*\*\**

*\* \file des.h*

*\**

*\* \brief DES block cipher*

*\**

*\* \warning DES is considered a weak cipher and its use constitutes a*

*\* security risk. We recommend considering stronger ciphers*

*\* instead.*

*\*/*

*/\**

*\* Copyright (C) 2006-2015, ARM Limited, All Rights Reserved*

*\* SPDX-License-Identifier: Apache-2.0*

*\**

*\* Licensed under the Apache License, Version 2.0 (the "License"); you may*

*\* not use this file except in compliance with the License.*

*\* You may obtain a copy of the License at*

*\**

*\** <http://www.apache.org/licenses/LICENSE-2.0>

*\**

*\* Unless required by applicable law or agreed to in writing, software*

*\* distributed under the License is distributed on an "AS IS" BASIS, WITHOUT*

*\* WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.*

*\* See the License for the specific language governing permissions and*

*\* limitations under the License.*

*\**

*\* This file is part of mbed TLS (*[https://tls.mbed.org](https://tls.mbed.org/)*)*

*\**

*\*/*

**#ifndef** MBEDTLS\_DES\_H

**#define** MBEDTLS\_DES\_H

**#if** !**defined**(MBEDTLS\_CONFIG\_FILE)

**#include** "config.h"

**#else**

**#include** MBEDTLS\_CONFIG\_FILE

**#endif**

**#include** <stddef.h>

**#include** <stdint.h>

**#define** MBEDTLS\_DES\_ENCRYPT 1

**#define** MBEDTLS\_DES\_DECRYPT 0

**#define** MBEDTLS\_ERR\_DES\_INVALID\_INPUT\_LENGTH -0x0032 */\*\*< The data input has an invalid length. \*/*

*/\* MBEDTLS\_ERR\_DES\_HW\_ACCEL\_FAILED is deprecated and should not be used. \*/*

**#define** MBEDTLS\_ERR\_DES\_HW\_ACCEL\_FAILED -0x0033 */\*\*< DES hardware accelerator failed. \*/*

**#define** MBEDTLS\_DES\_KEY\_SIZE 8

**#ifdef** \_\_cplusplus

**extern** "C" {

**#endif**

**#if** !**defined**(MBEDTLS\_DES\_ALT)

*// Regular implementation*

*//*

*/\*\**

*\* \brief DES context structure*

*\**

*\* \warning DES is considered a weak cipher and its use constitutes a*

*\* security risk. We recommend considering stronger ciphers*

*\* instead.*

*\*/*

**typedef** **struct** mbedtls\_des\_context

{

uint32\_t sk[32]; */\*!< DES subkeys \*/*

}

mbedtls\_des\_context;

*/\*\**

*\* \brief Triple-DES context structure*

*\*/*

**typedef** **struct** mbedtls\_des3\_context

{

uint32\_t sk[96]; */\*!< 3DES subkeys \*/*

}

mbedtls\_des3\_context;

**#else** */\* MBEDTLS\_DES\_ALT \*/*

**#include** "des\_alt.h"

**#endif** */\* MBEDTLS\_DES\_ALT \*/*

*/\*\**

*\* \brief Initialize DES context*

*\**

*\* \param ctx DES context to be initialized*

*\**

*\* \warning DES is considered a weak cipher and its use constitutes a*

*\* security risk. We recommend considering stronger ciphers*

*\* instead.*

*\*/*

void **mbedtls\_des\_init**( mbedtls\_des\_context \*ctx );

*/\*\**

*\* \brief Clear DES context*

*\**

*\* \param ctx DES context to be cleared*

*\**

*\* \warning DES is considered a weak cipher and its use constitutes a*

*\* security risk. We recommend considering stronger ciphers*

*\* instead.*

*\*/*

void **mbedtls\_des\_free**( mbedtls\_des\_context \*ctx );

*/\*\**

*\* \brief Initialize Triple-DES context*

*\**

*\* \param ctx DES3 context to be initialized*

*\*/*

void **mbedtls\_des3\_init**( mbedtls\_des3\_context \*ctx );

*/\*\**

*\* \brief Clear Triple-DES context*

*\**

*\* \param ctx DES3 context to be cleared*

*\*/*

void **mbedtls\_des3\_free**( mbedtls\_des3\_context \*ctx );

