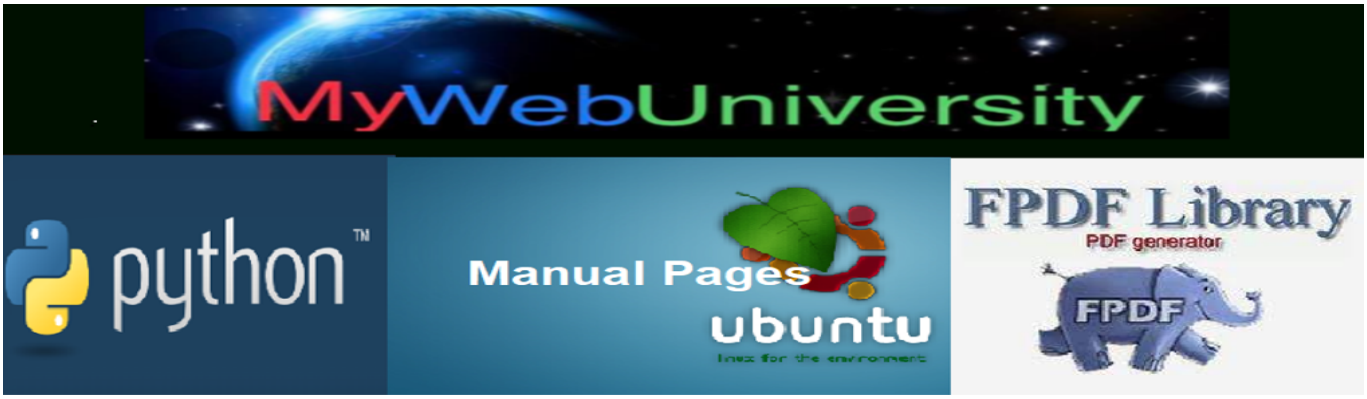

Rocky Enterprise Linux 9.2 Manual Pages on command 'Crypt::Mode::OFB.3pm'

$ man Crypt::Mode::OFB.3pm

Crypt::Mode::OFB(3pm) User Contributed Perl Documentation Crypt::Mode::OFB(3pm)

NAME

Crypt::Mode::OFB - Block cipher mode OFB [Output feedback]

SYNOPSIS

```
use Crypt::Mode::OFB;
my $m = Crypt::Mode::OFB->new('AES');

#(en|de)crypt at once
my $ciphertext = $m->encrypt($plaintext, $key, $iv);
my $plaintext = $m->decrypt($ciphertext, $key, $iv);

#encrypt more chunks
$m->start_encrypt($key, $iv);
my $ciphertext = $m->add('some data');
$ciphertext .= $m->add('more data');

#decrypt more chunks
$m->start_decrypt($key, $iv);
my $plaintext = $m->add($some_ciphertext);
$plaintext .= $m->add($more_ciphertext);
```

DESCRIPTION

This module implements OFB cipher mode. NOTE: it works only with ciphers from CryptX (Crypt::Cipher::NNNN).

METHODS

new

```
my $m = Crypt::Mode::OFB->new($name);
#or
my $m = Crypt::Mode::OFB->new($name, $cipher_rounds);

# $name ..... one of 'AES', 'Anubis', 'Blowfish', 'CAST5', 'Camellia', 'DES', 'DES_EDE',
#                 'KASUMI', 'Khazad', 'MULTI2', 'Noekeon', 'RC2', 'RC5', 'RC6',
#                 'SAFERP', 'SAFER_K128', 'SAFER_K64', 'SAFER_SK128', 'SAFER_SK64',
#                 'SEED', 'Skipjack', 'Twofish', 'XTEA', 'IDEA', 'Serpent'
#                 simply any <NAME> for which there exists Crypt::Cipher::<NAME>
# $cipher_rounds ... optional num of rounds for given cipher
```

encrypt

```
my $ciphertext = $m->encrypt($plaintext, $key, $iv);
```

decrypt

```
my $plaintext = $m->decrypt($ciphertext, $key, $iv);
```

start_encrypt

```
$m->start_encrypt($key, $iv);
```

start_decrypt

```
$m->start_decrypt($key, $iv);
```

add

```
# in encrypt mode
my $plaintext = $m->add($ciphertext);
```

```
# in decrypt mode
my $ciphertext = $m->add($plaintext);
```

SEE ALSO

- CryptX, Crypt::Cipher
- Crypt::Cipher::AES, Crypt::Cipher::Blowfish, ...
- <https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation#Output_feedback_.28OFB.29>