

Barry Austin
Interactive Strategies
doBoard

Crypto Your PHP

Crypto, You Say?

There are two kinds of cryptography in this world: cryptography that will stop your kid sister from reading your files, and cryptography that will stop major governments from reading your files. This book is about the latter.

Bruce Schneier, *Applied Cryptography*

Crypto, You Say?

- What crypto isn't:

```
$notEncrypted = base64_encode($data);
```

```
$notEncrypted = urlencode($data);
```

```
$notEncrypted = crc32($data);
```

Crypto, You Say?

- What crypto is:

```
$encrypted = mcrypt_generic($mcryptResource, $data);
```

```
$hash = hash($algorithm, $data);
```

```
$hmac = hash_hmac($algorithm, $data, $key);
```

When to Use Crypto

- Need protection for confidentiality
- Need protection for integrity
- Need to verify identity
- Need to interoperate

Encrypting Data in Transit

- HTTPS

- HTTPS

- HTTPS

Encrypting Data in Transit

- Okay, other options do exist
 - SSH
 - GnuPG
 - have I mentioned HTTPS?

Encrypting Data in Storage

- Store only what you really need
- Two-way: symmetric encryption
- One-way: cryptographic hash/HMAC

Password Encryption - Transit

- Basic: HTTPS encryption of login data (POST)
- Mid-grade: challenge-response
- High-grade: don't use password

Password Encryption - Storage

- Plain hash is vulnerable
- HMAC in database
- External identity store

Password Encryption - Example

- SHA256 HMAC used for storage
- Login form POSTs password via HTTPS
- Validate by comparing HMAC of the supplied password against HMAC stored for user

Algorithms

- DES has been broken
- 3DES is okay but showing age
- Rijndael is strong and well supported

Algorithms

- MD5 has been broken
- SHA-1 showing some weakness
- SHA-2 is strong and well supported
 - SHA256 is a specific implementation of SHA-2

Algorithms

- PHP doesn't have AES algorithm??

Algorithms

- PHP doesn't have AES algorithm??
- AES is a standard, not an algorithm per se
 - U.S. FIPS 197
 - Rijndael-128 algorithm (block size 128 bits)
 - key sizes 128-, 192-, or 256-bits

Practices

- Use proven methods
- Take care with initialization
- Keep control of keys
- Be mindful of replay or man-in-the-middle

Use Existing Modules

- KADM5
- RADIUS
- SSH2
- OAuth
- OpenSSL
- Crack
- Hash
- GnuPG

...etc

When to Get Help

- Off the beaten path
- Compliance
- Pucker factor

Resources

- <http://www.schneier.com/cryptography.html>
- <http://php.net/manual/en/refs.crypto.php>
- <http://doboard.com>