

Ordo

0.3.4

Generated by Doxygen 1.8.6

Sun Jul 27 2014 23:46:11



# Contents

- 1 Main Page** **1**
  
- 2 Data Structure Index** **5**
  - 2.1 Data Structures . . . . . 5
  
- 3 File Index** **7**
  - 3.1 File List . . . . . 7
  
- 4 Data Structure Documentation** **9**
  - 4.1 AES\_PARAMS Struct Reference . . . . . 9
    - 4.1.1 Detailed Description . . . . . 9
    - 4.1.2 Field Documentation . . . . . 9
      - 4.1.2.1 rounds . . . . . 9
  - 4.2 BLOCK\_MODE\_PARAMS Union Reference . . . . . 9
    - 4.2.1 Detailed Description . . . . . 10
  - 4.3 BLOCK\_PARAMS Union Reference . . . . . 10
    - 4.3.1 Detailed Description . . . . . 10
  - 4.4 CBC\_PARAMS Struct Reference . . . . . 11
    - 4.4.1 Detailed Description . . . . . 11
    - 4.4.2 Field Documentation . . . . . 11
      - 4.4.2.1 padding . . . . . 11
  - 4.5 ECB\_PARAMS Struct Reference . . . . . 11
    - 4.5.1 Detailed Description . . . . . 11
    - 4.5.2 Field Documentation . . . . . 11
      - 4.5.2.1 padding . . . . . 11
  - 4.6 HASH\_PARAMS Union Reference . . . . . 12
    - 4.6.1 Detailed Description . . . . . 12
  - 4.7 ORDO\_VERSION Struct Reference . . . . . 12
    - 4.7.1 Detailed Description . . . . . 13
    - 4.7.2 Field Documentation . . . . . 13
      - 4.7.2.1 id . . . . . 13
      - 4.7.2.2 version . . . . . 13

4.7.2.3	system	13
4.7.2.4	arch	13
4.7.2.5	build	13
4.7.2.6	features	13
4.7.2.7	feature_list	13
4.8	RC4_PARAMS Struct Reference	13
4.8.1	Detailed Description	14
4.8.2	Field Documentation	14
4.8.2.1	drop	14
4.9	SKEIN256_PARAMS Struct Reference	14
4.9.1	Detailed Description	14
4.9.2	Field Documentation	14
4.9.2.1	schema	14
4.9.2.2	version	15
4.9.2.3	reserved	15
4.9.2.4	out_len	15
4.9.2.5	unused	15
4.10	STREAM_PARAMS Union Reference	15
4.10.1	Detailed Description	15
4.11	THREEFISH256_PARAMS Struct Reference	16
4.11.1	Detailed Description	16
4.11.2	Field Documentation	16
4.11.2.1	tweak	16
<b>5</b>	<b>File Documentation</b>	<b>17</b>
5.1	include/ordo.h File Reference	17
5.1.1	Detailed Description	18
5.1.2	Function Documentation	18
5.1.2.1	ordo_enc_block	18
5.1.2.2	ordo_enc_stream	18
5.1.2.3	ordo_digest	19
5.1.2.4	ordo_hmac	19
5.2	include/ordo/auth/hmac.h File Reference	20
5.2.1	Detailed Description	21
5.2.2	Function Documentation	21
5.2.2.1	hmac_init	21
5.2.2.2	hmac_update	22
5.2.2.3	hmac_final	23
5.2.2.4	hmac_bsize	23
5.3	include/ordo/common/error.h File Reference	24

---

5.3.1	Detailed Description	24
5.3.2	Enumeration Type Documentation	24
5.3.2.1	ORDO_ERROR	24
5.3.3	Function Documentation	25
5.3.3.1	ordo_error_msg	25
5.4	include/ordo/common/identification.h File Reference	26
5.4.1	Detailed Description	26
5.4.2	Macro Definition Documentation	26
5.4.2.1	PRIM_UNKNOWN	26
5.4.3	Enumeration Type Documentation	26
5.4.3.1	PRIM_TYPE	26
5.4.4	Function Documentation	27
5.4.4.1	prim_avail	27
5.4.4.2	prim_name	27
5.4.4.3	prim_type	27
5.4.4.4	prim_from_name	27
5.4.4.5	prims_by_type	28
5.4.4.6	prim_default	28
5.5	include/ordo/common/interface.h File Reference	28
5.5.1	Detailed Description	29
5.6	include/ordo/common/query.h File Reference	29
5.6.1	Detailed Description	30
5.6.2	Enumeration Type Documentation	30
5.6.2.1	ORDO_QUERY	30
5.7	include/ordo/common/version.h File Reference	31
5.7.1	Detailed Description	31
5.7.2	Function Documentation	31
5.7.2.1	ordo_version	31
5.8	include/ordo/digest/digest.h File Reference	32
5.8.1	Detailed Description	33
5.8.2	Macro Definition Documentation	33
5.8.2.1	ordo_digest_init	33
5.8.2.2	ordo_digest_update	33
5.8.2.3	ordo_digest_final	34
5.8.2.4	ordo_digest_bsize	34
5.8.3	Function Documentation	34
5.8.3.1	digest_length	34
5.9	include/ordo/enc/enc_block.h File Reference	35
5.9.1	Detailed Description	36
5.9.2	Function Documentation	36

---

5.9.2.1	<code>enc_block_init</code>	36
5.9.2.2	<code>enc_block_update</code>	37
5.9.2.3	<code>enc_block_final</code>	37
5.9.2.4	<code>enc_block_key_len</code>	38
5.9.2.5	<code>enc_block_iv_len</code>	38
5.9.2.6	<code>enc_block_bsize</code>	38
5.10	<code>include/ordo/enc/enc_stream.h</code> File Reference	38
5.10.1	Detailed Description	40
5.10.2	Macro Definition Documentation	40
5.10.2.1	<code>ordo_enc_stream_init</code>	40
5.10.2.2	<code>ordo_enc_stream_update</code>	40
5.10.2.3	<code>ordo_enc_stream_final</code>	40
5.10.2.4	<code>ordo_enc_stream_bsize</code>	40
5.10.3	Function Documentation	41
5.10.3.1	<code>enc_stream_key_len</code>	41
5.11	<code>include/ordo/internal/alg.h</code> File Reference	41
5.11.1	Detailed Description	41
5.11.2	Macro Definition Documentation	41
5.11.2.1	<code>bits</code>	41
5.11.2.2	<code>bytes</code>	42
5.11.2.3	<code>offset</code>	42
5.11.3	Function Documentation	42
5.11.3.1	<code>pad_check</code>	42
5.11.3.2	<code>xor_buffer</code>	42
5.11.3.3	<code>inc_buffer</code>	43
5.12	<code>include/ordo/internal/implementation.h</code> File Reference	43
5.12.1	Detailed Description	43
5.13	<code>include/ordo/internal/sys.h</code> File Reference	43
5.13.1	Detailed Description	43
5.14	<code>include/ordo/kdf/hkdf.h</code> File Reference	44
5.14.1	Detailed Description	44
5.14.2	Function Documentation	44
5.14.2.1	<code>kdf_hkdf</code>	44
5.15	<code>include/ordo/kdf/pbkdf2.h</code> File Reference	45
5.15.1	Detailed Description	45
5.15.2	Function Documentation	46
5.15.2.1	<code>kdf_pbkdf2</code>	46
5.16	<code>include/ordo/misc/curve25519.h</code> File Reference	47
5.16.1	Detailed Description	47
5.16.2	Function Documentation	47

---

5.16.2.1	curve25519_gen	47
5.16.2.2	curve25519_pub	48
5.16.2.3	curve25519_ecdh	49
5.17	include/ordo/misc/endianness.h File Reference	49
5.17.1	Detailed Description	49
5.18	include/ordo/misc/os_random.h File Reference	49
5.18.1	Detailed Description	50
5.18.2	Function Documentation	50
5.18.2.1	os_random	50
5.18.2.2	os_secure_random	50
5.19	include/ordo/misc/utils.h File Reference	51
5.19.1	Detailed Description	51
5.19.2	Function Documentation	51
5.19.2.1	ctcmp	51
5.20	include/ordo/primitives/block_ciphers.h File Reference	52
5.20.1	Detailed Description	53
5.20.2	Function Documentation	53
5.20.2.1	block_init	53
5.20.2.2	block_forward	53
5.20.2.3	block_inverse	53
5.20.2.4	block_final	54
5.20.2.5	block_query	55
5.20.2.6	block_bsize	55
5.21	include/ordo/primitives/block_ciphers/aes.h File Reference	56
5.21.1	Detailed Description	56
5.21.2	Function Documentation	56
5.21.2.1	aes_init	56
5.21.2.2	aes_forward	57
5.21.2.3	aes_inverse	57
5.21.2.4	aes_final	57
5.21.2.5	aes_query	57
5.21.2.6	aes_bsize	57
5.22	include/ordo/primitives/block_ciphers/block_params.h File Reference	57
5.22.1	Detailed Description	58
5.23	include/ordo/primitives/block_ciphers/nullcipher.h File Reference	58
5.23.1	Detailed Description	59
5.23.2	Function Documentation	59
5.23.2.1	nullcipher_init	59
5.23.2.2	nullcipher_forward	60
5.23.2.3	nullcipher_inverse	60

5.23.2.4	nullcipher_final	60
5.23.2.5	nullcipher_query	60
5.23.2.6	nullcipher_bsize	60
5.24	include/ordo/primitives/block_ciphers/threefish256.h File Reference	60
5.24.1	Detailed Description	61
5.24.2	Function Documentation	61
5.24.2.1	threefish256_init	61
5.24.2.2	threefish256_forward	62
5.24.2.3	threefish256_inverse	62
5.24.2.4	threefish256_final	62
5.24.2.5	threefish256_query	62
5.24.2.6	threefish256_bsize	62
5.25	include/ordo/primitives/block_modes.h File Reference	62
5.25.1	Detailed Description	63
5.25.2	Function Documentation	64
5.25.2.1	block_mode_init	64
5.25.2.2	block_mode_update	64
5.25.2.3	block_mode_final	64
5.25.2.4	block_mode_query	65
5.25.2.5	block_mode_bsize	65
5.26	include/ordo/primitives/block_modes/cbc.h File Reference	66
5.26.1	Detailed Description	66
5.26.2	Function Documentation	67
5.26.2.1	cbc_init	67
5.26.2.2	cbc_update	67
5.26.2.3	cbc_final	67
5.26.2.4	cbc_query	67
5.26.2.5	cbc_bsize	67
5.27	include/ordo/primitives/block_modes/cfb.h File Reference	68
5.27.1	Detailed Description	68
5.27.2	Function Documentation	69
5.27.2.1	cfb_init	69
5.27.2.2	cfb_update	69
5.27.2.3	cfb_final	69
5.27.2.4	cfb_query	69
5.27.2.5	cfb_bsize	69
5.28	include/ordo/primitives/block_modes/ctr.h File Reference	69
5.28.1	Detailed Description	70
5.28.2	Function Documentation	70
5.28.2.1	ctr_init	71



5.28.2.2	ctr_update	71
5.28.2.3	ctr_final	71
5.28.2.4	ctr_query	71
5.28.2.5	ctr_bsize	71
5.29	include/ordo/primitives/block_modes/ecb.h File Reference	71
5.29.1	Detailed Description	72
5.29.2	Function Documentation	72
5.29.2.1	ecb_init	73
5.29.2.2	ecb_update	73
5.29.2.3	ecb_final	73
5.29.2.4	ecb_query	73
5.29.2.5	ecb_bsize	73
5.30	include/ordo/primitives/block_modes/mode_params.h File Reference	73
5.30.1	Detailed Description	74
5.31	include/ordo/primitives/block_modes/ofb.h File Reference	74
5.31.1	Detailed Description	75
5.31.2	Function Documentation	75
5.31.2.1	ofb_init	75
5.31.2.2	ofb_update	75
5.31.2.3	ofb_final	75
5.31.2.4	ofb_query	75
5.31.2.5	ofb_bsize	75
5.32	include/ordo/primitives/hash_functions.h File Reference	76
5.32.1	Detailed Description	76
5.32.2	Function Documentation	77
5.32.2.1	hash_init	77
5.32.2.2	hash_update	77
5.32.2.3	hash_final	77
5.32.2.4	hash_query	77
5.32.2.5	hash_bsize	78
5.33	include/ordo/primitives/hash_functions/hash_params.h File Reference	78
5.33.1	Detailed Description	79
5.34	include/ordo/primitives/hash_functions/md5.h File Reference	79
5.34.1	Detailed Description	79
5.34.2	Function Documentation	80
5.34.2.1	md5_init	80
5.34.2.2	md5_update	80
5.34.2.3	md5_final	80
5.34.2.4	md5_query	80
5.34.2.5	md5_bsize	80

5.35	<a href="#">include/ordo/primitives/hash_functions/sha1.h File Reference</a>	80
5.35.1	<a href="#">Detailed Description</a>	81
5.35.2	<a href="#">Function Documentation</a>	81
5.35.2.1	<a href="#">sha1_init</a>	81
5.35.2.2	<a href="#">sha1_update</a>	81
5.35.2.3	<a href="#">sha1_final</a>	82
5.35.2.4	<a href="#">sha1_query</a>	82
5.35.2.5	<a href="#">sha1_bsize</a>	82
5.36	<a href="#">include/ordo/primitives/hash_functions/sha256.h File Reference</a>	82
5.36.1	<a href="#">Detailed Description</a>	83
5.36.2	<a href="#">Function Documentation</a>	83
5.36.2.1	<a href="#">sha256_init</a>	83
5.36.2.2	<a href="#">sha256_update</a>	83
5.36.2.3	<a href="#">sha256_final</a>	83
5.36.2.4	<a href="#">sha256_query</a>	83
5.36.2.5	<a href="#">sha256_bsize</a>	83
5.37	<a href="#">include/ordo/primitives/hash_functions/skein256.h File Reference</a>	84
5.37.1	<a href="#">Detailed Description</a>	84
5.37.2	<a href="#">Function Documentation</a>	84
5.37.2.1	<a href="#">skein256_init</a>	84
5.37.2.2	<a href="#">skein256_update</a>	85
5.37.2.3	<a href="#">skein256_final</a>	85
5.37.2.4	<a href="#">skein256_query</a>	85
5.37.2.5	<a href="#">skein256_bsize</a>	85
5.38	<a href="#">include/ordo/primitives/stream_ciphers.h File Reference</a>	86
5.38.1	<a href="#">Detailed Description</a>	87
5.38.2	<a href="#">Function Documentation</a>	87
5.38.2.1	<a href="#">stream_init</a>	87
5.38.2.2	<a href="#">stream_update</a>	87
5.38.2.3	<a href="#">stream_final</a>	87
5.38.2.4	<a href="#">stream_query</a>	88
5.38.2.5	<a href="#">stream_bsize</a>	88
5.39	<a href="#">include/ordo/primitives/stream_ciphers/rc4.h File Reference</a>	89
5.39.1	<a href="#">Detailed Description</a>	89
5.39.2	<a href="#">Function Documentation</a>	89
5.39.2.1	<a href="#">rc4_init</a>	90
5.39.2.2	<a href="#">rc4_update</a>	90
5.39.2.3	<a href="#">rc4_final</a>	90
5.39.2.4	<a href="#">rc4_query</a>	90
5.39.2.5	<a href="#">rc4_bsize</a>	90

---

5.40 <a href="#">include/ordo/primitives/stream_ciphers/stream_params.h File Reference</a> . . . . .	90
5.40.1 Detailed Description . . . . .	91
<b>Index</b>	<b>92</b>



# Chapter 1

## Main Page

### Symmetric Cryptography Library

This is the github repository for Ordo, a minimalist cryptography library with an emphasis on symmetric cryptography, which strives to meet high performance, portability, and security standards, while remaining modular in design to facilitate adding new features and maintaining existing ones. The library is written in standard C with system-specific features, but some sections are assembly-optimized for efficiency. Note that while the library is technically usable at this point, it is still very much a work in progress and mustn't be deployed in security-sensitive applications.

### Status

! [Build Status] (<https://travis-ci.org/TomCrypto/Ordo.png?branch=master>)

What's new in 0.3.4:

- added HKDF, SHA-1
- all hash functions now have a fixed, immutable output length, which simplifies code and reduces the likelihood of overflow or underflow (in exchange, HKDF can be used to stretch insufficiently large hash outputs in a safe and generic fashion - DRBG's are probably next on the list)
- improved some of the hash function code, particularly the padding implementation
- restored HMAC to apply hash parameters to the inner hash (result of the above)
- added a `prim_default()` function to get default primitives
- added some unit tests for a few modules (work in progress)
- simplified the library implementation a bit
- fixed a few bugs

TODO:

- work on tests (!)
- go over build system

### Feature Map

This table doesn't include every single feature but gives a high level overview of what is available so far:

Block Ciphers	Stream Ciphers	Hash Functions	Modes	Authenticat-ion	Key Derivation	Misc
AES	RC4	MD5	ECB	HMAC	PBKDF2	CSPRNG
Threefish-256	-	SHA-1	CBC	-	HKDF	Curve25519
-	-	SHA-256	OFB	-	-	-
-	-	Skein-256	CFB	-	-	-
-	-	-	CTR	-	-	-

## Documentation

Ordo is documented for Doxygen, and you can automatically generate all documentation by using the `doc` build target, if deemed available on your system (you will need `doxygen`, and `pdflatex` with a working TeX environment for the LaTeX output). The HTML documentation will be generated in `doc/html`, and the LaTeX documentation will be generated in `doc/latex`, which you can then typeset using the generated makefile.

You can also access a recent version of the documentation online through the [project page](#).

## How To Build

We support recent versions of MSVC, GCC, ICC (Linux only), MinGW, and Clang. Other compilers are not officially supported. The build system used is CMake, which has a few configuration options to tweak the library according to your needs. A `build` folder is provided for you to point CMake to. Python (2.7 or 3.3 or similar) is also required.

- `LTO`: use link-time optimization, this should be enabled for optimal performance.
- `ARCH`: the architecture to use, pick the one most appropriate for your hardware.
- `NATIVE`: tune the build for the current hardware (e.g. `-march` for GCC).
- `COMPAT`: remove some advanced compiler settings for older compiler versions (for GCC only, if this is enabled `LTO` and `NATIVE` have no effect)

Note the system is autodetected and automatically included in the build. Additional options, such as the use of special hardware instructions, may become available once an architecture is selected, if they are supported. Link-time optimization may not be available on older compilers (it will let you know). For the Intel compiler (ICC) with native optimization, architecture autodetection is not available - pass the appropriate architecture in `ICC_TARGET` (e.g. `-DICC_TARGET=SSE4.2`).

If you are not using the `cmake-gui` utility, the command-line options to configure the library are:

```
cd build && cmake .. [-DARCH=arch] [[-DFEATURE=on] ...] [-DLTO=off] [-DNATIVE=off] [-DCOMPAT=on]
```

For instance, a typical configuration for `x86_64` machines with the AES-NI instructions could be:

```
cd build && cmake .. -DARCH=amd64 -DAES_NI=on
```

The test driver and sample programs are located in the `extra` folder.

## Assembly Support

We use the `NASM` assembler for our assembly files. For Linux and other Unix-based operating systems this should work out of the box after installing the assembler. For MSVC on Windows using the Visual Studio generators, custom build rules have been set up to autodetect `NASM` and get it to automatically compile assembly files, but they have not been tested (and may not necessarily work) for all versions of Visual Studio.

### Static Linking

If you wish to link statically to the library, please define the `ORDO_STATIC_LIB` preprocessor token in your project so that the Ordo headers can configure themselves accordingly (otherwise, they will assume you are linking to a shared library, which may raise some unwelcome compiler warnings as well as forbidding access to the internal headers).

### Compatibility

The library will run everywhere a near-C89 compiler (i.e. with `stdint.h` and `long long` support) is available, however system-dependent modules will not be available without an implementation for these platforms. For better performance, specialized algorithm implementations may be available for your system and processor architecture.

### Conclusion

Of course, do not use Ordo for anything other than testing or contributing for now! It can only be used once it has been completed and extensively checked (and even then, there may still be flaws and bugs, as in any other software).





