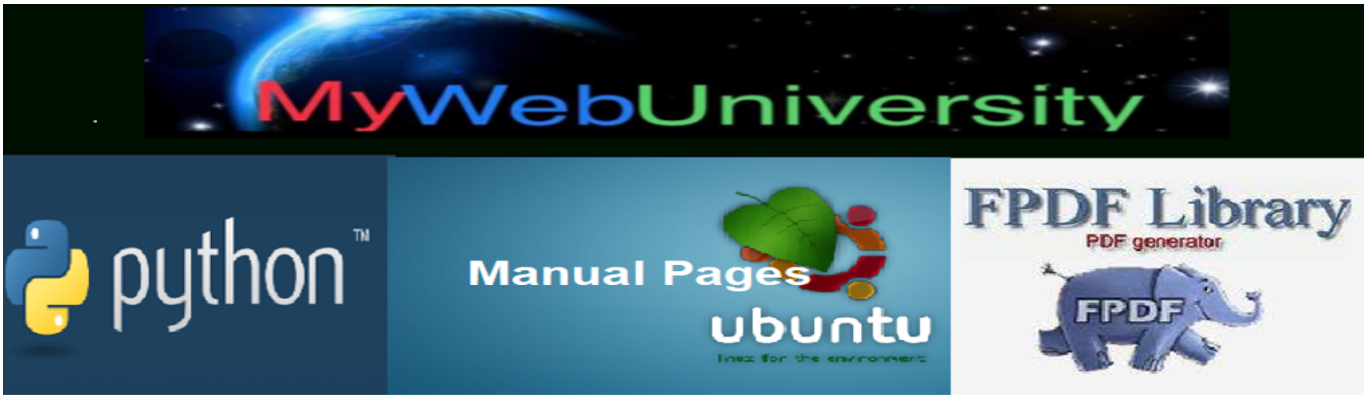

Rocky Enterprise Linux 9.2 Manual Pages on command 'Crypt::Digest::CHAES.3pm'

$ man Crypt::Digest::CHAES.3pm

Crypt::Digest::CHAES(3pm) User Contributed Perl Documentation Crypt::Digest::CHAES(3pm)

NAME

Crypt::Digest::CHAES - Hash function - CipherHash based on AES [size: 128 bits]

SYNOPSIS

```
### Functional interface:
use Crypt::Digest::CHAES qw( chaes chaes_hex chaes_b64 chaes_b64u
                             chaes_file chaes_file_hex chaes_file_b64 chaes_file_b64u );

# calculate digest from string/buffer
$chaes_raw  = chaes('data string');
$chaes_hex  = chaes_hex('data string');
$chaes_b64  = chaes_b64('data string');
$chaes_b64u = chaes_b64u('data string');
# calculate digest from file
$chaes_raw  = chaes_file('filename.dat');
$chaes_hex  = chaes_file_hex('filename.dat');
$chaes_b64  = chaes_file_b64('filename.dat');
$chaes_b64u = chaes_file_b64u('filename.dat');
# calculate digest from filehandle
$chaes_raw  = chaes_file(*FILEHANDLE);
$chaes_hex  = chaes_file_hex(*FILEHANDLE);
```

```
$chaes_b64  = chaes_file_b64(*FILEHANDLE);
$chaes_b64u = chaes_file_b64u(*FILEHANDLE);

### OO interface:
use Crypt::Digest::CHAES;

$d = Crypt::Digest::CHAES->new;
$d->add('any data');
$d->addfile('filename.dat');
$d->addfile(*FILEHANDLE);
$result_raw  = $d->digest;     # raw bytes
$result_hex  = $d->hexdigest;  # hexadecimal form
$result_b64  = $d->b64digest;  # Base64 form
$result_b64u = $d->b64udigest; # Base64 URL Safe form
```

DESCRIPTION

Provides an interface to the CHAES digest algorithm.

