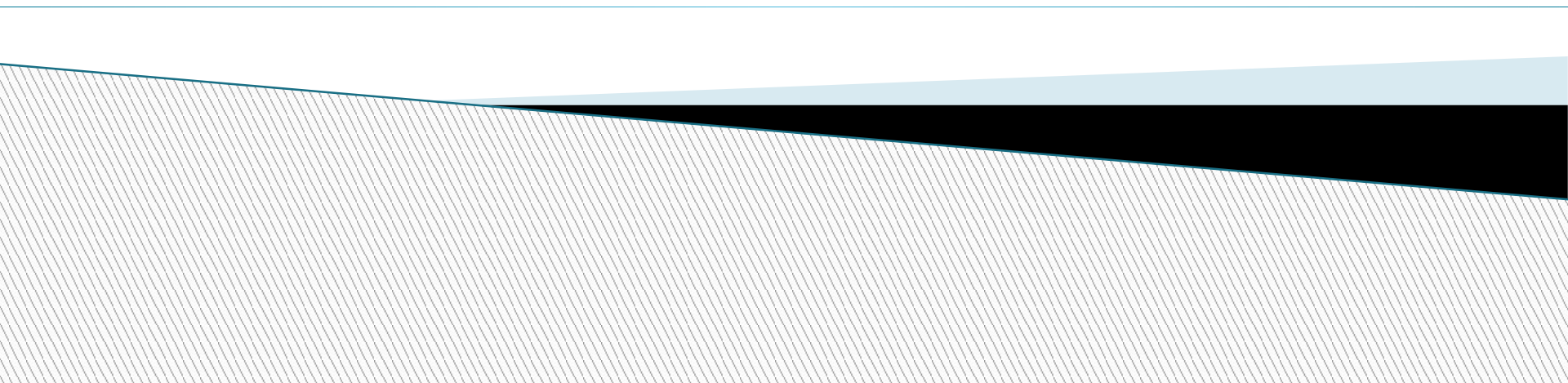


Criptografia & Hashing no PHP

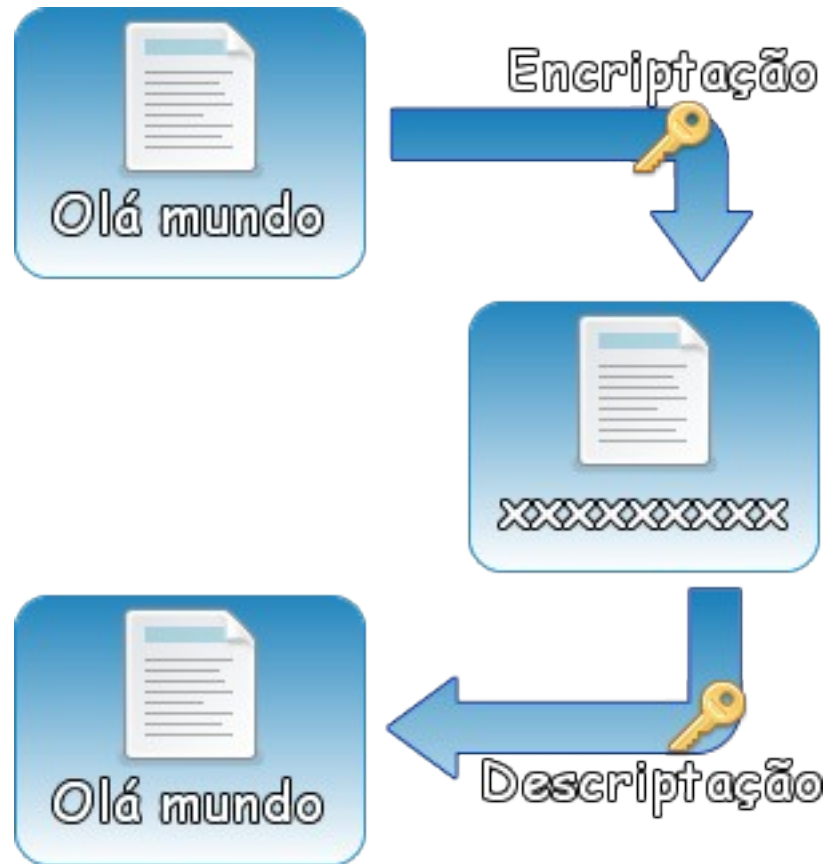
Prof.: Alisson Chiquitto
chiquitto@unipar.br



Criptografia

- ▶ **Criptografia** (Do Grego *kryptós*, "escondido", e *gráphein*, "escrita") é o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário (detentor da "chave secreta")