# Chapter 2

## Data Structure Index

### 2.1 Data Structures

Here are the data structures with brief descriptions:

- [AES\\_PARAMS](#)
  - AES block cipher parameters . . . . . 9
- [BLOCK\\_MODE\\_PARAMS](#)
  - Polymorphic block mode parameter union . . . . . 9
- [BLOCK\\_PARAMS](#)
  - Polymorphic block cipher parameter union . . . . . 10
- [CBC\\_PARAMS](#)
  - CBC parameters . . . . . 11
- [ECB\\_PARAMS](#)
  - ECB parameters . . . . . 11
- [HASH\\_PARAMS](#)
  - Polymorphic hash function parameter union . . . . . 12
- [ORDO\\_VERSION](#)
  - Library version information . . . . . 12
- [RC4\\_PARAMS](#)
  - RC4 stream cipher parameters . . . . . 13
- [SKEIN256\\_PARAMS](#)
  - Skein-256 hash function parameters . . . . . 14
- [STREAM\\_PARAMS](#)
  - Polymorphic stream cipher parameter union . . . . . 15
- [THREEFISH256\\_PARAMS](#)
  - Threefish-256 block cipher parameters . . . . . 16



# Chapter 3

## File Index

### 3.1 File List

Here is a list of all documented files with brief descriptions:

include/ordo.h	
Wrapper	17
include/ordo/auth/hmac.h	
Module	20
include/ordo/common/error.h	
Utility	24
include/ordo/common/identification.h	
Utility	26
include/ordo/common/interface.h	
API	28
include/ordo/common/query.h	
Utility	29
include/ordo/common/version.h	
Utility	31
include/ordo/digest/digest.h	
Module	32
include/ordo/enc/enc_block.h	
Module	35
include/ordo/enc/enc_stream.h	
Module	38
include/ordo/internal/alg.h	
<b>Internal</b> , Utility	41
include/ordo/internal/implementation.h	
<b>Internal</b> , API	43
include/ordo/internal/sys.h	
<b>Internal</b> , Utility	43
include/ordo/kdf/hkdf.h	
Module	44
include/ordo/kdf/pbkdf2.h	
Module	45
include/ordo/misc/curve25519.h	
Misc. asymmetric module (temp)	47
include/ordo/misc/endianness.h	
Utility	49
include/ordo/misc/os_random.h	
Module	49
include/ordo/misc/utls.h	
Utility	51

include/ordo/primitives/block_ciphers.h	
Abstraction Layer	52
include/ordo/primitives/block_modes.h	
Abstraction Layer	62
include/ordo/primitives/hash_functions.h	
Abstraction Layer	76
include/ordo/primitives/stream_ciphers.h	
Abstraction Layer	86
include/ordo/primitives/block_ciphers/aes.h	
Primitive	56
include/ordo/primitives/block_ciphers/block_params.h	
Primitive Parameters	57
include/ordo/primitives/block_ciphers/nullcipher.h	
Primitive	58
include/ordo/primitives/block_ciphers/threefish256.h	
Primitive	60
include/ordo/primitives/block_modes/cbc.h	
Primitive	66
include/ordo/primitives/block_modes/cfb.h	
Primitive	68
include/ordo/primitives/block_modes/ctr.h	
Primitive	69
include/ordo/primitives/block_modes/ecb.h	
Primitive	71
include/ordo/primitives/block_modes/mode_params.h	
Primitive Parameters	73
include/ordo/primitives/block_modes/ofb.h	
Primitive	74
include/ordo/primitives/hash_functions/hash_params.h	
Primitive Parameters	78
include/ordo/primitives/hash_functions/md5.h	
Primitive	79
include/ordo/primitives/hash_functions/sha1.h	
Primitive	80
include/ordo/primitives/hash_functions/sha256.h	
Primitive	82
include/ordo/primitives/hash_functions/skein256.h	
Primitive	84
include/ordo/primitives/stream_ciphers/rc4.h	
Primitive	89
include/ordo/primitives/stream_ciphers/stream_params.h	
Primitive Parameters	90

## Chapter 4

# Data Structure Documentation

### 4.1 AES\_PARAMS Struct Reference

AES block cipher parameters.

```
#include <block_params.h>
```

#### Data Fields

- unsigned int [rounds](#)

#### 4.1.1 Detailed Description

AES block cipher parameters.

#### 4.1.2 Field Documentation

##### 4.1.2.1 unsigned int rounds

The number of rounds to use.

#### Warning

The defaults are 10 for a 128-bit key, 12 for a 192-bit key, 14 for a 256-bit key, and are standardized. It is **strongly** discouraged to lower the number of rounds below the defaults.

The documentation for this struct was generated from the following file:

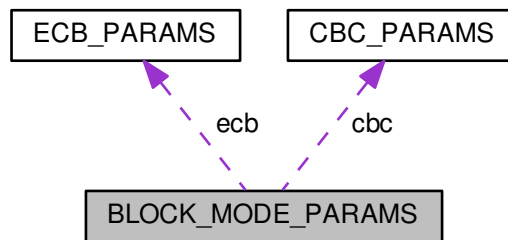
- include/ordo/primitives/block\_ciphers/[block\\_params.h](#)

### 4.2 BLOCK\_MODE\_PARAMS Union Reference

Polymorphic block mode parameter union.

```
#include <mode_params.h>
```

Collaboration diagram for BLOCK\_MODE\_PARAMS:



#### 4.2.1 Detailed Description

Polymorphic block mode parameter union.

The documentation for this union was generated from the following file:

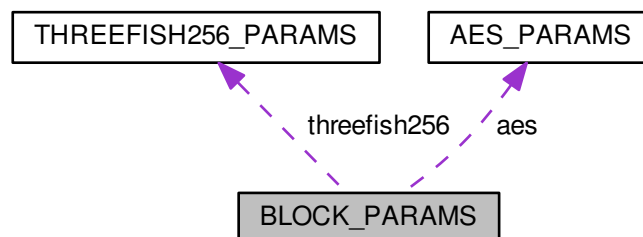
- [include/ordo/primitives/block\\_modes/mode\\_params.h](#)

### 4.3 BLOCK\_PARAMS Union Reference

Polymorphic block cipher parameter union.

```
#include <block_params.h>
```

Collaboration diagram for BLOCK\_PARAMS:



#### 4.3.1 Detailed Description

Polymorphic block cipher parameter union.

The documentation for this union was generated from the following file:

- [include/ordo/primitives/block\\_ciphers/block\\_params.h](#)

## 4.4 CBC\_PARAMS Struct Reference

CBC parameters.

```
#include <mode_params.h>
```

### Data Fields

- int [padding](#)

#### 4.4.1 Detailed Description

CBC parameters.

#### 4.4.2 Field Documentation

##### 4.4.2.1 int padding

Whether padding should be used.

#### Remarks

- Set to 0 to disable padding, and 1 to enable it.  
Padding is enabled by default if parameters are not used.

The documentation for this struct was generated from the following file:

- [include/ordo/primitives/block\\_modes/mode\\_params.h](#)

## 4.5 ECB\_PARAMS Struct Reference

ECB parameters.

```
#include <mode_params.h>
```

### Data Fields

- int [padding](#)

#### 4.5.1 Detailed Description

ECB parameters.

#### 4.5.2 Field Documentation

##### 4.5.2.1 int padding

Whether padding should be used.

**Remarks**

Set to 0 to disable padding, and 1 to enable it.  
 Padding is enabled by default if parameters are not used.

The documentation for this struct was generated from the following file:

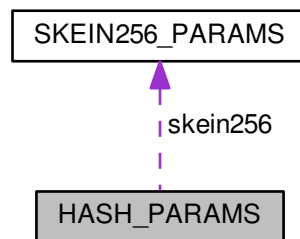
- [include/ordo/primitives/block\\_modes/mode\\_params.h](#)

**4.6 HASH\_PARAMS Union Reference**

Polymorphic hash function parameter union.

```
#include <hash_params.h>
```

Collaboration diagram for HASH\_PARAMS:

**4.6.1 Detailed Description**

Polymorphic hash function parameter union.

The documentation for this union was generated from the following file:

- [include/ordo/primitives/hash\\_functions/hash\\_params.h](#)

**4.7 ORDO\_VERSION Struct Reference**

Library version information.

```
#include <version.h>
```

**Data Fields**

- unsigned int [id](#)
- const char \* [version](#)
- const char \* [system](#)
- const char \* [arch](#)
- const char \* [build](#)
- const char \*const \* [features](#)
- const char \* [feature\\_list](#)



### 4.7.1 Detailed Description

Library version information.

Contains version information for the library.

### 4.7.2 Field Documentation

#### 4.7.2.1 unsigned int id

The version as an integer of the form XXYYZZ, e.g. 30242 == 3.2.42.

#### 4.7.2.2 const char\* version

The version e.g. "2.7.0".

#### 4.7.2.3 const char\* system

The target system e.g. "linux".

#### 4.7.2.4 const char\* arch

The target architecture e.g. "amd64".

#### 4.7.2.5 const char\* build

A string which contains version, system and architecture.

#### 4.7.2.6 const char\* const\* features

A null-terminated list of targeted features.

#### 4.7.2.7 const char\* feature\_list

The list of features, as a space-separated string.

The documentation for this struct was generated from the following file:

- [include/ordo/common/version.h](#)

## 4.8 RC4\_PARAMS Struct Reference

RC4 stream cipher parameters.

```
#include <stream_params.h>
```

### Data Fields

- unsigned int [drop](#)

### 4.8.1 Detailed Description

RC4 stream cipher parameters.

### 4.8.2 Field Documentation

#### 4.8.2.1 unsigned int drop

The number of keystream bytes to drop prior to encryption.

#### Remarks

Setting this implements the given RC4-drop variant.

If this [RC4\\_PARAMS](#) structure is **not** passed to the RC4 stream cipher primitive, the default drop amount is 2048.

The documentation for this struct was generated from the following file:

- `include/ordo/primitives/stream_ciphers/stream_params.h`

## 4.9 SKEIN256\_PARAMS Struct Reference

Skein-256 hash function parameters.

```
#include <hash_params.h>
```

### Data Fields

- `uint8_t schema` [4]
- `uint8_t version` [2]
- `uint8_t reserved` [2]
- `uint64_t out_len`
- `uint8_t unused` [16]

### 4.9.1 Detailed Description

Skein-256 hash function parameters.

#### Remarks

Refer to the Skein specification to know more about what each of these parameter fields stand for.

#### Warning

This structure is **packed**, to improve performance while hashing the configuration block, be careful if taking pointers to members of the structure as correct alignment is NOT guaranteed.

### 4.9.2 Field Documentation

#### 4.9.2.1 uint8\_t schema[4]

The schema identifier, on four bytes.

## 4.9.2.2 uint8\_t version[2]

The version number, on two bytes.

## 4.9.2.3 uint8\_t reserved[2]

Reserved, should be left zero according to the Skein specification.

## 4.9.2.4 uint64\_t out\_len

Hash function output length, in **bits**.

## Warning

This parameter affects the hash function's digest length.  
Must be 256 or `skein256_init()` will return `ORDO_ARG`.

## 4.9.2.5 uint8\_t unused[16]

Unused, should be left zero according to the Skein specification.

The documentation for this struct was generated from the following file:

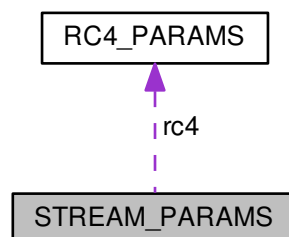
- [include/ordo/primitives/hash\\_functions/hash\\_params.h](#)

## 4.10 STREAM\_PARAMS Union Reference

Polymorphic stream cipher parameter union.

```
#include <stream_params.h>
```

Collaboration diagram for STREAM\_PARAMS:



### 4.10.1 Detailed Description

Polymorphic stream cipher parameter union.

The documentation for this union was generated from the following file:

- [include/ordo/primitives/stream\\_ciphers/stream\\_params.h](#)

## 4.11 THREEFISH256\_PARAMS Struct Reference

Threefish-256 block cipher parameters.

```
#include <block_params.h>
```

### Data Fields

- `uint64_t tweak` [2]

#### 4.11.1 Detailed Description

Threefish-256 block cipher parameters.

#### 4.11.2 Field Documentation

##### 4.11.2.1 `uint64_t tweak`[2]

The tweak word, on a pair of 64-bit words.

The documentation for this struct was generated from the following file:

- `include/ordo/primitives/block_ciphers/block_params.h`

# Chapter 5

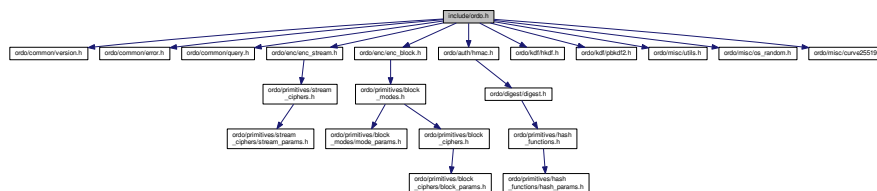
## File Documentation

### 5.1 include/ordo.h File Reference

Wrapper.

```
#include "ordo/common/version.h"  
#include "ordo/common/error.h"  
#include "ordo/common/query.h"  
#include "ordo/enc/enc_stream.h"  
#include "ordo/enc/enc_block.h"  
#include "ordo/auth/hmac.h"  
#include "ordo/kdf/hkdf.h"  
#include "ordo/kdf/pbkdf2.h"  
#include "ordo/misc/utils.h"  
#include "ordo/misc/os_random.h"  
#include "ordo/misc/curve25519.h"
```

Include dependency graph for ordo.h:



### Functions

- ORDO\_PUBLIC int `ordo_enc_block` (`prim_t` cipher, const void \*cipher\_params, `prim_t` mode, const void \*mode\_params, int direction, const void \*key, size\_t key\_len, const void \*iv, size\_t iv\_len, const void \*in, size\_t in\_len, void \*out, size\_t \*out\_len)
- ORDO\_PUBLIC int `ordo_enc_stream` (`prim_t` cipher, const void \*params, const void \*key, size\_t key\_len, void \*inout, size\_t len)
- ORDO\_PUBLIC int `ordo_digest` (`prim_t` hash, const void \*params, const void \*in, size\_t in\_len, void \*digest)
- ORDO\_PUBLIC int `ordo_hmac` (`prim_t` hash, const void \*params, const void \*key, size\_t key\_len, const void \*in, size\_t in\_len, void \*fingerprint)

### 5.1.1 Detailed Description

Wrapper. This is the highest-level API for Ordo, which forgoes the use of cryptographic contexts completely, resulting in more concise code at the cost of reduced flexibility - in other words, if you can afford to use them, you probably want to do so.

Usage snippet (compare to snippet in [digest.h](#)):

```
const char x[] = "Hello, world!";
unsigned char out[32]; // 256 bits
int err = ordo_digest(HASH_SHA256, 0, x, strlen(x), out);
if (err) printf("Error encountered!\n");
// out = 315f5bdb76d0...
```

Some specialized headers are *not* included by this header - these are the endianness header & all primitive headers (their parameters are included), if you need their functionality please include them explicitly.

### 5.1.2 Function Documentation

**5.1.2.1** `ORDO_PUBLIC int ordo_enc_block ( prim_t cipher, const void * cipher_params, prim_t mode, const void * mode_params, int direction, const void * key, size_t key_len, const void * iv, size_t iv_len, const void * in, size_t in_len, void * out, size_t * out_len )`

Encrypts or decrypts data using a block cipher with a mode of operation.

#### Parameters

in	<i>cipher</i>	The block cipher to use.
in	<i>cipher_params</i>	The block cipher parameters.
in	<i>mode</i>	The mode of operation to use.
in	<i>mode_params</i>	The mode of operation parameters.
in	<i>direction</i>	1 for encryption, 0 for decryption.
in	<i>key</i>	The cryptographic key to use.
in	<i>key_len</i>	The length in bytes of the key.
in	<i>iv</i>	The initialization vector.
in	<i>iv_len</i>	The length in bytes of the IV.
in	<i>in</i>	The input plaintext/ciphertext buffer.
in	<i>in_len</i>	The length of the input buffer.
out	<i>out</i>	The output ciphertext/plaintext buffer.
out	<i>out_len</i>	The length of the output buffer.

#### Returns

`ORDO_SUCCESS` on success, else an error code.

#### Remarks

The `out` buffer should be large enough to accommodate the entire ciphertext which may be larger than the plaintext if a mode where padding is enabled and used, see padding notes in [enc\\_block.h](#).

**5.1.2.2** `ORDO_PUBLIC int ordo_enc_stream ( prim_t cipher, const void * params, const void * key, size_t key_len, void * inout, size_t len )`

Encrypts or decrypts data using a stream cipher.

**Parameters**

<i>in</i>	<i>cipher</i>	The stream cipher to use.
<i>in</i>	<i>params</i>	The stream cipher parameters.
<i>in, out</i>	<i>inout</i>	The plaintext or ciphertext buffer.
<i>in</i>	<i>len</i>	The length, in bytes, of the buffer.
<i>in</i>	<i>key</i>	The cryptographic key to use.
<i>in</i>	<i>key_len</i>	The length, in bytes, of the key.

**Returns**

[ORDO\\_SUCCESS](#) on success, else an error code.

**Remarks**

Stream ciphers do not strictly speaking require an initialization vector - if such a feature is needed, it is recommended to use a key derivation function to derive an encryption key from a master key using a pseudorandomly generated nonce.

Encryption is always done in place. If you require out-of-place encryption, make a copy of the plaintext prior to encryption.

**Warning**

By design, encryption and decryption are equivalent for stream ciphers - an implication is that encrypting a message twice using the same key yields the original message.

### 5.1.2.3 `ORDO_PUBLIC int ordo_digest ( prim_t hash, const void * params, const void * in, size_t in_len, void * digest )`

Calculates the digest of a buffer using any hash function.

**Parameters**

<i>in</i>	<i>hash</i>	The hash function to use.
<i>in</i>	<i>params</i>	The hash function parameters.
<i>in</i>	<i>in</i>	The input buffer to hash.
<i>in</i>	<i>in_len</i>	The length in bytes of the buffer.
<i>out</i>	<i>digest</i>	The output buffer for the digest.

**Returns**

[ORDO\\_SUCCESS](#) on success, else an error code.

### 5.1.2.4 `ORDO_PUBLIC int ordo_hmac ( prim_t hash, const void * params, const void * key, size_t key_len, const void * in, size_t in_len, void * fingerprint )`

Calculates the HMAC fingerprint of a buffer using any hash function.

**Parameters**

<i>in</i>	<i>hash</i>	The hash function to use.
<i>in</i>	<i>params</i>	The hash function parameters.
<i>in</i>	<i>key</i>	The key to use for authentication.

in	<i>key_len</i>	The length in bytes of the key.
in	<i>in</i>	The input buffer to authenticate.
in	<i>in_len</i>	The length, in bytes, of the input buffer.
out	<i>fingerprint</i>	The output buffer for the fingerprint.

#### Returns

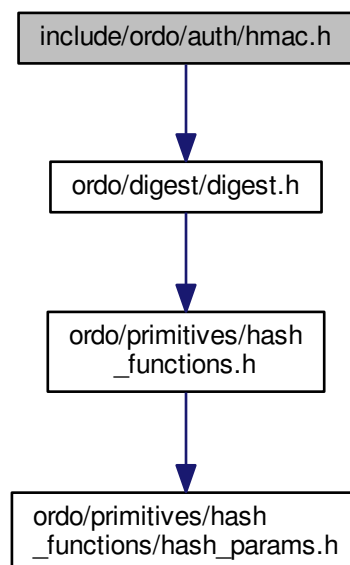
`ORDO_SUCCESS` on success, else an error code.

## 5.2 include/ordo/auth/hmac.h File Reference

Module.

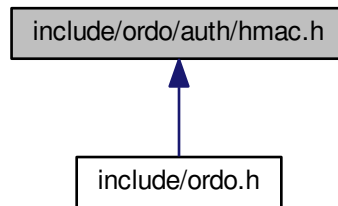
```
#include "ordo/digest/digest.h"
```

Include dependency graph for hmac.h:





This graph shows which files directly or indirectly include this file:



## Functions

- ORDO\_PUBLIC int [hmac\\_init](#) (struct HMAC\_CTX \*ctx, const void \*key, size\_t key\_len, [prim\\_t](#) hash, const void \*params)
- ORDO\_PUBLIC void [hmac\\_update](#) (struct HMAC\_CTX \*ctx, const void \*in, size\_t in\_len)
- ORDO\_PUBLIC int [hmac\\_final](#) (struct HMAC\_CTX \*ctx, void \*fingerprint)
- ORDO\_PUBLIC size\_t [hmac\\_bsize](#) (void)

### 5.2.1 Detailed Description

Module. Module for computing HMAC's (Hash-based Message Authentication Codes), which combine a hash function with a cryptographic key securely in order to provide both authentication and integrity, as per RFC 2104.

### 5.2.2 Function Documentation

5.2.2.1 ORDO\_PUBLIC int [hmac\\_init](#) ( struct HMAC\_CTX \* *ctx*, const void \* *key*, size\_t *key\_len*, [prim\\_t](#) *hash*, const void \* *params* )

Initializes an HMAC context, provided optional parameters.

#### Parameters

in	<i>ctx</i>	An allocated HMAC context.
in	<i>key</i>	The cryptographic key to use.
in	<i>key_len</i>	The size, in bytes, of the key.
out	<i>hash</i>	A hash function primitive to use.
out	<i>params</i>	Hash function specific parameters.

#### Returns

[ORDO\\_SUCCESS](#) on success, else an error code.

#### Remarks

The hash parameters apply to the inner hash operation only, which is the one used to hash the raw message and masked key.

5.2.2.2 ORDO\_PUBLIC void hmac\_update ( struct HMAC\_CTX \* *ctx*, const void \* *in*, size\_t *in\_len* )

Updates an HMAC context, feeding more data into it.

## Parameters

<code>in</code>	<code>ctx</code>	An initialized HMAC context.
<code>in</code>	<code>in</code>	The data to feed into the context.
<code>in</code>	<code>in_len</code>	The length, in bytes, of the data.

## Remarks

This function has the same properties, with respect to the input buffer, as the `digest_update()` function.

## 5.2.2.3 ORDO\_PUBLIC int hmac\_final ( struct HMAC\_CTX \* ctx, void \* fingerprint )

Finalizes a HMAC context, returning the final fingerprint.

## Parameters

<code>in</code>	<code>ctx</code>	An initialized HMAC context.
<code>out</code>	<code>fingerprint</code>	The output buffer for the fingerprint.

## Returns

`ORDO_SUCCESS` on success, else an error code.

## Remarks

The fingerprint length is equal to the underlying hash function's digest length, which can be queried via `hash-_digest_length()`.

## 5.2.2.4 ORDO\_PUBLIC size\_t hmac\_bsize ( void )

Gets the size in bytes of an `HMAC_CTX`.

## Returns

The size in bytes of the structure.

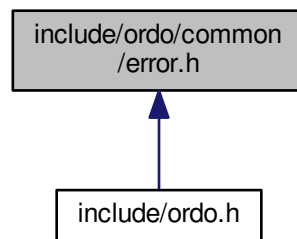
**Remarks**

Binary compatibility layer.

**5.3 include/ordo/common/error.h File Reference**

Utility.

