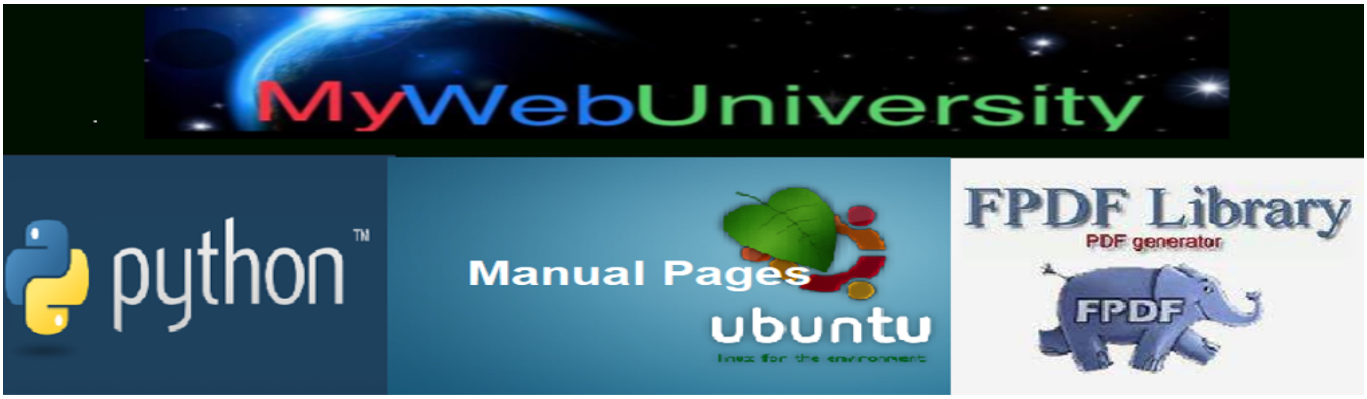

Rocky Enterprise Linux 9.2 Manual Pages on command 'Crypt::AuthEnc::OCB.3pm'

$ man Crypt::AuthEnc::OCB.3pm

Crypt::AuthEnc::OCB(3pm) User Contributed Perl Documentation Crypt::AuthEnc::OCB(3pm)

NAME

Crypt::AuthEnc::OCB - Authenticated encryption in OCBv3 mode

SYNOPSIS

```
### OO interface
use Crypt::AuthEnc::OCB;

# encrypt and authenticate
my $ae = Crypt::AuthEnc::OCB->new("AES", $key, $nonce, $tag_len);
$ae->adata_add('additional_authenticated_data1');
$ae->adata_add('additional_authenticated_data2');
my $ct = $ae->encrypt_add('data1');
$ct .= $ae->encrypt_add('data2');
$ct .= $ae->encrypt_add('data3');
$ct .= $ae->encrypt_last('rest of data');
my $tag = $ae->encrypt_done();

# decrypt and verify
my $ae = Crypt::AuthEnc::OCB->new("AES", $key, $nonce, $tag_len);
$ae->adata_add('additional_authenticated_data1');
$ae->adata_add('additional_authenticated_data2');
```

```
my $pt = $ae->decrypt_add('ciphertext1');
$pt .= $ae->decrypt_add('ciphertext2');
$pt .= $ae->decrypt_add('ciphertext3');
$pt .= $ae->decrypt_last('rest of data');
my $tag = $ae->decrypt_done();
die "decrypt failed" unless $tag eq $expected_tag;

#or
my $result = $ae->decrypt_done($expected_tag); # 0 or 1

### functional interface
use Crypt::AuthEnc::OCB qw(ocb_encrypt_authenticate ocb_decrypt_verify);

my ($ciphertext, $tag) = ocb_encrypt_authenticate('AES', $key, $nonce, $adata, $tag_len, $plaintext);
my $plaintext = ocb_decrypt_verify('AES', $key, $nonce, $adata, $ciphertext, $tag);
```

DESCRIPTION

This module implements OCB v3 according to <https://tools.ietf.org/html/rfc7253>

EXPORT

Nothing is exported by default.

You can export selected functions:

```
use Crypt::AuthEnc::OCB qw(ocb_encrypt_authenticate ocb_decrypt_verify);
```

FUNCTIONS

ocb_encrypt_authenticate

```
my ($ciphertext, $tag) = ocb_encrypt_authenticate($cipher, $key, $nonce, $adata, $tag_len, $plaintext);

# $cipher .. 'AES' or name of any other cipher with 16-byte block len
# $key ..... AES key of proper length (128/192/256bits)
# $nonce ... unique nonce/salt (no need to keep it secret)
```

```
    # $adata ... additional authenticated data
    # $tag_len . required length of output tag

  ocb_decrypt_verify
     my $plaintext = ocb_decrypt_verify($cipher, $key, $nonce, $adata, $ciphertext, $tag);
     # on error returns undef

METHODS
  new
    my $ae = Crypt::AuthEnc::OCB->new($cipher, $key, $nonce, $tag_len);

    # $cipher .. 'AES' or name of any other cipher with 16-byte block len
    # $key ..... AES key of proper length (128/192/256bits)
    # $nonce ... unique nonce/salt (no need to keep it secret)
    # $tag_len . required length of output tag

  adata_add
    $ae->adata_add($adata);                    #can be called multiple times

  encrypt_add
    $ciphertext = $ae->encrypt_add($data);      # can be called multiple times

    #BEWARE: size of $data has to be multiple of blocklen (16 for AES)

  encrypt_last
    $ciphertext = $ae->encrypt_last($data);

  encrypt_done
    $tag = $ae->encrypt_done();                # returns $tag value

  decrypt_add
    $plaintext = $ae->decrypt_add($ciphertext);    # can be called multiple times
```

```
    #BEWARE: size of $ciphertext has to be multiple of blocklen (16 for AES)

  decrypt_last
    $plaintext = $ae->decrypt_last($data);

  decrypt_done
    my $tag = $ae->decrypt_done;          # returns $tag value
    #or
    my $result = $ae->decrypt_done($tag);  # returns 1 (success) or 0 (failure)

  clone
    my $ae_new = $ae->clone;
```

SEE ALSO

- CryptX, Crypt::AuthEnc::CCM, Crypt::AuthEnc::GCM, Crypt::AuthEnc::EAX
- <https://en.wikipedia.org/wiki/OCB_mode>
- <https://tools.ietf.org/html/rfc7253>