
HashCrypto Documentation

Release 0.4

Jan Brohl

Mar 19, 2017

Contents

1	hashcrypto package	3
1.1	Submodules	3
1.2	hashcrypto.bytesop_fallback module	3
1.3	Module contents	3
2	Indices and tables	5
	Python Module Index	7

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

Contents:

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`

h

`hashcrypto`, [3](#)

`hashcrypto.bytesop_fallback`, [3](#)

B

block() (hashcrypto.HashCrypt method), 4

C

CFB (class in hashcrypto), 3

CTR (class in hashcrypto), 3

D

decrypt() (hashcrypto.CFB method), 3

decrypt() (hashcrypto.CTR method), 3

decrypt() (hashcrypto.OFB method), 4

decrypt_block() (hashcrypto.CFB method), 3

decrypt_block() (hashcrypto.CTR method), 3

decrypt_file() (in module hashcrypto), 4

decrypt_stream() (hashcrypto.HashCrypt method), 4

E

encrypt() (hashcrypto.CFB method), 3

encrypt() (hashcrypto.CTR method), 3

encrypt() (hashcrypto.OFB method), 4

encrypt_block() (hashcrypto.CTR method), 3

encrypt_file() (hashcrypto.HashCrypt method), 4

encrypt_stream() (hashcrypto.HashCrypt method), 4

H

hash_name() (hashcrypto.HashCrypt method), 4

HashCrypt (class in hashcrypto), 3

hashcrypto (module), 3

hashcrypto.bytesop_fallback (module), 3

header() (hashcrypto.HashCrypt method), 4

header() (hashcrypto.WithIV method), 4

header() (hashcrypto.WithNonce method), 4

I

IVError, 4

K

keystream() (hashcrypto.CTR method), 3

keystream() (hashcrypto.OFB method), 4

M

make_iv() (hashcrypto.WithIV class method), 4

make_nonce() (hashcrypto.WithNonce class method), 4

O

OFB (class in hashcrypto), 4

op_xor() (in module hashcrypto.bytesop_fallback), 3

P

pack_plus() (in module hashcrypto), 4

R

read_file() (in module hashcrypto), 4

read_plus() (in module hashcrypto), 4

S

suggest_iv_size() (hashcrypto.WithIV class method), 4

suggest_key_size() (hashcrypto.HashCrypt class method), 4

suggest_nonce_size() (hashcrypto.CTR class method), 3

U

unpack_plus() (in module hashcrypto), 4

W

WithIV (class in hashcrypto), 4

WithNonce (class in hashcrypto), 4