This graph shows which files directly or indirectly include this file:

**Enumerations**

- enum `ORDO_ERROR` {  
`ORDO_SUCCESS`, `ORDO_FAIL`, `ORDO_LEFTOVER`, `ORDO_KEY_LEN`,  
`ORDO_PADDING`, `ORDO_ARG` }

**Functions**

- `ORDO_PUBLIC` const char \* `ordo_error_msg` (int code)

**5.3.1 Detailed Description**

Utility. This header exposes error codes emitted by the library. Code which uses the library should always use the explicit error codes to check for errors, with the sole exception of `ORDO_SUCCESS` which is guaranteed to be zero.

**5.3.2 Enumeration Type Documentation****5.3.2.1 enum ORDO\_ERROR**

Error codes used by the library.

**Enumerator**

***ORDO\_SUCCESS*** The function succeeded

**Remarks**

This is always defined as zero and is returned if a function encountered no error, unless specified otherwise.

***ORDO\_FAIL*** The function failed due to an external error.

**Remarks**

This often indicates failure of an external component, such as the pseudorandom number generator provided by the OS (see [os\\_random](#)). The library is not responsible for this error.

**ORDO\_LEFTOVER** User input was left over unprocessed.

**Remarks**

This applies to block cipher modes of operation for which padding has been disabled. If the input plaintext length is not a multiple of the cipher's block size, then the remaining incomplete block cannot be handled without padding, which is an error as it generally leads to inconsistent behavior on the part of the user.

**ORDO\_KEY\_LEN** The key length provided is invalid.

**Remarks**

This occurs if you provide a key of an invalid length, such as passing a 128-bit key into a cipher which expects a 192-bit key. Primitives either have a range of possible key lengths (often characterized by a minimum and maximum key length, but this varies among algorithms) or only one specific key length. If you need to accept arbitrary length keys, you should consider hashing your key in some fashion before using it for encryption, for instance using a KDF.

The [block\\_query\(\)](#) function can be used to select a good key length for a given block cipher via the [KEY\\_LEN\\_Q](#) query code. For stream ciphers, use [stream\\_query\(\)](#).

**ORDO\_PADDING** The padding was not recognized and decryption could not be completed.

**Remarks**

This applies to block cipher modes for which padding is enabled. If the last block containing padding information is malformed, the padding will generally be unreadable and the correct message length cannot be retrieved, making correct decryption impossible. Note this is not guaranteed to occur if the padding block is corrupted. In other words, if [ORDO\\_PADDING](#) is returned, the padding block is certainly corrupted, however it may still be even if the library returns success (the returned plaintext will then be incorrect). If you **must** ensure the plaintext is decrypted correctly - and you probably should - you will want to use a MAC (Message Authentication Code) along with encryption, or an authenticated block cipher mode of operation.

**ORDO\_ARG** An invalid argument was passed to a function.

**Remarks**

This is a generic error which is returned when the library finds an invalid parameter which would lead to inconsistent, undefined, or profoundly insecure behavior. Make sure your arguments are correct and do not contradict one another.

Keep in mind that the library cannot possibly catch all such errors, and you should still read the documentation if you are not sure what you are doing is valid.

### 5.3.3 Function Documentation

#### 5.3.3.1 **ORDO\_PUBLIC** `const char* ordo_error_msg ( int code )`

Generates a readable error message from an error code.

**Parameters**

<code>in</code>	<code>code</code>	The error code to interpret.
-----------------	-------------------	------------------------------

**Returns**

A null-terminated string containing the error description.

**Remarks**

This function is intended for debugging purposes.

## 5.4 include/ordo/common/identification.h File Reference

Utility.

### Macros

- #define [PRIM\\_UNKNOWN](#)

### Typedefs

- typedef int [prim\\_t](#)  
*Data type which holds a primitive identifier.*

### Enumerations

- enum [PRIM\\_TYPE](#)

### Functions

- ORDO\_PUBLIC int [prim\\_avail](#) ([prim\\_t](#) prim)
- ORDO\_PUBLIC const char \* [prim\\_name](#) ([prim\\_t](#) prim)
- ORDO\_PUBLIC enum [PRIM\\_TYPE](#) [prim\\_type](#) ([prim\\_t](#) prim)
- ORDO\_PUBLIC [prim\\_t](#) [prim\\_from\\_name](#) (const char \*name)
- ORDO\_PUBLIC const [prim\\_t](#) \* [prims\\_by\\_type](#) (enum [PRIM\\_TYPE](#) type)
- ORDO\_PUBLIC [prim\\_t](#) [prim\\_default](#) (enum [PRIM\\_TYPE](#) type)

#### 5.4.1 Detailed Description

Utility. This header contains definitions assigning an identifier to each primitive in the library - hash functions, block ciphers, modes of operation, and so on - which can then be used in higher level API's for abstraction purposes and more expressive code. This header also provides functionality relating to primitive management, e.g. which primitives are available, etc...

Note the zero ID will always stand for an error situation e.g. a primitive is not available. The zero ID is **never** a valid primitive identifier.

This also allows for a quick overview of what is implemented in Ordo.

#### 5.4.2 Macro Definition Documentation

##### 5.4.2.1 #define PRIM\_UNKNOWN

Value representing an unknown primitive, defined as zero.

##### Remarks

You can use this to check for errors or for comparisons.

#### 5.4.3 Enumeration Type Documentation

##### 5.4.3.1 enum PRIM\_TYPE

Enumerates the different types of primitives (values start at 1).

## 5.4.4 Function Documentation

### 5.4.4.1 ORDO\_PUBLIC int prim\_avail ( prim\_t prim )

Checks whether a primitive is available.

#### Parameters

<i>in</i>	<i>prim</i>	A primitive identifier.
-----------	-------------	-------------------------

#### Returns

0 if the primitive is not available, 1 otherwise.

### 5.4.4.2 ORDO\_PUBLIC const char\* prim\_name ( prim\_t prim )

Returns the name of a primitive.

#### Parameters

<i>in</i>	<i>prim</i>	A primitive identifier.
-----------	-------------	-------------------------

#### Returns

The name of the primitive as a human-readable string, or zero, if the primitive does not exist (i.e. invalid identifier passed).

#### Remarks

Do not rely on this being constant, use it for display only.

#### Warning

Will **not** work if the primitive is not available.

### 5.4.4.3 ORDO\_PUBLIC enum PRIM\_TYPE prim\_type ( prim\_t prim )

Returns the type of a given primitive.

#### Parameters

<i>in</i>	<i>prim</i>	A primitive identifier.
-----------	-------------	-------------------------

#### Returns

The type of the primitive, or zero on error.

#### Warning

Will **not** work if the primitive is not available.

### 5.4.4.4 ORDO\_PUBLIC prim\_t prim\_from\_name ( const char \* name )

Returns a primitive identifier from a name.

**Parameters**

<i>in</i>	<i>name</i>	A primitive name.
-----------	-------------	-------------------

**Returns**

The corresponding primitive identifier, or zero on error.

**Warning**

Will **not** work if the primitive is not available.

**5.4.4.5 ORDO\_PUBLIC const prim\_t\* prims\_by\_type ( enum PRIM\_TYPE type )**

Returns a list of available primitives of a given type.

**Parameters**

<i>in</i>	<i>type</i>	A primitive type.
-----------	-------------	-------------------

**Returns**

A zero-terminated list of such primitives.

**5.4.4.6 ORDO\_PUBLIC prim\_t prim\_default ( enum PRIM\_TYPE type )**

Returns the default available primitive of a given type.

**Parameters**

<i>in</i>	<i>type</i>	A primitive type.
-----------	-------------	-------------------

**Returns**

The default primitive, or zero if none exists.

**Warning**

It is recommended to keep at least one primitive of every type in the library, in order for some software (e.g. the test driver) to work properly, but this is not strictly required (so that heavily stripped builds of the library will still work properly).

The return value of this function depends on which primitives are available, and even though they are loosely prioritized, based on an arbitrary strength/performance scale, there is *absolutely* no guarantee the primitive returned will be suitable for use (in the context of your application). Use this when you do not care about the characteristics of a primitive beyond its type.

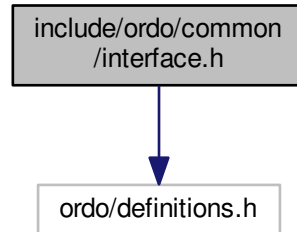
**5.5 include/ordo/common/interface.h File Reference**

API.



```
#include "ordo/definitions.h"
```

Include dependency graph for interface.h:



### 5.5.1 Detailed Description

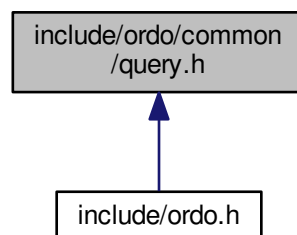
API. This header contains some preprocessor definitions which try to abstract compiler-specific features (such as packing, export mechanisms, aliasing semantics), and will be included in every other header in the library.

The definitions.h header is autogenerated by the build system, and depends on the architecture and the primitives built into the library.

## 5.6 include/ordo/common/query.h File Reference

Utility.

This graph shows which files directly or indirectly include this file:



### Enumerations

- enum `ORDO_QUERY` { `KEY_LEN_Q`, `BLOCK_SIZE_Q`, `DIGEST_LEN_Q`, `IV_LEN_Q` }

### 5.6.1 Detailed Description

Utility. This header contains declarations for query codes used when querying information from primitives or other library objects. The query must return a length or something relating to size, which is why it is used for key lengths and related quantities.

The query codes provide a lightweight mechanism to select suitable parameters when using the library, and, alternatively, iterating over all possible parameters when necessary, while still retaining some level of abstraction in user code.

All query functions take the following arguments:

- query code (one of the codes defined here)
- suggested value (type `size_t`)

They have the following properties (where *X* stands for the relevant quantity of the concerned primitive, e.g. "valid key length for some block cipher"):

- `query(code, 0)` returns the **smallest** *X*.
- `query(code, (size_t)-1)` returns the **largest** *X*.
- if `query(code, n) == n` then *n* is an *X*.
- if *n* is less than the largest *X*, then `query(code, n) > n`.
- if `query(code, n + 1) == n` then *n* is the **largest** *X*. Otherwise `query(code, n + 1)` returns the next *X* (in increasing order).

The motivation for designing this interface in this fashion is to ensure no information loss occurs when user input is provided to the library. For instance, if the user provides a 160-bit key to AES, he will first query the block cipher key length using `KEY_LEN_Q`, suggesting a 160-bit key, and the AES cipher will correctly identify the ideal key length as 192 bits, and not 128 bits (which would lead to part of the key being unused). This allows software using the library to dynamically adjust to whatever cryptographic primitives are in use without compromising security.

### 5.6.2 Enumeration Type Documentation

#### 5.6.2.1 enum `ORDO_QUERY`

Query codes used by the library. These end in `_Q`.

##### Enumerator

**`KEY_LEN_Q`** Query code to retrieve a key length.

Applicable to:

- block ciphers
- stream ciphers

**`BLOCK_SIZE_Q`** Query code to retrieve a block size.

Applicable to:

- block ciphers
- hash functions

##### Remarks

For hash functions, this is taken to be the input size of the message block to the compression function or, more formally, the amount of data required to trigger a compression function iteration. This may not be meaningful for all hash functions.

**`DIGEST_LEN_Q`** Query code to retrieve the default digest length of a hash function.

**Remarks**

The suggested value is ignored for this query code.

Applicable to:

- hash functions

**IV\_LEN\_Q** Query code to retrieve an initialization vector length.

Applicable to:

- block modes

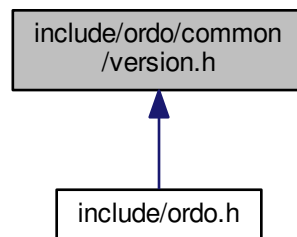
**Remarks**

As the block mode of operation primitives use block ciphers internally, the returned initialization vector length might depend on the block cipher (likely its block size).

## 5.7 include/ordo/common/version.h File Reference

Utility.

This graph shows which files directly or indirectly include this file:



### Data Structures

- struct [ORDO\\_VERSION](#)  
*Library version information.*

### Functions

- `ORDO_PUBLIC` const struct [ORDO\\_VERSION](#) \* `ordo_version` (void)

#### 5.7.1 Detailed Description

Utility. This header exposes functionality relating to the library's version.

#### 5.7.2 Function Documentation

##### 5.7.2.1 `ORDO_PUBLIC` const struct `ORDO_VERSION`\* `ordo_version` ( void )

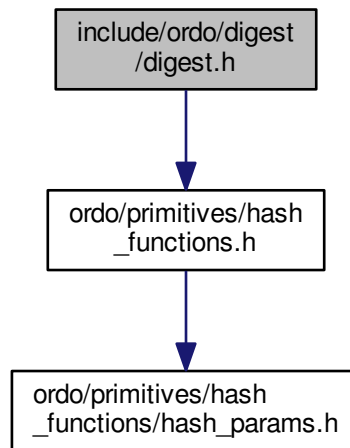
Returns an [ORDO\\_VERSION](#) structure for this library build.

## 5.8 include/ordo/digest/digest.h File Reference

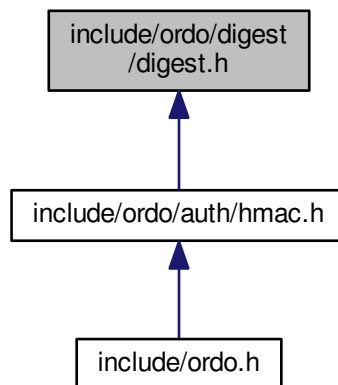
Module.

```
#include "ordo/primitives/hash_functions.h"
```

Include dependency graph for digest.h:



This graph shows which files directly or indirectly include this file:



### Macros

- #define [ordo\\_digest\\_init](#)
- #define [ordo\\_digest\\_update](#)
- #define [ordo\\_digest\\_final](#)

- `#define ordo_digest_bsize`

## Functions

- `ORDO_PUBLIC size_t digest_length (prim_t hash)`

### 5.8.1 Detailed Description

Module. Module to compute cryptographic digests, using cryptographic hash function primitives.

The advantage of using this digest module instead of the hash function abstraction layer is this keeps track of the hash function primitive for you within an opaque `DIGEST_CTX` context structure, simplifying code and making it less error-prone.

Usage snippet:

```
struct DIGEST_CTX ctx;

int err = digest_init(&ctx, HASH_SHA256, 0);
if (err) printf("Got error!\n");

const char x[] = "Hello, world!";
digest_update(&ctx, x, strlen(x));

unsigned char out[32];
digest_final(&ctx, out);
// out = 315f5bdb76d0...
```

### 5.8.2 Macro Definition Documentation

#### 5.8.2.1 `#define ordo_digest_init`

Initializes a digest context.

Parameters

<code>in, out</code>	<code>ctx</code>	A digest context.
<code>in</code>	<code>primitive</code>	A hash function primitive.
<code>in</code>	<code>params</code>	Hash function parameters.

Returns

`ORDO_SUCCESS` on success, else an error code.

Remarks

It is always valid to pass 0 into `params` if you don't want to use special features offered by a specific hash function.

Warning

It is **not** valid to initialize digest contexts more than once before calling `digest_final()`, this is because some algorithms may allocate additional memory depending on the parameters given.

#### 5.8.2.2 `#define ordo_digest_update`

Feeds data into a digest context.

**Parameters**

<code>in, out</code>	<code>ctx</code>	An initialized digest context.
<code>in</code>	<code>in</code>	The data to feed into the context.
<code>in</code>	<code>in_len</code>	The length, in bytes, of the data.

**Remarks**

This function has the same property as `hash_update()`, in that it will concatenate the input buffers of successive calls.

It is valid to pass a zero-length buffer (`in_len == 0`), which will do nothing (if this is the case, `in` may be 0).

**5.8.2.3 #define ordo\_digest\_final**

Finalizes a digest context, returning the digest of all the data fed into it through successive `digest_update()` calls.

**Parameters**

<code>in, out</code>	<code>ctx</code>	An initialized digest context.
<code>out</code>	<code>digest</code>	The output buffer for the digest.

**Remarks**

The `digest` buffer should be large enough to accommodate the digest - you can query the hash function's default digest length in bytes by the `digest_length()` function.

Calling this function immediately after `digest_init()` is valid and will return the so-called "zero-length" digest, which is the digest of the input of length zero.

**Warning**

After this function returns, you may not call `digest_update()` again until you reinitialize the context using `digest_init()`.

**5.8.2.4 #define ordo\_digest\_bsize**

Gets the size in bytes of a `DIGEST_CTX`.

**Returns**

The size in bytes of the structure.

**Remarks**

Binary compatibility layer.

**5.8.3 Function Documentation****5.8.3.1 ORDO\_PUBLIC size\_t digest\_length ( prim\_t hash )**

Returns the default digest length of a hash function.

## Parameters

<code>in</code>	<code>hash</code>	A hash function primitive.
-----------------	-------------------	----------------------------

## Returns

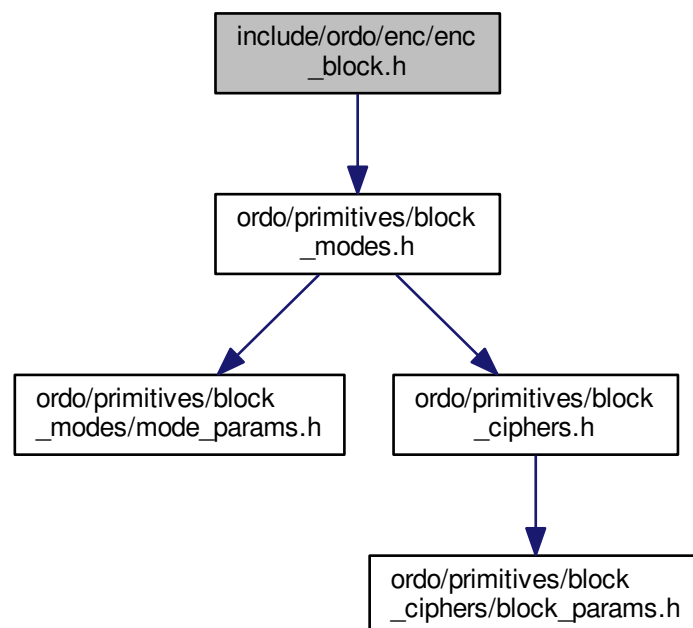
The length of the digest to be written in the `digest` parameter of `digest_final()`.

## 5.9 include/ordo/enc/enc\_block.h File Reference

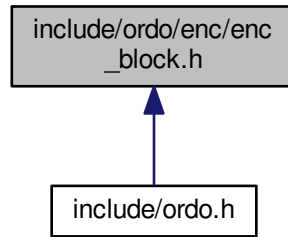
Module.

```
#include "ordo/primitives/block_modes.h"
```

Include dependency graph for `enc_block.h`:



This graph shows which files directly or indirectly include this file:



## Functions

- ORDO\_PUBLIC int [enc\\_block\\_init](#) (struct ENC\_BLOCK\_CTX \*ctx, const void \*key, size\_t key\_len, const void \*iv, size\_t iv\_len, int direction, [prim\\_t](#) cipher, const void \*cipher\_params, [prim\\_t](#) mode, const void \*mode\_params)
- ORDO\_PUBLIC void [enc\\_block\\_update](#) (struct ENC\_BLOCK\_CTX \*ctx, const void \*in, size\_t in\_len, void \*out, size\_t \*out\_len)
- ORDO\_PUBLIC int [enc\\_block\\_final](#) (struct ENC\_BLOCK\_CTX \*ctx, void \*out, size\_t \*out\_len)
- ORDO\_PUBLIC size\_t [enc\\_block\\_key\\_len](#) ([prim\\_t](#) cipher, size\_t key\_len)
- ORDO\_PUBLIC size\_t [enc\\_block\\_iv\\_len](#) ([prim\\_t](#) cipher, [prim\\_t](#) mode, size\_t iv\_len)
- ORDO\_PUBLIC size\_t [enc\\_block\\_bsize](#) (void)

### 5.9.1 Detailed Description

Module. Module to encrypt plaintext and decrypt ciphertext with different block ciphers and modes of operation. Note it is always possible to skip this API and directly use the lower-level functions available in the individual mode of operation headers, but this interface abstracts away some of the more boilerplate details and so should be preferred.

If you wish to use the lower level API, you will need to manage your block cipher contexts yourself, which can give more flexibility in some particular cases but is often unnecessary.

The padding algorithm for modes of operation which use padding is PKCS7 (RFC 5652), which appends N bytes of value N, where N is the number of padding bytes required, in bytes (between 1 and the block cipher's block size).

### 5.9.2 Function Documentation

5.9.2.1 ORDO\_PUBLIC int [enc\\_block\\_init](#) ( struct ENC\_BLOCK\_CTX \* ctx, const void \* key, size\_t key\_len, const void \* iv, size\_t iv\_len, int direction, [prim\\_t](#) cipher, const void \* cipher\_params, [prim\\_t](#) mode, const void \* mode\_params )

Initializes a block encryption context.

#### Parameters

<code>in, out</code>	<code>ctx</code>	A block encryption context.
----------------------	------------------	-----------------------------



in	<i>key</i>	The cryptographic key to use.
in	<i>key_len</i>	The length, in bytes, of the key.
in	<i>iv</i>	The initialization vector to use.
in	<i>iv_len</i>	The length, in bytes, of the IV.
in	<i>direction</i>	1 for encryption, 0 for decryption.
in	<i>cipher</i>	The block cipher primitive to use.
in	<i>cipher_params</i>	Block cipher specific parameters.
in	<i>mode</i>	The block mode primitive to use.
in	<i>mode_params</i>	Mode of operation specific parameters.

#### Returns

[ORDO\\_SUCCESS](#) on success, else an error code.

#### Remarks

The initialization vector may be 0, if the mode of operation does not require one - consult the documentation of the mode to know what it expects.

