

15. Cryptographic Services

The modules described in this chapter implement various algorithms of a cryptographic nature. They are available at the discretion of the installation. On Unix systems, the `crypt` module may also be available. Here's an overview:

- 15.1. `hashlib` — Secure hashes and message digests
 - 15.1.1. Hash algorithms
 - 15.1.2. SHAKE variable length digests
 - 15.1.3. Key derivation
 - 15.1.4. BLAKE2
 - 15.1.4.1. Creating hash objects
 - 15.1.4.2. Constants
 - 15.1.4.3. Examples
 - 15.1.4.3.1. Simple hashing
 - 15.1.4.3.2. Using different digest sizes
 - 15.1.4.3.3. Keyed hashing
 - 15.1.4.3.4. Randomized hashing
 - 15.1.4.3.5. Personalization
 - 15.1.4.3.6. Tree mode
 - 15.1.4.4. Credits
- 15.2. `hmac` — Keyed-Hashing for Message Authentication
- 15.3. `secrets` — Generate secure random numbers for managing secrets
 - 15.3.1. Random numbers
 - 15.3.2. Generating tokens
 - 15.3.2.1. How many bytes should tokens use?
 - 15.3.3. Other functions
 - 15.3.4. Recipes and best practices