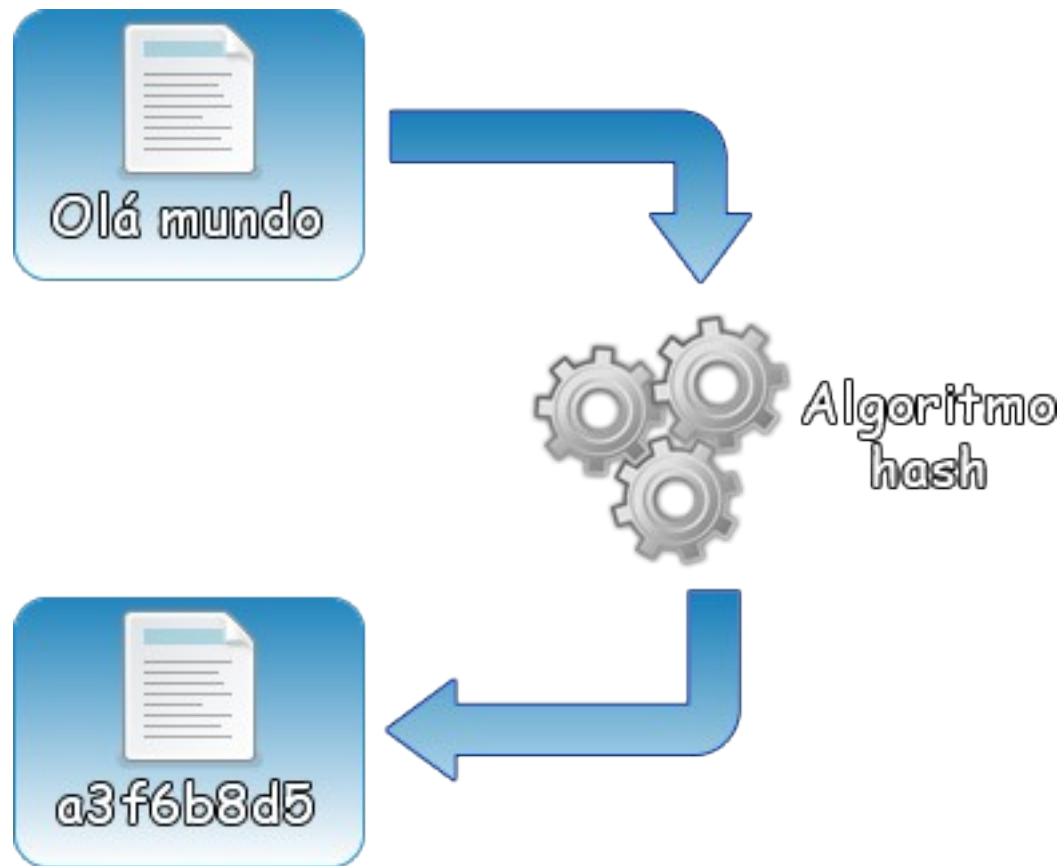
Criptografia



Hashing

- ▶ Um **hash** é uma sequência de bits geradas por um algoritmo, em geral representada em base hexadecimal, que permite a visualização em letras e números (0 a 9 e A a F).

Hashing



Criptografia & Hashing no PHP

▶ Criptografias

- Biblioteca Mcrypt

<http://it.php.net/manual/en/book.mcrypt.php>

▶ Hashing

- Biblioteca Hash

<http://it.php.net/manual/en/book.hash.php>

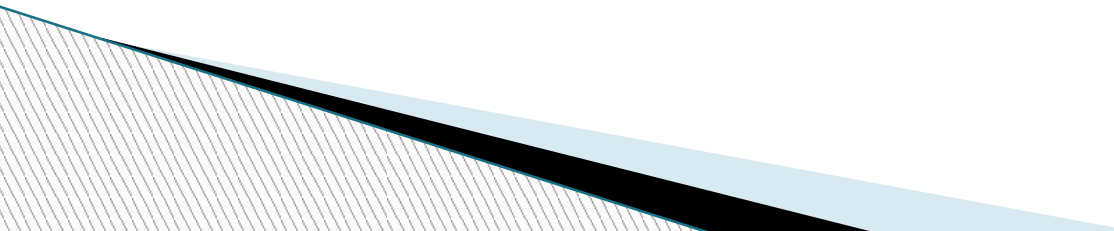
- Função md5()

<http://php.net/md5>

- Função sha1()

<http://php.net/sha1>

Biblioteca Mcrypt

- ▶ Suporta uma grande variedade de blocos de algoritmos, como DES, 3DES, Blowfish (default), entre outros.
 - ▶ Suporta os métodos CBC, OFB, CFB e ECB.
 - ▶ Muito utilizada para criptografar dados usando chaves simétricas.
- 

Mcrypt: Cifras suportadas

- ▶ `mcrypt_list_algorithms()` – Retorna um array com as cifras suportadas pelo sistema;
http://php.net/mcrypt_list_algorithms

```
print_r(mcrypt_list_algorithms());  
// Array ( [0] => cast-128 [1] => gost  
[2] => rijndael-128 [3] => twofish [4]  
=> cast-256 [5] => loki97 )
```