#### 5.9.2.2 ORDO\_PUBLIC void enc\_block\_update ( struct ENC\_BLOCK\_CTX \* ctx, const void \* in, size\_t in\_len, void \* out, size\_t \* out\_len )

Encrypts or decrypts a data buffer.

#### Parameters

in, out	<i>ctx</i>	A block encryption context.
in	<i>in</i>	The plaintext or ciphertext buffer.
in	<i>in_len</i>	Length, in bytes, of the input buffer.
out	<i>out</i>	The ciphertext or plaintext buffer.
out	<i>out_len</i>	The number of bytes written to <i>out</i> .

#### Remarks

This function might not immediately encrypt all data fed into it, and will write the amount of input bytes effectively encrypted in *out\_len*. However, it does **not** mean that the plaintext left over has been "rejected" or "ignored". It **has** been taken into account but the corresponding ciphertext simply can't be produced until more data is fed into it (or until [enc\\_block\\_final\(\)](#) is called).

Some modes of operation always process all input data, in which case they may allow *out\_len* to be 0 - check the documentation of the relevant mode of operation.

#### 5.9.2.3 ORDO\_PUBLIC int enc\_block\_final ( struct ENC\_BLOCK\_CTX \* ctx, void \* out, size\_t \* out\_len )

Finalizes a block encryption context.

#### Parameters

in, out	<i>ctx</i>	A block encryption context.
out	<i>out</i>	The ciphertext or plaintext buffer.
out	<i>out_len</i>	The number of bytes written to <i>out</i> .

#### Returns

[ORDO\\_SUCCESS](#) on success, else an error code.

**Remarks**

The function will return up to one block size's worth of data and may not return any data at all. For example, for the CBC mode of operation (with padding on), this function will, for encryption, append padding bytes to the final plaintext block, and return the padding block, whereas for decryption, it will take that padding block and strip the padding off, returning the last few bytes of plaintext.

Some modes of operation always process all input data, in which case they may allow `out_len` to be 0 - check the documentation of the relevant mode of operation.

**5.9.2.4 ORDO\_PUBLIC size\_t enc\_block\_key\_len ( prim\_t cipher, size\_t key\_len )**

Queries the key length of a block cipher.

**Parameters**

in	<i>cipher</i>	A block cipher primitive.
in	<i>key_len</i>	A suggested key length.

**Returns**

A suitable key length to use for this cipher.

**5.9.2.5 ORDO\_PUBLIC size\_t enc\_block\_iv\_len ( prim\_t cipher, prim\_t mode, size\_t iv\_len )**

Queries the IV length of a block mode and block cipher.

**Parameters**

in	<i>cipher</i>	A block cipher primitive.
in	<i>mode</i>	A block mode primitive.
in	<i>iv_len</i>	A suggested IV length.

**Returns**

A suitable IV length to use for this mode and cipher.

**5.9.2.6 ORDO\_PUBLIC size\_t enc\_block\_bsize ( void )**

Gets the size in bytes of an `ENC_BLOCK_CTX`.

**Returns**

The size in bytes of the structure.

**Remarks**

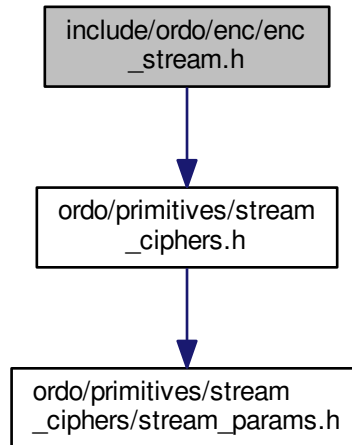
Binary compatibility layer.

**5.10 include/ordo/enc/enc\_stream.h File Reference**

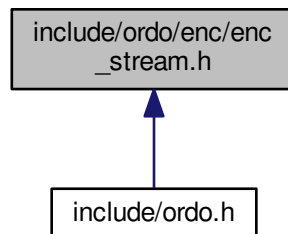
Module.

```
#include "ordo/primitives/stream_ciphers.h"
```

Include dependency graph for enc\_stream.h:



This graph shows which files directly or indirectly include this file:



## Macros

- `#define ordo_enc_stream_init`
- `#define ordo_enc_stream_update`
- `#define ordo_enc_stream_final`
- `#define ordo_enc_stream_bsize`

## Functions

- `ORDO_PUBLIC size_t enc_stream_key_len (prim_t cipher, size_t key_len)`

### 5.10.1 Detailed Description

Module. Interface to encrypt plaintext and decrypt ciphertext with various stream ciphers.

### 5.10.2 Macro Definition Documentation

#### 5.10.2.1 `#define ordo_enc_stream_init`

Initializes a stream encryption context.

##### Parameters

<code>in, out</code>	<code>ctx</code>	A stream encryption context.
<code>in</code>	<code>key</code>	The cryptographic key to use.
<code>in</code>	<code>key_size</code>	The size, in bytes, of the key.
<code>in</code>	<code>params</code>	Stream cipher specific parameters.

##### Returns

`ORDO_SUCCESS` on success, else an error code.

#### 5.10.2.2 `#define ordo_enc_stream_update`

Encrypts or decrypts a data buffer.

##### Parameters

<code>in, out</code>	<code>ctx</code>	A stream encryption context.
<code>in, out</code>	<code>buffer</code>	The plaintext or ciphertext buffer.
<code>in</code>	<code>len</code>	Number of bytes to read from the buffer.

##### Warning

By nature, stream ciphers encrypt and decrypt data the same way, in other words, if you encrypt data twice, you will get back the original data.

##### Remarks

Stream encryption is always done in place by design.

#### 5.10.2.3 `#define ordo_enc_stream_final`

Finalizes a stream encryption context.

##### Parameters

<code>in, out</code>	<code>ctx</code>	A stream encryption context.
----------------------	------------------	------------------------------

#### 5.10.2.4 `#define ordo_enc_stream_bsize`

Gets the size in bytes of an `ENC_STREAM_CTX`.

##### Returns

The size in bytes of the structure.

**Remarks**

Binary compatibility layer.

**5.10.3 Function Documentation****5.10.3.1 ORDO\_PUBLIC size\_t enc\_stream\_key\_len ( prim\_t cipher, size\_t key\_len )**

Queries a stream cipher for its key length.

**Parameters**

in	<i>cipher</i>	The stream cipher to query.
in	<i>key_len</i>	A suggested key length.

**Returns**

*key\_len* if and only if *key\_len* is a valid key length for this stream cipher. Otherwise, returns the nearest valid key length greater than *key\_len*. However, if no such key length exists, it will return the largest key length admitted by the stream cipher.

**5.11 include/ordo/internal/alg.h File Reference****Internal, Utility****Macros**

- #define [bits](#)(n)
- #define [bytes](#)(n)
- #define [offset](#)(ptr, len)

**Functions**

- ORDO\_HIDDEN size\_t [pad\\_check](#) (const void \*buffer, size\_t len)
- ORDO\_HIDDEN void [xor\\_buffer](#) (void \*RESTRICT dst, const void \*RESTRICT src, size\_t len)
- ORDO\_HIDDEN void [inc\\_buffer](#) (unsigned char \*buffer, size\_t len)

**5.11.1 Detailed Description**

**Internal, Utility** This header provides various utility functions which are used by some library modules and a few convenience macros. It is not to be used outside the library, and this is enforced by an include guard. If you really must access it, define the `ORDO_INTERNAL_ACCESS` token before including it.

**5.11.2 Macro Definition Documentation****5.11.2.1 #define bits( n )**

Converts bits into bytes (rounded down to the nearest byte boundary).

**Remarks**

As an example, `bits(256)` returns 32 (bytes).

### 5.11.2.2 #define bytes( n )

Converts bytes into bits (as a multiple of 8 bits).

#### Remarks

As an example, `bytes (32)` returns 256 (bits).

### 5.11.2.3 #define offset( ptr, len )

Computes a byte-based offset.

#### Parameters

<code>in</code>	<code>ptr</code>	Base pointer.
<code>in</code>	<code>len</code>	Offset (in bytes).

#### Returns

The pointer exactly `len` bytes after `ptr`.

#### Remarks

This is a dangerous macro, in the sense it can lead to accessing data at unaligned addresses, and so should be used carefully.

## 5.11.3 Function Documentation

### 5.11.3.1 ORDO\_HIDDEN size\_t pad\_check ( const void \* buffer, size\_t len )

Checks whether a buffer conforms to PKCS #7 padding.

#### Parameters

<code>in</code>	<code>buffer</code>	The buffer to verify, starting at the first data byte (not at the first padding byte).
<code>in</code>	<code>len</code>	The length in bytes of the buffer.

#### Returns

The message length if the buffer is valid, or 0 otherwise. The message can therefore be recovered as the first `N` bytes.

#### Remarks

PKCS padding is defined as appending `N` bytes of padding data at the end of the message, each with binary value `N`, with `N` between 1 and the block size of the block cipher used such that the length of the message plus `N` is a multiple of the block cipher's block size.

#### Warning

This implies the buffer must be at least `padding` bytes long.

### 5.11.3.2 ORDO\_HIDDEN void xor\_buffer ( void \*RESTRICT dst, const void \*RESTRICT src, size\_t len )

Performs a bitwise exclusive-or of one buffer onto another.

**Parameters**

<i>in, out</i>	<i>dst</i>	The destination buffer.
<i>in</i>	<i>src</i>	The source buffer.
<i>in</i>	<i>len</i>	The number of bytes to process.

**Remarks**

This is conceptually equivalent to  $dst \wedge= src$ .

**Warning**

The source and destination buffers may not overlap.

**5.11.3.3 ORDO\_HIDDEN void inc\_buffer ( unsigned char \* buffer, size\_t len )**

Increments a buffer of arbitrary length, as though it were a `len` byte integer stored as a byte array.

**Parameters**

<i>in, out</i>	<i>buffer</i>	The buffer to increment in-place.
<i>in</i>	<i>len</i>	The size, in bytes, of the buffer.

**Remarks**

Carry propagation is done left-to-right.

**5.12 include/ordo/internal/implementation.h File Reference****Internal, API****5.12.1 Detailed Description**

**Internal, API** This header contains some compiler-dependent macros, for defining various semantics which the users of this library should not depend on. It is an error to include this header in any code outside the Ordo implementation.

Every source file will include this header.

**5.13 include/ordo/internal/sys.h File Reference****Internal, Utility****5.13.1 Detailed Description**

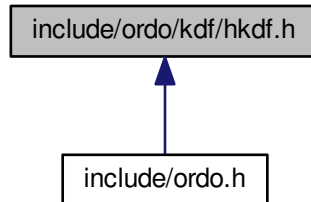
**Internal, Utility** This header provides system-dependent functionality and is internal to the library. It probably shouldn't ever be used from outside the library.

See [alg.h](#) about internal headers.

## 5.14 include/ordo/kdf/hkdf.h File Reference

Module.

This graph shows which files directly or indirectly include this file:



### Functions

- ORDO\_PUBLIC int `kdf_hkdf` (`prim_t hash`, `const void *params`, `const void *key`, `size_t key_len`, `const void *salt`, `size_t salt_len`, `const void *info`, `size_t info_len`, `void *out`, `size_t out_len`)

#### 5.14.1 Detailed Description

Module. Module for the HMAC-based Extract-and-Expand Key Derivation Function. HKDF is a key stretching function which takes in a cryptographically secure key (**not** a password) and an optional salt, and generates a longer keystream deterministically.

Just like PBKDF2, HKDF does not require the use of contexts.

#### 5.14.2 Function Documentation

5.14.2.1 ORDO\_PUBLIC int `kdf_hkdf` ( `prim_t hash`, `const void * params`, `const void * key`, `size_t key_len`, `const void * salt`, `size_t salt_len`, `const void * info`, `size_t info_len`, `void * out`, `size_t out_len` )

Derives a key using HKDF.

##### Parameters

in	<i>hash</i>	The hash function to use (the PRF used will be an instantiation of HMAC with it).
in	<i>params</i>	Hash-specific parameters.
in	<i>key</i>	The key to derive a keystream from.
in	<i>key_len</i>	The length in bytes of the key.
in	<i>salt</i>	The cryptographic salt to use.
in	<i>salt_len</i>	The length in bytes of the salt.
in	<i>info</i>	An application specific string.
in	<i>info_len</i>	The length in bytes of the info string.



out	<i>out</i>	The output buffer for the derived key.
in	<i>out_len</i>	The required length, in bytes, of the key.

**Returns**

`ORDO_SUCCESS` on success, else an error code.

**Remarks**

The salt may be zero-length in which case the buffer may be zero, and the info buffer may be zero-length as well.

The password or out buffers cannot be zero-length.

**Warning**

The HKDF algorithm distinguishes between zero-length salt, and no salt at all - thus, if you want to pass a zero-length salt (which is not recommended) pass a nonzero pointer with a zero length. If you want to pass no salt, pass a zero pointer with a zero length.

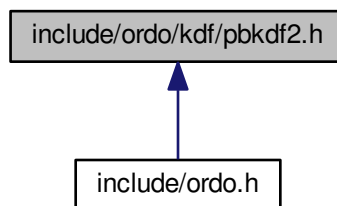
There is a maximum output length, of 255 multiplied by the digest length of the chosen hash function. This is by design.

**Remarks**

The `out` buffer should be at least `out_len` bytes long.

**5.15 include/ordo/kdf/pbkdf2.h File Reference****Module.**

This graph shows which files directly or indirectly include this file:

**Functions**

- `ORDO_PUBLIC int kdf_pbkdf2 (prim_t hash, const void *params, const void *pwd, size_t pwd_len, const void *salt, size_t salt_len, uintmax_t iterations, void *out, size_t out_len)`

**5.15.1 Detailed Description**

Module. Module for the PBKDF2 algorithm (Password-Based Key Derivation Function v2) which combines a keyed PRF (here HMAC) with a salt in order to generate secure cryptographic keys, as per RFC 2898. Also features a variable iteration count (work factor) to help thwart brute-force attacks.

Unlike most other cryptographic modules, the PBKDF2 API does not follow the traditional init/update/final pattern but is a context-free function as its inputs are almost always known in advance. As such this module does not benefit from the use of contexts.

## 5.15.2 Function Documentation

5.15.2.1 `ORDO_PUBLIC int kdf_pbkdf2 ( prim_t hash, const void * params, const void * pwd, size_t pwd_len, const void * salt, size_t salt_len, uintmax_t iterations, void * out, size_t out_len )`

Derives a key using PBKDF2.

### Parameters

in	<i>hash</i>	The hash function to use (the PRF used will be an instantiation of HMAC with it).
in	<i>params</i>	Hash-specific parameters.
in	<i>pwd</i>	The password to derive a key from.
in	<i>pwd_len</i>	The length in bytes of the password.
in	<i>salt</i>	The cryptographic salt to use.
in	<i>salt_len</i>	The length in bytes of the salt.
in	<i>iterations</i>	The number of PBKDF2 iterations to use.
out	<i>out</i>	The output buffer for the derived key.
in	<i>out_len</i>	The required length, in bytes, of the key.

### Returns

`ORDO_SUCCESS` on success, else an error code.

### Remarks

The salt may be zero-length in which case the buffer may be zero.  
The password or out buffers cannot be zero-length.

### Warning

There is a maximum output length of  $2^{32} - 1$  multiplied by the digest length of the chosen hash function, but it is unlikely to be reached as derived keys are generally no longer than a few hundred bits. Reaching the limit will result in an `ORDO_ARG` error code. This limit is mandated by the PBKDF2 specification.

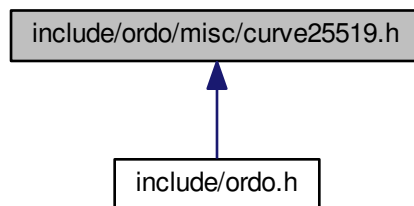
**Remarks**

The `out` buffer should be at least `out_len` bytes long.

**5.16 include/ordo/misc/curve25519.h File Reference**

Misc. asymmetric module (temp)

This graph shows which files directly or indirectly include this file:

**Functions**

- ORDO\_PUBLIC int [curve25519\\_gen](#) (void \*priv)
- ORDO\_PUBLIC void [curve25519\\_pub](#) (void \*pub, const void \*priv)
- ORDO\_PUBLIC void [curve25519\\_ecdh](#) (void \*shared, const void \*priv, const void \*other)

**5.16.1 Detailed Description**

Misc. asymmetric module (temp) This header provides access to the curve25519 asymmetric elliptic curve DH algorithm. It is in this folder temporarily as an experimental module.

**5.16.2 Function Documentation****5.16.2.1 ORDO\_PUBLIC int curve25519\_gen ( void \* *priv* )**

Generates a random private key.

**Parameters**

<code>out</code>	<code>priv</code>	Output buffer for the private key.
------------------	-------------------	------------------------------------

**Returns**

[ORDO\\_SUCCESS](#) on success, else an error code.

**Remarks**

The private key is exactly 32 bytes (256 bits) long.  
This function uses [os\\_secure\\_random\(\)](#).

5.16.2.2 ORDO\_PUBLIC void curve25519\_pub ( void \* *pub*, const void \* *priv* )

Retrieves the public key corresponding to a private key.

**Parameters**

out	<i>pub</i>	Output buffer for the public key.
in	<i>priv</i>	The private key to be used.

**Remarks**

The public key is exactly 32 bytes (256 bits) long.

The private key must be in the proper format - that is, correctly masked according to the curve25519 specification (relating to the first and last bytes of the private key).

### 5.16.2.3 ORDO\_PUBLIC void curve25519\_ecdh ( void \* *shared*, const void \* *priv*, const void \* *other* )

Computes the shared secret between two keypairs.

**Parameters**

out	<i>shared</i>	Output buffer for the shared secret.
in	<i>priv</i>	The private key of the first keypair.
in	<i>other</i>	The public key of the second keypair.

**Remarks**

The shared secret is exactly 32 bytes (256 bits) long.

**Warning**

This shared secret is **unique** to a given pair of keypairs, thus it should be treated as long-term key material, i.e. don't use it directly for encryption or other (derive secondary keys from it).

## 5.17 include/ordo/misc/endianness.h File Reference

Utility.

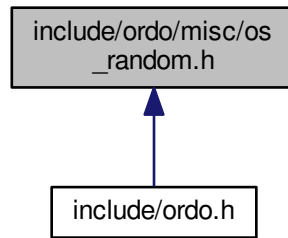
### 5.17.1 Detailed Description

Utility. This header provides endianness functionality. You may use it freely as it has a stable API and is public. Only supports little/big endian for now.

## 5.18 include/ordo/misc/os\_random.h File Reference

Module.

This graph shows which files directly or indirectly include this file:



## Functions

- ORDO\_PUBLIC int [os\\_random](#) (void \*out, size\_t len)
- ORDO\_PUBLIC int [os\\_secure\\_random](#) (void \*out, size\_t len)

### 5.18.1 Detailed Description

Module. Exposes the OS CSPRNG (Cryptographically Secure PseudoRandom Number Generator) interface, which is basically a cross-platform wrapper to the OS-provided entropy pool. To learn more about how it is implemented, go to the source code or find out what facilities your operating system provides for entropy gathering.

### 5.18.2 Function Documentation

#### 5.18.2.1 ORDO\_PUBLIC int os\_random ( void \* out, size\_t len )

Generates cryptographically secure pseudorandom numbers.

##### Parameters

out	<i>out</i>	The destination buffer.
in	<i>len</i>	The number of bytes to generate.

##### Returns

[ORDO\\_SUCCESS](#) on success, else an error code.

##### Remarks

This function uses the CSPRNG provided by your operating system.

If the platform does not provide this feature, this function will always fail with the [ORDO\\_FAIL](#) error message, and any data in the buffer should be discarded as indeterminate.

#### 5.18.2.2 ORDO\_PUBLIC int os\_secure\_random ( void \* out, size\_t len )

Generates cryptographically secure pseudorandom numbers, the function will make a best effort attempt to access the operating system entropy pool and so, ideally, should return exactly `len` bytes of entropy, whereas the [os\\_random\(\)](#) function need only return enough entropy for the output stream to be computationally indistinguishable from a non-random stream. However, keep in mind that this function is **not required** to behave as such.

## Parameters

out	<i>out</i>	The destination buffer.
in	<i>len</i>	The number of bytes to generate.

## Returns

`ORDO_SUCCESS` on success, else an error code.

## Warning

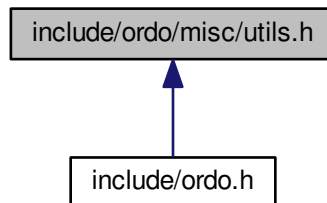
If your platform doesn't provide this feature, this function will fall back to `os_random()` (there is no way to know whether this feature is available, this is by design).

You should not need to know whether this feature is available, as this function will make a "best effort" attempt to obtain entropy from the operating system - you should use this function for high security uses such as generating private keys (it has a high cost so don't use it for e.g. nonces and initialization vectors).

## 5.19 include/ordo/misc/utls.h File Reference

Utility.

This graph shows which files directly or indirectly include this file:



## Functions

- `ORDO_PUBLIC int ctcmp` (const void \*x, const void \*y, size\_t len)

## 5.19.1 Detailed Description

Utility. This header contains utility functions, which are of use to developers who will use the library, for instance, constant-time comparisons, and so on.

## 5.19.2 Function Documentation

5.19.2.1 `ORDO_PUBLIC int ctcmp` ( const void \* x, const void \* y, size\_t len )

Performs a constant-time comparison between two buffers.

## Parameters

in	<i>x</i>	The 1st buffer.
in	<i>y</i>	The 2nd buffer.
in	<i>len</i>	Length in bytes.

## Returns

Returns a positive value if the buffers match, 0 otherwise.