*/\*\**

*\* \brief Set key parity on the given key to odd.*

*\**

*\* DES keys are 56 bits long, but each byte is padded with*

*\* a parity bit to allow verification.*

*\**

*\* \param key 8-byte secret key*

*\**

*\* \warning DES is considered a weak cipher and its use constitutes a*

*\* security risk. We recommend considering stronger ciphers*

*\* instead.*

*\*/*

void **mbedtls\_des\_key\_set\_parity**( unsigned char key[MBEDTLS\_DES\_KEY\_SIZE] );

*/\*\**

*\* \brief Check that key parity on the given key is odd.*

*\**

*\* DES keys are 56 bits long, but each byte is padded with*

*\* a parity bit to allow verification.*

*\**

*\* \param key 8-byte secret key*

*\**

*\* \return 0 is parity was ok, 1 if parity was not correct.*

*\**

*\* \warning DES is considered a weak cipher and its use constitutes a*

*\* security risk. We recommend considering stronger ciphers*

*\* instead.*

*\*/*

int **mbedtls\_des\_key\_check\_key\_parity**( **const** unsigned char key[MBEDTLS\_DES\_KEY\_SIZE] );

*/\*\**

*\* \brief Check that key is not a weak or semi-weak DES key*

*\**

*\* \param key 8-byte secret key*

*\**

*\* \return 0 if no weak key was found, 1 if a weak key was identified.*

*\**

*\* \warning DES is considered a weak cipher and its use constitutes a*

*\* security risk. We recommend considering stronger ciphers*

*\* instead.*

*\*/*

int **mbedtls\_des\_key\_check\_weak**( **const** unsigned char key[MBEDTLS\_DES\_KEY\_SIZE] );

*/\*\**

*\* \brief DES key schedule (56-bit, encryption)*

*\**

*\* \param ctx DES context to be initialized*

*\* \param key 8-byte secret key*

*\**

*\* \return 0*

*\**

*\* \warning DES is considered a weak cipher and its use constitutes a*

*\* security risk. We recommend considering stronger ciphers*

*\* instead.*

*\*/*

int **mbedtls\_des\_setkey\_enc**( mbedtls\_des\_context \*ctx, **const** unsigned char key[MBEDTLS\_DES\_KEY\_SIZE] );

*/\*\**

*\* \brief DES key schedule (56-bit, decryption)*

*\**

*\* \param ctx DES context to be initialized*

*\* \param key 8-byte secret key*

*\**

*\* \return 0*

*\**

*\* \warning DES is considered a weak cipher and its use constitutes a*

*\* security risk. We recommend considering stronger ciphers*

*\* instead.*

*\*/*

int **mbedtls\_des\_setkey\_dec**( mbedtls\_des\_context \*ctx, **const** unsigned char key[MBEDTLS\_DES\_KEY\_SIZE] );

*/\*\**

*\* \brief Triple-DES key schedule (112-bit, encryption)*

*\**

*\* \param ctx 3DES context to be initialized*

*\* \param key 16-byte secret key*

*\**

*\* \return 0*

*\*/*

int **mbedtls\_des3\_set2key\_enc**( mbedtls\_des3\_context \*ctx,

**const** unsigned char key[MBEDTLS\_DES\_KEY\_SIZE \* 2] );

*/\*\**

*\* \brief Triple-DES key schedule (112-bit, decryption)*

*\**

*\* \param ctx 3DES context to be initialized*

*\* \param key 16-byte secret key*

*\**

*\* \return 0*

*\*/*

int **mbedtls\_des3\_set2key\_dec**( mbedtls\_des3\_context \*ctx,

**const** unsigned char key[MBEDTLS\_DES\_KEY\_SIZE \* 2] );

*/\*\**

*\* \brief Triple-DES key schedule (168-bit, encryption)*

*\**

*\* \param ctx 3DES context to be initialized*

*\* \param key 24-byte secret key*

*\**

*\* \return 0*

*\*/*

int **mbedtls\_des3\_set3key\_enc**( mbedtls\_des3\_context \*ctx,

**const** unsigned char key[MBEDTLS\_DES\_KEY\_SIZE \* 3] );

*/\*\**

*\* \brief Triple-DES key schedule (168-bit, decryption)*

*\**

*\* \param ctx 3DES context to be initialized*

*\* \param key 24-byte secret key*

*\**

*\* \return 0*

*\*/*

int **mbedtls\_des3\_set3key\_dec**( mbedtls\_des3\_context \*ctx,

**const** unsigned char key[MBEDTLS\_DES\_KEY\_SIZE \* 3] );

*/\*\**

*\* \brief DES-ECB block encryption/decryption*

*\**

*\* \param ctx DES context*

*\* \param input 64-bit input block*

*\* \param output 64-bit output block*

*\**

*\* \return 0 if successful*

*\**

*\* \warning DES is considered a weak cipher and its use constitutes a*

*\* security risk. We recommend considering stronger ciphers*

*\* instead.*

*\*/*

int **mbedtls\_des\_crypt\_ecb**( mbedtls\_des\_context \*ctx,

**const** unsigned char input[8],

unsigned char output[8] );