EXPORT

Nothing is exported by default.

You can export selected functions:

```
use Crypt::Digest::CHAES qw(chaes chaes_hex chaes_b64 chaes_b64u
                            chaes_file chaes_file_hex chaes_file_b64 chaes_file_b64u);
```

Or all of them at once:

```
use Crypt::Digest::CHAES ':all';
```

FUNCTIONS

chaes

Logically joins all arguments into a single string, and returns its CHAES digest encoded

as a binary string.

```
$chaes_raw = chaes('data string');
#or
$chaes_raw = chaes('any data', 'more data', 'even more data');
```

chaes_hex

Logically joins all arguments into a single string, and returns its CHAES digest encoded as a hexadecimal string.

```
$chaes_hex = chaes_hex('data string');
#or
$chaes_hex = chaes_hex('any data', 'more data', 'even more data');
```

chaes_b64

Logically joins all arguments into a single string, and returns its CHAES digest encoded as a Base64 string, with trailing '=' padding.

```
$chaes_b64 = chaes_b64('data string');
#or
$chaes_b64 = chaes_b64('any data', 'more data', 'even more data');
```

chaes_b64u

Logically joins all arguments into a single string, and returns its CHAES digest encoded as a Base64 URL Safe string (see RFC 4648 section 5).

```
$chaes_b64url = chaes_b64u('data string');
#or
$chaes_b64url = chaes_b64u('any data', 'more data', 'even more data');
```

chaes_file

Reads file (defined by filename or filehandle) content, and returns its CHAES digest encoded as a binary string.

```
$chaes_raw = chaes_file('filename.dat');
#or
$chaes_raw = chaes_file(*FILEHANDLE);
```

chaes_file_hex

Reads file (defined by filename or filehandle) content, and returns its CHAES digest encoded as a hexadecimal string.

```
$chaes_hex = chaes_file_hex('filename.dat');
#or
$chaes_hex = chaes_file_hex(*FILEHANDLE);
```

BEWARE: You have to make sure that the filehandle is in binary mode before you pass it as argument to the addfile() method.

chaes_file_b64

Reads file (defined by filename or filehandle) content, and returns its CHAES digest encoded as a Base64 string, with trailing '=' padding.

```
$chaes_b64 = chaes_file_b64('filename.dat');
#or
$chaes_b64 = chaes_file_b64(*FILEHANDLE);
```

chaes_file_b64u

Reads file (defined by filename or filehandle) content, and returns its CHAES digest encoded as a Base64 URL Safe string (see RFC 4648 section 5).

```
$chaes_b64url = chaes_file_b64u('filename.dat');
#or
$chaes_b64url = chaes_file_b64u(*FILEHANDLE);
```

The OO interface provides the same set of functions as Crypt::Digest.

new

```
$d = Crypt::Digest::CHAES->new();
```

clone

```
$d->clone();
```

reset

```
$d->reset();
```

add

```
$d->add('any data');
#or
$d->add('any data', 'more data', 'even more data');
```

addfile

```
$d->addfile('filename.dat');
#or
$d->addfile(*FILEHANDLE);
```

add_bits

```
$d->add_bits($bit_string);   # e.g. $d->add_bits("111100001010");
#or
$d->add_bits($data, $nbits); # e.g. $d->add_bits("\xF0\xA0", 16);
```

hashsize

```
$d->hashsize;
#or
Crypt::Digest::CHAES->hashsize();
#or
Crypt::Digest::CHAES::hashsize();
```

digest

```
$result_raw = $d->digest();
```

hexdigest

```
$result_hex = $d->hexdigest();
```

b64digest

```
$result_b64 = $d->b64digest();
```

b64udigest

```
$result_b64url = $d->b64udigest();
```

SEE ALSO

- CryptX, Crypt::Digest
- <https://en.wikipedia.org/wiki/Cryptographic_hash_function#Hash_functions_based_on_block_ciphers>