## Warning

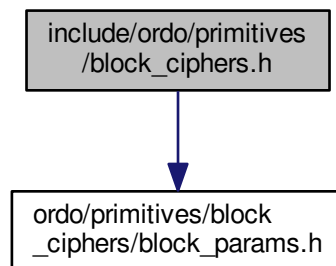
This function is for equality only, not ordering.

## 5.20 include/ordo/primitives/block\_ciphers.h File Reference

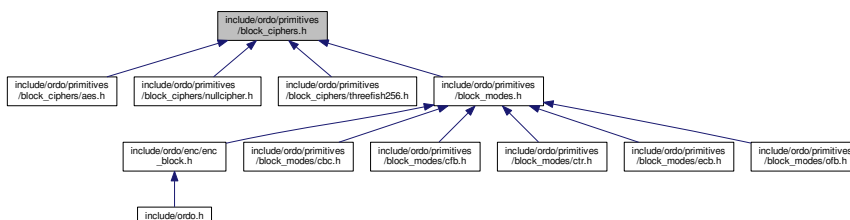
Abstraction Layer.

```
#include "ordo/primitives/block_ciphers/block_params.h"
```

Include dependency graph for block\_ciphers.h:



This graph shows which files directly or indirectly include this file:



## Functions

- ORDO\_PUBLIC int [block\\_init](#) (struct BLOCK\_STATE \*state, const void \*key, size\_t key\_len, [prim\\_t](#) primitive, const void \*params)
- ORDO\_PUBLIC void [block\\_forward](#) (const struct BLOCK\_STATE \*state, void \*block)



- ORDO\_PUBLIC void [block\\_inverse](#) (const struct BLOCK\_STATE \*state, void \*block)
- ORDO\_PUBLIC void [block\\_final](#) (struct BLOCK\_STATE \*state)
- ORDO\_PUBLIC size\_t [block\\_query](#) (prim\_t primitive, int query, size\_t value)
- ORDO\_PUBLIC size\_t [block\\_bsize](#) (void)

### 5.20.1 Detailed Description

Abstraction Layer. This abstraction layer declares all the block ciphers, and also makes them available to higher level modules. This does not actually do encryption at all but simply abstracts block cipher permutations, the encryption modules are in the `enc` folder: [enc\\_block.h](#).

### 5.20.2 Function Documentation

5.20.2.1 ORDO\_PUBLIC int [block\\_init](#) ( struct BLOCK\_STATE \* state, const void \* key, size\_t key\_len, prim\_t primitive, const void \* params )

Initializes a block cipher state.

#### Parameters

in, out	<i>state</i>	A block cipher state.
in	<i>key</i>	The cryptographic key to use.
in	<i>key_len</i>	The length, in bytes, of the key.
in	<i>primitive</i>	A block cipher primitive.
in	<i>params</i>	Block cipher specific parameters.

#### Returns

[ORDO\\_SUCCESS](#) on success, else an error code.

5.20.2.2 ORDO\_PUBLIC void [block\\_forward](#) ( const struct BLOCK\_STATE \* state, void \* block )

Applies a block cipher's forward permutation.

#### Parameters

in	<i>state</i>	An initialized block cipher state.
in, out	<i>block</i>	A data block to permute.

#### Remarks

The block should be the size of the block cipher's block size.

5.20.2.3 ORDO\_PUBLIC void [block\\_inverse](#) ( const struct BLOCK\_STATE \* state, void \* block )

Applies a block cipher's inverse permutation.

#### Parameters

in	<i>state</i>	An initialized block cipher state.
in, out	<i>block</i>	A data block to permute.

#### Remarks

The block should be the size of the block cipher's block size.

5.20.2.4 ORDO\_PUBLIC void block\_final ( struct BLOCK\_STATE \* *state* )

Finalizes a block cipher state.

**Parameters**

<code>in, out</code>	<code>state</code>	A block cipher state.
----------------------	--------------------	-----------------------

**5.20.2.5 ORDO\_PUBLIC size\_t block\_query ( prim\_t primitive, int query, size\_t value )**

Queries a block cipher for suitable parameters.

**Parameters**

<code>in</code>	<code>primitive</code>	A block cipher primitive.
<code>in</code>	<code>query</code>	A query code.
<code>in</code>	<code>value</code>	A suggested value.

**Returns**

A suitable parameter of type `query` based on `value`.

**See Also**

[query.h](#)

**5.20.2.6 ORDO\_PUBLIC size\_t block\_bsize ( void )**

Gets the size in bytes of a `BLOCK_STATE`.

**Returns**

The size in bytes of the structure.

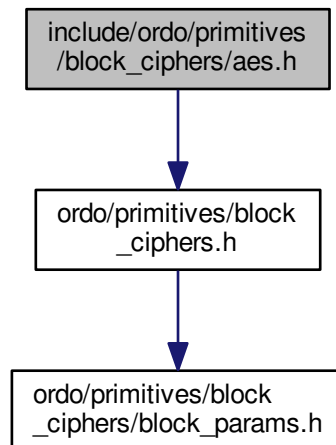
**Remarks**

Binary compatibility layer.

**5.21 include/ordo/primitives/block\_ciphers/aes.h File Reference**

Primitive.

```
#include "ordo/primitives/block_ciphers.h"
Include dependency graph for aes.h:
```

**Functions**

- ORDO\_PUBLIC int [aes\\_init](#) (struct AES\_STATE \*state, const void \*key, size\_t key\_len, const struct [AES\\_PARAMS](#) \*params)
- ORDO\_PUBLIC void [aes\\_forward](#) (const struct AES\_STATE \*state, void \*block)
- ORDO\_PUBLIC void [aes\\_inverse](#) (const struct AES\_STATE \*state, void \*block)
- ORDO\_PUBLIC void [aes\\_final](#) (struct AES\_STATE \*state)
- ORDO\_PUBLIC size\_t [aes\\_query](#) (int query, size\_t value)
- ORDO\_PUBLIC size\_t [aes\\_bsize](#) (void)

**5.21.1 Detailed Description**

Primitive. AES (Advanced Encryption Standard) is a block cipher. It has a 128-bit block size and three possible key sizes, namely 128, 192 and 256 bits. It is based on the Rijndael cipher and was selected as the official encryption standard on November 2001 (FIPS 197).

**5.21.2 Function Documentation**

**5.21.2.1** ORDO\_PUBLIC int [aes\\_init](#) ( struct AES\_STATE \* *state*, const void \* *key*, size\_t *key\_len*, const struct [AES\\_PARAMS](#) \* *params* )

## See Also

[block\\_init\(\)](#)

## Return values

<a href="#">ORDO_KEY_LEN</a>	if the key length is not 16, 24, or 32 (bytes).
<a href="#">ORDO_ARG</a>	if parameters were provided and requested zero rounds or more than 20 rounds.

5.21.2.2 **ORDO\_PUBLIC** void `aes_forward` ( const struct AES\_STATE \* *state*, void \* *block* )

## See Also

[block\\_forward\(\)](#)

5.21.2.3 **ORDO\_PUBLIC** void `aes_inverse` ( const struct AES\_STATE \* *state*, void \* *block* )

## See Also

[block\\_inverse\(\)](#)

5.21.2.4 **ORDO\_PUBLIC** void `aes_final` ( struct AES\_STATE \* *state* )

## See Also

[block\\_final\(\)](#)

5.21.2.5 **ORDO\_PUBLIC** size\_t `aes_query` ( int *query*, size\_t *value* )

## See Also

[block\\_query\(\)](#)

5.21.2.6 **ORDO\_PUBLIC** size\_t `aes_bsize` ( void )

Gets the size in bytes of an `AES_STATE`.

## Returns

The size in bytes of the structure.

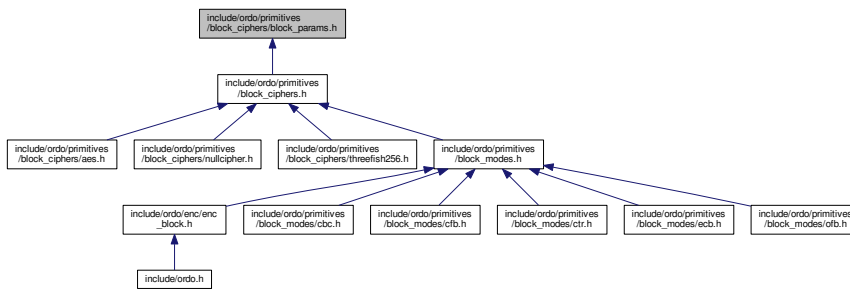
## Remarks

Binary compatibility layer.

## 5.22 include/ordo/primitives/block\_ciphers/block\_params.h File Reference

Primitive Parameters.

This graph shows which files directly or indirectly include this file:



## Data Structures

- struct [THREEFISH256\\_PARAMS](#)

*Threefish-256 block cipher parameters.*

- struct [AES\\_PARAMS](#)

*AES block cipher parameters.*

- union [BLOCK\\_PARAMS](#)

*Polymorphic block cipher parameter union.*

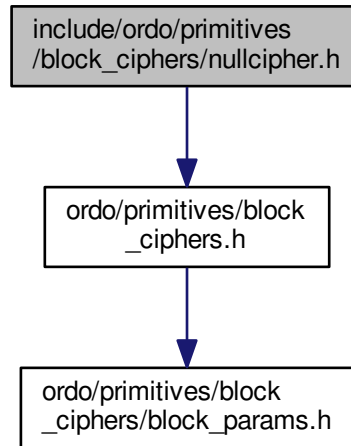
### 5.22.1 Detailed Description

Primitive Parameters. This header contains parameter structures for all block ciphers.

## 5.23 include/ordo/primitives/block\_ciphers/nullcipher.h File Reference

Primitive.

```
#include "ordo/primitives/block_ciphers.h"  
Include dependency graph for nullcipher.h:
```



## Functions

- ORDO\_PUBLIC int [nullcipher\\_init](#) (struct NULLCIPHER\_STATE \*state, const void \*key, size\_t key\_len, const void \*params)
- ORDO\_PUBLIC void [nullcipher\\_forward](#) (const struct NULLCIPHER\_STATE \*state, void \*block)
- ORDO\_PUBLIC void [nullcipher\\_inverse](#) (const struct NULLCIPHER\_STATE \*state, void \*block)
- ORDO\_PUBLIC void [nullcipher\\_final](#) (struct NULLCIPHER\_STATE \*state)
- ORDO\_PUBLIC size\_t [nullcipher\\_query](#) (int query, size\_t value)
- ORDO\_PUBLIC size\_t [nullcipher\\_bsize](#) (void)

### 5.23.1 Detailed Description

Primitive. This cipher is only used to debug the library and does absolutely nothing, in other words, it is the identity permutation. It accepts no key, that is it only accepts a key length of zero bytes. Its block size is 128 bits and is arbitrarily chosen.

### 5.23.2 Function Documentation

5.23.2.1 ORDO\_PUBLIC int `nullcipher_init ( struct NULLCIPHER_STATE * state, const void * key, size_t key_len, const void * params )`

See Also

[block\\_init\(\)](#)

## Return values

<code>ORDO_KEY_LEN</code>	if the key length is not zero.
---------------------------	--------------------------------

5.23.2.2 `ORDO_PUBLIC void nullcipher_forward ( const struct NULLCIPHER_STATE * state, void * block )`

## See Also

`block_forward()`

5.23.2.3 `ORDO_PUBLIC void nullcipher_inverse ( const struct NULLCIPHER_STATE * state, void * block )`

## See Also

`block_inverse()`

5.23.2.4 `ORDO_PUBLIC void nullcipher_final ( struct NULLCIPHER_STATE * state )`

## See Also

`block_final()`

5.23.2.5 `ORDO_PUBLIC size_t nullcipher_query ( int query, size_t value )`

## See Also

`block_query()`

5.23.2.6 `ORDO_PUBLIC size_t nullcipher_bsize ( void )`

Gets the size in bytes of a `NULLCIPHER_STATE`.

## Returns

The size in bytes of the structure.

## Remarks

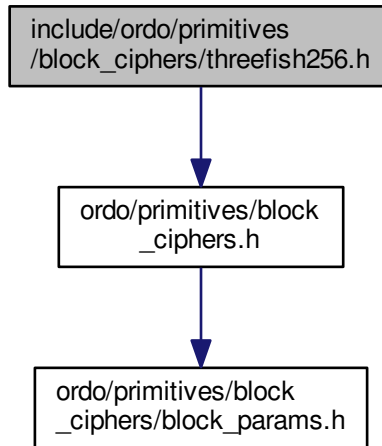
Binary compatibility layer.

## 5.24 `include/ordo/primitives/block_ciphers/threefish256.h` File Reference

Primitive.



```
#include "ordo/primitives/block_ciphers.h"  
Include dependency graph for threefish256.h:
```



## Functions

- ORDO\_PUBLIC int [threefish256\\_init](#) (struct THREEFISH256\_STATE \*state, const void \*key, size\_t key\_len, const struct THREEFISH256\_PARAMS \*params)
- ORDO\_PUBLIC void [threefish256\\_forward](#) (const struct THREEFISH256\_STATE \*state, void \*block)
- ORDO\_PUBLIC void [threefish256\\_inverse](#) (const struct THREEFISH256\_STATE \*state, void \*block)
- ORDO\_PUBLIC void [threefish256\\_final](#) (struct THREEFISH256\_STATE \*state)
- ORDO\_PUBLIC size\_t [threefish256\\_query](#) (int query, size\_t value)
- ORDO\_PUBLIC size\_t [threefish256\\_bsize](#) (void)

### 5.24.1 Detailed Description

Primitive. Threefish-256 is a block cipher with a 256-bit block size and a 256-bit key size. It also has an optional 128-bit tweak, which can be set through the cipher parameters.

The Threefish ciphers were originally designed to be used as a building block for the Skein hash function family.

### 5.24.2 Function Documentation

5.24.2.1 ORDO\_PUBLIC int [threefish256\\_init](#) ( struct THREEFISH256\_STATE \* state, const void \* key, size\_t key\_len, const struct THREEFISH256\_PARAMS \* params )

See Also

[block\\_init\(\)](#)

## Return values

<code>ORDO_KEY_LEN</code>	if the key length is not 32 (bytes).
---------------------------	--------------------------------------

5.24.2.2 `ORDO_PUBLIC void threefish256_forward ( const struct THREEFISH256_STATE * state, void * block )`

## See Also

`block_forward()`

5.24.2.3 `ORDO_PUBLIC void threefish256_inverse ( const struct THREEFISH256_STATE * state, void * block )`

## See Also

`block_inverse()`

5.24.2.4 `ORDO_PUBLIC void threefish256_final ( struct THREEFISH256_STATE * state )`

## See Also

`block_final()`

5.24.2.5 `ORDO_PUBLIC size_t threefish256_query ( int query, size_t value )`

## See Also

`block_query()`

5.24.2.6 `ORDO_PUBLIC size_t threefish256_bsize ( void )`

Gets the size in bytes of a `THREEFISH256_STATE`.

## Returns

The size in bytes of the structure.

## Remarks

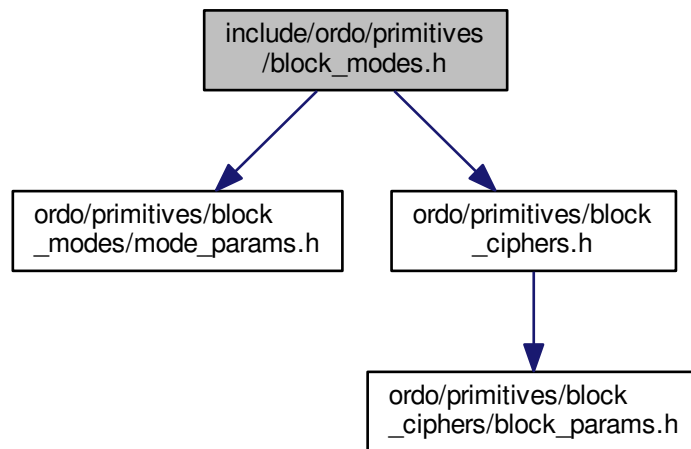
Binary compatibility layer.

## 5.25 `include/ordo/primitives/block_modes.h` File Reference

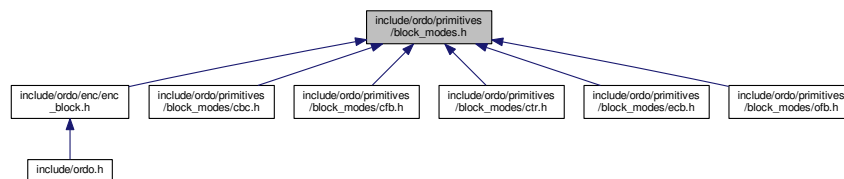
Abstraction Layer.

```
#include "ordo/primitives/block_modes/mode_params.h"
#include "ordo/primitives/block_ciphers.h"
```

Include dependency graph for block\_modes.h:



This graph shows which files directly or indirectly include this file:



## Functions

- ORDO\_PUBLIC int `block_mode_init` (struct BLOCK\_MODE\_STATE \*state, struct BLOCK\_STATE \*cipher\_state, const void \*iv, size\_t iv\_len, int direction, `prim_t` primitive, const void \*params)
- ORDO\_PUBLIC void `block_mode_update` (struct BLOCK\_MODE\_STATE \*state, struct BLOCK\_STATE \*cipher\_state, const void \*in, size\_t in\_len, void \*out, size\_t \*out\_len)
- ORDO\_PUBLIC int `block_mode_final` (struct BLOCK\_MODE\_STATE \*state, struct BLOCK\_STATE \*cipher\_state, void \*out, size\_t \*out\_len)
- ORDO\_PUBLIC size\_t `block_mode_query` (`prim_t` mode, `prim_t` cipher, int query, size\_t value)
- ORDO\_PUBLIC size\_t `block_mode_bsize` (void)

### 5.25.1 Detailed Description

Abstraction Layer. This abstraction layer declares all the block modes of operation in the library, making them available to higher level modules.

Note "block cipher mode of operation" is shortened to "block mode" in code and documentation to minimize noise and redundancy.

## 5.25.2 Function Documentation

5.25.2.1 `ORDO_PUBLIC int block_mode_init ( struct BLOCK_MODE_STATE * state, struct BLOCK_STATE * cipher_state, const void * iv, size_t iv_len, int direction, prim_t primitive, const void * params )`

Initializes a block mode state.

### Parameters

<code>in, out</code>	<code>state</code>	A block mode state.
<code>in</code>	<code>cipher_state</code>	A block cipher state.
<code>in</code>	<code>iv</code>	The initialization vector to use.
<code>in</code>	<code>iv_len</code>	The length, in bytes, of the IV.
<code>in</code>	<code>direction</code>	1 for encryption, 0 for decryption.
<code>in</code>	<code>primitive</code>	A block mode primitive.
<code>in</code>	<code>params</code>	Block mode specific parameters.

### Returns

`ORDO_SUCCESS` on success, else an error code.

5.25.2.2 `ORDO_PUBLIC void block_mode_update ( struct BLOCK_MODE_STATE * state, struct BLOCK_STATE * cipher_state, const void * in, size_t in_len, void * out, size_t * out_len )`

Encrypts or decrypts a buffer.

### Parameters

<code>in, out</code>	<code>state</code>	A block mode state.
<code>in</code>	<code>cipher_state</code>	A block cipher state.
<code>in</code>	<code>in</code>	The input buffer.
<code>in</code>	<code>in_len</code>	The length, in bytes, of the input.
<code>out</code>	<code>out</code>	The output buffer.
<code>out</code>	<code>out_len</code>	A pointer to an integer to which to write the number of output bytes that can be returned to the user. Remaining input data has <b>not</b> been ignored and should not be passed again.

### Warning

In-place encryption (by letting `in` be the same buffer as `out`) is always supported, however the buffers may **not** overlap.

5.25.2.3 `ORDO_PUBLIC int block_mode_final ( struct BLOCK_MODE_STATE * state, struct BLOCK_STATE * cipher_state, void * out, size_t * out_len )`

Finalizes a block mode state.

### Parameters

<code>in, out</code>	<code>state</code>	A block mode state.
<code>in</code>	<code>cipher_state</code>	A block cipher state.
<code>out</code>	<code>out</code>	The output buffer.
<code>out</code>	<code>out_len</code>	A pointer to an integer to which to store the number of bytes written to <code>out</code> .

### Returns

`ORDO_SUCCESS` on success, else an error code.

**Remarks**

This function will return any input bytes which were not returned by calls to `block_mode_update()` (in the correct order).

**5.25.2.4 ORDO\_PUBLIC size\_t block\_mode\_query ( prim\_t mode, prim\_t cipher, int query, size\_t value )**

Queries a block mode for suitable parameters.

**Parameters**

in	<i>mode</i>	A block mode primitive.
in	<i>cipher</i>	A block cipher primitive.
in	<i>query</i>	A query code.
in	<i>value</i>	A suggested value.

**Returns**

A suitable parameter of type `query` based on `value`.

**See Also**

[query.h](#)

**5.25.2.5 ORDO\_PUBLIC size\_t block\_mode\_bsize ( void )**

Gets the size in bytes of a `BLOCK_MODE_STATE`.

**Returns**

The size in bytes of the structure.

