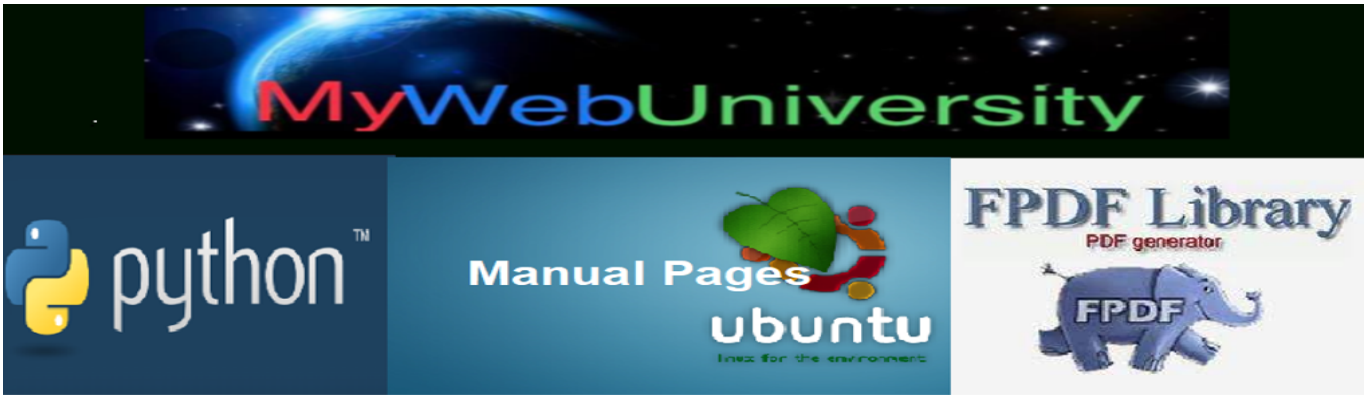

Rocky Enterprise Linux 9.2 Manual Pages on command 'Crypt::Cipher::AES.3pm'

$ man Crypt::Cipher::AES.3pm

Crypt::Cipher::AES(3pm) User Contributed Perl Documentation Crypt::Cipher::AES(3pm)

NAME

Crypt::Cipher::AES - Symmetric cipher AES (aka Rijndael), key size: 128/192/256 bits

SYNOPSIS

```
### example 1
use Crypt::Mode::CBC;

my $key = '...'; # length has to be valid key size for this cipher
my $iv = '...';  # 16 bytes
my $cbc = Crypt::Mode::CBC->new('AES');
my $ciphertext = $cbc->encrypt("secret data", $key, $iv);

### example 2 (slower)
use Crypt::CBC;
use Crypt::Cipher::AES;

my $key = '...'; # length has to be valid key size for this cipher
my $iv = '...';  # 16 bytes
my $cbc = Crypt::CBC->new( -cipher=>'Cipher::AES', -key=>$key, -iv=>$iv );
my $ciphertext = $cbc->encrypt("secret data");
```

DESCRIPTION

This module implements the AES cipher. Provided interface is compliant with Crypt::CBC module.

BEWARE: This module implements just elementary "one-block-(en|de)cryption" operation - if you want to encrypt/decrypt generic data you have to use some of the cipher block modes - check for example Crypt::Mode::CBC, Crypt::Mode::CTR or Crypt::CBC (which will be slower).

METHODS

new

```
$c = Crypt::Cipher::AES->new($key);
#or
$c = Crypt::Cipher::AES->new($key, $rounds);
```

encrypt

```
$ciphertext = $c->encrypt($plaintext);
```

decrypt

```
$plaintext = $c->decrypt($ciphertext);
```

keysize

```
$c->keysize;
#or
Crypt::Cipher::AES->keysize;
#or
Crypt::Cipher::AES::keysize;
```

blocksize

```
$c->blocksize;
#or
Crypt::Cipher::AES->blocksize;
#or
Crypt::Cipher::AES::blocksize;
```

max_keysize

```
$c->max_keysize;
#or
Crypt::Cipher::AES->max_keysize;
#or
Crypt::Cipher::AES::max_keysize;
```

min_keysize

```
$c->min_keysize;
#or
Crypt::Cipher::AES->min_keysize;
#or
Crypt::Cipher::AES::min_keysize;
```

default_rounds

```
$c->default_rounds;
#or
Crypt::Cipher::AES->default_rounds;
#or
Crypt::Cipher::AES::default_rounds;
```

SEE ALSO

- CryptX, Crypt::Cipher
- <https://en.wikipedia.org/wiki/Advanced_Encryption_Standard>