Digest::MD5

José Pedro Oliveira
(jpo@di.uminho.pt)

Grupo de Sistemas Distribuídos
Departamento de Informática
Escola de Engenharia
Universidade do Minho

Administração de Sistemas I
2006-2007

Conteúdo

Introdução

Módulo Digest::MD5

Este módulo permite que se utilize o algoritmo **MD5 Message Digest** em programas Perl. Este algoritmo recebe como entrada uma mensagem de comprimento arbitrário e produz como saída um número de 128-bit denominado *fingerprint* ou *message digest* da mensagem.

Autor

Gisle Aas

Homepage

`http://search.cpan.org/dist/Digest-MD5/`

Conteúdo

Digest::MD5 - interface imperativo

Funções

O módulo Digest::MD5 fornece um interface imperativo para utilização básica. Este interface disponibiliza as seguintes funções:

- `md5($data, ...)`
- `md5_hex($data, ...)`
- `md5_base64($data, ...)`

Nota

Nenhuma das funções acima é exportada automaticamente.

Interface imperativo: exemplo 1

Sem importar símbolos adicionais

```
1  #!/usr/bin/perl -w
2  use strict;
3
4  use Digest::MD5;
5
6  my $msg = "Texto da mensagem\n";
7
8  my $md5 = Digest::MD5::md5_hex($msg);
9
10 print "$md5\n";
```

Interface imperativo: exemplo 2

Importando o símbolo `md5_hex`

```
1  #!/usr/bin/perl -w
2  use strict;
3
4  use Digest::MD5 qw(md5_hex);
5
6  my $msg = "Texto da mensagem\n";
7
8  my $md5 = md5_hex($msg);
9
10 print "$md5\n";
```

Conteúdo

Digest::MD5 - interface object oriented

Métodos

Para utilização mais avançada é disponibilizado um interface *Object Oriented*. A utilização deste interface permite tratar mensagens de comprimento arbitrário e manipular ficheiros. Este interface disponibiliza os seguintes métodos:

- `$md5 = Digest::MD5->new`
- `$md5->add($data, ...)`
- `$md5->addfile($iohandle)`
- `$md5->digest`
- `$md5->hexdigest`
- `$md5->b64digest`
- `...`

Interface Object Oriented: exemplo 1

Não é necessário importar símbolos adicionais

```
1  #!/usr/bin/perl -w
2  use strict;
3  use Digest::MD5;
4
5  my ($obj, $md5);
6
7  open(FILE, "<ficheiro.txt") or die "Erro: $!";
8  binmode(FILE);                  # Windows
9  $obj = Digest::MD5->new;
10 $obj->addfile(*FILE);
11 $md5 = $obj->hexdigest;
12 close(FILE);
13
14 print "$md5\n";
```


Interface Object Oriented: exemplo 2

Não é necessário importar símbolos adicionais

```
1  #!/usr/bin/perl -w
2  use strict;
3  use Digest::MD5;
4
5  my ($obj, $md5);
6
7  open(FILE, "<ficheiro.txt") or die "Erro: $!";
8  binmode(FILE);                  # Windows
9
10 $md5 = Digest::MD5->new->addfile(*FILE)->hexdigest;
11
12 close(FILE);
13
14 print "$md5\n";
```


Referências adicionais

Referências adicionais

- RFC 1321 - The MD5 Message-Digest Algorithm
  `http://www.ietf.org/rfc/rfc1321.txt`
- MD5 To Be Considered Harmful Someday
  `http://developers.slashdot.org/article.pl?sid=04/12/07/2019244`
- MD5 Collisions
  `http://cryptography.hyperlink.cz/MD5_collisions.html`
- Digest::* - Interfaces Perl para vários algoritmos de Digest
- Digest::SHA1 - Interface Perl para o algoritmo SHA-1

Conteúdo