## Remarks

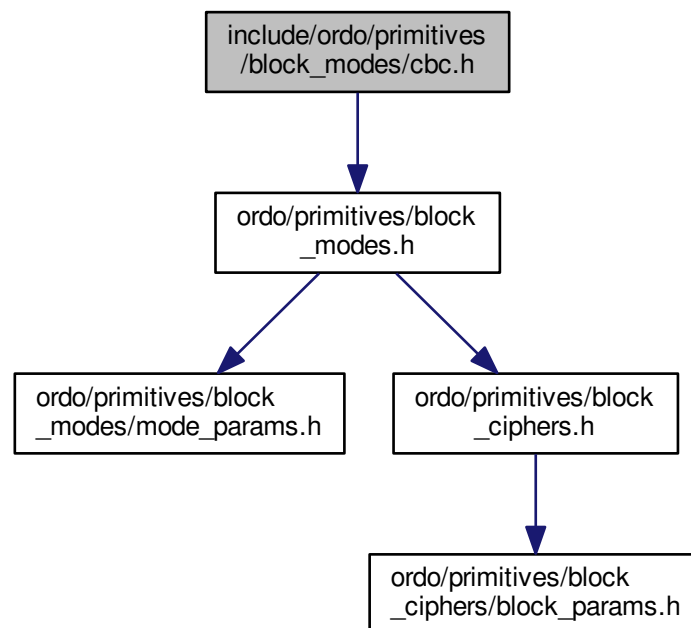
Binary compatibility layer.

## 5.26 include/ordo/primitives/block\_modes/cbc.h File Reference

Primitive.

```
#include "ordo/primitives/block_modes.h"
```

Include dependency graph for cbc.h:



### Functions

- `ORDO_PUBLIC int cbc_init` (struct CBC\_STATE \*state, struct BLOCK\_STATE \*cipher\_state, const void \*iv, size\_t iv\_len, int dir, const struct CBC\_PARAMS \*params)
- `ORDO_PUBLIC void cbc_update` (struct CBC\_STATE \*state, struct BLOCK\_STATE \*cipher\_state, const void \*in, size\_t in\_len, void \*out, size\_t \*out\_len)
- `ORDO_PUBLIC int cbc_final` (struct CBC\_STATE \*state, struct BLOCK\_STATE \*cipher\_state, void \*out, size\_t \*out\_len)
- `ORDO_PUBLIC size_t cbc_query` (prim\_t cipher, int query, size\_t value)
- `ORDO_PUBLIC size_t cbc_bsize` (void)

#### 5.26.1 Detailed Description

Primitive. The CBC mode divides the input message into blocks of the cipher's block size, and encrypts them in a sequential fashion, where each block depends on the previous one (and the first block depends on the initialization vector). If the input message's length is not a multiple of the cipher's block size, a padding mechanism is enabled by default which will pad the message to the correct length (and remove the extra data upon decryption). If padding is

explicitly disabled through the mode of operation's parameters, the input's length must be a multiple of the cipher's block size.

If padding is enabled, `cbc_final()` requires a valid pointer to be passed in the `out_len` parameter and will always return a full blocksize of data, containing the last few ciphertext bytes containing the padding information.

If padding is disabled, `out_len` is also required, and will return the number of unprocessed plaintext bytes in the context. If this is any value other than zero, the function will also fail with `ORDO_LEFTOVER`.

## 5.26.2 Function Documentation

5.26.2.1 **ORDO\_PUBLIC** int `cbc_init` ( struct CBC\_STATE \* *state*, struct BLOCK\_STATE \* *cipher\_state*, const void \* *iv*, size\_t *iv\_len*, int *dir*, const struct CBC\_PARAMS \* *params* )

See Also

[block\\_mode\\_init\(\)](#)

5.26.2.2 **ORDO\_PUBLIC** void `cbc_update` ( struct CBC\_STATE \* *state*, struct BLOCK\_STATE \* *cipher\_state*, const void \* *in*, size\_t *in\_len*, void \* *out*, size\_t \* *out\_len* )

See Also

[block\\_mode\\_update\(\)](#)

5.26.2.3 **ORDO\_PUBLIC** int `cbc_final` ( struct CBC\_STATE \* *state*, struct BLOCK\_STATE \* *cipher\_state*, void \* *out*, size\_t \* *out\_len* )

See Also

[block\\_mode\\_final\(\)](#)

5.26.2.4 **ORDO\_PUBLIC** size\_t `cbc_query` ( prim\_t *cipher*, int *query*, size\_t *value* )

See Also

[block\\_mode\\_query\(\)](#)

5.26.2.5 **ORDO\_PUBLIC** size\_t `cbc_bsize` ( void )

Gets the size in bytes of a `CBC_STATE`.

Returns

The size in bytes of the structure.

Remarks

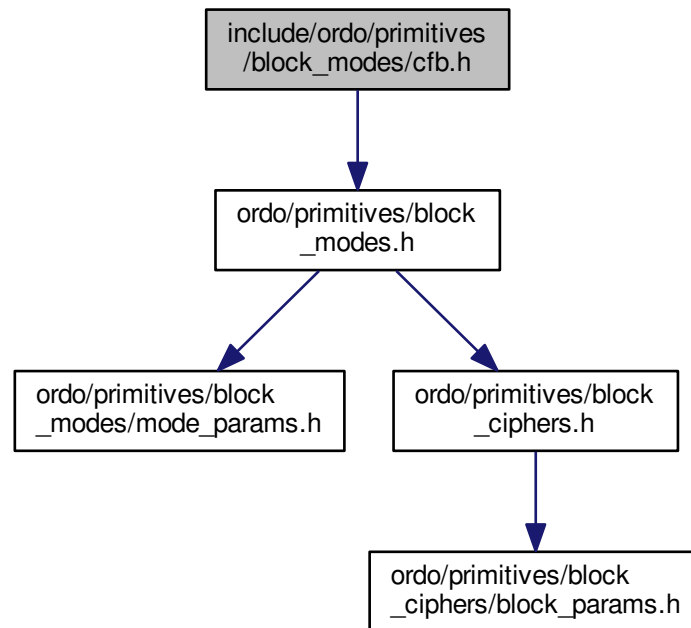
Binary compatibility layer.

## 5.27 include/ordo/primitives/block\_modes/cfb.h File Reference

Primitive.

```
#include "ordo/primitives/block_modes.h"
```

Include dependency graph for cfb.h:



### Functions

- `ORDO_PUBLIC int cfb_init` (struct CFB\_STATE \*state, struct BLOCK\_STATE \*cipher\_state, const void \*iv, size\_t iv\_len, int dir, const void \*params)
- `ORDO_PUBLIC void cfb_update` (struct CFB\_STATE \*state, struct BLOCK\_STATE \*cipher\_state, const void \*in, size\_t in\_len, void \*out, size\_t \*out\_len)
- `ORDO_PUBLIC int cfb_final` (struct CFB\_STATE \*state, struct BLOCK\_STATE \*cipher\_state, void \*out, size\_t \*out\_len)
- `ORDO_PUBLIC size_t cfb_query` (prim\_t cipher, int query, size\_t value)
- `ORDO_PUBLIC size_t cfb_bsize` (void)

#### 5.27.1 Detailed Description

Primitive. The CFB mode generates a keystream by repeatedly encrypting an initialization vector and mixing in the plaintext, effectively turning a block cipher into a stream cipher. As such, CFB mode requires no padding, and the ciphertext size will always be equal to the plaintext size.

Note that the CFB keystream depends on the plaintext fed into it, as opposed to OFB mode. This also means the block cipher's inverse permutation is never used.

`cfb_final()` accepts 0 as an argument for `out_len` since by design the CFB mode of operation does not produce any final data. However, if a valid pointer is passed, its value will be set to zero as expected.



## 5.27.2 Function Documentation

5.27.2.1 **ORDO\_PUBLIC** int `cfb_init` ( struct CFB\_STATE \* *state*, struct BLOCK\_STATE \* *cipher\_state*, const void \* *iv*, size\_t *iv\_len*, int *dir*, const void \* *params* )

See Also

[block\\_mode\\_init\(\)](#)

5.27.2.2 **ORDO\_PUBLIC** void `cfb_update` ( struct CFB\_STATE \* *state*, struct BLOCK\_STATE \* *cipher\_state*, const void \* *in*, size\_t *in\_len*, void \* *out*, size\_t \* *out\_len* )

See Also

[block\\_mode\\_update\(\)](#)

5.27.2.3 **ORDO\_PUBLIC** int `cfb_final` ( struct CFB\_STATE \* *state*, struct BLOCK\_STATE \* *cipher\_state*, void \* *out*, size\_t \* *out\_len* )

See Also

[block\\_mode\\_final\(\)](#)

5.27.2.4 **ORDO\_PUBLIC** size\_t `cfb_query` ( prim\_t *cipher*, int *query*, size\_t *value* )

See Also

[block\\_mode\\_query\(\)](#)

5.27.2.5 **ORDO\_PUBLIC** size\_t `cfb_bsize` ( void )

Gets the size in bytes of a CFB\_STATE.

Returns

The size in bytes of the structure.

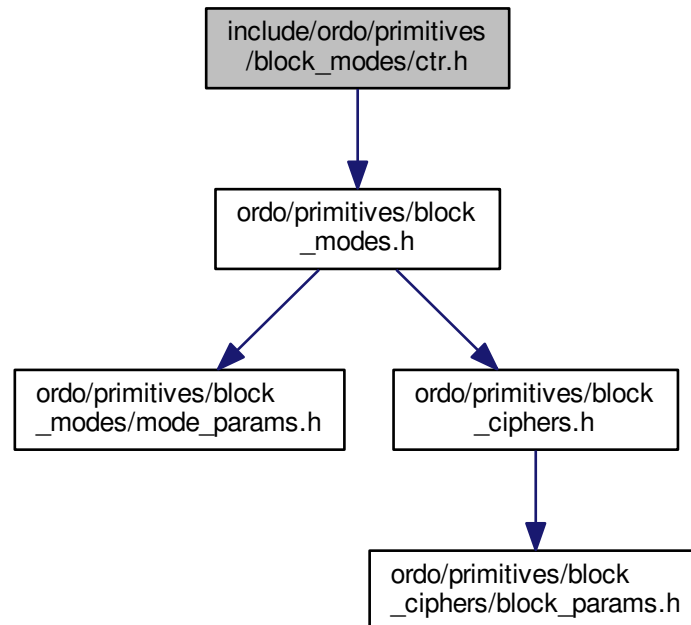
Remarks

Binary compatibility layer.

## 5.28 include/ordo/primitives/block\_modes/ctr.h File Reference

Primitive.

```
#include "ordo/primitives/block_modes.h"
Include dependency graph for ctr.h:
```



## Functions

- ORDO\_PUBLIC int [ctr\\_init](#) (struct CTR\_STATE \*state, struct BLOCK\_STATE \*cipher\_state, const void \*iv, size\_t iv\_len, int dir, const void \*params)
- ORDO\_PUBLIC void [ctr\\_update](#) (struct CTR\_STATE \*state, struct BLOCK\_STATE \*cipher\_state, const void \*in, size\_t in\_len, void \*out, size\_t \*out\_len)
- ORDO\_PUBLIC int [ctr\\_final](#) (struct CTR\_STATE \*state, struct BLOCK\_STATE \*cipher\_state, void \*out, size\_t \*out\_len)
- ORDO\_PUBLIC size\_t [ctr\\_query](#) (prim\_t cipher, int query, size\_t value)
- ORDO\_PUBLIC size\_t [ctr\\_bsize](#) (void)

### 5.28.1 Detailed Description

Primitive. The CTR mode generates a keystream by repeatedly encrypting a counter starting from some initialization vector, effectively turning a block cipher into a stream cipher. As such, CTR mode requires no padding, and outlen will always be equal to inlen.

Note that the CTR keystream is independent of the plaintext, and is also spatially coherent (using a given initialization vector on a len-byte message will "use up" len bytes of the keystream) so care must be taken to avoid reusing the initialization vector in an insecure way. This also means the block cipher's inverse permutation is never used.

[ctr\\_final\(\)](#) accepts 0 as an argument for `out_len` since by design the CTR mode of operation does not produce any final data. However, if a valid pointer is passed, its value will be set to zero as expected.

### 5.28.2 Function Documentation

5.28.2.1 **ORDO\_PUBLIC** int ctr\_init ( struct CTR\_STATE \* *state*, struct BLOCK\_STATE \* *cipher\_state*, const void \* *iv*, size\_t *iv\_len*, int *dir*, const void \* *params* )

See Also

[block\\_mode\\_init\(\)](#)

5.28.2.2 **ORDO\_PUBLIC** void ctr\_update ( struct CTR\_STATE \* *state*, struct BLOCK\_STATE \* *cipher\_state*, const void \* *in*, size\_t *in\_len*, void \* *out*, size\_t \* *out\_len* )

See Also

[block\\_mode\\_update\(\)](#)

5.28.2.3 **ORDO\_PUBLIC** int ctr\_final ( struct CTR\_STATE \* *state*, struct BLOCK\_STATE \* *cipher\_state*, void \* *out*, size\_t \* *out\_len* )

See Also

[block\\_mode\\_final\(\)](#)

5.28.2.4 **ORDO\_PUBLIC** size\_t ctr\_query ( prim\_t *cipher*, int *query*, size\_t *value* )

See Also

[block\\_mode\\_query\(\)](#)

5.28.2.5 **ORDO\_PUBLIC** size\_t ctr\_bsize ( void )

Gets the size in bytes of a CTR\_STATE.

Returns

The size in bytes of the structure.

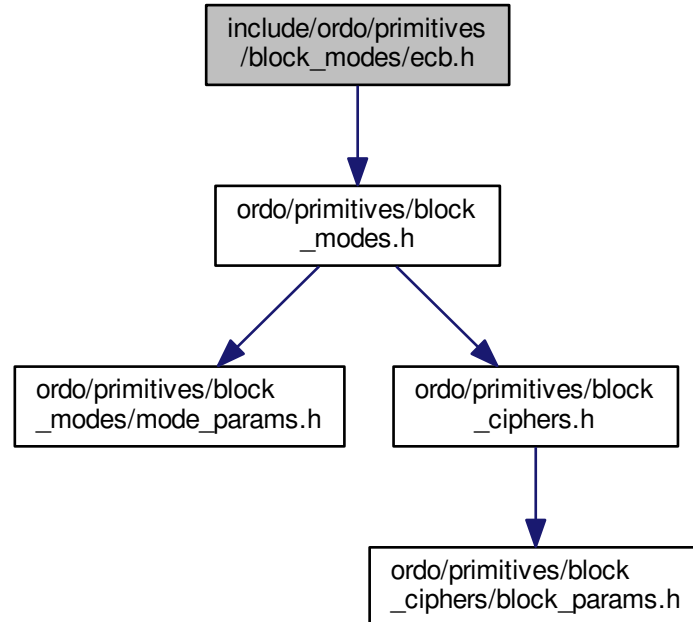
Remarks

Binary compatibility layer.

## 5.29 include/ordo/primitives/block\_modes/ecb.h File Reference

Primitive.

```
#include "ordo/primitives/block_modes.h"
Include dependency graph for ecb.h:
```



## Functions

- ORDO\_PUBLIC int [ecb\\_init](#) (struct ECB\_STATE \*state, struct BLOCK\_STATE \*cipher\_state, const void \*iv, size\_t iv\_len, int dir, const struct [ECB\\_PARAMS](#) \*params)
- ORDO\_PUBLIC void [ecb\\_update](#) (struct ECB\_STATE \*state, struct BLOCK\_STATE \*cipher\_state, const void \*in, size\_t in\_len, void \*out, size\_t \*out\_len)
- ORDO\_PUBLIC int [ecb\\_final](#) (struct ECB\_STATE \*state, struct BLOCK\_STATE \*cipher\_state, void \*out, size\_t \*out\_len)
- ORDO\_PUBLIC size\_t [ecb\\_query](#) (prim\_t cipher, int query, size\_t value)
- ORDO\_PUBLIC size\_t [ecb\\_bsize](#) (void)

### 5.29.1 Detailed Description

Primitive. The ECB mode divides the input message into blocks of the cipher's block size, and encrypts them individually and independently. If the input message's length is not a multiple of the cipher's block size, a padding mechanism is enabled by default which will pad the message to the correct length (and remove the extra data upon decryption). Padding may be disabled via [ECB\\_PARAMS](#), putting constraints on the input message.

The ECB mode does not require an initialization vector.

Note that the ECB mode is insecure in almost all situations and is not recommended for general purpose use.

### 5.29.2 Function Documentation

5.29.2.1 `ORDO_PUBLIC int ecb_init ( struct ECB_STATE * state, struct BLOCK_STATE * cipher_state, const void * iv, size_t iv_len, int dir, const struct ECB_PARAMS * params )`

See Also

`block_mode_init()`

5.29.2.2 `ORDO_PUBLIC void ecb_update ( struct ECB_STATE * state, struct BLOCK_STATE * cipher_state, const void * in, size_t in_len, void * out, size_t * out_len )`

See Also

`block_mode_update()`

5.29.2.3 `ORDO_PUBLIC int ecb_final ( struct ECB_STATE * state, struct BLOCK_STATE * cipher_state, void * out, size_t * out_len )`

See Also

`block_mode_final()`

5.29.2.4 `ORDO_PUBLIC size_t ecb_query ( prim_t cipher, int query, size_t value )`

See Also

`block_mode_query()`

5.29.2.5 `ORDO_PUBLIC size_t ecb_bsize ( void )`

Gets the size in bytes of a `ECB_STATE`.

Returns

The size in bytes of the structure.

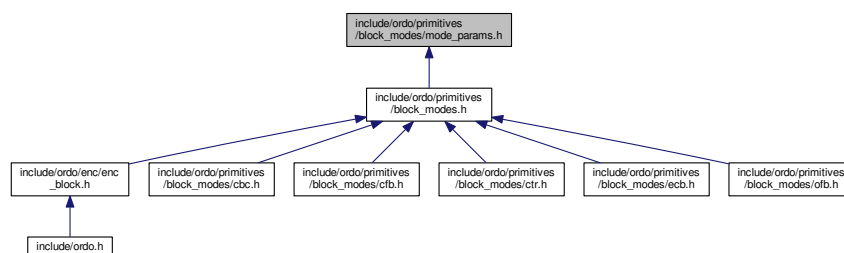
Remarks

Binary compatibility layer.

## 5.30 include/ordo/primitives/block\_modes/mode\_params.h File Reference

Primitive Parameters.

This graph shows which files directly or indirectly include this file:



## Data Structures

- struct [ECB\\_PARAMS](#)  
*ECB parameters.*
- struct [CBC\\_PARAMS](#)  
*CBC parameters.*
- union [BLOCK\\_MODE\\_PARAMS](#)  
*Polymorphic block mode parameter union.*

### 5.30.1 Detailed Description

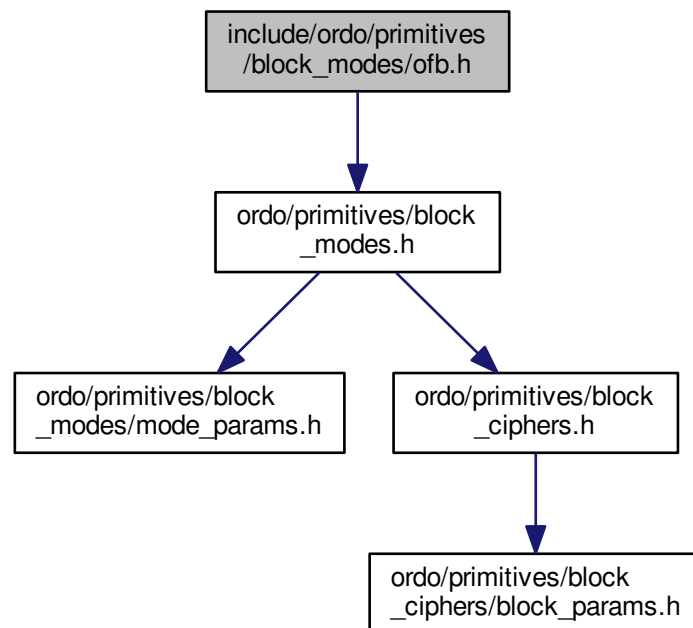
Primitive Parameters. This header contains parameter structures for all block modes.

### 5.31 include/ordo/primitives/block\_modes/ofb.h File Reference

Primitive.

```
#include "ordo/primitives/block_modes.h"
```

Include dependency graph for ofb.h:



## Functions

- ORDO\_PUBLIC int [ofb\\_init](#) (struct OFB\_STATE \*state, struct BLOCK\_STATE \*cipher\_state, const void \*iv, size\_t iv\_len, int dir, const void \*params)
- ORDO\_PUBLIC void [ofb\\_update](#) (struct OFB\_STATE \*state, struct BLOCK\_STATE \*cipher\_state, const void \*in, size\_t in\_len, void \*out, size\_t \*out\_len)

- ORDO\_PUBLIC int `ofb_final` (struct OFB\_STATE \*state, struct BLOCK\_STATE \*cipher\_state, void \*out, size\_t \*out\_len)
- ORDO\_PUBLIC size\_t `ofb_query` (prim\_t cipher, int query, size\_t value)
- ORDO\_PUBLIC size\_t `ofb_bsize` (void)

### 5.31.1 Detailed Description

Primitive. The OFB mode generates a keystream by repeatedly encrypting an initialization vector, effectively turning a block cipher into a stream cipher. As such, OFB mode requires no padding, and outlen will always be equal to inlen.

Note that the OFB keystream is independent of the plaintext, so a key/iv pair must never be used for more than one message. This also means the block cipher's inverse permutation is never used.

`ofb_final()` accepts 0 as an argument for `out_len` since by design the OFB mode of operation does not produce any final data. However, if a valid pointer is passed, its value will be set to zero as expected.

