HashCrypto Documentation

Release 0.4

Jan Brohl

Mar 19, 2017

Contents

As there was no code-review yet, this library should be considered NOT READY FOR PRODUCTION.

Contents:

CHAPTER 1

hashcrypto package

Submodules

hashcrypto.bytesop_fallback module

hashcrypto.bytesop_fallback.**op_xor**(*a*, *b*)
XOR two bytes-like objects.

Module contents

class hashcrypto.**CFB**(*key*, *hash_constructor=<built-in function openssl_sha512>*, *start_iv=None*)
Bases: *hashcrypto.WithIV*

decrypt(*cipher_blocks*, *iv=None*)

decrypt_block(*b*, *iv*)

encrypt(*plain_blocks*, *iv=None*)

class hashcrypto.**CTR**(*key*, *hash_constructor=<built-in function openssl_sha512>*, *nonce=None*)
Bases: *hashcrypto.WithNonce*

decrypt(*plain_blocks*, *counter_start=0*)

decrypt_block(*b*, *counter*)

encrypt(*plain_blocks*, *counter_start=0*)

encrypt_block(*b*, *counter*)

keystream(*counter_start*)

classmethod suggest_nonce_size(*hash_constructor*)

class hashcrypto.**HashCrypt**(*key*, *hash_constructor=<built-in function openssl_sha512>*)
Bases: object

block(*b*)

decrypt_stream(*infile*, *outfile*, **args*, ***kwargs*)

encrypt_file(*infile*, *outfile*, **args*, ***kwargs*)

encrypt_stream(*infile*, *outfile*, **args*, ***kwargs*)

hash_name()

header()

classmethod suggest_key_size(*hash_constructor*)

exception hashcrypto.**IVError**
Bases: exceptions.ValueError

class hashcrypto.**OFB**(*key*, *hash_constructor=<built-in function openssl_sha512>*, *start_iv=None*)
Bases: *hashcrypto.WithIV*

decrypt(*plain_blocks*, *iv=None*)

encrypt(*plain_blocks*, *iv=None*)

keystream(*iv=None*)

class hashcrypto.**WithIV**(*key*, *hash_constructor=<built-in function openssl_sha512>*, *start_iv=None*)
Bases: *hashcrypto.HashCrypt*

header()

classmethod make_iv(*hash_constructor*)

classmethod suggest_iv_size(*hash_constructor*)

class hashcrypto.**WithNonce**(*key*, *hash_constructor=<built-in function openssl_sha512>*, *nonce=None*)
Bases: *hashcrypto.HashCrypt*

header()

classmethod make_nonce(*hash_constructor=<built-in function openssl_sha512>*)

hashcrypto.**decrypt_file**(*infile*, *outfile*, *key*)

hashcrypto.**pack_plus**(*b*)

hashcrypto.**read_file**(*infile*, *block_size*)

hashcrypto.**read_plus**(*f*)

hashcrypto.**unpack_plus**(*b*)

CHAPTER 2

Indices and tables

- genindex
- modindex
- search

Python Module Index

h

Index