MD5

A primeira que vou falar é sem dúvida a mais comum, chama md5 que é um algoritmo de um hash de 128 bits. Não vou tentar explicar o que é hash nem algoritmo agora… Só vou explicar como você pode usar o md5 na sua aplicação.

O md5 gera uma string alfa-numérica de 32 caracteres, não importa se você tá gerando o md5 de duas letras ou de um texto de 20 parágrafos… O md5 gerado sempre vai ter 32 caracteres.

Você pode usar o md5 na hora de salvar um dado sigiloso (senhas) o banco… Com isso, ninguém tem acesso à senha original do cliente. Depois é só comparar o md5 do que foi digitado no campo senha (na hora do login) com o que está armazenado no banco, se bater, tá tudo certo.

Infelizmente o md5 tem um "problema"… Você pode, com muita dificuldade (preste atenção: muita dificuldade), gerar dois md5 iguais. Duas strings diferentes que acabem como um mesmo md5. Isso é raríssimo, mas pode acontecer.

Pra usar o md5 no PHP é só usar da seguinte forma:

```
<?php
$string = 'O rato reu a ropa do rei de Roma';
$codificada = md5($string);
echo "Resultado da codificação usando md5: " . $codificada;
// 54cf74d1acdb4037ab956c269b63c8ac
```

SHA1

A outra **hash** de mão única é o sha1. Ele é praticamente identico ao md5, só que tem 160 bits, o que acaba criando uma string-resultado maior: 40 caracteres alfa-numéricos. Outro ponto do sha1 é que, por ser 160 bits e gerar uma cadeia de caracteres maior, uma colisão (encontrar duas strings que, codificadas, sejam a mesma coisa) é bem mais rara que numa chave de 128bits.

Usar o sha1 no PHP é exatamente a mesma coisa que o md5, só que mudando o nome da função:

```
<?php
$string = 'O rato reu a ropa do rei de Roma';
$codificada = sha1($string);
echo "Resultado da codificação usando sha1: " . $codificada;
// b186b709f7cf5a1d98d413379a66e511df8d59a4
```

BASE64

É um método para codificação dos dados para transferência na Internet. Ela é uma codificação de mão dupla, e usando uma segunda função você pode descobrir a string original de uma string codificada.

Para usar ela no PHP você tem as duas formas:

```php
<?php
$string = 'O rato reu a ropa do rei de Roma';
$codificada = base64_encode($string);
echo "Resultado da codificação usando base64: " . $codificada;
// TyByYXRvIHJldSBhIHJvcGEgZG8gcmVpIGRlIFJvbWE=
echo "
";
$original = base64_decode($codificada);
echo "Resultado da decodificação usando base64: " . $original;
// O rato reu a ropa do rei de Roma
// Note que $original vai ser idêntica a $string
```

Viram como é simples? Com esses recursos é possível deixar a aplicação bem mais segura e, por que não, organizada.