**#if** **defined**(MBEDTLS\_CIPHER\_MODE\_CBC)

*/\*\**

*\* \brief DES-CBC buffer encryption/decryption*

*\**

*\* \note Upon exit, the content of the IV is updated so that you can*

*\* call the function same function again on the following*

*\* block(s) of data and get the same result as if it was*

*\* encrypted in one call. This allows a "streaming" usage.*

*\* If on the other hand you need to retain the contents of the*

*\* IV, you should either save it manually or use the cipher*

*\* module instead.*

*\**

*\* \param ctx DES context*

*\* \param mode MBEDTLS\_DES\_ENCRYPT or MBEDTLS\_DES\_DECRYPT*

*\* \param length length of the input data*

*\* \param iv initialization vector (updated after use)*

*\* \param input buffer holding the input data*

*\* \param output buffer holding the output data*

*\**

*\* \warning DES is considered a weak cipher and its use constitutes a*

*\* security risk. We recommend considering stronger ciphers*

*\* instead.*

*\*/*

int **mbedtls\_des\_crypt\_cbc**( mbedtls\_des\_context \*ctx,

int mode,

size\_t length,

unsigned char iv[8],

**const** unsigned char \*input,

unsigned char \*output );

**#endif** */\* MBEDTLS\_CIPHER\_MODE\_CBC \*/*

*/\*\**

*\* \brief 3DES-ECB block encryption/decryption*

*\**

*\* \param ctx 3DES context*

*\* \param input 64-bit input block*

*\* \param output 64-bit output block*

*\**

*\* \return 0 if successful*

*\*/*

int **mbedtls\_des3\_crypt\_ecb**( mbedtls\_des3\_context \*ctx,

**const** unsigned char input[8],

unsigned char output[8] );

**#if** **defined**(MBEDTLS\_CIPHER\_MODE\_CBC)

*/\*\**

*\* \brief 3DES-CBC buffer encryption/decryption*

*\**

*\* \note Upon exit, the content of the IV is updated so that you can*

*\* call the function same function again on the following*

*\* block(s) of data and get the same result as if it was*

*\* encrypted in one call. This allows a "streaming" usage.*

*\* If on the other hand you need to retain the contents of the*

*\* IV, you should either save it manually or use the cipher*

*\* module instead.*

*\**

*\* \param ctx 3DES context*

*\* \param mode MBEDTLS\_DES\_ENCRYPT or MBEDTLS\_DES\_DECRYPT*

*\* \param length length of the input data*

*\* \param iv initialization vector (updated after use)*

*\* \param input buffer holding the input data*

*\* \param output buffer holding the output data*

*\**

*\* \return 0 if successful, or MBEDTLS\_ERR\_DES\_INVALID\_INPUT\_LENGTH*

*\*/*

int **mbedtls\_des3\_crypt\_cbc**( mbedtls\_des3\_context \*ctx,

int mode,

size\_t length,

unsigned char iv[8],

**const** unsigned char \*input,

unsigned char \*output );

**#endif** */\* MBEDTLS\_CIPHER\_MODE\_CBC \*/*

*/\*\**

*\* \brief Internal function for key expansion.*

*\* (Only exposed to allow overriding it,*

*\* see MBEDTLS\_DES\_SETKEY\_ALT)*

*\**

*\* \param SK Round keys*

*\* \param key Base key*

*\**

*\* \warning DES is considered a weak cipher and its use constitutes a*

*\* security risk. We recommend considering stronger ciphers*

*\* instead.*

*\*/*

void **mbedtls\_des\_setkey**( uint32\_t SK[32],

**const** unsigned char key[MBEDTLS\_DES\_KEY\_SIZE] );

*/\*\**

*\* \brief Checkup routine*

*\**

*\* \return 0 if successful, or 1 if the test failed*

*\*/*

int **mbedtls\_des\_self\_test**( int verbose );

**#ifdef** \_\_cplusplus

}

**#endif**

**#endif** */\* des.h \*/*