### 5.31.2 Function Documentation

5.31.2.1 ORDO\_PUBLIC int `ofb_init` ( struct OFB\_STATE \* state, struct BLOCK\_STATE \* cipher\_state, const void \* iv, size\_t iv\_len, int dir, const void \* params )

See Also

`block_mode_init()`

5.31.2.2 ORDO\_PUBLIC void `ofb_update` ( struct OFB\_STATE \* state, struct BLOCK\_STATE \* cipher\_state, const void \* in, size\_t in\_len, void \* out, size\_t \* out\_len )

See Also

`block_mode_update()`

5.31.2.3 ORDO\_PUBLIC int `ofb_final` ( struct OFB\_STATE \* state, struct BLOCK\_STATE \* cipher\_state, void \* out, size\_t \* out\_len )

See Also

`block_mode_final()`

5.31.2.4 ORDO\_PUBLIC size\_t `ofb_query` ( prim\_t cipher, int query, size\_t value )

See Also

`block_mode_query()`

5.31.2.5 ORDO\_PUBLIC size\_t `ofb_bsize` ( void )

Gets the size in bytes of an OFB\_STATE.

Returns

The size in bytes of the structure.

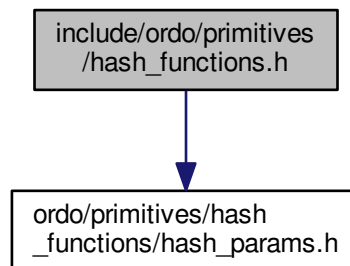
## Remarks

Binary compatibility layer.

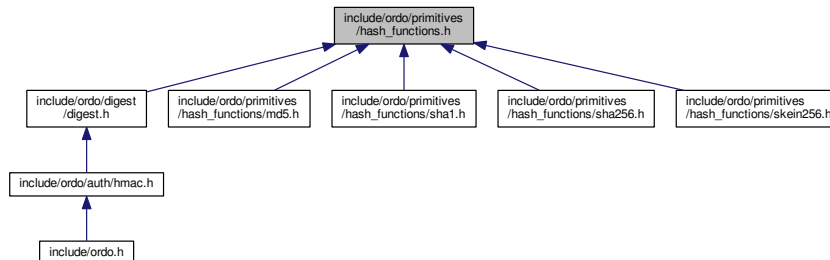
## 5.32 include/ordo/primitives/hash\_functions.h File Reference

Abstraction Layer.

```
#include "ordo/primitives/hash_functions/hash_params.h"
Include dependency graph for hash_functions.h:
```



This graph shows which files directly or indirectly include this file:



## Functions

- ORDO\_PUBLIC int [hash\\_init](#) (struct HASH\_STATE \*state, [prim\\_t](#) primitive, const void \*params)
- ORDO\_PUBLIC void [hash\\_update](#) (struct HASH\_STATE \*state, const void \*buffer, size\_t len)
- ORDO\_PUBLIC void [hash\\_final](#) (struct HASH\_STATE \*state, void \*digest)
- ORDO\_PUBLIC size\_t [hash\\_query](#) ([prim\\_t](#) primitive, int query, size\_t value)
- ORDO\_PUBLIC size\_t [hash\\_bsize](#) (void)

### 5.32.1 Detailed Description

Abstraction Layer. This abstraction layer declares all the hash functions and also makes them available to higher level modules - for a slightly more convenient wrapper to this interface, you can use [digest.h](#).



## 5.32.2 Function Documentation

### 5.32.2.1 ORDO\_PUBLIC int hash\_init ( struct HASH\_STATE \* state, prim\_t primitive, const void \* params )

Initializes a hash function state.

#### Parameters

in, out	<i>state</i>	A hash function state.
in	<i>primitive</i>	A hash function primitive.
in	<i>params</i>	Hash function specific parameters.

#### Returns

`ORDO_SUCCESS` on success, else an error code.

### 5.32.2.2 ORDO\_PUBLIC void hash\_update ( struct HASH\_STATE \* state, const void \* buffer, size\_t len )

Updates a hash function state by appending a buffer to the message this state is to calculate the cryptographic digest of.

#### Parameters

in, out	<i>state</i>	An initialized hash function state.
in	<i>buffer</i>	A buffer to append to the message.
in	<i>len</i>	The length, in bytes, of the buffer.

#### Remarks

This function has the property that doing `update (x)` followed by `update (y)` is equivalent to `update (x || y)`, where `||` denotes concatenation.

Passing a buffer of length zero is a no-op.

### 5.32.2.3 ORDO\_PUBLIC void hash\_final ( struct HASH\_STATE \* state, void \* digest )

Finalizes a hash function state, outputting the final digest.

#### Parameters

in, out	<i>state</i>	An initialized hash function state.
out	<i>digest</i>	A buffer in which to write the digest.

#### Remarks

The `digest` buffer should be as large as the hash function's digest length (unless you changed it via custom parameters).

### 5.32.2.4 ORDO\_PUBLIC size\_t hash\_query ( prim\_t primitive, int query, size\_t value )

Queries a hash function for suitable parameters.

#### Parameters

in	<i>primitive</i>	A hash function primitive.
in	<i>query</i>	A query code.
in	<i>value</i>	A suggested value.

### Returns

A suitable parameter of type `query` based on `value`.

### See Also

[query.h](#)

#### 5.32.2.5 ORDO\_PUBLIC size\_t hash\_bsize ( void )

Gets the size in bytes of a `HASH_STATE`.

### Returns

The size in bytes of the structure.

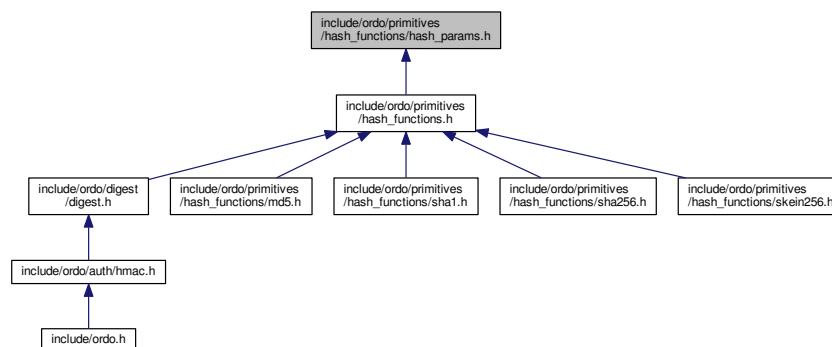
### Remarks

Binary compatibility layer.

## 5.33 include/ordo/primitives/hash\_functions/hash\_params.h File Reference

Primitive Parameters.

This graph shows which files directly or indirectly include this file:



## Data Structures

- struct [SKEIN256\\_PARAMS](#)  
*Skein-256 hash function parameters.*
- union [HASH\\_PARAMS](#)  
*Polymorphic hash function parameter union.*

## Macros

- `#define SKEIN256_PARAMS_DEFAULT`  
*The default Skein-256 configuration block.*

### 5.33.1 Detailed Description

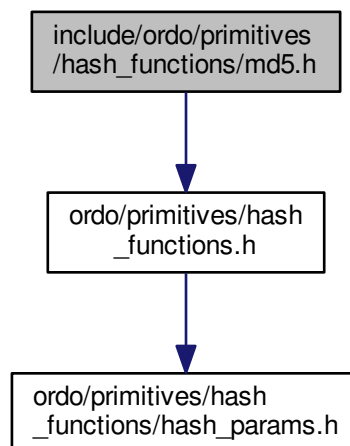
Primitive Parameters. This header contains parameter structures for all hash functions.

## 5.34 include/ordo/primitives/hash\_functions/md5.h File Reference

Primitive.

```
#include "ordo/primitives/hash_functions.h"
```

Include dependency graph for md5.h:



## Functions

- `ORDO_PUBLIC int md5_init` (struct MD5\_STATE \*state, const void \*params)
- `ORDO_PUBLIC void md5_update` (struct MD5\_STATE \*state, const void \*buffer, size\_t len)
- `ORDO_PUBLIC void md5_final` (struct MD5\_STATE \*state, void \*digest)
- `ORDO_PUBLIC size_t md5_query` (int query, size\_t value)
- `ORDO_PUBLIC size_t md5_bsize` (void)

### 5.34.1 Detailed Description

Primitive. The MD5 hash function, which produces a 128-bit digest.

## 5.34.2 Function Documentation

5.34.2.1 `ORDO_PUBLIC int md5_init ( struct MD5_STATE * state, const void * params )`

See Also

[hash\\_init\(\)](#)

Remarks

The `params` parameter is ignored.

5.34.2.2 `ORDO_PUBLIC void md5_update ( struct MD5_STATE * state, const void * buffer, size_t len )`

See Also

[hash\\_update\(\)](#)

5.34.2.3 `ORDO_PUBLIC void md5_final ( struct MD5_STATE * state, void * digest )`

See Also

[hash\\_final\(\)](#)

5.34.2.4 `ORDO_PUBLIC size_t md5_query ( int query, size_t value )`

See Also

[hash\\_query\(\)](#)

5.34.2.5 `ORDO_PUBLIC size_t md5_bsize ( void )`

Gets the size in bytes of an `MD5_STATE`.

Returns

The size in bytes of the structure.

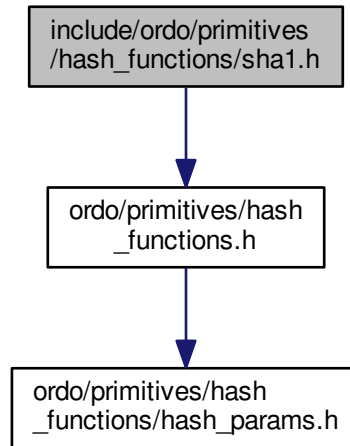
Remarks

Binary compatibility layer.

## 5.35 `include/ordo/primitives/hash_functions/sha1.h` File Reference

Primitive.

```
#include "ordo/primitives/hash_functions.h"
Include dependency graph for sha1.h:
```



## Functions

- ORDO\_PUBLIC int [sha1\\_init](#) (struct SHA1\_STATE \*state, const void \*params)
- ORDO\_PUBLIC void [sha1\\_update](#) (struct SHA1\_STATE \*state, const void \*buffer, size\_t len)
- ORDO\_PUBLIC void [sha1\\_final](#) (struct SHA1\_STATE \*state, void \*digest)
- ORDO\_PUBLIC size\_t [sha1\\_query](#) (int query, size\_t value)
- ORDO\_PUBLIC size\_t [sha1\\_bsize](#) (void)

### 5.35.1 Detailed Description

Primitive. The SHA-1 hash function, which produces a 160-bit digest.

### 5.35.2 Function Documentation

5.35.2.1 ORDO\_PUBLIC int [sha1\\_init](#) ( struct SHA1\_STATE \* *state*, const void \* *params* )

See Also

[hash\\_init\(\)](#)

Remarks

The `params` parameter is ignored.

5.35.2.2 ORDO\_PUBLIC void [sha1\\_update](#) ( struct SHA1\_STATE \* *state*, const void \* *buffer*, size\_t *len* )

See Also

[hash\\_update\(\)](#)

5.35.2.3 ORDO\_PUBLIC void sha1\_final ( struct SHA1\_STATE \* state, void \* digest )

See Also

[hash\\_final\(\)](#)

5.35.2.4 ORDO\_PUBLIC size\_t sha1\_query ( int query, size\_t value )

See Also

[hash\\_query\(\)](#)

5.35.2.5 ORDO\_PUBLIC size\_t sha1\_bsize ( void )

Gets the size in bytes of a SHA1\_STATE.

Returns

The size in bytes of the structure.

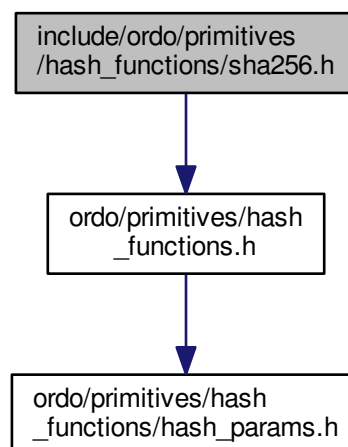
Remarks

Binary compatibility layer.

## 5.36 include/ordo/primitives/hash\_functions/sha256.h File Reference

Primitive.

```
#include "ordo/primitives/hash_functions.h"  
Include dependency graph for sha256.h:
```



## Functions

- ORDO\_PUBLIC int [sha256\\_init](#) (struct SHA256\_STATE \*state, const void \*params)
- ORDO\_PUBLIC void [sha256\\_update](#) (struct SHA256\_STATE \*state, const void \*buffer, size\_t len)
- ORDO\_PUBLIC void [sha256\\_final](#) (struct SHA256\_STATE \*state, void \*digest)
- ORDO\_PUBLIC size\_t [sha256\\_query](#) (int query, size\_t value)
- ORDO\_PUBLIC size\_t [sha256\\_bsize](#) (void)

### 5.36.1 Detailed Description

Primitive. The SHA-256 hash function, which produces a 256-bit digest.

### 5.36.2 Function Documentation

5.36.2.1 ORDO\_PUBLIC int [sha256\\_init](#) ( struct SHA256\_STATE \* *state*, const void \* *params* )

See Also

[hash\\_init\(\)](#)

Remarks

The `params` parameter is ignored.

5.36.2.2 ORDO\_PUBLIC void [sha256\\_update](#) ( struct SHA256\_STATE \* *state*, const void \* *buffer*, size\_t *len* )

See Also

[hash\\_update\(\)](#)

5.36.2.3 ORDO\_PUBLIC void [sha256\\_final](#) ( struct SHA256\_STATE \* *state*, void \* *digest* )

See Also

[hash\\_final\(\)](#)

5.36.2.4 ORDO\_PUBLIC size\_t [sha256\\_query](#) ( int *query*, size\_t *value* )

See Also

[hash\\_query\(\)](#)

5.36.2.5 ORDO\_PUBLIC size\_t [sha256\\_bsize](#) ( void )

Gets the size in bytes of a `SHA256_STATE`.

Returns

The size in bytes of the structure.

Remarks

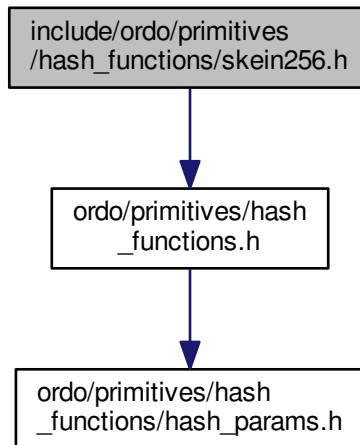
Binary compatibility layer.

## 5.37 include/ordo/primitives/hash\_functions/skein256.h File Reference

Primitive.

```
#include "ordo/primitives/hash_functions.h"
```

Include dependency graph for skein256.h:



### Functions

- ORDO\_PUBLIC int [skein256\\_init](#) (struct SKEIN256\_STATE \*state, const struct SKEIN256\_PARAMS \*params)
- ORDO\_PUBLIC void [skein256\\_update](#) (struct SKEIN256\_STATE \*state, const void \*buffer, size\_t len)
- ORDO\_PUBLIC void [skein256\\_final](#) (struct SKEIN256\_STATE \*state, void \*digest)
- ORDO\_PUBLIC size\_t [skein256\\_query](#) (int query, size\_t value)
- ORDO\_PUBLIC size\_t [skein256\\_bsize](#) (void)

#### 5.37.1 Detailed Description

Primitive. This is the Skein-256 hash function, which produces a 256-bit digest by default (but has parameters to output a longer digest) and has a 256-bit internal state. This implementation supports messages up to a length of  $2^{64} - 1$  bytes instead of the  $2^{96} - 1$  available, but we trust this will not be an issue. This is a rather flexible hash with lots of options. Currently, the only options supported are:

- free access to configuration block (in fact, [SKEIN256\\_PARAMS](#) is the configuration block, and a default one is used if not provided) with the exception of the output length which must remain 256 bits.

Note arbitrary output length used to be supported, but is no longer, since parameters should not leak through the interface, and this feature is also available in a more generic way via key stretching modules such as HKDF or DRBG.

#### 5.37.2 Function Documentation

5.37.2.1 ORDO\_PUBLIC int [skein256\\_init](#) ( struct SKEIN256\_STATE \* state, const struct SKEIN256\_PARAMS \* params )



## See Also

[hash\\_init\(\)](#)

## Return values

<a href="#">ORDO_ARG</a>	if parameters were provided, but requested an output length of zero bytes.
--------------------------	--

5.37.2.2 **ORDO\_PUBLIC** void `skein256_update` ( struct SKEIN256\_STATE \* *state*, const void \* *buffer*, size\_t *len* )

## See Also

[hash\\_update\(\)](#)

5.37.2.3 **ORDO\_PUBLIC** void `skein256_final` ( struct SKEIN256\_STATE \* *state*, void \* *digest* )

## See Also

[hash\\_final\(\)](#)

5.37.2.4 **ORDO\_PUBLIC** size\_t `skein256_query` ( int *query*, size\_t *value* )

## See Also

[hash\\_query\(\)](#)

5.37.2.5 **ORDO\_PUBLIC** size\_t `skein256_bsize` ( void )

Gets the size in bytes of a SKEIN256\_STATE.

## Returns

The size in bytes of the structure.

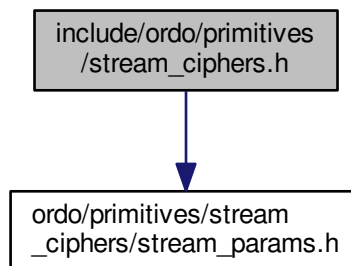
## Remarks

Binary compatibility layer.

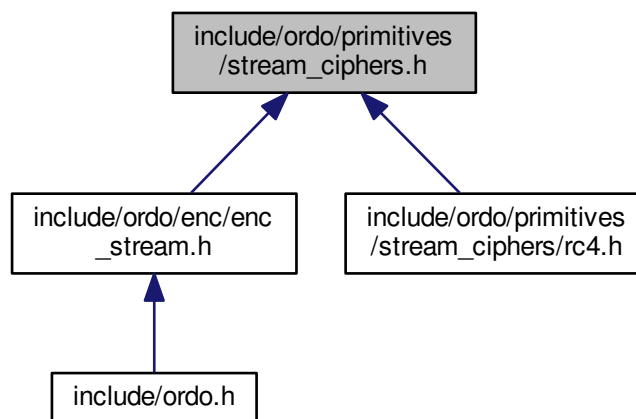
### 5.38 include/ordo/primitives/stream\_ciphers.h File Reference

Abstraction Layer.

```
#include "ordo/primitives/stream_ciphers/stream_params.h"
Include dependency graph for stream_ciphers.h:
```



This graph shows which files directly or indirectly include this file:



### Functions

- ORDO\_PUBLIC int [stream\\_init](#) (struct STREAM\_STATE \*state, const void \*key, size\_t key\_len, [prim\\_t](#) primitive, const void \*params)
- ORDO\_PUBLIC void [stream\\_update](#) (struct STREAM\_STATE \*state, void \*buffer, size\_t len)

- ORDO\_PUBLIC void [stream\\_final](#) (struct STREAM\_STATE \*state)
- ORDO\_PUBLIC size\_t [stream\\_query](#) (prim\_t primitive, int query, size\_t value)
- ORDO\_PUBLIC size\_t [stream\\_bsize](#) (void)

### 5.38.1 Detailed Description

Abstraction Layer. This abstraction layer declares all the stream ciphers and also makes them available to higher level modules. This does not actually do encryption at all but simply abstracts the stream cipher primitives - encryption modules are in the `enc` folder: [enc\\_stream.h](#).

### 5.38.2 Function Documentation

**5.38.2.1** ORDO\_PUBLIC int [stream\\_init](#) ( struct STREAM\_STATE \* *state*, const void \* *key*, size\_t *key\_len*, prim\_t *primitive*, const void \* *params* )

Initializes a stream cipher state.

#### Parameters

in, out	<i>state</i>	A stream cipher state.
in	<i>key</i>	The cryptographic key to use.
in	<i>key_len</i>	The length, in bytes, of the key.
in	<i>primitive</i>	A stream cipher primitive.
in	<i>params</i>	Stream cipher specific parameters.

#### Returns

[ORDO\\_SUCCESS](#) on success, else an error code.

**5.38.2.2** ORDO\_PUBLIC void [stream\\_update](#) ( struct STREAM\_STATE \* *state*, void \* *buffer*, size\_t *len* )

Encrypts or decrypts a buffer using a stream cipher state.

#### Parameters

in, out	<i>state</i>	An initialized stream cipher state.
in, out	<i>buffer</i>	The buffer to encrypt or decrypt.
in	<i>len</i>	The length, in bytes, of the buffer.

#### Remarks

Encryption and decryption are equivalent, and are done in place.

This function is stateful and will update the passed state (by generating keystream material), unlike block ciphers, which are deterministic permutations.

**5.38.2.3** ORDO\_PUBLIC void [stream\\_final](#) ( struct STREAM\_STATE \* *state* )

Finalizes a stream cipher state.

#### Parameters

<code>in, out</code>	<code>state</code>	An initialized stream cipher state.
----------------------	--------------------	-------------------------------------

#### 5.38.2.4 ORDO\_PUBLIC `size_t stream_query ( prim_t primitive, int query, size_t value )`

Queries a stream cipher for suitable parameters.

##### Parameters

<code>in</code>	<code>primitive</code>	A stream cipher primitive.
<code>in</code>	<code>query</code>	A query code.
<code>in</code>	<code>value</code>	A suggested value.

##### Returns

A suitable parameter of type `query` based on `value`.

##### See Also

[query.h](#)

#### 5.38.2.5 ORDO\_PUBLIC `size_t stream_bsize ( void )`

Gets the size in bytes of a `STREAM_STATE`.

##### Returns

The size in bytes of the structure.

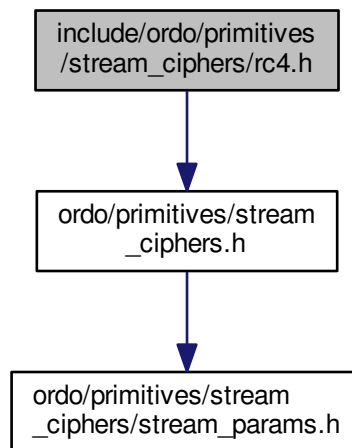
## Remarks

Binary compatibility layer.

