



**Full credit is given to the above companies including the Operating System (OS) that this PDF file was generated!**

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

***\$ man Crypt::Cipher::Khazad.3pm***

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

**NAME**

Crypt::Cipher::Khazad - Symmetric cipher Khazad, key size: 128 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('Khazad');
```

```
my $ciphertext = $cbc->encrypt("secret data", $key, $iv);
```

### example 2 (slower)

```
use Crypt::CBC;
```

```
use Crypt::Cipher::Khazad;
```

```
my $key = '...'; # length has to be valid key size for this cipher
```

```
my $iv = '...'; # 16 bytes
```

```
my $cbc = Crypt::CBC->new( -cipher=>'Cipher::Khazad', -key=>$key, -iv=>$iv );
```

```
my $ciphertext = $cbc->encrypt("secret data");
```

## DESCRIPTION

This module implements the Khazad 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

```
$c = Crypt::Cipher::Khazad->new($key);
```

#or

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

encrypt

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

decrypt

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

keysize

```
$c->keysize;
```

#or

```
Crypt::Cipher::Khazad->keysize;
```

#or

```
Crypt::Cipher::Khazad::keysize;
```

blocksize

```
$c->blocksize;
```

#or

```
Crypt::Cipher::Khazad->blocksize;
```

#or

```
Crypt::Cipher::Khazad::blocksize;
```

max\_keysize

```
$c->max_keysize;
```

```
#or
```

```
Crypt::Cipher::Khazad->max_keysize;
```

```
#or
```

```
Crypt::Cipher::Khazad::max_keysize;
```

min\_keysize

```
$c->min_keysize;
```

```
#or
```

```
Crypt::Cipher::Khazad->min_keysize;
```

```
#or
```

```
Crypt::Cipher::Khazad::min_keysize;
```

default\_rounds

```
$c->default_rounds;
```

```
#or
```

```
Crypt::Cipher::Khazad->default_rounds;
```

```
#or
```

```
Crypt::Cipher::Khazad::default_rounds;
```

SEE ALSO

? CryptX, Crypt::Cipher

? <<https://en.wikipedia.org/wiki/KHAZAD>>

perl v5.34.0

2022-02-06

Crypt::Cipher::Khazad(3pm)