

NAME

EVP_CIPHER-ARIA – The ARIA EVP_CIPHER implementations

DESCRIPTION

Support for ARIA symmetric encryption using the **EVP_CIPHER** API.

Algorithm Names

The following algorithms are available in the default provider:

“ARIA-128-CBC”, “ARIA-192-CBC” and “ARIA-256-CBC”
“ARIA-128-CFB”, “ARIA-192-CFB”, “ARIA-256-CFB”, “ARIA-128-CFB1”, “ARIA-192-CFB1”,
“ARIA-256-CFB1”, “ARIA-128-CFB8”, “ARIA-192-CFB8” and “ARIA-256-CFB8”
“ARIA-128-CTR”, “ARIA-192-CTR” and “ARIA-256-CTR”
“ARIA-128-ECB”, “ARIA-192-ECB” and “ARIA-256-ECB”
“AES-192-OCB”, “AES-128-OCB” and “AES-256-OCB”
“ARIA-128-OFB”, “ARIA-192-OFB” and “ARIA-256-OFB”
“ARIA-128-CCM”, “ARIA-192-CCM” and “ARIA-256-CCM”
“ARIA-128-GCM”, “ARIA-192-GCM” and “ARIA-256-GCM”

Parameters

This implementation supports the parameters described in “PARAMETERS” in **EVP_EncryptInit**(3).

SEE ALSO

provider-cipher(7), **OSSL_PROVIDER-default**(7)

COPYRIGHT

Copyright 2021 The OpenSSL Project Authors. All Rights Reserved.

Licensed under the Apache License 2.0 (the “License”). You may not use this file except in compliance with the License. You can obtain a copy in the file LICENSE in the source distribution or at [<https://www.openssl.org/source/license.html>](https://www.openssl.org/source/license.html).