Mcrypt: Encriptar strings

- ▶ Para encriptar strings usamos a função `mcrypt_encrypt()`;
- ▶ Declaração: `mcrypt_encrypt($cipher , $key , $data , $mode , $iv);`
- ▶ Retorna uma string em binario. Use `bin2hex()` para converter para hexadecimal;

Mcrypt: Encriptar strings

- ▶ Parâmetros da função `mcrypt_encrypt()`
 - `$cipher` = Algoritmo de criptografia;
 - `$key` = Chave secreta;
 - `$data` = String a criptografar;
 - `$mode` = Modo da criptografia – Na maioria dos casos use `MCRYPT_MODE_ECB`;
 - `$iv` = Utilizado para a inicialização;

Mcrypt: Encryptar strings

```
$cipher = MCRYPT_RIJNDAEL_256;  
$mode = MCRYPT_MODE_ECB;  
  
$iv_size = mcrypt_get_iv_size($cipher,  
$mode);  
$iv = mcrypt_create_iv($iv_size,  
MCRYPT_RAND);  
$key = "CHAVE SECRETA";  
$text = "TEXTO PARA CRIPTOGRAFIAR";  
$crypttext = mcrypt_encrypt($cipher, $key  
, $text, $mode, $iv);  
  
echo strlen($crypttext) . "<br>";  
echo bin2hex($crypttext);
```

Mcrypt: Descriptar strings

- ▶ Para descriptar strings usamos a função `mcrypt_decrypt()`;
- ▶ Declaração: `mcrypt_decrypt($cipher , $key , $data , $mode , $iv);`
- ▶ Retorna a string descriptografada;

Mcrypt: Descriptar strings

- ▶ Parâmetros da função `mcrypt_decrypt()`
 - `$cipher` = Algoritmo de criptografia;
 - `$key` = Chave secreta;
 - `$data` = String a criptografar;
 - `$mode` = Modo da criptografia – Na maioria dos casos use `MCRYPT_MODE_ECB`;
 - `$iv` = Utilizado para a inicialização;

Mcrypt: Descriptar strings

```
$decrypttext = mcrypt_decrypt( $cipher ,  
    $key , $crypttext , $mode , $iv );
```

```
echo strlen($decrypttext) . "<br>";
```

```
echo $decrypttext . "<br>";
```

Hash: MD5

- ▶ Hash de 16bytes (128 bits);
- ▶ Muito utilizado por softwares Peer-to-peer para verificar integridade de arquivos;
- ▶ Muito utilizada na verificação de senhas;
- ▶ <http://pt.wikipedia.org/wiki/MD5>

Hash: função md5()

- ▶ A função md5(\$string);
- ▶ Parâmetros:
 - \$string = String a ser calculada
- ▶ Calcula o hash md5 de uma string;
- ▶ Retorna uma string com 32 caracteres hexadecimais;
- ▶ <http://php.net/md5>

Hash: função md5()

```
$string = '123123';  
echo md5($string);  
// 4297f44b13955235245b2497399d7a93
```

Hash: Família SHA

- ▶ Possui muitos algoritmos de hash;
- ▶ O mais utilizado é o SHA1, que é considerado o sucessor do MD5;
- ▶ <http://pt.wikipedia.org/wiki/Sha1>

Hash: função sha1()

- ▶ A função sha1(\$string);
- ▶ Parâmetros:
 - \$string = String a ser calculada
- ▶ Calcula o hash sha1 de uma string;
- ▶ Retorna uma string com 40 caracteres hexadecimais;
- ▶ <http://php.net/sha1>

Hash: função sha1()

```
$string = 'Universidade Paranaense';  
echo sha1($string);  
// 5b62b4f85ff011ed77a18095b09de4d9f5c312ad
```

Biblioteca Hash

- ▶ Suporta uma grande variedade de blocos de algoritmos, como MD5 e a família SHA.

Hash: Cifras suportadas

- ▶ `hash_algos()` – Retorna um array com as cifras suportadas pelo sistema;
- ▶ <http://it.php.net/manual/en/function.hash-algos.php>

```
print_r(hash_algos());  
// Array ( [0] => md2 [1] => md4 [2] =>  
md5 [3] => sha1 [4] => sha224 [5] =>  
sha256 [6] => sha384 [7] => sha512 )
```

Hash: Encriptar strings

- ▶ Para encontrar o hash de strings usamos a função `hash()`;
- ▶ Declaração: `hash (string $algo , string $data [, bool $raw_output = false]);`
- ▶ Retorna o hash de `$data`;

Hash: Encriptar strings

- ▶ Parâmetros da função hash()
 - \$algo = Algoritmo de hash;
 - \$data = String a ser hashed;
 - \$raw_output = Se true, o retorno da função será em binário;

Hash: Enciptar strings

```
$string = 'Unipar';  
$hash = hash ( 'sha512' , $string );  
echo $hash;
```