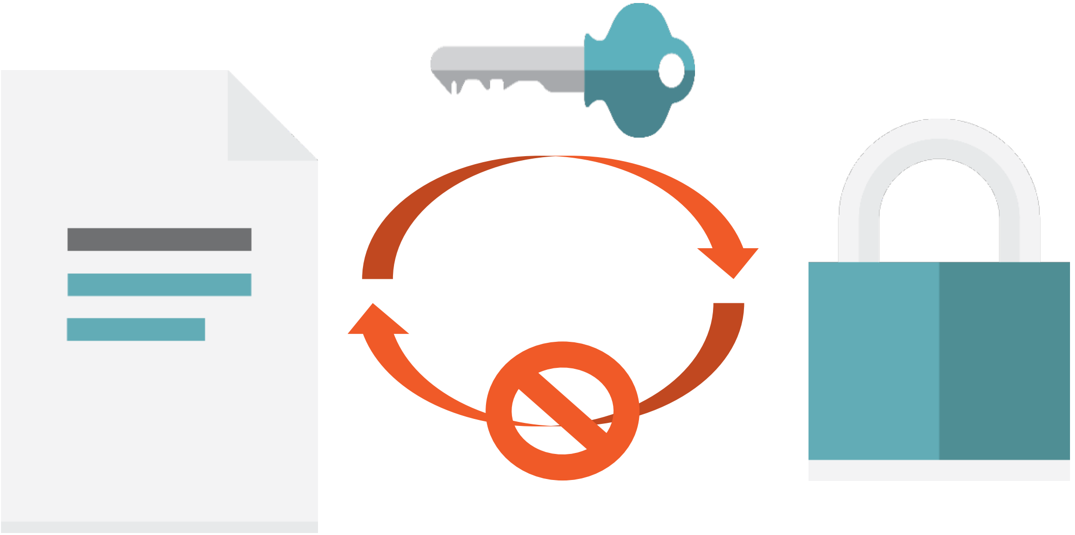
Storing Passwords

Christian Wenz

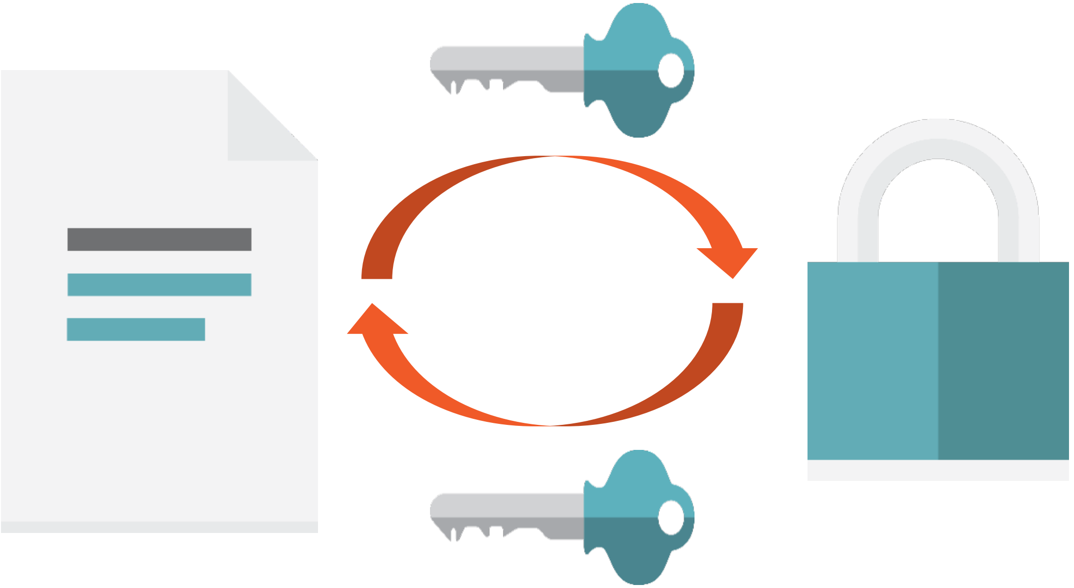
@chwenz

Hashing vs Encryption

Hashing



Encryption



Hashing Algorithms

✗	✗	bcrypt

Demo

Cracking MD5 hashes with little effort

Hashing with PHP

Hashing algorithms

md5()

sha1()

Generic hashing function

crypt()

hash()

Password Hashing API

password_get_info()

password_hash()

password_needs_rehash()

password_verify()

```
$pw = password_hash(
  't0p s€cret',
  PASSWORD_DEFAULT);
```

◀ Create password hash

```
$pw = password_hash(
  't0p s€cret',
  PASSWORD_DEFAULT,
  [ 'cost' => 11 ]);
```

◀ Increase the algorithmic cost for hashing

```
$result = password_verify(
  't0p s€cret', $pw);
```

◀ Verify that a hash belongs to a password

More Password Hashing Functions

password_get_info()

password_needs_rehash()

Summary

Hash passwords, do not encrypt them

Do not use outdated algorithms like MD5 or SHA1

Use PHP’s Password Hashing API