## 5.39 include/ordo/primitives/stream\_ciphers/rc4.h File Reference

Primitive.

```
#include "ordo/primitives/stream_ciphers.h"  
Include dependency graph for rc4.h:
```



## Functions

- ORDO\_PUBLIC int [rc4\\_init](#) (struct RC4\_STATE \*state, const void \*key, size\_t key\_len, const struct [RC4\\_PARAMS](#) \*params)
- ORDO\_PUBLIC void [rc4\\_update](#) (struct RC4\_STATE \*state, void \*buffer, size\_t len)
- ORDO\_PUBLIC void [rc4\\_final](#) (struct RC4\_STATE \*state)
- ORDO\_PUBLIC size\_t [rc4\\_query](#) (int query, size\_t value)
- ORDO\_PUBLIC size\_t [rc4\\_bsize](#) (void)

### 5.39.1 Detailed Description

Primitive. RC4 is a stream cipher, which accepts keys between 40 and 2048 bits (in multiples of 8 bits only). It accepts a parameter consisting of the number of initial keystream bytes to drop immediately after key schedule, effectively implementing RC4-drop[n]. If no drop parameter is passed, the implementation drops 2048 bytes by default.

Be aware that even with a drop, it isn't secure to encrypt more than a few hundred megabytes of data with the same key (due to a distinguisher attack that can distinguish between an RC4 keystream and a random stream). If you are concerned, use a different algorithm or rekey at generous intervals.

### 5.39.2 Function Documentation

5.39.2.1 **ORDO\_PUBLIC** int rc4\_init ( struct RC4\_STATE \* *state*, const void \* *key*, size\_t *key\_len*, const struct RC4\_PARAMS \* *params* )

See Also

[stream\\_init\(\)](#)

Return values

<a href="#">ORDO_KEY_LEN</a>	if the key length was less than 40 bits (5 bytes) or more than 2048 bits (256 bytes).
------------------------------	---

Remarks

The amount of keystream bytes to drop can be set via the `params` argument, see [RC4\\_PARAMS](#). By default, 2048 bytes are dropped.

5.39.2.2 **ORDO\_PUBLIC** void rc4\_update ( struct RC4\_STATE \* *state*, void \* *buffer*, size\_t *len* )

See Also

[stream\\_update\(\)](#)

5.39.2.3 **ORDO\_PUBLIC** void rc4\_final ( struct RC4\_STATE \* *state* )

See Also

[stream\\_final\(\)](#)

5.39.2.4 **ORDO\_PUBLIC** size\_t rc4\_query ( int *query*, size\_t *value* )

See Also

[stream\\_query\(\)](#)

5.39.2.5 **ORDO\_PUBLIC** size\_t rc4\_bsize ( void )

Gets the size in bytes of an `RC4_STATE`.

Returns

The size in bytes of the structure.

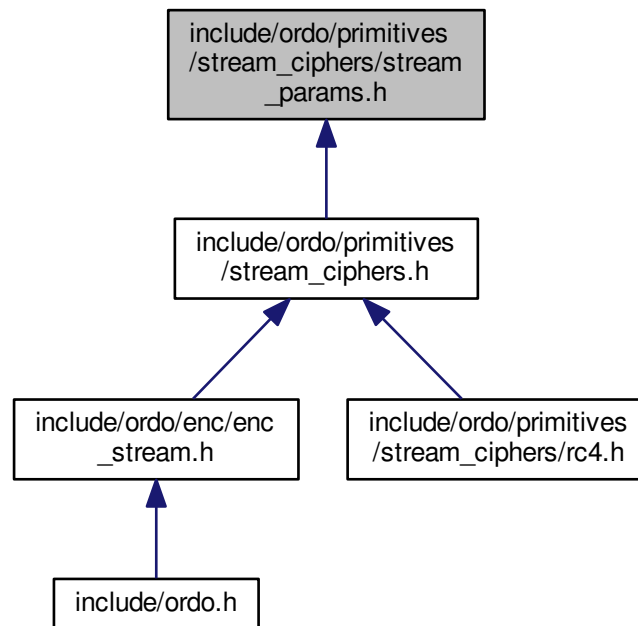
Remarks

Binary compatibility layer.

## 5.40 include/ordo/primitives/stream\_ciphers/stream\_params.h File Reference

Primitive Parameters.

This graph shows which files directly or indirectly include this file:



## Data Structures

- struct [RC4\\_PARAMS](#)  
*RC4 stream cipher parameters.*
- union [STREAM\\_PARAMS](#)  
*Polymorphic stream cipher parameter union.*

### 5.40.1 Detailed Description

Primitive Parameters. This header contains parameter structures for all stream ciphers.

# Index

- AES\_PARAMS, 9
  - rounds, 9
- aes.h
  - aes\_bsize, 57
  - aes\_final, 57
  - aes\_forward, 57
  - aes\_init, 56
  - aes\_inverse, 57
  - aes\_query, 57
- aes\_bsize
  - aes.h, 57
- aes\_final
  - aes.h, 57
- aes\_forward
  - aes.h, 57
- aes\_init
  - aes.h, 56
- aes\_inverse
  - aes.h, 57
- aes\_query
  - aes.h, 57
- alg.h
  - bits, 41
  - bytes, 41
  - inc\_buffer, 43
  - offset, 42
  - pad\_check, 42
  - xor\_buffer, 42
- arch
  - ORDO\_VERSION, 13
- BLOCK\_SIZE\_Q
  - query.h, 30
- BLOCK\_MODE\_PARAMS, 9
- BLOCK\_PARAMS, 10
- bits
  - alg.h, 41
- block\_bsize
  - block\_ciphers.h, 55
- block\_ciphers.h
  - block\_bsize, 55
  - block\_final, 53
  - block\_forward, 53
  - block\_init, 53
  - block\_inverse, 53
  - block\_query, 55
- block\_final
  - block\_ciphers.h, 53
- block\_forward
  - block\_ciphers.h, 53
- block\_init
  - block\_ciphers.h, 53
- block\_inverse
  - block\_ciphers.h, 53
- block\_mode\_bsize
  - block\_modes.h, 65
- block\_mode\_final
  - block\_modes.h, 64
- block\_mode\_init
  - block\_modes.h, 64
- block\_mode\_query
  - block\_modes.h, 65
- block\_mode\_update
  - block\_modes.h, 64
- block\_modes.h
  - block\_mode\_bsize, 65
  - block\_mode\_final, 64
  - block\_mode\_init, 64
  - block\_mode\_query, 65
  - block\_mode\_update, 64
- block\_query
  - block\_ciphers.h, 55
- build
  - ORDO\_VERSION, 13
- bytes
  - alg.h, 41
- CBC\_PARAMS, 11
  - padding, 11
- cbc.h
  - cbc\_bsize, 67
  - cbc\_final, 67
  - cbc\_init, 67
  - cbc\_query, 67
  - cbc\_update, 67
- cbc\_bsize
  - cbc.h, 67
- cbc\_final
  - cbc.h, 67
- cbc\_init
  - cbc.h, 67
- cbc\_query
  - cbc.h, 67
- cbc\_update
  - cbc.h, 67
- cfb.h
  - cfb\_bsize, 69
  - cfb\_final, 69
  - cfb\_init, 69
  - cfb\_query, 69



- cfb\_update, 69
- cfb\_bsize
  - cfb.h, 69
- cfb\_final
  - cfb.h, 69
- cfb\_init
  - cfb.h, 69
- cfb\_query
  - cfb.h, 69
- cfb\_update
  - cfb.h, 69
- ctcmp
  - utils.h, 51
- ctr.h
  - ctr\_bsize, 71
  - ctr\_final, 71
  - ctr\_init, 70
  - ctr\_query, 71
  - ctr\_update, 71
- ctr\_bsize
  - ctr.h, 71
- ctr\_final
  - ctr.h, 71
- ctr\_init
  - ctr.h, 70
- ctr\_query
  - ctr.h, 71
- ctr\_update
  - ctr.h, 71
- curve25519.h
  - curve25519\_ecdh, 49
  - curve25519\_gen, 47
  - curve25519\_pub, 47
- curve25519\_ecdh
  - curve25519.h, 49
- curve25519\_gen
  - curve25519.h, 47
- curve25519\_pub
  - curve25519.h, 47
- DIGEST\_LEN\_Q
  - query.h, 30
- digest.h
  - digest\_length, 34
  - ordo\_digest\_bsize, 34
  - ordo\_digest\_final, 34
  - ordo\_digest\_init, 33
  - ordo\_digest\_update, 33
- digest\_length
  - digest.h, 34
- drop
  - RC4\_PARAMS, 14
- ECB\_PARAMS, 11
  - padding, 11
- ecb.h
  - ecb\_bsize, 73
  - ecb\_final, 73
  - ecb\_init, 72
  - ecb\_query, 73
  - ecb\_update, 73
- ecb\_bsize
  - ecb.h, 73
- ecb\_final
  - ecb.h, 73
- ecb\_init
  - ecb.h, 72
- ecb\_query
  - ecb.h, 73
- ecb\_update
  - ecb.h, 73
- enc\_block.h
  - enc\_block\_bsize, 38
  - enc\_block\_final, 37
  - enc\_block\_init, 36
  - enc\_block\_iv\_len, 38
  - enc\_block\_key\_len, 38
  - enc\_block\_update, 37
- enc\_block\_bsize
  - enc\_block.h, 38
- enc\_block\_final
  - enc\_block.h, 37
- enc\_block\_init
  - enc\_block.h, 36
- enc\_block\_iv\_len
  - enc\_block.h, 38
- enc\_block\_key\_len
  - enc\_block.h, 38
- enc\_block\_update
  - enc\_block.h, 37
- enc\_stream.h
  - enc\_stream\_key\_len, 41
  - ordo\_enc\_stream\_bsize, 40
  - ordo\_enc\_stream\_final, 40
  - ordo\_enc\_stream\_init, 40
  - ordo\_enc\_stream\_update, 40
- enc\_stream\_key\_len
  - enc\_stream.h, 41
- error.h
  - ORDO\_ARG, 25
  - ORDO\_FAIL, 24
  - ORDO\_KEY\_LEN, 25
  - ORDO\_LEFTOVER, 25
  - ORDO\_PADDING, 25
  - ORDO\_SUCCESS, 24
- error.h
  - ORDO\_ERROR, 24
  - ordo\_error\_msg, 25
- feature\_list
  - ORDO\_VERSION, 13
- features
  - ORDO\_VERSION, 13
- HASH\_PARAMS, 12
- hash\_bsize
  - hash\_functions.h, 78
- hash\_final

- hash\_functions.h, 77
- hash\_functions.h
  - hash\_bsize, 78
  - hash\_final, 77
  - hash\_init, 77
  - hash\_query, 77
  - hash\_update, 77
- hash\_init
  - hash\_functions.h, 77
- hash\_query
  - hash\_functions.h, 77
- hash\_update
  - hash\_functions.h, 77
- hkdf.h
  - kdf\_hkdf, 44
- hmac.h
  - hmac\_bsize, 23
  - hmac\_final, 23
  - hmac\_init, 21
  - hmac\_update, 21
- hmac\_bsize
  - hmac.h, 23
- hmac\_final
  - hmac.h, 23
- hmac\_init
  - hmac.h, 21
- hmac\_update
  - hmac.h, 21
- IV\_LEN\_Q
  - query.h, 31
- id
  - ORDO\_VERSION, 13
- identification.h
  - PRIM\_TYPE, 26
  - PRIM\_UNKNOWN, 26
  - prim\_avail, 27
  - prim\_default, 28
  - prim\_from\_name, 27
  - prim\_name, 27
  - prim\_type, 27
  - prims\_by\_type, 28
- inc\_buffer
  - alg.h, 43
- include/ordo.h, 17
- include/ordo/auth/hmac.h, 20
- include/ordo/common/error.h, 24
- include/ordo/common/identification.h, 26
- include/ordo/common/interface.h, 28
- include/ordo/common/query.h, 29
- include/ordo/common/version.h, 31
- include/ordo/digest/digest.h, 32
- include/ordo/enc/enc\_block.h, 35
- include/ordo/enc/enc\_stream.h, 38
- include/ordo/internal/alg.h, 41
- include/ordo/internal/implementation.h, 43
- include/ordo/internal/sys.h, 43
- include/ordo/kdf/hkdf.h, 44
- include/ordo/kdf/pbkdf2.h, 45
- include/ordo/misc/curve25519.h, 47
- include/ordo/misc/endianness.h, 49
- include/ordo/misc/os\_random.h, 49
- include/ordo/misc/utils.h, 51
- include/ordo/primitives/block\_ciphers.h, 52
- include/ordo/primitives/block\_ciphers/aes.h, 56
- include/ordo/primitives/block\_ciphers/block\_params.h, 57
- include/ordo/primitives/block\_ciphers/nullcipher.h, 58
- include/ordo/primitives/block\_ciphers/threefish256.h, 60
- include/ordo/primitives/block\_modes.h, 62
- include/ordo/primitives/block\_modes/cbc.h, 66
- include/ordo/primitives/block\_modes/cfb.h, 68
- include/ordo/primitives/block\_modes/ctr.h, 69
- include/ordo/primitives/block\_modes/ecb.h, 71
- include/ordo/primitives/block\_modes/mode\_params.h, 73
- include/ordo/primitives/block\_modes/ofb.h, 74
- include/ordo/primitives/hash\_functions.h, 76
- include/ordo/primitives/hash\_functions/hash\_params.h, 78
- include/ordo/primitives/hash\_functions/md5.h, 79
- include/ordo/primitives/hash\_functions/sha1.h, 80
- include/ordo/primitives/hash\_functions/sha256.h, 82
- include/ordo/primitives/hash\_functions/skein256.h, 84
- include/ordo/primitives/stream\_ciphers.h, 86
- include/ordo/primitives/stream\_ciphers/rc4.h, 89
- include/ordo/primitives/stream\_ciphers/stream\_params.h, 90
- KEY\_LEN\_Q
  - query.h, 30
- kdf\_hkdf
  - hkdf.h, 44
- kdf\_pbkdf2
  - pbkdf2.h, 46
- md5.h
  - md5\_bsize, 80
  - md5\_final, 80
  - md5\_init, 80
  - md5\_query, 80
  - md5\_update, 80
- md5\_bsize
  - md5.h, 80
- md5\_final
  - md5.h, 80
- md5\_init
  - md5.h, 80
- md5\_query
  - md5.h, 80
- md5\_update
  - md5.h, 80
- nullcipher.h
  - nullcipher\_bsize, 60
  - nullcipher\_final, 60
  - nullcipher\_forward, 60
  - nullcipher\_init, 59

- nullcipher\_inverse, 60
  - nullcipher\_query, 60
- nullcipher\_bsize
  - nullcipher.h, 60
- nullcipher\_final
  - nullcipher.h, 60
- nullcipher\_forward
  - nullcipher.h, 60
- nullcipher\_init
  - nullcipher.h, 59
- nullcipher\_inverse
  - nullcipher.h, 60
- nullcipher\_query
  - nullcipher.h, 60
- ORDO\_ARG
  - error.h, 25
- ORDO\_FAIL
  - error.h, 24
- ORDO\_KEY\_LEN
  - error.h, 25
- ORDO\_LEFTOVER
  - error.h, 25
- ORDO\_PADDING
  - error.h, 25
- ORDO\_SUCCESS
  - error.h, 24
- ORDO\_ERROR
  - error.h, 24
- ORDO\_QUERY
  - query.h, 30
- ORDO\_VERSION, 12
  - arch, 13
  - build, 13
  - feature\_list, 13
  - features, 13
  - id, 13
  - system, 13
  - version, 13
- ofb.h
  - ofb\_bsize, 75
  - ofb\_final, 75
  - ofb\_init, 75
  - ofb\_query, 75
  - ofb\_update, 75
- ofb\_bsize
  - ofb.h, 75
- ofb\_final
  - ofb.h, 75
- ofb\_init
  - ofb.h, 75
- ofb\_query
  - ofb.h, 75
- ofb\_update
  - ofb.h, 75
- offset
  - alg.h, 42
- ordo.h
  - ordo\_digest, 19
  - ordo\_enc\_block, 18
  - ordo\_enc\_stream, 18
  - ordo\_hmac, 19
  - ordo\_digest
    - ordo.h, 19
  - ordo\_digest\_bsize
    - digest.h, 34
  - ordo\_digest\_final
    - digest.h, 34
  - ordo\_digest\_init
    - digest.h, 33
  - ordo\_digest\_update
    - digest.h, 33
  - ordo\_enc\_block
    - ordo.h, 18
  - ordo\_enc\_stream
    - ordo.h, 18
  - ordo\_enc\_stream\_bsize
    - enc\_stream.h, 40
  - ordo\_enc\_stream\_final
    - enc\_stream.h, 40
  - ordo\_enc\_stream\_init
    - enc\_stream.h, 40
  - ordo\_enc\_stream\_update
    - enc\_stream.h, 40
  - ordo\_error\_msg
    - error.h, 25
  - ordo\_hmac
    - ordo.h, 19
  - ordo\_version
    - version.h, 31
- os\_random
  - os\_random.h, 50
- os\_random.h
  - os\_random, 50
  - os\_secure\_random, 50
- os\_secure\_random
  - os\_random.h, 50
- out\_len
  - SKEIN256\_PARAMS, 15
- PRIM\_TYPE
  - identification.h, 26
- PRIM\_UNKNOWN
  - identification.h, 26
- pad\_check
  - alg.h, 42
- padding
  - CBC\_PARAMS, 11
  - ECB\_PARAMS, 11
- pbkdf2.h
  - kdf\_pbkdf2, 46
- prim\_avail
  - identification.h, 27
- prim\_default
  - identification.h, 28
- prim\_from\_name
  - identification.h, 27
- prim\_name

- identification.h, 27
- prim\_type
  - identification.h, 27
- prims\_by\_type
  - identification.h, 28
- query.h
  - BLOCK\_SIZE\_Q, 30
  - DIGEST\_LEN\_Q, 30
  - IV\_LEN\_Q, 31
  - KEY\_LEN\_Q, 30
- query.h
  - ORDO\_QUERY, 30
- RC4\_PARAMS, 13
  - drop, 14
- rc4.h
  - rc4\_bsize, 90
  - rc4\_final, 90
  - rc4\_init, 89
  - rc4\_query, 90
  - rc4\_update, 90
- rc4\_bsize
  - rc4.h, 90
- rc4\_final
  - rc4.h, 90
- rc4\_init
  - rc4.h, 89
- rc4\_query
  - rc4.h, 90
- rc4\_update
  - rc4.h, 90
- reserved
  - SKEIN256\_PARAMS, 15
- rounds
  - AES\_PARAMS, 9
- SKEIN256\_PARAMS, 14
  - out\_len, 15
  - reserved, 15
  - schema, 14
  - unused, 15
  - version, 14
- STREAM\_PARAMS, 15
- schema
  - SKEIN256\_PARAMS, 14
- sha1.h
  - sha1\_bsize, 82
  - sha1\_final, 81
  - sha1\_init, 81
  - sha1\_query, 82
  - sha1\_update, 81
- sha1\_bsize
  - sha1.h, 82
- sha1\_final
  - sha1.h, 81
- sha1\_init
  - sha1.h, 81
- sha1\_query
  - sha1.h, 82
- sha1\_update
  - sha1.h, 81
- sha256.h
  - sha256\_bsize, 83
  - sha256\_final, 83
  - sha256\_init, 83
  - sha256\_query, 83
  - sha256\_update, 83
- sha256\_bsize
  - sha256.h, 83
- sha256\_final
  - sha256.h, 83
- sha256\_init
  - sha256.h, 83
- sha256\_query
  - sha256.h, 83
- sha256\_update
  - sha256.h, 83
- skein256.h
  - skein256\_bsize, 85
  - skein256\_final, 85
  - skein256\_init, 84
  - skein256\_query, 85
  - skein256\_update, 85
- skein256\_bsize
  - skein256.h, 85
- skein256\_final
  - skein256.h, 85
- skein256\_init
  - skein256.h, 84
- skein256\_query
  - skein256.h, 85
- skein256\_update
  - skein256.h, 85
- stream\_bsize
  - stream\_ciphers.h, 88
- stream\_ciphers.h
  - stream\_bsize, 88
  - stream\_final, 87
  - stream\_init, 87
  - stream\_query, 88
  - stream\_update, 87
- stream\_final
  - stream\_ciphers.h, 87
- stream\_init
  - stream\_ciphers.h, 87
- stream\_query
  - stream\_ciphers.h, 88
- stream\_update
  - stream\_ciphers.h, 87
- system
  - ORDO\_VERSION, 13
- THREEFISH256\_PARAMS, 16
  - tweak, 16
- threefish256.h
  - threefish256\_bsize, 62
  - threefish256\_final, 62

- threefish256\_forward, [62](#)
- threefish256\_init, [61](#)
- threefish256\_inverse, [62](#)
- threefish256\_query, [62](#)
- threefish256\_bsize
  - threefish256.h, [62](#)
- threefish256\_final
  - threefish256.h, [62](#)
- threefish256\_forward
  - threefish256.h, [62](#)
- threefish256\_init
  - threefish256.h, [61](#)
- threefish256\_inverse
  - threefish256.h, [62](#)
- threefish256\_query
  - threefish256.h, [62](#)
- tweak
  - THREEFISH256\_PARAMS, [16](#)
- unused
  - SKEIN256\_PARAMS, [15](#)
- utils.h
  - ctcmp, [51](#)
- version
  - ORDO\_VERSION, [13](#)
  - SKEIN256\_PARAMS, [14](#)
- version.h
  - ordo\_version, [31](#)
- xor\_buffer
  - alg.h, [42](#)