption.

\$iv: This should be a unique 16 character string which will be used for the iv table

Return Values

Decrypted **string** (or **int** 0 for error)

Example

```
<pre><?
// create your custom key and IV value

$key="0123456789abcdef"; // this is 16 bytes, or 128 bits
$iv="abcdef0123456789"; // this needs to be 16 bytes long

$data="This is my super secret encrypted string";

// round up the string length to the nearest multiple of 16

$len=intval((strlen($data)+1)/16)*16;
```

```
// encrypt the data

$encrypted_data = aes_encrypt($data,$len,$key,$iv);

// store encrypted data into a base64-encoded string for easy transport

$base64_encrypted = base64_encode($encrypted_data);

print("Your encrypted data is: ".$base64_encrypted);

// this will yield:
// fcPkxhW0UM4VIYB1CsbK/7wEBuC4WAwc05tDBkcMXbfmf/g0Hqdnrz5qHBRVY8Ls

// base64 decode the string again

$base64_decrypted = base64_decode($base64_encrypted);

// we will use the calculated length from the encryption as the strlen()
function
// may not yield a valid result if the encrypted string has a zero in it.

// decryption routine

$plain_data = aes_decrypt(&$base64_decrypted,$len,$key,$iv);

print("\r\nYour decrypted data is: ".$plain_data);

?>
```

The above example will output something similar to:

```
Your encrypted data is:
fcPkxhW0UM4VIYB1CsbK/7wEBuC4WAwc05tDBkcMXbckp5yUp4a92BeD7VpVGwd1
Your decrypted data is: This is my super secret encrypted string
```

See Also

[aes_encrypt\(\)](#) - Encrypt data using the AES algorithm</html>

aes_decrypt

WMMEGA FW >= 2.1147 WM-M2 FW >= 3.1147

Decrypt AES-encrypted data in **string**

Description

`string` aes_decrypt (`string` \$data , `int` \$length , `string` \$key , `string` \$iv)

Decrypts the string \$data with length \$length bytes. Pass the encryption key and iv value in the corresponding fields.

Parameter

\$data: AES-encrypted string - it should be a multiple of 16 bytes long

\$length: length of encrypted string

\$key: Encryption key - this should be multiples of 16 bytes long. A 16 character string will yield 128-bit encryption.

\$iv: This should be a unique 16 character string which will be used for the iv table

Return Values

Decrypted `string` (or `int` 0 for error)

Example

```
<pre><?
// create your custom key and IV value

$key="0123456789abcdef"; // this is 16 bytes, or 128 bits
$iv="abcdef0123456789"; // this needs to be 16 bytes long

$data="This is my super secret encrypted string";

// round up the string length to the nearest multiple of 16
$len=intval((strlen($data)+1)/16)*16;

// encrypt the data

$encrypted_data = aes_encrypt($data,$len,$key,$iv);

// store encrypted data into a base64-encoded string for easy transport

$base64_encrypted = base64_encode($encrypted_data);
```

```
print("Your encrypted data is: ".$base64_encrypted);

// this will yield:
// fcPkxhW0UM4VIYB1CsbK/7wEBuC4WAwc05tDBkcMXbmf/g0Hqdnrz5qHBRVY8Ls

// base64 decode the string again

$base64_decrypted = base64_decode($base64_encrypted);

// we will use the calculated length from the encryption as the strlen()
function
// may not yield a valid result if the encrypted string has a zero in it.

// decryption routine

$plain_data = aes_decrypt(&$base64_decrypted,$len,$key,$iv);

print("\r\nYour decrypted data is: ".$plain_data);

?>
```

The above example will output something similar to:

```
Your encrypted data is:
fcPkxhW0UM4VIYB1CsbK/7wEBuC4WAwc05tDBkcMXbckp5yUp4a92BeD7VpVGwd1
Your decrypted data is: This is my super secret encrypted string
```

See Also

[aes_encrypt\(\)](#) - Encrypt data using the AES algorithm

From:

<http://wattmon.com/dokuwiki/> - **Wattmon Documentation Wiki**

Permanent link:

http://wattmon.com/dokuwiki/uphp/functions/aes_decrypt?rev=1565937415

Last update: **2021/09/13 05:56**

